Citrix Endpoint Management

Citrix Endpoint Management es una solución para la administración de puntos finales, que ofrece funciones de administración de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM). Con Citrix Endpoint Management, puede administrar las directivas de dispositivos y aplicaciones, y entregar aplicaciones a los usuarios. La información de su empresa permanece protegida con una seguridad estricta para la identidad, los dispositivos, las aplicaciones, los datos y las redes.

Responsabilidades de Citrix® y del cliente

Citrix Cloud Operations se encarga de varias tareas de infraestructura y supervisión. Como resultado, puede centrarse en la experiencia del usuario y en la administración de dispositivos, aplicaciones y directivas.

Responsabilidades de Citrix:

- Nodos del servidor de Citrix Endpoint Management
- Integración y configuración inicial de NetScaler Gateway (servicio o local)
- Equilibrador de carga de NetScaler Gateway
- Base de datos
- Configuración del software Cloud Connector
- Integración de autenticación SAML con ShareFile
- Supervisión del sitio de Citrix Endpoint Management: Instancia, base de datos, conectividad empresarial (LDAP), túnel VPN (si corresponde), certificado SSL público, licencias de Citrix Endpoint Management

Responsabilidades del cliente:

- Administración y actualizaciones de NetScaler Gateway (local)
- Máquinas donde están instalados Cloud Connectors y Gateway Connector (para el servicio Citrix Gateway)
- LDAP/Active Directory

- DNS
- ShareFile: Configuración inicial de ShareFile, instalación del controlador de zonas de almacenamiento local, actualizaciones de Citrix Files
- Configuración de Citrix Endpoint Management: Dispositivos, directivas, aplicaciones, grupos de entrega, acciones y certificados de cliente

Integración con Microsoft Endpoint Manager

Citrix Endpoint Management se integra con Microsoft Endpoint Manager (MEM). Esa integración añade el valor de la micro VPN de Citrix Endpoint Management a las aplicaciones compatibles con Microsoft Intune, como el navegador Microsoft Edge. Con la integración, puede:

- Proteja las aplicaciones de Office 365 con acceso condicional con Azure AD. Para obtener más información, consulte Integrar con el acceso condicional de Azure AD.
- Envuelva sus propias aplicaciones de línea de negocio con Intune y Citrix para proporcionar capacidades de micro VPN dentro de un contenedor de administración de aplicaciones móviles (MAM) de Intune.
- Administre y entregue aplicaciones de Office 365, aplicaciones de línea de negocio y Citrix Secure Mail en un solo contenedor. Este método de administración proporciona la máxima seguridad y productividad. Por ejemplo, puede:
    - Bloquear dispositivos o sistemas operativos individuales
    - Personalizar las directivas de ActiveSync según los dispositivos, usuarios o grupos de usuarios
    - Poner en cuarentena a nivel de dispositivo
    - Supervisar conexiones o dispositivos individuales
    - Evitar los riesgos de seguridad del almacenamiento en caché de credenciales y datos

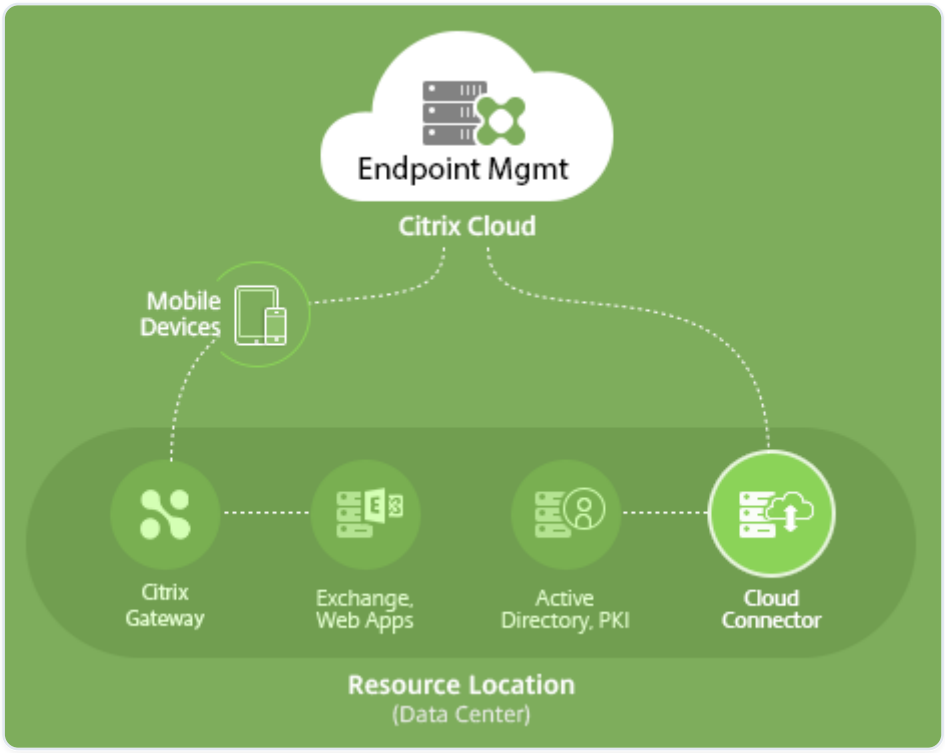
Utilice Citrix Endpoint Management MDM+MAM o Intune MDM para administrar dispositivos. Para obtener más información, consulte Integración de Citrix Endpoint Management con Microsoft Endpoint Manager.

Cloud Connector y ubicaciones de recursos

Se conecta a Citrix Endpoint Management a través de Cloud Connector. Cloud Connector sirve como canal de comunicación entre Citrix Cloud y sus ubicaciones de recursos. Cloud Connector

permite la administración en la nube sin necesidad de configuraciones complejas de red o infraestructura, como VPN o túneles IPsec.

Las ubicaciones de recursos tienen los recursos necesarios para ofrecer servicios a sus suscriptores. Para Citrix Endpoint Management, las ubicaciones de recursos son sus servidores NetScaler Gateway, LDAP, DNS y PKI.



Para obtener más información sobre Cloud Connector y las ubicaciones de recursos, consulte Acerca de Citrix Endpoint Management.

Primeros pasos con Citrix Endpoint Management

Sugerencia:

XenMobile® Migration Service

Si utiliza XenMobile Server localmente, nuestro XenMobile Migration Service puede ayudarle a empezar con Citrix Endpoint Management. La migración de XenMobile Server a Citrix Endpoint Management no requiere que vuelva a inscribir los dispositivos.

Para obtener más información, póngase en contacto con su comercial de Citrix local, ingeniero de sistemas o socio de Citrix.

> Para obtener más información sobre nuestro servicio de migración, consulte 3 razones para pasarse al servicio Citrix Endpoint Management.

> Para saber por qué migrar, cómo migrar y los beneficios de migrar a Citrix Endpoint Management, visite el Catálogo de cursos del servicio de migración de CEM, o consulte la guía Servicio de migración de Citrix Endpoint Management (CEM).

> Cuando evalúa o compra Citrix Endpoint Management, el equipo de operaciones de Citrix Endpoint Management proporciona ayuda continua para la incorporación. El equipo de operaciones también se comunica con usted para asegurarse de que los servicios principales de Citrix Endpoint Management se ejecutan y configuran correctamente. Esta figura muestra los pasos de incorporación.



Para registrarse en una cuenta de Citrix y solicitar una prueba de Citrix Endpoint Management, póngase en contacto con su representante de ventas de Citrix. Cuando esté listo para continuar, vaya a https://onboarding.cloud.com.

Para una descripción general rápida de la incorporación y configuración de Citrix Endpoint Management, vea este vídeo.

<iframe src="https://www.youtube.com/embed/ycFLYxn7aII" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
¿Quiere saber más antes de empezar? Pruebe estos recursos:

Documentación de Citrix Endpoint Management: Proporciona la documentación completa de Citrix Endpoint Management, desde la incorporación hasta la configuración inicial y la configuración avanzada. Un artículo de "Novedades" describe las nuevas funciones y correcciones. Citrix le notifica cuando ese artículo está disponible para una nueva versión.

Manual de incorporación de Citrix Endpoint Management**:** Consolida toda la información disponible sobre Citrix Endpoint Management, para que pueda seguir habilitando e incorporando Citrix

Endpoint Management sin problemas. Puede utilizar el documento para registrar los cambios de sus procesos internos y para documentar sus diseños funcionales y de alto nivel.

Manual de implementación de Citrix Endpoint Management**:** La planificación de una implementación de Citrix Endpoint Management implica muchas consideraciones. El manual incluye recomendaciones, preguntas frecuentes y casos de uso para su entorno de Citrix Endpoint Management.

SalesIQ**:** Más recursos para nuestros socios de Citrix.

Pasos siguientes

Para obtener información sobre el proceso de incorporación de Citrix Endpoint Management, consulte Incorporación y configuración de recursos.

Una vez que haya completado la incorporación, consulte Preparar la inscripción de dispositivos y la entrega de recursos.

Anuncios de desuso

Para obtener un aviso anticipado de las funciones de Citrix Endpoint Management que se están eliminando progresivamente, consulte Desuso.

Soporte de Citrix Endpoint Management

Para obtener detalles sobre cómo acceder a la información y las herramientas relacionadas con el soporte en la consola de Citrix Endpoint Management, consulte Supervisar y dar soporte.

Las actualizaciones continuas de la versión de Citrix Endpoint Management se producen aproximadamente cada dos semanas. Para usted, el cliente, este proceso es transparente. Las actualizaciones iniciales se aplican solo a los sitios internos de Citrix y luego se aplican a los entornos de los clientes de forma gradual. Entregamos las actualizaciones de forma incremental en oleadas para garantizar la calidad del producto y maximizar la disponibilidad.

Los clientes de Citrix Endpoint Management reciben actualizaciones y comunicaciones directamente del equipo de operaciones en la nube de Citrix Endpoint Management. Esas actualizaciones le mantienen al día con las nuevas funciones, los problemas conocidos, los problemas solucionados, etc.

El equipo de operaciones en la nube de Citrix mantiene los entornos de Citrix Endpoint Management con los últimos parches acumulativos de Citrix Endpoint Management. Para obtener parches o correcciones específicos que se requieran antes del parche acumulativo, póngase en contacto con el Soporte técnico de Citrix.

Si tiene algún problema con su entorno, póngase en contacto con el Soporte técnico de Citrix o con su equipo de cuentas de Citrix. Estos problemas pueden incluir la inscripción de dispositivos móviles, el acceso a la consola de Citrix Endpoint Management o problemas con Citrix Secure Mail.

Si necesita alguna integración o cambio en NetScaler Gateway en la nube o en Citrix Endpoint Management, envíe una solicitud a través del Soporte técnico de Citrix.

Estos son algunos ejemplos de cambios que puede solicitar:

- Integración de Citrix Files con NetScaler Gateway en la nube
- Cambiar el tipo de autenticación de NetScaler Gateway
- Validar la conectividad con los recursos del centro de datos del cliente
- Cambiar la configuración de túnel dividido para micro VPN
- Reiniciar los componentes de Citrix Endpoint Management debido a algunos cambios en la configuración del servidor

Acuerdo de nivel de servicio

Citrix Endpoint Management utiliza las mejores prácticas del sector para lograr la escala de la nube y un alto grado de disponibilidad del servicio.

Para obtener todos los detalles sobre el compromiso de Citrix con la disponibilidad de los servicios de Citrix Cloud, consulte el Acuerdo de nivel de servicio.

Novedades

Citrix tiene como objetivo ofrecer nuevas funciones y actualizaciones de productos a los clientes de Citrix Endpoint Management cuando estén disponibles. Las nuevas versiones aportan más valor, por lo que no hay razón para retrasar las actualizaciones.

- Las actualizaciones continuas de Citrix Endpoint Management se publican aproximadamente cada tres meses.
- Estas actualizaciones no provocan ningún tiempo de inactividad para su instancia o para los usuarios de dispositivos.
- No todas las versiones tienen nuevas funciones y algunas actualizaciones incluyen correcciones y mejoras de rendimiento.

Para usted, el cliente, este proceso es transparente. Aplicamos las actualizaciones iniciales solo a los sitios internos de Citrix®, y luego a los entornos de los clientes de forma gradual. La entrega incremental de actualizaciones por fases ayuda a garantizar la calidad del producto y a maximizar la disponibilidad.

También recibe actualizaciones y comunicaciones de Citrix Endpoint Management directamente del equipo de operaciones en la nube de Citrix Endpoint Management. Esas actualizaciones le mantienen al día sobre las nuevas funciones, los problemas conocidos, los problemas resueltos, etc.

Para obtener más detalles, incluida la escala de la nube y la disponibilidad del servicio, consulte el Acuerdo de Nivel de Servicio de Citrix Endpoint Management. Para supervisar las interrupciones del servicio y el mantenimiento programado, consulte el Panel de estado del servicio.

Citrix Endpoint Management 26.8.0

- **Compatibilidad con la instalación de actualizaciones de seguridad en la directiva de dispositivos de configuración de actualizaciones de software:** Se ha añadido una nueva configuración, **Instalar actualizaciones de seguridad**, a la directiva de dispositivos de configuración de actualizaciones de software para dispositivos iOS. Esta configuración especifica si el usuario puede controlar la instalación automática de las actualizaciones de seguridad disponibles. Esta función está disponible para iOS 18 y versiones posteriores. El

valor predeterminado es **Permitido**. Para obtener más información, consulte la directiva de dispositivos de configuración de actualizaciones de software.

- **Compatibilidad con la directiva de dispositivos de configuración de aplicaciones:** Se ha añadido una nueva directiva de dispositivos, **Configuración de aplicaciones**, en **Configuraciones (declarativas)**. Esta directiva le permite configurar listas de aplicaciones permitidas y denegadas mediante la gestión declarativa de dispositivos de Apple. Esta directiva solo es compatible con dispositivos iOS 27 y versiones posteriores supervisados. Para obtener más información, consulte la directiva de dispositivos de configuración de aplicaciones.
- **Compatibilidad con la directiva de dispositivos de configuración de inteligencia externa:** Se ha añadido una nueva directiva de dispositivos, **Configuración de inteligencia externa**, en **Configuraciones (declarativas)**. Esta directiva le permite gestionar integraciones de IA externas en dispositivos iOS 26.4 y versiones posteriores supervisados. Para obtener más información, consulte la directiva de dispositivos de configuración de inteligencia externa.
- **Compatibilidad con la directiva de dispositivos de configuración de inteligencia:** Se ha añadido una nueva directiva de dispositivos, **Configuración de inteligencia**, en **Configuraciones (declarativas)**. Esta directiva le permite gestionar las funciones de Apple Intelligence en dispositivos iOS 26.4 y versiones posteriores supervisados. Para obtener más información, consulte la directiva de dispositivos de configuración de inteligencia.
- **Compatibilidad con iOS 27:** Citrix Endpoint Management y las aplicaciones de productividad de Citrix Mobile ahora son compatibles con iOS 27.
- **Renovación del certificado APNs de Secure Hub:** El certificado del servicio de notificaciones push de Apple (APNs) de Secure Hub para Citrix Endpoint Management 26.5 caduca el November 9, 2026. Esta actualización renueva automáticamente el certificado APNs de Secure Hub a un nuevo certificado, válido hasta el September 18, 2027.
- **Desaprobación del modo de administrador de dispositivos heredados de Android:** El modo de administrador de dispositivos heredados de Android está desaprobado en Citrix Endpoint Management a partir de CEM 26.8.0. La plataforma **Android (DA heredado)** de la aplicación MDX se renombra como **Android (solo Citrix MAM)** para que la utilicen los dispositivos Android inscritos solo en el modo Citrix MAM.

Problemas resueltos en CEM 26.8.0

- Los usuarios no pueden instalar aplicaciones opcionales del Programa de compras por volumen (VPP) a través de Secure Hub cuando se asignan más de 2100 licencias y las instalaciones se redirigen a la App Store.

Citrix Endpoint Management 26.5.0

- **Compatibilidad con aplicaciones de administrador de credenciales en dispositivos Android Enterprise:** Se ha agregado una nueva configuración, **Aplicaciones de administrador de credenciales**, a la directiva de restricciones para dispositivos Android Enterprise. Esta configuración controla si una aplicación puede actuar como proveedor de credenciales y está establecida en **Desactivado** de forma predeterminada. La función está disponible en Android 14 y versiones posteriores y requiere Secure Hub versión 26.5.0 o posterior. Para obtener más información, consulte Directiva de restricciones.
- **Compatibilidad con Android 17:** Citrix Endpoint Management y las aplicaciones de productividad móvil de Citrix ahora son compatibles con dispositivos Android Enterprise que ejecutan Android 17. Para obtener detalles sobre seguridad y privacidad, consulte la documentación para desarrolladores de Android.

Problemas resueltos en CEM 26.5.0

- La edición manual del estado **Fuera de cumplimiento** de un dispositivo en la consola de CEM no activa una sincronización del estado de cumplimiento con Azure AD.
- Las actualizaciones de aplicaciones de iOS a través de la API REST `/api/v1/application/store/{id}/platform/iphone` fallan con el error 1493.
- Las llamadas a la API REST pública, como la consulta de dispositivos, fallan con el error 1001 después de migrar de Citrix Cloud Secure Client a la autenticación de entidad de servicio.

Citrix Endpoint Management 26.2.0

- **Mejora del inventario de aplicaciones para admitir la recuperación del tamaño de las aplicaciones de iOS 26.x:** Citrix Endpoint Management admite la recuperación de información sobre el tamaño de las aplicaciones para dispositivos que ejecutan iOS 26.x. Puede encontrar la información en **Detalles del dispositivo > Aplicaciones**.
- **Solución de problemas mejorada del certificado de dispositivo:** Citrix Endpoint Management ahora incluye una actualización del lado del servidor para admitir la mejora de la solución de problemas del certificado de dispositivo introducida en **Citrix Secure Hub**. Cuando está habilitada, esta función permite a los usuarios finales ver el estado de salud del certificado del dispositivo y solucionar automáticamente los problemas de certificado directamente desde la aplicación **Secure Hub**.

Para habilitar esta función para los usuarios existentes, los administradores de clientes deben agregar la propiedad de cliente `aeDeviceCertRenewSupport`. Para obtener más información, consulte Propiedades de cliente.

Para obtener más información sobre esta función en el lado del cliente, consulte Mejora de la solución de problemas del certificado de dispositivo.

- **Compatibilidad con la recuperación de información de dispositivos relacionada con la red del operador para dispositivos iOS:** Citrix Endpoint Management ahora admite la recuperación de información adicional de dispositivos relacionada con la red del operador para cada SIM en dispositivos iOS. Puede ver estos detalles en **Detalles del dispositivo > Propiedades > Información de la SIM de la ranura x**. Los campos recién admitidos incluyen:
  - Ranura x — versión de la configuración del operador
  - Ranura x — red del operador actual
  - Ranura x — código de país móvil actual (anteriormente listado en Información de red)
  - Ranura x — código de red móvil actual (anteriormente listado en Información de red)
  - Ranura x — se prefiere el uso de datos
  - Ranura x — está en itinerancia
  - Ranura x — se prefiere la voz
  - Ranura x — ID de etiqueta
- **Compatibilidad con la autenticación OAuth para Microsoft Exchange Online:** Microsoft anuncia que Exchange Online eliminará permanentemente la compatibilidad con la autenticación básica con el envío de cliente (SMTP AUTH) en March 2026 y alcanzará el 100 % de rechazos el April 30, 2026. Para obtener más información, consulte Exchange Online retirará la autenticación básica para el envío de cliente (SMTP AUTH).

  Citrix Endpoint Management admite la autenticación OAuth para el servidor SMTP. Habilite esta capacidad seleccionando **Microsoft Exchange Online OAuth 2.0** y proporcionando el **ID de inquilino**, el **ID de cliente** y el **Secreto de cliente** requeridos. Citrix recomienda cambiar a la autenticación OAuth si utiliza Microsoft Exchange Online. Para obtener detalles de configuración, consulte Notificaciones.

Problemas resueltos en CEM 26.2.0

- Las operaciones como la administración de dispositivos, aplicaciones y grupos de entrega en la consola de Citrix Endpoint Management se vuelven notablemente más lentas y, a veces, fallan.

Citrix Endpoint Management 25.11.0

- **Renovación del certificado APNs de Secure Hub:** El certificado del servicio de notificaciones push de Apple (APNs) de Secure Hub para Citrix Endpoint Management 25.9 caduca el January 4, 2026. Esta actualización renueva automáticamente el certificado APNs de Secure Hub a un nuevo certificado, válido hasta el November 9, 2026.

Problemas solucionados en CEM 25.11.0

- Cuando un dispositivo iOS tiene una política de bloqueo de aplicaciones para una aplicación desinstalada, el dispositivo se bloquea con el error 'La aplicación Acceso guiado no está disponible. Póngase en contacto con su administrador' y la pantalla táctil deja de responder, incluso después de un reinicio forzado.
- Cuando un administrador carga un archivo de aplicación para actualizar una aplicación empresarial existente para cualquier plataforma móvil, la actualización falla. La creación de una nueva aplicación empresarial no se ve afectada, solo la edición de aplicaciones existentes.

Citrix Endpoint Management 25.9.0

- **Compatibilidad con Android 16:** Citrix Endpoint Management y las aplicaciones de productividad de Citrix Mobile ahora son compatibles con los dispositivos Android Enterprise que ejecutan Android 16. Para obtener detalles sobre seguridad y privacidad, consulte la documentación para desarrolladores de Android.
- **Compatibilidad con iOS 26:** Citrix Endpoint Management y las aplicaciones de productividad de Citrix Mobile ahora son compatibles con iOS 26.
- **Compatibilidad con notificaciones de actualización de políticas MDX heredadas:** Citrix Endpoint Management ahora muestra alertas de actualización cuando las aplicaciones MDX existentes de Secure Mail y Secure Web que utilizan políticas heredadas se actualizan a la versión 25.9.0.
- **Compatibilidad con nuevas asignaciones de certificados seguros para la autenticación basada en certificados:** Se introduce un nuevo método de asignación para permitir una mayor flexibilidad en la emisión de certificados que cumplan con los requisitos de asignación segura. Citrix Endpoint Management (CEM) ahora añade `URL=tag:microsoft.com`, `2022-09-14:sid:<user's SID>` al Nombre alternativo del sujeto (SAN) de los certificados.

  - Para habilitar esta función para los usuarios existentes, los administradores de clientes deben añadir la propiedad de cliente `MICROSOFT_CERTIFICATE_STRONG_MAPPING`. Para obtener más detalles, consulte Propiedades de cliente.
  - La asignación de certificados seguros solo es compatible con **Windows Server 2019 y versiones posteriores**. Para obtener más información, consulte Asignación segura de Microsoft.

- **Compatibilidad con nuevas opciones del Asistente de configuración de iOS en la página Programas de implementación de Apple:** Apple añade algunas pantallas nuevas de opciones del Asistente de configuración de iOS para la inscripción en Apple Business Management. Las siguientes nuevas opciones se añaden en la página **Configuración > Programas de implementación de Apple > Opciones del Asistente de configuración de iOS**. Puede configurar Citrix Endpoint Management (CEM) para omitir esas pantallas. Para obtener más información, consulte Opciones del Asistente de configuración de iOS.
  - Botón de acción
  - Modo de bloqueo
  - Inteligencia
  - Botón de la cámara
- **Compatibilidad con nuevas restricciones de iOS para la versión 18.x de iOS:** En la directiva de restricciones para iOS, se han agregado las siguientes nuevas configuraciones para bloquear el acceso a Apple Intelligence (IA) o restringir algunas de las nuevas funciones. Estas configuraciones son aplicables para las versiones de iOS 18 y posteriores. El valor predeterminado es **Activado**. Para obtener más información, consulte Directiva de restricciones.
  - Permitir integraciones de inteligencia externa
  - Permitir iniciar sesión en integraciones de inteligencia externa
  - Permitir respuestas inteligentes de Mail
  - Permitir transcripción de Notas
  - Permitir resumen de Safari
  - Permitir resumen de inteligencia visual
  - Permitir resumen de transcripción de Notas
  - Permitir informe de Apple Intelligence
  - Permitir modificación de la aplicación de llamadas predeterminada

  - Permitir modificación de la aplicación de mensajería predeterminada
  - Permitir ID de espacio de trabajo de inteligencia externa
  - Modificación del navegador predeterminado
  - Permitir control remoto de FaceTime

- **Compatibilidad con nuevas restricciones de iOS para la versión 17.x de iOS:** En la directiva de restricciones para iOS, se ha agregado la siguiente nueva configuración para las versiones de iOS 17.2 y posteriores. El valor predeterminado es **Activado**. Para obtener más información, consulte Directiva de restricciones.

  - Permitir buzón de voz en vivo

- **Cuadro de texto de la política de configuración administrada:** Cuando el cliente utiliza **Knox Service Plugin** junto con la **política de configuración administrada**, la longitud máxima de caracteres para todos los cuadros de texto en **Separated Apps Policies** aumenta a 8.192 caracteres.
- **Compatibilidad mejorada con doble SIM y eSIM para dispositivos Android Enterprise:** Citrix Endpoint Management (CEM) ahora proporciona compatibilidad integral con doble SIM para dispositivos Android Enterprise para garantizar la paridad de funciones con iOS. Esta mejora permite a los administradores ver todas las tarjetas SIM y eSIM instaladas en las propiedades del dispositivo, incluidas las configuraciones con dos tarjetas SIM físicas, una tarjeta SIM más una eSIM o dos eSIM. Esta actualización aborda la creciente adopción de dispositivos Android Enterprise con doble SIM y proporciona a los clientes una visibilidad completa de sus opciones de conectividad de dispositivos móviles, igualando las capacidades de eSIM entregadas anteriormente para dispositivos iOS. Esta función solo es compatible con:

  - Secure Hub versión 25.7.0 o posterior, y
  - Android 13 o posterior

Problemas resueltos en CEM 25.9.0

- La alerta de Legacy MDX sigue mostrándose en la consola de CEM incluso cuando no se ha cargado ninguna aplicación de Legacy MDX.
- Los dispositivos del Programa de inscripción de dispositivos (DEP) siguen realizando la inscripción **MDM+MAM** incluso cuando el perfil de inscripción está configurado como **solo MDM**.
- Cuando la función **Mostrar nueva vista** está habilitada, el recuento de dispositivos se muestra incorrectamente incluso cuando se aplican filtros a la lista de dispositivos.

- Los dispositivos Android Enterprise no reciben las notificaciones de la **aplicación de inscripción** enviadas por los administradores a través de Citrix Endpoint Management™ (CEM).
- Los usuarios de iOS no pueden iniciar las aplicaciones Secure Mail/Secure Web y experimentan el error "No se puede abrir" al redirigir de Secure Mail/Secure Web a Secure Hub.

Citrix Endpoint Management 25.7.0

- **Flujo de trabajo de autenticación de usuario mejorado:** Los usuarios que inscribieron dispositivos con Active Directory (AD) local y luego se integraron con el proveedor de identidades de Citrix mediante Microsoft Azure Active Directory (AAD) no necesitan volver a inscribirse. Puede sincronizar cuentas desde su Active Directory local con Microsoft Azure Active Directory. Para obtener más información, consulte Flujo de trabajo de autenticación de usuario.

Citrix Endpoint Management 25.5.0

- **Sincronización con Apple Business Management para administrar las asignaciones de dispositivos:** Citrix Endpoint Management (CEM) ahora garantiza una asignación precisa de dispositivos al sincronizarse con Apple Business Management (ABM). Esta actualización verifica que solo los dispositivos asignados correctamente aparezcan en CEM, lo que evita registros de dispositivos que se han eliminado de CEM y se han asignado a otra solución de administración de proveedores. Por ejemplo, si los dispositivos se mueven a otra solución, ya no aparecen en CEM después de la sincronización. Esta función se controla mediante una propiedad de servidor de inquilino administrada por el cliente, `remove.unassigned.abm.devices`. De forma predeterminada, esta propiedad está establecida en **False**. Para obtener más información, consulte Propiedades del servidor.

> **Nota:**
>
> Los dispositivos de Apple Business Management (ABM) ya inscritos no se eliminan de CEM, incluso si un administrador intenta moverlos.

- **Compatibilidad con la administración declarativa de dispositivos (DDM):** Se introduce una nueva función, "Compatibilidad con la administración declarativa de dispositivos", para permitir la compatibilidad con la administración declarativa de dispositivos (DDM) de Apple en

iOS 15 y versiones posteriores. Esta función mejora el rendimiento y la escalabilidad al utilizar un modelo de datos declarativo, lo que reduce la dependencia de los comandos serializados y el sondeo de dispositivos. Para obtener más información, consulte Aprovechar el modelo de datos de administración declarativa para escalar dispositivos. Póngase en contacto con su administrador para habilitar esta función si es necesario.

Las siguientes directivas de dispositivos declarativas son compatibles cuando se habilita la función DDM:

- Cuenta de Google
- Código de acceso
- Aplicación de actualizaciones de software
- Configuración de actualizaciones de software
- Suscripciones de estado
- Identidad de usuario

Problemas resueltos en CEM 25.5.0

- El administrador de Control de acceso basado en roles (RBAC) cierra sesión inesperadamente al alternar **Mostrar nueva vista** en la página Dispositivo si no tiene el permiso **Propiedades del servidor**.
- Cuando la función Mostrar nueva vista está habilitada, los administradores de Control de acceso basado en roles (RBAC) ven inesperadamente el cuadro de entrada de búsqueda.
- Algunas directivas no se implementan en dispositivos AE durante la reinscripción cuando la **Condición de implementación** se establece en "Solo cuando la implementación anterior haya fallado" en la **Programación de implementación**.

Citrix Endpoint Management 25.3.0

- **Compatibilidad con filtros persistentes en la página Dispositivo:** En la nueva página de dispositivos, los filtros ahora son compatibles con todas las opciones **filtrables**. Estos filtros se guardan entre sesiones para el usuario que ha iniciado sesión, lo que elimina la necesidad de que el administrador vuelva a aplicar los mismos filtros cada vez que visita la página del dispositivo. Los filtros se eliminan automáticamente si se anula la selección de la columna correspondiente.
- **Compatibilidad para conservar la eSIM cuando el sistema borra el dispositivo:** Se ha añadido una nueva configuración, **Conservar eSIM al borrar**, a la Directiva de restricciones.

Esta configuración garantiza que la eSIM se conserve cuando el sistema borra el dispositivo debido a varios intentos fallidos de contraseña o cuando se selecciona la opción **Borrar todo el contenido y la configuración** en **Configuración > General > Restablecer**. Esta función está disponible para las versiones de iOS 17.2 y posteriores, con la configuración predeterminada establecida en **Desactivado**. Para obtener más información, consulte la Directiva de restricciones.

Problemas resueltos en CEM 25.3.0

- Cuando falla la renovación del certificado MDM, Citrix Endpoint Management (CEM) marca el certificado antiguo como revocado, lo que impide que Secure Hub (SH) se vuelva a conectar al servidor. Como resultado, SH no puede comunicarse con el servidor utilizando el certificado antiguo, aunque aún no haya caducado.
- El icono de la aplicación del Programa de compras por volumen (VPP) no se actualiza cuando la aplicación se actualiza a una nueva versión.

Citrix Endpoint Management 25.1.0

- **Renovación del certificado APNs de Secure Hub:** El certificado del servicio de notificaciones push de Apple (APNs) de Secure Hub para Citrix Endpoint Management 24.10 caduca el February 9, 2025. Esta actualización renueva automáticamente el certificado APNs de Secure Hub a un nuevo certificado, válido hasta el January 4, 2026.
- **Compatibilidad para bloquear o restringir Apple Intelligence para iOS:** En la directiva de restricciones para iOS, se han añadido nuevas configuraciones para bloquear el acceso a Apple Intelligence (IA) o restringir algunas de las nuevas funciones. Estas configuraciones se aplican a las versiones de iOS 18 y posteriores, con la configuración predeterminada establecida en **Activado**. Para obtener más información, consulte la Directiva de restricciones. Las nuevas configuraciones incluyen:
  - Genmoji
  - Image Playground
  - Image Wand
  - iPhone Mirroring
  - Personalized Handwriting Results
  - Writing Tools
  - Call Recording

  - Aplicaciones a ocultar
  - Aplicaciones a bloquear
  - Resumen de correo
  - Mensajería RCS

- **Compatibilidad con el bloqueo o la restricción de Apple Intelligence para macOS:** En la política de restricciones para macOS, se han añadido nuevas configuraciones para bloquear el acceso a Apple Intelligence (IA) o restringir algunas de las nuevas funciones. Estas configuraciones se aplican a las versiones 15 y posteriores de macOS, con el valor predeterminado establecido en **Activado**. Para obtener más información, consulte la Política de restricciones. Las nuevas configuraciones incluyen:
  - Image Playground
  - Duplicación de iPhone
  - Herramientas de escritura
  - Permitir la modificación del uso compartido de medios

Problemas resueltos en CEM 25.1.0

- Se estaban generando numerosos certificados de carga útil para dispositivos AE.
- Algunas políticas no se implementan en los dispositivos AE durante la reinscripción cuando la **Condición de implementación** está establecida en "Solo cuando la implementación anterior ha fallado" en la **Programación de implementación**.
- Cuando intenta sincronizar aplicaciones del Programa de Compra por Volumen (VPP) específicas de GEO con el servidor de Citrix Endpoint Management (CEM), la sincronización falla sin ningún mensaje de error. Las aplicaciones VPP no se reflejan en la lista de aplicaciones de Citrix Endpoint Management ni siquiera durante la sincronización manual de compra por volumen.

Citrix Endpoint Management 24.10.0

- **Autenticación con administración basada en grupos de Azure Active Directory:** Citrix Endpoint Management admite la autenticación de identidad basada en grupos a través de Azure Active Directory (AAD), lo que permite a los administradores gestionar el acceso a nivel de grupo utilizando la pertenencia a grupos de AAD. Esta actualización ofrece mayor flexibilidad y seguridad mejorada a través de controles de grupo centralizados. Si bien esta nueva funcionalidad agiliza la gestión de acceso, el mecanismo de inicio de sesión heredado

de Citrix Identity también permanece disponible para garantizar la compatibilidad con versiones anteriores. Para obtener más información, consulte Autenticación con administración basada en grupos de Azure Active Directory.

- **Soporte para el bloqueo de aplicaciones de terceros distribuidas por la web:** En la política de Restricción, se ha añadido una nueva configuración **Aplicaciones de distribución web** para bloquear las aplicaciones de terceros distribuidas por la web en dispositivos iOS. Esta configuración es aplicable para versiones de iOS 17.5 y posteriores. Para obtener más información, consulte Política de restricciones. Póngase en contacto con su administrador para habilitar esta función si es necesario.
- **Experiencia de plataforma unificada:** Citrix Endpoint Management permite una experiencia de plataforma unificada al proporcionar una navegación unificada en todos los productos de Citrix. Esta función cambia la ubicación de la barra de navegación en la interfaz de usuario general y añade una nueva barra de navegación izquierda.
- **Mejora de Citrix Endpoint Management para admitir el servidor CA de Windows 2022:** Citrix Endpoint Management admite los siguientes servidores CA:
  - Windows Server 2016
  - Windows Server 2019
  - Windows Server 2022
- **La pestaña Monitor está en desuso:** La pestaña Monitor en Citrix Endpoint Management está en desuso a partir de octubre de 2024. Para obtener más información, consulte Elementos en desuso y eliminaciones.
- **Actualizar el documento de la API REST pública para incluir la API de modo perdido del dispositivo:** Se ha añadido la API de modo perdido en el documento de la API REST pública.
- **Modificar la llamada a la API para que sea un cuerpo de publicación en lugar de una URL:** Se ha actualizado la llamada a la API para incluir los datos en el cuerpo de la solicitud en lugar de en la URL en el documento de la API REST pública.
- **Compatibilidad con Android 15:** Citrix Endpoint Management y las aplicaciones de productividad móvil de Citrix ahora son compatibles con las actualizaciones de dispositivos Android Enterprise a Android 15. Para obtener más información sobre los beneficios de seguridad y privacidad, consulte la documentación para desarrolladores de Android.
- **Compatibilidad con iOS 18:** Citrix Endpoint Management y las aplicaciones de productividad móvil de Citrix ahora son compatibles con iOS 18, pero actualmente no admiten todas las nuevas funciones de iOS 18.

- **Compatibilidad con macOS 15:** Citrix Endpoint Management y las aplicaciones de productividad móvil de Citrix ahora son compatibles con macOS 15, pero actualmente no admiten todas las nuevas funciones de macOS 15.

Problemas resueltos en CEM 24.10.0

- La conectividad de prueba de VPP y la sincronización de VPP fallaron para algunas aplicaciones.

Citrix Endpoint Management 24.8.0

- **Compatibilidad con la retroalimentación de configuraciones administradas (vista previa técnica):** La función de retroalimentación de configuración administrada permite a los administradores obtener retroalimentación sobre el estado de las aplicaciones desde dispositivos Android configurados con políticas de configuración administrada. Para obtener más información, consulte Compatibilidad con la retroalimentación de configuraciones administradas (vista previa técnica).
- **Aplicación de cumplimiento para dispositivos Android (vista previa técnica):** Para los dispositivos Android inscritos en el modo Propietario del dispositivo, el administrador del cliente puede gestionar el cumplimiento del dispositivo. Para obtener más información, consulte Aplicación de cumplimiento para dispositivos Android (vista previa técnica).

Problemas resueltos en CEM 24.8.0

- La acción segura 'Eliminar todos los usuarios' falló en el iPad compartido.
- Algunas aplicaciones públicas de iOS en Citrix Endpoint Management no se pueden encontrar en la Apple Store.
- En Citrix Endpoint Management 24.4.0, el inicio de sesión único (SSO) de SAML falla después de renovar el certificado SAML al usar CEM como proveedor de identidades (IDP) de SSO de SAML.
- En un escenario de autenticación basada en certificados, Secure Hub experimenta problemas de funcionalidad debido a un fallo en la renovación del certificado. El administrador del sistema podría notar que la generación de certificados PKI nunca se detiene, particularmente en la plataforma Android.
- La opción Actualizar no está disponible en la tienda de Secure Hub para aplicaciones habilitadas para MAM SDK con una nueva versión.

Citrix Endpoint Management 24.6.0

- **Compatibilidad con el bloqueo de aplicaciones de terceros para iOS 17.4 y versiones posteriores:** En la política de restricciones, se ha añadido una nueva configuración, **Mercado de aplicaciones alternativo**, para evitar la instalación de aplicaciones de mercados alternativos desde la web y evitar que las aplicaciones de mercados alternativos ya instaladas instalen otras aplicaciones. Para obtener más información, consulte Política de dispositivos de restricciones.
- **Compatibilidad con Firebase Cloud Messaging para usar la nueva API HTTP v1:** Las API heredadas de FCM para HTTP serán obsoletas por Google el June 21, 2024. Para que FCM funcione correctamente con la nueva API, se ha añadido un nuevo campo **Archivo de clave de cuenta de servicio** a la página de Firebase Cloud Messaging para que pueda cargar el archivo JSON de la clave de cuenta de servicio. Para obtener más información, consulte Firebase Cloud Messaging.

Problemas resueltos en CEM 24.6.0

- Después de que un administrador actualiza el grupo de AD, las aplicaciones móviles asignadas al grupo de entrega se vuelven inaccesibles para los usuarios finales y los usuarios pueden volverse anónimos.
- Los registros de Secure Hub no se pueden enviar al servicio de asistencia de TI cuando el cliente selecciona **Enviar registros del dispositivo al servicio de asistencia de TI** directamente en la configuración de **Soporte al cliente**.

Citrix Endpoint Management 24.4.0

- **Se ha añadido una nueva política de dispositivos de clave de Knox Platform for Enterprise:** Se ha añadido una nueva política de dispositivos **Knox Platform for Enterprise Key**. Esta política le permite proporcionar la información de licencia necesaria de Samsung Knox Platform for Enterprise (KPE) y utilizar las licencias de KPE para mejorar la seguridad de su dispositivo Samsung. Para obtener más información, consulte Política de dispositivos de clave de Knox Platform for Enterprise.
- **Aplicar una versión mínima del sistema operativo para completar la configuración en la inscripción automatizada:** Con iOS 17, los MDM ahora pueden aplicar una versión mínima del sistema operativo en los dispositivos que se inscriben al usar la inscripción automatizada de dispositivos. Para obtener más información, consulte el paso 3 en Agregar su cuenta a Citrix Endpoint Management.

- **Compatible con la función Volver al servicio de iOS 17:** Con la función Volver al servicio, el servidor MDM puede enviar un comando de borrado que incluye los detalles de Wi-Fi y un perfil de inscripción MDM predeterminado al dispositivo del usuario. A continuación, el dispositivo borra automáticamente todos los datos del usuario, se conecta a la red Wi-Fi especificada y se vuelve a inscribir en el servidor MDM mediante el perfil de inscripción proporcionado.
- **Compatibilidad con Samsung Enhanced Attestation v3:** Samsung Enhanced Attestation v3 mejora la funcionalidad de seguridad de CEM en los dispositivos Samsung Knox. Para obtener más información, consulte Samsung Knox Enhanced Attestation.
- **Modernizar la clasificación y el filtrado en la inscripción de dispositivos:** Las vistas de lista en CEM son actualmente difíciles de navegar y menos fáciles de usar. Al mover las opciones de filtrado y clasificación a los encabezados de columna, los clientes pueden combinar fácilmente estas funciones, lo que hace que sea mucho más sencillo e intuitivo encontrar los datos que necesitan.
- **Compatibilidad para instalar actualizaciones del sistema operativo inmediatamente para dispositivos iOS:** En la política de dispositivos de actualización del sistema operativo, se ha añadido un nuevo botón de opción llamado **Instalar lo antes posible** en las opciones de actualización del sistema operativo para iOS. Esta función le permite instalar las actualizaciones del sistema operativo descargadas previamente inmediatamente para dispositivos iOS. Para obtener más información, consulte Política de dispositivos de actualización del sistema operativo para iOS.
- **Mejorar el reinicio automático de la conexión VPN Always-On:** Se ha añadido una nueva configuración administrada **VPN Always On (opcional)** a la aplicación Citrix Secure Access, que debe establecerse en "true" para que esta mejora funcione de forma fiable para los perfiles de VPN Always On. Para obtener más información, consulte Configurar el protocolo Citrix SSO para Android y Crear una configuración administrada de Android Enterprise para Citrix SSO.

Problemas resueltos en CEM 24.4.0

- Las aplicaciones empresariales pueden notificar un número de versión incorrecto después de la actualización en dispositivos iOS.
- Los dispositivos iOS inscritos solicitan introducir el UPN en Secure Hub.

Citrix Endpoint Management 24.1.0

Esta versión aborda varios problemas que ayudan a mejorar el rendimiento y la estabilidad generales. No se han añadido nuevas funciones.

Citrix Endpoint Management 23.12.0

Se ha añadido un nuevo campo obligatorio "Dominio" en la configuración 802.1x para Android: Se ha añadido un nuevo campo **Dominio** en la página de configuración de la **política de red de la plataforma Android Enterprise** para el tipo de autenticación **802.1x EAP**. Para obtener más información, consulte Configuración 802.1x para Android.

Problemas conocidos actuales

Problemas conocidos en Citrix Endpoint Management 25.9.0

Cuando un administrador carga un archivo de aplicación para actualizar una aplicación empresarial existente para iOS, macOS o Android (administrador de dispositivos heredado), la actualización falla. La creación de una nueva aplicación empresarial no se ve afectada, solo la edición de aplicaciones existentes.

Problemas conocidos en Citrix Endpoint Management 22.6.0

De forma intermitente, la selección de los tres tipos de registros (**Depuración**, **Auditoría de administrador**, **Auditoría de usuario**) para descargar en **Solución de problemas y soporte > Registros** no funciona. Solo se descargan los registros de depuración. Como solución alternativa, puede descargar cada registro por separado o abrir el explorador en modo incógnito para descargar todos los registros marcando las tres casillas de verificación.

Al crear un enlace web en Android Enterprise, se produce un error al intentar guardar la aplicación con un icono. Este error es un problema de los servicios de Google. Como solución alternativa, guarde la aplicación sin cargar un icono.

Las directivas de Samsung Knox/SAFE siguen activas en los dispositivos inscritos incluso después de la desaprobación, y no se pueden deshabilitar ni configurar. Como solución alternativa, anule la inscripción y vuelva a inscribir el dispositivo.

Problemas conocidos en Citrix Endpoint Management 22.4.0

Al buscar un usuario de Active Directory inscrito en la ficha **Monitor**, no se muestran dispositivos inscritos para el usuario. Aún puede ver las directivas y aplicaciones asignadas al usuario, y usar todas las acciones de seguridad desde **Administrar > Dispositivos**. Se ven afectados tanto los dispositivos iOS como los Android inscritos.

Las aplicaciones privadas no se publican con Android Enterprise debido a un problema en los servicios de Google. Actualizaremos nuestra documentación cuando se resuelva el problema.

Problemas conocidos en Citrix Endpoint Management 21.12.0

Después de migrar a RBAC basado en Citrix Cloud, los usuarios administradores con permiso de acceso total en Citrix Cloud también obtienen permiso de acceso total en CEM, incluso si tenían permisos personalizados antes de la migración. Como solución alternativa, puede actualizar los permisos de administrador en la página de administración de identidades y accesos de Citrix Cloud con el acceso requerido.

Los clientes que se incorporaron antes de 2018 tienen acceso de administrador local a la consola. Los usuarios administradores de CEM con permisos para agregar o editar usuarios locales también pueden agregar o editar usuarios locales en Citrix Cloud. Estos permisos incluyen cambiar las contraseñas de los usuarios locales. Para solucionar este problema, puede llamar a Soporte para que se bloquee el acceso directo de administrador local a la consola, permitiendo solo el acceso de administrador de Citrix Cloud.

Problemas conocidos en Citrix Endpoint Management 21.11.0

En los dispositivos iOS inscritos solo en MAM, las aplicaciones empresariales no se instalan.

El uso de la directiva **Actualizar automáticamente aplicaciones administradas** para Android Enterprise no se aplica en los dispositivos cuando el servidor CEM se actualiza a 21.11.0. El error de la directiva afecta a las actualizaciones de aplicaciones en el dispositivo. Como solución alternativa, un administrador puede editar y guardar la directiva para actualizar los valores predeterminados.

Problemas conocidos en Citrix Endpoint Management 21.10.0

La directiva de dispositivo VPN no funciona correctamente en los dispositivos Windows 11 administrados. Hemos informado de este problema a Microsoft y estamos trabajando con ellos para resolverlo. Proporcionaremos actualizaciones sobre cualquier progreso.

Problemas conocidos en Citrix Endpoint Management 21.9.1

En dispositivos Android inscritos en el modo de perfil de trabajo en dispositivos propiedad de la empresa: Los usuarios pueden ver errores que indican que no pueden instalar o buscar aplicaciones en su perfil personal. Si ven esos errores, actualice la aplicación Google Play Store y vuelva a intentarlo.

Problemas conocidos en Citrix Endpoint Management 21.5.0

Los usuarios no pueden autenticarse en Azure Active Directory (AAD) si:

1. Inscriben su dispositivo en Citrix Endpoint Management con credenciales de AAD.
2. Inician una aplicación de Office 365 y completan el registro de AAD.
3. Eliminan su cuenta de la aplicación Microsoft Authenticator.
4. Inician una aplicación de Office 365 y cierran sesión.

Como solución alternativa, anule la inscripción del dispositivo en Citrix Endpoint Management y vuelva a inscribirlo.

Problemas conocidos en Citrix Endpoint Management 21.4.0

La reinscripción falla en los dispositivos iOS si el usuario que intenta reinscribirse es un usuario de Azure Active Directory diferente al usuario inscrito originalmente en el dispositivo. Como solución alternativa, anule el registro del usuario original de la aplicación Microsoft Authenticator en el dispositivo antes de volver a inscribirlo.

Problemas conocidos en Citrix Endpoint Management 21.2.0

Al agregar Citrix Secure Web como aplicación MDX para Android Enterprise, Managed Google Play no puede encontrar la aplicación utilizando el identificador de la aplicación. Si busca "Citrix Secure Web" en lugar del identificador de la aplicación, Managed Google Play puede encontrar la aplicación. Este problema es un error de Google.

La importación del certificado de escucha SSL podría fallar. Vuelva a empaquetar el almacén de claves del certificado siguiendo los pasos de CTX-297153.

Problemas conocidos en Citrix Endpoint Management 20.10.1

Si actualiza Citrix ADC local a la versión 13.0-64.35 o posterior, y Citrix Endpoint Management no está habilitado para Workspace: El inicio de sesión único en Citrix Files o la URL del dominio de

ShareFile produce un error. El usuario no puede iniciar sesión. Este error solo ocurre en un explorador con la opción **Inicio de sesión de empleado de la empresa**.

Para solucionar este problema: Si aún no ha ejecutado los siguientes comandos desde la CLI de ADC en NetScaler Gateway, ejecútelos para habilitar el SSO global:

```
set vpn parameter SSO ON
```

```
bind vpn vs <vsName> -portalTheme X1
```

Para obtener más información, consulte:

- Versión de Citrix ADC
- Configuraciones de SSO afectadas

Una vez completada la solución alternativa, los usuarios pueden autenticarse en Citrix Files o en la URL del dominio de ShareFile mediante SSO en un explorador con la opción **Inicio de sesión de empleado de la empresa**.

Problemas conocidos en Citrix Endpoint Management 20.2.1

Después de configurar ShareFile con una URL de ShareFile en la consola de Citrix Endpoint Management, al hacer clic en el botón **Probar conexión** se produce un error. Para resolver este problema, inhabilite la autenticación multifactor para ShareFile. Obtenga más información sobre este problema y la solución alternativa en este Restablecer número de teléfono de usuario para la verificación en dos pasos.

Problemas conocidos en Citrix Endpoint Management 20.1.0

Al agregar usuarios a una biblioteca en Citrix Cloud, Citrix Endpoint Management informa de que la operación se ha realizado correctamente, pero los usuarios no se agregan.

Problemas conocidos en Citrix Endpoint Management 19.11.0

Las aplicaciones MDX y públicas no se pueden eliminar de la consola. Como solución alternativa, seleccione la aplicación que desea eliminar y, a continuación, haga clic en **Editar**. Deseleccione **Android Enterprise** y seleccione cualquier otra plataforma de la lista de plataformas. Guarde la aplicación. A continuación, puede eliminar la aplicación.

Problemas conocidos en Citrix Endpoint Management 19.5.0

Al inscribir un dispositivo Citrix Ready® workspace hub, defina la dirección MAC de Ethernet (eth0) en la lista de permitidos para evitar errores de inscripción.

Problemas conocidos en Citrix Endpoint Management 19.4.1

Al desplazarse por las opciones de la directiva de dispositivo GPO de Windows, los botones de radio y las casillas de verificación se omiten.

Problemas conocidos en Citrix Endpoint Management 19.2.1

Si anula la inscripción de una empresa de Android Enterprise eliminándola a través de la consola de administración de Google: El intento de volver a inscribir la empresa podría fallar. Utilice siempre la consola de Citrix Endpoint Management para anular la inscripción de una empresa de Android Enterprise, como se describe en Anular la inscripción de una empresa de Android Enterprise. Los clientes de Google Workspace deben seguir las instrucciones de Anular la inscripción de una empresa de Android Enterprise.

Problemas conocidos en Citrix Endpoint Management 19.2.0

Al crear una aplicación de tienda pública en Citrix Endpoint Management 10.18.3: En la página Configuración de la aplicación para iPad, si hace clic en **Atrás** sin buscar aplicaciones y, a continuación, hace clic en **Siguiente**, se produce el siguiente problema. Los botones de navegación parecen no responder y no le permiten buscar aplicaciones. El problema ocurre al crear aplicaciones de tienda pública tanto para iOS como para Android.

Problemas conocidos en Citrix Endpoint Management 10.19.1

Después de completar el proceso de registro en la página **Parámetros > Android Enterprise**, aparece el siguiente mensaje de error: `A configuration error occurred. Please try again`. Al cerrar el mensaje de error, la configuración de Android Enterprise se guarda, pero **Habilitar Android Enterprise** está **Desactivado**. Para solucionar este problema, reduzca el número de categorías de aplicaciones a 30 o menos.

Problemas conocidos en Citrix Endpoint Management 10.18.5

Cuando una aplicación de Chrome se configura como una aplicación obligatoria para dispositivos Chrome OS: Es posible que los usuarios deban cerrar sesión y volver a iniciarla para instalar la aplicación. Este problema de terceros es el error de Google con ID #76022819.

Problemas conocidos en Citrix Endpoint Management 10.18.3

Después de eliminar un administrador de Citrix Cloud que tiene un dispositivo inscrito: Citrix Endpoint Management no actualiza el rol de usuario en la consola de Citrix Endpoint Management hasta que el administrador vuelve a iniciar sesión desde la aplicación Citrix Secure Hub o el portal de autoayuda.

Problemas conocidos en Citrix Endpoint Management 10.7.4

Si configura Citrix Endpoint Management para el inicio de sesión único (SSO) mediante el proveedor de identidades de Citrix con Azure Active Directory: Cuando un administrador o usuario de Citrix Endpoint Management es redirigido a la pantalla de **inicio de sesión de Azure Active Directory**, la pantalla incluye el mensaje "Página de inicio de sesión para Citrix Secure Hub." El mensaje correcto es "Página de inicio de sesión para la consola de Citrix Endpoint Management."

Historial de novedades

Hemos trasladado las secciones sobre versiones anteriores de Citrix Endpoint Management de Novedades a este artículo.

Citrix Endpoint Management 23.9.0

> **Nota:**
>
> Las actualizaciones de la documentación de Citrix Endpoint Management 23.9.0 se han revertido debido a la reversión de la versión del producto.

Citrix Endpoint Management 23.7.0

- **API Play Integrity:** La API Play Integrity sustituye a la API SafetyNet Attestation, que pronto quedará obsoleta, según la cronología de obsolescencia de Google. Para obtener más información y los pasos para habilitar esta API, consulte Habilitar la API Play Integrity.
- **Compatibilidad con eSIM y capacidades de doble SIM en dispositivos iOS:** Citrix Endpoint Management ahora es compatible con las capacidades de eSIM y doble SIM en dispositivos iOS. La compatibilidad con eSIM le permite recuperar información como el número de teléfono, IMEI, ICCID del dispositivo iOS y mostrarla en la interfaz de usuario de Citrix Endpoint Management. Para obtener más información sobre las propiedades del dispositivo, consulte Nombres y valores de las propiedades del dispositivo.

Citrix Endpoint Management 23.6.0

Compatibilidad con dispositivos macOS 14: Citrix Endpoint Management ahora es compatible con los dispositivos Apple que utilizan macOS 14. Para obtener más información, consulte la lista de sistemas operativos compatibles.

Esta versión aborda varios problemas que contribuyen a mejorar el rendimiento y la estabilidad generales.

Citrix Endpoint Management 23.4.0

Esta versión aborda varios problemas que contribuyen a mejorar el rendimiento y la estabilidad generales. No se añadieron nuevas funciones.

Citrix Endpoint Management 23.2.0

Esta versión aborda varios problemas que contribuyen a mejorar el rendimiento y la estabilidad generales. No se añadieron nuevas funciones.

Citrix Endpoint Management 23.1.0

Esta versión aborda varios problemas que contribuyen a mejorar el rendimiento y la estabilidad generales. No se han añadido nuevas funciones.

Citrix Endpoint Management 22.12.0

Esta versión aborda varios problemas que contribuyen a mejorar el rendimiento y la estabilidad generales. No se han añadido nuevas funciones.

Citrix Endpoint Management 22.10.0

Las siguientes funciones se están implementando para los clientes comerciales. Las implementaciones para los clientes del gobierno de EE. UU. comenzarán en un plazo de tres meses. Para conocer las diferencias de funciones entre las ofertas comerciales y las del gobierno de EE. UU., consulte Servicio Citrix Endpoint Management para el gobierno de EE. UU..

Se ha eliminado la directiva de Protección de información de Windows. Para obtener más información, consulte Desuso.

Compatibilidad con Windows 11 22H2. Citrix Endpoint Management ahora permite a los administradores de TI inscribir dispositivos Windows 11 22H2 con CEM mediante la funcionalidad MDM existente. Consulte Escritorio y tableta Windows para obtener más información sobre la inscripción de dispositivos Windows.

macOS 13 ahora es compatible. Citrix Endpoint Management ahora es compatible con dispositivos Apple que utilizan macOS versión 13.

Esta versión también aborda varios problemas que contribuyen a mejorar el rendimiento y la estabilidad generales.

Citrix Endpoint Management 22.9.0

Compatibilidad con Android 13 e iOS 16. Citrix Endpoint Management ahora es compatible con Android 13 e iOS 16.

Tipo de procesador y arquitectura del procesador. Los dispositivos Windows en la consola de CEM ahora también muestran el tipo de procesador y la arquitectura del procesador para cada dispositivo.

Esta versión también aborda varios problemas que contribuyen a mejorar el rendimiento y la estabilidad generales.

Citrix Endpoint Management 22.7.0

Esta versión aborda varios problemas que contribuyen a mejorar el rendimiento y la estabilidad generales. No se han añadido nuevas funciones.

Correcciones

De forma intermitente, la selección de los tres tipos de registros (**Depuración**, **Auditoría de administrador**, **Auditoría de usuario**) para descargar en **Solución de problemas y soporte > Registros** no funciona. Solo se descargan los registros de depuración. Como solución alternativa, puede descargar cada registro por separado o abrir el explorador en modo incógnito para descargar todos los registros marcando las tres casillas.

Al crear un enlace web en Android Enterprise, se produce un error al intentar guardar la aplicación con un icono. Se trata de un problema de los servicios de Google. Como solución alternativa, guarde la aplicación sin cargar un icono.

Las directivas de Samsung Knox/SAFE siguen activas en los dispositivos inscritos incluso después de su desuso, y no se pueden inhabilitar ni configurar. Como solución alternativa, anule la inscripción del dispositivo y vuelva a inscribirlo.

Citrix Endpoint Management 22.6.0

Se ha añadido una nueva directiva de restricción para permitir aplicaciones que no sean de Google Play para todos los perfiles del dispositivo. Consulte Directiva de dispositivo de restricciones para obtener más información.

Se ha dejado de admitir la interfaz de proveedor de servicios móviles (MSP). Se ha añadido una nueva propiedad de servidor que elimina la interfaz de MSP de la consola. Consulte Propiedades del servidor para obtener más información.

Se ha dejado de admitir la puerta de enlace SMS de Nexmo. Se ha dejado de admitir Nexmo SMS al añadir una propiedad de servidor llamada deprecate.carrier.sms.gateway, que está establecida en True de forma predeterminada. Nexmo SMS también se ha dejado de admitir en el portal de autoayuda. Consulte Notificaciones para obtener más información.

Las aplicaciones seleccionadas ahora pueden comunicarse entre perfiles de trabajo y personales para Android Enterprise. Hay un nuevo botón de alternancia llamado Enable connected apps disponible en la directiva de restricciones para Android Enterprise, que permite a las aplicaciones seleccionadas usar datos de trabajo y personales. Consulte Directiva de restricciones para obtener más información.

Google está dejando de admitir varias API utilizadas para categorías de aplicaciones y licencias en Citrix Endpoint Management:

- Ahora se seleccionan las aplicaciones para añadir en lugar de aprobar. Consulte Aplicaciones de la tienda de aplicaciones administradas.
- Ahora se organizan las aplicaciones en colecciones en lugar de categorías para Android Enterprise. Consulte Organizar aplicaciones (Android Enterprise).
- Ya no es necesario aprobar las aplicaciones MDX. Consulte Agregar una aplicación MDX.
- Ya no se pueden desasociar las licencias de aplicaciones de los usuarios. Consulte Agregar aplicaciones.

Citrix Endpoint Management 22.5.0

Se ha eliminado la compatibilidad con la directiva de restricción 'Permitir la conexión automática a puntos de acceso de WiFi Sense' para dispositivos Windows 10. Para obtener más información, consulte Configuración de equipos de escritorio/tabletas Windows.

Esta versión también resuelve varios problemas que contribuyen a mejorar el rendimiento y la estabilidad generales.

Citrix Endpoint Management 22.4.0

Se ha añadido una nueva opción a la directiva de dispositivo de actualización del SO para establecer un período de congelación durante el cual no se puedan instalar actualizaciones del SO. Consulte Directiva de dispositivo de actualización del SO para obtener más información.

Esta versión también resuelve varios problemas que contribuyen a mejorar el rendimiento y la estabilidad generales.

Citrix Endpoint Management 22.3.0

Ahora se pueden eliminar automáticamente los dispositivos que han estado inactivos durante un período de tiempo establecido. (Vista previa) Se ha añadido una nueva propiedad de servidor como vista previa llamada **Permite la eliminación de dispositivos que se han marcado como inactivos durante un período de tiempo especificado**, que ejecutará un trabajo en segundo plano para eliminar los dispositivos que han estado inactivos durante un tiempo especificado (en días). Consulte Propiedades del servidor para obtener más información.

Esta versión también resuelve varios problemas que contribuyen a mejorar el rendimiento y la estabilidad generales.

Citrix Endpoint Management 22.2.0

Se ha añadido una nota a la directiva de dispositivo de inventario de aplicaciones que indica que debe esperar 24 horas para que aparezcan los resultados del inventario al usar un dispositivo Windows 11. Consulte Directiva de dispositivo de inventario de aplicaciones para obtener más información.

Se ha añadido la opción 'Predeterminado' a la 'Directiva de actualización del sistema' para Android Enterprise, lo que permite a los administradores restaurar la directiva de actualización del sistema a su valor predeterminado. Consulte Directiva de dispositivo de actualización del SO para obtener más información.

Se ha añadido una nueva directiva de restricción para permitir aplicaciones que no sean de Google Play para todos los perfiles del dispositivo. Consulte Directiva de dispositivo de restricciones para obtener más información.

Se ha eliminado la compatibilidad con las siguientes funciones:

- **Rol RBAC: inscriptor de dispositivos compartidos y COSU**
- **Android - Sony y HTC**
- **Modo de inscripción de alta seguridad**
- **Credenciales derivadas**
- **SEAMS**
- **Dispositivos Windows Phone** Consulte Desuso para obtener más información.

Se agregó una nueva directiva de restricción para restringir la copia, el pegado y la importación de archivos de un perfil personal a un perfil de trabajo. Para obtener más información, consulte Directiva de dispositivo de restricciones.

Citrix Endpoint Management 22.1.0

Esta versión soluciona varios problemas que contribuyen a mejorar el rendimiento y la estabilidad generales. No se agregaron nuevas funciones.

Citrix Endpoint Management 21.12.0

Compatibilidad con la inscripción de dispositivos iOS habilitados para el Programa de implementación de Apple mediante Citrix Identity Provider. Al implementar dispositivos iOS a través del Programa de implementación de Apple, ahora puede permitir que los usuarios de Apple Business Manager utilicen Citrix Identity Provider como proveedor de identidades para inscribir sus dispositivos. Esta función admite la autenticación con Azure Active Directory y con Okta a través de Citrix Cloud. Para obtener más información, consulte Implementar dispositivos a través del Programa de implementación de Apple.

Permitir a los usuarios configurar y usar un proxy en iOS de forma predeterminada. Los usuarios con dispositivos iOS ahora pueden usar un proxy que hayan configurado en su dispositivo de forma predeterminada. Para evitar el uso de proxies del lado del cliente, cambie la propiedad de cliente de esta función a **false**. Para obtener más información sobre esta configuración, consulte Propiedades de cliente.

Se agregó la directiva de dispositivo Bluetooth para dispositivos iOS. Ahora puede configurar una directiva de dispositivo Bluetooth para habilitar o deshabilitar Bluetooth en dispositivos iOS supervisados. Para obtener más información sobre esta configuración, consulte Directiva de dispositivo Bluetooth.

Problemas resueltos en Citrix Endpoint Management 21.12.0

El uso de la directiva **Actualizar automáticamente aplicaciones administradas** para Android Enterprise no se aplica en los dispositivos cuando el servidor CEM se actualiza a 21.11.0. El error de la directiva afecta a las actualizaciones de aplicaciones en el dispositivo. Como solución alternativa, un administrador puede editar y guardar la directiva para actualizar los valores predeterminados.

Citrix Endpoint Management 21.11.0

Configure una prioridad para la actualización automática de aplicaciones administradas de Android Enterprise. Ahora puede especificar si las aplicaciones administradas de Android Enterprise se actualizan automáticamente con prioridad baja o alta. También puede posponer las actualizaciones automáticas. Para obtener más información, consulte Directiva de dispositivo de actualización automática de aplicaciones administradas.

Compatibilidad de la directiva de dispositivo de notificaciones de aplicaciones con la configuración de Tipo de agrupación y Tipo de vista previa. Con estas dos configuraciones, puede controlar cómo se agrupan y previsualizan las notificaciones de aplicaciones en dispositivos iOS supervisados. Para obtener más información, consulte Directiva de dispositivo de notificaciones de aplicaciones.

La directiva de dispositivo de atributos de aplicación admite más atributos de aplicación de iOS. Ahora puede especificar los siguientes atributos para las aplicaciones instaladas en dispositivos iOS:

- **Aplicación extraíble:** Especifique si los usuarios pueden eliminar una aplicación cuando es una aplicación administrada. Se aplica a iOS 14 y versiones posteriores.

Atributos para la función de dominios asociados:

- **Dominios asociados:** Especifique los dominios asociados que se agregarán a una aplicación. Se aplica a iOS 13 y versiones posteriores.
- **Habilitar descarga directa de dominio asociado:** Especifique si se debe habilitar la verificación de asociación de sitio reclamado directamente en los dominios. Se aplica a iOS 14 y versiones posteriores.

Para obtener más información, consulte Directiva de dispositivo de atributos de aplicación.

Problemas resueltos en Citrix Endpoint Management 21.11.0

De forma intermitente, al hacer clic en **Exportar script de configuración** en la página **Configuración > NetScaler Gateway**, recibe un archivo CSV dañado. Como solución alternativa, descargue el script de configuración al agregar o editar una configuración de NetScaler Gateway.

Citrix Endpoint Management 21.10.1

Extensión de bloqueo del dispositivo tras inactividad. El tiempo máximo de inactividad del dispositivo antes de que se bloquee se ha aumentado a 15 minutos. Para obtener más información, consulte Directiva de dispositivo de código de acceso.

Se agregó la configuración de restricción para pegar contenido de aplicaciones iOS. La directiva de dispositivo de restricciones ahora admite **Requerir portapapeles administrado** para iOS. Con esta configuración de restricción, puede bloquear o permitir pegar contenido de aplicaciones administradas a aplicaciones no administradas, y viceversa.

Esta configuración se aplica a iOS 15 y versiones posteriores. Para obtener más información, consulte Directiva de dispositivo de restricciones para iOS.

Problemas resueltos en Citrix Endpoint Management 21.10.1

La política de red no se implementa en dispositivos iOS y macOS que utilizan tipos de seguridad de red WPA2 y WPA3.

Citrix Endpoint Management 21.10.0

Asignar roles personalizados para administradores de la nube en Citrix Cloud. Los nuevos clientes de Citrix Endpoint Management incorporados después del October 4, 2021 ahora pueden asignar roles personalizados a los administradores de la nube en Citrix Cloud. Antes, tenía que asignar roles personalizados en Citrix Endpoint Management. Esta función le permite realizar sus personalizaciones relacionadas con el administrador sin tener que cambiar entre Citrix Cloud y Citrix Endpoint Management. Además, las plantillas **COSU devices enroller** y **Shared devices enroller** se eliminaron de Citrix Endpoint Management. **COSU devices enroller** ahora se gestiona a través de perfiles de inscripción y **Shared devices enroller** se gestiona a nivel de plataforma con el modo quiosco o Citrix Launcher.

Compatibilidad con dispositivos Windows 11. Ahora puede usar Citrix Endpoint Management para administrar dispositivos Windows 11. Para obtener más información, consulte la lista de compatibilidad de sistemas operativos.

El modo de inscripción de usuario de iOS ya está disponible como vista previa pública. Ahora puede aprovechar las funciones de inscripción de usuario de Apple en dispositivos iOS y iPadOS. La inscripción de usuario integra los ID de Apple administrados para crear una identidad de usuario en los dispositivos. Para obtener más información sobre la inscripción de usuario, consulte ID de Apple administrados.

Valor máximo actualizado para el seguimiento de la ubicación de dispositivos iOS. Ahora puede configurar la política de ubicación para rastrear la ubicación de un dispositivo iOS durante un máximo de 10 horas. Consulte Política de dispositivos de ubicación.

Problemas resueltos en Citrix Endpoint Management 21.10.0

Al actualizar un rol de administrador en la consola de Citrix Cloud, el cambio no se refleja en la consola de Citrix Endpoint Management. Este problema es estrictamente un problema de interfaz de usuario y no afecta a ninguna funcionalidad. Solo los clientes incorporados en la versión 21.10.0 o posterior se ven afectados.

Al crear un perfil de inscripción para que los dispositivos Android se inscriban en el perfil de trabajo en el modo de dispositivos corporativos, debe habilitar la configuración **BYOD work profile**. Si no habilita esta configuración, los dispositivos no se inscribirán.

Citrix Endpoint Management 21.9.1

Configure Azure AD u Okta como proveedor de identidades para inscribir y administrar dispositivos de usuario sin un Cloud Connector (vista previa). Si configura un proveedor de identidades a través de Citrix Cloud, no necesita un Cloud Connector para establecer la comunicación entre Citrix Endpoint Management y Citrix Cloud. Citrix Endpoint Management aún requiere un Cloud Connector para lo siguiente:

- LDAP
- Servidor PKI
- Consultas DNS internas
- Citrix Virtual Apps™

Para obtener más información sobre esta función, consulte Autenticación del proveedor de identidades.

Compatibilidad con dispositivos iOS 15 y macOS 12. Ahora puede usar Citrix Endpoint Management para administrar dispositivos iOS 15 y macOS 12. Para obtener más información, consulte la Lista de compatibilidad con sistemas operativos.

VPN siempre activa para Android Enterprise. Ahora puede habilitar una VPN siempre activa para dispositivos Android Enterprise. También puede optar por habilitar una función de bloqueo. Las aplicaciones requieren una conexión VPN para acceder a la red, a menos que las excluya del bloqueo. Para obtener más información, consulte Directiva de dispositivo VPN.

Los dispositivos Android 11+ totalmente administrados se inscriben en el modo de perfil de trabajo en dispositivos corporativos. El nuevo modo separa aún más los perfiles personal y de trabajo en un dispositivo. Este cambio ofrece a una organización un mayor control sobre el perfil administrado y ofrece a los usuarios más privacidad en su perfil personal. Para obtener más información, consulte Android Enterprise.

Posibilidad de establecer el consentimiento global para las aplicaciones cliente. Ahora puede establecer el consentimiento global para que los usuarios no necesiten dar su consentimiento en cada dispositivo. Para obtener más información, consulte Configurar Citrix Endpoint Management para la administración de cumplimiento de Azure AD.

Ahora se detectan los cambios en los permisos de Azure AD. Cuando se produce un cambio en los permisos de Azure AD, Citrix Endpoint Management ahora advierte automáticamente sobre el cambio para que pueda aprobarlo mediante la configuración de **administración de cumplimiento de Azure AD**. Siga el enlace de consentimiento y haga clic en **Aprobar** para

aceptar los cambios. Anteriormente, tenía que iniciar esta aprobación manualmente. Para obtener más información, consulte Configurar Citrix Endpoint Management para la administración de cumplimiento de Azure AD.

Problemas resueltos en Citrix Endpoint Management 21.9.1

Si agrega reglas de implementación a un grupo de entrega, las reglas de implementación nuevas o existentes a nivel de recurso (directivas, aplicaciones, acciones) ya no se aplican.

La función Exportar datos de Citrix Endpoint Management no exporta conjuntos completos de datos. Utilice estas soluciones alternativas para recuperar datos sobre los dispositivos administrados:

- Exporte datos desde la consola navegando a **Analizar > Informes > Inscripción de dispositivos**.
- Exporte datos mediante la API de informes. Para obtener información sobre la API de informes, consulte la documentación para desarrolladores.

Si accede a Citrix Endpoint Management a través de Citrix Cloud, agregar una aplicación empresarial para macOS provoca un error de autorización. Como solución alternativa, póngase en contacto con el soporte técnico y solicite acceso directo a su consola de Citrix Endpoint Management. A continuación, podrá agregar aplicaciones empresariales para dispositivos macOS.

Citrix Endpoint Management 21.9.0

Configuración de directivas de credenciales de Chrome OS (versión preliminar). La configuración de directivas de credenciales ya está disponible para Chrome OS. Los dispositivos Chromebook pueden usar la directiva de credenciales para aprovechar la administración de certificados integrada del sistema operativo Chrome. Los administradores pueden cargar el certificado privado de una autoridad de certificación para firmar y emitir los certificados de cliente. Este certificado permite a Citrix Endpoint Management crear y enviar certificados a los dispositivos Chromebook. Para obtener más información, consulte Directiva de dispositivo de credenciales.

Problemas resueltos en Citrix Endpoint Management 21.9.0

Después de inscribir un dispositivo iOS 15 o macOS 12, el perfil de configuración MDM aparece como "No verificado".

Citrix Endpoint Management 21.8.0

Compatibilidad con Android 12. Citrix Endpoint Management ahora es compatible con las actualizaciones de dispositivos Android Enterprise a Android 12. Para obtener un resumen de los beneficios de seguridad y privacidad, consulte la documentación de Android.

Compatibilidad con la edición de la salida JSON al generar un código QR para la inscripción de Android Enterprise. Al generar un código QR para la inscripción de Android Enterprise, ahora puede agregar información de inscripción al código QR editando directamente la salida JSON. Para obtener más información, consulte Android Enterprise.

Actualizar automáticamente las aplicaciones opcionales administradas. Las aplicaciones opcionales administradas ahora reciben actualizaciones automáticamente. Esta función incluye aplicaciones empresariales opcionales, aplicaciones opcionales de compra por volumen y aplicaciones públicas opcionales. Para obtener información sobre las aplicaciones de compra por volumen, consulte Agregar una cuenta de compra por volumen de Apple.

Usar Active Directory para autenticar a los usuarios cuando conectan sus dispositivos macOS a redes Wi-Fi. Citrix Endpoint Management ahora admite la autenticación con Active Directory para dispositivos macOS cada vez que se conectan a la red Wi-Fi configurada. Esta función se aplica solo a los siguientes tipos de seguridad:

- **WEP Enterprise**
- **WPA Enterprise**
- **WPA2 Enterprise**
- **Cualquiera (Enterprise)**

Para obtener más información, consulte Directiva de dispositivos de red.

Clonar un grupo de entrega para usarlo como base para un nuevo grupo de entrega. Esta función le permite copiar un grupo de entrega complejo que incluye varias directivas, aplicaciones y acciones. Luego puede editar la copia, como agregar perfiles de inscripción o un nuevo conjunto de usuarios de Active Directory. Para obtener más información, consulte Clonar un grupo de entrega.

Disponibilidad general de la conformidad de dispositivos de Azure AD. Citrix Endpoint Management ahora admite la conformidad de dispositivos de Azure AD a través de directivas de acceso condicional de Azure AD. Para obtener más información sobre esta función, consulte Integrar con el acceso condicional de Azure AD.

Problemas resueltos en Citrix Endpoint Management 21.8.0

Los usuarios con ciertos caracteres especiales en su nombre de usuario o contraseña no pueden inscribirse.

Citrix Endpoint Management 21.7.1

Esta versión incluye mejoras que ayudan a optimizar el rendimiento y la estabilidad generales.

Problemas resueltos en Citrix Endpoint Management 21.7.1

Al configurar un proveedor de identidades para Citrix Endpoint Management, si no configura los campos opcionales, los usuarios finales no pueden autenticarse.

Citrix Endpoint Management 21.7.0

Si se autentica con Azure Active Directory u Okta a través de Citrix Cloud, ahora puede crear diferentes perfiles de inscripción para dispositivos iOS y Android. Al configurar Azure Active Directory u Okta como métodos de autenticación a través de Citrix Cloud, Citrix Endpoint Management admite varios perfiles de inscripción con diferentes tipos de inscripción. Para obtener más información, consulte Perfiles de inscripción.

Etiquete automáticamente los dispositivos por tipo de dispositivo y modo de inscripción. Si habilita la propiedad de servidor `enable.device.tagging`, Citrix Endpoint Management etiqueta cualquier dispositivo recién inscrito. Puede usar las etiquetas de dispositivo para implementar directivas y aplicaciones o configurar grupos de entrega. Citrix Endpoint Management aplica etiquetas a los dispositivos para lo siguiente:

- Etiquetas BYOD
    - Inscripción de usuario de iOS
    - Perfil de trabajo de Android Enterprise
- Etiquetas corporativas
    - Dispositivos corporativos totalmente administrados de Android Enterprise
    - Inscripción masiva
        - Dispositivos de Apple Business Manager
        - Dispositivos de Apple School Manager
        - Dispositivos Windows AutoPilot
        - Inscripción masiva de Android Enterprise

Para obtener más información, consulte Propiedades del servidor

Para los clientes de Citrix Endpoint Management con la experiencia de espacio de trabajo habilitada: Citrix Endpoint Management admite la autenticación con Azure Active Directory, Okta y un NetScaler Gateway local para los usuarios que se inscriben en MDM a través de la aplicación Citrix Workspace. Para obtener más información, consulte Autenticación con Azure Active Directory a través de Citrix Cloud, Autenticación con Okta a través de Citrix Cloud y Autenticación con un NetScaler Gateway local a través de Citrix Cloud.

Citrix Endpoint Management 21.6.0

Se cambió el nombre de la directiva de dispositivos Wi-Fi a directiva de dispositivos de red. Cambiamos el nombre de la directiva de dispositivos Wi-Fi a "directiva de dispositivos de red" para admitir Ethernet en macOS. Para macOS, además de la opción Wi-Fi, ahora tiene las siguientes opciones de Ethernet:

- Ethernet global
- Primera Ethernet activa
- Segunda Ethernet activa
- Tercera Ethernet activa
- Primera Ethernet
- Segunda Ethernet
- Tercera Ethernet

Para obtener más información, consulte Directiva de dispositivos de red.

Compatibilidad con Apple Business Manager (ABM) y Eliminar todos los usuarios para iPads compartidos. Los usuarios ahora pueden iniciar sesión en iPads compartidos mediante cuentas de ABM. La acción de seguridad Eliminar todos los usuarios también está disponible para iPads compartidos. Para obtener más información, consulte iPads compartidos.

Cargue certificados a dispositivos iOS de forma masiva con la API REST de Citrix Endpoint Management. Si cargar los certificados uno a uno no es práctico, utilice la API REST del servidor de Citrix Endpoint Management para cargar los certificados a los dispositivos iOS de forma masiva.

1. Configure una directiva de dispositivo VPN de iOS con el tipo de conexión **Always on IKEv2**.
2. Seleccione **Device Certificate Based on Device Identity** como método de autenticación del dispositivo.

3. Seleccione el **Device identity type** que desea utilizar.
4. Importe sus certificados de dispositivo de forma masiva con la API REST.

Para obtener información sobre cómo configurar la directiva de dispositivo VPN, consulte Directiva de dispositivo VPN. Para obtener información sobre cómo importar certificados de forma masiva, consulte Cargar certificados a dispositivos iOS de forma masiva con la API REST.

Obsoleto el modo de túnel completo para aplicaciones iOS. A partir de esta versión, MDX ya no admite el modo de túnel completo en las aplicaciones de productividad móvil de Citrix para iOS. Las siguientes opciones se eliminan de la directiva de aplicación de acceso a la red:

- Usar configuración anterior
- Tunneled - Full VPN
- Tunelizado - VPN completa y SSO web

Si utiliza las directivas **Tunneled - Full VPN** o **Tunneled - Full VPN and Web SSO**, debe cambiar a la directiva **Tunneled - Web SSO**. Sus correos electrónicos no se sincronizarán si sigue utilizando las directivas obsoletas. Para obtener más información, consulte Consideraciones de SSO y proxy para aplicaciones MDX.

Selección de certificados más informativa. Al configurar una PKI de Microsoft, una PKI genérica, una directiva de credenciales o proveedores de credenciales, el menú de certificados proporciona información más útil para distinguir los certificados. Esta información incluye:

- El nombre del certificado
- La fecha a partir de la cual el certificado es válido
- La fecha hasta la cual el certificado es válido
- El número de serie del certificado

Citrix Endpoint Management 21.5.1

Esta versión incluye mejoras que contribuyen a optimizar el rendimiento y la estabilidad generales.

Citrix Endpoint Management 21.5.0

Renovación del certificado APNs de Citrix Secure Hub. El certificado del Servicio de notificaciones push de Apple (APNs) de Citrix Secure Hub para Citrix Endpoint Management caduca el June 17, 2021. Esta actualización renueva el certificado APNs de Citrix Secure Hub, que caducará el May 7, 2022.

Conformidad con FIPS 140-2. Los componentes del lado del servidor de Citrix Endpoint Management ahora cumplen con FIPS 140-2. Para obtener más información, consulte Conformidad con FIPS 14-2.

Problemas resueltos en Citrix Endpoint Management 21.5.0

Tenemos una nueva API "Get Devices by Filters" que resuelve problemas en las API "Get Devices by Filters" anteriores y devuelve resultados paginados para hasta 100 dispositivos a la vez. Consulte la sección "3.16.3 Get Devices by Filters" en el PDF Public API for REST Services.

Cuando utiliza un ID de paquete para buscar una aplicación de Google Play para agregarla a la consola de Citrix Endpoint Management, el campo obligatorio **Nombre** aparece vacío. Aun así, puede introducir el nombre de la aplicación manualmente.

Citrix Endpoint Management 21.4.0

Citrix ha recibido la verificación para el conjunto de soluciones de administración avanzada de Google Android Enterprise. Consulte Citrix Endpoint Management obtiene una nueva verificación de Android Enterprise.

Integrar con el acceso condicional de Azure AD (versión preliminar). Ahora puede configurar Citrix Endpoint Management para aplicar la compatibilidad con el acceso condicional de Azure AD a las aplicaciones de Office 365. Esta función, ahora en versión preliminar, le permite implementar la metodología de confianza cero para los usuarios de dispositivos al implementar aplicaciones de Office 365. Puede utilizar el estado del dispositivo, la puntuación de riesgo, la ubicación y las protecciones del dispositivo para definir el acceso a las aplicaciones de Office 365 en dispositivos Android Enterprise e iOS administrados. Para obtener información, consulte Integrar con el acceso condicional de Azure AD.

Utilice reglas de propiedades de dispositivos Android para administrar la implementación de un grupo de entrega en dispositivos Android Enterprise. Si inscribe varios dispositivos Android Enterprise al mismo usuario, ahora puede implementar recursos del grupo de entrega en función del perfil de inscripción del dispositivo o del ID del paquete de la aplicación. Dentro del grupo de entrega, utilice las propiedades del dispositivo para la plataforma Android para crear reglas avanzadas para dispositivos Android Enterprise nuevos o existentes. Para obtener más información, consulte Agregar un grupo de entrega.

Compatibilidad con la rotación de la contraseña de administrador para dispositivos macOS inscritos a través del Programa de implementación de Apple. Al agregar su cuenta de Apple Business Manager a Citrix Endpoint Management, puede especificar la configuración para crear una cuenta de administrador en el dispositivo macOS. Citrix Endpoint Management crea

automáticamente la cuenta de administrador en el dispositivo durante el flujo de trabajo del Asistente de configuración. Los usuarios inician sesión en su dispositivo macOS con la información especificada. Citrix Endpoint Management ahora admite la rotación de la contraseña de esa cuenta de administrador para mejorar la seguridad. Para obtener más información, consulte Implementar dispositivos a través del Programa de implementación de Apple.

La nueva configuración del servicio AutoDiscovery a través de Citrix Cloud. El servicio AutoDiscovery ahora está alojado en Citrix Cloud. Citrix migró todas las configuraciones de servicio de AutoDiscovery existentes sin interrupción del servicio. Para acceder al nuevo servicio AutoDiscovery o cambiar su configuración, vaya a `https://adsui.cloud.com` (comercial) o `https://adsui.cem.cloud.us/` (gubernamental). Para obtener más información, consulte Configurar el servicio AutoDiscovery para Citrix Endpoint Management.

En la nueva configuración del servicio AutoDiscovery, use la configuración de **Puerto MAM** en lugar de **FQDN de NetScaler Gateway** para dirigir el tráfico de MAM a su centro de datos. Si introduce un nombre de dominio completo junto con el puerto de su NetScaler Gateway, el dispositivo cliente utiliza la configuración del ajuste **Puerto MAM**.

Cuando vaya a `https://adsui.cloud.com` (comercial) o `https://adsui.cem.cloud.us/` (gubernamental) para acceder a la nueva interfaz de usuario del servicio AutoDiscovery, un bloqueador de anuncios puede impedir que el sitio se abra. Para acceder al servicio AutoDiscovery, desactive el bloqueador de anuncios para todo el sitio web.

Se han añadido ajustes a las restricciones de Android Enterprise. Hemos añadido dos ajustes a todos los modos de inscripción para alinearlos más estrechamente con la configuración de Google y simplificar la configuración.

- **Permitir el uso compartido de Bluetooth:** Si no está seleccionada, los usuarios no pueden establecer el uso compartido de Bluetooth saliente en su dispositivo.
- **Permitir la desinstalación de aplicaciones:** Permite a los usuarios desinstalar aplicaciones desde Managed Google Play Store.

Además, hemos movido la configuración **Permitir actualización inalámbrica** de la directiva de restricciones a la directiva de actualización del sistema operativo.

Para obtener más información sobre estos cambios, consulte Directiva de dispositivo de restricciones y Directiva de dispositivo de actualización del SO.

Compatibilidad con la entrega de aplicaciones MDX desde una red de entrega de contenido (CDN). La compatibilidad con CDN ya está disponible para las aplicaciones MDX. Para acelerar la

entrega de descargas de aplicaciones, la CDN envía esas aplicaciones MDX a los dispositivos de los usuarios ubicados cerca de un servidor de Citrix Endpoint Management. El uso de la CDN reduce los tiempos de descarga de las aplicaciones. Para empezar, consulte Entregar aplicaciones MDX desde la CDN de Citrix.

Problemas resueltos en Citrix Endpoint Management 21.4.0

Las aplicaciones empresariales no se instalan en dispositivos que ejecutan macOS 11.0 o posterior, pero la consola de Citrix Endpoint Management muestra que se han instalado correctamente.

Citrix Endpoint Management 21.3.0

Flujo simplificado para agregar aplicaciones de Android Enterprise a entornos administrados por Intune. Ahora puede agregar aplicaciones de Android Enterprise a la consola de Citrix Endpoint Management y a la consola de Intune al mismo tiempo. Para obtener más información sobre este flujo de trabajo, consulte Agregar aplicaciones de Android Enterprise a la biblioteca de Citrix Cloud.

Generar un código QR para la inscripción de Android Enterprise. Citrix Endpoint Management ahora puede generar códigos QR para la inscripción de Android Enterprise. Al usar la consola de Citrix Endpoint Management para generar un código QR para las inscripciones, evita sitios externos que pueden ser maliciosos. Para obtener más información sobre la generación de códigos QR, consulte Crear un código QR.

Compatibilidad con tokens de arranque para dispositivos macOS. Citrix Endpoint Management ahora admite el depósito de tokens de arranque para dispositivos macOS. Se genera un token de arranque durante el flujo de trabajo del Asistente de configuración. Una de las ventajas de depositar tokens de arranque con Citrix Endpoint Management es que las cuentas remotas se pueden habilitar para FileVault y pueden desbloquear el volumen de FileVault. Para obtener más información, consulte Token de arranque.

Citrix Endpoint Management 21.2.0

La aplicación **Citrix Launcher** actualizada le permite restringir el acceso de los usuarios a una aplicación o a un pequeño conjunto de aplicaciones en dispositivos Android Enterprise. También puede, opcionalmente, cargar una imagen de logotipo personalizada para el icono de **Citrix Launcher** y especificar una contraseña que los usuarios deben introducir para salir de la aplicación. Para obtener más información, consulte Citrix Launcher.

Nuevas opciones del Asistente de configuración para iOS y macOS. Ahora puede especificar más pantallas de configuración para omitir cuando los usuarios configuren dispositivos iOS o macOS.

- iOS
  - **Restauración completada:** Impide que los usuarios vean si una restauración se completa durante la configuración. Para iOS 14.0 y versiones posteriores.
  - **Actualización completada:** Impide que los usuarios vean si una actualización de software se completa durante la configuración. Para iOS 14.0 y versiones posteriores.
- macOS
  - **Accesibilidad:** Impide que el usuario escuche Voice Over automáticamente. Solo disponible si el dispositivo está conectado a Ethernet. Para macOS 11 y versiones posteriores.
  - **Biométrico:** Impide que el usuario configure Touch ID y Face ID. Para macOS 10.12.4 y versiones posteriores.
  - **True Tone:** Impide que los usuarios configuren sensores de cuatro canales para ajustar dinámicamente el balance de blancos de la pantalla. Para macOS 10.13.6 y versiones posteriores.
  - **Apple Pay:** Impide que los usuarios configuren Apple Pay. Si esta opción está desactivada, los usuarios deben configurar Touch ID y Apple ID. Asegúrese de que las opciones **Apple ID** y **Biométrico** estén desactivadas.
  - **Tiempo de uso:** Impide que los usuarios activen Tiempo de uso. Para macOS 10.15 y versiones posteriores.

Para obtener más información sobre cómo configurar las opciones de configuración, consulte Implementar dispositivos a través del programa de implementación de Apple.

Las cargas de archivos PKG de macOS ahora están limitadas por el tiempo de carga en lugar del tamaño del archivo. Ahora puede cargar archivos PKG más grandes, como Microsoft Office para dispositivos macOS. Citrix Endpoint Management ha eliminado el límite de tamaño de archivo anterior de 0,5 GB y, en su lugar, limita el tiempo de carga del archivo. De forma predeterminada, debe completar la carga en 100 segundos. Para obtener más información, consulte Agregar una aplicación empresarial.

Citrix Endpoint Management ya no admite algoritmos criptográficos débiles para la autenticación basada en certificados. Cuando cree una solicitud de firma de certificado para un

proveedor de credenciales en la consola de Citrix Endpoint Management, elija un cifrado más seguro. Para obtener la lista de algoritmos de firma eliminados, consulte Desuso.

Problemas resueltos en Citrix Endpoint Management 21.2.0

Al crear un usuario, se crean dos certificados PKI para el mismo usuario. Es posible que el usuario no pueda acceder a sitios web internos a través de Citrix Secure Web o recibir correo electrónico a través de Citrix Secure Mail.

Al agregar un rol RBAC, Citrix Endpoint Management deja de responder después de estas acciones:

- Aplicar un permiso a un grupo de usuarios específico y, a continuación, desmarcar una casilla de verificación de dominio de Active Directory.
- Seleccionar repetidamente un elemento de acceso autorizado o un elemento de función de consola.

Citrix Endpoint Management 21.1.1

> **Nota:**

> Como resultado de una interrupción, es posible que se haya eliminado el historial de su grupo de entrega. La recopilación del historial del grupo de entrega se ha reanudado.

> **Nuevo aspecto.** Citrix ha actualizado la consola de Citrix Endpoint Management con nuevos colores, fuentes, conmutadores y otros cambios de formato. Es posible que algunos elementos nuevos de la interfaz de usuario no se carguen correctamente hasta que borre la caché del navegador y actualice la página.

Política de desinstalación de aplicaciones ahora disponible para macOS. Ahora puede eliminar aplicaciones administradas de dispositivos macOS mediante la política de desinstalación de aplicaciones. Para obtener más información, consulte la política de dispositivos de desinstalación de aplicaciones.

Mejoras para un grupo de entrega. Ahora puede administrar la implementación de un grupo de entrega utilizando reglas de propiedades de dispositivo junto con las reglas de propiedades de usuario existentes. Si inscribe varios dispositivos al mismo usuario, ahora puede crear filtros avanzados dentro del grupo de entrega basados en las propiedades únicas del dispositivo, como

la propiedad del dispositivo, el modelo, la versión del sistema operativo, el cumplimiento y otros. Para obtener más información, consulte Agregar un grupo de entrega.

Las API ya están disponibles para crear informes. Las API de informes son API de solo lectura que utilizan JSON como lenguaje de consulta. Las API le permiten hacer lo siguiente:

- Crear informes de cumplimiento sólidos sobre el control de versiones de aplicaciones, la aplicación de parches del sistema operativo del dispositivo, el progreso de la migración de Android DA (heredado) a Android Enterprise y mucho más.
- Emitir consultas personalizadas contra su base de datos en la nube de forma segura.
- Exportar datos sobre su servicio en la nube, como listas de aplicaciones, dispositivos, usuarios, inscripciones y software.
- Guardar información en formato JSON o CSV.

Estas API son el equivalente en la nube a tener acceso a una base de datos local y ejecutar consultas SQL personalizadas. Para obtener más información sobre las API de informes, consulte la documentación en el portal para desarrolladores de Citrix.

Citrix Endpoint Management 21.1.0

Autentíquese en la API de REST con las claves de API de Citrix Cloud. Ahora puede generar el ID de cliente y el secreto de cliente únicos para acceder a la API de REST mediante su cuenta de Citrix Cloud. Para obtener más información, consulte API de REST.

Reorganización de las restricciones de Android Enterprise. La configuración de restricciones para Android Enterprise se ha reorganizado para mayor claridad. En ocasiones, se han realizado cambios menores en los nombres de las configuraciones. Para obtener más información sobre la reorganización, consulte Configuración de Android Enterprise.

Citrix Endpoint Management 20.12.0

Esta versión incluye mejoras que ayudan a optimizar el rendimiento y la estabilidad generales.

Utilice Azure Active Directory (AAD) u Okta para autenticarse al inscribir dispositivos Android Enterprise (versión preliminar). La capacidad de usar AAD u Okta como métodos de autenticación al inscribir dispositivos Android Enterprise ya está disponible como versión preliminar. Esta función admite los modos BYOD y totalmente administrado, además de los perfiles de inscripción mejorados. Para obtener más información sobre el uso de Okta para el inicio de sesión único, consulte Autenticación con Okta a través de Citrix Cloud. Para obtener más

información sobre el uso de AAD para el inicio de sesión único, consulte Autenticación con Azure Active Directory a través de Citrix Cloud.

Instalación de aplicaciones empresariales y de compra por volumen en dispositivos macOS como aplicaciones administradas. La configuración **Forzar que la aplicación sea administrada** ya está disponible para macOS. Si desea administrar una aplicación que está instalada pero aún no administrada, active la configuración para esa aplicación e impleméntela en los dispositivos. La aplicación se instala automáticamente como una aplicación administrada. Los usuarios no reciben ninguna solicitud. Si implementa una aplicación en dispositivos donde la aplicación no existe, la aplicación se instala como una aplicación administrada independientemente del estado de la configuración. Para obtener más información, consulte Agregar una aplicación empresarial y Configurar las aplicaciones de compra por volumen.

Problemas resueltos en Citrix Endpoint Management 20.12.0

Las plantillas de notificación predeterminadas utilizan el nombre XenMobile en lugar de Citrix Endpoint Management.

Es posible que los usuarios de Android Enterprise no reciban las aplicaciones añadidas después de inscribirse.

Las claves de recuperación de cifrado de BitLocker para dispositivos Windows no están disponibles en el portal de autoayuda (SHP). Cuando habilita la configuración **Recuperación de unidad de SO** en la directiva de dispositivos BitLocker y cifra un dispositivo Windows inscrito con BitLocker, las claves de recuperación no aparecen en el SHP. Como solución alternativa, abra un tíquet de CEMHELP y solicite una conversación con SRE y la dirección de producto.

Citrix Endpoint Management 20.11.0

Eliminación de la compatibilidad con Android TouchDown. DigiCert dejó de admitir Android TouchDown a partir de July 2, 2018. Todas las opciones de Android TouchDown se han eliminado de la consola de Citrix Endpoint Management.

Citrix Endpoint Management 20.10.1

Limitar los métodos para acceder a la API REST. Al ponerse en contacto con el soporte de Citrix, puede asegurarse de que solo las cuentas de Citrix Cloud puedan acceder a la API REST. Las cuentas de administrador local no pueden acceder a la API con esta función habilitada. Consulte API REST.

Problemas resueltos en Citrix Endpoint Management 20.10.1

Los usuarios no reciben correos electrónicos de invitación a la inscripción.

Si configura Citrix Endpoint Management como una autoridad de certificación discrecional, las directivas de dispositivo de VPN, red y otras credenciales no se implementan.

Citrix Endpoint Management 20.10.0

Permitir direcciones MAC estáticas o dinámicas. Como parte de la directiva de red, los dispositivos iOS y iPadOS ahora pueden usar una dirección MAC diferente cada vez que se conectan a la red Wi-Fi configurada. También puede elegir que la dirección MAC permanezca estática. Sin embargo, el uso de una dirección MAC dinámica dificulta la identificación coherente del dispositivo, lo que mejora la privacidad. Consulte Directiva de red.

Usar Azure Active Directory (AAD) u Okta como plataformas de identidad. La capacidad de usar AAD u Okta como plataforma de identidad ya está disponible como vista previa pública. Los usuarios que se inscriben a través de Citrix Secure Hub pueden usar sus credenciales de AAD u Okta. Para usar cualquiera de estos métodos para el inicio de sesión único, configure NetScaler Gateway para la autenticación basada en certificados. Para obtener más información sobre el uso de Okta para el inicio de sesión único, consulte Autenticación con Okta a través de Citrix Cloud. Para obtener más información sobre el uso de AAD para el inicio de sesión único, consulte Autenticación con Azure Active Directory a través de Citrix Cloud.

Usar UPN o correo electrónico para la autenticación de Okta. Cuando configura Okta como su plataforma de identidad, puede permitir que los usuarios inicien sesión con su UPN o su dirección de correo electrónico. Consulte Inicio de sesión único con Okta.

Problemas resueltos en Citrix Endpoint Management 20.10.0

Los usuarios no reciben correos electrónicos de invitación a la inscripción.

Citrix Endpoint Management 20.9.1

Volver a implementar directivas asignadas a dispositivos iOS y Android. Si el usuario elimina una directiva, ahora puede volver a implementarla en dispositivos iOS y Android. Vaya a **Administrar > Dispositivos > Directivas asignadas**, seleccione la directiva y haga clic en **Restablecer estado** para cambiar el estado de implementación a pendiente. Para obtener más información, consulte Métodos de inscripción admitidos para iOS y Métodos de inscripción admitidos para dispositivos Android.

La directiva de dispositivo FileVault ahora permite el almacenamiento y la rotación de claves. Con la directiva de dispositivo FileVault, ahora puede almacenar claves de recuperación personales en Citrix Endpoint Management. Los usuarios finales pueden solicitar su clave de recuperación mediante el portal de autoayuda, y los administradores pueden rotar las claves de recuperación personales mediante acciones de seguridad. Para obtener más información sobre las nuevas funciones, consulte Directiva de dispositivo FileVault.

Control más granular sobre las opciones de actualización de macOS. La directiva de dispositivo de actualización del SO ahora le permite controlar cómo los dispositivos macOS comprueban, descargan e instalan las actualizaciones. También puede configurar los tipos de actualizaciones de software permitidos. Para obtener más información sobre la nueva configuración, consulte Directiva de dispositivo de actualización del SO.

Problemas resueltos en Citrix Endpoint Management 20.9.1

El certificado MDM de algunos dispositivos iOS no se renueva. En ese caso, la página **Administrar > Dispositivos > Detalles del dispositivo > Certificados** muestra un certificado MDM de Apple que está a punto de caducar. El registro del servidor de Citrix Endpoint Management incluye el mensaje **The new MDM payload does not match the old payload**. Le recomendamos que vuelva a inscribir los dispositivos afectados para resolver este problema. El Soporte técnico de Citrix puede identificar los dispositivos que deben volver a inscribirse e implementar una mitigación temporal si es necesario.

Citrix Endpoint Management 20.9.0

Esta versión incluye mejoras que contribuyen a optimizar el rendimiento y la estabilidad generales.

Problemas resueltos en Citrix Endpoint Management 20.9.0

Cuando un usuario de Azure AD inicia sesión en algunos dispositivos Windows 10 unidos a Azure AD configurados como quiosco, el modo quiosco no se activa.

Justo después de inscribir un dispositivo con macOS 10.14 o posterior, las propiedades del dispositivo no siempre se rellenan en la consola de Citrix Endpoint Management. Reinicie el dispositivo para ver las propiedades.

Los recursos implementados a veces no surten efecto en los dispositivos macOS 10.14 o posterior hasta que se reinicia el dispositivo.

Citrix Endpoint Management 20.8.0

Uso más sencillo del alias de certificado en las configuraciones administradas. Utilice la nueva opción **Alias de certificado** de la directiva de dispositivo **Credenciales** con la directiva de dispositivo **Configuración administrada de Android Enterprise**. Esto permite que las aplicaciones se autentiquen en la VPN sin la intervención del usuario. En lugar de buscar el alias de credencial en los registros de la aplicación, cree el alias de credencial. Cree el alias escribiéndolo en el campo **Alias de certificado** de la directiva de dispositivo **Configuración administrada de Android Enterprise**. A continuación, escriba el mismo alias de certificado en la opción **Alias de certificado** de la directiva de dispositivo **Credenciales**. Consulte Directiva de configuraciones administradas y Directiva de dispositivo Credenciales.

La directiva de dispositivo de código de acceso permite mostrar aplicaciones y accesos directos en dispositivos Android Enterprise que no cumplen los requisitos. La directiva de dispositivo de código de acceso para Android Enterprise tiene una nueva opción, **Mostrar aplicaciones y accesos directos mientras el código de acceso no cumple los requisitos**. Habilite la opción para que las aplicaciones y los accesos directos permanezcan visibles cuando el código de acceso del dispositivo ya no cumpla los requisitos. Citrix recomienda crear una acción automatizada para marcar el dispositivo como no conforme cuando el código de acceso no cumpla los requisitos. Consulte Directiva de dispositivo de código de acceso.

Control de la configuración Usar un solo bloqueo en dispositivos Android Enterprise. La nueva configuración **Habilitar código de acceso unificado** en la directiva de dispositivo **Código de acceso** le permite controlar si un dispositivo requiere una contraseña independiente para el dispositivo y el perfil de trabajo. Antes de esta configuración, los usuarios controlaban este comportamiento con la configuración **Usar un solo bloqueo** en el dispositivo. Cuando **Habilitar código de acceso unificado** está **Activado**, los usuarios pueden usar la misma contraseña para el dispositivo que para el perfil de trabajo. Si **Habilitar código de acceso unificado** está **Desactivado**, los usuarios no pueden usar la misma contraseña para el dispositivo que para el perfil de trabajo. El valor predeterminado es **Desactivado**. La configuración **Habilitar bloqueo unificado** está disponible para dispositivos Android Enterprise que ejecutan Android 9.0 o posterior. Consulte Directiva de dispositivo de código de acceso.

Problemas resueltos en Citrix Endpoint Management 20.8.0

Si incorporó Citrix Endpoint Management en la versión 19.12.0 o posterior, para eliminar la suscripción a Android Enterprise, anule la inscripción de Android Enterprise desde la consola. A continuación, elimine la configuración de Google Play. Si hace clic primero en **Eliminar empresa** en Google Play Store, la suscripción a Android Enterprise permanece activa en la consola de Citrix Endpoint Management.

Citrix Endpoint Management 20.7.1

Se cambió el nombre del perfil en las pantallas de inscripción a Citrix Workspace. Cuando los usuarios inscriben su dispositivo en Citrix Endpoint Management, el nombre del perfil que se muestra ahora es Citrix Workspace. Puede personalizar este nombre y mostrar el nombre de su organización en su lugar. Para personalizar el nombre, cambie el valor de la nueva propiedad de servidor `apple.mdm.enrollment.profile.organization.name`. Consulte Propiedades del servidor.

Problemas corregidos en Citrix Endpoint Management 20.7.1

En algunos sitios en la nube, la página **Monitor** de la consola de Citrix Endpoint Management no se carga.

Al editar los valores de la propiedad de servidor `optional.user.identity.attributes` y guardar los cambios, aparece un mensaje de error.

Citrix Endpoint Management 20.7.0

Citrix Endpoint Management admite la autenticación con un NetScaler Gateway local como función de vista previa. Ahora puede configurar un NetScaler Gateway local como su proveedor de identidades para los usuarios que se inscriben a través de Citrix Secure Hub. Para obtener más información, consulte Autenticación con un NetScaler Gateway local a través de Citrix Cloud (versión preliminar).

Personalice la lista de atributos de usuario opcionales de Active Directory. Una nueva propiedad de servidor, `optional.user.identity.attributes`, le permite eliminar y restaurar atributos opcionales que Citrix Endpoint Management utiliza para identificar una cuenta de usuario en Active Directory. Para obtener más información, consulte Personalizar atributos de usuario de Active Directory.

Problemas corregidos en Citrix Endpoint Management 20.7.0

Las aplicaciones de compra por volumen de Apple iTunes no se pueden sincronizar con Citrix Endpoint Management.

Cuando instala varios Active Directory (AD) LDAP en Citrix Endpoint Management mediante Citrix Cloud Connector, solo el primer AD instalado se rellena en la configuración de Citrix Endpoint Management. Como solución alternativa, puede comprobar Citrix Cloud. Si esos dominios están marcados como no utilizados, márquelos manualmente como **Usados**. Marcar el dominio como usado lo hace disponible en Citrix Endpoint Management.

Si incorporó Citrix Endpoint Management en la versión 19.12.0 (diciembre de 2019) o posterior: al agregar varios dominios de autenticación LDAP, no puede cambiar el dominio predeterminado.

Citrix Endpoint Management 20.6.0

Si incorporó Citrix Endpoint Management después de la versión 19.8.0 (August 1, 2019), inicie sesión en Citrix Cloud y haga clic en el mosaico del servicio Citrix Endpoint Management para acceder a la consola. Todos los clientes que se incorporaron antes de la versión 19.8.0 pronto pasarán al inicio de sesión de Citrix Cloud. Para proporcionar seguridad mejorada, Citrix recomienda que configure un inicio de sesión único. Para obtener ayuda, póngase en contacto con el Soporte técnico de Citrix.

El certificado del Servicio de notificaciones push de Apple (APNs) de Citrix Secure Hub para Citrix Endpoint Management caduca el July 12, 2020. Como resultado, la notificación del agente falla y el envío de aplicaciones podría retrasarse en los dispositivos iOS. Esta actualización renueva el certificado APNs de Citrix Secure Hub, que caduca el June 18, 2021.

Deshabilite la capacidad de imprimir en los perfiles de trabajo de Android Enterprise o en dispositivos totalmente administrados. En la directiva de dispositivo Restricciones, la configuración **No permitir la impresión** le permite especificar si los usuarios pueden imprimir en cualquier impresora accesible desde el dispositivo Android Enterprise. Para obtener más información, consulte Configuración de Android Enterprise.

Configure el modo de conexión y la prioridad de red para macOS. En la directiva de dispositivo de red, habilite la configuración **Modo de conexión** para que los dispositivos macOS elijan cómo se unen los usuarios a la red. El dispositivo puede usar las credenciales del sistema o las credenciales introducidas en la ventana de inicio de sesión para autenticar al usuario. Si tiene varias redes, escriba un número en el campo **Prioridad** para establecer la prioridad de la conexión de red. El dispositivo elige la red con el número más bajo. Para obtener más información, consulte la configuración de macOS en Directiva de dispositivo de red.

Habilitar un proxy configurado en dispositivos iOS. Citrix Endpoint Management ahora requiere que habilite una nueva propiedad de cliente, `ALLOW_CLIENTSIDE_PROXY`, si desea permitir que los usuarios de iOS utilicen los servidores proxy que configuran en **Ajustes > Red**. Para obtener más información, consulte `ALLOW_CLIENTSIDE_PROXY` en Referencia de propiedades de cliente.

Actualizar automáticamente la directiva de aplicaciones administradas para aplicaciones de Google Play administradas. Esta nueva directiva le permite restringir la capacidad de los usuarios para configurar actualizaciones automáticas de aplicaciones para aplicaciones de Google

Play administradas en dispositivos Android Enterprise. Puede permitir a los usuarios configurar la directiva. O bien, puede especificar que las actualizaciones automáticas se apliquen siempre, nunca o solo cuando un dispositivo esté conectado a una red Wi-Fi.

Problemas resueltos en Citrix Endpoint Management 20.6.0

En la consola de Citrix Endpoint Management, no puede ver el ID de paquete de las aplicaciones iOS y Android encapsuladas en MDX.

Cuando Citrix Endpoint Management envía las consultas de los miembros del grupo de Active Directory, el servicio de identidad ejecuta las consultas de forma recursiva. Estas consultas consumen más recursos. Por lo tanto, los sitios con muchos usuarios de Active Directory pueden experimentar una interrupción en las operaciones diarias.

En la consola de Citrix Endpoint Management, el estado de algunas aplicaciones aparece como "Pendiente" aunque ya estén instaladas. Esta limitación se debe a macOS y es específica de los archivos PKG con diferentes identificadores de paquete y aplicación.

Citrix Endpoint Management 20.5.0

Configuración simplificada de aplicaciones administradas por Intune al usar la integración de Citrix Endpoint Management con Microsoft Endpoint Manager. Cuando configura aplicaciones administradas por Intune, ya no establece la opción **Forzar la administración de la aplicación** en la consola de Citrix Endpoint Management. Ahora establece la opción en la consola de EMS.

Compatibilidad para restringir la transferencia de contenido web para aplicaciones administradas por Intune publicadas a través de Microsoft Edge mediante la integración de Citrix Endpoint Management con Microsoft Endpoint Manager. La integración de Citrix Endpoint Management con Microsoft Endpoint Manager admite la nueva directiva de explorador administrado para Microsoft Edge, **Restringir la transferencia de contenido web con otras aplicaciones**, en la consola de EMS.

Desbloquear una cuenta de usuario local. Si un usuario alcanza el número máximo de intentos de inicio de sesión no válidos consecutivos, la cuenta de usuario local se bloquea durante 30 minutos. El sistema deniega todos los intentos de autenticación posteriores hasta que expire el período de bloqueo. Para desbloquear la cuenta en la consola de Citrix Endpoint Management, vaya a **Administrar > Usuarios**, seleccione la cuenta de usuario y haga clic en **Desbloquear usuario local**. Para obtener más información, consulte Para desbloquear una cuenta de usuario local. Para cambiar el número de intentos de inicio de sesión fallidos y el tiempo de bloqueo, actualice las propiedades del servidor **local.user.account.lockout.time** y

local.user.account.lockout.limit. Para obtener más información, consulte Propiedades del servidor.

La red de entrega de contenido (CDN) de Citrix ahora entrega aplicaciones empresariales para macOS (inscripción MDM). Para acelerar la entrega de descargas de aplicaciones, la CDN envía aplicaciones de macOS a los dispositivos de los usuarios ubicados cerca de los servidores de Citrix Endpoint Management en todo el mundo. Para obtener más información, consulte Entregar aplicaciones empresariales desde la CDN de Citrix.

Problemas resueltos en Citrix Endpoint Management 20.5.0

Los administradores con el permiso RBAC para exportar invitaciones de inscripción pueden exportar todas las invitaciones de inscripción, independientemente de las limitaciones.

Los intentos de implementar un script de PowerShell para activar una acción automatizada en dispositivos Windows pueden fallar con un error interno del servidor 500. El problema ocurre si deja el campo **Descripción** en la página **Información de la acción** en blanco y selecciona **Valor devuelto por la directiva** como desencadenador. Para solucionar el problema, no deje el campo **Descripción** en blanco cuando utilice **Valor devuelto por la directiva** como desencadenador.

Cuando edita una directiva de restricción de iOS existente, se produce un error.

Citrix Endpoint Management 20.4.1

Compatibilidad con la última API de proveedor de APNs basada en HTTP/2. La compatibilidad de Apple con el protocolo binario heredado del servicio de notificaciones push de Apple finaliza a partir del March 31, 2021. Apple recomienda utilizar la API de proveedor de APNs basada en HTTP/2 en su lugar. Citrix Endpoint Management ahora es compatible con la API basada en HTTP/2. Para obtener más información, consulte la actualización de noticias, "Apple Push Notification Service Update" en `<https://developer.apple.com/>`. Para obtener ayuda con la comprobación de conectividad a APNs, consulte Comprobaciones de conectividad.

Requisitos de contraseña para una cuenta de usuario local. Al agregar o modificar una cuenta de usuario local en la consola de Citrix Endpoint Management, asegúrese de seguir los requisitos de contraseña más recientes. Para obtener más información, consulte Para agregar una cuenta de usuario local.

Utilice el número de ID de paquete de la aplicación para agregar aplicaciones a la directiva de dispositivo de notificaciones de aplicaciones. Haga clic en **Agregar nuevo** y escriba el ID de paquete de la aplicación en el campo que aparece. Para obtener más información, consulte Directiva de dispositivo de notificaciones de aplicaciones.

Actualizaciones de directivas de dispositivo para iOS 13. Las directivas de dispositivo para iOS 13 ahora tienen las siguientes funciones:

- **Directiva de uso de red:** Hemos agregado más funciones a la directiva de uso de red de aplicaciones y la hemos renombrado a Directiva de uso de red. Ahora también puede configurar reglas de uso de red basadas en ICCID de SIM en dispositivos iOS 13. Consulte Directiva de dispositivo de uso de red
- **Directiva de restricciones:** Ahora puede restringir las sesiones temporales de dispositivos compartidos, la modificación de eSIM, Buscar mi iPhone y mucho más. Para obtener más información, consulte la sección de configuración de iOS en Directiva de dispositivo de restricciones.

Problemas resueltos en Citrix Endpoint Management 20.4.1

Con la autenticación y la inscripción de dispositivos basadas en Azure Active Directory, los usuarios con dispositivos Android no pueden inscribirse. Un error indica que la autenticación de usuario no tiene acceso al dispositivo.

Citrix Endpoint Management 20.4.0

Publique aplicaciones web para Android Enterprise en la consola de Citrix Endpoint Management. Ya no necesita ir a Google Play administrado o al portal para desarrolladores de Google para publicar aplicaciones web de Android Enterprise para Citrix Endpoint Management. Al hacer clic en **Cargar** en **Configurar > Aplicaciones > Enlace web**, se abre una interfaz de usuario de la tienda Google Play administrada para que cargue y guarde el archivo. La aprobación y publicación de la aplicación puede tardar unos 10 minutos. Para obtener más información, consulte Agregar un enlace web.

Actualizaciones de directivas de dispositivo para iOS 13. Las directivas de dispositivo para iOS 13 ahora tienen las siguientes funciones:

- **Directiva de bloqueo de aplicaciones:** Puede habilitar el control por voz y dar a los usuarios acceso al ajuste del control por voz. Consulte Directiva de dispositivo de bloqueo de aplicaciones.
- **Directiva de Exchange:** Puede habilitar o deshabilitar la sincronización de calendarios, contactos, correo, notas y recordatorios. Consulte Directiva de dispositivo de Exchange.
- **Directiva de eliminación de perfiles:** Se eliminaron las configuraciones para permitir la eliminación de directivas en dispositivos iOS, ya que iOS ya no admite esa función. Consulte Directiva de dispositivo de eliminación de perfiles.

- **Política de VPN:** Ahora puede incluir todo el tráfico de red o excluir las redes locales de la VPN, para los siguientes protocolos de conexión:
  - Protocolo AnyConnect heredado de Cisco para iOS
  - Protocolo SSL personalizado para iOS

  Ahora puede permitir que el tráfico fluya a través del túnel VPN celular cuando la Asistencia Wi-Fi se desconecta de la red Wi-Fi, para los siguientes protocolos de conexión:
  - Protocolos IKEv2 para iOS
- **Política de red:** Ahora puede usar WPA3 Personal y WPA3 Enterprise como opciones de **Tipo de seguridad**. Consulte Política de dispositivos de red.

Problemas resueltos en Citrix Endpoint Management 20.4.0

Los gráficos de visualización de datos del panel **Analizar** no se escalan correctamente al usar el zoom del explorador.

Cuando se utiliza la inscripción solo para MAM, los usuarios pueden seguir accediendo al portal de inscripción inalámbrica de Apple para MDM.

La acción de borrado selectivo falla cuando el dispositivo está en modo de espera.

Citrix Endpoint Management 20.3.0

Perfiles de inscripción mejorados habilitados para todos los clientes

Esta versión habilita para todos los clientes las funciones mejoradas de perfiles de inscripción que se lanzaron para algunos clientes en Citrix Endpoint Management 20.2.1. Para obtener información sobre esta función, consulte Configurar varios modos de administración de dispositivos y aplicaciones en un único entorno.

Los dispositivos Android se inscriben en Android Enterprise de forma predeterminada

A partir de esta versión, Android Enterprise es la opción de inscripción predeterminada para los dispositivos Android. Si Android Enterprise está habilitado para su implementación de Citrix Endpoint Management, todos los dispositivos Android recién inscritos o reinscritos se inscriben como dispositivos Android Enterprise de forma predeterminada.

Este cambio es compatible con los cambios que Google está realizando en Android. Google ha dejado de usar el modo de administrador de dispositivos para la administración de dispositivos y anima a los clientes a administrar todos los dispositivos Android mediante Android Enterprise. (Consulte Deprecación del administrador de dispositivos en las guías para desarrolladores de Google Android Enterprise).

A partir de Citrix Endpoint Management 19.11.0, Citrix comunicó las acciones necesarias para migrar todos los dispositivos Android a Android Enterprise. Para obtener más información sobre la compatibilidad de Citrix Endpoint Management con la transición a Android Enterprise, consulte la entrada del blog Android Enterprise como predeterminado para el servicio Citrix Endpoint Management.

Si su implementación de Citrix Endpoint Management incluye dispositivos que debe seguir administrando en modo de administrador de dispositivos, cree un perfil de inscripción para estos dispositivos heredados.

Para crear un perfil de inscripción para dispositivos heredados:

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Perfiles de inscripción**.
2. Para agregar un perfil de inscripción, haga clic en **Agregar**. En la página Información de inscripción, escriba un nombre para el perfil de inscripción.
3. Haga clic en **Siguiente** o seleccione **Android** en **Plataformas**. Aparece la página Configuración de inscripción.
4. Establezca **Administración** en **Administración de dispositivos heredados (no recomendado)**. Haga clic en **Siguiente**.
5. Seleccione **Asignación (opciones)**. Aparece la pantalla Asignación de grupos de entrega.
6. Elija el grupo de entrega o los grupos de entrega que tienen los administradores que inscriben los dispositivos dedicados. A continuación, haga clic en **Guardar**.

Para seguir administrando dispositivos heredados en modo de administrador de dispositivos, inscríbalos o reinscríbalos con este perfil. Los dispositivos de administrador de dispositivos se inscriben de forma similar a los dispositivos de perfil de trabajo, haciendo que los usuarios descarguen Citrix Secure Hub y proporcionando una URL de servidor de inscripción.

Problemas resueltos en Citrix Endpoint Management 20.3.0

Intentar ordenar los dispositivos por **Último acceso** o **Días de inactividad** provoca un error interno del servidor 500.

Para los clientes que utilizan Amazon Web Services y los nuevos perfiles de inscripción mejorados de Citrix: los dispositivos iOS no se inscriben. Como solución alternativa, cree un perfil de inscripción predeterminado que incluya todos los grupos de entrega. Consulte Para crear un perfil de inscripción.

Cuando se implementa una directiva de dispositivo de código de acceso en dispositivos macOS, la directiva se aplica a nivel de sistema en lugar de a nivel de usuario. Como resultado, no se solicita a los usuarios que cambien su código de acceso durante horas, o incluso días.

Citrix Endpoint Management 20.2.1

Configurar múltiples modos de administración de dispositivos y aplicaciones en un único entorno

> **Acerca de esta función:**

> La compatibilidad mejorada con perfiles de inscripción se implementará en dos versiones. Citrix® envía notificaciones sobre las próximas versiones.

> Hasta que la función de perfil de inscripción mejorado se habilite para usted, un perfil de inscripción solo limita el número de dispositivos que un usuario puede inscribir.

> Ahora puede configurar un único sitio de Citrix Endpoint Management para admitir varias configuraciones de inscripción. La función de los perfiles de inscripción se ha ampliado para incluir la configuración de inscripción para la administración de dispositivos y aplicaciones.

Los perfiles de inscripción admiten múltiples casos de uso y rutas de migración de dispositivos dentro de una única consola de Citrix Endpoint Management. Los casos de uso incluyen:

- Administración de dispositivos móviles (solo MDM)
- MDM+Administración de aplicaciones móviles (MAM)
- Solo MAM
- Inscripciones de propiedad corporativa
- Inscripciones BYOD (la capacidad de optar por no participar en la inscripción MDM)
- Migración de inscripciones de administrador de dispositivos Android a inscripciones de Android Enterprise (totalmente administrado, perfil de trabajo, dispositivo dedicado)

Los perfiles de inscripción reemplazan la propiedad de servidor ahora obsoleta, `xms.server.mode`. Este cambio no afecta a sus grupos de entrega existentes ni a los dispositivos inscritos.

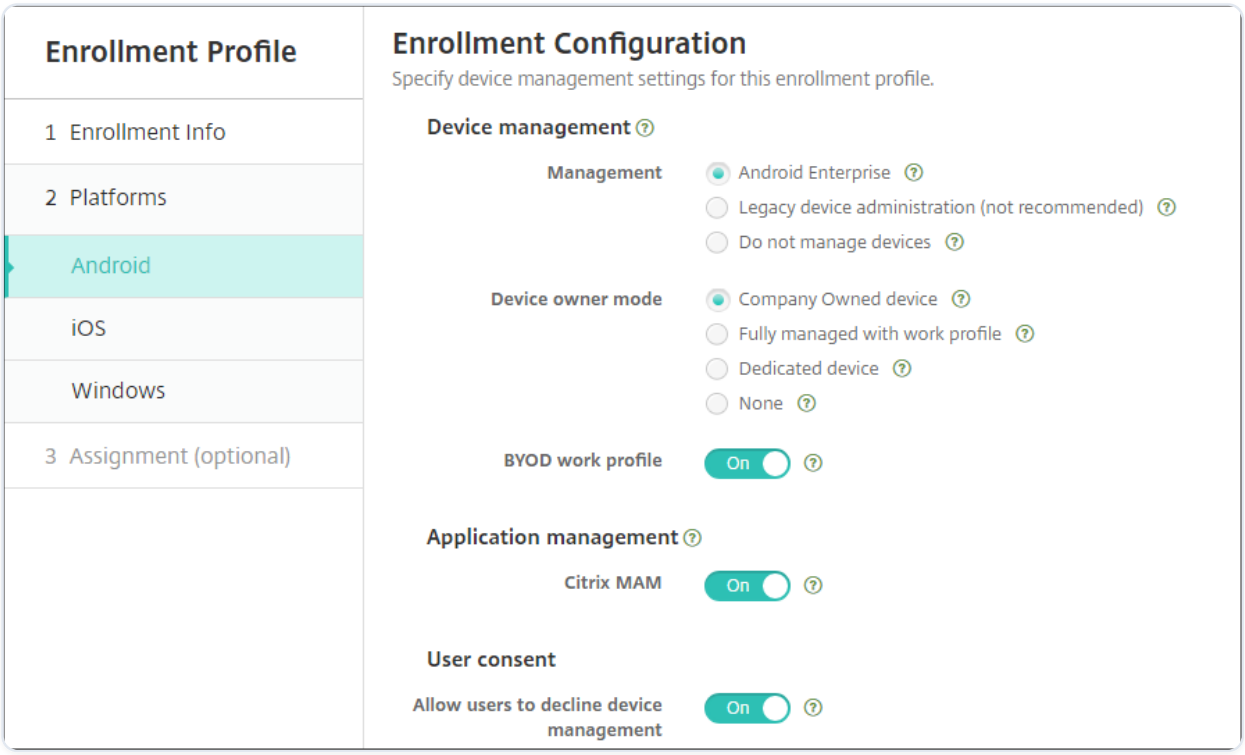
La siguiente tabla muestra la ruta de migración automatizada del modo de propiedad de servidor existente a la nueva función de perfil de inscripción:

PROPIEDAD DE SERVIDOR EXISTENTE	NUEVO MODO DE ADMINISTRACIÓN
Modo ENT (iOS)	Inscripción de dispositivos Apple con Citrix MAM
Modo ENT (Android)	Administrador de dispositivos heredado con Citrix MAM
Modo ENT (Android Enterprise)	Perfil de trabajo en dispositivos totalmente administrados, con Citrix MAM
Modo MAM (iOS y Android)	Citrix MAM
Modo MDM (iOS)	Inscripción de dispositivos Apple
Modo MDM (Android)	Administrador de dispositivos heredado
Modo MDM (Android Enterprise)	Perfil de trabajo en totalmente administrado

Cuando crea un grupo de entrega, puede adjuntar un perfil de inscripción al grupo. Si no adjunta un perfil de inscripción, Citrix Endpoint Management adjunta el perfil de inscripción global.

Los perfiles de inscripción ofrecen las siguientes funciones de administración de dispositivos:

- **Migración más sencilla del modo de administrador de dispositivos Android (DA) a Android Enterprise.** Para los dispositivos Android Enterprise, la configuración incluye un modo de propietario del dispositivo como: Totalmente administrado, perfil de trabajo en totalmente administrado o dedicado. Para obtener más información, consulte Android Enterprise.



Para esta actualización, las configuraciones actuales de Citrix Endpoint Management para el modo de servidor y **Configuración > Android Enterprise** se asignan a la nueva configuración del perfil de inscripción de la siguiente manera.

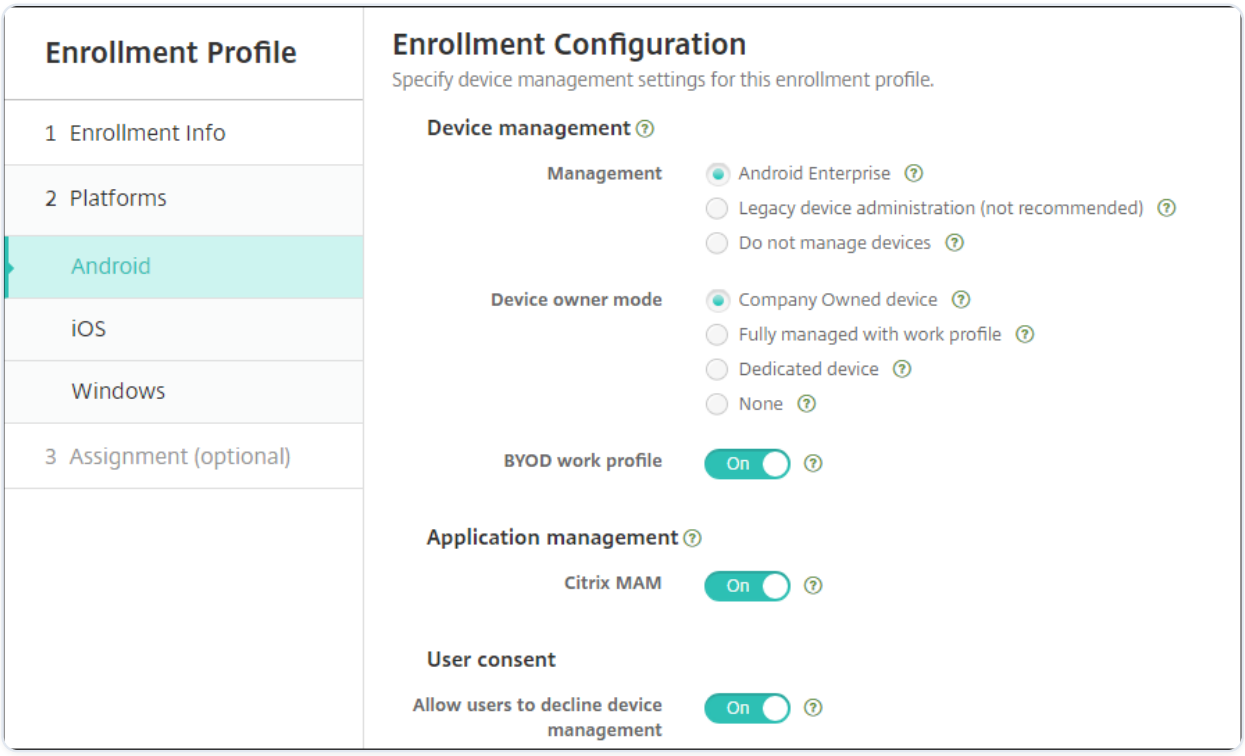
CONFIGURACIÓN ACTUAL	CONFIGURACIÓN DE ADMINISTRACIÓN	CONFIGURACIÓN DEL MODO DE PROPIETARIO DEL DISPOSITIVO	CONFIGURACIÓN DE CITRIX MAM
MDM; Google Play administrado (Android Enterprise)	Android Enterprise	Perfil de trabajo en totalmente administrado	Desactivado
MDM; Google Workspace (DA heredado)	DA heredado	no aplicable	Desactivado
MAM	No administrar dispositivos	no aplicable	Activado
MDM+MAM; Google Play administrado (Android Enterprise)	Android Enterprise*	Perfil de trabajo en totalmente administrado	Activado

CONFIGURACIÓN ACTUAL	CONFIGURACIÓN DE ADMINISTRACIÓN	CONFIGURACIÓN DEL MODO DE PROPIETARIO DEL DISPOSITIVO	CONFIGURACIÓN DE CITRIX MAM
MDM+MAM; Google Workspace (DA heredado)	DA heredado*	no aplicable	Activado

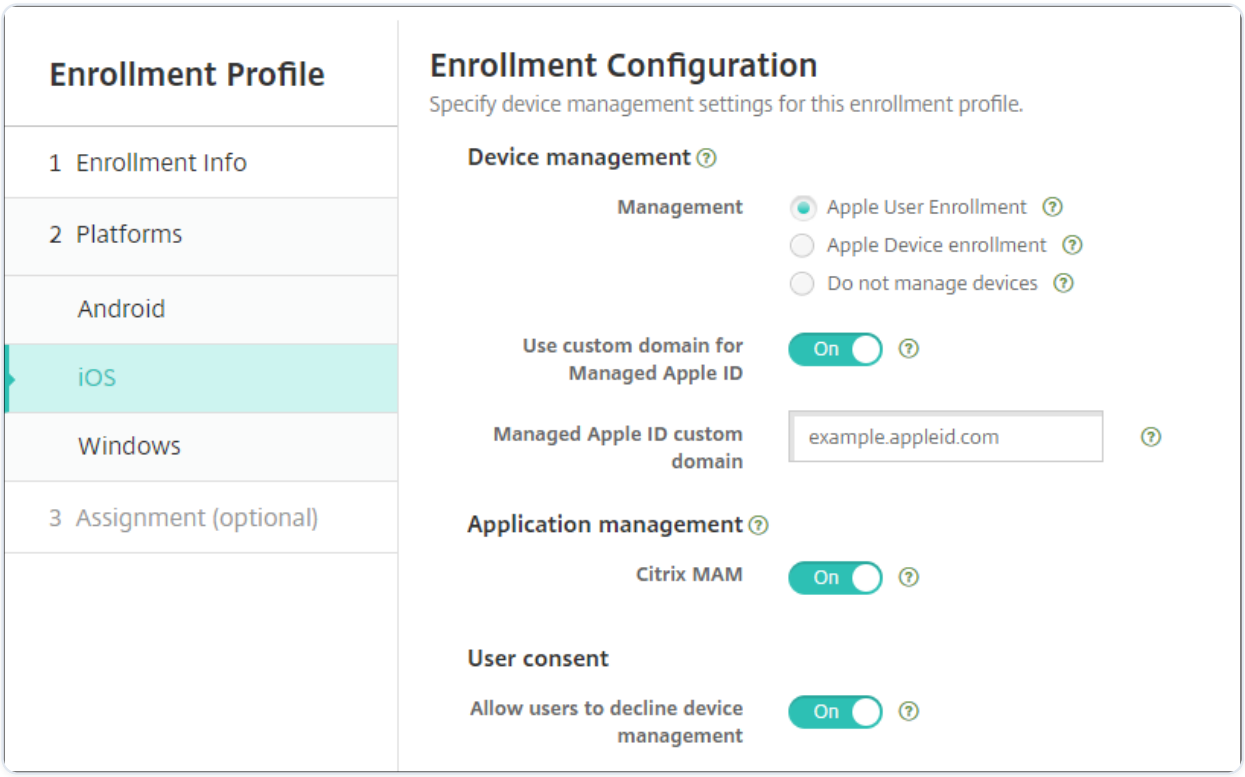
* Si la inscripción es obligatoria, **Permitir a los usuarios rechazar la administración de dispositivos** está **Desactivado**.

Después de la actualización, sus perfiles de inscripción actuales reflejan esas asignaciones. Considere si desea crear otros perfiles de inscripción para gestionar nuevos casos de uso a medida que abandona la DA heredada.

Si se incorpora a Citrix Endpoint Management 19.12.0 o posterior, el perfil de inscripción global tiene esta configuración predefinida.



- **Administración de iOS más sencilla.** Para los dispositivos iOS, la configuración incluye la opción de inscribir los dispositivos como administrados o no administrados.

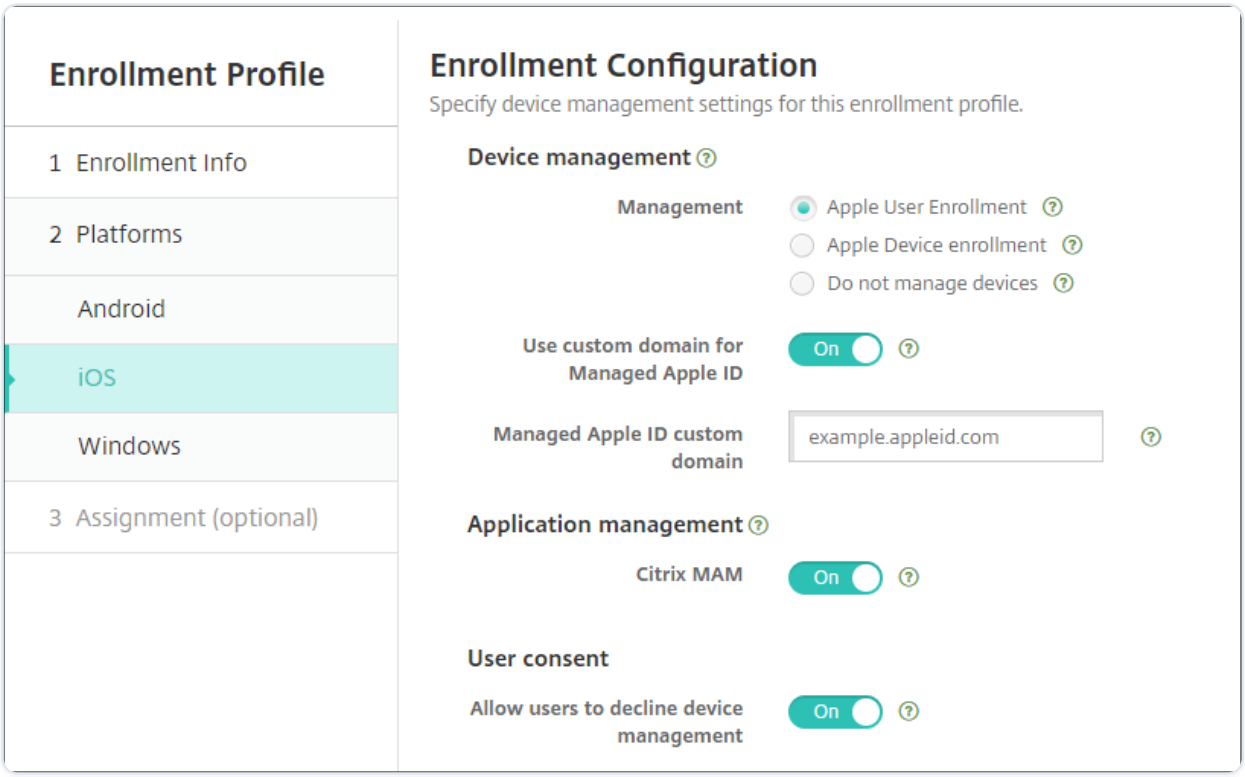


Para esta actualización, sus configuraciones anteriores se asignan a la nueva configuración del perfil de inscripción de la siguiente manera.

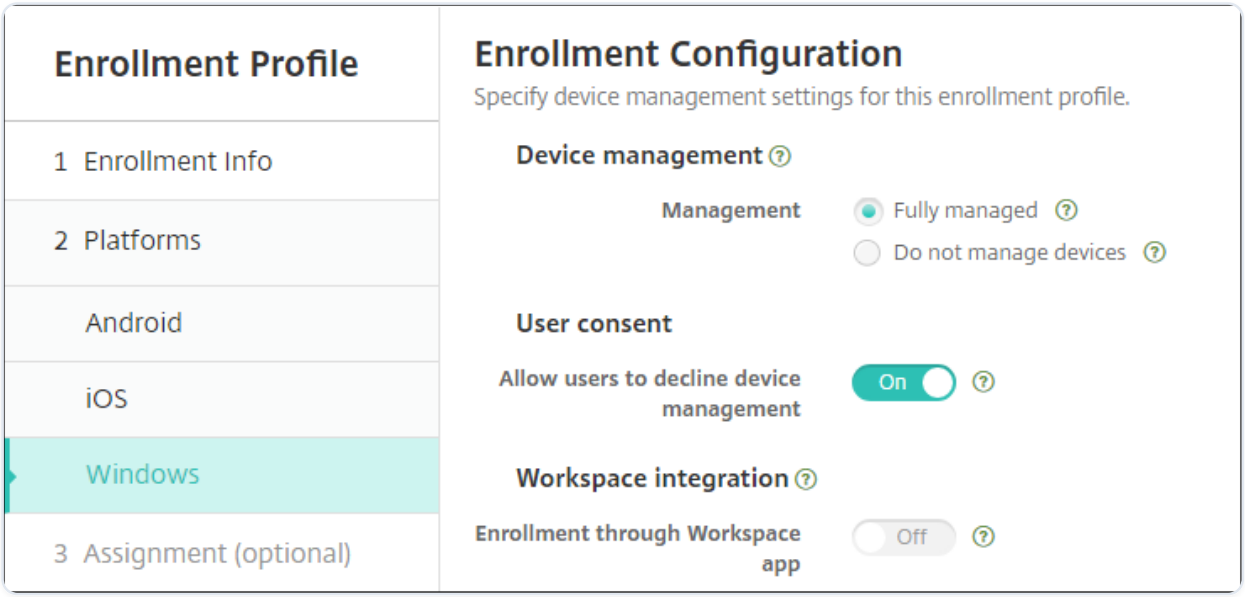
MODO DE SERVIDOR	CONFIGURACIÓN DE ADMINISTRACIÓN	CONFIGURACIÓN DE CITRIX MAM
MDM	Inscripción de dispositivos	Desactivado
MAM	No administrar dispositivos	Activado
MDM+MAM	Inscripción de dispositivos	Activado

Si la inscripción es obligatoria, **Permitir a los usuarios rechazar la administración de dispositivos** está **Desactivado**.

Si se incorpora a Citrix Endpoint Management 19.12.0 o posterior, el perfil de inscripción global tiene esta configuración predefinida.

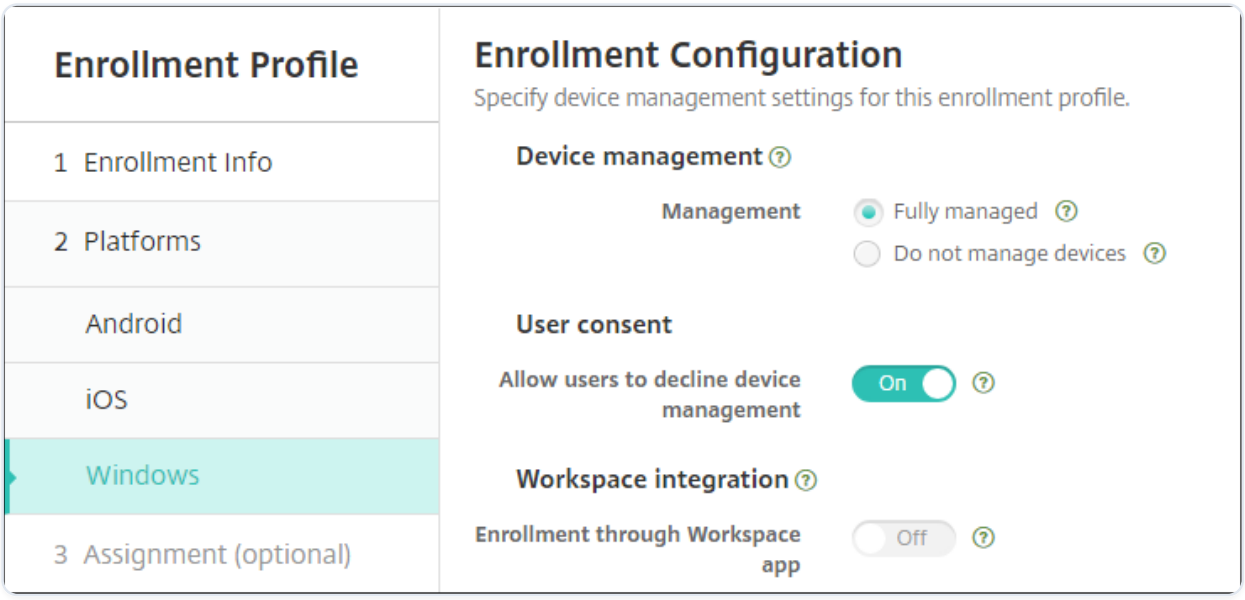


- **Permitir que los dispositivos Windows 10 se inscriban automáticamente en la aplicación Citrix Workspace.**



Para esta actualización, su configuración MDM anterior se asigna a la nueva configuración de perfil de inscripción **Totalmente administrado**.

Si se incorpora a Citrix Endpoint Management 19.12.0 o posterior, el perfil de inscripción global tiene esta configuración predefinida.



Existen las siguientes limitaciones para los perfiles de inscripción mejorados:

- La función de perfil de inscripción mejorado no funciona para dispositivos iOS y Android cuando Citrix Endpoint Management está integrado con Citrix Workspace.
- La función de perfil de inscripción mejorado no está disponible para invitaciones de inscripción con PIN de un solo uso o autenticación de dos factores.

Para obtener más información, consulte Perfiles de inscripción.

Otras actualizaciones en Citrix Endpoint Management 20.2.1

- **Inscripción simplificada de dispositivos Android Enterprise dedicados (COSU).** Citrix Endpoint Management ahora le permite inscribir dispositivos Android Enterprise dedicados (también conocidos como dispositivos COSU) creando un perfil de inscripción. Ya no es necesario crear una función de control de acceso basado en roles (RBAC) para inscribir dispositivos dedicados. Consulte Aprovisionamiento de dispositivos Android Enterprise dedicados.
- **Deshabilite la autenticación biométrica en dispositivos Android con la directiva de administración de Keyguard.** La directiva de dispositivo de administración de Keyguard ahora le permite deshabilitar el desbloqueo por huella dactilar, la autenticación facial, la autenticación de iris o toda la autenticación biométrica para dispositivos con Android 9.0 y versiones posteriores.
- **Obtenga orientación en el Centro de recursos.** Utilice el Centro de recursos para acceder a los datos del producto. Para obtener orientación desde el panel, haga clic en el icono de la esquina inferior derecha.



Problemas resueltos en Citrix Endpoint Management 20.2.1

Anteriormente, necesitaba permiso para editar dispositivos antes de poder usar la API de Citrix Endpoint Management para enviar notificaciones a los dispositivos. Ahora necesita el permiso Enviar notificación para enviar notificaciones.

Cuando inscribe un dispositivo de escritorio/tableta Windows habilitado para WEM y luego inscribe el mismo dispositivo en el MDM, la consola de Citrix Endpoint Management muestra dos entradas separadas para el dispositivo.

Citrix Endpoint Management 20.1.0

- **Compatibilidad con dispositivos Android Enterprise COPE.** Citrix Endpoint Management admite dispositivos Android Enterprise totalmente administrados con perfiles de trabajo. Google se refería anteriormente a esos dispositivos como dispositivos COPE (propiedad de la empresa y habilitados para uso personal).

  Los dispositivos Android Enterprise totalmente administrados tienen un perfil de dispositivo y un perfil de trabajo. Puede aplicar configuraciones de directiva separadas al dispositivo y al perfil de trabajo. Para esta versión:

  - Puede aplicar configuraciones separadas al dispositivo y al perfil de trabajo utilizando estas directivas de dispositivo: Credenciales, Administración de Keyguard, Código de acceso y Restricciones.
  - Puede aplicar la configuración del modo de ubicación de la directiva de dispositivo Ubicación al propio dispositivo COPE, pero no al perfil de trabajo del dispositivo COPE. Otras configuraciones de la directiva de dispositivo Ubicación no están disponibles para los dispositivos COPE. Consulte la directiva de dispositivo Ubicación.
  - Puede aplicar la acción de seguridad Bloquear por separado al dispositivo o al perfil de trabajo.

- **Inscripción automática de dispositivos Windows 10 a través de la aplicación Citrix Workspace.** Citrix Endpoint Management ahora puede inscribir automáticamente equipos de escritorio y tabletas Windows 10 mediante la aplicación Citrix Workspace.

Problemas resueltos en Citrix Endpoint Management 20.1.0

La página **Parámetros > Programa de implementación de Apple** no incluye opciones para omitir las nuevas pantallas del Asistente de configuración de iOS 13. Durante la inscripción, los usuarios deben hacer clic para avanzar por las pantallas de Introducción y Apariencia.

La ficha **Filtros** está abierta de forma predeterminada para **Administrar > Dispositivos**.

El inicio de sesión único (SSO) de ShareFile falla para clientes multiempresa en el mismo conjunto de máquinas virtuales.

Citrix Endpoint Management 19.12.0

Ahora puede configurar grupos de entrega para dispositivos Windows en función de las propiedades del dispositivo. (Versión preliminar) Al configurar grupos de entrega, ahora puede configurar grupos en función de las propiedades del dispositivo. Esta función solo está disponible para equipos de escritorio y tabletas Windows. Para solicitar acceso a esta función de versión preliminar, póngase en contacto con su representante de ventas o soporte de Citrix. Para obtener más información sobre esta función, consulte Agregar un grupo de entrega (versión preliminar).

Importe objetos de directiva de grupo (GPO) en Citrix Endpoint Management e impleméntelos directamente en dispositivos Windows 10. En lugar de depender de un administrador de AD para implementar GPO desde la consola de Administración de directivas de grupo, puede importar e implementar GPO a través de la consola de Citrix Endpoint Management. Consulte Directiva de dispositivo de configuración de GPO de Windows.

Instale aplicaciones EXE para equipos de escritorio y tabletas Windows. Ahora puede cargar aplicaciones EXE como aplicaciones empresariales para equipos de escritorio y tabletas Windows. Para obtener más información, consulte Agregar aplicaciones Win32 como aplicaciones empresariales.

Los usuarios ya no pueden quitar directivas de dispositivos iOS. Algunas directivas de dispositivo ya no permiten a los usuarios quitar la directiva de dispositivos iOS. La configuración **Permitir al usuario quitar la directiva** se ha quitado para iOS de las siguientes directivas: Directiva APN, Directiva de correo, Directiva de código de acceso, Directiva de perfil de aprovisionamiento, Directiva de proxy y Directiva VPN.

Problemas resueltos en Citrix Endpoint Management 19.12.0

Si actualiza el número de versión de una aplicación con la API REST pública de Citrix Endpoint Management y luego mediante la consola: La versión de la aplicación no se actualiza.

A veces, Citrix Endpoint Management no puede instalar aplicaciones EXE en dispositivos Windows porque el hash del archivo no es correcto.

Citrix Endpoint Management 19.11.0

Migración de Apple Volume Purchase Program a Apple Business Manager (ABM) y Apple School Manager (ASM)

Las empresas e instituciones que utilizan el Programa de compras por volumen de Apple (VPP) deben migrar a Aplicaciones y libros en Apple Business Manager o Apple School Manager antes de December 1, 2019.

Antes de migrar las cuentas VPP en Citrix Endpoint Management, consulte este artículo de soporte de Apple.

Si su organización o centro educativo solo utiliza el Programa de compras por volumen (VPP), puede inscribirse en ABM/ASM y, a continuación, invitar a los compradores de VPP existentes a su nueva cuenta de ABM/ASM. Para ASM, vaya a `<https://school.apple.com>`. Para ABM, vaya a `<https://business.apple.com>`.

Para actualizar su cuenta de Compras por volumen (anteriormente VPP) en Citrix Endpoint Management:

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje de la esquina superior derecha. Aparecerá la página **Parámetros**.
2. Haga clic en **Compras por volumen**. Aparecerá la página de configuración de **Compras por volumen**.
3. Asegúrese de que su cuenta de ABM o ASM tenga la misma configuración de aplicaciones que su cuenta VPP anterior.
4. En el portal de ABM o ASM, descargue un token actualizado.
5. En la consola de Citrix Endpoint Management, haga lo siguiente:
    a. Edite la cuenta de Compras por volumen existente con la información de token actualizada para esa ubicación.
    b. Edite sus credenciales de ABM o ASM. No cambie el sufijo.
    c. Haga clic en **Guardar** dos veces.

Para obtener más información, consulte:

- Compras por volumen de Apple

- Implementar dispositivos a través del Programa de implementación de Apple
- Inscripción masiva de dispositivos Apple(/es-es/citrix-endpoint-management/device-management/apple/ios-bulk-enrollment.html)

Los perfiles de inscripción controlan las opciones de inscripción para dispositivos Android

Los perfiles de inscripción ahora controlan cómo se inscriben los dispositivos Android si Android Enterprise está habilitado para su implementación de Citrix Endpoint Management. Los perfiles de inscripción determinan si los dispositivos Android se inscriben en el modo predeterminado de Android Enterprise (totalmente administrado o perfil de trabajo) o en el modo heredado (administrador de dispositivos).

De forma predeterminada, el perfil de inscripción global inscribe los dispositivos Android Enterprise nuevos y restablecidos de fábrica como dispositivos totalmente administrados e inscribe los dispositivos Android Enterprise BYOD como dispositivos con perfil de trabajo. Para obtener más información, consulte Android Enterprise.

Preparación de dispositivos Android heredados para Android Enterprise como inscripción predeterminada

Google está dejando de usar el modo de administrador de dispositivos para la administración de dispositivos y anima a los clientes a administrar todos los dispositivos Android en modo de propietario de dispositivo o modo de propietario de perfil. (Consulte Device admin deprecation en las guías para desarrolladores de Google Android Enterprise). Para admitir este cambio, Citrix convierte Android Enterprise en la opción de inscripción predeterminada para los dispositivos Android.

Este cambio significa que, si Android Enterprise está habilitado para su implementación de Citrix Endpoint Management, todos los dispositivos Android recién inscritos o reinscritos se inscriben como dispositivos Android Enterprise.

Para que pueda prepararse para este cambio, Citrix Endpoint Management ahora le permite crear perfiles de inscripción que controlan cómo se inscriben los dispositivos Android.

Es posible que su organización no esté lista para comenzar a administrar dispositivos Android heredados en modo de propietario de dispositivo o modo de propietario de perfil. En ese caso, puede seguir administrándolos en modo de administrador de dispositivos. Cree un perfil de inscripción para dispositivos heredados y vuelva a inscribir todos los dispositivos heredados inscritos.

Para crear un perfil de inscripción para dispositivos heredados:

1. En la consola de Citrix Endpoint Management, vaya a **Configure > Enrollment Profiles**.
2. Para agregar un perfil de inscripción, haga clic en **Add**. En la página Información de inscripción, escriba un nombre para el perfil de inscripción.
3. Haga clic en **Next** o seleccione **Android** en **Platforms**. Aparece la página Configuración de inscripción.
4. Establezca **Management** en **Legacy device administration (not recommended)**. Haga clic en **Next**.
5. Seleccione **Assignment (options)**. Aparece la pantalla Asignación de grupos de entrega.
6. Elija el grupo de entrega o los grupos de entrega que tienen los administradores que inscriben los dispositivos dedicados. Luego haga clic en **Guardar**.

Para seguir administrando los dispositivos heredados en el modo de administrador de dispositivos, inscríbalos o reinscríbalos con este perfil. Los dispositivos de administrador de dispositivos se inscriben de forma similar a los dispositivos de perfil de trabajo, haciendo que los usuarios descarguen Citrix Secure Hub y proporcionando una URL de servidor de inscripción.

Para obtener más información sobre la compatibilidad de Citrix Endpoint Management con la transición a Android Enterprise, consulte la entrada del blog, Android Enterprise as the default for Citrix Endpoint Management service.

Problemas resueltos en Citrix Endpoint Management 19.11.0

Al buscar una aplicación de Google Play Store en la consola de Citrix Endpoint Management, el nombre de la aplicación aparece vacío. Puede introducir el nombre manualmente para guardar la aplicación.

Después de cargar una aplicación MDX para Android Enterprise, es posible que la interfaz de usuario de la tienda de Google Play administrada no se abra en la consola de Citrix Endpoint Management. Hasta que se solucione el problema, vaya a la tienda de Google Play administrada para aprobar y guardar la aplicación manualmente.

Para iOS, el seguimiento de ubicación no funciona si hace lo siguiente: configurar e implementar una directiva de ubicación, habilitar el seguimiento desde las acciones de seguridad del dispositivo y, a continuación, eliminar la directiva de ubicación implementada y crear una nueva.

Los usuarios con apóstrofes en sus nombres de usuario no pueden inscribir sus dispositivos cuando su nombre de usuario se importa de LDAP.

Citrix Endpoint Management 19.10.0

Compatibilidad ampliada con Zebra OEMConfig. Citrix Endpoint Management ahora admite la administración de dispositivos Zebra mediante la herramienta administrativa de Zebra Technologies, Zebra OEMConfig. (Para obtener información, consulte el sitio web de Zebra Technologies.) Para administrar dispositivos con la aplicación Zebra OEMConfig, publique la aplicación y configure una directiva de dispositivo de configuraciones administradas.

Disponibilidad de la red de entrega de contenido (CDN) para aplicaciones de Windows. Ahora puede implementar aplicaciones de Windows mediante una red de entrega de contenido. Consulte Entregar aplicaciones empresariales desde la CDN de Citrix.

Compatibilidad con invitaciones de grupo para usuarios cuyos nombres incluyen caracteres especiales. Cuando elige un grupo para recibir invitaciones de inscripción, Citrix Endpoint Management ahora obtiene la lista de usuarios de Active Directory. La lista incluye usuarios cuyos nombres tienen caracteres especiales. Consulte Invitaciones de inscripción.

Problemas resueltos en Citrix Endpoint Management 19.10.0

Después de inscribir un dispositivo nuevo o reinscribir uno antiguo, aparece intermitentemente un mensaje de error en **Administrar > Dispositivos**.

Al seleccionar un dispositivo Chrome o Workspace hub en **Administrar > Dispositivos > Dispositivos inscritos** y, a continuación, hacer clic en **Editar**, aparece el siguiente mensaje: `A configuration error occurred. Please try again.` Ese mensaje también aparece al pasar el ratón por encima de esos dispositivos en la lista de dispositivos y hacer clic en **Mostrar más**. En cualquier caso, haga clic en **Aceptar** para continuar.

Citrix Endpoint Management 19.9.1

- **Compatibilidad con la administración de cifrado para iOS y Android.** Nota: Esta función está en desuso desde marzo de 2021. En su lugar, Citrix Endpoint Management utiliza el cifrado de dispositivos proporcionado por las plataformas iOS y Android. Citrix Endpoint Management complementa el cifrado basado en la plataforma con funciones como la comprobación de cumplimiento, disponible a través del SDK de Citrix MAM.
- **Compatibilidad con iPadOS.** Citrix Endpoint Management es compatible con iPadOS 13.x. Las directivas de dispositivo para iOS se aplican a los dispositivos que ejecutan iPadOS.
    - **Administración de aplicaciones simplificada para Android Enterprise.** Ya no es necesario ir a Google Play administrado o al portal de desarrolladores de Google para

aprobar o publicar aplicaciones para Citrix Endpoint Management. Como resultado, la aprobación y publicación de aplicaciones tarda unos 10 minutos en lugar de horas.

- **Apruebe aplicaciones de Android Enterprise para la tienda de aplicaciones pública en la consola de Citrix Endpoint Management.** Ahora puede aprobar aplicaciones de la tienda Google Play administrada sin salir de la consola de Citrix Endpoint Management. Después de introducir un nombre de aplicación en el campo de búsqueda, se abre la interfaz de usuario de la tienda Google Play administrada con las instrucciones para que apruebe y guarde la aplicación. Su aplicación se rellena en los resultados, lo que le permite configurar sus detalles. Consulte Agregar una aplicación de la tienda de aplicaciones pública.
- **Apruebe las aplicaciones MDX para Android Enterprise en la consola de Citrix Endpoint Management.** Ahora puede aprobar aplicaciones de la tienda Google Play administrada para Android Enterprise sin salir de la consola de Citrix Endpoint Management. Después de cargar un archivo MDX, se abre la interfaz de usuario de la tienda Google Play administrada con las instrucciones para que apruebe y guarde la aplicación. Consulte Agregar una aplicación MDX.
- **Publique aplicaciones empresariales para Android Enterprise en la consola de Citrix Endpoint Management.** Ya no es necesario registrarse para obtener una cuenta de desarrollador de Google Play al agregar una aplicación privada de Android Enterprise. La consola de Citrix Endpoint Management abre una interfaz de usuario de la tienda Google Play administrada para que cargue y publique el archivo APK. Consulte Agregar una aplicación empresarial.

- **Más funciones de administración de certificados para dispositivos Android Enterprise en modo de perfil de trabajo o modo totalmente administrado.** Además de instalar autoridades de certificación en el almacén de claves administrado, ahora puede administrar las siguientes funciones:

  - **Configure los certificados utilizados por aplicaciones administradas específicas.** La directiva de dispositivo Credenciales para Android Enterprise ahora incluye la configuración **Aplicaciones para usar los certificados**. Puede especificar las aplicaciones que usarán los certificados de usuario emitidos por el proveedor de credenciales seleccionado en esta directiva. Las aplicaciones obtienen acceso a los certificados de forma silenciosa durante el tiempo de ejecución. Para usar los certificados para todas las aplicaciones, deje la lista de aplicaciones en blanco. Consulte Directiva de dispositivo de credenciales.

  - **Elimine certificados de forma silenciosa del almacén de claves administrado o desinstale todos los certificados de autoridad de certificación que no sean del sistema.** Consulte Directiva de dispositivo de credenciales.
  - **Evite que los usuarios modifiquen las credenciales almacenadas en el almacén de claves administrado.** La directiva de dispositivo Restricciones para Android Enterprise ahora incluye la configuración **Permitir al usuario configurar credenciales de usuario**. De forma predeterminada, esa configuración está establecida como **Activada**. Consulte Directiva de dispositivo de restricciones.

- **Directiva de dispositivo de ubicación ahora disponible para Android Enterprise.** Puede definir la configuración de ubicación para dispositivos Android Enterprise que están administrados o que se ejecutan en modo de perfil administrado. El seguimiento de ubicación de Android requiere Android 8.5 y versiones posteriores. Consulte Directiva de dispositivo de ubicación.
- **Fácil acceso a las claves de recuperación de BitLocker.** Si un usuario pierde su clave de recuperación de BitLocker, desbloquear su dispositivo puede ser un desafío. Citrix Endpoint Management ahora muestra la clave de recuperación de BitLocker para escritorios y tabletas Windows en los detalles del dispositivo. Consulte Clave de recuperación de BitLocker.

Problemas resueltos en Citrix Endpoint Management 19.9.1

Después de agregar una propiedad personalizada con un carácter especial, los administradores no pueden acceder a la página Dispositivos en la consola de XenMobile®.

En macOS, las aplicaciones empresariales enviadas desde Citrix Endpoint Management permanecen en estado pendiente. Este problema de terceros es el error de Apple #50311461 y está corregido en macOS 10.14.4.

El rol RBAC `Tier 2 techs` no puede crear invitaciones de inscripción para un grupo de usuarios con más de 2000 usuarios. Solo los usuarios administrativos completos pueden crear las invitaciones.

En los dispositivos iOS, los administradores pueden perder la capacidad de enviar un comando de «desbloquear dispositivo» a los dispositivos protegidos con código de acceso después de que el dispositivo se actualice a iOS 13.1.x. Para resolver este problema, consulte `https://support.citrix.com/article/CTX262076`.

Citrix Endpoint Management 19.9.0

- **Administre las funciones de bloqueo de pantalla para el perfil de trabajo de Android Enterprise y los dispositivos totalmente administrados.** El bloqueo de pantalla de Android administra las pantallas de bloqueo del dispositivo y del desafío de trabajo. Utilice la directiva de dispositivo de administración de bloqueo de pantalla para controlar:

  - Administración del bloqueo de pantalla en dispositivos con perfil de trabajo. Puede especificar las funciones disponibles para los usuarios antes de que desbloqueen el bloqueo de pantalla del dispositivo y el bloqueo de pantalla del desafío de trabajo. Por ejemplo, de forma predeterminada, los usuarios pueden usar el desbloqueo con huella digital y ver notificaciones sin censura en la pantalla de bloqueo.
  - Administración del bloqueo de pantalla en dispositivos totalmente administrados y dedicados. Puede especificar las funciones disponibles, como agentes de confianza y cámara segura, antes de que desbloqueen la pantalla de bloqueo. O bien, puede optar por deshabilitar todas las funciones de bloqueo de pantalla.

  Consulte Directiva de dispositivo de administración de bloqueo de pantalla.

- **Restablecimiento de contraseña del contenedor Samsung Knox.** La acción de seguridad **Restablecimiento de contraseña del contenedor** ya no está disponible para los dispositivos Samsung Knox de Android Enterprise. Utilice la acción de seguridad **Bloqueo del contenedor** para restablecer las contraseñas de los contenedores Samsung Knox. La acción de seguridad **Restablecimiento de contraseña del contenedor** sigue estando disponible para los dispositivos Samsung en modo de administrador de dispositivos.
- **Configure la pista de producto para sus aplicaciones de Android Enterprise.** Al añadir una aplicación de tienda pública o una aplicación MDX para Android Enterprise, configure la pista de producto que desea enviar a los dispositivos de los usuarios. Por ejemplo, si tiene una pista diseñada para pruebas, puede seleccionarla y asignarla a un grupo de entrega específico. Para obtener más información sobre cómo implementar su versión, consulte el Centro de ayuda de Google Play. Para obtener información sobre cómo configurar la pista de producto, consulte Agregar una aplicación MDX o Agregar una aplicación de tienda pública.
- **Directiva de configuración de GPO de Windows habilitada automáticamente.** La directiva de configuración de GPO de Windows se habilita automáticamente si aprovisiona un sitio de Citrix Workspace Environment Management en Citrix Cloud. Para obtener más información, consulte Directiva de dispositivo de configuración de GPO de Windows.
- **Dispositivos administrados por Mobile Device Management (MDM) y Workspace Environment Management (WEM) fusionados en la consola.** Si un dispositivo está administrado tanto por MDM como por WEM, ahora se muestra como un solo dispositivo en la

consola de Citrix Endpoint Management. La etiqueta del dispositivo en la consola es **MDM, WEM**. Anteriormente, el dispositivo se mostraba como dos dispositivos diferentes. Ahora también puede eliminar dispositivos administrados por MDM y WEM.

Problemas resueltos en Citrix Endpoint Management 19.9.0

Después de implementar la directiva de dispositivo de acceso a aplicaciones, los dispositivos no conformes no activan la acción configurada.

No puede configurar las credenciales de administrador de Google Workspace para dispositivos Chrome OS.

La conectividad entre Citrix Endpoint Management y Apple School Manager falla.

Los dispositivos MAM borran las aplicaciones y los datos de las aplicaciones debido a un error al obtener los detalles del dominio del usuario. Como resultado, el dispositivo considera al usuario como eliminado.

Después de inscribir un dispositivo nuevo o volver a inscribir uno antiguo, aparece intermitentemente un mensaje de error en la ficha **Administrar**.

Citrix Endpoint Management 19.8.0

- **Para clientes existentes: Acceso restringido a puertos para la consola de Citrix Endpoint Management y el portal de autoayuda:**

  Para los clientes que se incorporaron antes de Citrix Endpoint Management 19.8.0 (August 1, 2019):

  - Puede exigir que los administradores inicien sesión en la consola de Citrix Cloud para el acceso SSO a la consola de Citrix Endpoint Management. Citrix recomienda encarecidamente todo el acceso a la consola a través de Citrix Cloud.

    Establezca la nueva propiedad de servidor `enable.cloud.console.sso` en **True**, lo que significa que no puede acceder directamente a la consola de Citrix Endpoint Management. Los intentos de acceder directamente a la consola de Citrix Endpoint Management en el puerto 4443 dan como resultado un error 500.
  - El acceso al portal de autoayuda solo está disponible a través del puerto 443. Los intentos de acceso a través del puerto 4443 ahora dan como resultado un mensaje de "Acceso denegado".

- **Para clientes que se incorporan a partir de Citrix Endpoint Management 19.8.0 (August 1, 2019):**
  - Los nuevos clientes inician sesión en la consola de Citrix Cloud para el acceso SSO a la consola de Citrix Endpoint Management.
  - El acceso al portal de autoayuda requiere un cambio en la propiedad del servidor. De forma predeterminada, los nuevos clientes no pueden acceder al portal de autoayuda.

    Para dar a sus usuarios acceso al portal de autoayuda, actualice `shp.console.enable` a **True**.

Problemas resueltos en Citrix Endpoint Management 19.8.0

Al importar un certificado de CA, la consola no muestra un certificado actualizado o nuevo en **Entidades PKI**.

Al configurar la política de dispositivo VPN para iOS para usar el protocolo Citrix SSO: Después de habilitar la configuración **Solicitar PIN al conectar** y guardar la política, esa configuración vuelve a **Desactivado**.

Para los clientes que han migrado desde versiones anteriores, al abrir la ficha **Administrar** en la consola, se muestra un error si se ha eliminado el perfil de inscripción de un dispositivo.

Citrix Endpoint Management 19.7.1

- **Acceder a todas las aplicaciones de Google Play en la tienda administrada de Google Play.** La propiedad de servidor **Acceder a todas las aplicaciones en la tienda administrada de Google Play** hace que todas las aplicaciones de la tienda pública de Google Play sean accesibles desde la tienda administrada de Google Play. Al establecer esta propiedad en **true**, se permite el acceso a las aplicaciones de la tienda pública de Google Play para todos los usuarios de Android Enterprise. Los administradores pueden usar la política de dispositivo Restricciones para controlar el acceso a estas aplicaciones.
- **Habilitar aplicaciones del sistema en dispositivos Android Enterprise.** Para permitir a los usuarios ejecutar aplicaciones del sistema preinstaladas en el modo de perfil de trabajo de Android Enterprise o en el modo totalmente administrado, configure la política de dispositivo Restricciones. Esa configuración concede al usuario acceso a las aplicaciones predeterminadas del dispositivo, como la cámara, la galería y otras. Para restringir el acceso a una aplicación en particular, establezca los permisos de la aplicación mediante la política de permisos de aplicaciones.

Problemas resueltos en Citrix Endpoint Management 19.7.1

Al enviar un enlace de inscripción mediante SMTP/SMS, el enlace enviado no funciona.

Al intentar actualizar una aplicación pública de iOS mediante la consola de Citrix Endpoint Management, se muestra un error de configuración.

Algunas aplicaciones de compra por volumen de terceros no se actualizan automáticamente. Este problema se produjo debido a nombres de host bloqueados. Para obtener más información, consulte `<https://support.apple.com/es-es/HT201999>`.

Al agregar Microsoft Word o PowerPoint para iOS a la biblioteca de aplicaciones en la nube, la asignación de la aplicación a un grupo de usuarios falla. Debe eliminar y volver a agregar cualquier aplicación de Intune que experimente este problema.

Citrix Endpoint Management 19.6.1

- **La política de dispositivo de ubicación ahora permite el seguimiento de dispositivos para Android.** Ahora puede habilitar el seguimiento de dispositivos para sondear dispositivos específicos con la frecuencia que defina. Puede usar esta política para rastrear al personal de entrega para obtener estimaciones de entrega más precisas, rastrear dispositivos perdidos o robados, o aplicar límites geográficos. Para obtener más información, consulte política de dispositivo de ubicación.

Problemas resueltos en Citrix Endpoint Management 19.6.1

Los iconos de las aplicaciones no se muestran en la consola de Citrix Endpoint Management para las aplicaciones que se cargaron automáticamente.

Una vez finalizado el período de tiempo en la propiedad del servidor `bulk.enrollment.fetchRosterInfoDelay` y un dispositivo de Apple School Manager se sincroniza con el servidor: La cuenta de usuario de Apple School Manager se elimina del servidor y el dispositivo pasa a un estado anónimo.

Los usuarios con caracteres alemanes especiales, como las diéresis, en su nombre para mostrar no pueden inscribirse.

El siguiente mensaje de error aparece al intentar configurar una aplicación pública mediante la nueva URL de la aplicación de Apple Store: "No se pudo encontrar la aplicación que introdujo. Compruebe la URL e inténtelo de nuevo."

Citrix Endpoint Management 19.6.0

- **Actualizaciones automáticas para aplicaciones de compra por volumen de Apple.** Al agregar una cuenta de compra por volumen (**Parámetros > Parámetros de iOS**), ahora puede habilitar las actualizaciones automáticas para todas las aplicaciones de iOS. Consulte el parámetro **Actualización automática de aplicaciones** en Compra por volumen de Apple.

Problemas resueltos en Citrix Endpoint Management 19.6.0

Se muestra el siguiente error al agregar una clave de Registro a una directiva de Windows Embedded Compact si la longitud del valor del Registro supera los 2048 caracteres: `Console error: could not execute statement; SQL [n/a]; nested exception is org.hibernate.exception.DataException: could not execute statement`.

Durante la instalación del perfil en un dispositivo iOS, aparece "No verificado" en la información del perfil.

Cuando un usuario de Azure AD inicia sesión en algunos dispositivos Windows 10 unidos a Azure AD configurados como quioscos, el modo quiosco no se activa. Este problema no ocurre si introduce el nombre de usuario de Azure AD en el formato `azuread\user`. Para obtener más información, consulte Directiva de dispositivos de quiosco.

Los iconos de las aplicaciones no se muestran en la consola de Citrix Endpoint Management para las aplicaciones que se cargaron automáticamente.

Al agregar una cuenta de compra por volumen (**Parámetros > Parámetros de iOS**), aparece el siguiente mensaje si el token supera los 350 caracteres: `The entered company token is not valid, please enter a new one.`

Citrix Endpoint Management 19.5.0

- **Cambio en el flujo de trabajo de inscripción de MDM para iOS.** Para mejorar la seguridad de la plataforma reduciendo las instalaciones de perfiles engañosas, Apple lanzó un nuevo flujo de trabajo para inscribir manualmente dispositivos en MDM. Este nuevo flujo de trabajo afecta a todas las soluciones MDM, incluida Citrix Endpoint Management.

  No hay cambios para la inscripción de MDM en los servidores asignados en Apple Business Manager o Apple School Manager. Los cambios en el flujo de trabajo son solo para la inscripción manual en MDM.

  Citrix también ha simplificado la inscripción. Anteriormente, los usuarios de dispositivos iOS recibían dos mensajes durante la inscripción: un mensaje para la CA raíz y un mensaje para el

certificado de dispositivo MDM. Citrix instaló la CA raíz para tener flexibilidad al usar certificados firmados y sin firmar. Dado que todas las implementaciones de Citrix Cloud utilizan certificados de confianza, la CA raíz ya no es necesaria.

Los usuarios de dispositivos iOS solo reciben el mensaje del certificado de dispositivo MDM durante la inscripción. Ese mensaje se etiqueta como "Servicio de perfiles de XenMobile".

Para admitir este cambio, Citrix cambió el valor de la propiedad del servidor, `ios.mdm.enrollment.installRootCaIfRequired`, a `false`. Se abre una ventana de Safari durante la inscripción de MDM para simplificar la instalación del perfil para los usuarios. Para obtener más información, consulte Inscribir dispositivos iOS y el siguiente vídeo de YouTube:



- **Cambios para los nuevos clientes de Citrix Endpoint Management:**
  - **Implementación de la experiencia Workspace.** Puede crear un grupo de entrega independiente, denominado Workspace, para empezar a implementar la experiencia Workspace en los nuevos dispositivos. Al utilizar el grupo de entrega Workspace, puede ofrecer la experiencia Workspace a un grupo pequeño sin interrumpir a todos los usuarios.
  - **Directivas y aplicaciones preconfiguradas para nuevos clientes de Citrix Endpoint Management 19.5.0.** Si se incorpora a partir de Citrix Endpoint Management 19.5.0 o posterior, preconfiguramos algunas directivas de dispositivo y aplicaciones de productividad móvil. Esa configuración le permite implementar inmediatamente la

funcionalidad básica para los usuarios del dispositivo. Consulte Directivas de dispositivo predeterminadas y aplicaciones de productividad móvil.

- **Directiva de dispositivo Knox Platform for Enterprise para Android Enterprise (obsoleta).** Ahora puede introducir las claves de licencia KPE Premium y Standard para dispositivos Android Enterprise que ejecuten Knox versión 3.0 o posterior.
- **Directiva de dispositivo de sesión pública para Chrome OS.** Ahora puede configurar dispositivos Chrome OS para admitir sesiones de invitado. Para obtener información sobre cómo configurar esta directiva, consulte Directiva de dispositivo de sesión pública.
- **Cambios en los permisos de RBAC.** El permiso RBAC Agregar/Eliminar usuarios locales ahora se divide en dos permisos: Agregar usuarios locales y Eliminar usuarios locales.

Problemas resueltos en Citrix Endpoint Management 19.5.0

Las aplicaciones empresariales no se actualizan silenciosamente en dispositivos supervisados que ejecutan iOS 11.4 o posterior.

Al editar una directiva de dispositivo, aparece el siguiente mensaje de error: `A configuration error occurred. Please try again`.

Citrix Endpoint Management 19.4.1

- **Mediante la integración de Workspace Environment Management (WEM) con Citrix Endpoint Management, puede administrar todos los dispositivos Windows unidos a un dominio compatibles.** Esta integración ofrece los siguientes beneficios y funciones:
  - Solo con WEM, las implementaciones de MDM no son posibles. Solo con Citrix Endpoint Management, está limitado a administrar dispositivos Windows 10. Al integrar los dos productos:
    - WEM puede acceder a las funciones de MDM
    - Puede administrar un espectro más amplio de sistemas operativos Windows a través de Citrix Endpoint Management.
  - Esa administración se realiza mediante la configuración de GPO de Windows. Actualmente, los administradores importan un archivo ADMX a Citrix Endpoint Management y lo envían a equipos de escritorio y tabletas con Windows 10 para configurar aplicaciones específicas. Mediante la directiva de dispositivo Configuración de GPO de Windows, puede configurar GPO y enviar cambios al servicio WEM. El agente WEM aplica entonces los GPO a los dispositivos y sus aplicaciones.

- La administración de MDM no es un requisito para la integración de WEM. Cualquier dispositivo compatible con WEM puede recibir configuraciones de GPO, incluso si Citrix Endpoint Management no es compatible con ese dispositivo de forma nativa.
- Para obtener una lista de los dispositivos compatibles, consulte Requisitos del sistema operativo.
- Los dispositivos que reciben la directiva de dispositivo Configuración de GPO de Windows se ejecutan en un nuevo modo de Citrix Endpoint Management llamado WEM. En la lista de dispositivos inscritos de **Administrar > Dispositivos**, la columna **Modo** para los dispositivos administrados por WEM muestra **WEM**.

Para obtener más información, consulte Directiva de dispositivo Configuración de GPO de Windows.

- **La entrega de aplicaciones empresariales por CDN es ahora la predeterminada para los nuevos clientes de multitenencia de Citrix Endpoint Management 19.4.1.** Si es un nuevo cliente en la región de Asia Pacífico, póngase en contacto con su representante de soporte de Citrix para habilitar la entrega por CDN. En todas las regiones, los clientes existentes que deseen entregar aplicaciones empresariales mediante CDN deben volver a cargar las aplicaciones existentes después de habilitar la función. Consulte Entregar aplicaciones empresariales desde la CDN de Citrix.
- **Compatibilidad con aplicaciones web y SaaS y enlaces web para Android Enterprise.** Citrix Endpoint Management ahora admite la entrega de enlaces para aplicaciones web o SaaS y enlaces web a dispositivos Android Enterprise. Las aplicaciones web y SaaS y los enlaces web se agregan para Android Enterprise de la misma manera que se agregan para otras plataformas. Consulte Agregar una aplicación web o SaaS y Agregar un enlace web.
- **Más restricciones para dispositivos Chrome OS:**
  - **Mostrar instrucciones en dispositivos inhabilitados.** Ahora puede agregar un mensaje personalizado para mostrar en dispositivos Chrome OS inhabilitados.
  - **Permitir a los usuarios instalar extensiones, aplicaciones y temas específicos.** Introduzca la lista de URL para permitir la descarga desde esas fuentes.

  Para obtener más información, consulte Configuración de Chrome OS.

Problemas resueltos en Citrix Endpoint Management 19.4.1

En los dispositivos Android Enterprise, es posible que los siguientes tipos de aplicaciones no aparezcan en Citrix Secure Hub: Aplicaciones de tiendas de aplicaciones públicas configuradas en la plataforma Google Play y aplicaciones empresariales configuradas en la plataforma Android.

Las aplicaciones de Android Enterprise no aparecen en los dispositivos hasta que se anulan la inscripción y se vuelven a inscribir. Las aplicaciones también aparecen si las actualiza en sus grupos de entrega.

Las acciones automatizadas podrían no implementarse en dispositivos Android Enterprise.

El nombre y el propietario de su empresa de Android Enterprise podrían no mostrarse correctamente en la consola de administración de Google Play Store.

Citrix Endpoint Management 19.3.1

Problemas resueltos en Citrix Endpoint Management 19.3.1

Si implementó una directiva de dispositivo de Store para dispositivos de escritorio y tabletas con Windows 10 antes de la versión 19.3.1: Cuando un usuario hace clic en el enlace de la tienda de Windows en el menú Inicio, aparece un mensaje: "500 Internal Server Error" o "HTTP Status 404 - Either you've reached an old URL or this device isn't registered". Para resolver este problema, debe volver a crear e implementar su directiva de dispositivo de Store.

Si un grupo de usuarios de Active Directory está asignado a un permiso de rol de RBAC, no puede eliminar la configuración de LDAP que tiene ese grupo de usuarios. Como solución alternativa, si desasigna el grupo de Active Directory correspondiente de RBAC, puede eliminar el dominio.

Citrix Endpoint Management 19.3.0

- **Compatibilidad con Samsung Knox en la unificación de directivas de Android Enterprise.** Para dispositivos Android Enterprise que ejecutan Samsung Knox 3.0 o posterior y Android 8.0 o posterior: Knox y Android Enterprise se combinan en una solución unificada de administración de dispositivos y perfiles. Configure los ajustes de Knox en la página de Android Enterprise de las siguientes directivas de dispositivo:
    - **Directiva de dispositivo de actualización del SO.** Controle las actualizaciones FOTA de Samsung Enterprise. Consulte Directiva de dispositivo de actualización del SO.
    - **Directiva de dispositivo de código de acceso.** Consulte Directiva de dispositivo de código de acceso.
    - **Directiva de dispositivo de restricciones.** Consulte Directiva de dispositivo de restricciones.
    - **Directiva de dispositivo de clave de licencia de Samsung MDM (obsoleta).** Configure la clave de licencia de Knox.

- **Directiva de dispositivo de inventario de aplicaciones para Android Enterprise.** Ahora puede recopilar un inventario de las aplicaciones de Android Enterprise en los dispositivos administrados. Para obtener más información, consulte Directiva de dispositivo de inventario de aplicaciones.
- **Directiva de dispositivo de archivos para Android Enterprise.** Ahora puede agregar archivos de script a Citrix Endpoint Management para realizar funciones en dispositivos Android Enterprise. Consulte Directiva de dispositivo de archivos.
- **Bloquear y restablecer la contraseña para Android Enterprise.** Citrix Endpoint Management ahora es compatible con la acción de seguridad Bloquear y restablecer contraseña para dispositivos Android Enterprise inscritos en el modo de perfil de trabajo que ejecutan Android 8.0 o superior. Consulte Acciones de seguridad.
- **Compatibilidad con Azure Active Directory en un quiosco en dispositivos de escritorio y tabletas con Windows 10.** Ahora puede añadir dispositivos de Azure AD unidos a un dominio en modo Quiosco. Consulte Directiva de dispositivos de quiosco.
- **Para los clientes de Citrix Endpoint Management con la experiencia de espacio de trabajo habilitada: Citrix Endpoint Management admite la autenticación federada a través de la aplicación Citrix Workspace en iOS y Android.** Esta función no es compatible con Azure Active Directory. Para obtener información, consulte Elegir o cambiar métodos de autenticación.
- **Cambio en la API REST pública.** La API pública de Citrix Endpoint Management para servicios REST ahora incluye una API para modificar los detalles de la plataforma dentro del contenedor para aplicaciones MDX. Consulte la "Sección 3.15.2.4 Actualizar los detalles de la plataforma dentro del contenedor para aplicaciones MDX" en el PDF, API pública para servicios REST.

Problemas resueltos en Citrix Endpoint Management 19.3.0

El bloqueo remoto de dispositivos Android Enterprise totalmente administrados mediante la acción de seguridad **Bloquear con código de acceso** podría fallar sin notificarle el error. Para asegurarse de que un dispositivo está bloqueado, configure **Bloquear con código de acceso** dos veces. El dispositivo se bloquea con el segundo código de acceso que configure.

Si la empresa se elimina de Managed Google Play y se actualiza en el servidor de Citrix Endpoint Management, los dispositivos Android Enterprise a veces no pueden inscribirse.

Para la integración de Citrix Endpoint Management con Microsoft Endpoint Manager: Los cambios realizados en el nombre o la descripción de una aplicación de la tienda Intune no se guardan.

Después de editar una aplicación Intune de iOS, la aplicación no se instalará desde la aplicación Microsoft Company Portal.

Si se le asigna permiso como administrador personalizado de Citrix Cloud en lugar de administrador completo, no podrá hacer clic en el botón **Administrar** para navegar por los recursos.

Desuso de las versiones de TLS

Para mejorar la seguridad del servicio Citrix Endpoint Management, Citrix ahora bloquea cualquier comunicación a través de Transport Layer Security (TLS) 1.0 y 1.1. Debido a su seguridad debilitada, el Consejo PCI está dejando de usar TLS 1.0.

Cómo le afecta este cambio

Si utiliza la administración de aplicaciones móviles a través de un NetScaler Gateway (NetScaler Gateway) local, debe actualizar su servicio de equilibrio de carga para habilitar TLS 1.2.

Las versiones anteriores de los siguientes conectores solo admiten TLS 1.0:

- Conector de Citrix Endpoint Management para Exchange ActiveSync
- Conector de NetScaler Gateway para Exchange ActiveSync

Actualice el conector de la siguiente manera:

- Si utiliza el conector de Citrix Endpoint Management para Exchange ActiveSync compilación 10.1.3 o anterior, actualice a la compilación 10.1.4 o posterior.
- Si utiliza el conector de NetScaler Gateway para Exchange ActiveSync compilación 8.5.0 o anterior, actualice a la compilación 8.5.1.11 o posterior.

Qué hacer

Si utiliza un NetScaler Gateway (NetScaler Gateway) local, habilite TLS 1.2 en el servicio de equilibrio de carga. Para obtener más información, consulte `<https://support.citrix.com/article/CTX247095>`.

Para descargar cualquiera de los conectores para Exchange ActiveSync:

```
1.  Go to `<https://www.citrix.com/downloads>`.

1.  Navigate to **Citrix Endpoint Management (and Citrix XenMobile Server)
> XenMobile Server (on-premises) > Product Software > XenMobile Server 10
> Server Components**.
```

```
1.  Locate the connector tile and then click **Download File**.
```

Citrix Endpoint Management 19.2.1

- **Ejecute varias aplicaciones en un quiosco en dispositivos Chrome.** Ahora puede agregar varias aplicaciones a la directiva de quiosco para Chrome OS. Opcionalmente, puede iniciar aplicaciones automáticamente cuando el usuario inicia el dispositivo. Consulte la directiva de dispositivos de quiosco.

Problemas resueltos en Citrix Endpoint Management 19.2.1

Después de anular la inscripción de un dispositivo Android Enterprise y volver a inscribirlo, es posible que las aplicaciones aprobadas no aparezcan en los dispositivos inscritos en el modo de perfil de trabajo.

Cuando los usuarios ejecutan Citrix Secure Mail por primera vez en Intune MDM+MAM, la configuración guía a los usuarios a través de un flujo de trabajo para seleccionar Intune MAM/ XenMobile.

Citrix Endpoint Management 19.2.0

- **Distribuya aplicaciones empresariales desde una red de entrega de contenido (CDN).** Cuando un usuario no se encuentra cerca de un servidor de Citrix Endpoint Management, la entrega de aplicaciones empresariales puede tardar un tiempo. Para descargas de aplicaciones más rápidas, puede hacer que las aplicaciones empresariales se entreguen desde ubicaciones de red de entrega de contenido (CDN) en todo el mundo. La compatibilidad con CDN para aplicaciones empresariales está disponible para aplicaciones iOS (inscripción MDM o MAM) y aplicaciones Android (inscripción MDM o MAM). La compatibilidad con CDN para aplicaciones empresariales no está disponible para aplicaciones de Windows. Para empezar, consulte Distribuir aplicaciones empresariales desde Citrix CDN.
- **Cambio en la inscripción de dispositivos DEP para Citrix Workspace.** Si Citrix Endpoint Management está integrado con Citrix Workspace, la aplicación Citrix Workspace se incluye en el paquete de implementación de DEP como una aplicación obligatoria. Esta función requiere que configure los ajustes de su cuenta DEP para iOS con las credenciales requeridas desactivadas. Citrix Secure Hub solicita a los usuarios que inscriban el dispositivo en Citrix Workspace antes de inscribirlo en Citrix Endpoint Management.
- **La propiedad de servidor ios.mdm.enrollment.installRootCalfRequired ahora está establecida en false.** Citrix Endpoint Management utiliza una cadena de certificados de

confianza pública, por lo que no es necesario insertar una CA raíz en los dispositivos. Como resultado, los usuarios de dispositivos iOS ya no reciben una solicitud para instalar una CA raíz durante la inscripción.

- **Las directivas de red y credenciales ahora son compatibles con Apple TV OS.** Además, ahora puede configurar la directiva de dispositivo de seguridad de AirPlay para controlar qué dispositivos pueden conectarse a los dispositivos Apple TV. Para obtener más información, consulte los artículos sobre las directivas de dispositivo Red, Credenciales y Seguridad de Airplay.
- **Directiva de dispositivo de ubicación ahora disponible para Android Enterprise.** Puede definir la configuración de ubicación para los dispositivos Android Enterprise que se administran o se ejecutan en modo de perfil administrado. Consulte Directiva de dispositivo de ubicación.
- **Compatibilidad mejorada con Alexa for Business.** Citrix Endpoint Management ahora incluye compatibilidad con las conferencias de Alexa for Business, la adición de habilidades de Alexa a sus organizaciones y la edición de grupos de habilidades. Consulte Alexa for Business.
- **Acciones automatizadas para la directiva de agente de Windows.** Con la directiva de agente de Windows, puede automatizar acciones para ejecutarlas en equipos de escritorio y tabletas Windows en función de los valores del registro. Para obtener más información, consulte los artículos Directiva de dispositivo de agente de Windows y Acciones automatizadas.
- **Para Android Enterprise, la opción Sin restricciones para los caracteres obligatorios en un código de acceso ahora está obsoleta.** Los dispositivos Android Enterprise que ejecutan Android 7 o una versión posterior ya no admiten un código de acceso creado sin restricciones de caracteres. Si anteriormente estableció **Caracteres obligatorios** en **Sin restricciones**, esta actualización cambia ese valor a **Solo números**. Este cambio no afecta a la experiencia de inicio de sesión actual del usuario. Para obtener más información, consulte Configuración de Android Enterprise.

Problemas resueltos en Citrix Endpoint Management 19.2.0

Cuando se elimina una aplicación de la biblioteca de Intune y un usuario intenta eliminarla de la biblioteca de Citrix Cloud, no puede eliminarla.

Después de cargar una aplicación de Google Play en la consola de Endpoint Manager sin agregar una imagen de icono de aplicación: si más tarde carga una imagen para la aplicación, la imagen no aparece en la lista de aplicaciones.

Citrix Endpoint Management 19.1.2

- **Directiva de dispositivo de archivos ahora disponible para Android Enterprise.** Puede agregar archivos de script a Citrix Endpoint Management para realizar funciones en dispositivos Android Enterprise. Consulte Directiva de dispositivo de archivos.
- **Configurar la configuración de zona horaria para dispositivos Chrome OS.** Ahora puede seleccionar una zona horaria para el dispositivo Chrome y especificar cómo detectar la zona horaria. Para obtener más información, consulte Directiva de dispositivo de restricciones.
- **Los permisos de grupo de un administrador de RBAC ahora restringen la información de usuario que se muestra en las páginas Usuarios e Invitaciones de inscripción.** Anteriormente, la consola de Citrix Endpoint Management incluía información para todos los usuarios locales y usuarios de dominio en las páginas **Administrar > Usuarios** y **Administrar > Invitaciones de inscripción**.

  Para especificar qué grupos de usuarios tiene permiso un administrador de RBAC para ver y administrar, edite el rol de administrador y especifique los grupos de usuarios. Para obtener más información, consulte Configurar roles con RBAC.
- **Iniciar aplicaciones de terceros desde la aplicación Citrix Workspace.** Para los clientes con Citrix Workspace habilitado: antes de implementar nuevas aplicaciones para los usuarios, puede agregar una lista de URL separadas por comas para iniciar las aplicaciones desde la aplicación Citrix Workspace. Para obtener más información, consulte Agregar aplicaciones.

Problemas solucionados en Citrix Endpoint Management 19.1.2

No se pueden cargar versiones de APK de Google Play Services posteriores a la 11.5.09 en la consola de Citrix Endpoint Management.

Al editar aplicaciones de Windows Desktop y Tablet en **Configurar > Aplicaciones > Tienda de aplicaciones pública**, aparece este mensaje: "Error en la búsqueda de aplicaciones". Al buscar esas aplicaciones, aparece este mensaje: "Error al conectar con la URL de la tienda de aplicaciones de escritorio de Windows: No se pudieron recuperar los detalles de la aplicación pública".

Avisos de terceros

Citrix Endpoint Management podría incluir software de terceros con licencia bajo los términos definidos en el siguiente documento:

Avisos de terceros de Citrix Endpoint Management

Desuso

Los anuncios de este artículo son un aviso anticipado de las funciones de Citrix Endpoint Management que se están eliminando gradualmente, para que pueda tomar decisiones comerciales oportunas. Citrix supervisa el uso y los comentarios de los clientes para determinar cuándo se retirarán. Los anuncios pueden cambiar en versiones posteriores y es posible que no incluyan todas las funciones o características obsoletas. Para obtener detalles sobre el soporte del ciclo de vida del producto, consulte el artículo Política de soporte del ciclo de vida del producto.

Importante:

Gracias por utilizar la herramienta Citrix Endpoint Management Analyzer; lo agradecemos. Debido a nuestra cadencia de lanzamiento frecuente y estable, esta herramienta ya no es necesaria. Citrix ha decidido detener este servicio a partir de March 31, 2023. Le recomendamos que utilice las comprobaciones de conectividad disponibles en la consola de Citrix Endpoint Management o en Citrix NetScaler Gateway. Para obtener más información, consulte Comprobaciones de conectividad.

Elementos obsoletos y eliminaciones

La siguiente lista muestra las funciones de Citrix Endpoint Management que están obsoletas o se han eliminado.

Los elementos *obsoletos* no se eliminan de inmediato. Citrix® sigue dando soporte a un elemento obsoleto hasta que se elimine en una versión futura.

Los elementos *eliminados* se eliminan o ya no se admiten en Citrix Endpoint Management.

Para obtener información sobre las aplicaciones de productividad móvil que llegaron al final de su vida útil, consulte Aplicaciones EOL y obsoletas.

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
Administre las aplicaciones de Microsoft Intune a través de la biblioteca de	Soporte obsoleto para la gestión de aplicaciones de Microsoft Intune a través de la	Marzo de 2025	Abril de 2025	Sin alternativa.

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
Citrix Cloud™ (CC).	biblioteca CC. No se verá afectado si ya tiene aplicaciones de Intune en uso.			
Dos restricciones solo para dispositivos Samsung totalmente administrados para Android Enterprise.	Se han dejado de usar estas configuraciones de la política de restricciones: Habilitar la verificación de arranque de confianza de ODE y Habilitar la comprobación de revocación.	Febrero de 2025	Marzo de 2025	Sin alternativa
Restricciones solo para contenedores Samsung Knox para Android Enterprise.	Se han dejado de usar estas configuraciones de la política de restricciones: Mover aplicaciones al contenedor, Forzar la autenticación multifactor, Forzar la autenticación para el contenedor y Habilitar el teclado seguro.	Febrero de 2025	Objetivo: junio de 2025	Sin alternativa

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
Integración con ShareFile	La integración con ShareFile se dejará de usar si ShareFile (ahora Progress) interrumpe el soporte.	Enero de 2025		Sin alternativa
Pestaña Monitor	Pestaña Monitor obsoleta en Citrix Endpoint Management.	Septiembre de 2024	Octubre de 2024	Sin alternativa
Oferta de Citrix Endpoint Management Government	Soporte obsoleto para la oferta de Citrix Endpoint Management Government.	Enero de 2022	Julio de 2022	Edición Standard de Citrix Endpoint Management
API de atestación SafetyNet	Soporte obsoleto para la atestación SafetyNet de Android según el anuncio de Google aquí.	Julio de 2023	Noviembre de 2023	API de Play Integrity
Chrome OS	Se ha dejado de dar soporte a Chrome OS.	Julio de 2022	Mayo de 2023	Sin alternativa
tvOS	Se ha dejado de dar soporte a tvOS.	Julio de 2022	Mayo de 2023	Sin alternativa

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
Windows Information Protection (WIP)	Se ha dejado de dar soporte a Windows Information Protection según el anuncio de Microsoft aquí.	Agosto de 2022	Octubre de 2022	Sin alternativa
Citrix Endpoint Management Analyzer	Se ha dejado de admitir la herramienta Citrix Endpoint Management Analyzer.	Julio de 2022	Objetivo: March 31, 2023	Sin alternativa
Administración de dispositivos Workspace Hub	Se ha dejado de admitir los dispositivos Citrix Ready® workspace hub.	Enero de 2022	Junio de 2022	Sin alternativa
Microsoft Store para Empresas	Se ha dejado de admitir Microsoft Store para Empresas. Microsoft ya no es compatible con esta plataforma. Para obtener más información, consulte la documentación de Microsoft.	Julio de 2021	Objetivo: Marzo de 2023	Sin alternativa
Samsung SAFE	Compatibilidad con Samsung	Enero de 2022	Junio de 2022	Utilice Android Enterprise.

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
	SAFE en desuso.			
XML personalizado para Zebra	Compatibilidad con XML personalizado en dispositivos Zebra en desuso.	Enero de 2022	Junio de 2022	Utilice la configuración administrada de Android Enterprise.
Identidades PKI: Genérica, Symantec PKI, DigiCert y Entrust	Compatibilidad con entidades PKI de adaptador genéricas, DigiCert Managed y Entrust en desuso.	Junio de 2021	Enero de 2022	Sin alternativa
Android para Workspace	Compatibilidad obsoleta con Android para Workspace	Enero de 2022	Abril de 2022	Sin alternativa
Pasarela SMS del operador	Compatibilidad obsoleta con las notificaciones de la pasarela SMS de Nexmo	Enero de 2022	Abril de 2022	Utilice notificaciones del servidor SMTP
Proveedor de servicios móviles (MSP)	Compatibilidad obsoleta con la interfaz de MSP para consultar dispositivos Blackberry y otros dispositivos Exchange	Enero de 2022	Abril de 2022	Sin alternativa

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
	ActiveSync y emitir operaciones			
MDX Toolkit	Dejar de dar soporte a MDX Toolkit en favor del SDK de Mobile App Management (MAM). Durante el período de transición, puede usar tanto las aplicaciones encapsuladas con MDX como las desarrolladas con el SDK de MAM.	Marzo de 2020	Julio de 2023	Para seguir administrando sus aplicaciones empresariales, utilice el SDK de MAM.
Rol RBAC - Inscriptor de dispositivos compartidos e inscriptor de dispositivos COSU	Dejar de dar soporte a la configuración predefinida de Control de acceso basado en roles tanto para el inscriptor de dispositivos compartidos como para el inscriptor de dispositivos COSU.	Julio de 2021	Diciembre de 2021	Configure los dispositivos iOS a través de (/es-es/citrix-endpoint-management/device-management/apple/shared-ipads.html#prerequisites-for-shared-ipads). Configure los dispositivos Android COSU (dedicados) a través de (/es-

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
				es/citrix-endpoint-management/users/enrollment-profiles.html).
Restricción de permitir la conexión automática a puntos de acceso de Wi-Fi Sense para dispositivos Windows.	Eliminar el soporte para la restricción de permitir la conexión automática a puntos de acceso de Wi-Fi Sense para dispositivos Windows 10. Windows 10 ya no admite esta función. Para obtener más información, consulte la (https://docs.microsoft.com/es-es/windows/configuration/manage-wifi-sense-in-enterprise).	Octubre de 2021	Febrero de 2022	Sin alternativa
MDX: Servidor de puerta de enlace alternativo	Dejar de usar la autenticación por pasos para dispositivos iOS y Android.	Marzo de 2020	Septiembre de 2021	Sin alternativa

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
MDX: Micro VPN (modo de túnel completo)	Se dejó de usar un túnel de red privada virtual (VPN) completo para dispositivos iOS y Android.	Marzo de 2020	Septiembre de 2021	Utilice el modo SSO web del SDK de MAM o cree una directiva VPN por aplicación con el tipo de conexión Citrix SSO.
MDX: Compatibilidad con archivos PAC	Se dejó de admitir un archivo de configuración automática de proxy (PAC) con una implementación de túnel VPN completo para dispositivos iOS y Android.	Marzo de 2020	Septiembre de 2021	Utilice NetScaler Gateway para conectarse a través de un servidor proxy para acceder a redes internas.
Compatibilidad con dispositivos compartidos MDX	Se ha dejado de admitir la compatibilidad con dispositivos compartidos para aplicaciones MDX.	Marzo de 2020	Septiembre de 2021	Para Android Enterprise, utilice dispositivos compartidos inscritos como dispositivos dedicados. Para iOS, utilice Apple School Manager o GroundControl.
Android - Sony	Se ha dejado de admitir la compatibilidad	Enero de 2021	Febrero de 2022	Utilice Android Enterprise

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
	con dispositivos Android Sony y las directivas específicas de Sony.			
Android - HTC	Se ha dejado de admitir la compatibilidad con dispositivos Android HTC y las directivas específicas de HTC.	Enero de 2021	Febrero de 2022	Usar Android Enterprise
Android - Amazon	Se ha dejado de admitir los dispositivos Android Amazon y las directivas específicas de Amazon.	Enero de 2021	Febrero de 2022	Usar Android Enterprise
Inscripción móvil de Knox (DA heredado)	Se ha dejado de admitir la inscripción móvil de Knox (KME) en el modo de administrador de dispositivos heredado en todas las versiones de Android.	May 4, 2021	Septiembre de 2021	Use KME para inscribirse en el modo Android Enterprise. Android 8, 9, 10 y 11 son compatibles con Android Enterprise.
Modo de inscripción de alta seguridad	Se ha dejado de admitir la generación de invitaciones de	Julio de 2021	Febrero de 2022	Consulte Invitaciones de inscripción para ver una lista de

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
	inscripción con el modo de seguridad de inscripción de **alta seguridad**.			los modos de seguridad de inscripción admitidos.
Credenciales derivadas	Se ha dejado de admitir las credenciales derivadas y la aplicación Citrix Derived Credential Manager.	Marzo de 2021	Diciembre de 2021	Consulte iOS para ver una lista de los tipos de autenticación admitidos para iOS.
Puertos salientes de APNs	El soporte de Apple para el protocolo binario heredado de APNs finaliza a partir del March 31, 2021. Apple recomienda que utilice la API de proveedor de APNs basada en HTTP/2 en su lugar. Como parte de este cambio, estamos dejando de admitir los puertos 2195 y 2196, utilizados para enviar notificaciones APNs a	Octubre de 2020	Marzo de 2021	Utilice el puerto 443 en su lugar. Consulte Requisitos de red y firewall.

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
	`*.push.apple.com`.			
Servicio MDX	Se ha dejado de admitir el Servicio MDX en favor del SDK de Mobile App Management (MAM). Durante el período de transición, puede utilizar tanto las aplicaciones encapsuladas con MDX mediante MDX Toolkit como las aplicaciones desarrolladas con el SDK de MAM.	Marzo de 2020	Septiembre de 2021	Para seguir encapsulando sus aplicaciones empresariales, utilice MDX Toolkit.
Configuración de invitaciones de inscripción en el portal de autoayuda	Se ha dejado de admitir que los usuarios generen invitaciones de inscripción desde el portal de autoayuda.	Julio de 2021	Julio de 2021	Póngase en contacto con su administrador para generar invitaciones de inscripción en la consola de Citrix Endpoint Management.
Configuración de invitaciones de inscripción	Se ha dejado de admitir el uso de IMEI, número de serie y UDID de	Abril de 2021	Julio de 2021	Al crear una invitación de inscripción, configure los ajustes

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
	un dispositivo para crear una invitación de inscripción.			disponibles en **Administrar > Invitaciones de inscripción** en la consola de Citrix Endpoint Management.
Algoritmos de firma de autenticación basados en certificados (cifrados no FIPS y débiles)	Se ha dejado de admitir los siguientes algoritmos de firma: SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA, SHA1withDSA, RIPEMD160withRSA, RIPEMD128withRSA, RIPEMD256withRSA.	Mayo de 2020	Junio de 2021	Al crear una CSR para un proveedor de credenciales en la consola de Citrix Endpoint Management (**Parámetros > Proveedores de credenciales > Solicitud de firma de certificado**), elija un cifrado más seguro.
Aplicaciones de movilidad de Citrix y aplicaciones Workspace para Android 7.x e iOS 12.x	Se ha dejado de admitir las versiones de Android 7.x e iOS 12.x de Citrix Secure Hub, Citrix Secure Mail, Citrix Secure Web y la	Abril de 2021	Junio de 2021	Utilice, como mínimo, la versión actual y la anterior de cada plataforma de sistema operativo principal. Los dispositivos antiguos siguen

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
	aplicación Citrix Workspace.			inscritos. Sin embargo, Citrix no prueba ni admite los dispositivos heredados.
Compatibilidad con tokens de software RSA para Android	Se ha dejado de admitir la importación directa de tokens de software RSA en Citrix Secure Hub para Android.	Enero de 2021	Febrero de 2021	Puede importar el token de software RSA dentro de la aplicación RSA Secure ID disponible en Google Play. A continuación, puede usar el token para la autenticación de NetScaler Gateway.
Internet Explorer 11	Se ha dejado de admitir el uso de Internet Explorer con la consola de Citrix Endpoint Management.	Enero de 2021	Enero de 2021	Utilice la versión más reciente de estos navegadores web: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari
Comprobaciones de configuración de Gateway en Citrix Endpoint Management Analyzer	Se ha dejado de admitir la opción de comprobación de la configuración de Gateway.	Noviembre de 2020	Noviembre de 2020	Utilice la comprobación de Citrix Insight Services en Analyzer para comprobar las configuraciones

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
				de Citrix ADC para la preparación de la implementación de Citrix Endpoint Management.
Aplicaciones publicadas para el modo de administrador de dispositivos heredado en dispositivos Android Enterprise	Ya no entregamos aplicaciones publicadas para la plataforma DA heredada a los dispositivos inscritos en Android Enterprise.	Octubre de 2020	Noviembre de 2020	Para los dispositivos Android Enterprise, publique aplicaciones para la plataforma Android Enterprise. Para seguir publicando aplicaciones DA heredadas en dispositivos en modo DA, cree un grupo de entrega independiente para esas aplicaciones.
Modo de administrador de dispositivos heredado para dispositivos Android 10	Google dejó de admitir algunas API de administrador de dispositivos. Citrix no admite dispositivos Android 10 inscritos en el	Febrero de 2020	Noviembre de 2020	Migre los dispositivos Android 10 a Android Enterprise.

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
	modo de administrador de dispositivos a partir de la actualización a Citrix Secure Hub que tiene como objetivo el nivel 29 de la API de Android.			
Android TouchDown	DigiCert dejó de ser compatible con Android TouchDown. Citrix eliminó la página de la plataforma Android TouchDown de la directiva de dispositivos de Exchange.	Julio de 2018	Noviembre de 2020	Recomendación: Use Citrix Secure Mail.
Nuevas inscripciones de Administrador de dispositivos para Android 10	Se dejó de admitir la inscripción o reinscripción en el modo de Administrador de dispositivos heredado en dispositivos Android 10. Los dispositivos ya inscritos siguen funcionando.	Febrero de 2020	Septiembre de 2020	Inscriba nuevos dispositivos Android 10+ en Android Enterprise.

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
Cifrado MDX	Se dejó de admitir el cifrado MDX y la función de cifrado MDX en la consola de Citrix Endpoint Management.	Octubre de 2019	Septiembre de 2020	Habilite el cifrado de plataforma iOS o Android mediante nuestra función de Administración de cifrado con comprobación de cumplimiento adicional. Asegúrese de haber probado y planificado la migración del cifrado MDX antes de julio de 2020.
Windows Mobile/CE	Se ha dejado de dar soporte a los dispositivos Windows Mobile/CE.	Abril de 2018	Septiembre de 2020	Utilice Windows 10 para equipos de escritorio y portátiles.
Contenedor Samsung SEAMS	Se ha dejado de dar soporte al contenedor Samsung SEAMS.	Junio de 2020	Agosto de 2020	Utilice Android Enterprise.
Soporte remoto	Se ha dejado de dar soporte al cliente de Soporte remoto.	Enero de 2019	Agosto de 2020	Sin alternativa

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
Aplicaciones de movilidad de Citrix y aplicaciones Workspace para Android 6.x y iOS 11.x	Se ha dejado de dar soporte a las versiones de Android 6.x y iOS 11.x de Citrix Secure Hub, Citrix Secure Mail, Citrix Secure Web y la aplicación Citrix Workspace.	Abril de 2020	Junio de 2020	Utilice, como mínimo, la versión actual y la anterior de cada plataforma de sistema operativo principal. Los dispositivos antiguos siguen inscritos. Sin embargo, Citrix no prueba ni admite los dispositivos heredados.
Extensiones de red de Citrix Secure Hub para iOS	Se ha dejado de usar el marco de Network Extension que permitía personalizar las funciones de red para dispositivos iOS. Versión 20.3.0 de Citrix Secure Hub.	Octubre de 2018	Marzo de 2020	Sin alternativa
Inicio de sesión de API mediante cuentas locales	Los administradores ya no pueden iniciar sesión en la API de REST con una cuenta local.	Octubre de 2020		Los administradores pueden iniciar sesión con una cuenta de Citrix Cloud. Consulte REST API.

ELEMENTO	DESCRIPCIÓN	DESUSO ANUNCIADO	ELIMINADO	ALTERNATIVA
Certificados SSL (Secure Sockets Layer) autofirmados	Compatibilidad obsoleta con certificados SSL autofirmados para todas las plataformas de dispositivos.	Mayo de 2020		Sustituya su certificado autofirmado existente por un certificado SSL de confianza de una entidad de certificación (CA) conocida.
Túnel VPN completo - Android	Compatibilidad obsoleta con el túnel VPN completo de Android.	Marzo de 2020	Septiembre de 2021	Modo SSO web de MAM SDK.
Permitir el cambio de modo VPN - Android	Compatibilidad obsoleta con el cambio de modo VPN de Android.	Marzo de 2020	Septiembre de 2021	Sin alternativa
Intercambio de documentos entrantes - Android	Compatibilidad obsoleta con el intercambio de documentos entrantes de Android.	Marzo de 2020	Septiembre de 2021	Sin alternativa

Requisitos del sistema

Mientras espera que Citrix aprovisione Citrix Endpoint Management, asegúrese de preparar su implementación de Citrix Endpoint Management instalando Cloud Connector. Aunque Citrix aloja y entrega su solución Citrix Endpoint Management, se requiere cierta comunicación y configuración de puertos. Esa configuración conecta la infraestructura de Citrix Endpoint Management con los servicios corporativos, como Active Directory.

Requisitos de Cloud Connector

Citrix utiliza Cloud Connector para integrar la arquitectura de Citrix Endpoint Management en su infraestructura existente. Cloud Connector integra las siguientes ubicaciones de recursos en Citrix Endpoint Management de forma segura a través del puerto 443: LDAP, servidor PKI, consultas DNS internas y enumeración de Citrix Workspace.

- Al menos dos máquinas dedicadas con Windows Server unidas a su dominio de Active Directory. Las máquinas pueden ser virtuales o físicas. La máquina donde va a instalar el Connector debe estar sincronizada con la hora UTC para una correcta instalación y funcionamiento. Para obtener una lista completa de los requisitos más recientes, consulte los materiales de implementación proporcionados por su equipo de cuentas de Citrix.

  El asistente de incorporación le guiará a través de la instalación de Cloud Connector en esas máquinas.
- Para obtener más requisitos del sistema de la plataforma, consulte Citrix Cloud Connector.

Niveles funcionales de Active Directory compatibles

Para su uso con Citrix Endpoint Management, Citrix Cloud Connector admite los siguientes niveles funcionales de bosque y dominio en Active Directory.

NIVEL FUNCIONAL DEL BOSQUE	NIVEL FUNCIONAL DEL DOMINIO	CONTROLADORES DE DOMINIO COMPATIBLES
Windows Server 2016	Windows Server 2016	Windows Server 2016, Windows Server 2019

NIVEL FUNCIONAL DEL BOSQUE	NIVEL FUNCIONAL DEL DOMINIO	CONTROLADORES DE DOMINIO COMPATIBLES
Windows Server 2016	Windows Server 2019	Windows Server 2019
Windows Server 2019	Windows Server 2019	Windows Server 2019

Nota:

Los servidores Windows 2012 R2, 2012 y 2008 R2 ya no son compatibles, ya que han llegado al final de su ciclo de vida. Para obtener más información, consulte la documentación del ciclo de vida de los productos de Microsoft.

Requisitos de NetScaler Gateway

Citrix Endpoint Management requiere un NetScaler Gateway instalado en su ubicación de recursos para los siguientes escenarios:

- Necesita una micro VPN para acceder a los recursos de red internos para las aplicaciones de línea de negocio. Esas aplicaciones están encapsuladas con la tecnología Citrix MDX. La micro VPN necesita NetScaler Gateway para conectarse a las infraestructuras de back-end internas.
- Tiene previsto utilizar aplicaciones de productividad móvil de Citrix, como Citrix Secure Mail.
- Tiene previsto integrar Citrix Endpoint Management con Microsoft Endpoint Manager.

Los requisitos:

- Autenticación de dominio (LDAP)
- NetScaler Gateway 12.1 o superior, con una licencia de Plataforma/Universal

Para obtener más información, consulte Licencias.

- Certificado SSL público.

Para obtener más información, consulte Crear y usar certificados SSL en un dispositivo Citrix ADC.

- Dirección IP pública sin usar para el servidor virtual de NetScaler Gateway
- Nombre de dominio completo (FQDN) de resolución pública para el servidor virtual de NetScaler Gateway

- Certificados intermedios y raíz de Citrix Endpoint Management alojados en la nube (proporcionados en el paquete de scripts)
- Dirección IP privada interna sin usar para la IP del equilibrador de carga del proxy
- Para conocer los requisitos de puertos, consulte Requisitos de puertos de NetScaler Gateway más adelante en este artículo.
- Integración de Citrix Endpoint Management con Microsoft Endpoint Manager
- Implementar una instancia de Citrix ADC VPX en Microsoft Azure

Para obtener información sobre los requisitos de NetScaler Gateway, consulte los materiales de implementación proporcionados por su equipo de cuentas de Citrix.

Para obtener información sobre los requisitos de Android Enterprise, consulte la sección Android Enterprise.

Requisitos de Citrix Files

Los servicios de sincronización y uso compartido de archivos de Citrix Files están disponibles en la oferta de servicio Premium de Citrix Endpoint Management. El controlador de zonas de almacenamiento amplía el almacenamiento en la nube de software como servicio (SaaS) de Citrix Files al proporcionar almacenamiento de datos privados a su cuenta de Citrix Files.

Requisitos del controlador de zonas de almacenamiento:

- Una máquina física o virtual dedicada
- Windows Server 2012 R2 (Datacenter, Standard o Essentials), Windows Server 2016, Windows Server 2019 o Windows Server 2022
- 2 vCPU
- 4 GB de RAM
- 50 GB de espacio en disco duro
- Roles de servidor para Servidor web (IIS):
    - Desarrollo de aplicaciones: ASP. NET 4.5.2
    - Seguridad: Autenticación básica
    - Seguridad: Autenticación de Windows

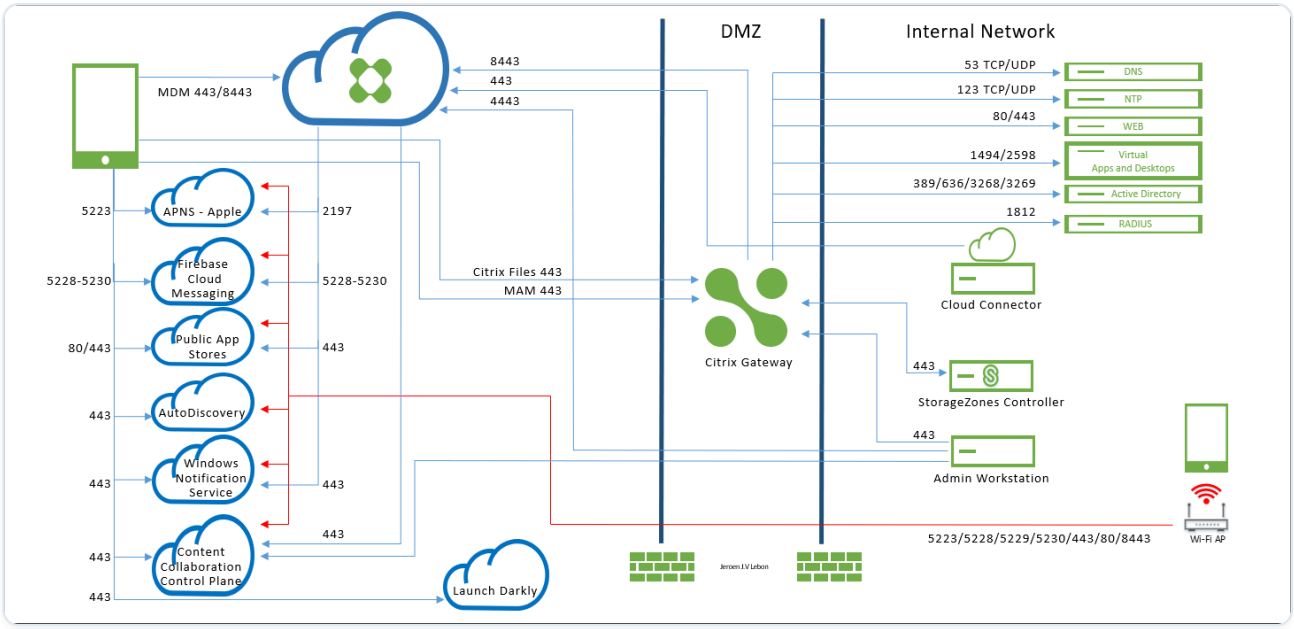
Requisitos de la plataforma Citrix Files:

- El instalador de Citrix Files requiere privilegios administrativos en el servidor Windows

- Nombre de usuario de administrador de Citrix Files

Requisitos de puertos

Para permitir que los dispositivos y las aplicaciones se comuniquen con Citrix Endpoint Management, debe abrir puertos específicos en sus firewalls. El siguiente diagrama muestra el flujo de tráfico para Citrix Endpoint Management.



Las siguientes secciones enumeran los puertos que debe abrir. Para obtener información sobre las URL que utilizan las aplicaciones de productividad móvil, consulte Administración de indicadores de funciones.

Requisitos de puertos de NetScaler Gateway

Abra los puertos para permitir las conexiones de usuario desde Citrix Secure Hub y Citrix Workspace a través de NetScaler Gateway a:

- Citrix Endpoint Management
- StoreFront
- Otros recursos de red internos, como sitios web de intranet

Para obtener más información sobre NetScaler Gateway, consulte Configuración de los ajustes de su entorno de Citrix Endpoint Management en la documentación de NetScaler Gateway. Para obtener información sobre las direcciones IP, consulte Cómo utiliza NetScaler Gateway las direcciones IP en la documentación de NetScaler Gateway.

PUERTO TCP	DESCRIPCIÓN	ORIGEN	DESTINO
53 (TCP y UDP)	Se utiliza para conexiones DNS.	SNIP de NetScaler Gateway	Servidor DNS
80/443	NetScaler Gateway pasa la conexión micro VPN al recurso de red interno a través del segundo firewall.	SNIP de NetScaler Gateway	Sitios web de intranet
123 (TCP y UDP)	Se utiliza para los servicios del Protocolo de tiempo de red (NTP).	SNIP de NetScaler Gateway	Servidor NTP
389	Se utiliza para conexiones LDAP no seguras.	NSIP de NetScaler Gateway (o, si se utiliza un equilibrador de carga, SNIP)	Servidor de autenticación LDAP o Microsoft Active Directory
443	Se utiliza para las conexiones a StoreFront desde Citrix Workspace a Citrix Virtual Apps and Desktops.	Internet	NetScaler Gateway
443	Se utiliza para las conexiones a Citrix Endpoint Management para la entrega de aplicaciones web, móviles y SaaS.	Internet	NetScaler Gateway
443	Se utiliza para la comunicación del Cloud Connector: LDAP, DNS, PKI y enumeración de Citrix Workspace.	Servidores Cloud Connector	`https://*.citrixworkspaceapi.net`, `https://*.cloud.com` (commercial),

PUERTO TCP	DESCRIPCIÓN	ORIGEN	DESTINO
			`https://*.blob.core.windows.net/`, `https://*.servicebus.windows.net`
443	Se utiliza para acceder al portal de autoayuda de Citrix Endpoint Management, si está habilitado, a través del navegador.	Punto de acceso (navegador)	Citrix Endpoint Management (`https://<sitename>/zdm/shp`)
636	Se utiliza para conexiones LDAP seguras.	NSIP de NetScaler Gateway (o, si se utiliza un equilibrador de carga, SNIP)	Servidor de autenticación LDAP o Active Directory
1494	Se utiliza para conexiones ICA a aplicaciones basadas en Windows en la red interna. Citrix recomienda mantener este puerto abierto.	SNIP de NetScaler Gateway	Aplicaciones y Escritorios Virtuales de Citrix
1812	Se utiliza para conexiones RADIUS.	NSIP de NetScaler Gateway	Servidor de autenticación RADIUS
2598	Se utiliza para conexiones a aplicaciones basadas en Windows en la red interna mediante la fiabilidad de la sesión. Citrix	SNIP de NetScaler Gateway	Aplicaciones y Escritorios Virtuales de Citrix

PUERTO TCP	DESCRIPCIÓN	ORIGEN	DESTINO
	recomienda mantener este puerto abierto.		
3269	Se utiliza para conexiones LDAP seguras de Catálogo global de Microsoft.	NSIP de NetScaler Gateway (o, si se utiliza un equilibrador de carga, SNIP)	Servidor de autenticación LDAP o Active Directory
4443	Se utiliza para que un administrador acceda a la consola de Citrix Endpoint Management a través del explorador.	Punto de acceso (explorador)	Citrix Endpoint Management
8443	Se utiliza para la inscripción, la tienda de aplicaciones y la administración de aplicaciones móviles (MAM).	SNIP de NetScaler Gateway	Citrix Endpoint Management
8443	Puerto de Secure Ticket Authority (STA) utilizado para el token de autenticación de Citrix Secure Mail	SNIP de NetScaler Gateway	Citrix Endpoint Management

Requisitos de red y firewall

Para permitir que los dispositivos y las aplicaciones se comuniquen con Citrix Endpoint Management, debe abrir puertos específicos en sus firewalls. Las siguientes tablas enumeran esos puertos.

Abrir puertos desde la red interna a Citrix Cloud:

PUERTO TCP	IP DE ORIGEN	DESCRIPCIÓN	DESTINO	IP DE DESTINO	
443		Cloud Connector	`https://*.citrixworkspacesapi.net`, `https://*.cloud.com` (commercial), `https://*.sharefile.com`, `https://cwsproduction.blob.core.windows.net/downloads`, `https://*.servicebus.windows.net`		
443		Administrative Console	`https://*.citrixworkspacesapi.net`, `https://*.cloud.com` (commercial), `https://*.citrix.com`, `https://cwsproduction.blob.core.window`		

PUERTO TCP	IP DE ORIGEN	DESCRIPCIÓN	DESTINO	IP DE DESTINO	
			`s.net/downloads`		
443		Acceso al portal de autoayuda de Citrix Endpoint Management a través de un navegador (si el portal está habilitado)	Citrix Endpoint Management		
4443		Acceso a la consola de Citrix Endpoint Management a través de un navegador	Citrix Endpoint Management		

Abrir puertos desde Internet a la DMZ:

PUERTO TCP	DESCRIPCIÓN	IP DE ORIGEN	DESTINO	IP DE DESTINO
443	Dispositivo cliente de Citrix Endpoint Management		IP de NetScaler Gateway	
443	Dispositivo cliente de Citrix Endpoint Management		VIP de NetScaler Gateway	

PUERTO TCP	DESCRIPCIÓN	IP DE ORIGEN	DESTINO	IP DE DESTINO
443	IP pública de Citrix Files	CTX208318	VIP de NetScaler Gateway	

Abrir puertos de la DMZ a la red interna:

PUERTO TCP	DESCRIPCIÓN	IP DE ORIGEN	DESTINO	IP DE DESTINO
389 o 636	NSIP de NetScaler Gateway		IP de Active Directory	
53 (UDP)	NSIP de NetScaler Gateway		IP del servidor DNS	
443	SNIP de NetScaler Gateway		IP del servidor Exchange (EAS)	
443	SNIP de NetScaler Gateway		Aplicaciones/ servicios web internos	
443	SNIP de NetScaler Gateway		IP del controlador de zonas de almacenamiento	

Abrir puertos de la red interna a la DMZ:

PUERTO TCP	DESCRIPCIÓN	IP DE ORIGEN	DESTINO	IP DE DESTINO
443	Cliente de administración		NSIP de NetScaler Gateway	

Puertos abiertos de la red interna a Internet:

CITRIX ENDPOINT MANAGEMENT™

PUERTO TCP	DESCRIPCIÓN	IP DE ORIGEN	DESTINO	IP DE DESTINO
443	IP del servidor de Exchange (EAS)		Oyentes de notificaciones push de Citrix Endpoint Management (1)	
443	IP del controlador de Storage zones		Plano de control de Citrix Files	CTX208318

`(1) us-east-1.mailboxlistener.xm.citrix.com, eu-west-1.mailboxlistener.xm.citrix.com, ap-southeast-1.mailboxlistener.xm.citrix.com`

Abrir puertos desde la red Wi-Fi corporativa a Internet:

PUERTO TCP	DESCRIPCIÓN	IP DE ORIGEN	DESTINO	IP DE DESTINO
8443 / 443	Dispositivo cliente de Citrix Endpoint Management		Citrix Endpoint Management	
5223	Dispositivo cliente de Citrix Endpoint Management		Servidores APNS de Apple	`17.0.0.0/8`
5228	Dispositivo cliente de Citrix Endpoint Management		Firebase Cloud Messaging	`android.apis.google.com, fcm.googleapis.com`
5229	Dispositivo cliente de Citrix Endpoint Management		Firebase Cloud Messaging	`android.apis.google.com, fcm.googleapis.com`

PUERTO TCP	DESCRIPCIÓN	IP DE ORIGEN	DESTINO	IP DE DESTINO
5230	Dispositivo cliente de Citrix Endpoint Management		Firebase Cloud Messaging	`android.apis.google.com`, `fcm.googleapis.com`
443	Dispositivo cliente de Citrix Endpoint Management		Firebase Cloud Messaging	`fcm.googleapis.com`
443	Dispositivo cliente de Citrix Endpoint Management		Windows Push Notification Service	`*.notify.windows.com`
443 / 80	Dispositivo cliente de Citrix Endpoint Management		Apple iTunes App Store	`ax.apps.apple.com`, `*.mzstatic.com`, `vpp.itunes.apple.com`
443 / 80	Dispositivo cliente de Citrix Endpoint Management		Google Play	`play.google.com`, `android.clients.google.com`, `android.l.google.com`, `android.com`, `google-analytics.com`
443 / 80	Dispositivo cliente de Citrix Endpoint Management		Microsoft App Store	`login.live.com`, `*.notify.windows.com`
443	Dispositivo cliente de Citrix		Servicio de detección automática de	`discovery.cem.cloud.us`

PUERTO TCP	DESCRIPCIÓN	IP DE ORIGEN	DESTINO	IP DE DESTINO
	Endpoint Management		Citrix Endpoint Management para iOS y Android	
443	Dispositivo cliente de Citrix Endpoint Management		Servicio de detección automática de Citrix Endpoint Management para Windows	`enterpriseenrollment.mycompany.com`, `discovery.cem.cloud.us`
443	IP del controlador de zonas de almacenamiento		Plano de control de Citrix Files	CTX208318
443	Dispositivo cliente de Citrix Endpoint Management		Google Mobile Management, Google APIs, Google Play Store APIs	`*.googleapis.com`
443	Dispositivo cliente de Citrix Endpoint Management		Comprobaciones de conectividad para versiones de CloudDPC anteriores a la v470. Las comprobaciones de conectividad de Android a partir de N MR1 requieren que `https://www.google.com/generate_204`	`connectivitycheck.android.com`, `www.google.com`

PUERTO TCP	DESCRIPCIÓN	IP DE ORIGEN	DESTINO	IP DE DESTINO
			sea accesible, o que la red Wi-Fi dada apunte a un archivo PAC accesible)	

Requisito de puerto para la conectividad del servicio AutoDiscovery

Esta configuración de puerto garantiza que los dispositivos Android que se conectan desde Citrix Secure Hub para Android puedan acceder al servicio AutoDiscovery (ADS) de Citrix Endpoint Management desde la red interna. La capacidad de acceder al ADS es importante al descargar cualquier actualización de seguridad disponible a través del ADS.

> **Nota:**
>
> Es posible que las conexiones ADS no sean compatibles con su servidor proxy. En este caso, permita que la conexión ADS omita el servidor proxy.

> Si desea habilitar el anclaje de certificados, complete los siguientes requisitos previos:

- **Recopile los certificados del servidor de Citrix Endpoint Management y de NetScaler Gateway:** Los certificados deben estar en formato PEM y deben ser un certificado público, no la clave privada.
- **Póngase en contacto con el soporte de Citrix y solicite la habilitación del anclaje de certificados:** Durante este proceso, se le pedirán sus certificados.

El anclaje de certificados requiere que los dispositivos se conecten a ADS antes de que el dispositivo se inscriba. Este requisito garantiza que la información de seguridad más reciente esté disponible para Citrix Secure Hub. Para que Citrix Secure Hub inscriba un dispositivo, este debe poder acceder a ADS. Por lo tanto, abrir el acceso a ADS dentro de la red interna es fundamental para permitir que los dispositivos se inscriban.

Para permitir el acceso a ADS para Citrix Secure Hub para Android/iOS, abra el puerto 443 para el siguiente FQDN:

FQDN	PUERTO	USO DE IP Y PUERTO
`discovery.cem.cloud.us`	443	Citrix Secure Hub - Comunicación ADS a través de CloudFront

Para obtener información sobre las direcciones IP admitidas, consulte Centros de almacenamiento basados en la nube de AWS.

Requisitos de red de Android Enterprise

Para obtener información sobre las conexiones salientes que debe tener en cuenta al configurar entornos de red para Android Enterprise, consulte el artículo de soporte de Google, Requisitos de red de Android Enterprise.

Requisitos de la aplicación

Citrix Endpoint Management admite añadir y mantener hasta 300 aplicaciones. Superar este límite hace que su sistema se vuelva inestable.

Compatibilidad de Citrix Endpoint Management

Para usar las nuevas funciones, correcciones y actualizaciones de directivas, Citrix® recomienda instalar la versión más reciente de lo siguiente:

- Citrix recomienda integrar el SDK de Mobile Application Management (MAM) con las aplicaciones empresariales de iOS y Android para aplicar las capacidades MDX a las aplicaciones.

  El MDX Toolkit tiene programado alcanzar el fin de vida útil (EOL) en julio de 2023. Para seguir administrando sus aplicaciones empresariales, debe incorporar el MAM SDK.
- Aplicaciones de productividad móvil

Este artículo resume las versiones de los componentes de Citrix Endpoint Management compatibles que puede integrar.

Las últimas versiones de Citrix Secure Hub, MDX Toolkit y las aplicaciones de productividad móvil son compatibles con la última versión y las dos versiones anteriores de Citrix Endpoint Management.

Aplicaciones de productividad móvil

Los usuarios acceden a las aplicaciones de productividad móvil desde las tiendas de aplicaciones públicas. La última versión de las aplicaciones de productividad móvil requiere la última versión de Citrix Secure Hub. Las dos versiones anteriores de las aplicaciones son compatibles con la última versión de Citrix Secure Hub.

Para obtener más información sobre la cadencia de lanzamiento por fases de dos semanas de las aplicaciones de productividad móvil, consulte Cronología de lanzamiento. Para obtener detalles de soporte, consulte Soporte para aplicaciones de productividad móvil.

MAM SDK

El MAM SDK proporciona funcionalidad MDX que no está cubierta por las plataformas iOS y Android. Puede hacer que esas aplicaciones estén disponibles en una tienda interna o en tiendas de aplicaciones públicas. Consulte SDK de aplicaciones MDX.

MDX Toolkit

El MDX Toolkit tiene programado alcanzar el fin de vida útil (EOL) en julio de 2023. Para seguir administrando sus aplicaciones empresariales, debe incorporar el MAM SDK.

Citrix admite las tres últimas versiones (n.n.n) del MDX Toolkit. Consulte Novedades del MDX Toolkit.

Compatibilidad con navegadores

La consola de Citrix Endpoint Management requiere uno de los siguientes navegadores web compatibles:

- Última versión de Google Chrome
- Última versión de Mozilla Firefox
- Última versión de Microsoft Edge
- Última versión de Apple Safari

Sistemas operativos de dispositivos compatibles

Este artículo trata sobre los dispositivos compatibles para la administración de la movilidad empresarial con Citrix Endpoint Management. Debido a las restricciones de la plataforma y las

funciones de seguridad, Citrix Endpoint Management no es compatible con todas las funciones en todas las plataformas.

Para conocer las últimas versiones de las aplicaciones de productividad móvil, consulte Compatibilidad con aplicaciones de productividad móvil.

Nota:

- Citrix admite las versiones actuales y anteriores de cada plataforma de sistema operativo principal. Algunas funciones de Citrix Endpoint Management no funcionan en versiones de plataforma anteriores. Para anuncios de desuso, consulte Desuso.
- Citrix Endpoint Management™ admite la administración de dispositivos para dispositivos Windows x86 y ARM.

Lista de compatibilidad con sistemas operativos

Citrix Endpoint Management admite los siguientes sistemas operativos:

- **Android:** 10.x, 11.x, 12.x, 13.x, 14.x, 15.x, 16.x, 17.x

  Citrix® recomienda actualizar a Android 10+ antes de usar Android Enterprise. Para obtener más información, consulte Consideraciones de Android.

- **iOS:** 13.x, 14.x, 15.x, 16.x, 17.x, 18.x, 26.x, 27.x

  Citrix Endpoint Management y las aplicaciones móviles de Citrix no son compatibles actualmente con todas las nuevas funciones disponibles para iOS 14.x, iOS 15.x, iOS 16.x, iOS 17.x, iOS 18.x, iOS 26.x e iOS 27.x.

- **iPadOS:** 13.x, 14.x, 15.x, 16.x, 17.x, 18.x, 26.x, 27.x

  Citrix Endpoint Management y las aplicaciones móviles de Citrix no son compatibles actualmente con todas las nuevas funciones de iPadOS 14.x, iPadOS 15.x, iPadOS 16.x, iPadOS 17.x, iPadOS 18.x, iPadOS 26.x y iPadOS 27.x.

- **macOS:** 11.x, 12.x, 13.x, 14.x, 15x

  Citrix Endpoint Management y las aplicaciones de productividad móvil de Citrix no son compatibles actualmente con todas las nuevas funciones disponibles para macOS 11, macOS 12, macOS 13, macOS 14 y macOS 15.

- **Equipos de escritorio y tabletas con Windows 10 y Windows 11:** (solo MDM)

- Windows 10 Professional y Windows 11 Professional
- Windows 10 Enterprise y Windows 11 Enterprise
- Windows 10 Education y Windows 11 Education
- Windows IoT Enterprise

Consulte la documentación de Microsoft para conocer el nivel de compatibilidad de un sistema operativo específico.

Consideraciones sobre Android

Antes de actualizar a Android 10 o posterior: Para obtener información sobre cómo la desaprobación de las API de administración de dispositivos de Google afecta a los dispositivos que ejecutan Android 10 o posterior, consulte Migrar de la administración de dispositivos a Android Enterprise. Consulte también este blog de Citrix.

- Google ha dejado de usar las API de administración de dispositivos, lo que afecta a los dispositivos que ejecutan Android 10 o posterior. La inscripción de dispositivos Android 10 o posterior en el modo de administración de dispositivos heredado falla. Citrix no admite la inscripción de dispositivos Android en el modo de administración de dispositivos.
- Citrix recomienda usar Android Enterprise para dispositivos Android. Para obtener más información, consulte Migrar de la administración de dispositivos a Android Enterprise.
- El cambio de la API de Google no afecta a los dispositivos inscritos en el modo solo MAM.
- Consulte también este blog de Citrix.

Antes de actualizar:

- Asegúrese de que la infraestructura de su servidor cumpla con los certificados de seguridad que tienen un nombre de host coincidente en la extensión subjectAltName (SAN).
- Para verificar un nombre de host, el servidor debe presentar un certificado con un SAN coincidente. Citrix solo confía en los certificados que tienen un SAN que coincide con el nombre de host.

Compatibilidad con idiomas

Las aplicaciones de productividad móvil de Citrix y la consola de Citrix Endpoint Management están adaptadas para su uso en idiomas distintos del inglés. La compatibilidad incluye caracteres y entrada de teclado que no son en inglés, incluso cuando la aplicación no está localizada en el idioma preferido del usuario. Para obtener más información sobre la compatibilidad con la

globalización para todos los productos de Citrix, consulte `<https://support.citrix.com/article/CTX119253>`.

En este artículo se enumeran los idiomas admitidos en la versión más reciente de Citrix Endpoint Management.

Consola de Citrix Endpoint Management y el portal de autoayuda

- Francés
- Alemán
- Español
- Japonés
- Coreano
- Portugués
- Chino simplificado

Aplicaciones de productividad móvil de Citrix

Una X indica que la aplicación está disponible en ese idioma en particular.

iOS y Android

IDIOMA	SECURE HUB	SECURE MAIL	SECURE WEB	SECURE NOTES	SECURE TASKS	QUICKED IT
Japonés	X	X	X	X	X	X
Chino simplificado	X	X	X	X	X	X
Chino tradicional	X	X	X	X	X	X
Francés	X	X	X	X	X	X
Alemán	X	X	X	X	X	X
Español	X	X	X	X	X	X

IDIOMA	SECURE HUB	SECURE MAIL	SECURE WEB	SECURE NOTES	SECURE TASKS	QUICKED IT
Coreano	X	X	X	X	X	X
Portugués	X	X	X	X	X	X
Neerlandés	X	X	X	X	X	X
Italiano	X	X	X	X	X	X
Danés	X	X	X	X	X	X
Sueco	X	X	X	X	X	X
Hebreo	X	X	X	X	X	Solo iOS
Árabe	X	X	X	X	X	X
Ruso	X	X	X	X	X	X
Turco	X	X	Solo Android	-	-	-
Polaco	X	X	X	-	-	-

Compatibilidad con idiomas de derecha a izquierda

La siguiente tabla resume la compatibilidad con texto en idiomas de Oriente Medio para cada aplicación. Una X indica que la función está disponible para esa plataforma. La compatibilidad con idiomas de derecha a izquierda no está disponible para dispositivos Windows.

APLICACIÓN	IOS	ANDROID
Citrix Secure Hub	X	X
Citrix Secure Mail	X	X
Citrix Secure Web	X	X
QuickEdit	X	X

Cumplimiento de FIPS 140-2

El Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) emite el Estándar Federal de Procesamiento de Información (FIPS). FIPS especifica los requisitos de seguridad para los módulos criptográficos utilizados en los sistemas de seguridad. FIPS 140-2 es la segunda versión de este estándar. Para obtener más información sobre los módulos FIPS 140 validados por NIST, consulte el Centro de Recursos de Seguridad Informática de NIST.

Todas las operaciones criptográficas de datos en reposo y datos en tránsito en iOS utilizan módulos criptográficos validados por FIPS. En Android, todas las operaciones criptográficas de datos en reposo utilizan módulos criptográficos validados por FIPS proporcionados por Citrix® o los módulos criptográficos de la plataforma proporcionados por el fabricante del dispositivo. Póngase en contacto con su representante de Citrix para obtener más información sobre los módulos del fabricante del dispositivo.

Todas las operaciones criptográficas de datos en reposo y datos en tránsito para la administración de dispositivos móviles (MDM) en dispositivos Windows compatibles utilizan módulos criptográficos validados por FIPS.

Todas las operaciones criptográficas de datos en reposo y datos en tránsito para Citrix Endpoint Management MDM utilizan módulos criptográficos validados por FIPS. Todos los datos en reposo y en tránsito para los flujos de MDM utilizan módulos criptográficos compatibles con FIPS de extremo a extremo. Esa seguridad incluye las operaciones criptográficas descritas anteriormente para dispositivos móviles, además de las operaciones criptográficas entre dispositivos móviles y NetScaler Gateway.

MDX Vault cifra las aplicaciones encapsuladas en MDX y los datos en reposo asociados tanto en dispositivos iOS como Android utilizando módulos criptográficos validados por FIPS.

Acerca de Citrix Endpoint Management

Citrix Endpoint Management es una solución de Unified Endpoint Management (UEM) que unifica todas las aplicaciones y puntos finales en una sola vista para aumentar la seguridad y mejorar la productividad. Para obtener una descripción general de UEM, consulte el informe técnico de Citrix Tech Zone, Citrix Endpoint Management.

Citrix Endpoint Management proporciona Mobile Device Management (MDM) y Mobile App Management (MAM).

Las funciones de MDM de Citrix Endpoint Management le permiten:

- Implementar directivas y aplicaciones en dispositivos.
- Recuperar inventarios de recursos.
- Realizar acciones en los dispositivos, como un borrado de dispositivo.

Las funciones de MAM de Citrix Endpoint Management le permiten:

- Proteger aplicaciones y datos en dispositivos móviles BYO.
- Distribuir aplicaciones móviles empresariales.
- Bloquear las aplicaciones y borrar sus datos.

Con una combinación de funciones de MDM y MAM, puede:

- Administrar un dispositivo corporativo mediante MDM
- Implementar directivas y aplicaciones en dispositivos
- Recuperar un inventario de recursos
- Borrar dispositivos
- Distribuir aplicaciones móviles empresariales
- Bloquear aplicaciones y borrar los datos de los dispositivos

La siguiente tabla resume las funciones de Citrix Endpoint Management compatibles con MDM, MAM o MDM+MAM.

FUNCIÓN (POR PLATAFORMA)	MDM (1)	MAM (2)	MDM+MAM
Android Enterprise:			
Compatibilidad con la inscripción de dispositivos	Sí	Sí	Sí
Compatibilidad con la autenticación de dominio	Sí	No	Sí
Compatibilidad con la autenticación de dominio más token de seguridad	No	No	Sí
Compatibilidad con la autenticación de certificado de cliente	No	Sí	Sí
Compatibilidad con la autenticación de certificado de cliente más dominio	No	No	Sí
Compatibilidad con certificado de cliente más token de seguridad	No	No	Sí
Compatibilidad con el proveedor de identidades de Azure AD	Sí	No	Sí
Compatibilidad con el proveedor de identidades de Okta	Sí	No	Sí
Inicio de sesión único en	Sí	No	Sí

FUNCIÓN (POR PLATAFORMA)	MDM (1)	MAM (2)	MDM+MAM
aplicaciones SaaS nativas			
Soporte de Citrix Content Delivery Network para aplicaciones empresariales	Sí	Sí	Sí
Soporte de Citrix Content Delivery Network para aplicaciones MDX	Sí	Sí	Sí
Soporte para dispositivos compartidos mediante el aprovisionamiento de dispositivos Android Enterprise (COSU) dedicados	Sí	No	Sí
Android (heredado):			
Soporte para la inscripción de dispositivos	Sí	Sí	Sí
Compatibilidad con autenticación de dominio o de dominio más token de seguridad	No	No	Sí
Compatibilidad con autenticación de certificado de cliente	No	Sí	Sí

FUNCIÓN (POR PLATAFORMA)	MDM (1)	MAM (2)	MDM+MAM
Compatibilidad con autenticación de certificado de cliente más dominio	No	No	Sí
Compatibilidad con certificado de cliente más token de seguridad	No	No	Sí
Compatibilidad con Azure AD y el proveedor de identidades de Citrix	Sí	No	Sí
Compatibilidad con el proveedor de identidades de Okta	Sí	No	Sí
Inicio de sesión único en aplicaciones SaaS nativas	Sí	No	Sí
Soporte de Citrix Content Delivery Network para aplicaciones empresariales	Sí	Sí	Sí
Soporte de Citrix Content Delivery Network para aplicaciones MDX	Sí	Sí	Sí
Chrome:			
Soporte para la inscripción de dispositivos	Sí	No	Sí

FUNCIÓN (POR PLATAFORMA)	MDM (1)	MAM (2)	MDM+MAM
Soporte para la autenticación con nombre de usuario y contraseña	Sí	No	Sí
iOS:			
Compatibilidad con la inscripción de dispositivos	Sí	Sí	Sí
Compatibilidad con la autenticación de dominio o de dominio más token de seguridad	No	No	Sí
Compatibilidad con la autenticación de certificados de cliente	No	Sí	Sí
Soporte para certificado de cliente más autenticación de dominio	No	No	Sí
Soporte para proveedor de identidades de Azure AD y Citrix	Sí	No	Sí
Soporte para proveedor de identidades de Okta	Sí	No	Sí
Inicio de sesión único en aplicaciones SaaS nativas	Sí	No	Sí

FUNCIÓN (POR PLATAFORMA)	MDM (1)	MAM (2)	MDM+MAM
Compatibilidad con Citrix Content Delivery Network para aplicaciones empresariales	Sí	Sí	Sí
Compatibilidad con Citrix Content Delivery Network para aplicaciones MDX	Sí	Sí	Sí
Integración con Apple Education	Sí	No	Sí
macOS:			
Compatibilidad con la inscripción de dispositivos	Sí	No	No
Compatibilidad con dominio o dominio más contraseña de un solo uso	Sí	No	No
Compatibilidad con URL de invitación más contraseña de un solo uso	Sí	No	No
Windows:			
Compatibilidad con la inscripción de dispositivos	Sí	No	No
Inscripción automática de dispositivos Windows 10 y	Sí	No	No

FUNCIÓN (POR PLATAFORMA)	MDM (1)	MAM (2)	MDM+MAM
Windows 11 a través de la aplicación Citrix Workspace			
Compatibilidad con la autenticación de dominio o de dominio más token de seguridad	Sí	No	No
Compatibilidad con la autenticación de certificado de cliente	Sí	No	No
Compatibilidad con la autenticación de certificado de cliente más dominio	Sí	No	No
Autenticación federada a través de Azure AD o proveedor de identidades de Citrix	Sí	No	No
Soporte de Citrix Content Delivery Network para aplicaciones empresariales	Sí	No	No
Integración de Workspace Environment Management™ (3)	Sí	No	No

Notas:

> (1) El orden de implementación se aplica solo a los dispositivos de un grupo de entrega que tiene un perfil de inscripción configurado para MDM.

> (2) La inscripción de MAM requiere NetScaler Gateway.

> (3) La integración de Workspace Environment Management (WEM) proporciona acceso a las funciones de MDM en una amplia gama de sistemas operativos Windows.

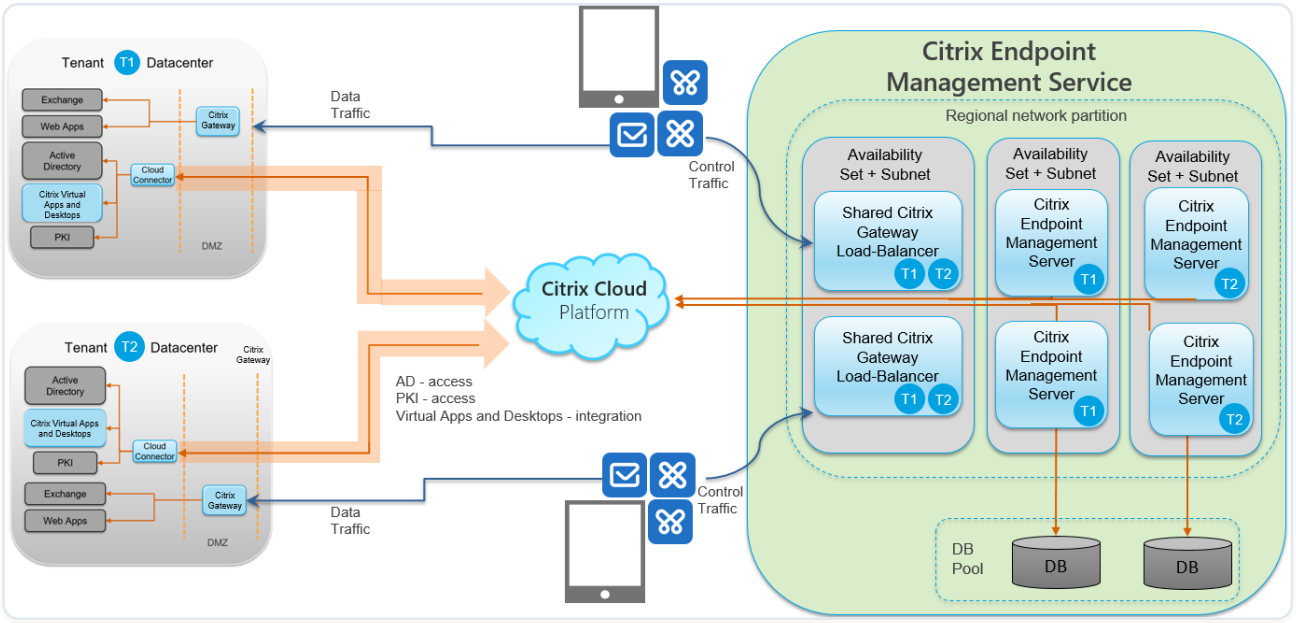
> Para obtener más información, consulte Modos de administración.

Arquitectura

Los requisitos de administración de dispositivos y aplicaciones de su organización determinan los componentes de Citrix Endpoint Management en su arquitectura de Citrix Endpoint Management. Los componentes de Citrix Endpoint Management son modulares y se complementan entre sí. Por ejemplo, su implementación incluye NetScaler Gateway:

- NetScaler Gateway proporciona a los usuarios acceso remoto a las aplicaciones móviles y rastrea los tipos de dispositivos de los usuarios.
- Citrix Endpoint Management es donde se administran esas aplicaciones y dispositivos.

El siguiente diagrama muestra una descripción general de la arquitectura de una implementación en la nube de Citrix Endpoint Management y su integración con su centro de datos.



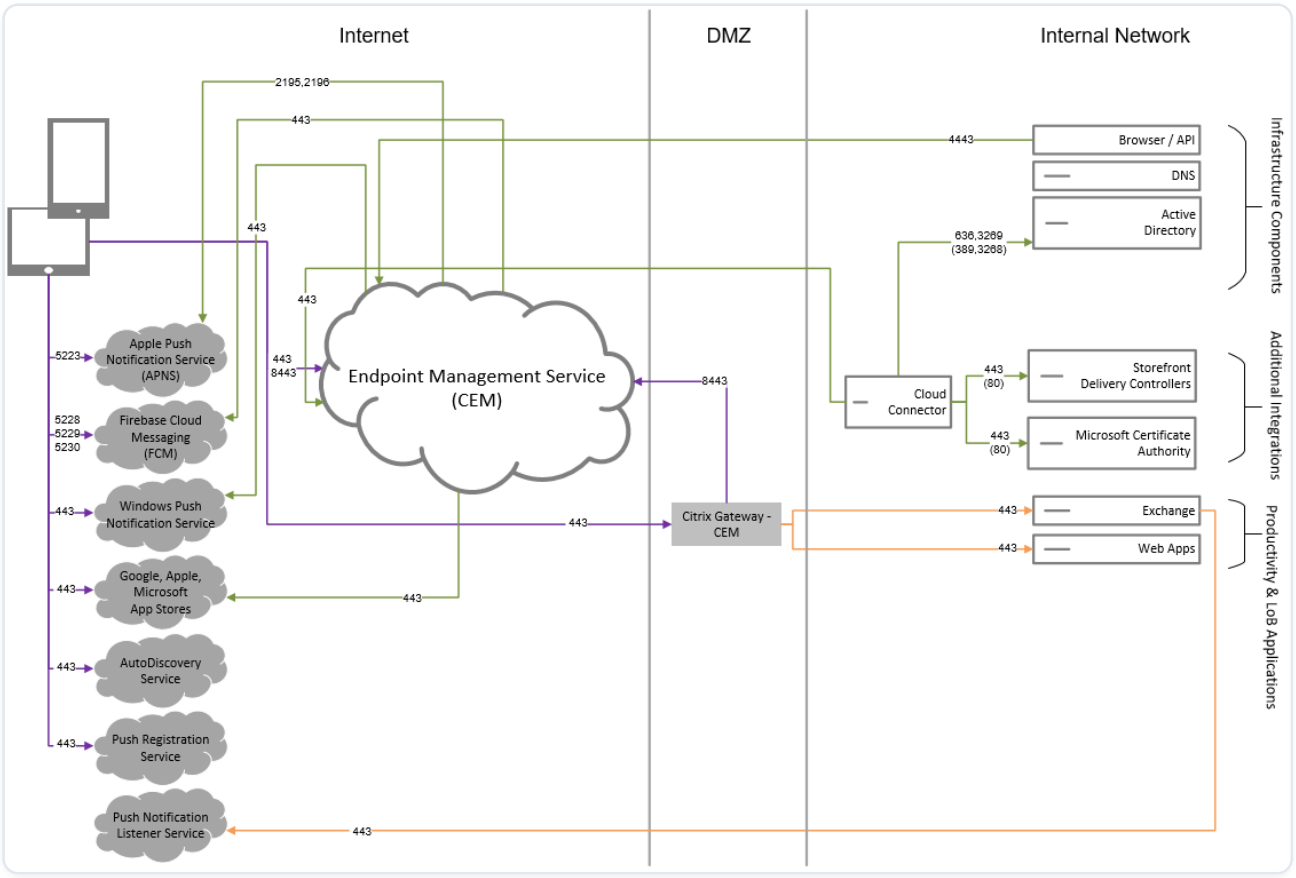
Las siguientes subsecciones tienen diagramas de arquitectura de referencia para:

- Citrix Endpoint Management
- Componentes opcionales como una entidad de certificación externa, el conector de Citrix Endpoint Management para Exchange ActiveSync y el flujo de tráfico MDM+MAM de Citrix Endpoint Management e Intune MAM.

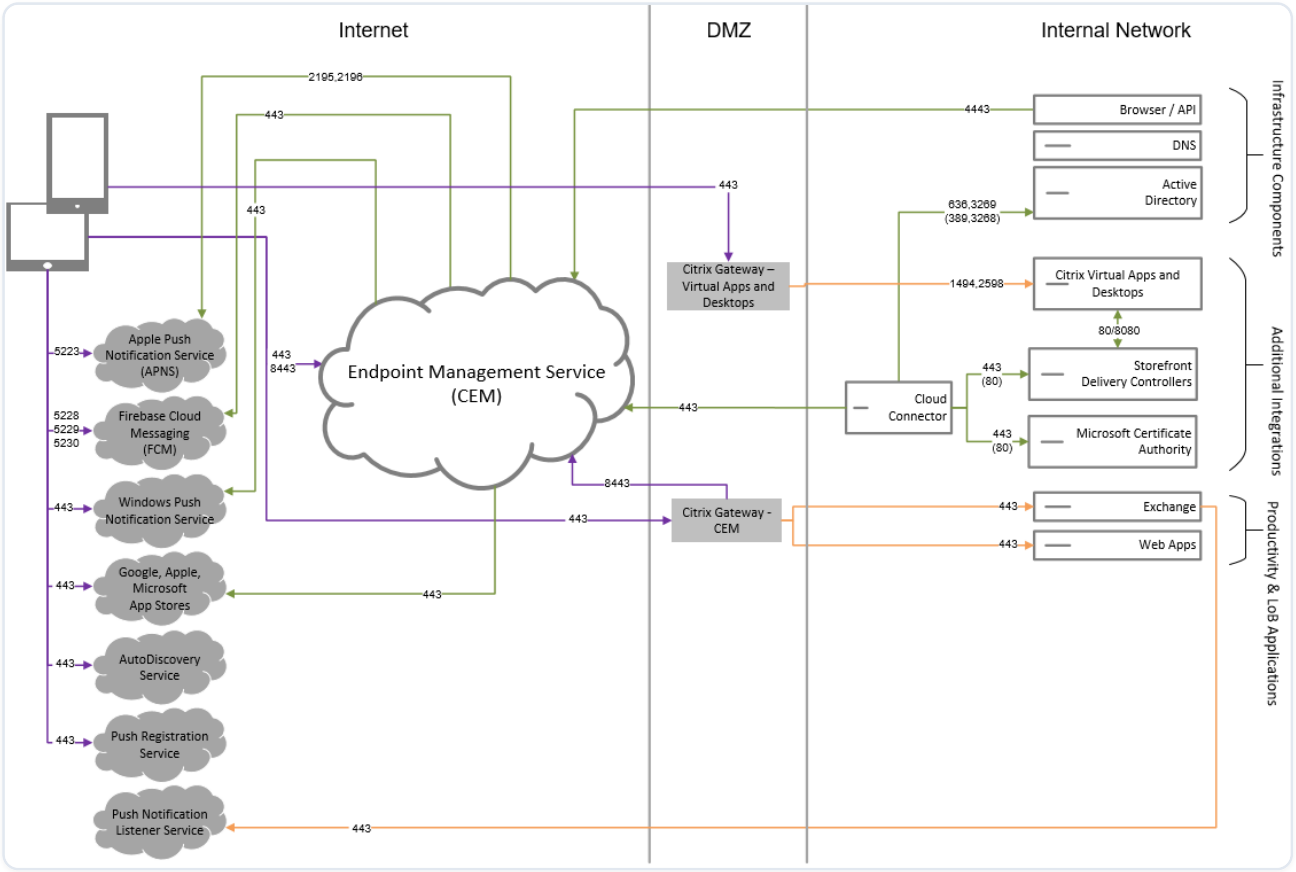
Para obtener más información sobre los requisitos de Citrix ADC y NetScaler Gateway, consulte la documentación del producto de Citrix en `<https://docs.citrix.com/>`.

Arquitectura de referencia principal

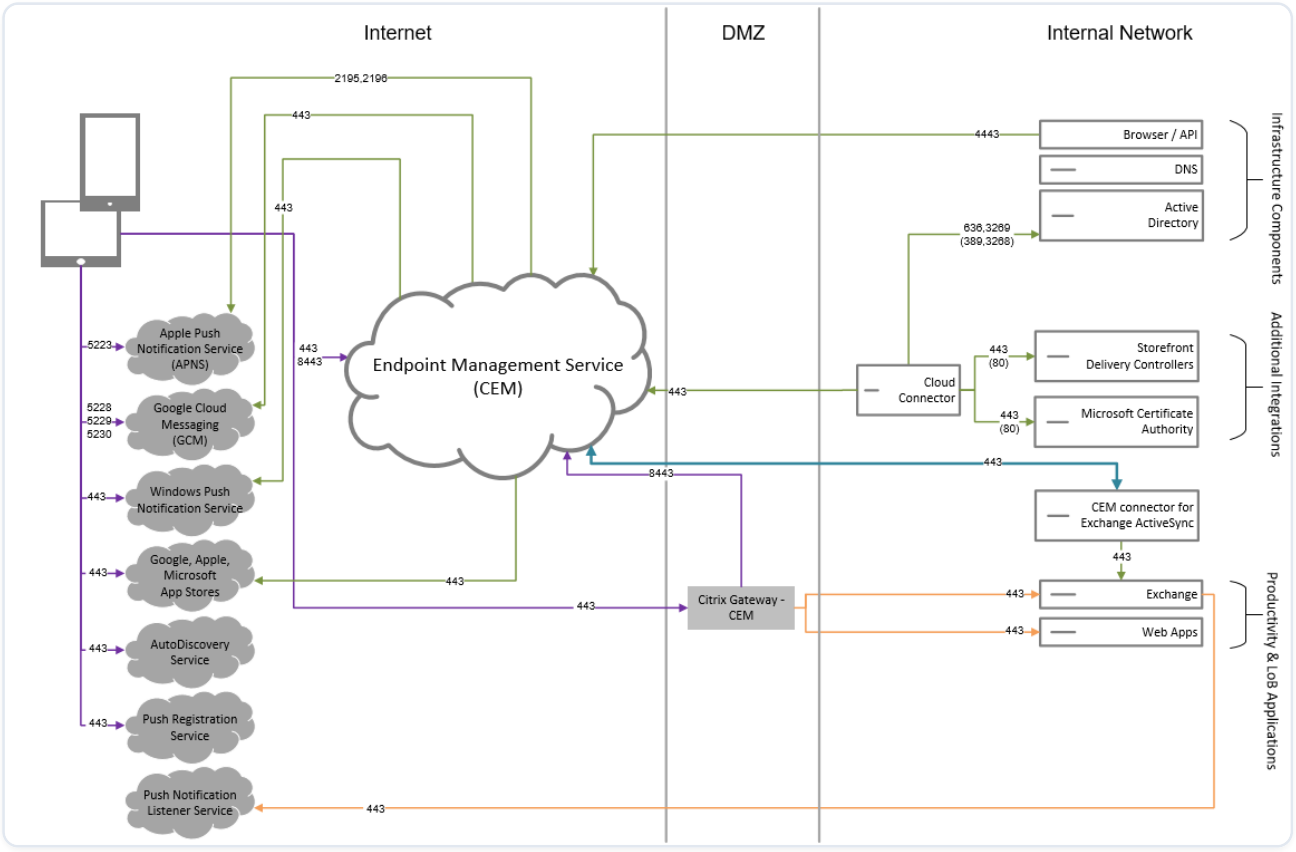
Para obtener detalles sobre los requisitos de puerto, consulte Requisitos del sistema.



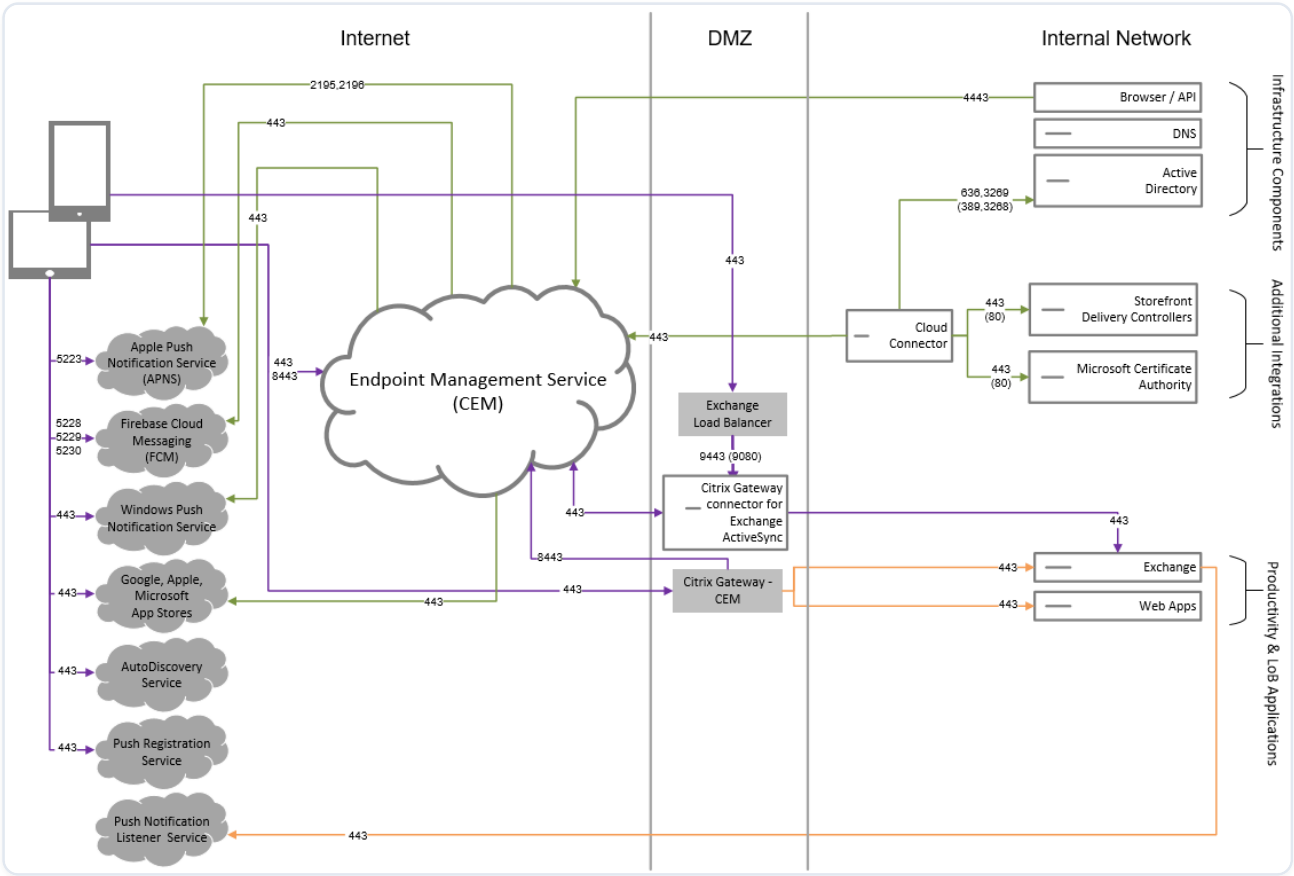
Arquitectura de referencia con Citrix Virtual Apps and Desktops™



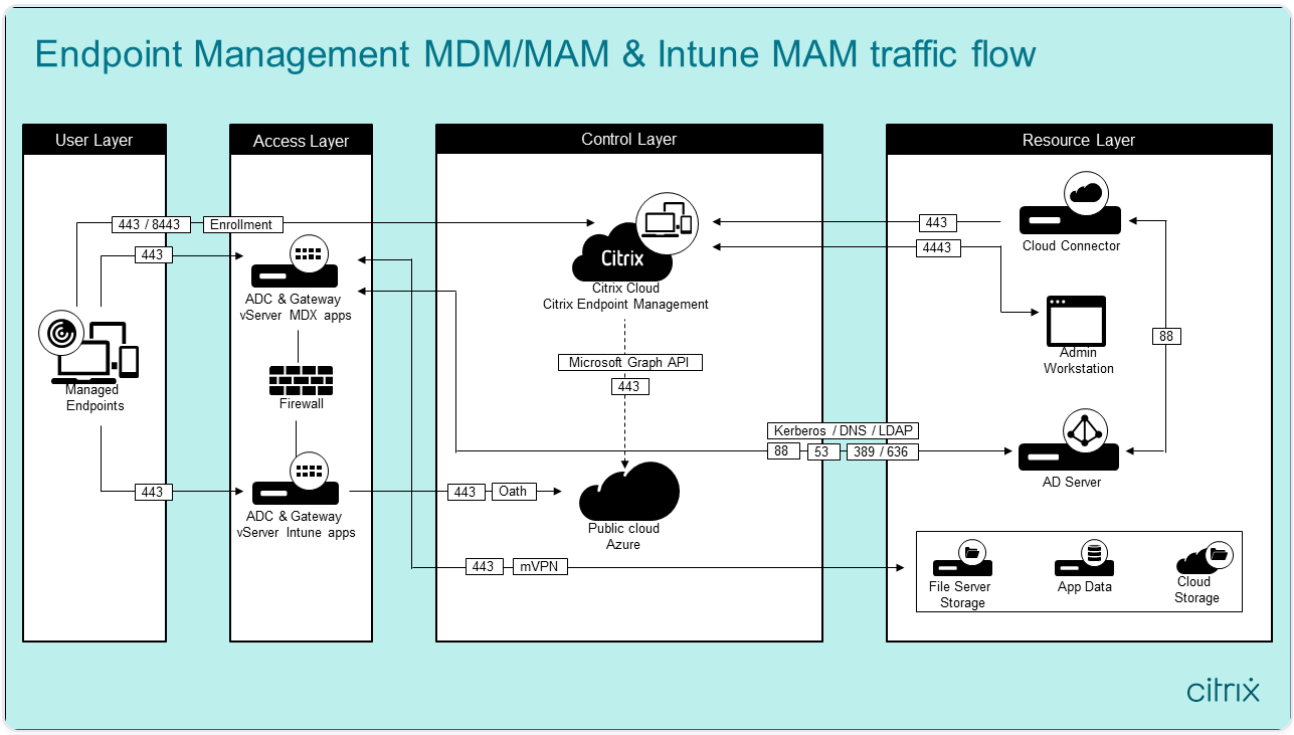
Arquitectura de referencia con el conector de Citrix Endpoint Management para Exchange ActiveSync



Arquitectura de referencia con el conector de NetScaler Gateway para Exchange ActiveSync



Arquitectura de referencia con Citrix Endpoint Management MDM+MAM e Intune MAM



Ubicaciones de recursos

Coloque las ubicaciones de recursos donde mejor se adapten a sus necesidades empresariales. Por ejemplo, en una nube pública, en una sucursal, en una nube privada o en un centro de datos. Los factores que determinan la elección de la ubicación incluyen:

- Proximidad a los suscriptores
- Proximidad a los datos
- Requisitos de escala
- Atributos de seguridad

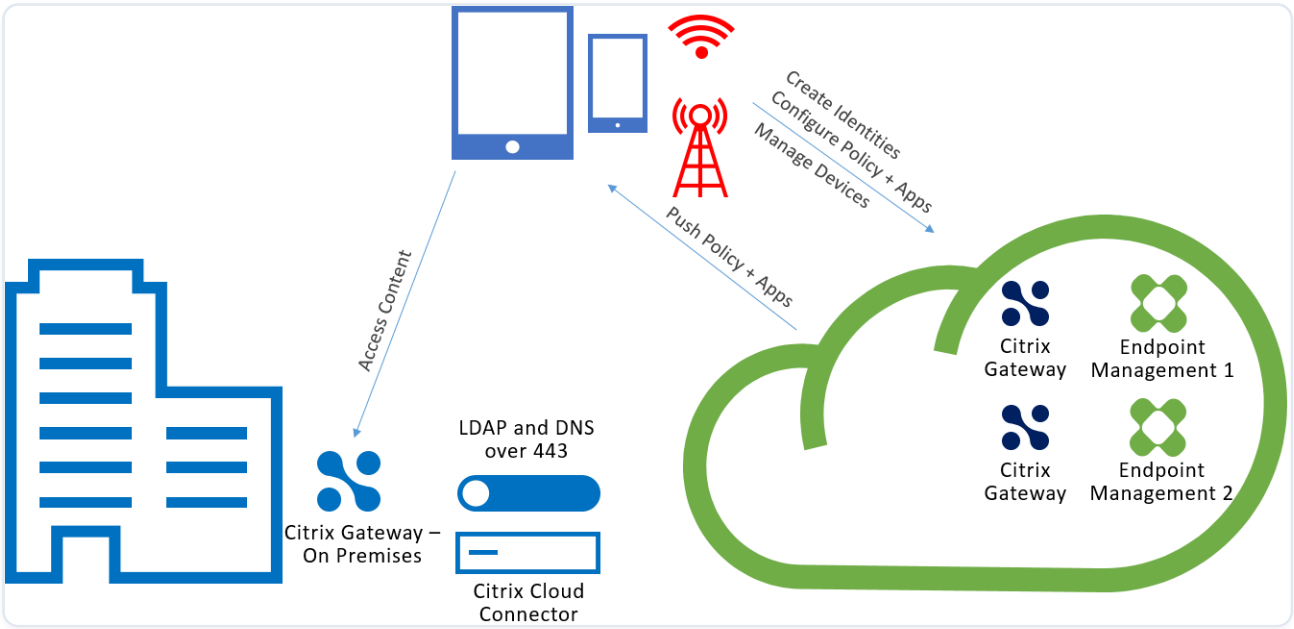
Puede crear cualquier número de ubicaciones de recursos. Por ejemplo, podría:

- Crear una ubicación de recursos en su centro de datos para la oficina central, basada en suscriptores y aplicaciones que requieren proximidad a los datos.
- Agregar una ubicación de recursos separada para sus usuarios globales en una nube pública. O bien, crear ubicaciones de recursos separadas en las sucursales para proporcionar las aplicaciones que mejor se adapten a los trabajadores de la sucursal.
- Agregar una ubicación de recursos adicional en una red separada que proporcione aplicaciones restringidas. Esta configuración proporciona visibilidad restringida a otros recursos y suscriptores sin necesidad de ajustar las otras ubicaciones de recursos.

Cloud Connector

Cloud Connector autentica y cifra toda la comunicación entre Citrix Cloud y sus ubicaciones de recursos. Cloud Connector es necesario para acceder a los siguientes servicios: LDAP, IdP, PKI Server, consultas DNS internas, Citrix Virtual Apps, NetScaler Gateway, Citrix Workspace y Microsoft Endpoint Manager.

El siguiente diagrama muestra el flujo de tráfico de Cloud Connector.



Cloud Connector establece conexiones con Citrix Cloud. Cloud Connector no acepta conexiones entrantes.

Cloud Connector solo está bajo carga durante la inscripción de dispositivos. Para obtener más información, consulte Consideraciones de escala y tamaño para Cloud Connectors.

Una solución que incluye Mobile App Management (MAM) requiere una micro VPN proporcionada por un NetScaler Gateway local. En este escenario:

- Los siguientes componentes se encuentran en su centro de datos:
  - Cloud Connector
  - NetScaler Gateway
  - Sus servidores para Exchange, aplicaciones web, Active Directory y PKI
- Los dispositivos móviles se comunican con Citrix Endpoint Management y su NetScaler Gateway local.

Componentes de Citrix Endpoint Management

Consola de Citrix Endpoint Management. Utilice la consola de administración de Citrix Endpoint Management para configurar Citrix Endpoint Management. Para obtener más información sobre el uso de la consola de Citrix Endpoint Management, consulte los artículos en Citrix Endpoint Management. Citrix le notificará cuando se actualicen los artículos de Novedades de Citrix Endpoint Management para una nueva versión.

Tenga en cuenta estas diferencias entre el servicio Citrix Endpoint Management y las versiones locales:

- El cliente de Remote Support no está disponible para Citrix Endpoint Management.
- Citrix no admite la integración de syslog en Citrix Endpoint Management con un servidor syslog local. En su lugar, puede descargar los registros desde la página **Solución de problemas y soporte** de la consola de Citrix Endpoint Management. Para ello, debe hacer clic en **Descargar todo**.

MAM SDK. El MDX Toolkit tiene previsto alcanzar el fin de vida útil (EOL) en julio de 2023. Para seguir administrando sus aplicaciones empresariales, debe incorporar el MAM SDK.

- El SDK de Mobile Application Management (MAM) proporciona una funcionalidad MDX que no está cubierta por las plataformas iOS y Android. Puede habilitar MDX y proteger aplicaciones iOS o Android. Puede hacer que esas aplicaciones estén disponibles en una tienda interna o en tiendas de aplicaciones públicas. Consulte MDX App SDK.

Aplicaciones de productividad móvil. Las aplicaciones de productividad móvil desarrolladas por Citrix proporcionan un conjunto de herramientas de productividad y comunicación dentro del entorno de Citrix Endpoint Management. Las políticas de su empresa protegen esas aplicaciones. Para obtener más información, consulte Aplicaciones de productividad móvil.

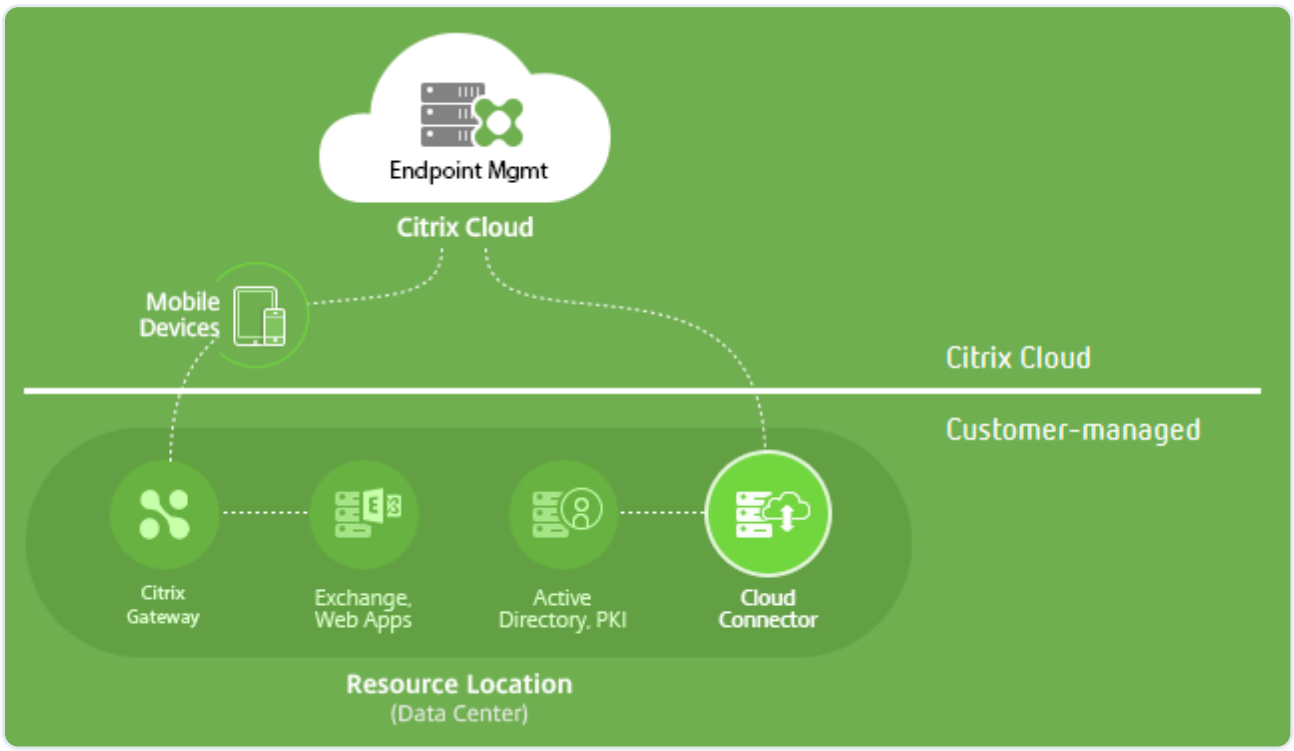
Conector de Citrix Endpoint Management para Exchange ActiveSync. El conector de Citrix Endpoint Management para Exchange ActiveSync proporciona acceso seguro al correo electrónico a los usuarios que utilizan aplicaciones de correo electrónico móvil nativas. El conector para Exchange ActiveSync proporciona filtrado de ActiveSync a nivel de servicio de Exchange. Como resultado, el filtrado solo se produce una vez que el correo llega al servicio de Exchange, en lugar de cuando entra en el entorno de Citrix Endpoint Management. El conector no requiere el uso de NetScaler Gateway. Puede implementar el conector sin cambiar el enrutamiento del tráfico ActiveSync existente. Para obtener más información, consulte Conector de Citrix Endpoint Management para Exchange ActiveSync.

Conector de NetScaler Gateway para Exchange ActiveSync. El conector de NetScaler Gateway para Exchange ActiveSync proporciona acceso seguro al correo electrónico a los usuarios que utilizan aplicaciones de correo electrónico móvil nativas. El conector para Exchange ActiveSync proporciona filtrado de ActiveSync en el perímetro. El filtrado utiliza NetScaler Gateway como proxy para el tráfico de ActiveSync. Como resultado, el componente de filtrado se encuentra en la ruta del flujo de tráfico de correo, interceptando el correo a medida que entra o sale del entorno. El conector para Exchange ActiveSync actúa como intermediario entre NetScaler Gateway y Citrix Endpoint Management. Para obtener más información, consulte Conector de NetScaler Gateway para Exchange ActiveSync.

Descripción general de la seguridad técnica de Citrix Endpoint Management

Citrix Cloud administra el plano de control para los entornos de Citrix Endpoint Management. El plano de control incluye el servidor de Citrix Endpoint Management, el equilibrador de carga de Citrix ADC y una base de datos de un solo inquilino. El servicio en la nube se integra con un centro de datos de cliente mediante Citrix Cloud Connector. Los clientes de Citrix Endpoint Management que utilizan Cloud Connector suelen administrar NetScaler Gateway en sus centros de datos.

La siguiente figura ilustra el servicio y sus límites de seguridad.



La información de esta sección:

- Ofrece una introducción a la funcionalidad de seguridad de Citrix Cloud.
- Define la división de responsabilidades entre Citrix y los clientes para proteger la implementación de Citrix Cloud.
- No es la guía de configuración o administración de Citrix Cloud ni de ninguno de sus componentes o servicios.

Para obtener información sobre la tecnología utilizada por Citrix Endpoint Management para ofrecer una seguridad integral de extremo a extremo, consulte Seguridad y productividad para la empresa móvil.

Flujo de datos

El plano de control tiene acceso de lectura limitado a los objetos de usuario y grupo. Esos objetos se encuentran en su directorio, DNS y servicios similares. El plano de control accede a esos servicios a través de Citrix Cloud Connector mediante conexiones HTTPS seguras.

Los datos de la empresa, como el correo electrónico, la intranet y el tráfico de aplicaciones web, fluyen directamente entre un dispositivo y los servidores de aplicaciones a través de NetScaler Gateway. NetScaler Gateway se implementa en el centro de datos del cliente.

Aislamiento de datos

El plano de control almacena los metadatos necesarios para administrar los dispositivos de usuario y sus aplicaciones móviles. El servicio en sí consta de una combinación de componentes multiempresa y de un solo inquilino. Sin embargo, según la arquitectura del servicio, los metadatos del cliente siempre se almacenan por separado para cada inquilino y se protegen mediante credenciales únicas.

Gestión de credenciales

El servicio gestiona los siguientes tipos de credenciales:

- **Credenciales de usuario:** Las credenciales de usuario se transmiten desde el dispositivo al plano de control a través de una conexión HTTPS. El plano de control valida estas credenciales con un directorio en el directorio del cliente a través de una conexión segura.
- **Credenciales de administrador:** Los administradores se autentican en Citrix Cloud, que utiliza el sistema de inicio de sesión de Citrix Online. Este proceso genera un token web JSON (JWT) firmado de un solo uso, que otorga al administrador acceso al servicio.
- **Credenciales de Active Directory:** El plano de control requiere credenciales de enlace para leer los metadatos de usuario de Active Directory. Estas credenciales se cifran mediante cifrado AES-256 y se guardan en una base de datos por inquilino.

Consideraciones de implementación

Citrix recomienda consultar la documentación de prácticas recomendadas publicada para implementar NetScaler Gateway en sus entornos.

Más recursos

Se recomienda a los clientes que revisen los boletines de seguridad relacionados con sus productos Citrix. Para obtener información sobre los boletines de seguridad nuevos y actualizados,

consulte Boletines de seguridad de Citrix. Considere también la posibilidad de registrarse para recibir alertas en su Configuración de alertas.

Consulte los siguientes recursos para obtener más información sobre seguridad:

- Sitio de seguridad de Citrix: `<https://www.citrix.com/security>`
- Documentación de Citrix Cloud: Guía de implementación segura para la plataforma Citrix Cloud
- Guía de implementación segura para Citrix ADC

Integración con el software Mobile Threat Defense

El software Mobile Threat Defense (MTD) detecta, analiza y ayuda a prevenir ciberataques avanzados contra dispositivos móviles empresariales. La combinación de MTD y Unified Citrix Endpoint Management (UEM) aumenta la seguridad y la visibilidad de su organización.

El software MTD proporciona datos de amenazas que Citrix Endpoint Management utiliza para:

- Proteger contra malware, phishing, ataques de red y ataques de intermediario
- Determinar el estado de cumplimiento del dispositivo
- Determinar los niveles de riesgo
- Realice acciones basadas en políticas para proteger sus aplicaciones, datos, dispositivos y red móvil

Citrix Endpoint Management se integra con los siguientes proveedores de MTD:

- Check Point
- Lookout
- Wandera
- Zimperium

Para obtener más información o para solicitar una demostración, póngase en contacto con nuestros socios de MTD o con su representante de ventas de Citrix.

Integración de Citrix Endpoint Management con Microsoft Endpoint Manager

La integración de Citrix Endpoint Management con Microsoft Endpoint Manager (MEM) añade el valor de la micro VPN de Citrix Endpoint Management a las aplicaciones compatibles con Microsoft Intune, como el explorador Microsoft Edge.

Para activar la integración, póngase en contacto con el equipo de operaciones de Citrix Cloud.

Esta versión admite los siguientes casos de uso:

- Intune MAM con Citrix Endpoint Management MDM+MAM.

  Este artículo se centra en el caso de uso de Intune MAM + Citrix Endpoint Management MDM+MAM. Después de añadir Citrix como su proveedor de MDM, configure las aplicaciones administradas por Intune para su entrega a los dispositivos.

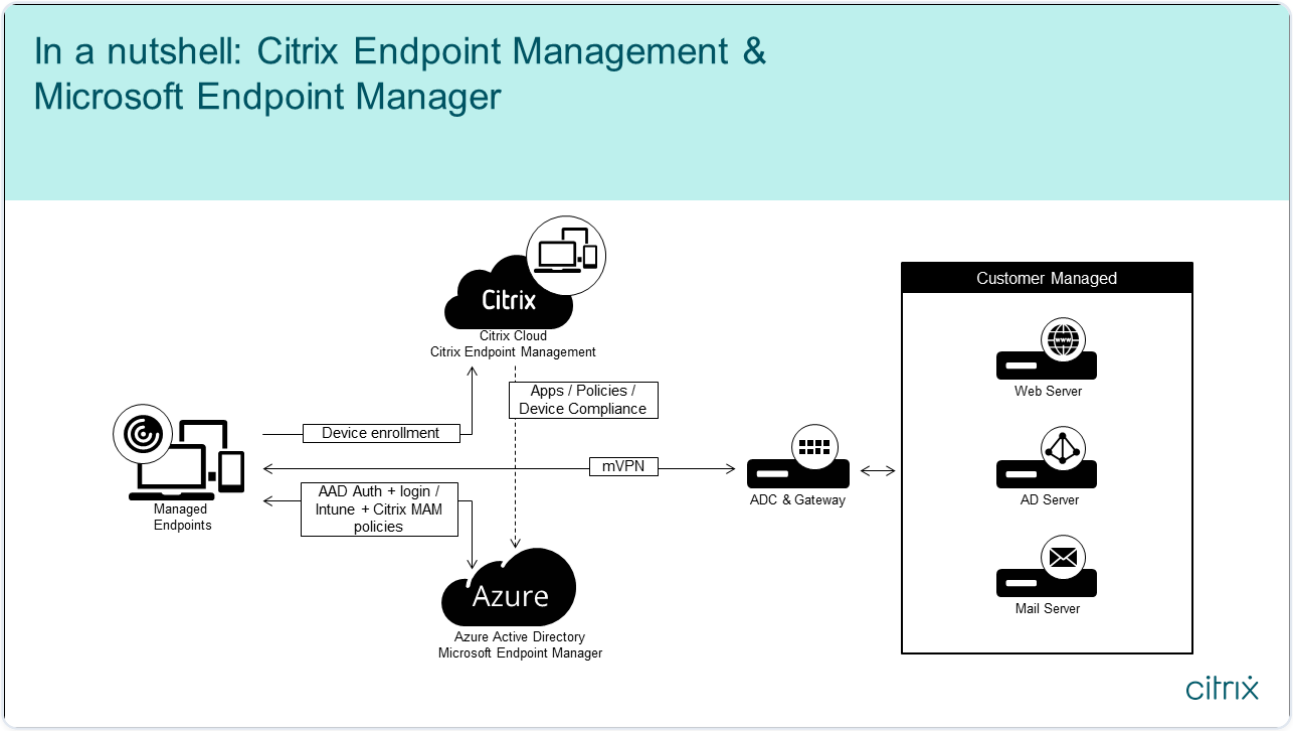
  > **Importante:**
  >
  > - Para este caso de uso, Citrix Secure Mail no admite la integración con Intune.
  > - La integración de Citrix Secure Mail con Intune está obsoleta y se eliminará en una versión futura. Consulte Novedades de Secure Mail para obtener más detalles.

- Intune MAM y Citrix Endpoint Management MDM.
- Intune MAM.
- Intune MAM e Intune MDM. Citrix Secure Mail para iOS admite el inicio de sesión único para este caso de uso.

Para obtener una guía gráfica y fácil de seguir sobre cómo configurar la integración de Citrix Endpoint Management con MEM, consulte Guía de introducción.

Para obtener información sobre la integración con el acceso condicional de Azure AD, consulte Integrar con el acceso condicional de Azure AD.

El siguiente diagrama proporciona una descripción general de la integración de Citrix Endpoint Management con Microsoft Endpoint Manager.



Requisitos del sistema

Habilitar MDX

- MAM SDK

  o

- MDX Toolkit

Microsoft

- Acceso a Azure Active Directory (AD) (con privilegios de administrador de inquilino)
- Inquilino habilitado para Intune

Regla de firewall

- Habilite una regla de firewall para permitir el tráfico DNS y SSL desde una IP de subred de NetScaler Gateway a `*.manage.microsoft.com`, `https://login.microsoftonline.com` y `https://graph.windows.net` (puertos 53 y 443)

Requisitos previos

- **Navegador Microsoft Edge:** El SDK de aplicaciones móviles está integrado en la aplicación del navegador Microsoft Edge para iOS y Android. Para obtener más información sobre Microsoft Edge, consulte la documentación de Microsoft Edge.
- **Cuenta de Citrix Cloud:** Para registrarse en una cuenta de Citrix y solicitar una prueba de Citrix Endpoint Management, póngase en contacto con su representante de ventas de Citrix. Cuando esté listo para continuar, vaya a https://onboarding.cloud.com. Para obtener más información sobre cómo solicitar una cuenta de Citrix Cloud, consulte Registrarse en Citrix Cloud.

  > **Nota:**
  >
  > El correo electrónico que proporcione debe ser una dirección que no esté asociada con Azure AD. Puede utilizar cualquier servicio de correo electrónico gratuito.

- **Certificados APNs para iOS:** Asegúrese de configurar el certificado APNs para iOS. Para obtener más información sobre cómo configurar estos certificados, consulte esta publicación del blog de Citrix: Creación e importación de certificados APNs.
- **Sincronización de Azure AD:** Configure la sincronización entre Azure AD y Active Directory local. No instale la herramienta de sincronización de AD en la máquina del controlador de dominio. Para obtener más información sobre cómo configurar esta sincronización, consulte la documentación de Microsoft sobre Azure Active Directory.

Configuración de NetScaler Gateway

Si está configurando una nueva implementación de Citrix Endpoint Management, instale uno de estos dispositivos NetScaler Gateway:

- NetScaler® Gateway VPX serie 3000 o superior
- NetScaler Gateway MPX o instancia SDX dedicada

Para usar NetScaler Gateway con la integración de Citrix Endpoint Management con MEM:

- Configure NetScaler Gateway con una interfaz de administración y una IP de subred.
- Utilice TLS 1.2 para toda la comunicación de cliente a servidor. Para obtener información sobre cómo configurar TLS 1.2 para NetScaler Gateway, consulte CTX247095.

Si utiliza la integración de Citrix Endpoint Management con MEM con una implementación MDM+MAM de Citrix Endpoint Management, configure dos Citrix Gateways. El tráfico de la aplicación MDX se enruta a través de un NetScaler Gateway. El tráfico de la aplicación Intune se enruta a través del otro NetScaler Gateway. Configure:

- Dos IP públicas.
- Opcionalmente, una IP con traducción de direcciones de red.
- Dos nombres DNS. Ejemplo: `https://mam.company.com`.
- Dos certificados SSL públicos. Configure certificados que coincidan con el nombre DNS público reservado o utilice certificados comodín.
- Un equilibrador de carga MAM con una dirección IP RFC 1918 interna no enrutable.
- Una cuenta de servicio LDAP de Active Directory.

Consentimiento a las solicitudes de permisos delegados

Para las aplicaciones administradas que requieren que los usuarios se autentiquen, las aplicaciones solicitan permisos de aplicación expuestos por Microsoft Graph. Al dar su consentimiento a estas solicitudes de permisos, la aplicación puede acceder a los recursos y las API necesarios. Algunas aplicaciones requieren el consentimiento del administrador global de Microsoft Azure AD. Para estos permisos delegados, el administrador global debe conceder a Citrix Cloud permiso para solicitar tokens. Los tokens habilitan los siguientes permisos. Para obtener más información, consulte referencia de permisos de Microsoft Graph.

- **Iniciar sesión y leer el perfil de usuario:** Este permiso permite a los usuarios iniciar sesión y conectarse a Azure AD. Citrix® no puede ver las credenciales de usuario.
- **Leer los perfiles básicos de todos los usuarios:** La aplicación lee las propiedades del perfil de los usuarios de la organización. Las propiedades incluyen el nombre para mostrar, el nombre y los apellidos, la dirección de correo electrónico y la foto de los usuarios de la organización.
- **Leer todos los grupos:** Este permiso permite especificar grupos de Azure AD para la asignación de aplicaciones y directivas.
- **Acceder al directorio como el usuario que ha iniciado sesión:** Este permiso verifica la suscripción a Intune y habilita las configuraciones de NetScaler Gateway y VPN.
- **Leer y escribir aplicaciones de Microsoft Intune:** La aplicación puede leer y escribir lo siguiente:
    - Propiedades administradas por Microsoft

- Asignaciones de grupo y el estado de las aplicaciones
- Configuraciones de aplicaciones
- Directivas de protección de aplicaciones

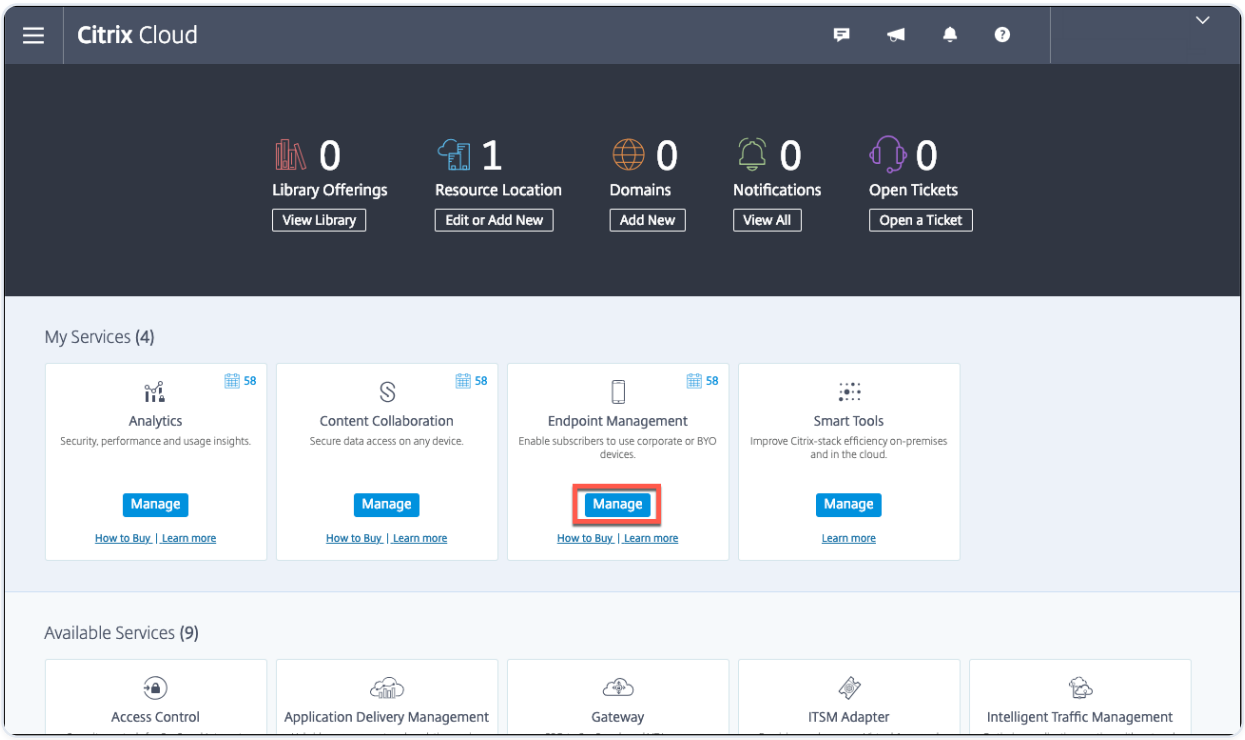
Además, durante la configuración de NetScaler Gateway, el administrador global de Azure AD debe:

- Aprobar el Active Directory elegido para la micro VPN. El administrador global también debe generar un secreto de cliente que NetScaler Gateway utiliza para comunicarse con Azure AD e Intune.
- No tener el rol de administrador de Citrix. En su lugar, el administrador de Citrix asigna cuentas de Azure AD a los usuarios con los privilegios de administrador de aplicaciones de Intune adecuados. El administrador de Intune asume entonces el rol de administrador de Citrix Cloud para gestionar Intune desde Citrix Cloud.

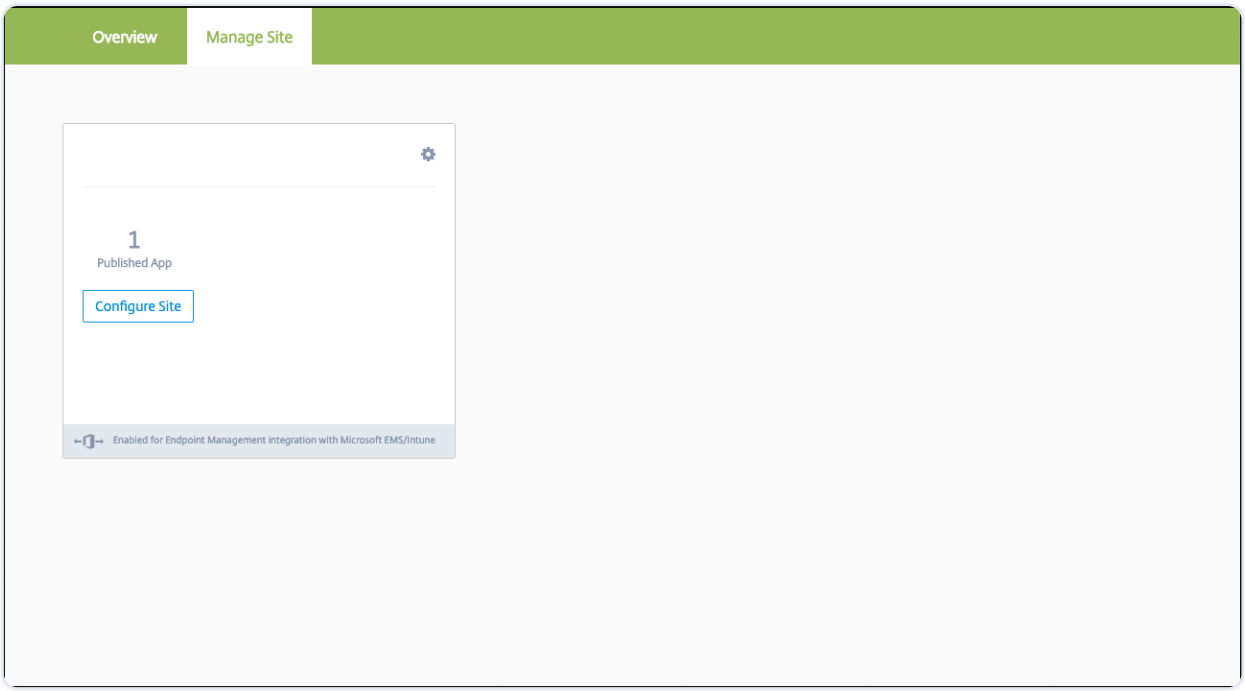
> **Nota:**
>
> Citrix solo utiliza la contraseña del administrador global de Intune durante la configuración y redirige la autenticación a Microsoft. Citrix no puede acceder a la contraseña.

Para configurar la integración de Citrix Endpoint Management con MEM

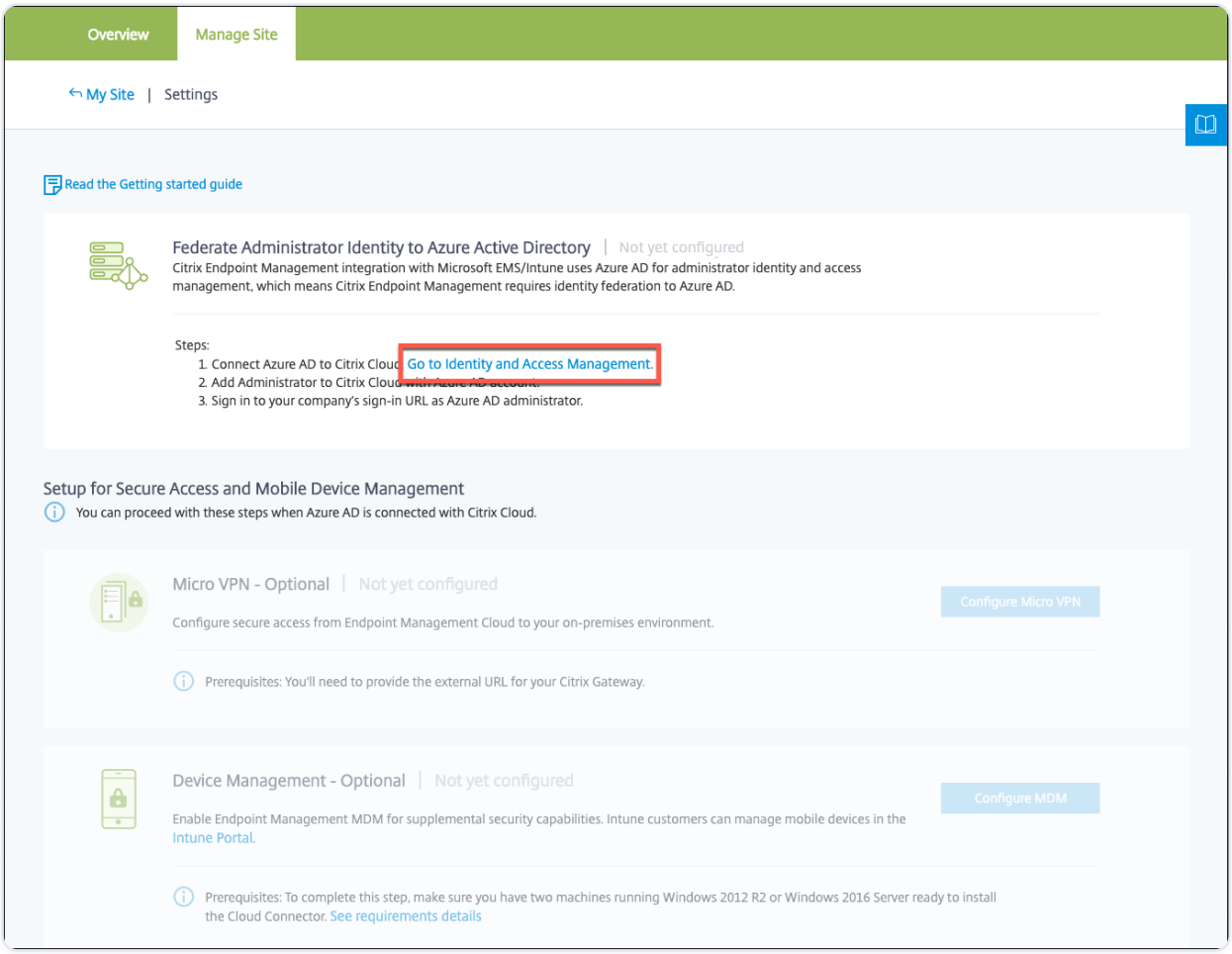
1. Inicie sesión en el sitio de Citrix Cloud y solicite una prueba de Citrix Endpoint Management.
2. Un ingeniero de ventas programará una reunión de incorporación con usted. Hágales saber que desea la integración de Citrix Endpoint Management con MEM. Cuando se apruebe su solicitud, haga clic en **Administrar**.



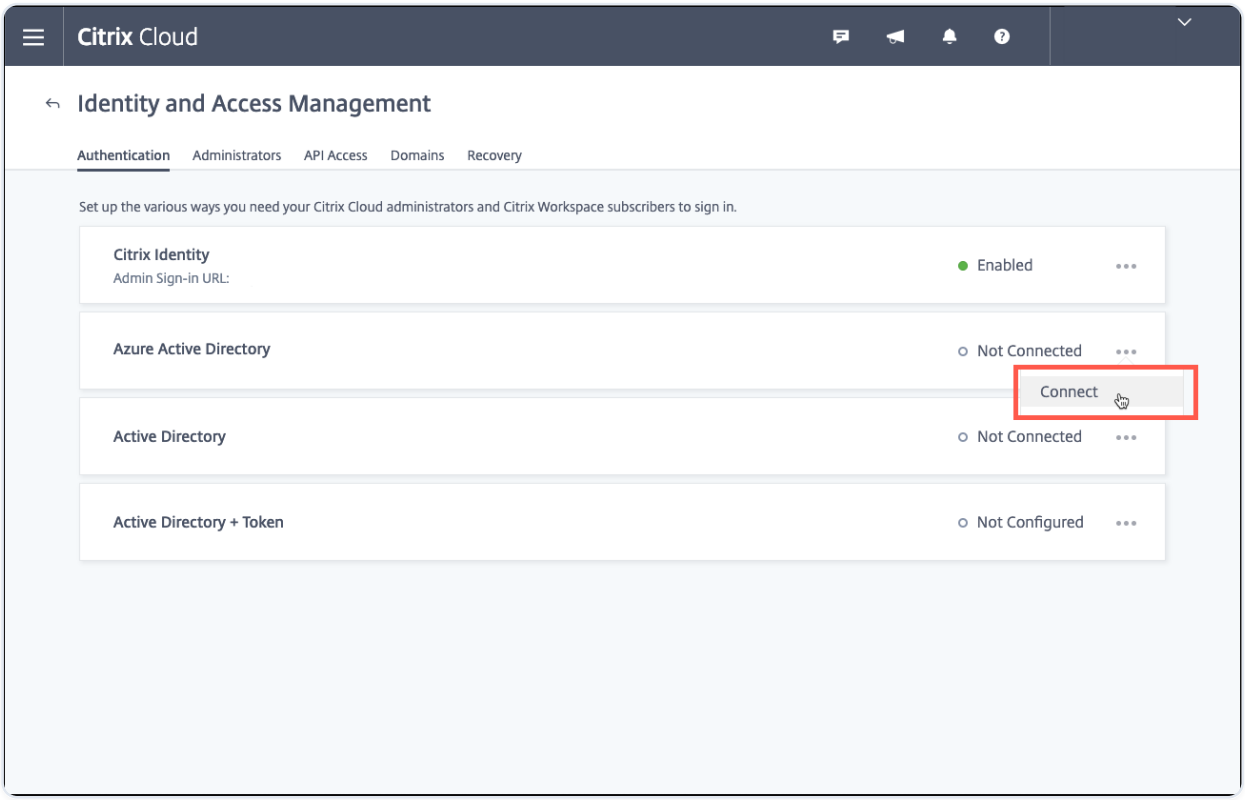
3. Desde aquí, puede hacer clic en el icono de engranaje en la parte superior derecha de su sitio o hacer clic en **Configurar sitio**.



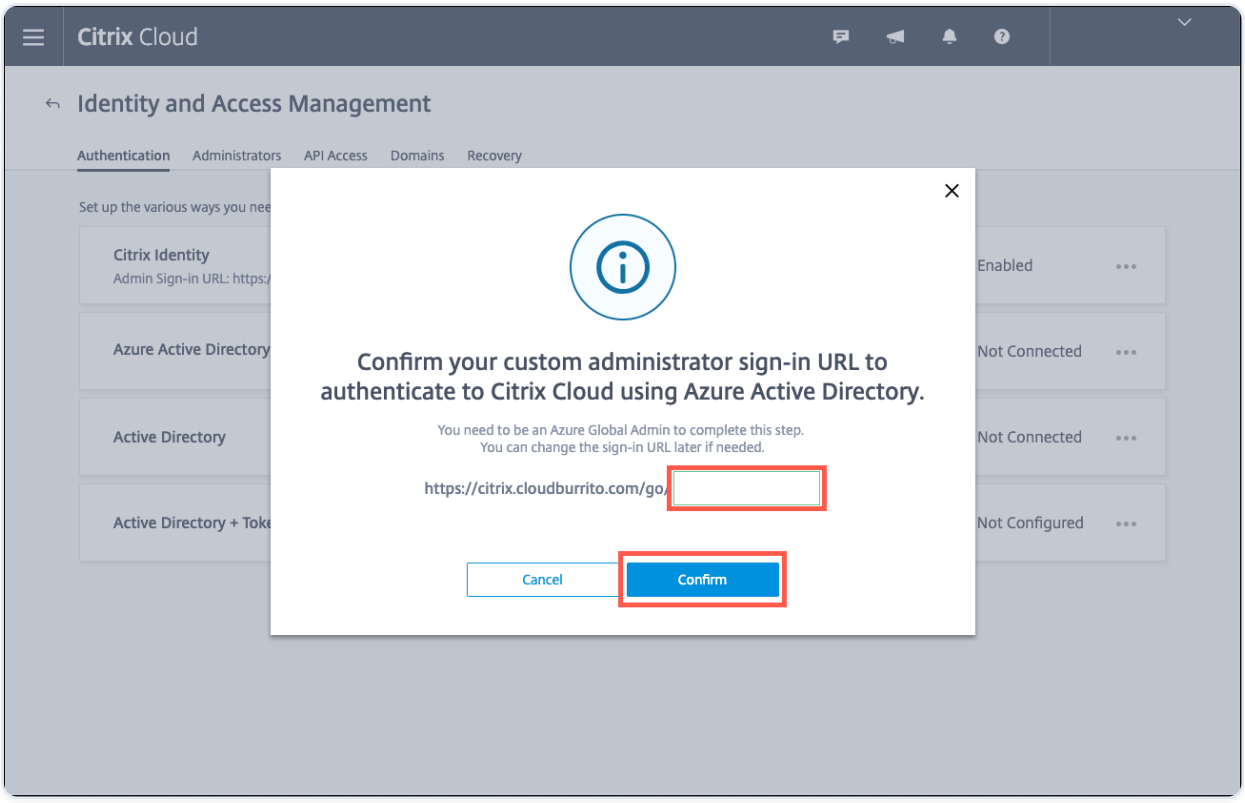
4. Siga el enlace del primer paso a la página de **Administración de identidades y accesos**.



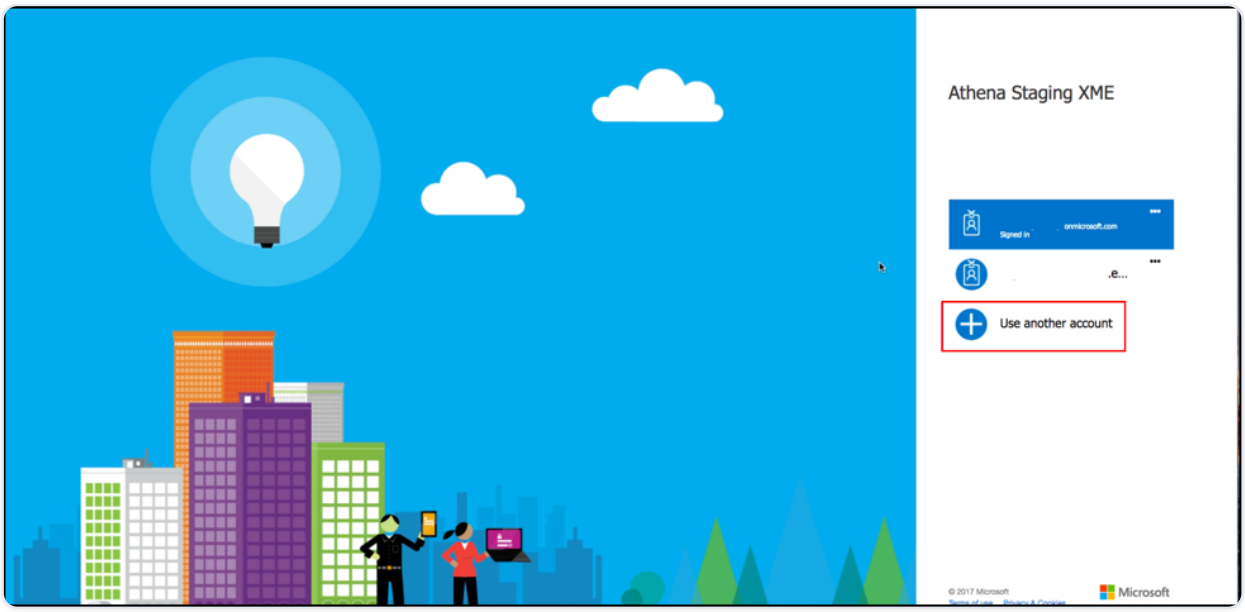
5. Haga clic en **Conectar** para conectar su instalación de Azure AD.



6. Introduzca una URL de inicio de sesión única que el administrador de Azure AD utilizará para iniciar sesión y, a continuación, haga clic en **Confirmar**.

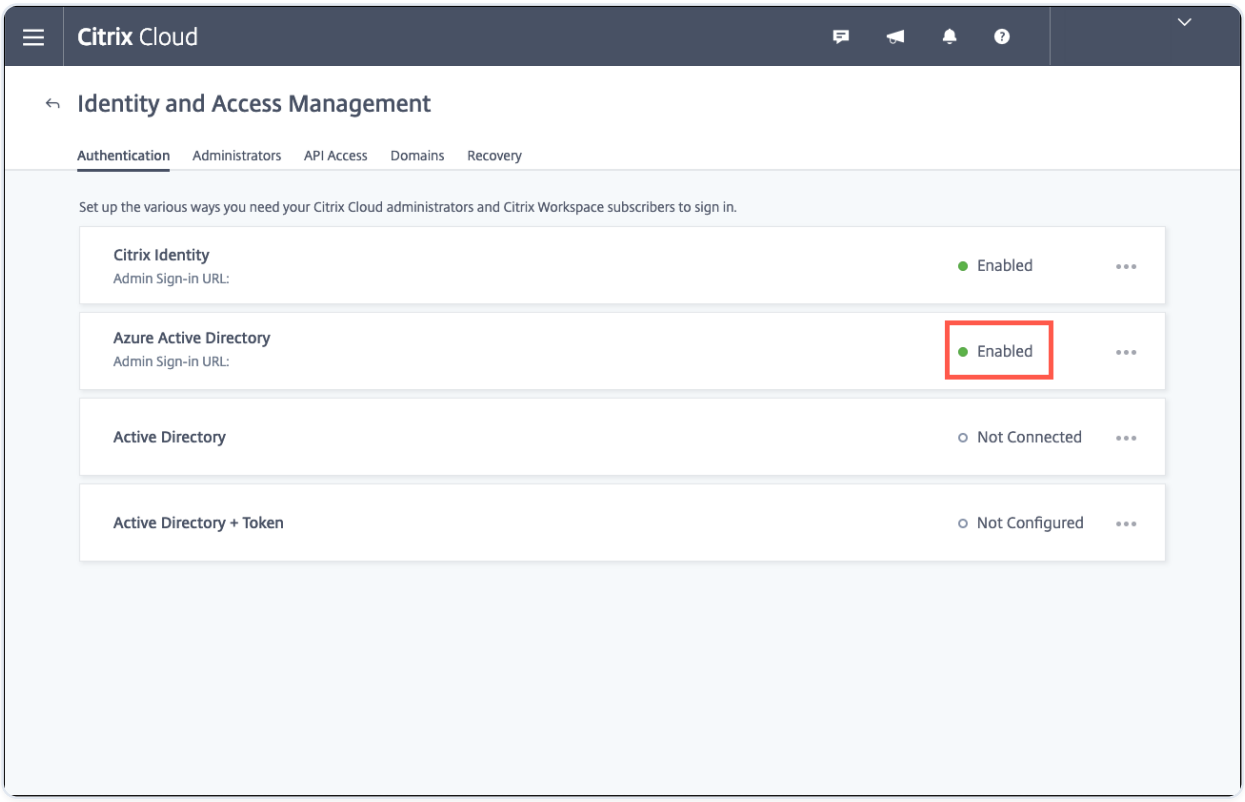


7. Añada una cuenta de administrador global de Azure AD y, a continuación, acepte la solicitud de permisos.



](/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems6.png)

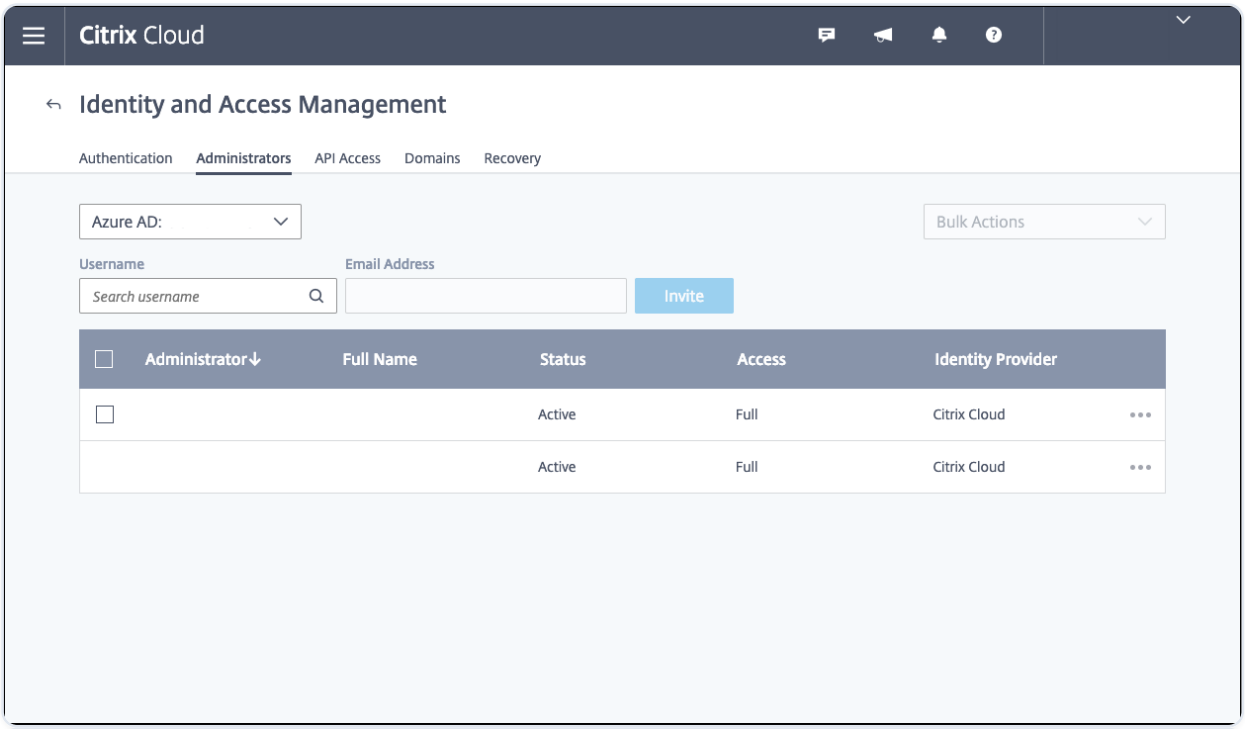
8. Confirme que su instancia de Azure AD se conecta correctamente. Para indicar una conexión correcta, el texto **No conectado** cambia a **Habilitado**.

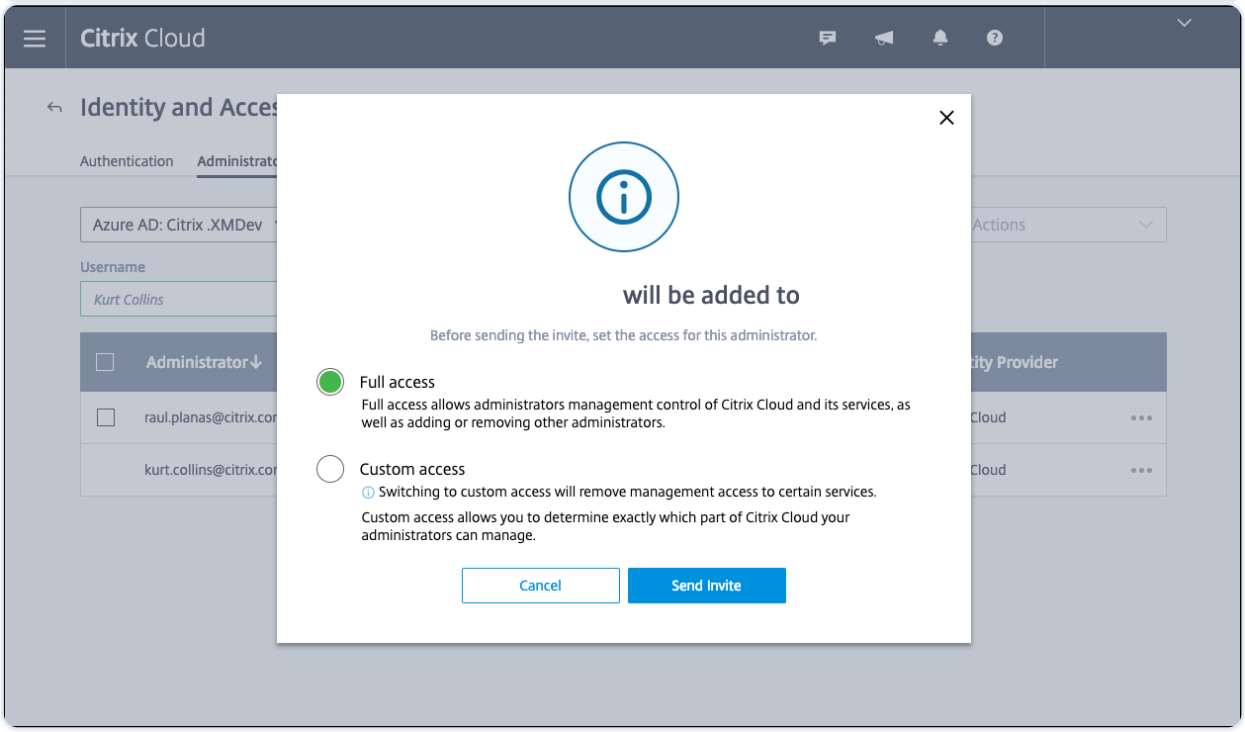


9. Haga clic en la ficha **Administradores** y, a continuación, agregue su administrador de Azure AD Intune como administrador de Citrix Cloud. Seleccione Azure AD o Citrix Identity en el menú desplegable y, a continuación, busque el nombre de usuario que desea agregar. Haga clic en **Invitar** y, a continuación, conceda al usuario **Acceso total** o **Acceso personalizado** antes de hacer clic en **Enviar invitación**.

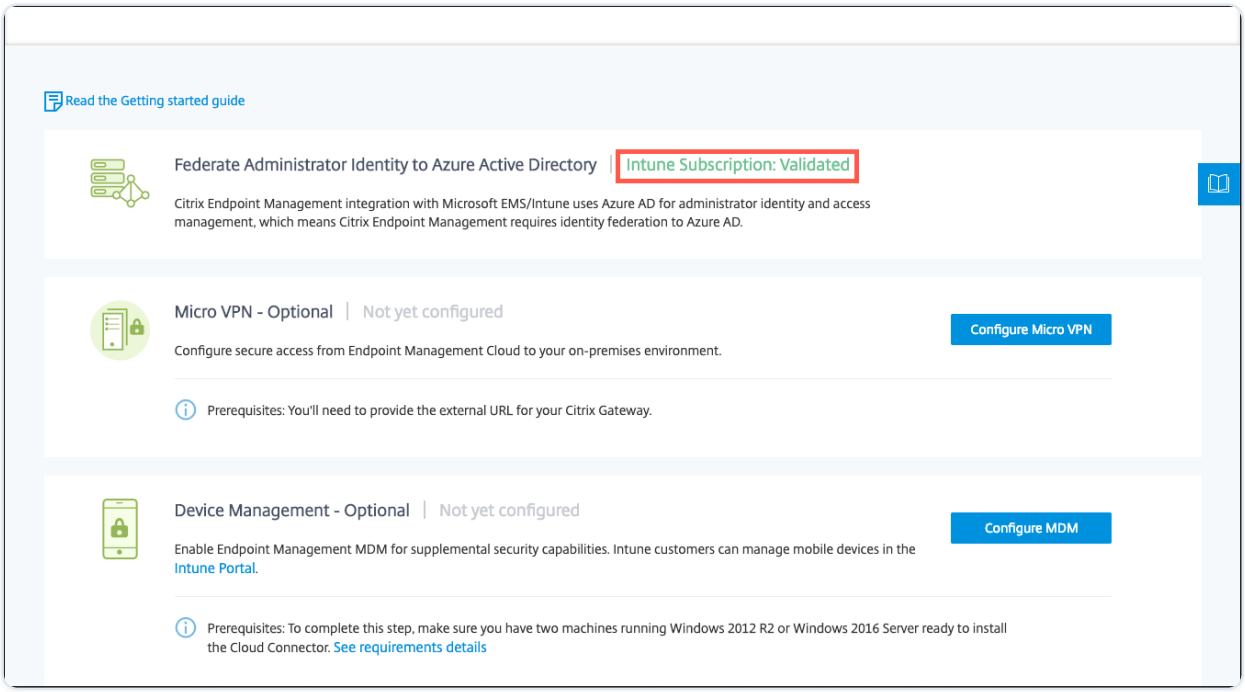
> **Nota:**
>
> Citrix Endpoint Management requiere las siguientes reglas para el **Acceso personalizado:** Biblioteca y Citrix Endpoint Management.
>
> Como resultado, el administrador de Azure AD Intune recibe una invitación por correo electrónico para crear una contraseña e iniciar sesión en Citrix Cloud. Antes de que el administrador inicie sesión, asegúrese de cerrar sesión en todas las demás cuentas.

El administrador de Azure AD Intune debe seguir los pasos restantes de este procedimiento.





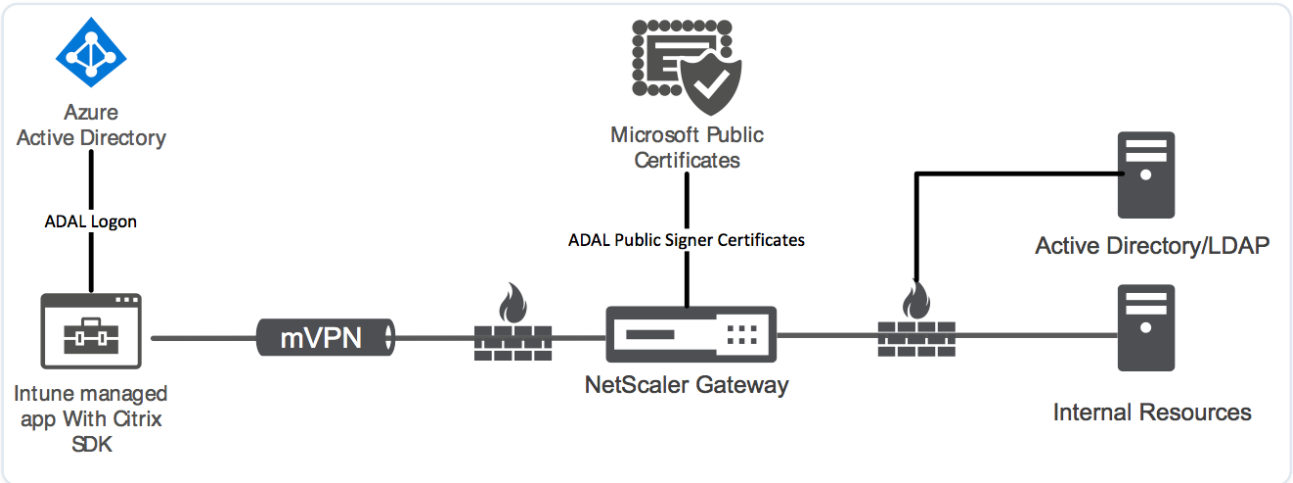
10. Después de iniciar sesión con la nueva cuenta, en **Citrix Endpoint Management**, haga clic en **Administrar**. Si configura todo correctamente, la página muestra que el administrador de Azure AD ha iniciado sesión y que su suscripción a Intune es válida.



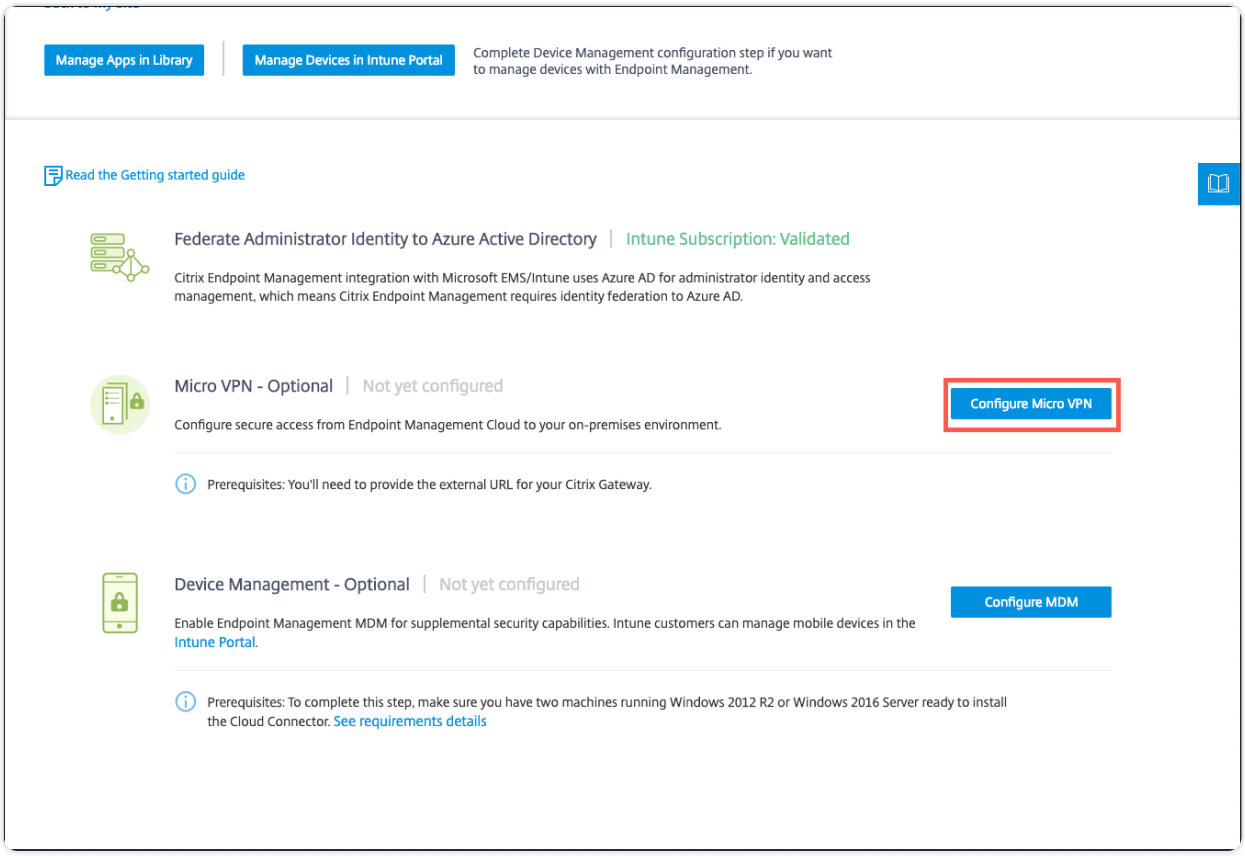
Para configurar NetScaler Gateway para micro VPN

Para usar micro VPN con Intune, debe configurar NetScaler Gateway para que se autentique en Azure AD. Un servidor virtual de NetScaler Gateway existente no funciona para este caso de uso.

Primero, configure Azure AD para que se sincronice con el Active Directory local. Este paso es necesario para asegurarse de que la autenticación entre Intune y NetScaler Gateway se realice correctamente.

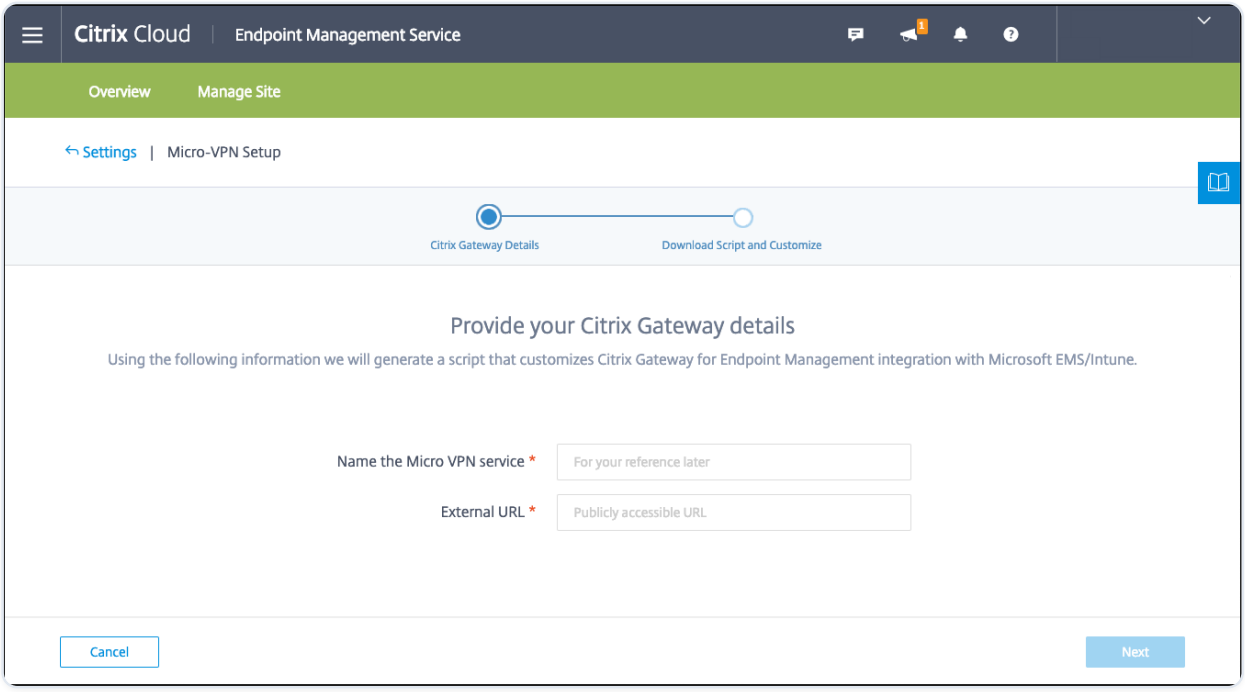


1. En la consola de Citrix Cloud, en **Citrix Endpoint Management**, haga clic en **Administrar**.
2. Junto a **Micro VPN**, haga clic en **Configurar Micro VPN**.

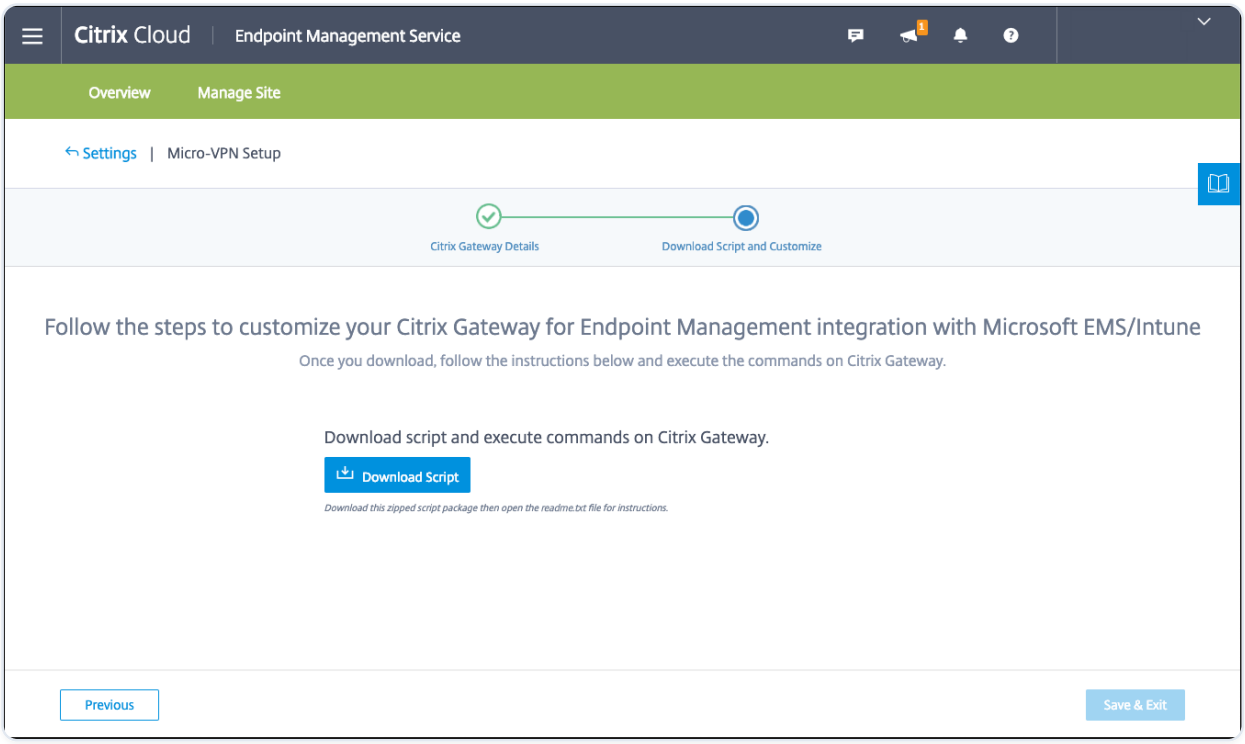


3. Introduzca un nombre para el servicio de micro VPN y la URL externa de su NetScaler Gateway y, a continuación, haga clic en **Siguiente**.

   Este script configura NetScaler Gateway para admitir Azure AD y las aplicaciones de Intune.



4. Haga clic en **Descargar script**. El archivo .zip incluye un archivo Léame con instrucciones para implementar el script. Aunque puede Guardar y salir desde aquí, la Micro VPN no se configura hasta que ejecute el script en su instalación de NetScaler Gateway.



Nota:

Cuando termine el proceso de configuración de NetScaler Gateway, si ve un estado de OAuth distinto de COMPLETE, consulte la sección Solución de problemas.

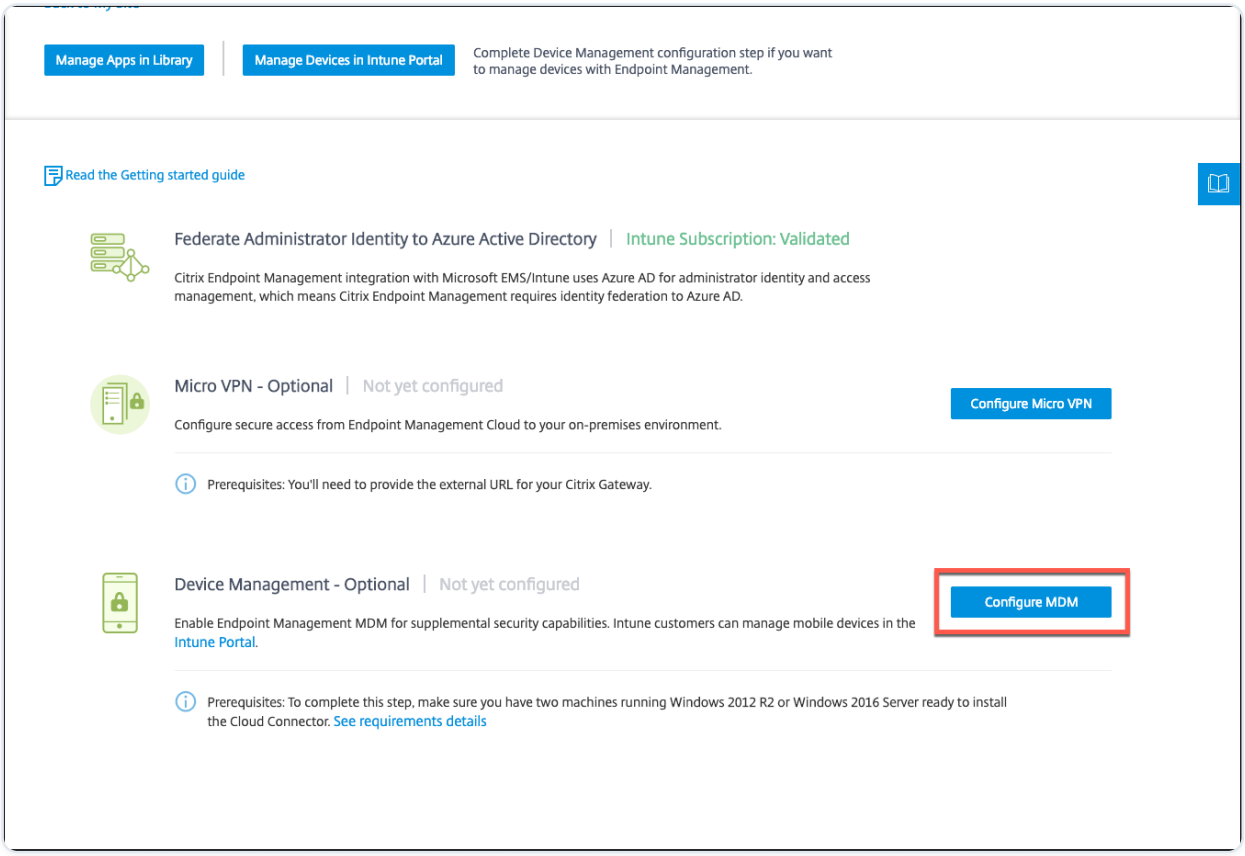
Para configurar la administración de dispositivos

Si desea administrar dispositivos además de aplicaciones, elija un método de administración de dispositivos. Puede usar Citrix Endpoint Management MDM+MAM o Intune MDM.

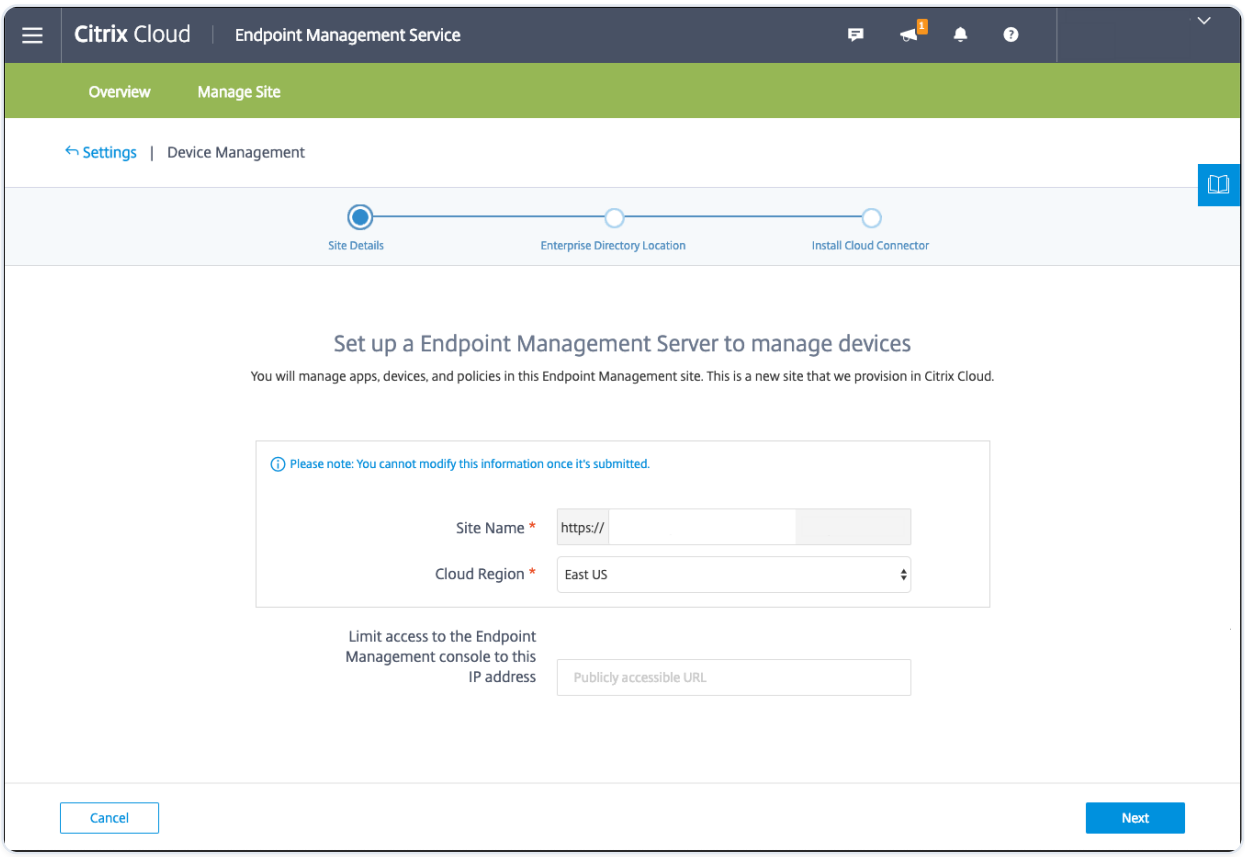
Nota:

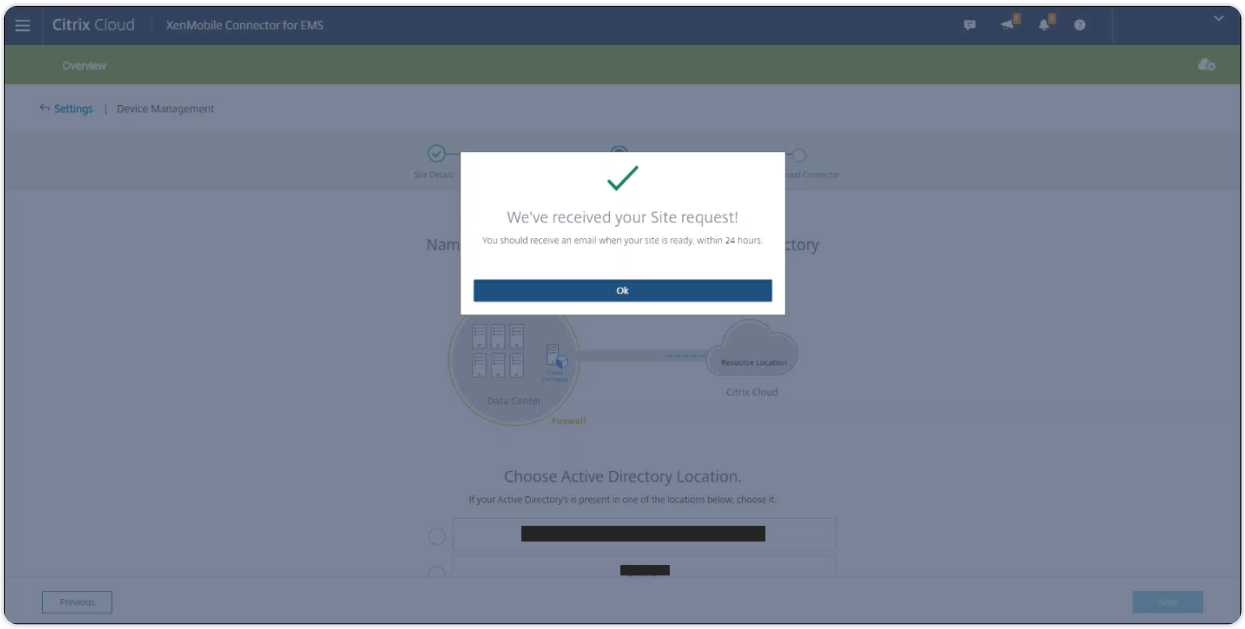
La consola utiliza Intune MDM de forma predeterminada. Para usar Intune como proveedor de MDM, consulte la documentación de Microsoft Intune.

1. En la consola de Citrix Cloud, en Integración de Citrix Endpoint Management con MEM, haga clic en **Administrar**. Junto a **Administración de dispositivos - Opcional**, haga clic en **Configurar MDM**.

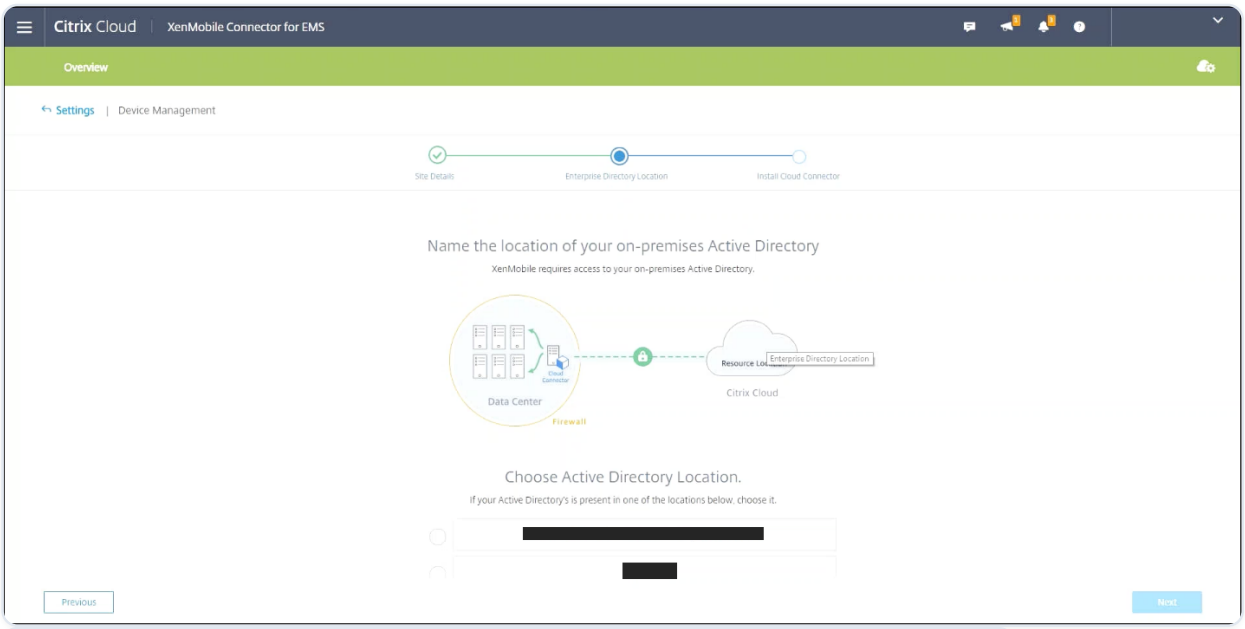


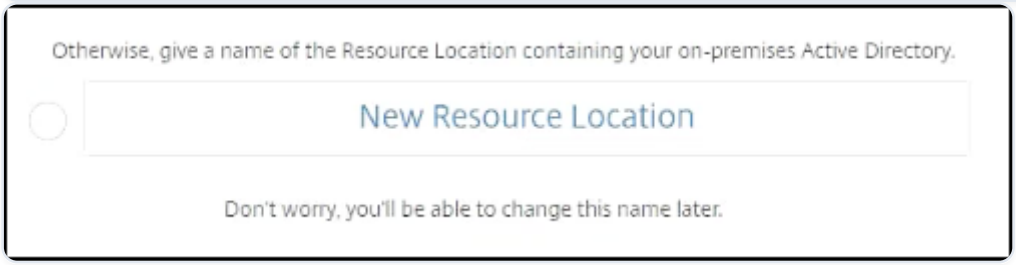
2. Introduzca un nombre de sitio único, seleccione la región de la nube más cercana a usted y, a continuación, haga clic en **Solicitar un sitio**. Recibirá un correo electrónico cuando su sitio esté listo.



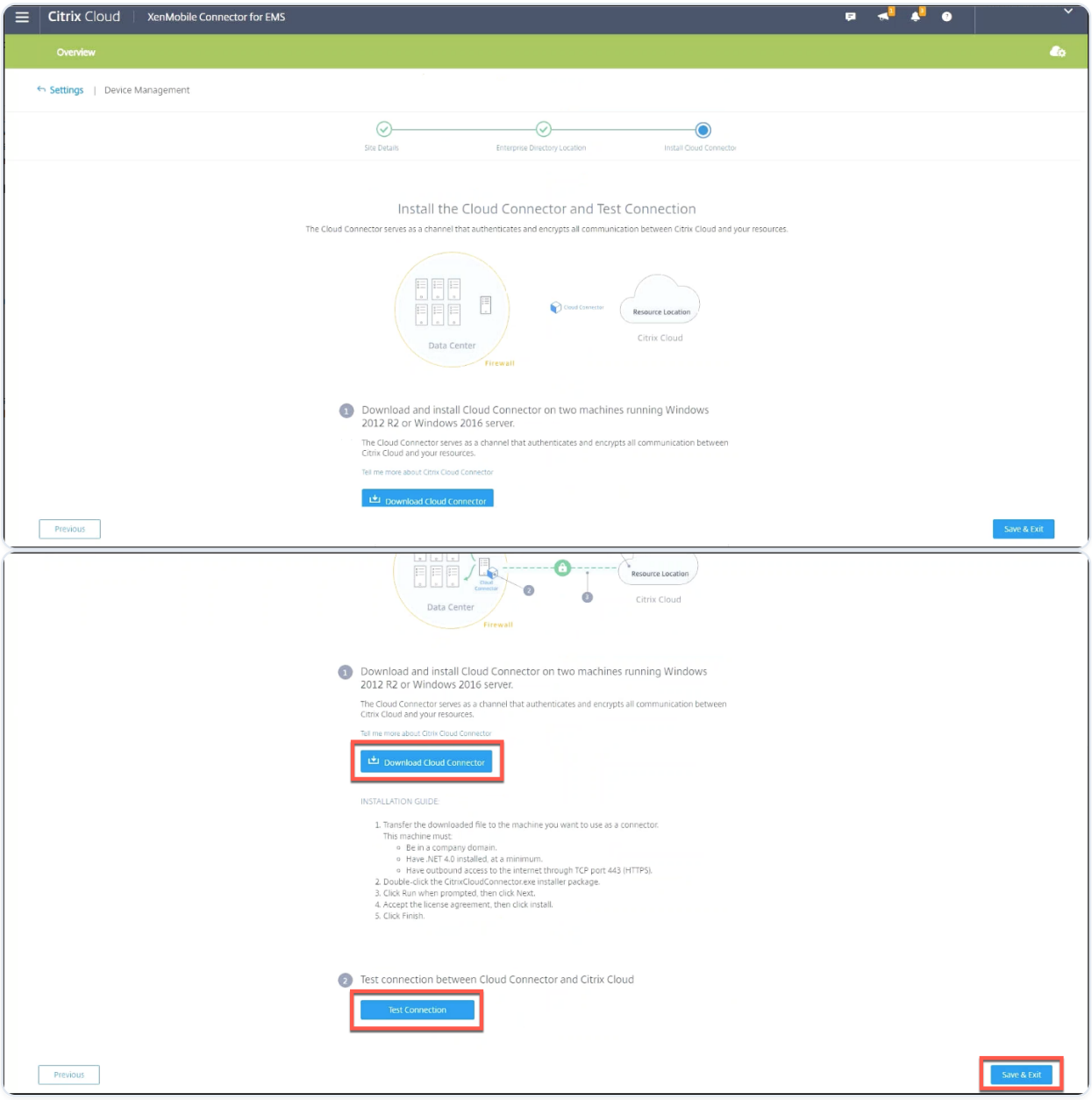


3. Haga clic en **Aceptar** para cerrar el mensaje. Seleccione una ubicación de Active Directory para asociarla a su sitio o cree una ubicación de recursos y, a continuación, haga clic en **Siguiente**.

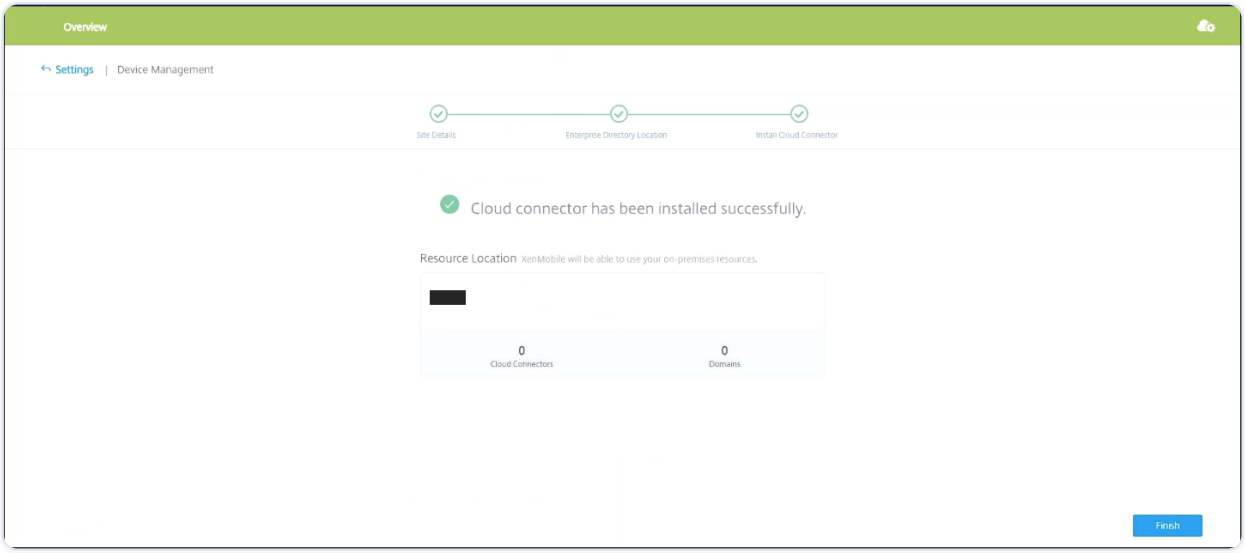




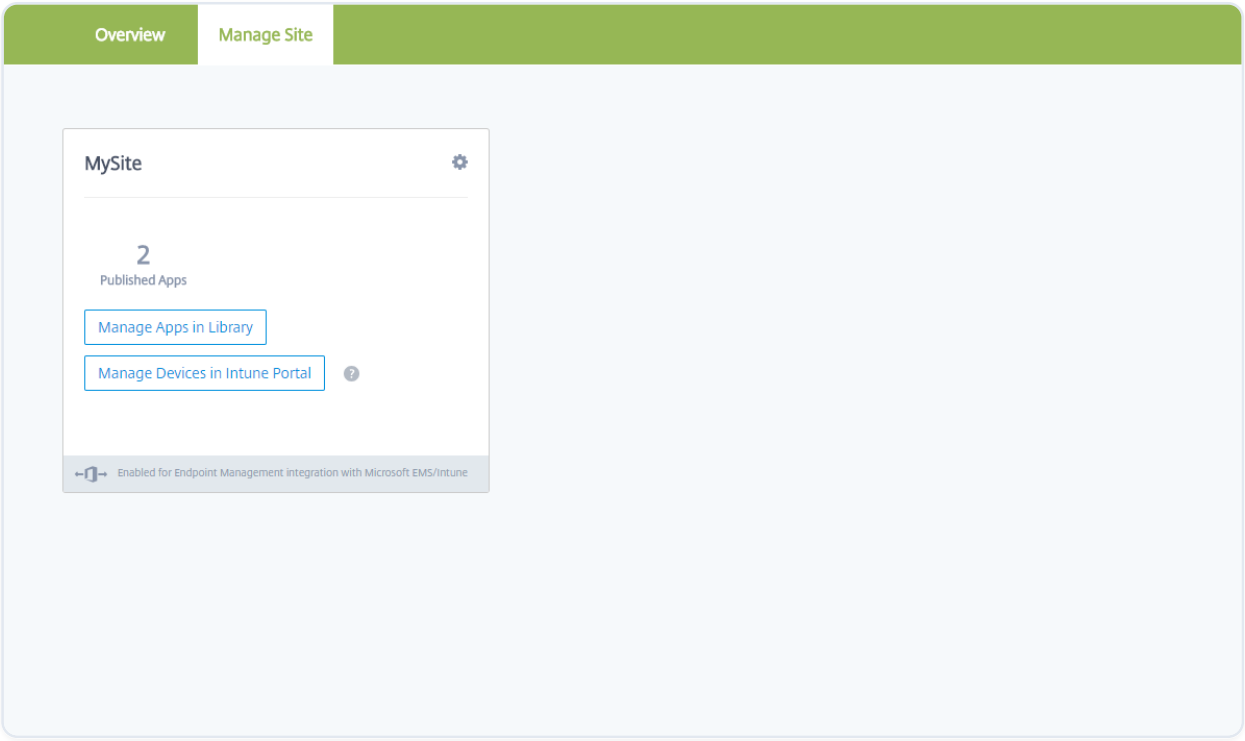
4. Haga clic en **Descargar Cloud Connector** y siga las instrucciones en pantalla para instalar el conector de la nube. Después de la instalación, haga clic en **Probar conexión** para verificar la conexión entre Citrix Cloud y Cloud Connector.



5. Haga clic en **Guardar y salir** para finalizar. Aparecerá la ubicación de sus recursos. Al hacer clic en **Finalizar**, volverá a la pantalla de configuración.



6. Ahora puede acceder a la consola de Citrix Endpoint Management desde el mosaico de su sitio. Desde aquí, puede realizar tareas de administración de MDM y asignar directivas de dispositivos. Para obtener más información sobre las directivas de dispositivos, consulte Directivas de dispositivos.



Configurar aplicaciones administradas por Intune para su entrega a los dispositivos

Nota:

A partir de April 1, 2025, la administración de aplicaciones de Microsoft Intune a través de la Biblioteca ya no estará disponible. Si necesita ayuda con los servicios pertinentes, póngase en contacto con el Soporte de Citrix para habilitar esta función.

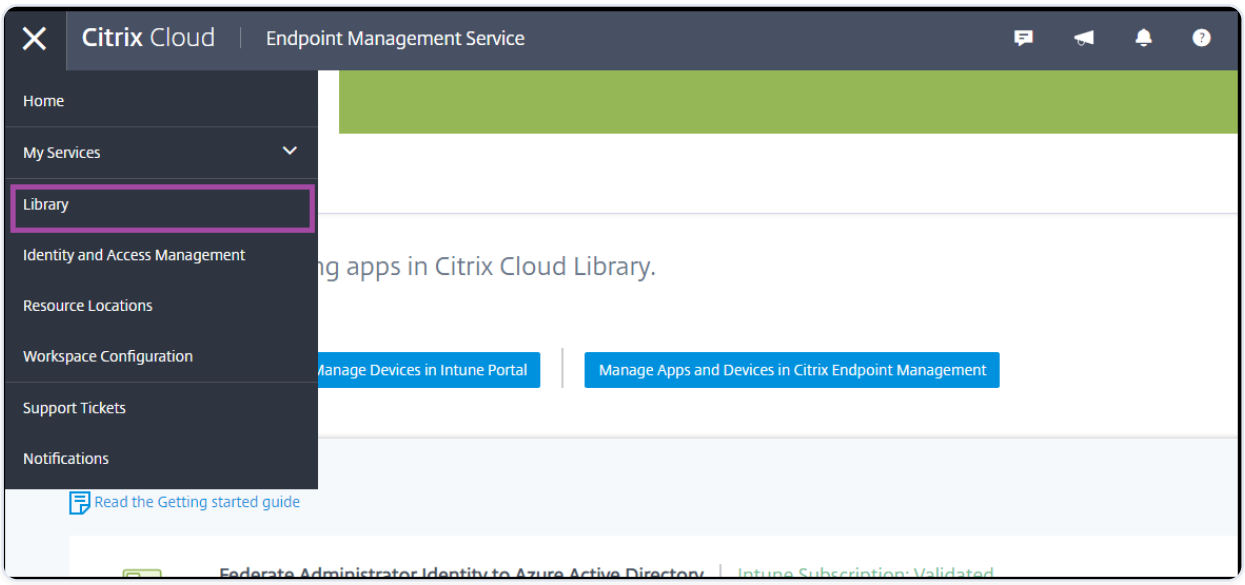
Para configurar las aplicaciones administradas por Intune para su entrega:

- Agregue las aplicaciones a la biblioteca de Citrix Cloud
- Cree directivas de dispositivos de Citrix Endpoint Management para controlar el flujo de datos
- Cree un grupo de entrega para las aplicaciones y las directivas

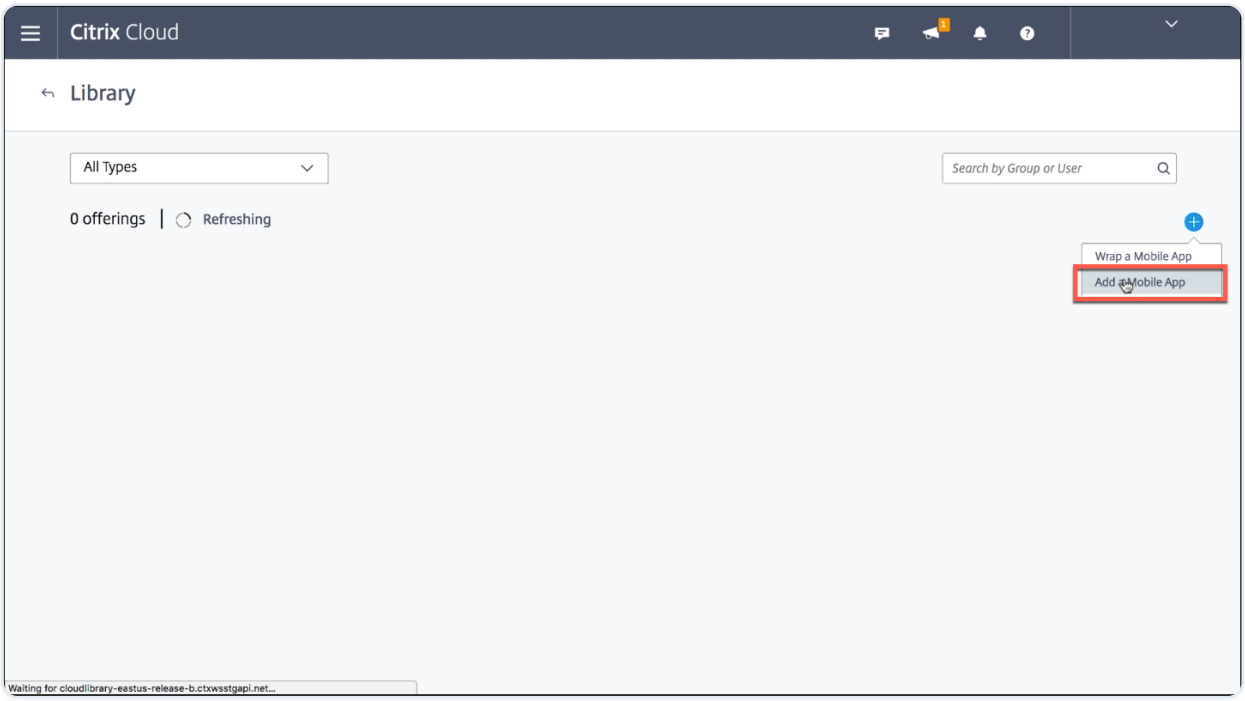
Agregar aplicaciones de Microsoft Intune a la biblioteca de Citrix Cloud

Para cada aplicación que quiera agregar:

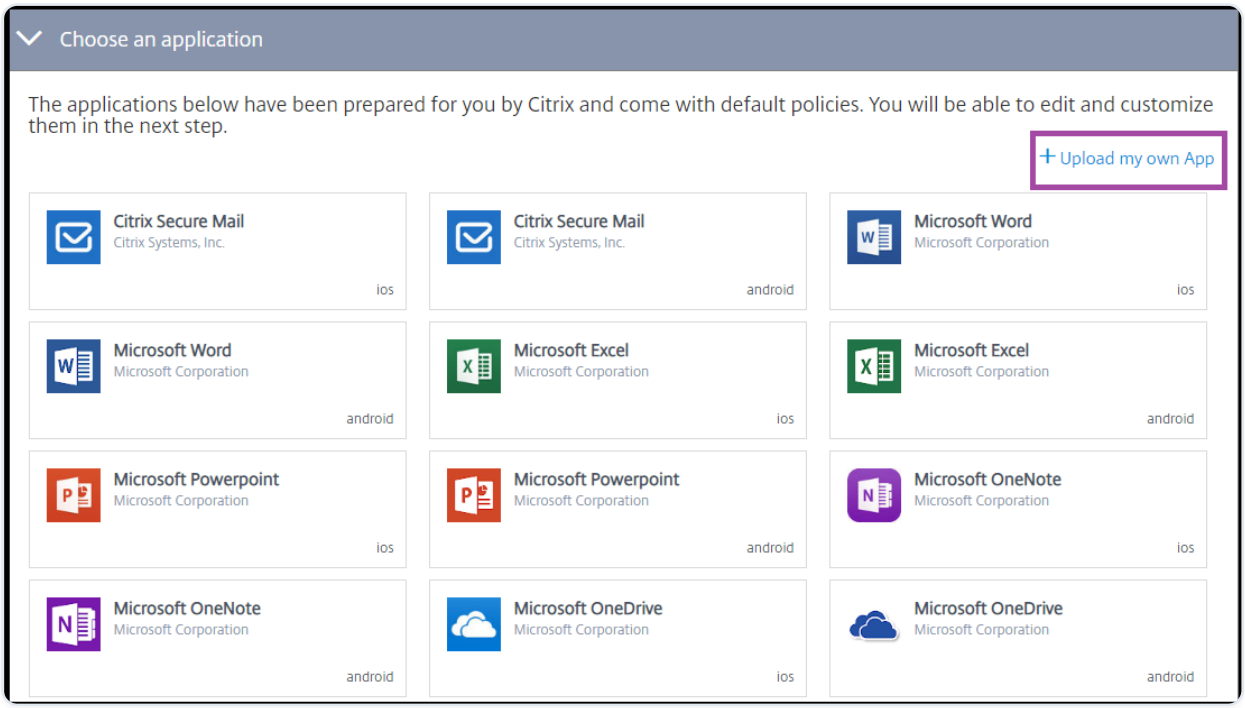
1. Desde la consola de Citrix Cloud, haga clic en el icono de menú y, a continuación, haga clic en **Biblioteca**.



2. Haga clic en el icono de signo más en la parte superior derecha y, a continuación, haga clic en **Agregar una aplicación móvil**.



3. Si tiene Android Enterprise configurado en la consola de Citrix Endpoint Management, seleccione **Microsoft Intune Apps** en **Choose an application**. Seleccione una plantilla de aplicación para personalizar o haga clic en **Upload my own App**.

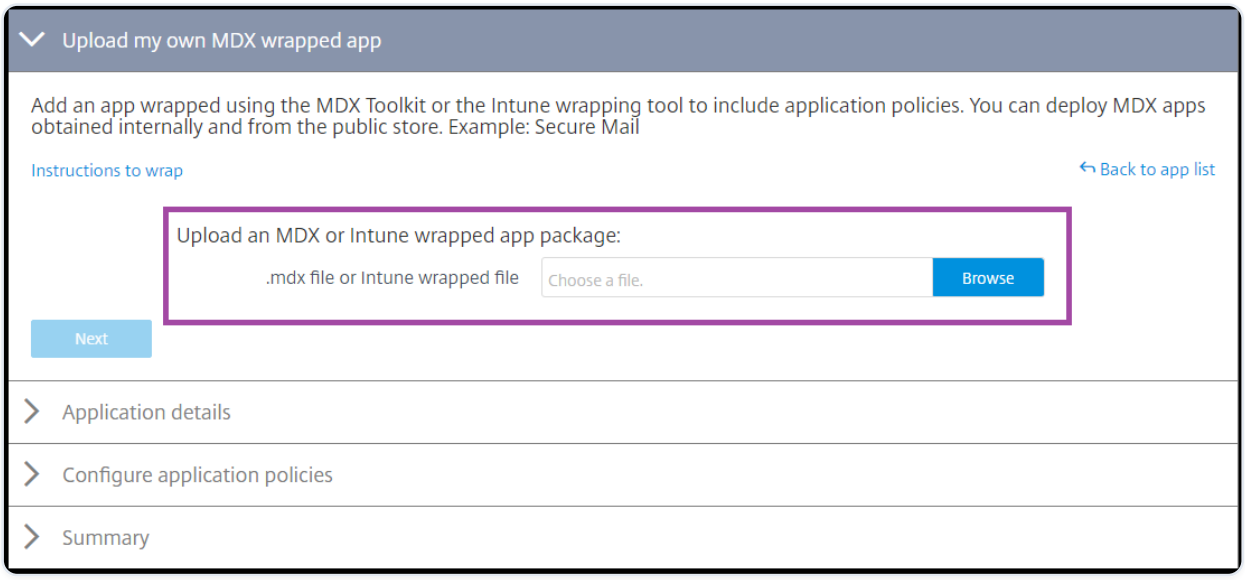


Citrix proporciona las plantillas de aplicaciones existentes, cada una de las cuales viene con un conjunto de directivas preconfiguradas de forma predeterminada. Para las aplicaciones que los clientes cargan, se aplican las siguientes directivas:

- **Archivos MDX:** Incluye aplicaciones habilitadas para MAM SDK o aplicaciones encapsuladas en MDX, como:
  - Directivas de protección de aplicaciones de Intune y las directivas MDX predeterminadas del paquete
  - Aplicaciones de la tienda pública, como las directivas de protección de aplicaciones de Intune y las directivas MDX predeterminadas que coinciden con el ID del paquete o el ID del paquete de instalación
- **Archivos IPA:** Directivas de protección de aplicaciones de Intune.
- **Archivos APK:** Directivas de protección de aplicaciones de Intune.

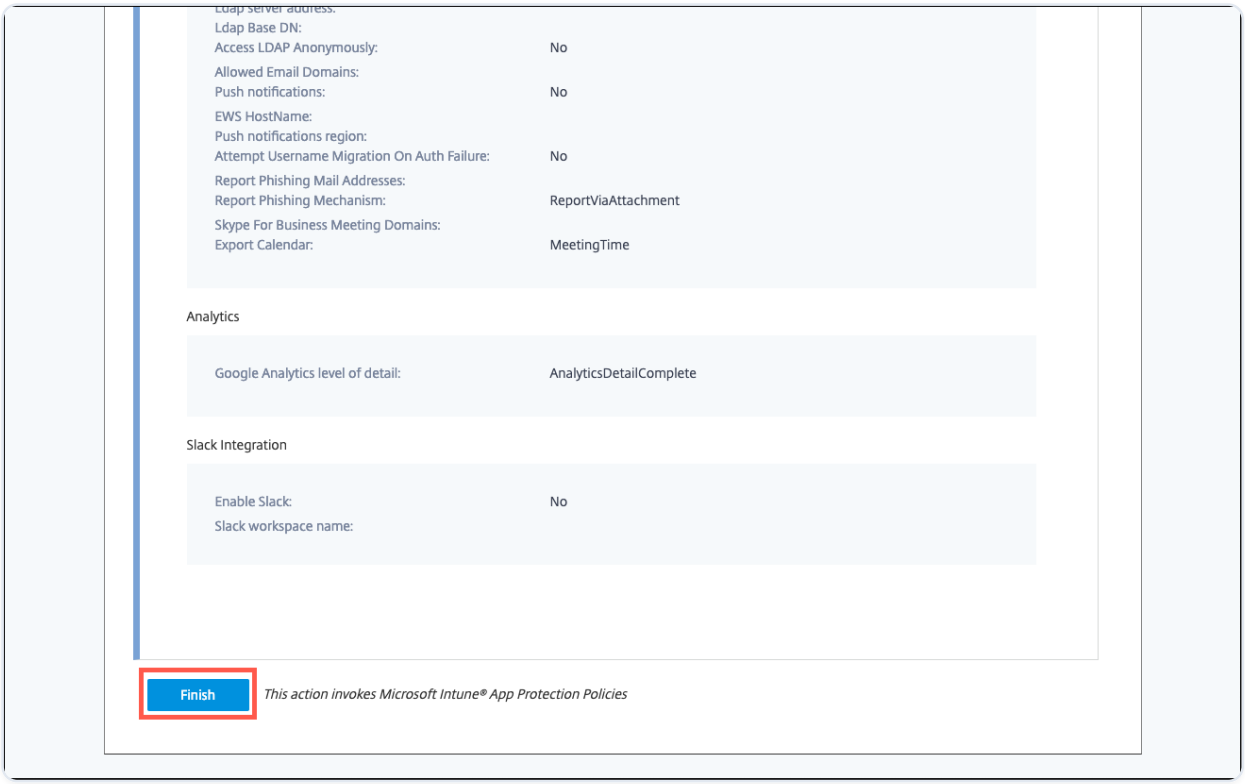
> **Nota:**
>
> Si la aplicación no está encapsulada con Intune, las directivas de protección de aplicaciones de Intune no se aplican.

4. Haga clic en **Upload my own App** y cargue su archivo .mdx o encapsulado en Intune.

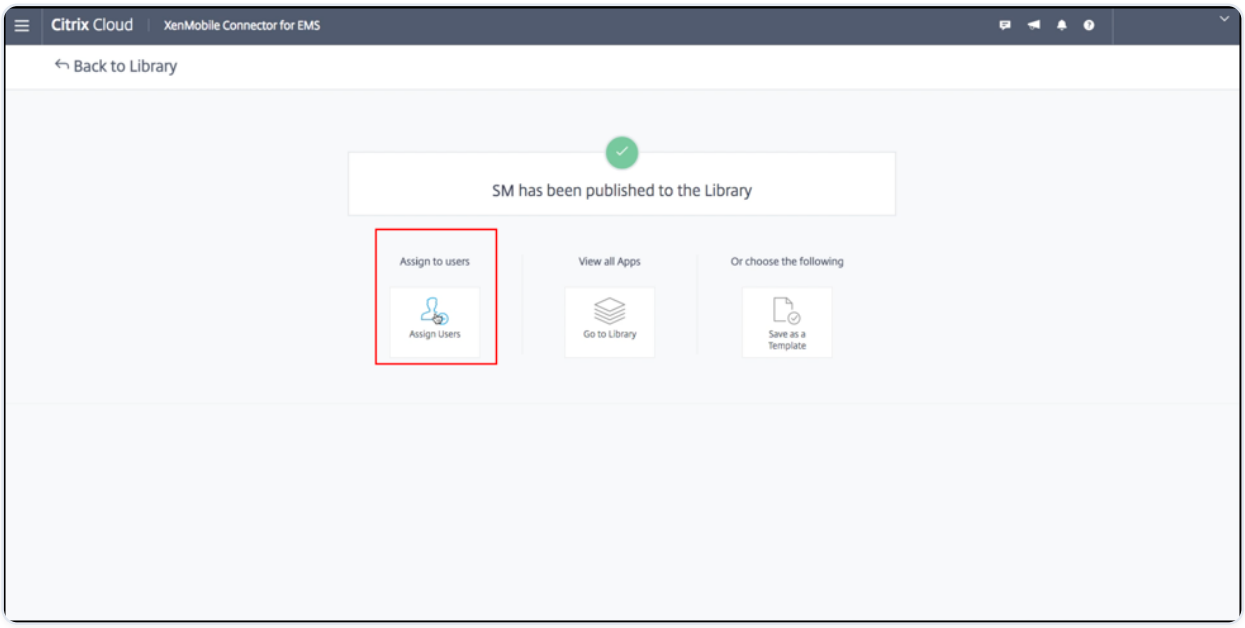


5. Introduzca un nombre y una descripción para la aplicación, elija si la aplicación es opcional u obligatoria y, a continuación, haga clic en **Next**.
6. Configure los ajustes de la aplicación. Las siguientes configuraciones permiten que los contenedores de Citrix Endpoint Management e Intune transfieran datos entre sí.
   - **Allow apps to receive data from other apps:** Seleccione **Policy managed apps**.
   - **Permitir que la aplicación transfiera datos a otras aplicaciones:** Seleccione **Todas las aplicaciones**.
   - **Restringir cortar, copiar, pegar con otras aplicaciones:** Seleccione **Aplicaciones administradas por directivas**.
7. Configure los repositorios de almacenamiento para los datos guardados. En **Seleccionar en qué servicios de almacenamiento se pueden guardar los datos corporativos**, seleccione **LocalStorage**.
8. Opcional: Configure las directivas de reubicación de datos, acceso y PIN para la aplicación. Haga clic en **Siguiente**.
9. Revise el resumen de la aplicación y, a continuación, haga clic en **Finalizar**.

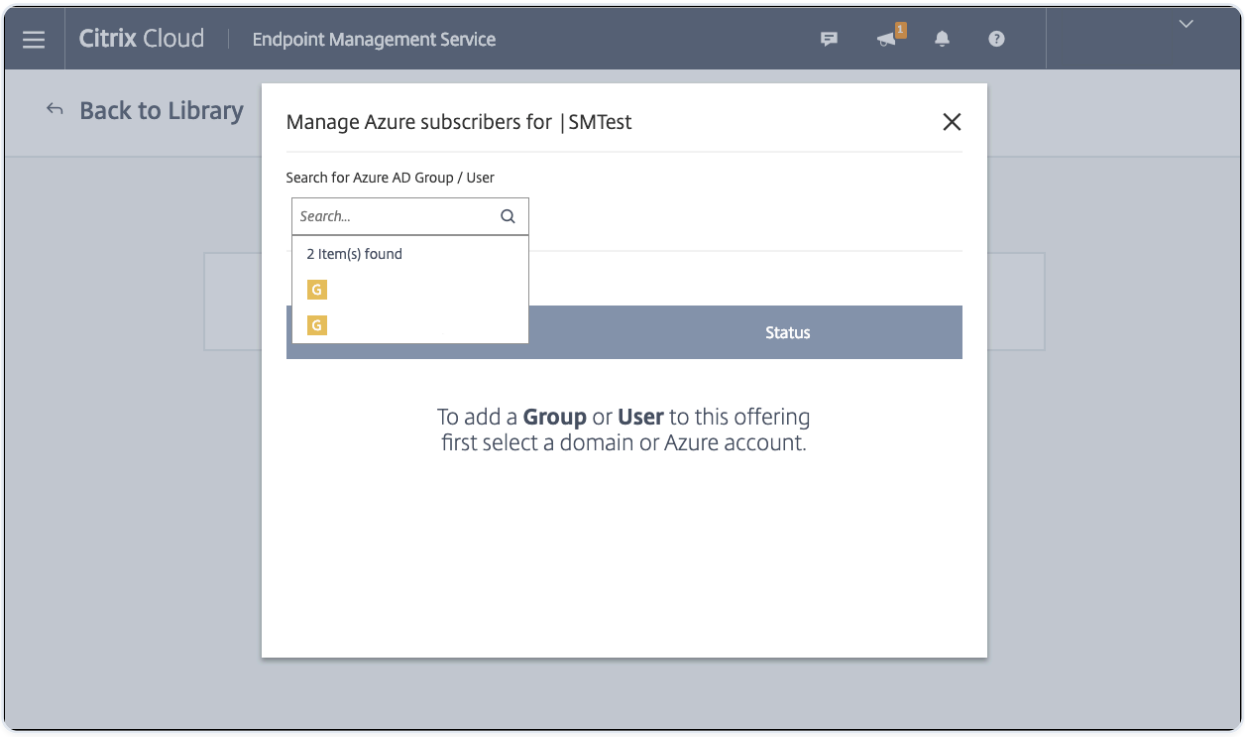
   El proceso de configuración de la aplicación puede tardar unos minutos. Cuando el proceso se complete, un mensaje indicará que la aplicación se ha publicado en la biblioteca.



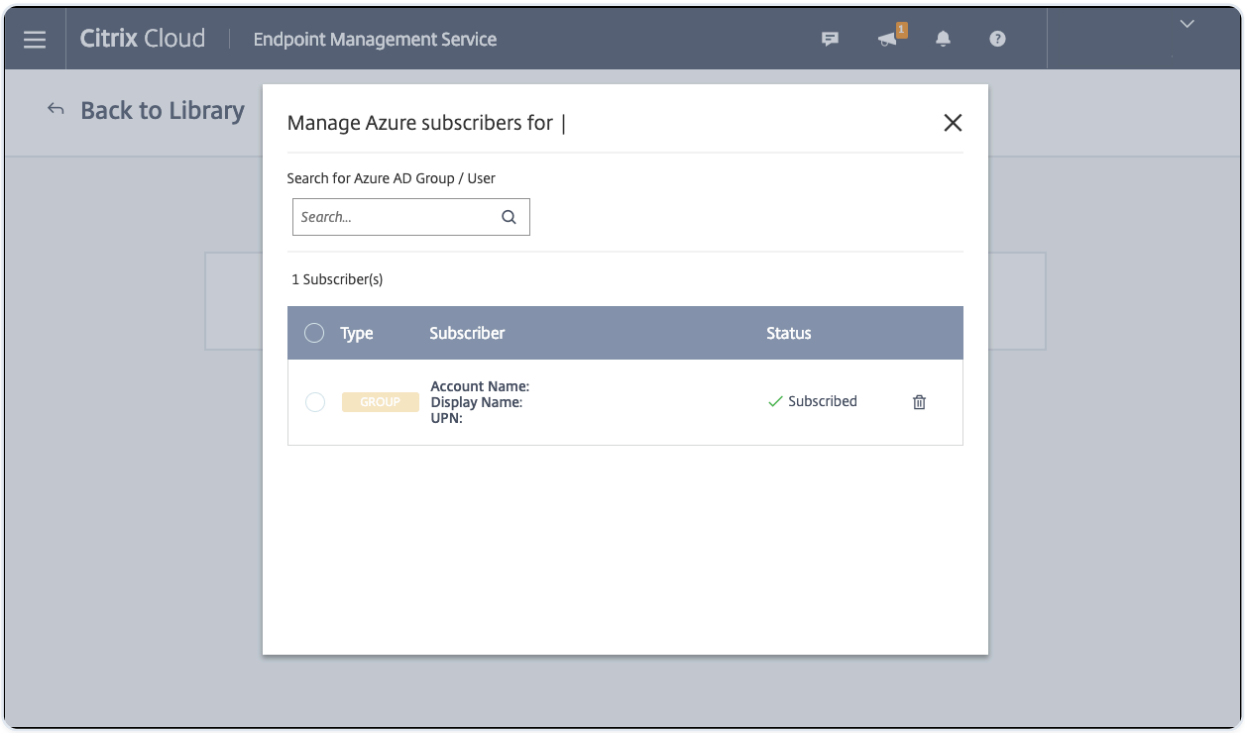
10. Para asignar grupos de usuarios a la aplicación, haga clic en **Asignar usuarios**.



11. En el cuadro de búsqueda, busque grupos de usuarios y haga clic para agregarlos. No puede agregar usuarios individuales.



12. Cuando haya agregado todos los grupos que desee, cierre la ventana haciendo clic en la X.



Es posible que vea un error al agregar grupos de usuarios. Este error se produce cuando el grupo de usuarios no se ha sincronizado con el Directorio Activo local.

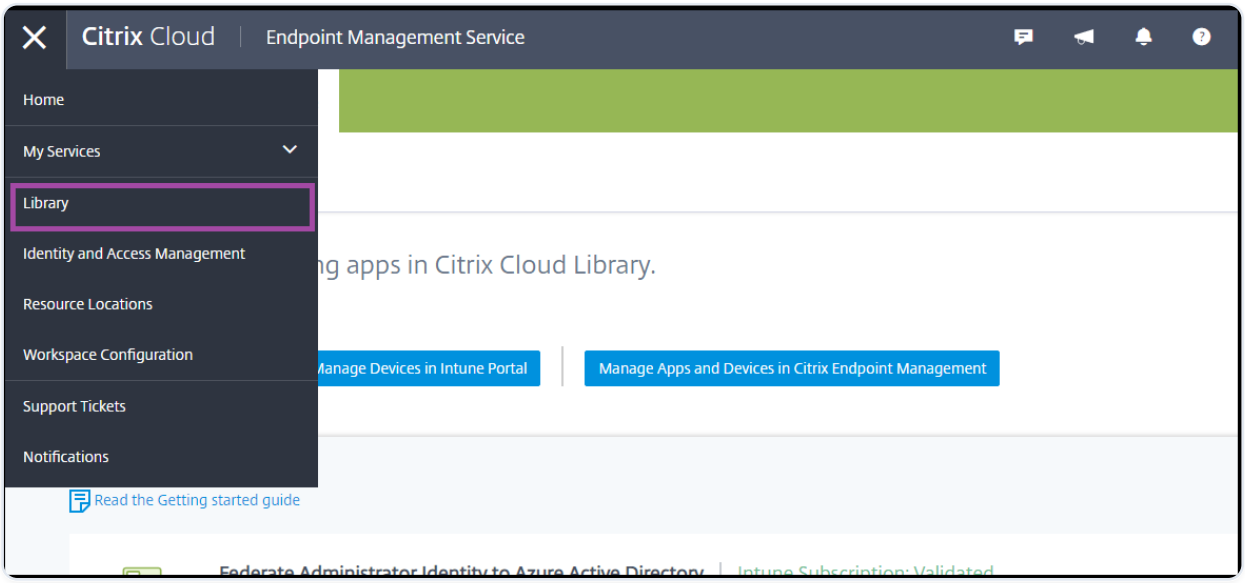
Agregar aplicaciones de Android Enterprise a la biblioteca de Citrix Cloud

Para añadir aplicaciones de Android Enterprise a la biblioteca de Citrix Cloud y establecer directivas de protección de aplicaciones de Intune, configure su entorno de nube con lo siguiente:

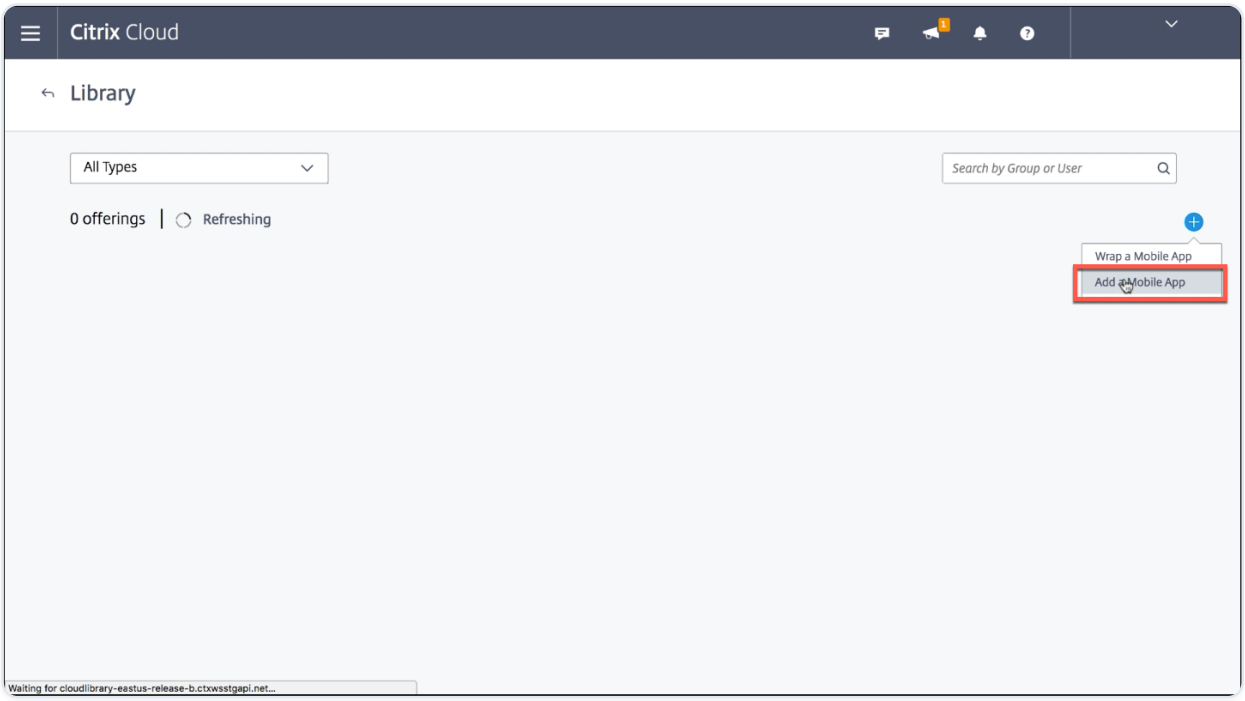
- Federar Citrix Cloud con su cuenta de Azure Active Directory (AAD). Consulte Conectar Azure Active Directory a Citrix Cloud.
- Configure LDAP y Cloud Connector en Citrix Endpoint Management.
- Configure Android Enterprise en Citrix Endpoint Management. Asegúrese de que los dispositivos Android Enterprise se inscriban en MDM+MAM. Para configurar Android Enterprise, consulte Android Enterprise.

Al seguir este procedimiento, se añaden aplicaciones de Android Enterprise a la consola de Citrix Endpoint Management y a la consola de Intune simultáneamente. Para cada aplicación de Android Enterprise que desee añadir:

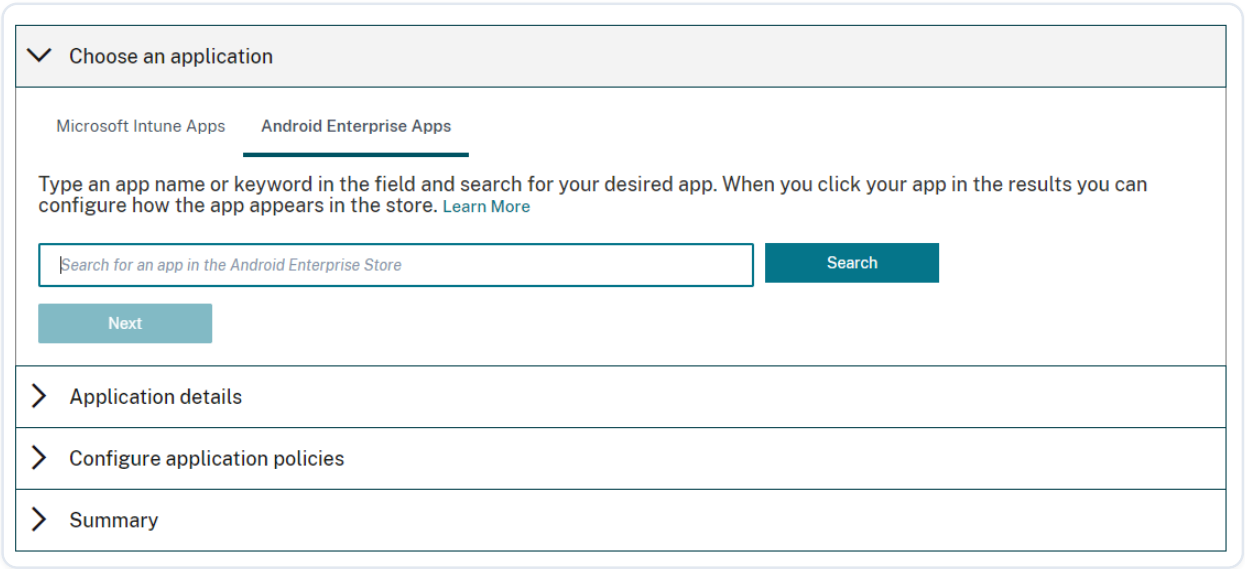
1. En la consola de Citrix Cloud, haga clic en el icono de menú y, a continuación, en **Biblioteca**.



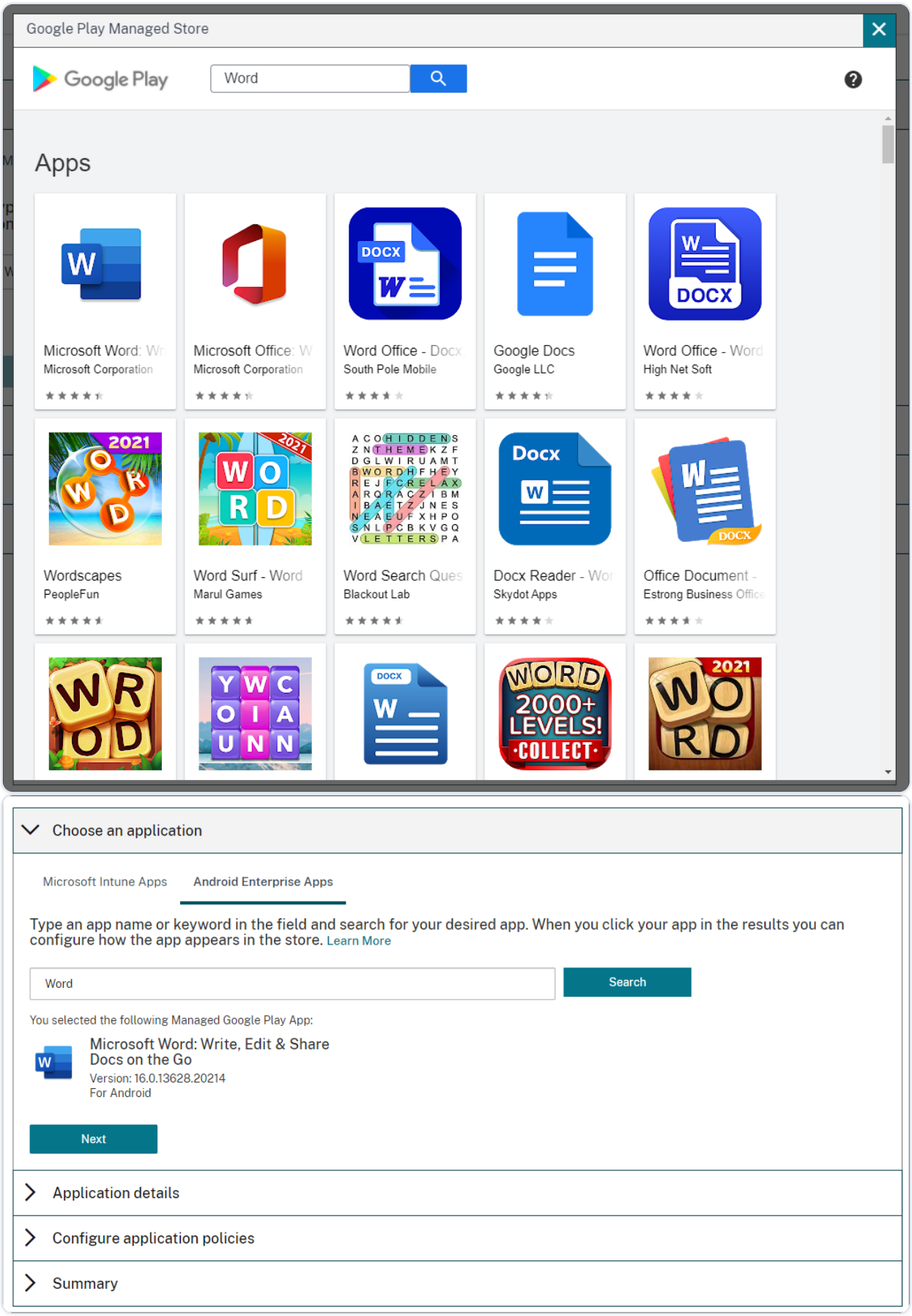
2. Haga clic en el icono de signo más en la parte superior derecha y, a continuación, en **Agregar una aplicación móvil**.



3. En **Elegir una aplicación**, seleccione **Aplicaciones de Android Enterprise**.



4. Busque una aplicación y apruébela en la ventana de Managed Google Play Store. Una vez que se cierre la ventana de Google, haga clic en **Siguiente**.



5. Añada los detalles de la aplicación y, a continuación, haga clic en **Siguiente**.

Detalles de la aplicación(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems-ae-app4.png)

6. Si buscó y seleccionó una aplicación de productividad móvil de Citrix, puede configurar las directivas de Micro VPN. Después de configurar esas directivas, haga clic en **Siguiente**.

   Directivas de Micro VPN(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems-ae-app5.png)

7. Configure las directivas de protección de aplicaciones de Intune. Haga clic en **Siguiente**.

   Directivas de Intune(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems-ae-app6.png)

8. Configure los ajustes de la aplicación. Las siguientes configuraciones permiten que los contenedores de Citrix Endpoint Management e Intune transfieran datos entre sí.

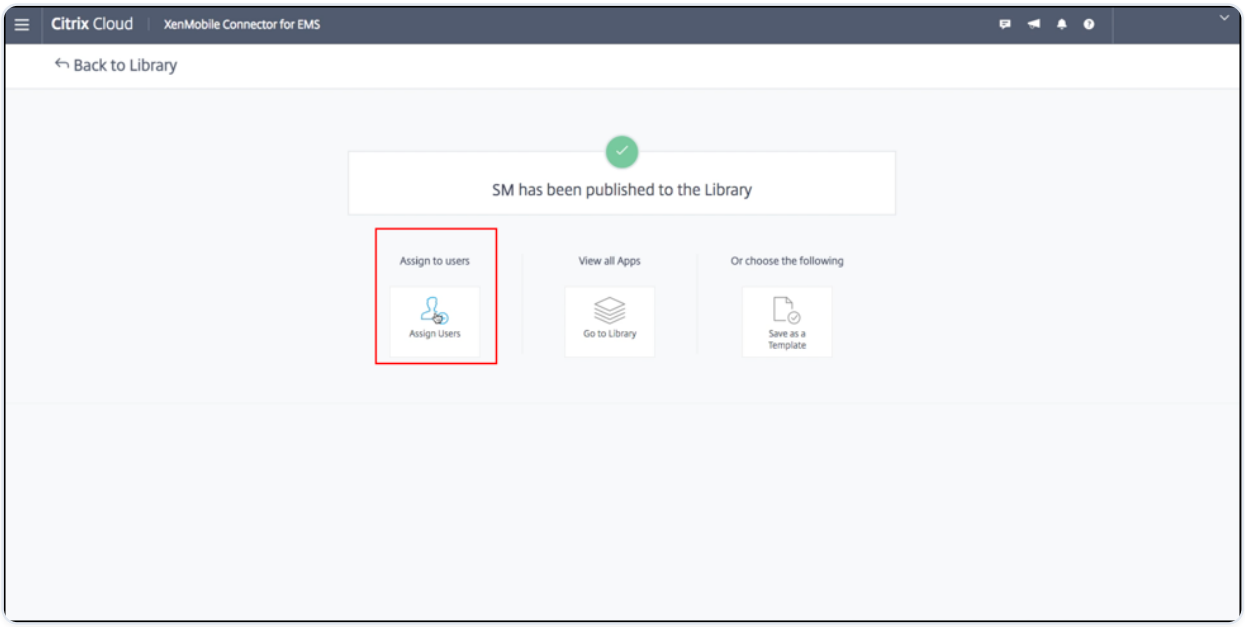
   - **Permitir que las aplicaciones reciban datos de otras aplicaciones:** Seleccione **Aplicaciones administradas por directivas**.
   - **Permitir que la aplicación transfiera datos a otras aplicaciones:** Seleccione **Todas las aplicaciones**.
   - **Restringir cortar, copiar y pegar con otras aplicaciones:** Seleccione **Aplicaciones administradas por directivas**.

9. Configure los repositorios de almacenamiento para los datos guardados. Para **Seleccionar en qué servicios de almacenamiento se pueden guardar los datos corporativos**, seleccione **LocalStorage**.
10. Opcional: Configure las directivas de reubicación de datos, acceso y PIN para la aplicación. Haga clic en **Siguiente**.
11. Revise el resumen de la aplicación y, a continuación, haga clic en **Finalizar**.

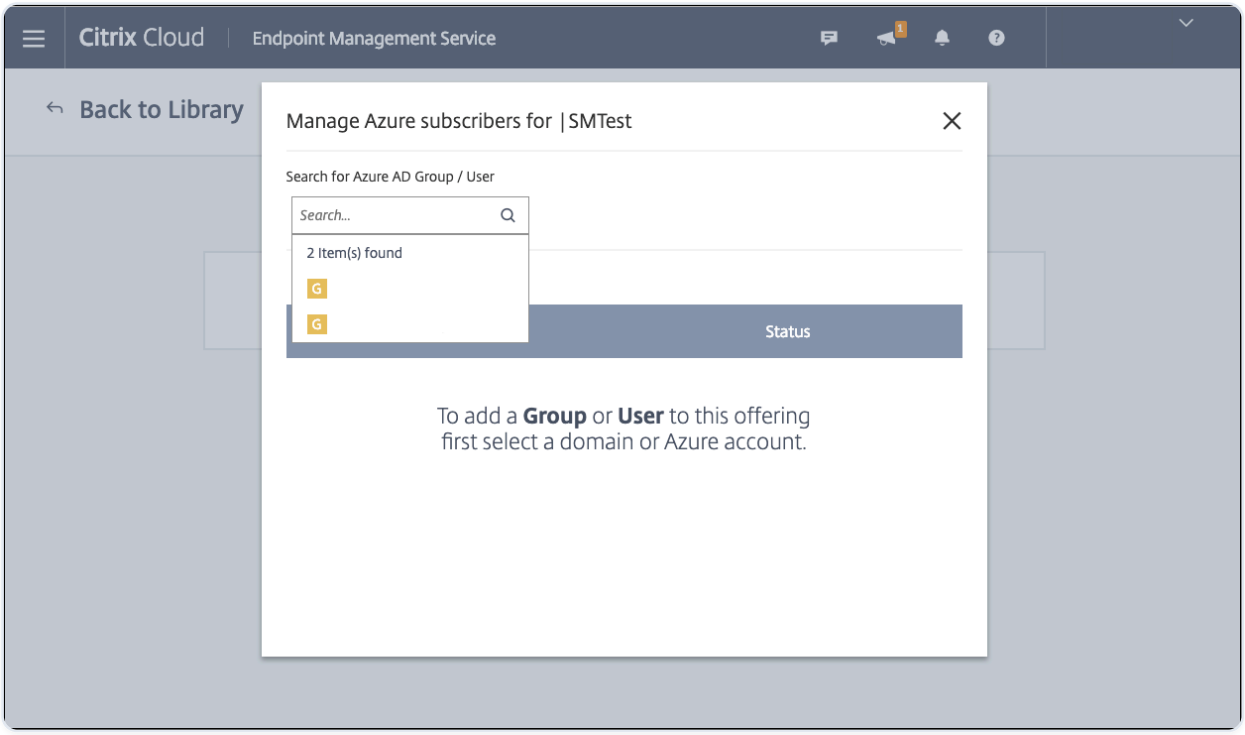
    El proceso de configuración de la aplicación puede tardar unos minutos. Cuando el proceso se complete, un mensaje indicará que la aplicación se ha publicado en la biblioteca. La aplicación está disponible en las consolas de Citrix Endpoint Management e Intune. En la consola de Citrix Endpoint Management, la aplicación forma parte de un nuevo grupo de entrega y se identifica como una aplicación de tienda de aplicaciones pública.

    Botón Finalizar(/en-us/citrix-endpoint-management/integration-with-mem/media/cem-connector-for-ems23.png)

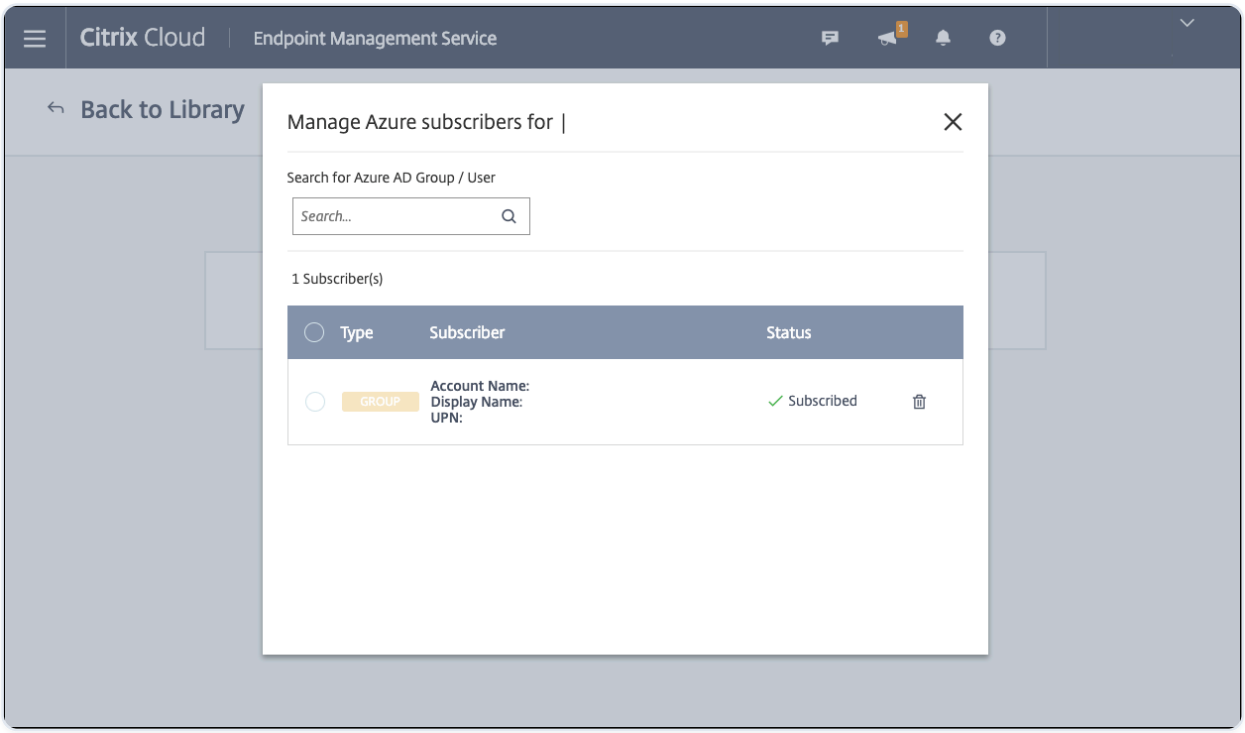
12. Para asignar grupos de usuarios a la aplicación, haga clic en **Asignar usuarios**.



13. En el cuadro de búsqueda, busque grupos de usuarios y haga clic para agregarlos. No puede agregar usuarios individuales.



14. Cuando haya agregado todos los grupos que desee, cierre la ventana haciendo clic en la X.



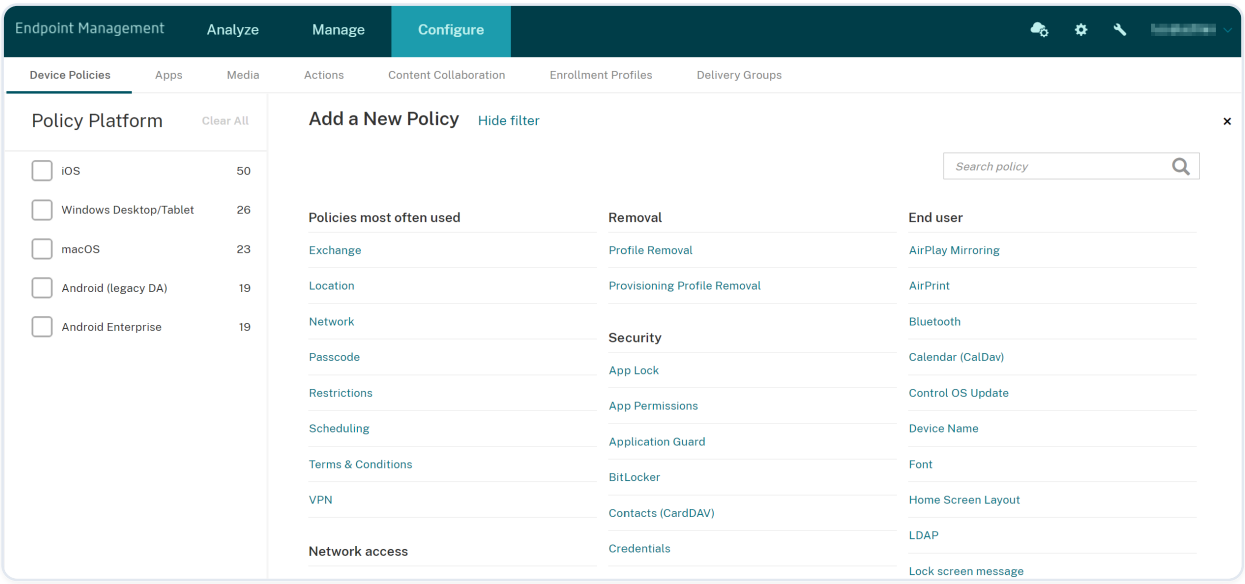
Es posible que vea un error al agregar grupos de usuarios. Este error se produce cuando el grupo de usuarios no se ha sincronizado con el Directorio Activo local.

Controlar el tipo de datos transferidos entre aplicaciones administradas

Controle el tipo de datos que se pueden transferir entre aplicaciones administradas dentro de los contenedores de Citrix Endpoint Management o Intune mediante las directivas de dispositivo de Citrix Endpoint Management. Puede configurar una directiva de restricciones para permitir solo los datos etiquetados como "corporativos". Configure una directiva de configuración de aplicaciones para etiquetar los datos.

Para configurar la directiva de dispositivo de restricciones:

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Directivas de dispositivo**.
2. En la página **Directivas de dispositivo**, haga clic en **Agregar**. Aparecerá la página **Agregar una nueva directiva**.



3. Haga clic en **Restricciones** en la lista de directivas.
4. En la página **Información de la directiva**, escriba un nombre y (opcionalmente) una descripción para la directiva. Haga clic en **Siguiente**.
5. Para crear una directiva de dispositivo para aplicaciones iOS, seleccione **iOS** en el panel **Plataformas**.
6. En **Seguridad - Permitir**, establezca **Documentos de aplicaciones administradas en aplicaciones no administradas** en **Desactivado**. Al establecer esta configuración en **Desactivado**, también se establecen **Aplicaciones no administradas leen contactos administrados** y **Aplicaciones administradas escriben contactos no administrados** en **Desactivado**. Haga clic en **Siguiente**.
7. Haga clic en **Siguiente** hasta que aparezca el botón **Guardar**. Haga clic en **Guardar**.

Configure la directiva de dispositivo de Configuración de aplicaciones para cada aplicación:

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Directivas de dispositivo**.
2. Haga clic en **Agregar**. Aparece la página **Agregar una nueva directiva**.
3. Haga clic en **Configuración de aplicaciones** en la lista de directivas.
4. En la página **Información de la directiva**, escriba un nombre y (opcionalmente) una descripción para la directiva. Haga clic en **Siguiente**.
5. Para crear una directiva de dispositivo para una aplicación iOS, seleccione **iOS** en el panel **Plataformas**.
6. Seleccione el identificador de la aplicación que se va a configurar.
7. Para las aplicaciones iOS, agregue el siguiente texto a **Contenido del diccionario**:

```
<dict>

    <key>IntuneMAMUPN</key>

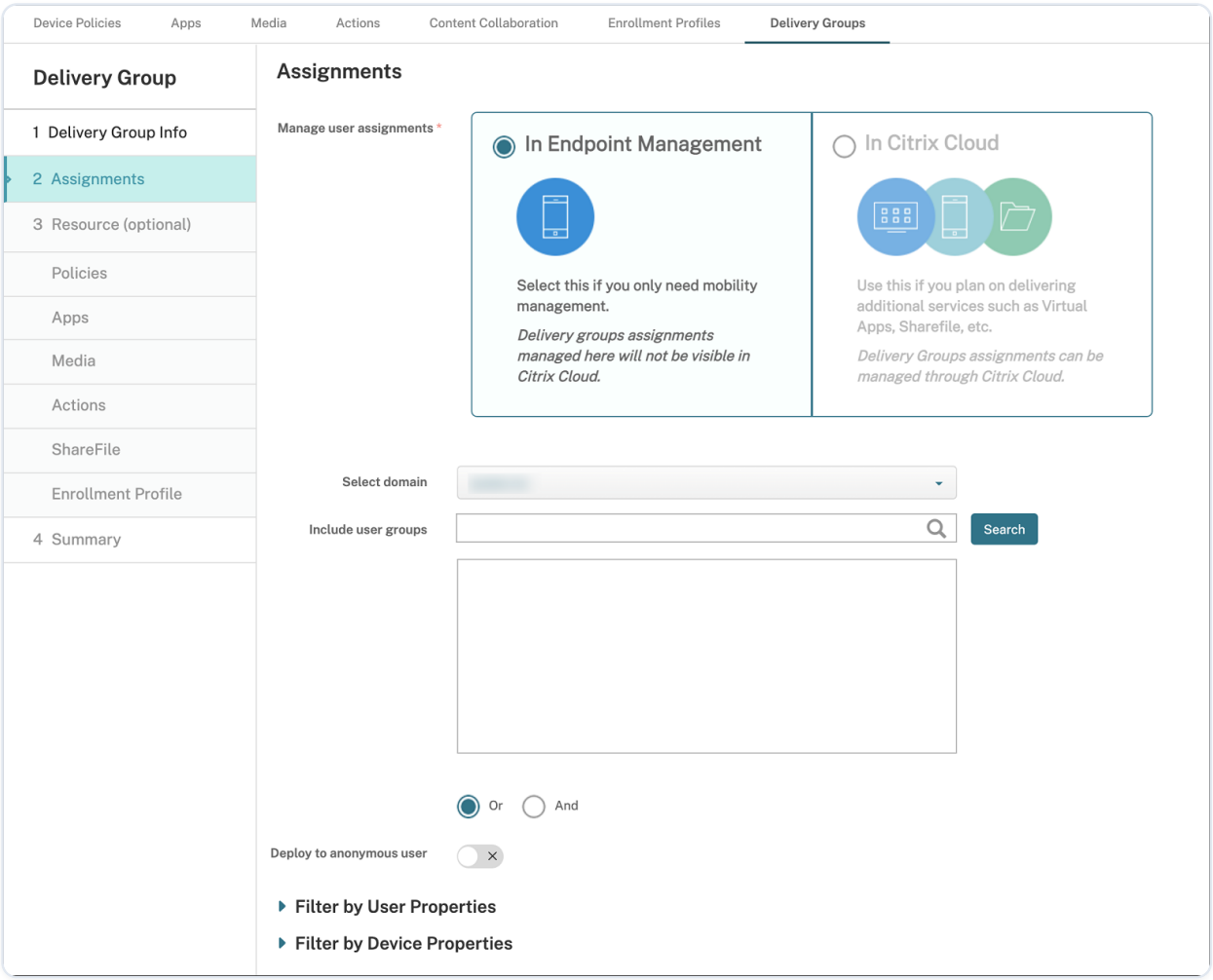
    <string>${user.userprincipalname}</string>

</dict>
```

8. Haga clic en **Comprobar diccionario**.
9. Haga clic en **Siguiente**.
10. Haga clic en **Guardar**.

Configurar grupos de entrega para las aplicaciones y las directivas de dispositivo

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Grupos de entrega**.
2. En la página **Grupos de entrega**, haga clic en **Agregar**. Aparece la página **Información del grupo de entrega**.
3. En la página **Información del grupo de entrega**, escriba un nombre y (opcionalmente) una descripción para el grupo de entrega. Haga clic en **Siguiente**.
4. En la página **Asignaciones**, especifique cómo quiere implementar el grupo de entrega: Elija **En Citrix Endpoint Management** o **En Citrix Cloud**.



5. Si eligió **En Citrix Endpoint Management**:

   - **Seleccionar dominio:** En la lista, seleccione el dominio desde el que desea elegir los usuarios.
   - **Incluir grupos de usuarios:** Realice una de las siguientes acciones:
     - En la lista de grupos de usuarios, haga clic en los grupos que quiere agregar. Los grupos seleccionados aparecen en la lista **Grupos de usuarios seleccionados**.
     - Haga clic en **Buscar** para ver una lista de todos los grupos de usuarios en el dominio seleccionado.
     - Escriba un nombre de grupo completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Buscar** para limitar la lista de grupos de usuarios.

   Para quitar un grupo de usuarios de la lista **Grupos de usuarios seleccionados**, realice una de las siguientes acciones:

     - En la lista **Grupos de usuarios seleccionados**, haga clic en la **X** junto a cada uno de los grupos que quiere quitar.

- Haga clic en **Buscar** para ver una lista de todos los grupos de usuarios en el dominio seleccionado. Desplácese por la lista y desactive la casilla de verificación de cada uno de los grupos que quiere quitar.
- Escriba un nombre de grupo completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Buscar** para limitar la lista de grupos de usuarios. Desplácese por la lista y desactive la casilla de verificación de cada uno de los grupos que quiere quitar.

6. Haga clic en **Siguiente**.
7. En la página **Directivas**, arrastre la directiva Restricciones y la directiva Configuración de aplicaciones que cree de izquierda a derecha. Haga clic en **Siguiente**.
8. En la página **Aplicaciones**, arrastre las aplicaciones que quiera entregar desde el lado izquierdo de la página a **Aplicaciones requeridas** o **Aplicaciones opcionales**. Haga clic en **Siguiente**.
9. Opcional: configure los ajustes en las páginas **Contenido multimedia**, **Acciones** e **Inscripciones**. O acepte los valores predeterminados de cada página y haga clic en **Siguiente**.
10. En la página **Resumen**, revise la configuración del grupo de entrega y haga clic en **Guardar** para crear el grupo de entrega.

Al publicar la aplicación en la consola de Intune, seleccione **Forzar la administración de las aplicaciones**. Se pedirá a los usuarios de dispositivos no supervisados que permitan la administración de la aplicación. Si los usuarios aceptan la solicitud, la aplicación se administra en el dispositivo. Si los usuarios rechazan la solicitud, la aplicación no estará disponible en el dispositivo.

Configurar Citrix Secure Mail

> **Nota:**
>
> La integración de Citrix Secure Mail con Intune está en desuso y se eliminará en una versión futura. Consulte Novedades de Secure Mail para obtener más detalles.

> Citrix Secure Mail ahora admite varias configuraciones. Puede encapsular Citrix Secure Mail en un contenedor MAM de Intune que se conecte a un servidor Exchange local. Puede conectar Citrix Secure Mail a cuentas de Exchange alojadas o de Office 365. Sin embargo,

> esta versión no admite la autenticación basada en certificados, por lo que debe usar LDAP en su lugar.

> **Importante:**

> Para usar Citrix Secure Mail en modo MDX, debe usar Citrix Endpoint Management MDM+MAM.

> Citrix Secure Mail también rellena automáticamente los nombres de usuario. Para habilitar esta función, primero debe configurar las siguientes directivas personalizadas.

1. Desde la consola de Citrix Endpoint Management, vaya a **Parámetros > Propiedades del servidor** y, a continuación, haga clic en **Agregar**.
2. En la lista, haga clic en **Clave personalizada** y, a continuación, en el campo **Clave**, escriba `xms.store.idpuser_attrs`.
3. Establezca el valor en **true** y, a continuación, en **Nombre para mostrar**, escriba `xms.store.idpuser_attrs`. Haga clic en **Guardar**.
4. Haga clic en **Propiedades del cliente** y, a continuación, en **Agregar**.
5. Seleccione **Clave personalizada** y, a continuación, escriba **SEND_LDAP_ATTRIBUTES** en el campo **Clave**.
6. Escriba `userPrincipalName=${user.userprincipalname},email=${user.mail},displayname=${user.displayname},sAMAccountName=${user.samaccountname},aadupn=${user.id_token.upn},aadtid=${user.id_token.tid}` en el campo **Valor**. Introduzca una descripción y, a continuación, haga clic en **Guardar**.

   Los siguientes pasos solo se aplican a dispositivos iOS.
7. Vaya a **Configurar > Directivas de dispositivo**, haga clic en Agregar y, a continuación, seleccione la directiva **Configuración de aplicaciones**.
8. Introduzca un nombre de directiva y, a continuación, haga clic en **Siguiente**.

   En la lista Identificador, haga clic en **Agregar nuevo**. En el cuadro de texto que aparece, introduzca el ID de paquete de su aplicación Citrix Secure Mail.
9. En el cuadro de contenido **Diccionario**, escriba el siguiente texto.

```
&lt;dict>

&lt;key>XenMobileUserAttributes&lt;/key>

&lt;dict>

&lt;key>userPrincipalName&lt;/key>

&lt;string>${user.userprincipalname}&lt;/string>

&lt;key>email&lt;/key>

&lt;string>${user.mail}&lt;/string>

&lt;key>displayname&lt;/key>

&lt;string>${user.displayname}&lt;/string>

&lt;key>sAMAccountName&lt;/key>

&lt;string>${user.samaccountname}&lt;/string>
```

```
&lt;key>aadupn&lt;/key>

&lt;string>${user.id_token.upn}&lt;/string>

&lt;key>aadtid&lt;/key>

&lt;string>${user.id_token.tid}&lt;/string>

&lt;/dict>

&lt;key>IntuneMAMUPN&lt;/key>

&lt;string>${user.id_token.upn}&lt;/string>

&lt;/dict>
```

10. Desactive la casilla **Escritorio/Tableta de Windows** y, a continuación, haga clic en **Siguiente**.
11. Seleccione los grupos de usuarios a los que quiere implementar la directiva y, a continuación, haga clic en **Guardar**.

Solución de problemas

Problemas generales

Problema: Al abrir una aplicación, aparece el siguiente mensaje de error: Se requiere directiva de aplicación.

Solución: Agregue directivas en la API de Microsoft Graph.

Problema: Tiene conflictos de directivas.

Resolución: Solo se permite una única directiva por aplicación.

Problema: Su aplicación no puede conectarse a recursos internos.

Resolución: Asegúrese de que los puertos de firewall correctos estén abiertos, de que utilice el ID de inquilino correcto, etc.

Problemas de NetScaler Gateway

La siguiente tabla enumera los problemas comunes con las configuraciones de NetScaler Gateway y sus soluciones. Para la resolución de problemas, habilite más registros y compruébelos haciendo lo siguiente:

1. En la interfaz de línea de comandos, ejecute el siguiente comando: `set audit syslogParams -logLevel ALL`
2. Compruebe los registros desde el shell mediante `tail -f /var/log/ns.log`

PROBLEMA	SOLUCIÓN
Los permisos necesarios para configurar la aplicación Gateway en Azure no están disponibles.	Compruebe si hay una licencia de Intune adecuada disponible. Intente usar el portal manage.windowsazure.com para ver si se puede agregar el permiso. Póngase en contacto con el soporte técnico de Microsoft si el problema persiste.
NetScaler Gateway no puede acceder a `login.microsoftonline.com` y `graph.windows.net`.	Desde NS Shell, compruebe si puede acceder al siguiente sitio web de Microsoft: `curl -v -k https://login.microsoftonline.com`. Luego, compruebe si DNS está configurado en NetScaler Gateway y si la configuración del firewall es correcta (en caso de que las solicitudes DNS estén bloqueadas por el firewall).
Aparece un error en ns.log después de configurar OAuthAction.	Compruebe si la licencia de Intune está habilitada y si la aplicación Azure Gateway tiene los permisos adecuados configurados.

PROBLEMA	SOLUCIÓN
El comando Sh OAuthAction no muestra el estado de OAuth como completo.	Compruebe la configuración de DNS y los permisos configurados en la aplicación Azure Gateway.
El dispositivo Android o iOS no muestra la solicitud de autenticación dual.	Compruebe si el logonSchema de ID de dispositivo de doble factor está vinculado al servidor virtual de autenticación.

Condición y estado de error de OAuth

ESTADO	CONDICIÓN DE ERROR
COMPLETO	Éxito
AADFORGRAPH	Secreto no válido, URL no resuelta, tiempo de espera de conexión agotado
MDMINFO	*manage.microsoft.com está inactivo o inaccesible
GRAPH	El punto de conexión de Graph está inactivo o inaccesible
CERTFETCH	No se puede comunicar con "Punto final de token: `https://login.microsoftonline.com`" debido a un error de DNS. Para validar esta configuración, vaya a la shell y escriba `curl https://login.microsoftonline.com`. Este comando debe validarse.

Limitaciones

Los siguientes elementos describen algunas limitaciones del uso de MEM con Citrix Endpoint Management.

- Al implementar aplicaciones con Citrix e Intune para admitir micro VPN: Cuando los usuarios proporcionan su nombre de usuario y contraseña para acceder a sitios de resumen, aunque sus credenciales sean válidas, aparece un error.

- Después de cambiar **Túnel dividido** de **Activado** a **Desactivado** y esperar a que caduque la sesión de puerta de enlace actual: El tráfico externo pasa directamente sin pasar por NetScaler Gateway hasta que el usuario inicie un sitio interno en modo VPN completa.
- Después de cambiar la política de Abrir en de solo **aplicaciones administradas** a **Todas las aplicaciones**, los usuarios no pueden abrir documentos en aplicaciones no administradas hasta que cierren y vuelvan a iniciar Citrix Secure Mail.
- Cuando el túnel dividido está **Activado** en modo VPN completa, y el DNS dividido cambia de local a remoto, los sitios internos no se cargan.

Problemas conocidos

Cuando la política de mVPN **Habilitar redirección http/https (con SSO)** está deshabilitada, Citrix Secure Mail no funciona.

Problemas conocidos de terceros

En Citrix Secure Mail para Android, cuando un usuario toca **Crear nuevo evento**, la página de creación de nuevo evento no se muestra.

Al implementar Citrix Secure Mail para iOS con Citrix e Intune para admitir micro VPN: La política de aplicación que oculta la pantalla de Citrix Secure Mail cuando los usuarios mueven la aplicación a segundo plano no se aplica.

Incorporación y configuración de recursos

Si es nuevo en Citrix, Citrix Cloud o Citrix Endpoint Management, este artículo le guiará a través del proceso de incorporación. Obtenga información sobre el flujo de trabajo y los detalles que necesita para empezar.

- **¿Por dónde empiezo?**
  - Si aún no ha comprado una suscripción a Citrix Endpoint Management, consulte Para nuevos clientes de Citrix.
  - Si tiene una suscripción a Citrix Endpoint Management, vaya a Cuando el botón Administrar esté disponible.
  - Si su sitio de Citrix Endpoint Management está aprovisionado, vaya a Configurar la autenticación.
- **¿Importa el orden de configuración?** Este artículo sigue una secuencia de configuración recomendada. Puede trabajar en un orden diferente. La consola de Citrix Endpoint Management le informará si faltan requisitos previos, a través de mensajes como "Configurar después del aprovisionamiento".
- **¿Qué hago después de la incorporación?** Una vez que complete la incorporación y la configuración de recursos descritas en este artículo, continúe su configuración en la consola de Citrix Endpoint Management. Para obtener información sobre los pasos siguientes, consulte Preparar la inscripción de dispositivos y la entrega de recursos.

Para nuevos clientes de Citrix®

Para clientes de Citrix Cloud nuevos en Citrix Endpoint Management:

Si ya ha comprado una suscripción a Citrix Endpoint Management, vaya a Cuando el botón Administrar esté disponible.

Si no ha configurado una cuenta de Citrix Cloud, consulte Registrarse en Citrix Cloud.

Si ya ha configurado una cuenta de Citrix Cloud, pero no ha comprado Citrix Endpoint Management, solicite una demostración del servicio.

1. Utilice sus credenciales de administrador de Citrix Cloud para iniciar sesión en su cuenta de Citrix Cloud. Aparecerá la página de inicio de Citrix Cloud.

   Todas las cuentas de administrador de Citrix Cloud se crean de la siguiente manera:

   - Los administradores de Citrix Cloud son administradores de Citrix Endpoint Management de forma predeterminada.
   - Los administradores de Citrix Cloud creados con acceso de cliente deben tener Citrix Endpoint Management seleccionado para poder administrar Citrix Endpoint Management.

2. En la página de inicio de Citrix Cloud, busque el mosaico del servicio Citrix Endpoint Management y haga clic en **Solicitar demostración**.
3. Rellene y envíe el formulario de solicitud de demostración. El botón del mosaico de servicios de Citrix Endpoint Management cambia a **Demostración solicitada**.

Si hace clic en el mosaico de servicios de Citrix Endpoint Management antes de que se procese su solicitud, aparecerá una pantalla que le indicará que se ponga en contacto con su representante o socio. Un representante de ventas de Citrix puede proporcionarle más información y detalles sobre el servicio.

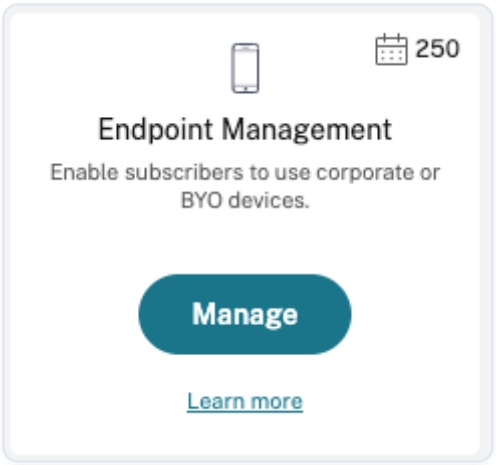
Mientras espera la prueba, asegúrese de preparar su implementación de Citrix Endpoint Management revisando los Requisitos del sistema. Aunque Citrix aloja y entrega su solución de Citrix Endpoint Management, debe gestionar algunos requisitos de comunicación y puertos.

Continúe con la siguiente sección.

Cuando el botón Administrar esté disponible

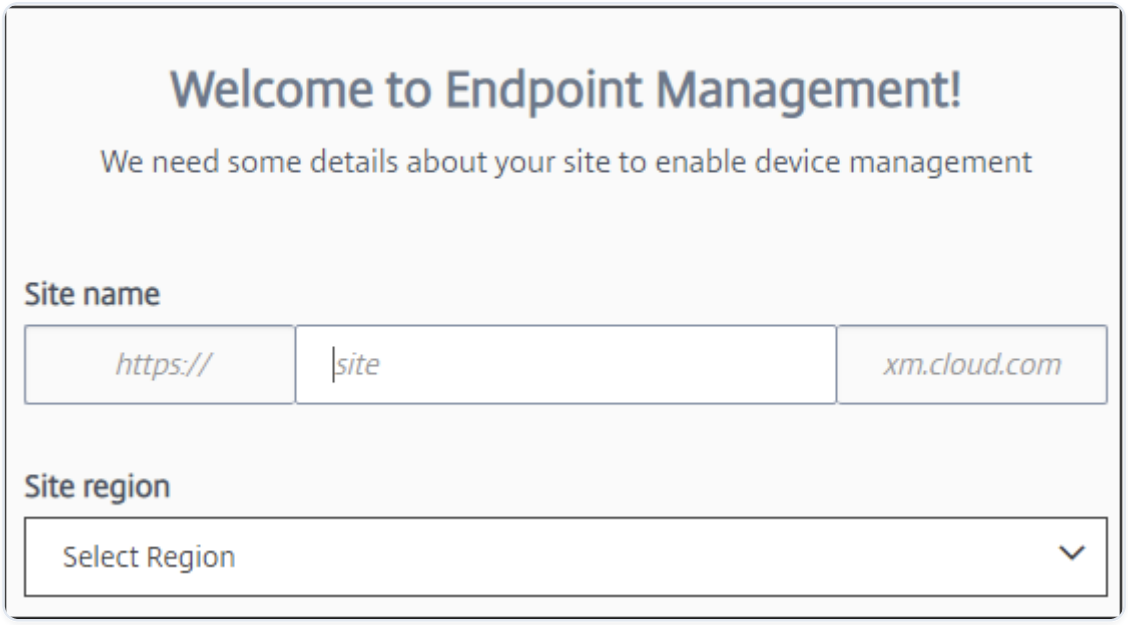
Este vídeo le guía a través de la incorporación:

<iframe src="https://www.youtube.com/embed/ycFLYxn7all" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Cuando su servicio de Citrix Endpoint Management esté disponible, el botón del mosaico de servicios de Citrix Endpoint Management cambiará a **Administrar**.



Para iniciar la configuración:

1. Inicie sesión en su cuenta de Citrix Cloud con sus credenciales de administrador de Citrix Cloud.
2. Haga clic en **Administrar** en el mosaico de Citrix Endpoint Management para acceder a la consola de Citrix Endpoint Management.
3. Escriba el nombre de su sitio y seleccione una región. Luego, seleccione **Guardar y continuar**.

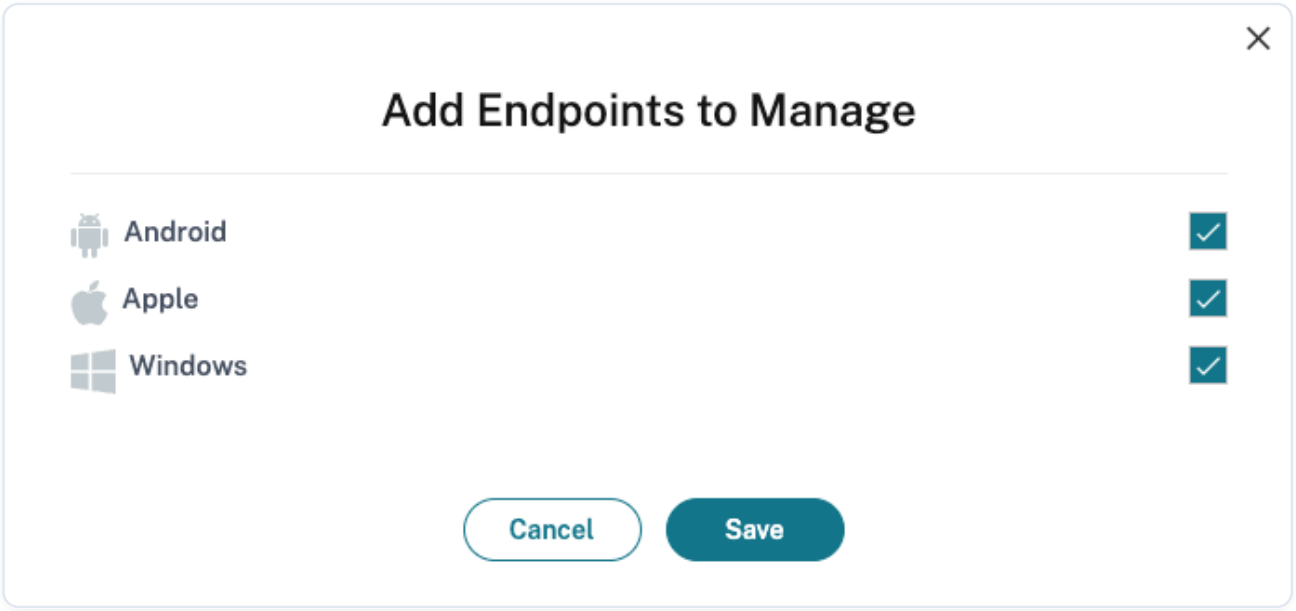


Nota:

Para solicitar las IP que se deben permitir, póngase en contacto con el representante de soporte de Citrix.

> La consola de Citrix Endpoint Management se abre con un mensaje que indica que estamos aprovisionando su suite y que algunas funciones de Citrix Endpoint Management están bloqueadas durante el aprovisionamiento.

1. En la pantalla de **Bienvenida**, haga clic en **Iniciar configuración**.
2. Seleccione los puntos finales que desea administrar y haga clic en **Guardar**. Puede agregar o borrar puntos finales en cualquier momento para mostrarlos u ocultarlos en la consola. Mostrar y ocultar puntos finales no afecta a su configuración.



Le enviaremos un correo electrónico cuando finalice el aprovisionamiento.

Centro de recursos



Haga clic en el icono del **Centro de recursos** para ver vídeos instructivos sin salir de la consola.

Durante el aprovisionamiento

Mientras aprovisionamos Citrix Endpoint Management, puede empezar con la configuración.

Configurar ubicaciones de recursos

Necesita ubicaciones de recursos antes de poder configurar las conexiones de Lightweight Directory Access Protocol (LDAP) para Citrix Endpoint Management. Las ubicaciones de recursos tienen los recursos necesarios para ofrecer servicios en la nube a sus suscriptores. Necesita una

ubicación de recursos por dominio. Para obtener ayuda, consulte el artículo de Citrix Cloud, Ubicaciones de recursos.

Mientras espera la prueba, asegúrese de preparar su implementación de Citrix Endpoint Management revisando los (/es-es/citrix-endpoint-management/system-requirements.html). Aunque Citrix aloja y entrega su solución de Citrix Endpoint Management, se requieren algunos requisitos de comunicación y puertos. Esa configuración conecta la infraestructura de Citrix Endpoint Management con los servicios corporativos, como Active Directory. La información que debe proporcionar se incluye en el (/es-es/citrix-endpoint-management/downloads/onboarding-handbook.pdf) en «Participación del ingeniero de ventas de prueba de Citrix Endpoint Management».

Una vez que esté autorizado para acceder a la prueba, el botón de **Citrix Endpoint Management** cambia a **Administrar**. Haga clic en **Administrar** para abrir la consola de Citrix Endpoint Management.

Configurar la autenticación

Una vez aprovisionado su sitio, puede continuar con la configuración. Le recomendamos que configure un proveedor de identidades (IdP) alojado en la nube o un Protocolo ligero de acceso a directorios (LDAP) para importar grupos, cuentas de usuario y propiedades relacionadas.

Para configurar IdP

Citrix Endpoint Management admite la autenticación con proveedores de identidades, como Azure Active Directory, Okta y NetScaler Gateway local.

Para configurar un IdP en Citrix Cloud y configurarlo para Citrix Endpoint Management:

- Autenticación con Azure Active Directory a través de Citrix Cloud(/es-es/citrix-endpoint-management/authentication/authentication-with-azure-active-directory-through-citrix-cloud.html)
- Autenticación con Okta a través de Citrix Cloud(/es-es/citrix-endpoint-management/authentication/authentication-with-okta-through-citrix-cloud.html)
- Autenticación con un NetScaler Gateway local a través de Citrix Cloud(/es-es/citrix-endpoint-management/authentication/authentication-with-citrix-gateway-through-citrix-cloud.html)

Para configurar LDAP

Puede configurar una conexión en Citrix Endpoint Management a uno o más directorios compatibles con LDAP para la autenticación basada en dominios. Citrix Endpoint Management admite grupos anidados en LDAP. Los grupos anidados se sincronizan diariamente a las 12 AM hora local.

Como parte de la configuración de LDAP, debe instalar al menos un Cloud Connector.

Para una descripción general rápida, vea este vídeo.

<iframe src="https://www.youtube.com/embed/LJ6IDZyfO8s" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Para configurar LDAP:

1. En la página **Configuración**, desplácese hasta el mosaico **LDAP** y, a continuación, haga clic en **Configurar**.
2. Siga las instrucciones en pantalla para descargar e instalar un Cloud Connector. Los Cloud Connectors son necesarios para habilitar la comunicación entre Citrix Cloud y sus recursos. Para obtener ayuda, consulte Citrix Cloud Connector.

Si tiene la configuración de LDAP y agrega Azure AD u Okta como proveedor de identidades, Citrix Endpoint Management sincroniza la información específica del IdP para sus grupos de Active Directory en la base de datos de Citrix Endpoint Management. Esta configuración no afecta a los grupos de entrega ni a las inscripciones de usuarios existentes. Sin embargo, no podrá agregar la configuración de LDAP en Citrix Endpoint Management posteriormente. Para obtener más información, consulte Autenticación del proveedor de identidades.

Si cambia la configuración de **Alias de dominio** o **Buscar usuario por** después de la inscripción, los usuarios deben volver a inscribirse. Para obtener más información sobre la configuración de LDAP, consulte Autenticación de dominio o de dominio más token de seguridad.

Después de configurar LDAP, puede continuar con la configuración de autenticación o configurar una plataforma específica.

Configurar NetScaler Gateway

Cuando se integra con Citrix Endpoint Management, NetScaler Gateway proporciona acceso remoto a dispositivos a su red interna y a sus recursos.

Citrix Endpoint Management requiere NetScaler Gateway para los siguientes escenarios:

- Necesita una micro VPN para acceder a los recursos de red internos para las aplicaciones de línea de negocio. Esas aplicaciones están encapsuladas con la tecnología Citrix MDX. La micro VPN necesita NetScaler Gateway para conectarse a las infraestructuras de back-end internas.
- Tiene previsto usar Citrix Endpoint Management para administrar aplicaciones (MAM o MDM+MAM). NetScaler Gateway no es necesario para administrar solo dispositivos (MDM).
- Tiene previsto integrar Citrix Endpoint Management con Microsoft Endpoint Manager. (Requiere un NetScaler Gateway local).

Para obtener una descripción general rápida, vea este vídeo.

<iframe src="https://www.youtube.com/embed/r79jdnVznE0" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
La siguiente tabla resume las funciones admitidas por las soluciones de NetScaler Gateway locales.

FUNCIONES COMPATIBLES	NETSCALER GATEWAY LOCAL
Citrix Secure Mail (STA)*	sí
En túnel - SSO web (inicio de sesión único web)	sí
VPN completa (no disponible para las aplicaciones de productividad móvil de Citrix para iOS)	sí
VPN por aplicación	sí
Inicio de sesión único móvil (control de acceso)	no
Alta disponibilidad	sí**
Implementación multi-POP	sí***
Compatibilidad con proxy	sí
Tunelización dividida	sí
DNS dividido	sí

* Configuración del servicio Citrix Cloud Secure Ticket Authority (STA)

** Configuración local

*** Configuración de equilibrio de carga de servidor global

Casos de uso de NetScaler Gateway local

Utilice uno o varios dispositivos NetScaler Gateway locales con Citrix Endpoint Management cuando:

- Necesite funciones de VPN por aplicación.
- Necesite tunelización completa, tunelización dividida, tunelización dividida inversa o DNS dividido. Recomendamos un túnel VPN completo para las conexiones que utilizan certificados de cliente o SSL de extremo a extremo a un recurso en la red interna.
- Utilice la integración de Citrix Endpoint Management con Microsoft Endpoint Manager.

El uso de NetScaler Gateway local implica una configuración y un mantenimiento significativos. Después de configurar LDAP y NetScaler Gateway en la consola de Citrix Endpoint Management, exporta un script desde esa consola. A continuación, ejecuta el script en NetScaler Gateway.

1. En la página **Configuración**, desplácese hasta el mosaico **NetScaler Gateway** y, a continuación, haga clic en **Iniciar configuración**.
2. Seleccione **NetScaler Gateway (local)** como tipo.
3. Siga las instrucciones en pantalla. Para obtener más información, consulte Configurar NetScaler Gateway local para usarlo con Citrix Endpoint Management.

Configurar el servidor de notificaciones

Para enviar notificaciones, debe configurar una puerta de enlace y un servidor de notificaciones. Un servidor de notificaciones garantiza la conectividad y la posibilidad de comunicación entre los usuarios finales y el administrador. Para configurar un servidor de notificaciones en Citrix Endpoint Management, consulte Notificaciones.

Configurar un certificado del servicio de notificaciones push de Apple (APNs) para dispositivos Apple

Citrix Endpoint Management requiere un certificado del servicio de notificaciones push de Apple (APNs) de Apple para inscribir y administrar dispositivos Apple. Citrix Endpoint Management también requiere un certificado APNs si tiene previsto usar notificaciones push para Citrix Secure

Mail para Apple. Para obtener información sobre Citrix Endpoint Management y APNs, consulte Notificaciones push para Citrix Secure Mail para iOS.

Para obtener un certificado de Apple, se requiere un ID de Apple y una cuenta de desarrollador. Para obtener más información, consulte el sitio web del Programa para desarrolladores de Apple.

Para obtener una descripción general rápida, vea este vídeo.

<iframe src="https://www.youtube.com/embed/pVj37DNBxMM" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Para configurar APNs con una solicitud de firma de certificado de Citrix:

1. En la página **Configuración**, expanda el mosaico **Apple**.
2. En el mosaico **Certificado APNs**, haga clic en **Configurar** y, a continuación, siga las instrucciones en pantalla.

Para obtener más información, consulte Certificados y autenticación.

Configurar Android Enterprise

Citrix Endpoint Management está completamente configurado después de crear grupos de entrega y asignar usuarios a esos grupos a través de Cloud Library. A partir de este momento, la administración de Citrix Endpoint Management se realiza dentro de Citrix Cloud. La interfaz combinada simplifica el cambio entre Citrix Cloud y Citrix Endpoint Management.

Puede configurar Android Enterprise para Citrix Endpoint Management con Google Play o Google Workspace.

1. **Si su organización no utiliza Google Workspace:** Puede utilizar Google Play administrado para registrar Citrix como su proveedor de EMM. Si utiliza Google Play administrado, aprovisiona cuentas de Google Play administradas para dispositivos y usuarios finales. Las cuentas de Google Play administradas proporcionan acceso a Google Play administrado, lo que permite a los usuarios instalar y utilizar las aplicaciones de trabajo que usted pone a su disposición. Si su organización utiliza un servicio de identidad de terceros, puede vincular las cuentas de Google Play administradas con sus cuentas de identidad existentes.

   Dado que este tipo de empresa no está vinculado a un dominio, puede crear más de una empresa para una sola organización. Por ejemplo, cada departamento o región dentro de una organización puede inscribirse como una empresa diferente. Esa configuración le permite utilizar diferentes empresas para administrar conjuntos separados de dispositivos y aplicaciones.

2. **Si su organización ya utiliza Google Workspace para proporcionar a los usuarios acceso a las aplicaciones de Google:** Puede utilizar Google Workspace para registrar Citrix como su EMM. Si su organización utiliza Google Workspace, tiene un ID de empresa existente y cuentas de Google existentes para los usuarios. Para utilizar Citrix Endpoint Management con Google Workspace, debe sincronizar con su directorio LDAP y recuperar la información de la cuenta de Google de Google mediante la API de directorio de Google.

   Este tipo de empresa está vinculado a un dominio existente. Por lo tanto, cada dominio solo puede crear una empresa. Para inscribir un dispositivo en Citrix Endpoint Management, cada usuario debe iniciar sesión manualmente con su cuenta de Google existente. La cuenta da a los usuarios acceso a Google Play administrado y a otros servicios de Google a través de su plan de Google Workspace.

Para una descripción general rápida, vea este vídeo.

<iframe src="https://www.youtube.com/embed/O_SpR-Eds9k" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>
Para empezar:

1. En la página **Configuración**, expanda el mosaico **Android**.
2. En el mosaico **Android Enterprise**, haga clic en **Configurar**.
3. Elija **Google Play** o **G Suite**, según cómo proporcione a los usuarios acceso a las aplicaciones de Google. Si configuró previamente la plataforma Android Enterprise con Google Play, la interfaz de usuario le llevará a Google Play Store para volver a inscribirse. Haga clic en **Volver a inscribirse**, vuelva a la consola de CEM y actualice la página.
4. Siga las instrucciones en pantalla.

Consulte:

- Crear una cuenta de Android Enterprise

Configurar Firebase Cloud Messaging

Citrix recomienda utilizar Firebase Cloud Messaging (FCM) para controlar cómo y cuándo los dispositivos Android se conectan a Citrix Endpoint Management. Citrix Endpoint Management envía notificaciones de conexión a los dispositivos Android que tienen FCM habilitado. Cualquier acción de seguridad o comando de implementación activa una notificación push para pedir al usuario que se vuelva a conectar al servidor de Citrix Endpoint Management. Consulte Firebase Cloud Messaging.

Integrar con Microsoft Endpoint Manager

La integración de Citrix Endpoint Management con Microsoft Endpoint Manager añade el valor de la micro VPN de Citrix Endpoint Management a las aplicaciones compatibles con Microsoft Intune, como el explorador Microsoft Edge.

La integración de Citrix Endpoint Management con MEM también permite a las empresas encapsular sus propias aplicaciones de línea de negocio con Intune y Citrix. La encapsulación de aplicaciones proporciona capacidades de micro VPN dentro de un contenedor de administración de aplicaciones móviles (MAM) de Intune. La micro VPN de Citrix Endpoint Management permite que sus aplicaciones accedan a los recursos locales. Puede administrar y entregar aplicaciones de Office 365, aplicaciones de línea de negocio y Citrix Secure Mail en un solo contenedor. Un único contenedor proporciona la máxima seguridad y productividad.

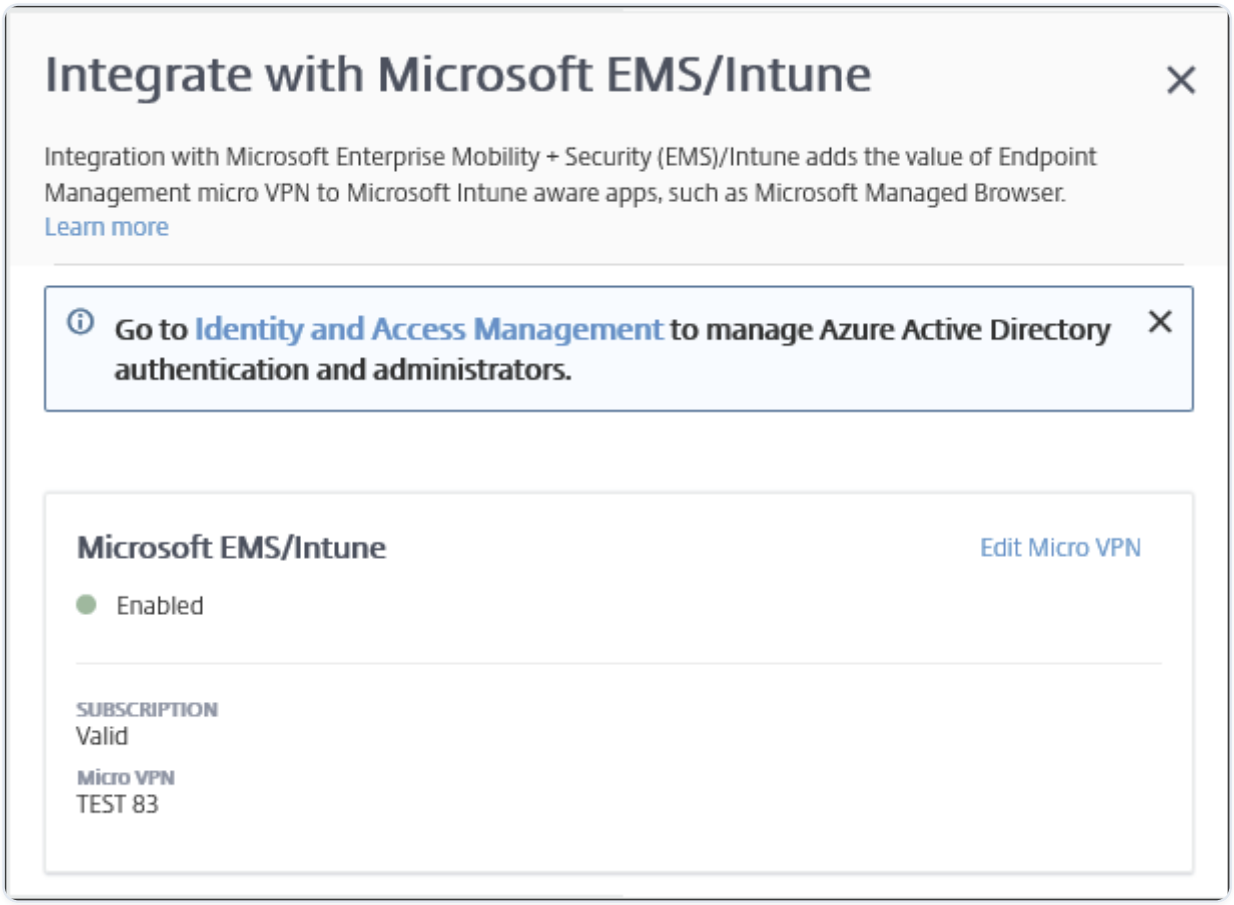
- Los administradores de Citrix Cloud son administradores de Citrix Endpoint Management de forma predeterminada.
- Los administradores de Citrix Cloud creados con acceso de cliente deben tener Citrix Endpoint Management seleccionado para poder administrar Citrix Endpoint Management.

En la consola de Citrix Endpoint Management, solo puede cambiar el rol y la pertenencia de un usuario. Para cambiar un rol en cualquier momento, acceda a la consola de Citrix Endpoint Management desde el panel de Citrix Cloud. Vaya a la ficha **Administrar** y haga clic en **Usuarios**. Seleccione un usuario específico y haga clic en **Modificar** para cambiar el rol. Para obtener más información, consulte Configurar roles con RBAC.

Para integrar con MEM, consulte Integración de Citrix Endpoint Management con Microsoft Endpoint Manager.

Después de completar la configuración en Citrix Cloud, vuelva a la consola de Citrix Endpoint Management de la siguiente manera: Vaya a la página **Inicio** de Citrix Cloud y, a continuación, haga clic en **Administrar** en el mosaico de **Citrix Endpoint Management**. A continuación, puede verificar si ha iniciado sesión en Citrix Endpoint Management con su cuenta de Azure Active Directory.

1. En la página **Parámetros**, desplácese hasta el mosaico **Integrar con Microsoft EMS/Intune**.
2. Haga clic en **Ver más**. La interfaz de usuario indica si ha habilitado la conexión correctamente.

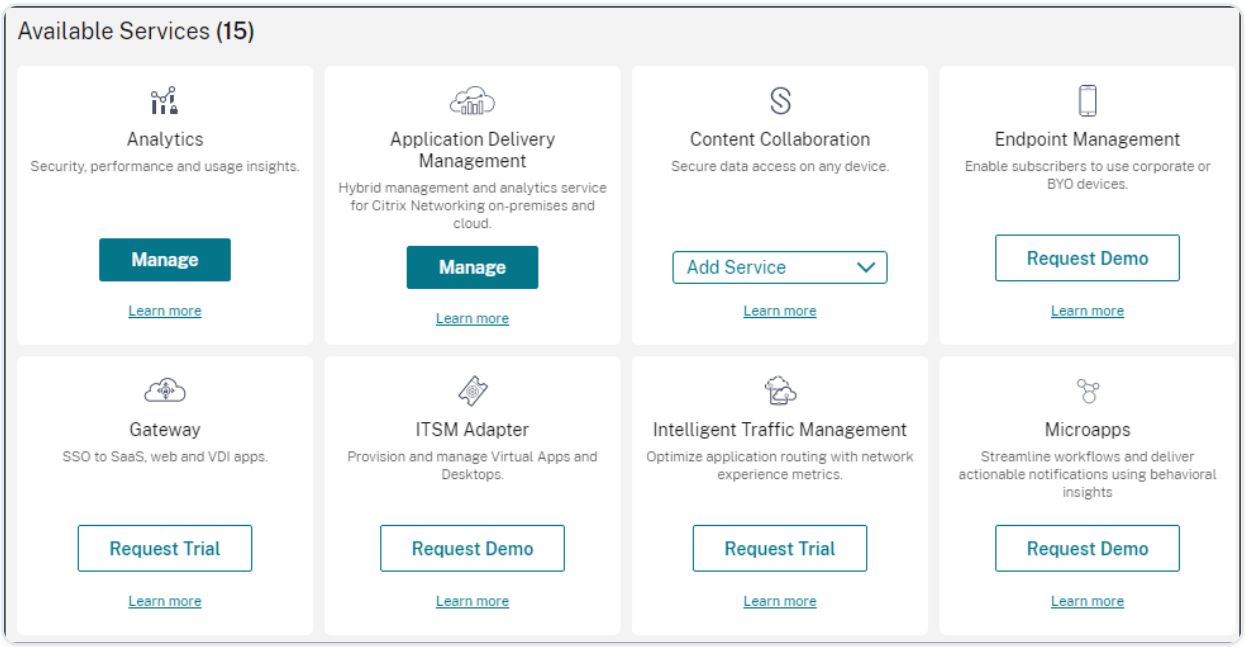


En la consola de Citrix Cloud, también puede cambiar nombres de usuario o contraseñas, y eliminar o modificar usuarios locales. Consulte Administración de identidades y accesos.

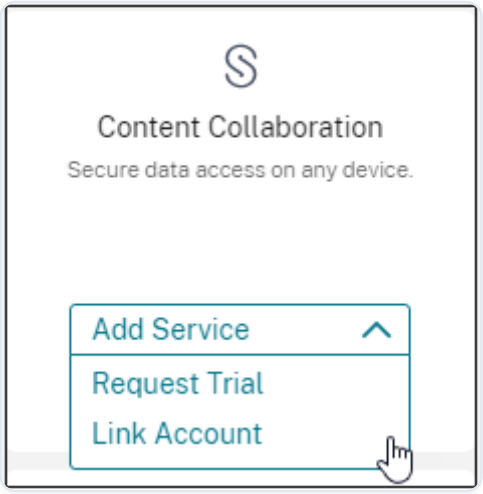
Vincular una cuenta de ShareFile existente a Citrix Cloud

Si tenía una cuenta de ShareFile antes de registrarse en Citrix Cloud, debe vincular esa cuenta a Citrix Cloud. Para vincular su cuenta, su dirección de correo electrónico debe ser un administrador de la cuenta de ShareFile. Cuando esté listo para continuar, vaya a `<https://onboarding.cloud.com>`.

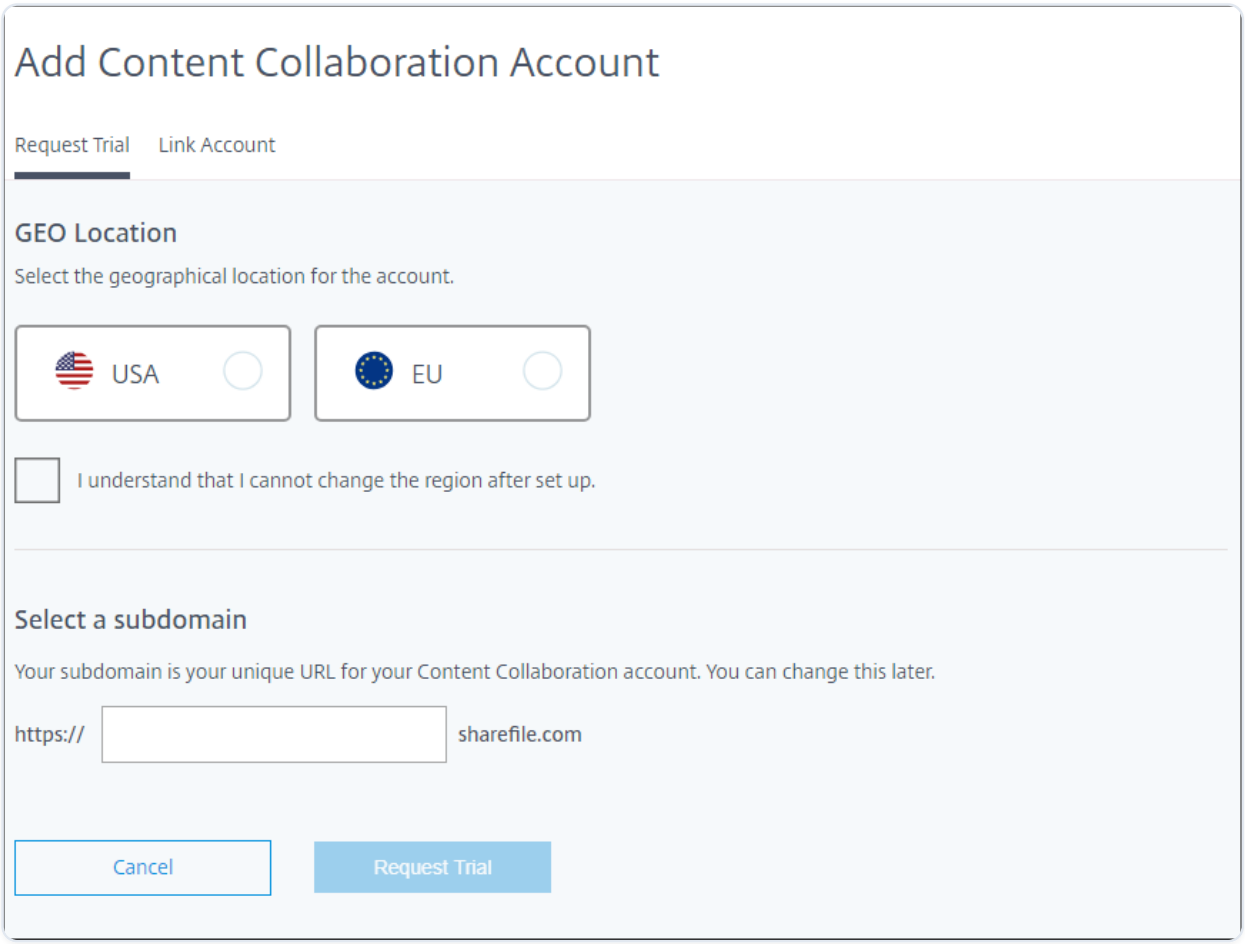
1. Después de iniciar sesión, aparece una pantalla similar a la siguiente.



2. En el mosaico de **ShareFile**, elija **Vincular cuenta**.



3. Después de confirmar su cuenta de ShareFile, aparece la siguiente página:



4. Haga clic en la ficha **Vincular cuenta** para completar el proceso. Puede administrar inmediatamente su cuenta de ShareFile desde Citrix Cloud.

Consideraciones de escala y tamaño para Cloud Connectors

Al evaluar el servicio Citrix Endpoint Management para el dimensionamiento y la escalabilidad, investigue y pruebe la configuración de los Cloud Connectors para sus requisitos específicos. Cloud Connector solo está bajo carga durante la inscripción de dispositivos. Un dimensionamiento insuficiente de las máquinas puede afectar negativamente el rendimiento del sistema.

Citrix® requiere dos Cloud Connectors por ubicación de recursos. Instale Cloud Connector en un servidor dedicado que no comparta responsabilidades con otros componentes o productos. En nuestras pruebas, los Cloud Connectors se implementaron en conjuntos de alta disponibilidad (**no están equilibrados por carga**).

Configuración de prueba

- Dos Windows Server 2019 dedicados, 2 vCPU, 4 GB de memoria
- Inscripciones de dispositivos Android e iOS en MDM+MAM, distribuidas uniformemente durante un período de 8 horas

- Citrix Endpoint Management configurado para inscribir 125 dispositivos por hora por cada 1.000 dispositivos
    - 1.000 dispositivos (125 inscripciones de dispositivos por hora)
    - 5.000 dispositivos (625 inscripciones de dispositivos por hora)
    - 10.000 dispositivos (1250 inscripciones de dispositivos por hora)
    - 20.000 dispositivos (2500 inscripciones de dispositivos por hora)

Resultados de la prueba

CLOUD CONNECTOR	1.000 DISPOSITIVOS	5.000 DISPOSITIVOS	10.000 DISPOSITIVOS	20.000 DISPOSITIVOS
CPU media	2%	2%	4%	4%
CPU máxima	8%	8%	10%	11%
Memoria media	73%	73%	75%	75%
Memoria máxima	76%	76%	76%	79%

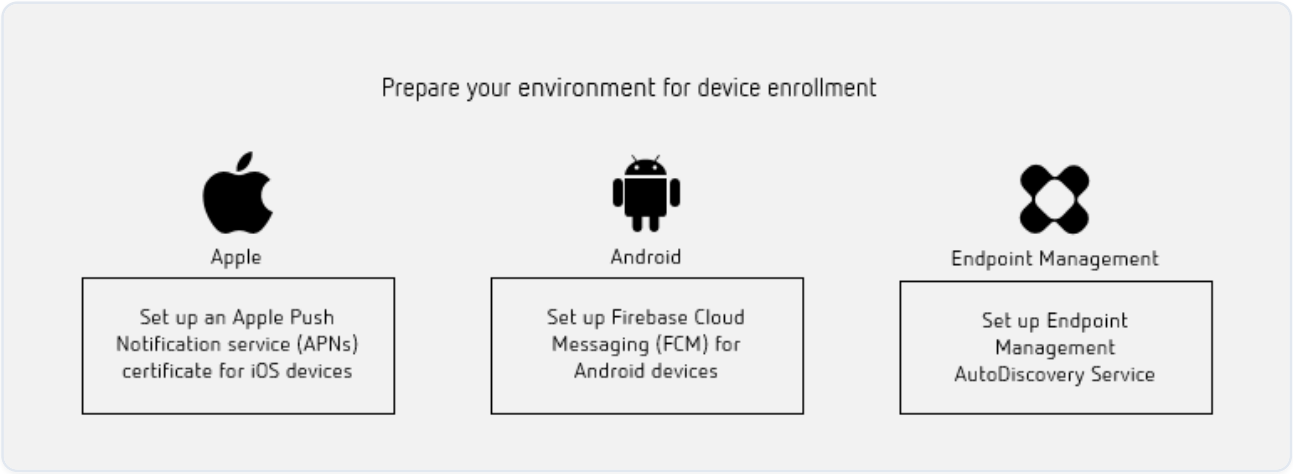
Preparar la inscripción de dispositivos y la entrega de recursos

Importante:

Antes de continuar, asegúrese de completar todas las tareas descritas en Incorporación y configuración de recursos.

Mantenga a sus usuarios informados sobre los próximos cambios. Consulte Bienvenido a su kit de adopción de usuarios de Citrix.

Citrix Endpoint Management admite varias opciones de inscripción. Este artículo cubre la configuración básica necesaria para permitir que todos los dispositivos compatibles se inscriban. El siguiente diagrama resume la configuración básica.



Para obtener una lista de los dispositivos compatibles, consulte Sistemas operativos de dispositivos compatibles.

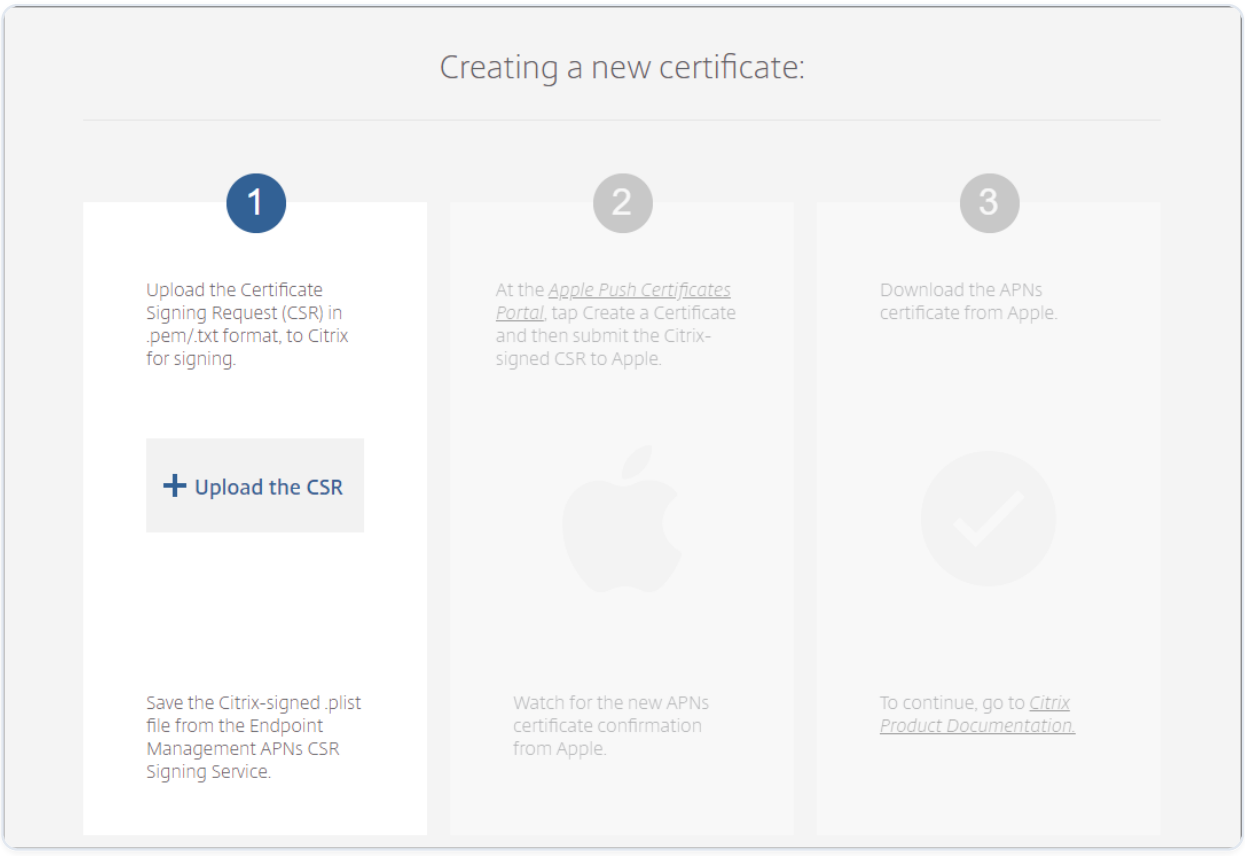
Configurar un certificado del servicio de notificaciones push de Apple (APNs) para dispositivos iOS

Importante:

El soporte de Apple para el protocolo binario heredado de APNs finaliza el March 31, 2021. Apple recomienda que utilice la API de proveedor de APNs basada en HTTP/2 en su lugar. A partir de la versión 20.1.0, Citrix Endpoint Management es compatible con la API basada en HTTP/2. Para obtener más información, consulte la actualización de noticias, "Actualización del servicio de notificaciones push de Apple" en `<https://developer.apple.com/>`. Para obtener ayuda con la comprobación de la conectividad a APNs, consulte Comprobaciones de conectividad.

Citrix Endpoint Management requiere un certificado del servicio de notificaciones push de Apple (APNs) de Apple para inscribir y administrar dispositivos iOS. Citrix Endpoint Management también requiere un certificado APNs para las notificaciones push de Citrix Secure Mail para iOS.

- Para obtener un certificado de Apple, se requiere un ID de Apple y una cuenta de desarrollador. Para obtener más información, consulte el sitio web del Programa para desarrolladores de Apple.
- Para obtener un certificado APNs e importarlo en Citrix Endpoint Management, consulte Certificados APNs.



- Para obtener más información sobre Citrix Endpoint Management y APNs, consulte Notificaciones push para Citrix Secure Mail para iOS.

Configurar Firebase Cloud Messaging (FCM) para dispositivos Android

Firebase Cloud Messaging (FCM) controla cómo y cuándo los dispositivos Android se conectan al servicio de Citrix Endpoint Management. Cualquier acción de seguridad o comando de implementación activa una notificación push. La notificación solicita a los usuarios que se vuelvan a conectar a Citrix Endpoint Management.

- La configuración de FCM requiere que configure su cuenta de Google. Para crear credenciales de Google Play, consulte Administrar la información de su cuenta de desarrollador. También utiliza Google Play para añadir, comprar y aprobar aplicaciones para su implementación en el espacio de trabajo de Android Enterprise en un dispositivo. Puede usar Google Play para implementar sus aplicaciones privadas de Android, aplicaciones públicas y aplicaciones de terceros.
- Para configurar FCM, consulte Firebase Cloud Messaging.

Configurar el servicio AutoDiscovery de Citrix Endpoint Management

El servicio AutoDiscovery simplifica el proceso de inscripción para los usuarios a través del descubrimiento de URL basado en correo electrónico. El servicio AutoDiscovery también ofrece funciones como la verificación de la inscripción, el anclaje de certificados (certificate pinning) y otros beneficios para los clientes de Citrix Workspace. El servicio, alojado en Citrix Cloud, es una parte importante de muchas implementaciones de Citrix Endpoint Management.

Con el servicio AutoDiscovery, los usuarios:

- Pueden usar sus credenciales de red corporativa para inscribir sus dispositivos.
- No necesitan introducir detalles sobre la dirección del servidor de Citrix Endpoint Management.
- Introducen su nombre de usuario en formato de nombre principal de usuario (UPN). Por ejemplo, `user@mycompany.com`.

Recomendamos que utilice el servicio AutoDiscovery para entornos de alta seguridad. El servicio AutoDiscovery admite el anclaje de certificados de clave pública (public key certificate pinning), lo que evita ataques de intermediario (man-in-the-middle). El anclaje de certificados garantiza que el certificado firmado por su empresa se utilice cuando los clientes de Citrix se comunican con Citrix

Endpoint Management. Para configurar el anclaje de certificados para sus sitios de Citrix Endpoint Management, póngase en contacto con el Soporte de Citrix. Para obtener información sobre el anclaje de certificados, consulte Anclaje de certificados.

Para acceder al servicio AutoDiscovery, vaya a `<https://adsui.cloud.com>` (comercial).

Requisitos previos

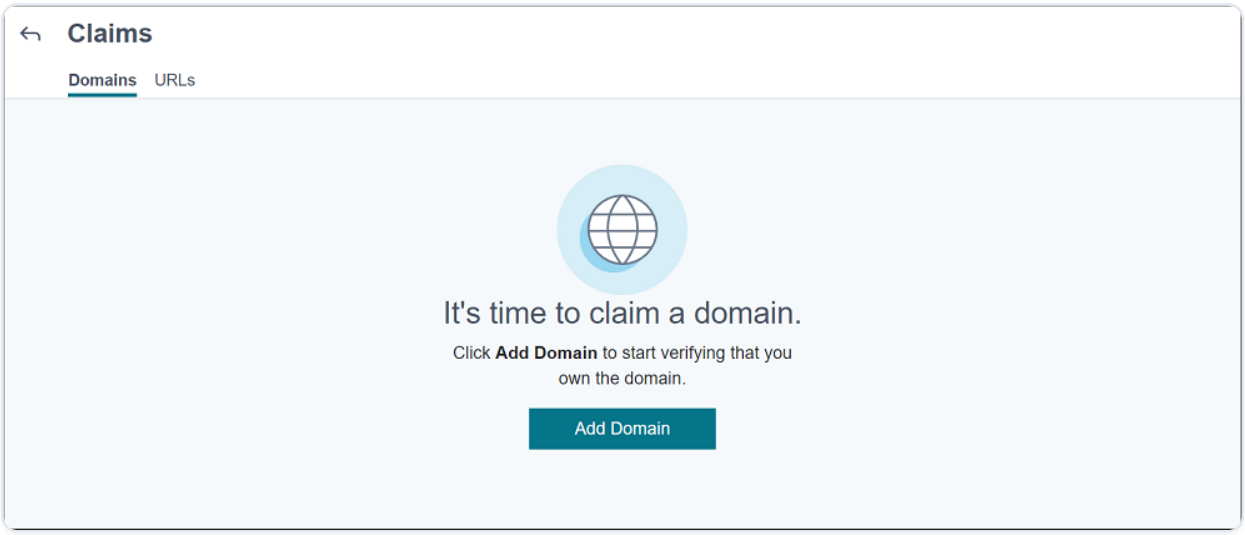
- El nuevo servicio AutoDiscovery en Citrix Cloud requiere la última versión de Citrix Secure Hub:
  - Para iOS, Citrix Secure Hub versión 21.6.0 o posterior
  - Para Android, Citrix Secure Hub versión 21.8.5 o posterior

    Los dispositivos que ejecutan versiones anteriores de Citrix Secure Hub podrían experimentar interrupciones en el servicio.
- Para acceder al nuevo servicio AutoDiscovery, debe tener una cuenta de administrador de Citrix Cloud con acceso completo. El servicio AutoDiscovery no admite cuentas de administrador con acceso personalizado. Si no tiene una cuenta, consulte Registrarse en Citrix Cloud.

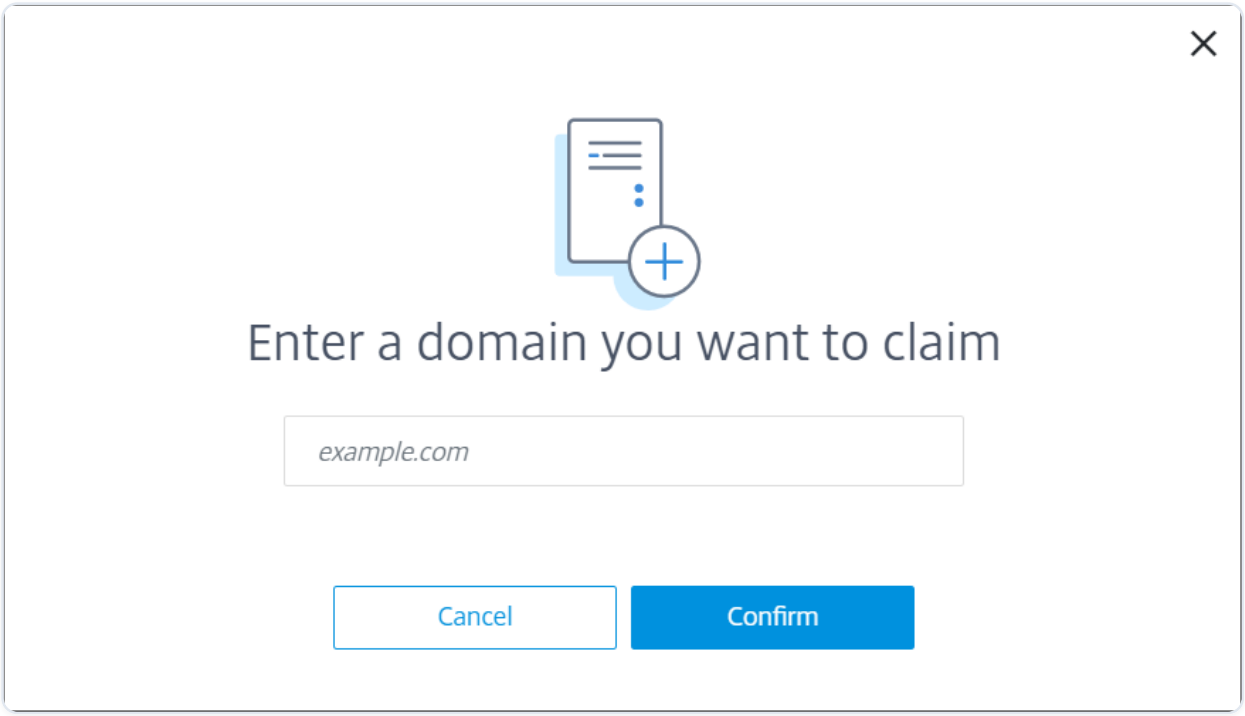
  Citrix migró todos los registros de AutoDiscovery existentes a Citrix Cloud sin interrupción del servicio. Los registros migrados no aparecen automáticamente en la nueva consola. Debe reclamar dominios en el nuevo servicio AutoDiscovery para demostrar la propiedad. Para obtener más información, consulte CTX312339.
- Antes de empezar a usar el servicio AutoDiscovery para sus implementaciones de Citrix Endpoint Management, verificar y reclame su dominio. Puede reclamar hasta 10 dominios. La reclamación asocia el dominio verificado con el servicio AutoDiscovery. Para reclamar más de 10 dominios, abra un ticket de SRE o póngase en contacto con el Soporte técnico de Citrix.
- Utilice la configuración de puerto MAM en lugar del FQDN de NetScaler Gateway para dirigir el tráfico MAM a su centro de datos. Si introduce un nombre de dominio completo junto con el puerto de su NetScaler Gateway, el dispositivo cliente utiliza la configuración del ajuste **Puerto MAM**.
- Si un bloqueador de anuncios impide que el sitio se abra, asegúrese de deshabilitar el bloqueador de anuncios para todo el sitio web.

Reclamar un dominio

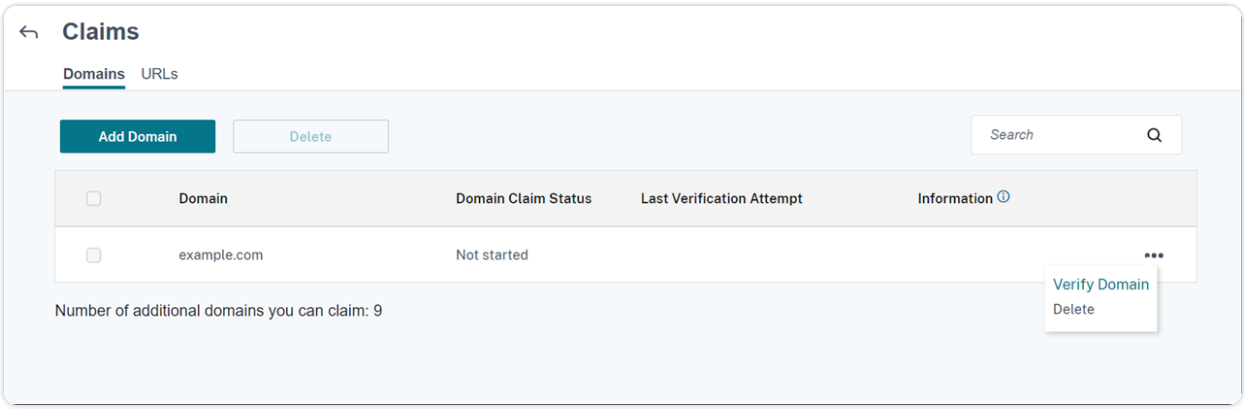
1. En la ficha **Reclamaciones > Dominios**, haga clic en **Agregar dominio**.



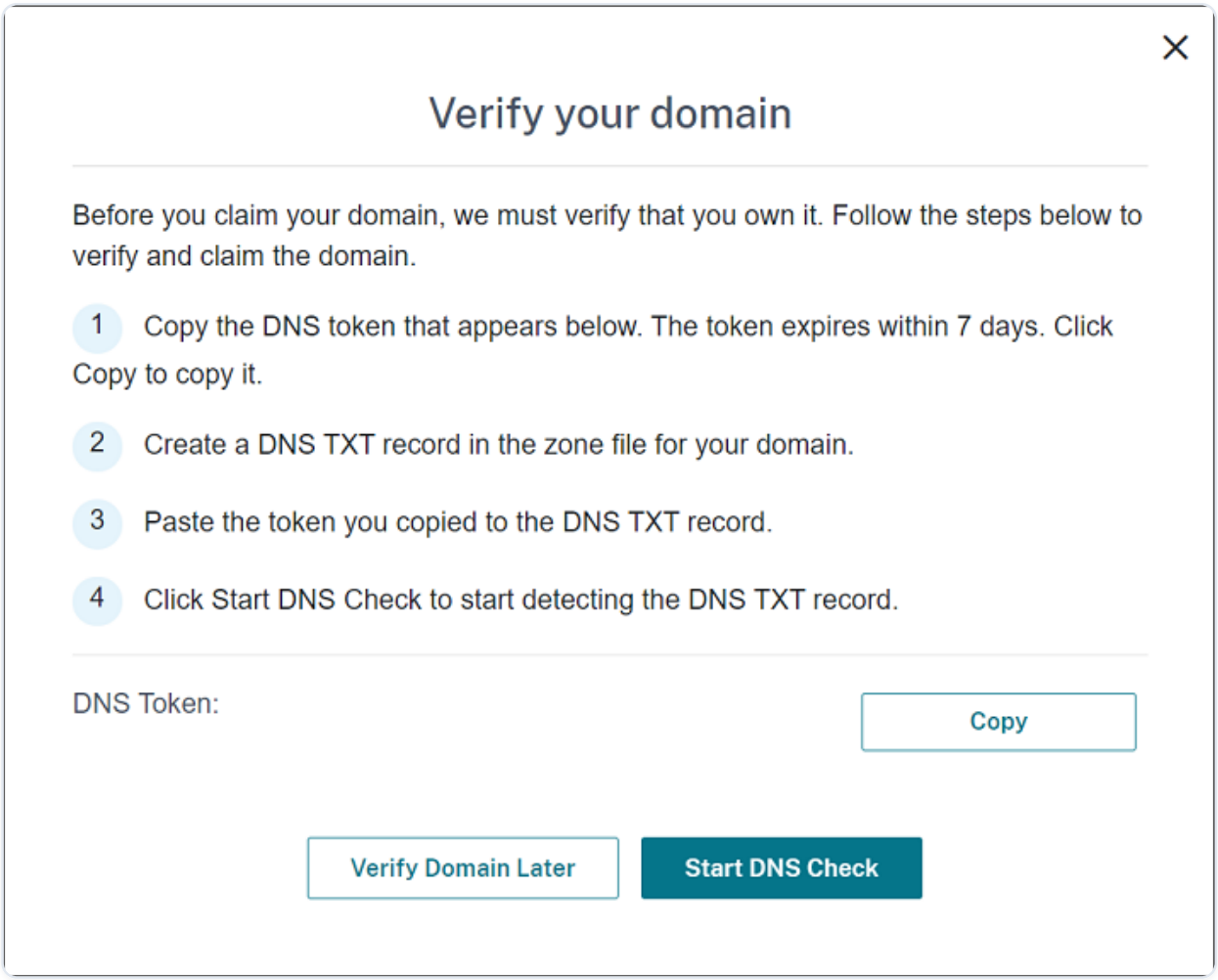
2. En el cuadro de diálogo que aparece, introduzca el nombre de dominio de su entorno de Citrix Endpoint Management y, a continuación, haga clic en **Confirmar**. Su dominio aparece en **Reclamaciones > Dominios**.



3. En el dominio que agregó, haga clic en el menú de puntos suspensivos y seleccione **verificar Domain** para iniciar el proceso de verificación. Aparece la página **verificar your domain**.



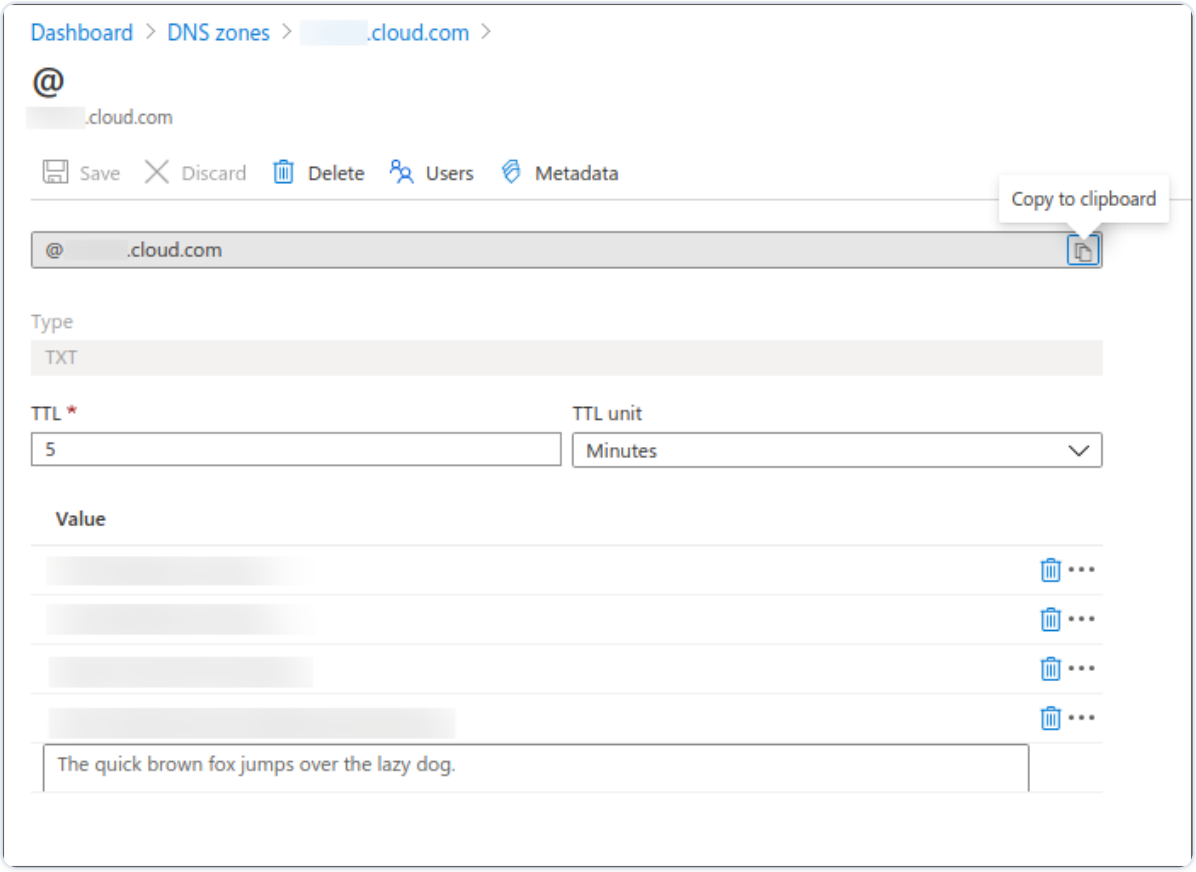
4. En la página **verificar your domain**, siga las instrucciones para verificar que es el propietario del dominio.



   a. Haga clic en **Copy** para copiar el token DNS en el portapapeles.

   b. Cree un registro DNS TXT en el archivo de zona de su dominio. Para ello, vaya al portal de su proveedor de alojamiento de dominios y añada el token DNS que copió.

      La siguiente captura de pantalla muestra un portal de proveedor de alojamiento de dominios. Su portal podría tener un aspecto diferente.



c. En Citrix Cloud, en la página **verificar your domain**, haga clic en **Start DNS Check** para empezar a detectar su registro DNS TXT. Si quiere verificar el dominio más tarde, haga clic en **verificar Domain Later**.

El proceso de verificación suele tardar aproximadamente una hora. Sin embargo, puede tardar hasta dos días en devolver una respuesta. Puede cerrar sesión y volver a iniciarla durante la comprobación de estado.

Una vez completada la configuración, el estado de su dominio cambia de **Pending** a **Verified**.

5. Después de reclamar su dominio, proporcione información sobre el servicio AutoDiscovery. Haga clic en el menú de puntos suspensivos del dominio que añadió y, a continuación, haga clic en **Add Citrix Endpoint Management Info**. Aparece la página **AutoDiscovery Service Information**.
6. Introduzca la siguiente información y, a continuación, haga clic en **Save**.

   - **Citrix Endpoint Management Server FQDN:** Introduzca el nombre de dominio completo del servidor de Citrix Endpoint Management. Por ejemplo: `example.xm.cloud.com`. Esta configuración se utiliza para el control del tráfico MDM y MAM.
   - **NetScaler Gateway FQDN:** Introduzca el nombre de dominio completo de NetScaler Gateway, en el formato FQDN o FQDN:puerto. Por ejemplo: `example.com`. Esta

configuración se utiliza para dirigir el tráfico MAM a su centro de datos. Para implementaciones solo de MDM, deje este campo en blanco.

> **Nota:**
>
> Citrix recomienda que utilice la configuración **MAM Port** en lugar de **NetScaler Gateway FQDN** para controlar el tráfico MAM. Si introduce un nombre de dominio completo junto con el puerto de su NetScaler Gateway, el dispositivo cliente utiliza la configuración de la opción **MAM Port**.

- **Instance Name:** Introduzca el nombre de instancia del servidor de Citrix Endpoint Management que configuró anteriormente. Si no está seguro de su nombre de instancia, deje el valor predeterminado **zdm**.
- **Puerto MDM:** Introduzca el puerto utilizado para el tráfico de control MDM y la inscripción MDM. Para los servicios basados en la nube, el valor predeterminado es 443.
- **Puerto MAM:** Introduzca el puerto utilizado para el tráfico de control MAM, la inscripción MAM, la inscripción de iOS y la enumeración de aplicaciones. Para los servicios basados en la nube, el valor predeterminado es 8443.

Solicitar AutoDiscovery para dispositivos Windows

Si tiene previsto inscribir dispositivos Windows, haga lo siguiente:

1. Póngase en contacto con el Soporte de Citrix y cree una solicitud de soporte para habilitar Windows AutoDiscovery.
2. Obtenga un certificado SSL firmado públicamente y no comodín para `enterpriseenrollment.mycompany.com`. La parte `mycompany.com` es el dominio que tiene las cuentas que los usuarios utilizan para inscribirse. Adjunte el certificado SSL en formato .pfx y su contraseña a la solicitud de soporte creada en el paso anterior.

   Para usar más de un dominio para inscribir dispositivos Windows, también puede usar un certificado multidominio con la siguiente estructura:

   - Un SubjectDN con un CN que especifica el dominio principal al que sirve (por ejemplo, enterpriseenrollment.mycompany1.com).
   - Los SAN apropiados para los dominios restantes (por ejemplo, enterpriseenrollment.mycompany2.com, enterpriseenrollment.mycompany3.com, etc.).

3. Cree un registro de nombre canónico (CNAME) en su DNS y asigne la dirección de su certificado SSL (enterpriseenrollment.mycompany.com) a autodisc.xm.cloud.com.

   Cuando un usuario de un dispositivo Windows se inscribe utilizando un UPN, el servidor de inscripción de Citrix:

   - Proporciona los detalles de su servidor Citrix Endpoint Management.
   - Indica al dispositivo que solicite un certificado válido a Citrix Endpoint Management.

En este punto, puede inscribir todos los dispositivos compatibles. Vaya a la siguiente sección para prepararse para entregar recursos a los dispositivos.

Integrar con el acceso condicional de Azure AD

Puede configurar Citrix Endpoint Management para aplicar la compatibilidad con el acceso condicional de Azure AD a las aplicaciones de Office 365. Esta función le permite implementar la metodología de confianza cero en los usuarios de dispositivos al implementar aplicaciones de Office 365. Puede usar el estado del dispositivo, la puntuación de riesgo, la ubicación y las protecciones del dispositivo para aplicar acciones automatizadas y definir el acceso a las aplicaciones de Office 365 en dispositivos Android Enterprise e iOS administrados.

Para aplicar el cumplimiento de dispositivos de Azure AD, debe configurar directivas de acceso condicional para aplicaciones individuales de Office 365. Puede restringir el acceso de los usuarios a aplicaciones específicas de Office 365 en dispositivos no administrados y no conformes, y permitir el acceso a aplicaciones individuales solo en dispositivos administrados y conformes.

Requisitos previos

- Para esta integración, debe tener una suscripción premium válida de Azure AD, incluidas las licencias de Intune y Microsoft Office 365.
- Citrix Secure Hub versión 21.4.0 y posteriores
- Configure Azure AD como proveedor de identidades (IdP) en Citrix Cloud y, a continuación, establezca la identidad de Citrix como el tipo de IdP para Citrix Endpoint Management. Para obtener más información, consulte Autenticación con Azure Active Directory a través de Citrix Cloud.
- Dé su consentimiento a la aplicación AAD multiempresa de Citrix para permitir que las aplicaciones móviles se autentiquen con la aplicación cliente de AAD. Solo es necesario si el administrador global de Azure estableció el valor de **Los usuarios pueden registrar**

aplicaciones en **No**. Configure esta opción en el portal de Azure en **Azure Active Directory > Usuarios > Configuración de usuario**. Para dar su consentimiento, consulte Configurar Citrix Endpoint Management para la administración de cumplimiento de Azure AD.

- Instale la aplicación Microsoft Authenticator en el dispositivo antes de iniciar el proceso de registro de dispositivos de Azure AD.
- Para la plataforma Android Enterprise, configure una aplicación de navegador web como la aplicación de tienda pública requerida.
- Deshabilite la configuración de **Valores predeterminados de seguridad** en la consola de Azure AD. Cuando inicia la configuración de Azure AD, reemplaza los valores predeterminados de seguridad por directivas de acceso condicional de Azure AD más granulares. Para obtener más información sobre los valores predeterminados de seguridad, consulte la documentación de Microsoft.

Configurar el cumplimiento de dispositivos mediante directivas de acceso condicional de Azure AD

Los pasos generales para configurar el cumplimiento de dispositivos mediante directivas de acceso condicional de Azure AD son los siguientes:

1. **Configuración de Citrix Endpoint Management:**
    - En el centro de administración de Microsoft Endpoint Manager, agregue **Citrix Workspace device compliance** como socio de cumplimiento para cada plataforma de dispositivos y asigne grupos de usuarios.
    - En Citrix Endpoint Management, sincronice la información del centro de administración de Microsoft Endpoint Manager.
2. **Configuración de Azure AD:** En el portal de Azure AD, configure las políticas de acceso condicional para las aplicaciones individuales de Office 365.
3. **Configuración de Citrix Endpoint Management:** Después de configurar las políticas de acceso condicional para las aplicaciones de Office 365, agregue la aplicación Microsoft Authenticator y las aplicaciones de Office 365 como aplicaciones de la tienda de aplicaciones pública en Citrix Endpoint Management. Asigne estas aplicaciones públicas al grupo de entrega y configúrelas como aplicaciones obligatorias.

Configurar Citrix Endpoint Management para la administración de cumplimiento de Azure AD

1. Inicie sesión en el Centro de administración de Microsoft Endpoint Manager y vaya a **Administración de inquilinos > Conectores y tokens > Administración de cumplimiento de dispositivos**. Haga clic en **Agregar socio de cumplimiento** y elija **Cumplimiento de dispositivos de Citrix Workspace** como socio de cumplimiento para cada plataforma de dispositivo. Luego, asigne grupos de usuarios.

   El centro de administración de Microsoft Endpoint Manager(/en-us/citrix-endpoint-management/media/partner-compliance-management.png)

2. En Citrix Endpoint Management, vaya a **Configuración > Administración de cumplimiento de Azure AD**.
3. Opcionalmente, establezca el consentimiento global para que los usuarios no necesiten dar su consentimiento en cada dispositivo. Junto a **Consentimiento de la aplicación cliente**, haga clic en **Proporcionar consentimiento**. Introduzca sus credenciales de administrador global de Azure AD y siga las indicaciones para proporcionar el consentimiento global para las aplicaciones cliente.
4. Haga clic en **Conectar** para sincronizar la información del centro de administración de Microsoft Endpoint Manager.

   Sincronizar información del centro de administración de Microsoft Endpoint Manager(/en-us/citrix-endpoint-management/media/device-compliance-connect.png)

   Un cuadro de diálogo le pide que acepte los permisos para esta configuración. Haga clic en **Aceptar**. Una vez completada la configuración, las plataformas de dispositivos sincronizadas aparecen en la lista.

   Solicitud de permiso(/en-us/citrix-endpoint-management/media/device-compliance-permissions-request.png)

Configurar políticas de acceso condicional en Azure AD

En el portal de Azure AD, configure las políticas de acceso condicional para las aplicaciones de Office 365 para aplicar el cumplimiento de dispositivos. Vaya a **Dispositivos > Acceso condicional > Políticas > Nueva política**. Para obtener más información, consulte la documentación de Microsoft.

Para configurar el cumplimiento de dispositivos para aplicaciones administradas por Intune:

- Configurar aplicaciones administradas por Intune para su entrega a dispositivos(/es-es/citrix-endpoint-management/integration-with-mem.html#configure-intune-managed-apps-for-delivery-to-devices)
- Requerir aplicaciones cliente aprobadas
- Requerir una directiva de protección de aplicaciones y una aplicación cliente aprobada para el acceso a aplicaciones en la nube

Configurar aplicaciones en Citrix Endpoint Management

Después de configurar las directivas de acceso condicional para las aplicaciones de Office 365, agregue la aplicación Microsoft Authenticator y las aplicaciones de Office 365 como aplicaciones de la tienda de aplicaciones pública en Citrix Endpoint Management. Asigne estas aplicaciones públicas al grupo de entrega y configúrelas como aplicaciones obligatorias. Para obtener información, consulte Agregar una aplicación de la tienda de aplicaciones pública.

Flujo de trabajo de autenticación de usuario

1. Los usuarios que inscribieron dispositivos con Active Directory (AD) local y que luego se integraron con el proveedor de identidades de Citrix mediante Microsoft Azure Active Directory (AAD) no necesitan volver a inscribirse. Puede sincronizar cuentas de su Active Directory local con Microsoft Azure Active Directory. Para obtener más información, consulte Preparar Active Directory y Azure AD.
2. Citrix Endpoint Management envía Microsoft Authenticator y las aplicaciones de Office 365 configuradas a un dispositivo como aplicaciones obligatorias. Si configuró una aplicación de navegador web como la aplicación de tienda pública obligatoria para la plataforma Android, Citrix Endpoint Management también la envía al dispositivo del usuario.
3. Citrix Secure Hub instala y muestra automáticamente todas las aplicaciones administradas a través de Citrix Endpoint Management.
4. Cuando un usuario intenta iniciar sesión en cualquier aplicación de Office 365 disponible, el dispositivo le pide que toque el enlace **Registro de Azure AD** para iniciar el proceso de registro.
5. Después de que el usuario toca el enlace de registro, se abre la aplicación Microsoft Authenticator. El usuario introduce las credenciales de Azure AD y acepta los términos de inscripción del dispositivo. Luego, la aplicación Microsoft Authenticator se cierra y Citrix Secure Hub se vuelve a abrir.

6. Citrix Secure Hub muestra un mensaje de que el registro del dispositivo en Azure AD se ha completado. Ahora el usuario puede usar las aplicaciones de Microsoft para acceder a sus recursos en la nube.

   Una vez completado el registro, Azure AD marca el dispositivo como administrado y compatible en la consola.

Directivas de dispositivo predeterminadas y aplicaciones de productividad móvil

Si se incorpora a partir de Citrix Endpoint Management 19.5.0 o posterior, preconfiguramos algunas directivas de dispositivo y aplicaciones de productividad móvil. Esa configuración le permite:

- Implementar inmediatamente la funcionalidad básica en los dispositivos
- Comience con las configuraciones de línea base recomendadas para un espacio de trabajo seguro

Para las plataformas Android, Android Enterprise, iOS, macOS y Windows Desktop/Tablet, su sitio tiene estas directivas de dispositivo preconfiguradas:

- **Directiva de dispositivo de código de acceso:** La directiva de dispositivo de código de acceso está **activada**, con todas las configuraciones predeterminadas de código de acceso habilitadas.
- **Directiva de dispositivo de inventario de aplicaciones:** La directiva de dispositivo de inventario de aplicaciones está **activada**.
- **Directiva de dispositivo de restricciones:** La directiva de dispositivo de restricciones está **activada**, con todas las configuraciones predeterminadas de restricciones habilitadas.

Esas directivas se encuentran en el grupo de entrega **AllUsers**, que contiene todos los usuarios locales y de Active Directory. Le recomendamos que utilice el grupo de entrega AllUsers solo para las pruebas iniciales. A continuación, cree sus grupos de entrega y deshabilite el grupo de entrega AllUsers. Puede reutilizar las directivas de dispositivo y las aplicaciones preconfiguradas en sus grupos de entrega.

Todas las directivas de dispositivo de Citrix Endpoint Management están documentadas en Directivas de dispositivo. Ese artículo incluye información sobre cómo usar la consola para editar directivas de dispositivo. Para obtener información sobre algunas directivas de dispositivo de uso común, consulte Directivas de dispositivo y comportamiento de casos de uso.

Para las plataformas iOS y Android, su sitio tiene estas aplicaciones de productividad móvil preconfiguradas:

- **Citrix Secure Mail**
- **Citrix Secure Web**
- **Citrix Files**

Esas aplicaciones se encuentran en el grupo de entrega **AllUsers**.

Para obtener más información, consulte Acerca de las aplicaciones de productividad móvil.

Continúe con la configuración de Citrix Endpoint Management

Una vez que complete la configuración básica para la inscripción de dispositivos, la forma en que configure Citrix Endpoint Management varía ampliamente según sus casos de uso. Por ejemplo:

- ¿Cuáles son sus requisitos de seguridad y cómo quiere equilibrar esos requisitos con la experiencia del usuario?
- ¿Qué plataformas de dispositivos admite?
- ¿Los usuarios son propietarios de sus dispositivos o utilizan dispositivos propiedad de la empresa?
- ¿Qué directivas de dispositivo quiere enviar a los dispositivos?
- ¿Qué tipos de aplicaciones proporciona a los usuarios?

Esta sección le ayuda a navegar por las muchas opciones de configuración dirigiéndole a los artículos de este conjunto de documentación.

A medida que complete la configuración en sitios de terceros, tome nota de la información y su ubicación, para consultarla cuando configure los ajustes de la consola de Citrix Endpoint Management.

- Seguridad y autenticación. Citrix Endpoint Management utiliza certificados para crear conexiones seguras y autenticar a los usuarios. Citrix proporciona certificados comodín para su instancia de Citrix Endpoint Management.
    - Para una explicación de los componentes de autenticación y las configuraciones recomendadas por nivel de seguridad, consulte el artículo "Conceptos avanzados", Autenticación. Consulte también Seguridad y experiencia del usuario.

  - Para obtener una descripción general de los componentes de autenticación utilizados durante las operaciones de Citrix Endpoint Management, consulte Certificados y autenticación.
  - Puede elegir entre los siguientes tipos de autenticación. La configuración de la autenticación incluye tareas en las consolas de Citrix Endpoint Management y NetScaler Gateway.
    - Autenticación de dominio o de dominio más token de seguridad
    - Certificado de cliente o certificado más autenticación de dominio
  - Para entregar certificados a los usuarios, configure:
    - Entidades PKI
    - Proveedores de credenciales
  - Modos de seguridad de inscripción de dispositivos. Los modos de seguridad de inscripción de dispositivos especifican los tipos de credenciales y los pasos de inscripción necesarios para que los usuarios inscriban sus dispositivos en Citrix Endpoint Management. Para obtener más información, consulte Configurar modos de seguridad de inscripción.
  - Para permitir que los usuarios se autentiquen con credenciales de Azure Active Directory, consulte Autenticarse con Azure Active Directory a través de Citrix Cloud.

- Inscripción de dispositivos
  - Hay programas disponibles para inscribir un gran número de dispositivos:
    - Implementar dispositivos a través de Apple Deployment Program
    - Inscripción masiva de dispositivos Apple
    - Inscribir dispositivos Windows de forma masiva
  - Para inscribir dispositivos Android, cree una cuenta de administrador de Android Enterprise. Consulte Android Enterprise. O bien, consulte Legacy Android Enterprise para clientes de Google Workspace.
  - Puede usar invitaciones de inscripción o enviar notificaciones para la inscripción.
    - Invitaciones de inscripción.
    - Notificaciones.
  - Para obtener más información sobre la inscripción, consulte Administración de dispositivos y los artículos de ese nodo.

- Directivas y administración de dispositivos
  - Directivas de dispositivos (MDM). Todas las directivas de dispositivos de Citrix Endpoint Management están documentadas en Directivas de dispositivos. Para obtener información sobre algunas directivas de dispositivos de uso común, consulte Comportamiento de las directivas de dispositivos y casos de uso.
  - Propiedades de cliente. Las propiedades de cliente contienen información que se proporciona directamente a Citrix Secure Hub en los dispositivos de usuario. Consulte Propiedades de cliente y Propiedades de cliente de Citrix Endpoint Management.
  - Grupos de entrega. Para ver un caso de uso de ejemplo relacionado con los grupos de entrega, consulte Comunidades de usuarios y Agregar un grupo de entrega.
- Preparar aplicaciones para la implementación
  - Para obtener información sobre las aplicaciones compatibles con Citrix Endpoint Management, consulte Agregar aplicaciones.
  - Puede administrar las licencias de aplicaciones iOS mediante Apple Volume Purchase. Para obtener más información, consulte Apple Volume Purchase.
  - Puede usar Citrix Endpoint Management para implementar iBooks que obtenga a través de Apple Volume Purchase. Consulte Agregar contenido multimedia.
  - Citrix proporciona aplicaciones de productividad móvil, incluidas Citrix Secure Mail y Citrix Secure Web. Consulte Acerca de las aplicaciones de productividad móvil.
  - Como alternativa a Citrix Secure Mail, puede entregar correo nativo a los dispositivos. Consulte:
    - Estrategia de correo electrónico
    - Conector de Citrix Endpoint Management para Exchange ActiveSync
    - Conector de NetScaler Gateway para Exchange ActiveSync
  - Para permitir a los usuarios transferir de forma segura documentos y datos a las aplicaciones de Microsoft Office 365, consulte Permitir la interacción segura con las aplicaciones de Office 365 y Directiva de dispositivos de Office.
  - Para obtener información general sobre las directivas de aplicaciones, consulte Directivas de aplicaciones y escenario de caso de uso.
  - MDX Toolkit es una tecnología de encapsulado de aplicaciones que prepara las aplicaciones empresariales para una implementación segura con Citrix Endpoint

Management. El SDK de MAM reemplaza a MDX Toolkit. MDX Toolkit tiene previsto alcanzar el fin de vida útil (EOL) en julio de 2023.

Para obtener información sobre el SDK de MAM, consulte Información general sobre el SDK de MAM.

- Para obtener más información sobre las aplicaciones, consulte otros artículos en Agregar aplicaciones.

- La función de control de acceso basado en roles (RBAC) de Citrix Endpoint Management le permite asignar roles predefinidos, o conjuntos de permisos, a usuarios y grupos. Estos permisos controlan el nivel de acceso que los usuarios tienen a las funciones del sistema. Para obtener más información, consulte Configurar roles con RBAC.
- Puede crear acciones automatizadas en Citrix Endpoint Management para especificar la acción que se debe realizar en respuesta a eventos, ciertas configuraciones o la presencia de aplicaciones en los dispositivos de los usuarios. Para obtener más información, consulte Acciones automatizadas.

Certificados y autenticación

Varios componentes desempeñan un papel en la autenticación durante las operaciones de Citrix Endpoint Management:

- **Citrix Endpoint Management:** El servidor de Citrix Endpoint Management es donde se definen la seguridad de la inscripción y la experiencia de inscripción. Las opciones para incorporar usuarios incluyen:
  - Si la inscripción debe ser abierta para todos o solo por invitación.
  - Si se requiere autenticación de dos factores o de tres factores. Las propiedades del cliente de Citrix Endpoint Management le permiten habilitar la autenticación con PIN de Citrix y configurar la complejidad y la caducidad del PIN.
- **NetScaler Gateway:** NetScaler Gateway proporciona la terminación para las sesiones SSL de micro VPN. NetScaler Gateway también proporciona seguridad de red en tránsito y le permite definir la experiencia de autenticación utilizada cada vez que un usuario accede a una aplicación.
- **Citrix Secure Hub:** Citrix Secure Hub y Citrix Endpoint Management trabajan juntos en las operaciones de inscripción. Citrix Secure Hub es la entidad en un dispositivo que se comunica con NetScaler Gateway: cuando una sesión caduca, Citrix Secure Hub obtiene un tíquet de autenticación de NetScaler Gateway y lo pasa a las aplicaciones MDX. Citrix recomienda el anclaje de certificados (certificate pinning), que evita los ataques de intermediario (man-in-the-middle). Para obtener más información, consulte esta sección del artículo de Citrix Secure Hub: Anclaje de certificados.

  Citrix Secure Hub también facilita el contenedor de seguridad MDX: Citrix Secure Hub envía directivas, crea una sesión con NetScaler Gateway cuando una aplicación agota el tiempo de espera y define el tiempo de espera y la experiencia de autenticación de MDX. Citrix Secure Hub también es responsable de la detección de jailbreak, las comprobaciones de geolocalización y cualquier directiva que aplique.
- **Directivas MDX:** Las directivas MDX crean la bóveda de datos en el dispositivo. Las directivas MDX dirigen las conexiones de micro VPN de vuelta a NetScaler Gateway, aplican restricciones del modo sin conexión y aplican directivas de cliente, como los tiempos de espera.

Citrix Endpoint Management autentica a los usuarios en sus recursos mediante los siguientes métodos de autenticación:

- Administración de dispositivos móviles (MDM)
    - Proveedores de identidades alojados en la nube (IdP)
    - Protocolo ligero de acceso a directorios (LDAP)
        - URL de invitación + PIN
        - Autenticación de dos factores
- Administración de aplicaciones móviles (MAM)
    - LDAP
    - Certificado
    - Token de seguridad La autenticación MAM requiere NetScaler Gateway.

Para obtener otros detalles de configuración, consulte los siguientes artículos:

- Cargar, actualizar y renovar certificados
- NetScaler Gateway y Citrix Endpoint Management
- Autenticación de dominio o de dominio más token de seguridad
- Certificado de cliente o autenticación de certificado más dominio
- Entidades PKI
- Proveedores de credenciales
- Certificados APNs
- SAML para el inicio de sesión único con Citrix Files
- Autenticación con Azure Active Directory a través de Citrix Cloud
- Autenticación con Okta a través de Citrix Cloud
- Autenticación con un NetScaler Gateway local a través de Citrix Cloud
- Para autenticarse en un servidor Wi-Fi, envíe un certificado a los dispositivos: Directiva de dispositivos de red
- Para enviar un certificado único no utilizado para la autenticación, como un certificado de autoridad de certificación (CA) raíz interna o una directiva específica: Directiva de dispositivos de credenciales

Certificados

Citrix Endpoint Management genera un certificado SSL (Secure Sockets Layer) autofirmado durante la instalación para proteger los flujos de comunicación al servidor. Reemplace el certificado SSL por un certificado SSL de confianza de una autoridad de certificación conocida.

Citrix Endpoint Management también utiliza su propio servicio de infraestructura de clave pública (PKI) u obtiene certificados de la CA para los certificados de cliente. Todos los productos de Citrix admiten certificados comodín y de nombre alternativo del sujeto (SAN). Para la mayoría de las implementaciones, solo necesita dos certificados comodín o SAN.

La autenticación de certificados de cliente proporciona una capa adicional de seguridad para las aplicaciones móviles y permite a los usuarios acceder sin problemas a las aplicaciones HDX. Cuando la autenticación de certificados de cliente está configurada, los usuarios escriben su PIN de Citrix para el acceso de inicio de sesión único (SSO) a las aplicaciones habilitadas para Citrix Endpoint Management. El PIN de Citrix también simplifica la experiencia de autenticación del usuario. El PIN de Citrix se utiliza para proteger un certificado de cliente o para guardar las credenciales de Active Directory localmente en el dispositivo.

Para inscribir y administrar dispositivos iOS con Citrix Endpoint Management, configure y cree un certificado del Servicio de notificaciones push de Apple (APNs) de Apple. Para conocer los pasos, consulte Certificados APNs.

La siguiente tabla muestra el formato y el tipo de certificado para cada componente de Citrix Endpoint Management:

COMPONENTE DE CITRIX ENDPOINT MANAGEMENT	FORMATO DE CERTIFICADO	TIPO DE CERTIFICADO REQUERIDO
NetScaler Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Raíz (NetScaler Gateway convierte PFX a PEM automáticamente.
Citrix Endpoint Management	.p12 (.pfx en equipos basados en Windows)	SSL, SAML, APNs (Citrix Endpoint Management también genera una PKI completa durante el proceso de instalación). **Importante:** Citrix Endpoint Management no admite certificados con extensión .pem. Para usar un certificado .pem, divida el

COMPONENTE DE CITRIX ENDPOINT MANAGEMENT	FORMATO DE CERTIFICADO	TIPO DE CERTIFICADO REQUERIDO
		archivo .pem en un certificado y una clave e importe cada uno en Citrix Endpoint Management.
StoreFront	PFX (PKCS #12)	SSL, raíz

Citrix Endpoint Management admite certificados de cliente con longitudes de bits de 4096 y 2048.

Para NetScaler Gateway y Citrix Endpoint Management, se recomienda obtener certificados de servidor de una CA pública, como Verisign, DigiCert o Thawte. Puede crear una solicitud de firma de certificado (CSR) desde NetScaler Gateway o la utilidad de configuración de Citrix Endpoint Management. Después de crear la CSR, la envía a la CA para que la firme. Cuando la CA devuelve el certificado firmado, puede instalarlo en NetScaler Gateway o Citrix Endpoint Management.

> **Importante:**

> Requisitos para certificados de confianza en iOS, iPadOS y macOS

> Apple tiene nuevos requisitos para los certificados de servidor TLS. verificar que todos los certificados cumplen los requisitos de Apple. Consulte la publicación de Apple, `<https://support.apple.com/es-es/HT210176>`.

> Apple está reduciendo la vida útil máxima permitida de los certificados de servidor TLS. Este cambio afecta solo a los certificados de servidor emitidos después de septiembre de 2020. Consulte la publicación de Apple, `<https://support.apple.com/es-es/HT211025>`.

Autenticación LDAP

Citrix Endpoint Management admite la autenticación basada en dominios para uno o varios directorios que cumplen con el Protocolo ligero de acceso a directorios (LDAP). LDAP es un protocolo de software que proporciona acceso a información sobre grupos, cuentas de usuario y

propiedades relacionadas. Para obtener más información, consulte Autenticación de dominio o de dominio más token de seguridad.

Autenticación del proveedor de identidades

Puede configurar un proveedor de identidades (IdP) a través de Citrix Cloud para inscribir y administrar dispositivos de usuario.

Casos de uso admitidos para IdP:

- Azure Active Directory a través de Citrix Cloud
  - La integración con Workspace es opcional
  - NetScaler Gateway configurado para la autenticación basada en certificados
  - Android Enterprise (Vista previa. Admite BYOD, dispositivos totalmente administrados y perfiles de inscripción mejorados)
  - iOS para inscripciones de MDM+MAM y MDM
  - iOS y macOS para inscripciones de Apple Business Manager
  - Android heredado (DA)

  Las funciones de inscripción automática, como Apple School Manager, no son compatibles actualmente.
- Okta a través de Citrix Cloud
  - La integración con Workspace es opcional
  - NetScaler Gateway configurado para la autenticación basada en certificados
  - Android Enterprise (Vista previa. Admite BYOD, dispositivos totalmente administrados y perfiles de inscripción mejorados)
  - iOS para inscripciones de MDM+MAM y MDM
  - iOS y macOS para inscripciones de Apple Business Manager
  - Android heredado (DA)

  Las funciones de inscripción automática, como Apple School Manager, no son compatibles actualmente.
- NetScaler Gateway local a través de Citrix Cloud
  - NetScaler Gateway configurado para la autenticación basada en certificados

- Android Enterprise (Vista previa. Admite BYOD, dispositivos totalmente administrados y perfiles de inscripción mejorados)
- iOS para inscripciones de MDM+MAM y MDM
- Android heredado (DA) Las funciones de inscripción automática, como Apple Deployment Program, no son compatibles actualmente.

Cargar, actualizar y renovar certificados

Le recomendamos que enumere los certificados necesarios para su implementación de Citrix Endpoint Management. Utilice la lista para realizar un seguimiento de las fechas de caducidad y las contraseñas de los certificados. Este artículo le ayuda a administrar los certificados durante toda su vida útil.

Su entorno podría incluir los siguientes certificados:

- Servidor de Citrix Endpoint Management
  - Certificado SSL para MDM FQDN (Necesario si migró de XenMobile Server a Citrix Endpoint Management. De lo contrario, Citrix gestiona este certificado).
  - Certificado SAML (para Citrix Files)
  - Certificados de CA raíz e intermedios para los certificados anteriores y cualquier otro recurso interno (StoreFront/Proxy, etc.)
  - Certificado APNs para la administración de dispositivos iOS
  - Certificado de usuario PKI para la conectividad a PKI (obligatorio si su entorno requiere autenticación basada en certificados)
- Kit de herramientas MDX
  - Certificado de desarrollador de Apple
  - Perfil de aprovisionamiento de Apple (por aplicación)
  - Certificado APNs de Apple (para usar con Citrix Secure Mail)
  - Archivo de almacén de claves de Android

  El SDK de MAM no encapsula aplicaciones, por lo que no requiere un certificado.
- NetScaler Gateway
  - Certificado SSL para FQDN de MDM
  - Certificado SSL para FQDN de Gateway

- Certificado SSL para FQDN de ShareFile SZC
- Certificado SSL para equilibrio de carga de Exchange (configuración de descarga)
- Certificado SSL para equilibrio de carga de StoreFront
- Certificados de CA raíz e intermedios para los certificados anteriores

Nota:

El dispositivo cliente debe tener el certificado raíz/intermedio necesario para establecer la confianza con la autoridad de certificación que emitió el certificado de servidor. De lo contrario, podría recibir el error SSL 61. Para resolver el problema:

1. Descargue u obtenga el archivo de certificado SSL raíz/intermedio (.crt o .cer) emitido por su proveedor de certificados SSL. Normalmente, el certificado raíz/intermedio/de servidor está presente en el paquete de certificados proporcionado por su proveedor de servicios SSL.
2. Instale el certificado raíz/intermedio en el dispositivo cliente.
3. Si hay un antivirus instalado en el dispositivo cliente, asegúrese de que el antivirus confíe en el certificado.

Cargar certificados

Cada certificado que carga tiene una entrada en la tabla Certificados, incluido un resumen de su contenido. Cuando configure componentes de integración de PKI que requieran un certificado, elija un certificado de servidor que cumpla los criterios. Por ejemplo, es posible que desee configurar Citrix Endpoint Management para que se integre con su autoridad de certificación (CA) de Microsoft. La conexión a la CA de Microsoft debe autenticarse mediante un certificado de cliente.

Es posible que Citrix Endpoint Management no tenga la clave privada de un certificado determinado. Del mismo modo, es posible que Citrix Endpoint Management no requiera una clave privada para los certificados cargados.

Esta sección proporciona procedimientos generales para cargar certificados. Para obtener detalles sobre cómo crear, cargar y configurar certificados de cliente, consulte Autenticación de certificado de cliente o certificado más dominio.

Tiene dos opciones para cargar certificados:

- Cargue los certificados en la consola individualmente.
- Realice una carga masiva de certificados mediante la API de REST. Esta opción solo está disponible para dispositivos iOS.

Al cargar certificados en la consola, puede:

- Importe un almacén de claves. Luego, identifique la entrada en el repositorio del almacén de claves que desea instalar, a menos que esté cargando un formato PKCS #12.
- Importe un certificado.

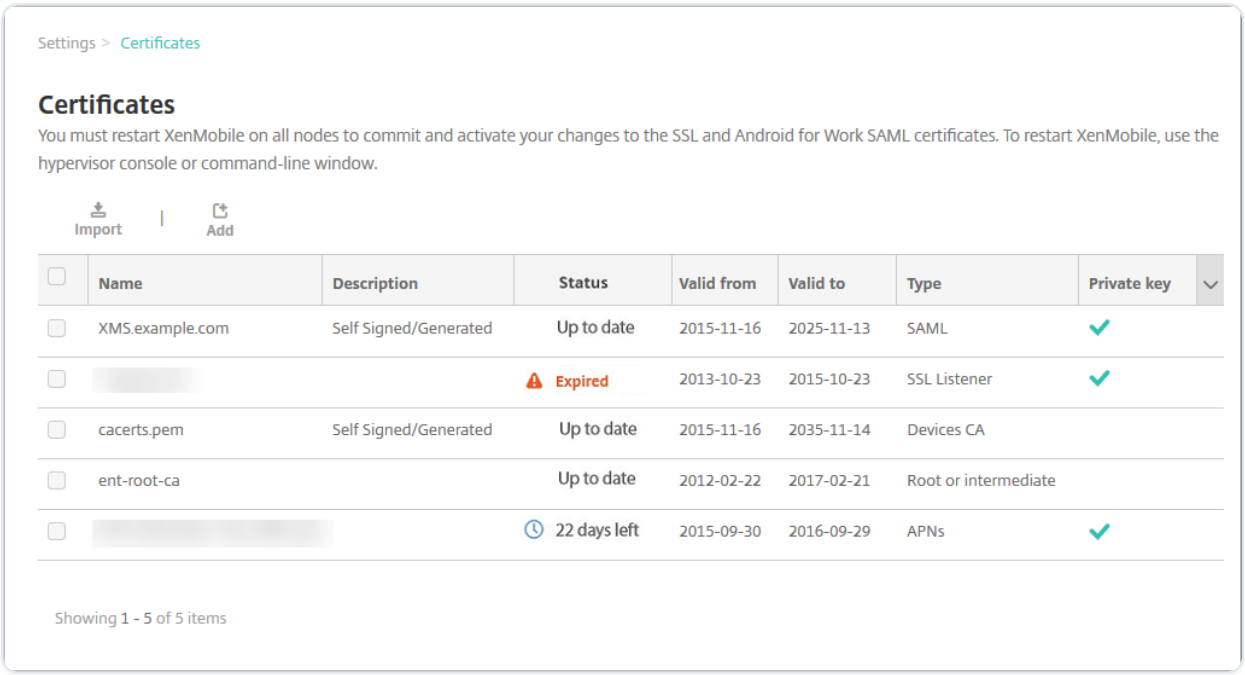
Puede cargar el certificado de CA (sin la clave privada) que la CA utiliza para firmar solicitudes. También puede cargar un certificado de cliente SSL (con la clave privada) para la autenticación de cliente.

Al configurar la entidad de CA de Microsoft, especifique el certificado de CA. Seleccione el certificado de CA de una lista de todos los certificados de servidor que son certificados de CA. Del mismo modo, al configurar la autenticación de cliente, puede seleccionar de una lista de todos los certificados de servidor para los que Citrix Endpoint Management tiene la clave privada.

Para importar un almacén de claves

Un almacén de claves es un repositorio de certificados de seguridad. Por diseño, los almacenes de claves pueden tener muchas entradas. Al cargar desde un almacén de claves, debe especificar el alias de entrada que identifica la entrada que desea cargar. Si no especifica un alias, se carga la primera entrada del almacén. Dado que los archivos PKCS #12 suelen tener solo una entrada, el campo de alias no aparece cuando selecciona PKCS #12 como tipo de almacén de claves.

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha de la consola. Utilice la barra de búsqueda para buscar y abrir la configuración de **Certificados**.



2. Haga clic en **Importar**. Aparece el cuadro de diálogo **Importar**.
3. Configure estos ajustes:

   - **Importar:** Seleccione **Almacén de claves**.

   La página de configuración de certificados(/en-us/citrix-endpoint-management/media/settings-certificates-import-keystore.png)

   - **Tipo de almacén de claves:** Haga clic en **PKCS #12** en la lista desplegable.
   - **Usar como:** En la lista, haga clic en cómo piensa usar el certificado. Las opciones disponibles son:

     - **Servidor:** Los certificados de servidor son certificados utilizados funcionalmente por Citrix Endpoint Management. Los certificados de servidor se cargan en la consola web de Citrix Endpoint Management. Esos certificados incluyen certificados de CA, certificados de RA y certificados para la autenticación de clientes con otros componentes de su infraestructura. Además, puede usar certificados de servidor como almacenamiento para los certificados que desea implementar en los dispositivos. Este uso se aplica especialmente a las CA utilizadas para establecer la confianza en el dispositivo.
     - **SAML:** La certificación del Lenguaje de marcado de aserción de seguridad (SAML) le permite proporcionar acceso SSO a servidores, sitios web y aplicaciones.
     - **APNs:** Los certificados APNs de Apple permiten la administración de dispositivos móviles a través de la red de notificaciones push de Apple.

    - **Agente de escucha SSL:** El agente de escucha de Secure Sockets Layer (SSL) notifica a Citrix Endpoint Management la actividad criptográfica SSL.

- **Archivo de almacén de claves:** Busque el almacén de claves que desea importar. El almacén de claves es un archivo .p12 o .pfx. Seleccione el archivo y haga clic en **Abrir**.
- **Contraseña:** Escriba la contraseña asignada al certificado.
- **Descripción:** Opcionalmente, escriba una descripción para el almacén de claves para ayudarle a distinguirlo de sus otros almacenes de claves.

4. Haga clic en **Importar**. El almacén de claves se añade a la tabla Certificados.

Para importar un certificado

Al importar un certificado, Citrix Endpoint Management intenta construir una cadena de certificados a partir de la entrada. Citrix Endpoint Management importa todos los certificados de una cadena para crear una entrada de certificado de servidor para cada certificado. Esta operación solo funciona si los certificados del archivo o la entrada del almacén de claves forman una cadena. Cada certificado subsiguiente de la cadena debe ser el emisor del certificado anterior.

Puede añadir una descripción opcional para el certificado importado. La descripción solo se adjunta al primer certificado de la cadena. Puede actualizar la descripción de los certificados restantes más adelante.

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha de la consola. Utilice la barra de búsqueda para encontrar y abrir la configuración de **Certificados**.
2. En la página **Certificados**, haga clic en **Importar**. Aparece el cuadro de diálogo **Importar**. Configure lo siguiente:

    - **Importar:** haga clic en **Certificado**.
    - **Usar como:** Seleccione cómo planea usar el certificado. Las opciones disponibles son:

        - **Servidor:** Los certificados de servidor son certificados utilizados funcionalmente por Citrix Endpoint Management. Los certificados de servidor se cargan en la consola web de Citrix Endpoint Management. Esos certificados incluyen certificados de CA, certificados de RA y certificados para la autenticación de clientes con otros componentes de su infraestructura. Además, puede usar certificados de servidor como almacenamiento para los certificados que desea implementar en los dispositivos. Esta opción se aplica especialmente a las CA utilizadas para establecer la confianza en el dispositivo.

    - **SAML:** La certificación Security Assertion Markup Language (SAML) le permite proporcionar acceso de inicio de sesión único (SSO) a servidores, sitios web y aplicaciones.
    - **Agente de escucha SSL:** El agente de escucha de Secure Sockets Layer (SSL) notifica a Citrix Endpoint Management la actividad criptográfica SSL.

- **Importación de certificado:** Busque el certificado que desea importar. Seleccione el archivo y haga clic en **Abrir**.
- **Archivo de clave privada:** Busque un archivo de clave privada opcional para el certificado. La clave privada se utiliza para el cifrado y descifrado junto con el certificado. Seleccione el archivo y haga clic en **Abrir**.
- **Descripción:** Escriba una descripción para el certificado, opcionalmente, para ayudarle a identificarlo de sus otros certificados.

3. Haga clic en **Importar**. El certificado se añade a la tabla Certificados.

Cargar certificados de forma masiva mediante la API de REST

A veces, cargar los certificados uno a uno no es razonable. En esos casos, realice una carga masiva de certificados mediante la API de REST. Este método admite certificados en formato .p12. Para obtener más información sobre la API de REST, consulte API de REST.

1. Cambie el nombre de cada uno de los archivos de certificado al formato `device_identity_value.p12`. El `device_identity_value` puede ser el IMEI, el número de serie o el MEID de cada dispositivo.

   Por ejemplo, si elige usar números de serie como método de identificación. Un dispositivo tiene el número de serie `A12BC3D4EFGH`, así que asigne el nombre `A12BC3D4EFGH.p12` al archivo de certificado que espera instalar en ese dispositivo.

2. Cree un archivo de texto para almacenar las contraseñas de los certificados .p12. En ese archivo, escriba el identificador del dispositivo y la contraseña de cada dispositivo en una nueva línea. Utilice el formato `device_identity_value=password`. Consulte lo siguiente:

   ```
   A12BC3D4EFGH.p12=password1!

   A12BC3D4EFIJ.p12=password2@

   A12BC3D4EFKL.p12=password3#
   ```

3. Empaquete todos los certificados y el archivo de texto que creó en un archivo .zip.

4. Inicie su cliente de API REST, inicie sesión en Citrix Endpoint Management y obtenga un token de autenticación.
5. Importe sus certificados y asegúrese de incluir lo siguiente en el cuerpo del mensaje:

```
{

    "alias": "",

    "useAs": "device",

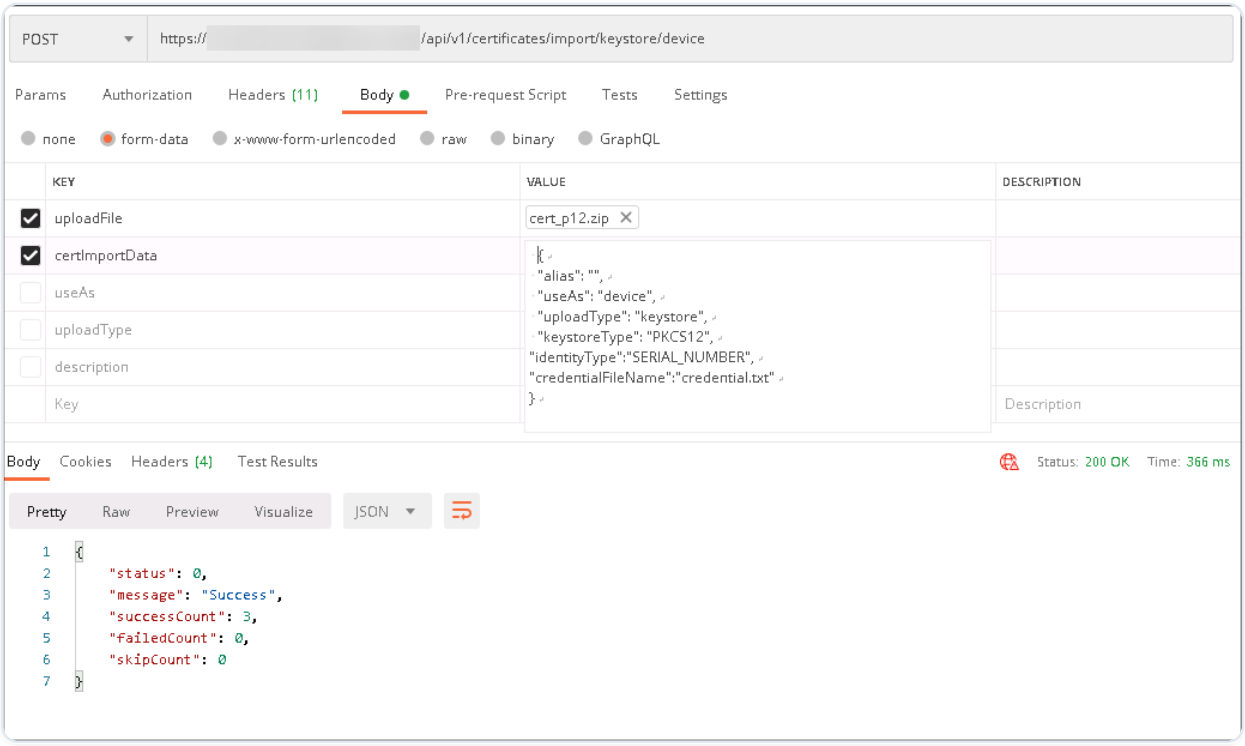
    "uploadType": "keystore",

    "keystoreType": "PKCS12",

    "identityType":"SERIAL_NUMBER",        # identity type can be
"SERIAL_NUMBER","IMEI","MEID"

    "credentialFileName":"credential.txt"   # The credential file name
in .zip

}
```

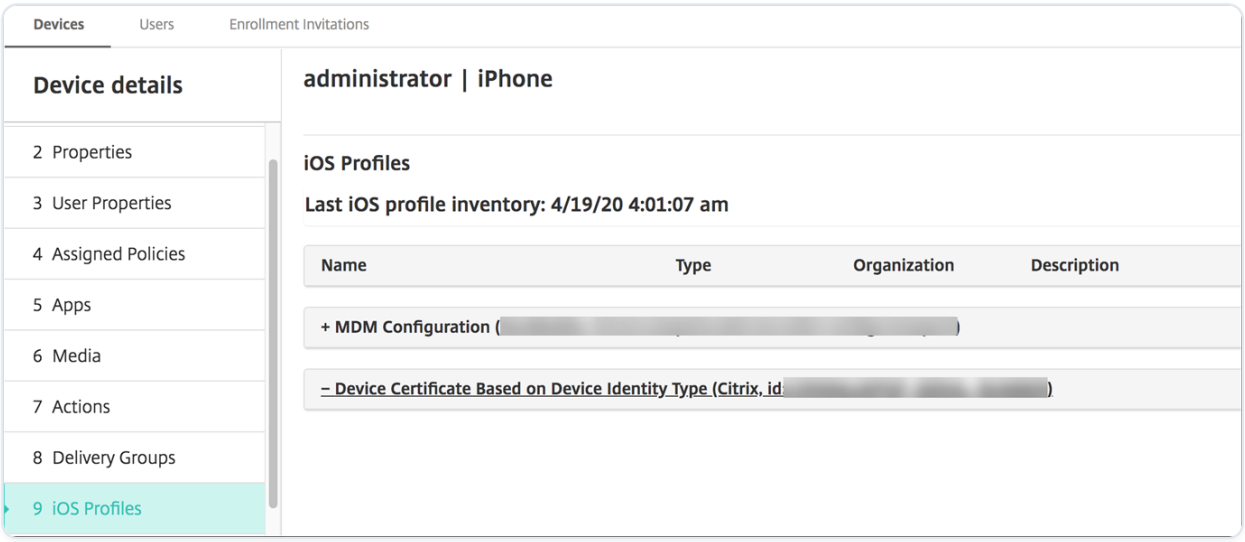


6. Cree una directiva VPN con el tipo de credencial **Always on IKEv2** y el método de autenticación de dispositivo **Device Certificate Based on Device Identity**. Seleccione el **tipo**

de identidad de dispositivo que utilizó en los nombres de archivo de su certificado. Consulte Directiva de dispositivo VPN.

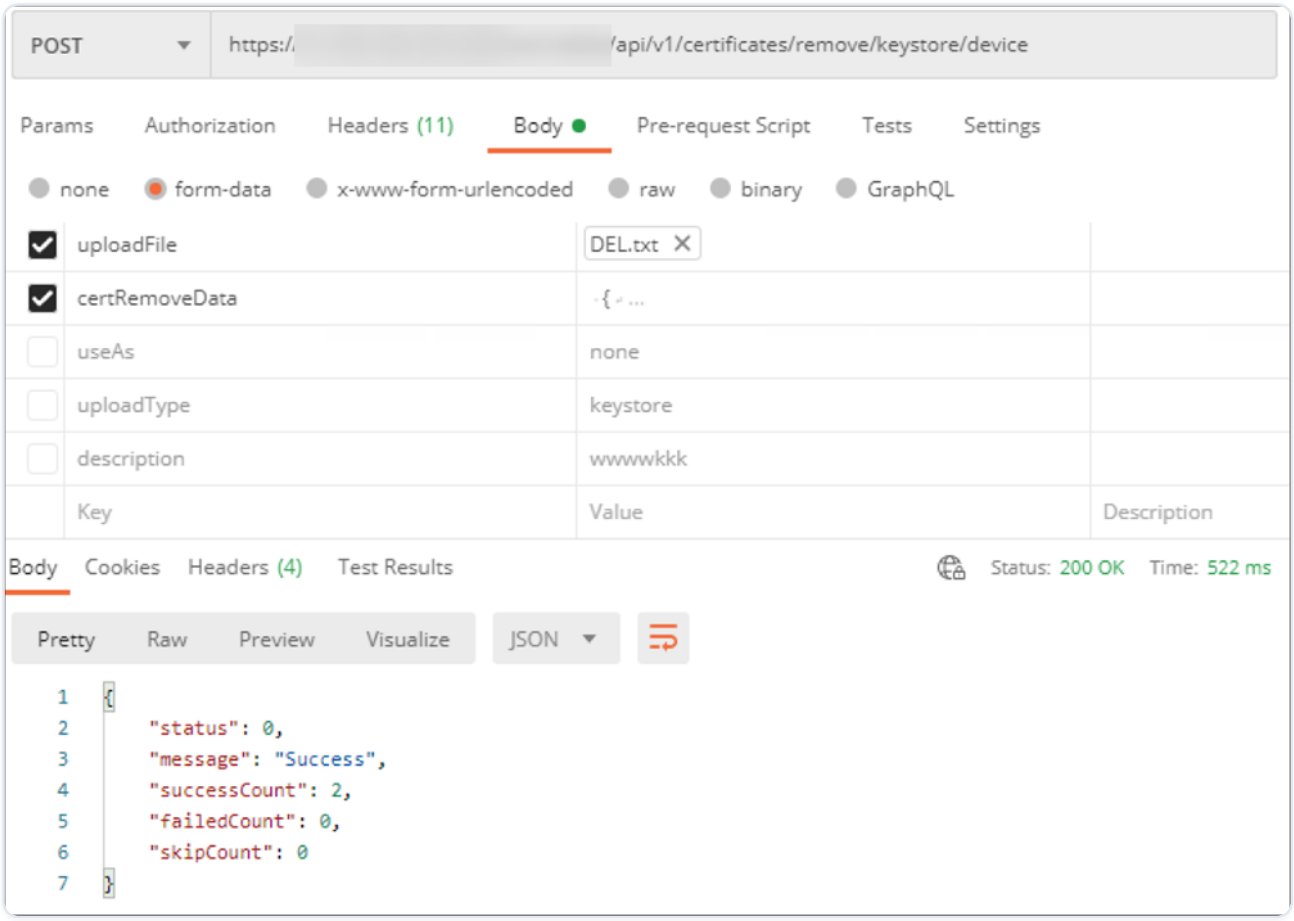
7. Inscriba un dispositivo iOS y espere a que se implemente la directiva VPN. Confirme la instalación del certificado comprobando la configuración de MDM en el dispositivo. También puede comprobar los detalles del dispositivo en la consola de Citrix Endpoint Management.





También puede eliminar certificados de forma masiva creando un archivo de texto con los `device_identity_value` enumerados para cada certificado que desee eliminar. En la API REST, llame a la API de eliminación y utilice la siguiente solicitud, reemplazando `device_identity_value` con el identificador apropiado:

```
{
    "identityType"="device_identity_value"
}
```



Actualizar un certificado

Citrix Endpoint Management solo permite que exista un certificado por clave pública en el sistema a la vez. Si intenta importar un certificado para el mismo par de claves que un certificado ya importado, puede:

- Reemplazar la entrada existente.
- Eliminar la entrada.

Después de cargar un nuevo certificado para reemplazar uno antiguo, no puede eliminar el certificado antiguo. Al configurar el ajuste Entidades PKI, ambos certificados existen en el menú **Certificado de cliente SSL**. El certificado más reciente aparece más abajo en la lista que el certificado antiguo.

Para actualizar sus certificados

1. Cree un certificado de reemplazo siguiendo los pasos de Certificado de cliente o certificado más autenticación de dominio.

> **Importante:**

> No utilice la opción de crear un certificado con la clave privada existente. Cuando crea un certificado para actualizar uno que está a punto de caducar, la clave privada también debe ser nueva.

2. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha de la consola. Utilice la barra de búsqueda para buscar y abrir el ajuste **Certificados**.
3. En el cuadro de diálogo **Importar**, importe el nuevo certificado.

Cuando actualiza un certificado de servidor, los componentes que utilizan el certificado anterior cambian automáticamente al nuevo certificado. Del mismo modo, si ha implementado el certificado de servidor en dispositivos, el certificado se actualiza automáticamente en la siguiente implementación.

Para actualizar un certificado APNs, siga los pasos para crear un certificado y, a continuación, vaya al portal de certificados push de Apple. Para obtener más información, consulte Renovar un certificado APNs.

Si su NetScaler Gateway está configurado para la descarga SSL, asegúrese de actualizar su equilibrador de carga con el nuevo cacert.pem.

> **Nota:**
>
> Si ha migrado de XenMobile local a Citrix Endpoint Management y está actualizando su certificado, póngase en contacto con el Soporte de Citrix después de completar los pasos anteriores. Deberá proporcionarles una copia del nuevo certificado (en formato PFX), incluida la contraseña del certificado. El Soporte de Citrix actualiza el NetScaler en la nube y reinicia los nodos de inquilino para finalizar el proceso de actualización del certificado.

Para actualizar una autoridad de certificación (CA) del servicio PKI

Puede solicitar a Citrix Cloud Operations que actualice o regenere las autoridades de certificación (CA) PKI internas en su implementación de Citrix Endpoint Management. Abra un caso de Soporte técnico para estas solicitudes.

```
When the new CAs are available, Cloud Operations lets you know that you
can proceed with renewing the device certificates for your users.
```

Renovar certificados de dispositivo

Si un certificado de un dispositivo caduca, el certificado deja de ser válido. Ya no podrá ejecutar transacciones seguras en su entorno ni acceder a los recursos de Citrix Endpoint Management. La Autoridad de certificación (CA) le pide que renueve su certificado SSL antes de la fecha de caducidad. Siga los pasos descritos anteriormente para actualizar el certificado y, a continuación, inicie una renovación de certificados en los dispositivos inscritos.

Para los dispositivos iOS, macOS y Android compatibles, puede iniciar la renovación de certificados a través de la acción de seguridad, Renovación de certificados. Puede renovar los certificados de dispositivo desde la consola de Citrix Endpoint Management o la API REST pública. Para los dispositivos Windows inscritos, los usuarios deben volver a inscribir sus dispositivos para recibir una nueva autoridad de certificación de dispositivos (CA).

La próxima vez que los dispositivos se conecten de nuevo a Citrix Endpoint Management, el servidor de Citrix Endpoint Management emitirá nuevos certificados de dispositivo basados en la nueva CA.

Para renovar certificados de dispositivo mediante la consola

1. Vaya a **Administrar > Dispositivos** y seleccione los dispositivos para los que quiere renovar los certificados de dispositivo.
2. Haga clic en **Proteger** y, a continuación, en **Renovación de certificados**.

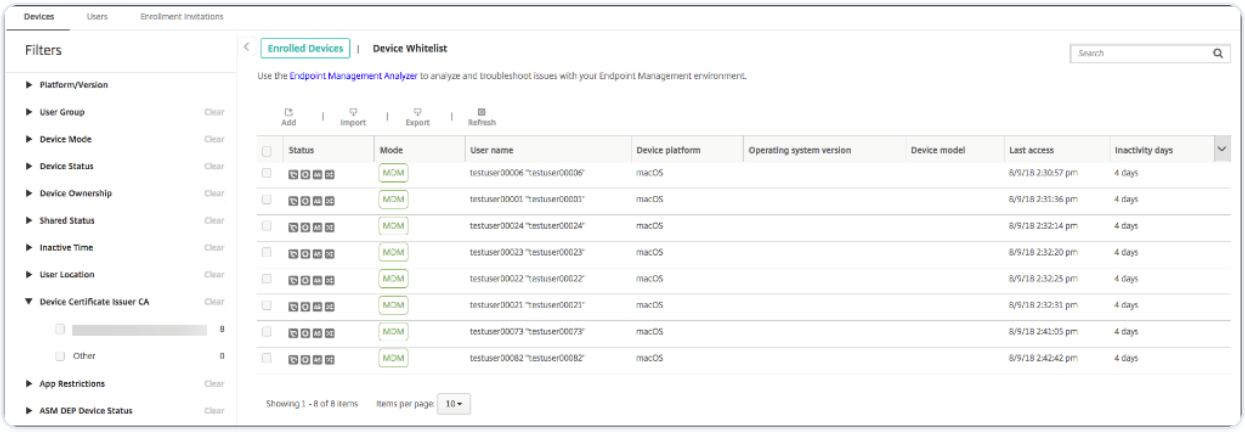


Los dispositivos inscritos siguen funcionando sin interrupciones. Citrix Endpoint Management emite un certificado de dispositivo cuando un dispositivo se conecta de nuevo al servidor.

Para consultar los dispositivos que se encuentran en un grupo de CA emisor de certificados de dispositivo específico:

1. En **Administrar > Dispositivos**, expanda el panel de **Filtros**.
2. En el panel de **Filtros**, expanda **CA emisor de certificados de dispositivo** y, a continuación, seleccione las CA emisoras que quiere renovar.

   En la tabla de dispositivos, aparecen los dispositivos de las CA emisoras seleccionadas.



Para renovar certificados de dispositivo mediante la API REST

Citrix Endpoint Management utiliza las siguientes autoridades de certificación (CA) internamente para PKI: CA raíz, CA de dispositivo y CA de servidor. Esas CA son un grupo lógico y tienen un nombre de grupo. Durante el aprovisionamiento de Citrix Endpoint Management, el servidor genera tres CA y les asigna el nombre de grupo «default».

La CA emite las siguientes API para administrar y renovar los certificados de dispositivo. Los dispositivos ya inscritos siguen funcionando sin interrupciones. Citrix Endpoint Management emite un certificado de dispositivo cuando un dispositivo se conecta de nuevo al servidor. Para obtener más información, descargue el PDF (/es-es/citrix-endpoint-management/downloads/public-rest-api.pdf).

- Devolver una lista de dispositivos que aún utilizan la CA antigua (consulte la sección 3.16.2 del PDF de la API pública para servicios REST)
- Renovar certificado de dispositivo (consulte la sección 3.16.58)
- Obtener todos los grupos de CA (consulte la sección 3.23.1)

Certificado APNs para Citrix Secure Mail

Los certificados del Servicio de notificaciones push de Apple (APNs) caducan cada año. Asegúrese de crear un certificado SSL de APNs y actualizarlo en el portal de Citrix antes de que caduque el certificado. Si el certificado caduca, los usuarios experimentarán inconsistencias con las notificaciones push de Citrix Secure Mail. Además, ya no podrá enviar notificaciones push para sus aplicaciones.

Certificado APNs para la administración de dispositivos iOS

Para inscribir y administrar dispositivos iOS con Citrix Endpoint Management, configure y cree un certificado APNs de Apple. Si el certificado caduca, los usuarios no podrán inscribirse en Citrix Endpoint Management y usted no podrá administrar sus dispositivos iOS. Para obtener más información, consulte (/es-es/citrix-endpoint-management/authentication/apns.html).

Puede ver el estado del certificado APNs y la fecha de caducidad iniciando sesión en el portal de certificados push de Apple. Asegúrese de iniciar sesión con el mismo usuario que creó el certificado.

También recibirá una notificación por correo electrónico de Apple 30 y 10 días antes de la fecha de caducidad. La notificación incluye la siguiente información:

```
The following Apple Push Notification Service certificate, created for
Apple ID CustomerID will expire on Date. Revoking or allowing this
certificate to expire will require existing devices to be re-enrolled with
a new push certificate.



Please contact your vendor to generate a new request (a signed CSR), then
visit https://identity.apple.com/pushcert to renew your Apple Push
Notification Service certificate.



Thank You,



Apple Push Notification Service
```

MDX Toolkit (certificado de distribución de iOS)

Una aplicación que se ejecuta en un dispositivo iOS físico (que no sean aplicaciones de la App Store de Apple) tiene estos requisitos de firma:

- Firme la aplicación con un perfil de aprovisionamiento.
- Firme la aplicación con un certificado de distribución correspondiente.

Para verificar que tiene un certificado de distribución de iOS válido, haga lo siguiente:

1. Desde el portal de desarrolladores empresariales de Apple, cree un ID de aplicación explícito para cada aplicación que planee empaquetar con MDX. Un ejemplo de ID de aplicación aceptable es: `com.CompanyName.ProductName`.
2. Desde el portal de desarrolladores empresariales de Apple, vaya a **Perfiles de aprovisionamiento > Distribución** y cree un perfil de aprovisionamiento interno. Repita este paso para cada ID de aplicación creado en el paso anterior.
3. Descargue todos los perfiles de aprovisionamiento. Para obtener más información, consulte Empaquetar aplicaciones móviles iOS.

Para confirmar que todos los certificados del servidor de Citrix Endpoint Management son válidos, haga lo siguiente:

1. En la consola de Citrix Endpoint Management, haga clic en **Configuración > Certificados**.
2. Compruebe que todos los certificados, incluidos los de APNs, SSL Listener, raíz e intermedios, son válidos.

Almacén de claves de Android

El almacén de claves es un archivo que contiene los certificados utilizados para firmar su aplicación Android. Cuando el período de validez de su clave caduca, los usuarios ya no pueden actualizar sin problemas a nuevas versiones de su aplicación.

NetScaler Gateway

Para obtener más información sobre cómo gestionar la caducidad de certificados para NetScaler Gateway, consulte Cómo gestionar la caducidad de certificados en NetScaler en el Centro de conocimientos de asistencia de Citrix.

Un certificado de NetScaler Gateway caducado impide que los usuarios se inscriban y accedan a Store. El certificado caducado también impide que los usuarios se conecten a Exchange Server cuando utilizan Citrix Secure Mail. Además, los usuarios no pueden enumerar ni abrir aplicaciones HDX (dependiendo de qué certificado haya caducado).

Expiry Monitor y Command Center pueden ayudarle a realizar un seguimiento de sus certificados de NetScaler Gateway. El Centro le notifica cuando el certificado caduca. Estas herramientas ayudan a supervisar los siguientes certificados de NetScaler Gateway:

- Certificado SSL para FQDN de MDM
- Certificado SSL para FQDN de Gateway
- Certificado SSL para FQDN de ShareFile SZC

- Certificado SSL para el equilibrio de carga de Exchange (configuración de descarga)
- Certificado SSL para el equilibrio de carga de StoreFront
- Certificados de CA raíz e intermedios para los certificados anteriores

NetScaler Gateway y Citrix Endpoint Management

Cuando se integra con Citrix Endpoint Management, NetScaler Gateway proporciona acceso remoto a dispositivos a su red y recursos internos. Citrix Endpoint Management crea una micro VPN desde las aplicaciones del dispositivo hasta NetScaler Gateway.

Puede utilizar el servicio Citrix Gateway (Vista previa) o NetScaler Gateway local, también conocido como NetScaler Gateway. Para obtener una descripción general de las dos soluciones de NetScaler Gateway, consulte Configurar el uso de NetScaler Gateway con Citrix Endpoint Management.

Configurar la autenticación para el acceso remoto de dispositivos a la red interna

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha de la consola. Aparece la página **Configuración**.
2. En **Servidor**, haga clic en **NetScaler Gateway**. Aparece la página **NetScaler Gateway**. En el siguiente ejemplo, existe una instancia de NetScaler Gateway.



3. Configure estos ajustes:
   - **Autenticación:** Seleccione si desea habilitar la autenticación. El valor predeterminado es **Activado**.
   - **Entregar certificado de usuario para autenticación:** Seleccione si desea que Citrix Endpoint Management comparta el certificado de autenticación con Citrix Secure Hub. Compartir el certificado permite a NetScaler Gateway gestionar la autenticación de certificado de cliente. El valor predeterminado es **Desactivado**.
   - **Proveedor de credenciales:** Haga clic en el proveedor de credenciales que desea usar en la lista desplegable. Para obtener más información, consulte Proveedores de credenciales.
4. Haga clic en **Guardar**.

Agregar una instancia del servicio Citrix Gateway (Vista previa)

Después de guardar la configuración de autenticación, agregue una instancia de NetScaler Gateway a Citrix Endpoint Management.

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha. Se abre la página **Configuración**.
2. En la página **Configuración**, desplácese hasta el mosaico de NetScaler Gateway y, a continuación, haga clic en **Iniciar configuración**. Aparece la página **NetScaler Gateway**.
3. Seleccione **Servicio Citrix Gateway (nube)** y especifique la ubicación de recursos para el servicio Gateway.

   Pantalla de configuración de NetScaler Gateway(/en-us/citrix-endpoint-management/media/settings-add-gateway-service.png)

   - **Ubicación de recursos para el servicio Gateway:** es necesaria si utiliza Citrix Secure Mail. Especifique la ubicación de recursos para el servicio STA. La ubicación de recursos debe incluir un NetScaler Gateway configurado. Si más adelante desea eliminar una ubicación de recursos configurada para el servicio Gateway, actualice esta configuración.

   Después de completar esos ajustes, haga clic en **Conectar** para establecer la conexión. Se agrega el nuevo NetScaler Gateway. El mosaico **Servicio Citrix Gateway (nube)** aparece en la página **Configuración**. Para editar una instancia, haga clic en **Ver más**. Si los conectores de Gateway no están disponibles en la ubicación de recursos seleccionada, haga clic en **Agregar conector de Gateway**. Siga las instrucciones en pantalla para instalar los conectores de Gateway. También puede agregar conectores de Gateway más tarde.
4. Haga clic en **Guardar y exportar script**.

   - **Guardar y exportar script**. Haga clic en el botón para guardar la configuración y exportar un paquete de configuración. Puede cargar un script del paquete en NetScaler Gateway para configurarlo con los ajustes de Citrix Endpoint Management. Para obtener más información, consulte "Configurar un NetScaler Gateway local para usarlo con Citrix Endpoint Management" después de estos pasos.

   Ha agregado el nuevo NetScaler Gateway. El mosaico **NetScaler Gateway** aparece en la página **Configuración**. Para editar una instancia, haga clic en **Ver más**.

Configurar un NetScaler Gateway local para usarlo con Citrix Endpoint Management

Para configurar un NetScaler Gateway local para usarlo con Citrix Endpoint Management, siga los pasos generales que se detallan en las siguientes secciones.

1. verificar que su entorno cumple los requisitos previos.
2. Exporte el paquete de scripts desde la consola de Citrix Endpoint Management.
3. Extraiga los archivos del paquete. Si solo utiliza directivas clásicas en NetScaler Gateway y ejecuta Citrix ADC 13.0 o anterior, utilice el script con "Classic" en el nombre del archivo. Si utiliza directivas avanzadas o ejecuta Citrix ADC 13.1 o posterior, utilice el script con "Advanced" en el nombre del archivo.
4. Ejecute el script adecuado en NetScaler Gateway. Consulte el archivo Léame proporcionado con los scripts para obtener las últimas instrucciones detalladas.
5. Pruebe la configuración.

Los scripts configuran estos ajustes de NetScaler Gateway necesarios para Citrix Endpoint Management:

- Servidores virtuales de NetScaler Gateway necesarios para MDM y MAM
- Directivas de sesión para los servidores virtuales de NetScaler Gateway
- Detalles del servidor de Citrix Endpoint Management
- Balanceador de carga proxy para la validación de certificados
- Directivas y acciones de autenticación para el servidor virtual de NetScaler Gateway. Los scripts describen la configuración de LDAP.
- Acciones y directivas de tráfico para el servidor proxy
- Perfil de acceso sin cliente
- Registro DNS local estático en NetScaler Gateway
- Otras vinculaciones: Directiva de servicio, certificado de CA

Los scripts no gestionan la siguiente configuración:

- Equilibrio de carga de Exchange
- Equilibrio de carga de Citrix Files
- Configuración de proxy ICA®
- Descarga SSL

Requisitos previos para usar los scripts de configuración de NetScaler Gateway

Requisitos de Citrix Endpoint Management:

- Complete la configuración de LDAP y NetScaler Gateway en Citrix Endpoint Management antes de exportar el paquete de scripts. Si cambia la configuración, exporte el paquete de scripts de nuevo.

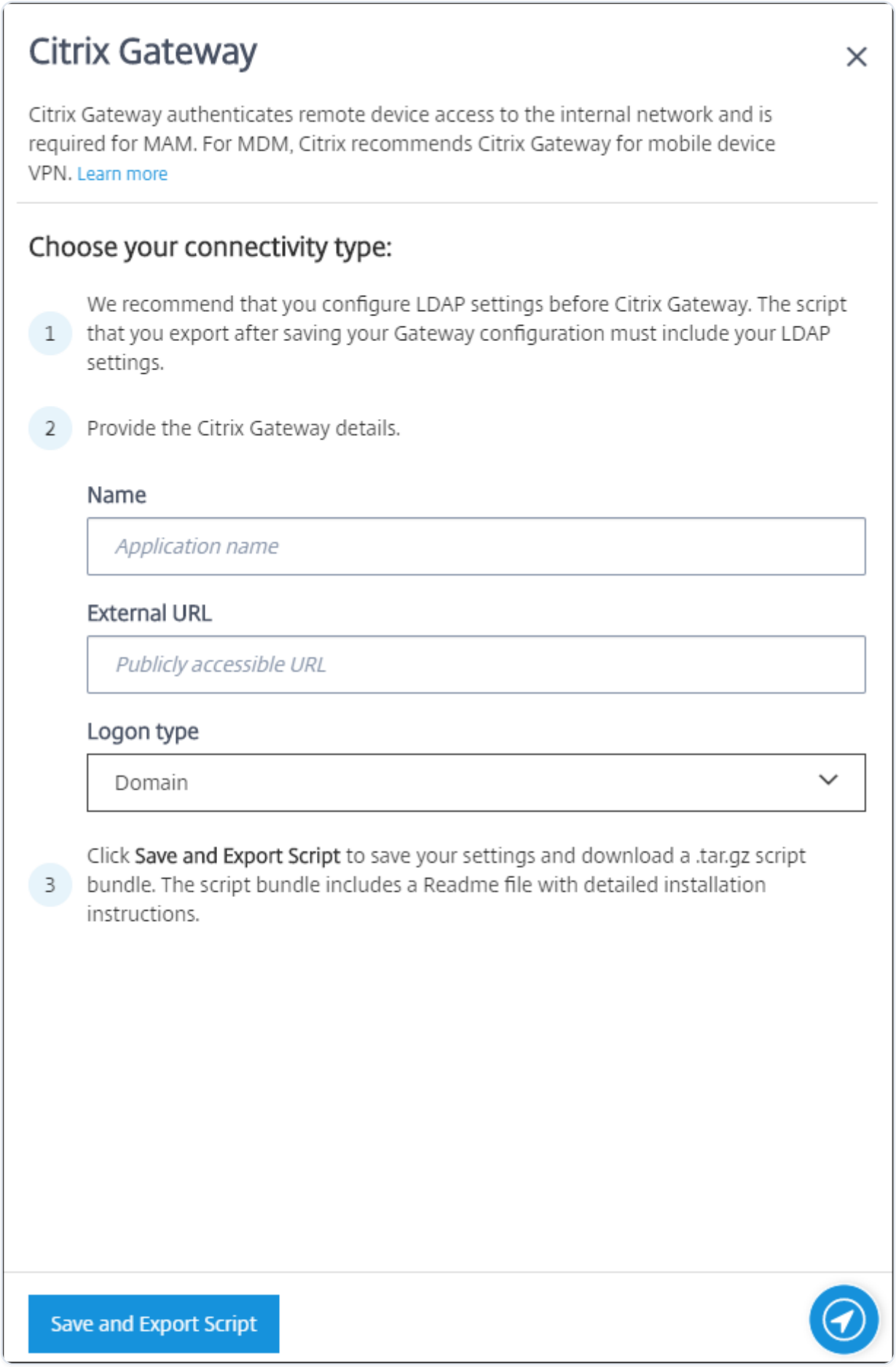
Requisitos de NetScaler Gateway:

- Cuando utilice la autenticación basada en certificados en NetScaler Gateway, debe crear certificados SSL en un dispositivo Citrix ADC. Consulte (/es-es/citrix-adc/13/ssl/how-to-articles/create-and-use-ssl-certificates-on-a-citrix-adc-appliance.html).
- NetScaler Gateway (versión mínima 11.0, compilación 70.12).
- La dirección IP de NetScaler Gateway está configurada y tiene conectividad con el servidor LDAP, a menos que LDAP esté equilibrado de carga.
- La dirección IP de la subred (SNIP) de NetScaler Gateway está configurada, tiene conectividad con los servidores back-end necesarios y tiene acceso a la red pública a través del puerto 8443/TCP.
- DNS puede resolver dominios públicos.
- NetScaler Gateway tiene licencias de plataforma/universal o de prueba. Para obtener más información, consulte `<https://support.citrix.com/article/CTX126049>`.

Exportar el paquete de scripts desde Citrix Endpoint Management

Después de guardar la configuración de autenticación, agregue una instancia de NetScaler Gateway a Citrix Endpoint Management.

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha. Se abre la página **Configuración**.
2. En la página **Configuración**, desplácese hasta el mosaico de NetScaler Gateway y, a continuación, haga clic en **Iniciar configuración**. Aparece la página **NetScaler Gateway**.
3. Seleccione **NetScaler Gateway (local)** y configure estos ajustes:



- **Nombre:** Escriba un nombre para la instancia de NetScaler Gateway.

- **URL externa:** Escriba la URL de acceso público para NetScaler Gateway. Por ejemplo, `https://receiver.com`.
- **Tipo de inicio de sesión:** Elija un tipo de inicio de sesión. Los tipos incluyen: **Dominio**, **Solo token de seguridad**, **Dominio y token de seguridad**, **Certificado**, **Certificado y dominio**, y **Certificado y token de seguridad**. El valor predeterminado es **Dominio**.

Si tiene varios dominios, utilice **Certificado y dominio**. Para obtener más información, consulte Configurar la autenticación para varios dominios.

La autenticación basada en certificados en NetScaler Gateway requiere una configuración adicional. Por ejemplo, debe cargar su certificado de CA raíz en su dispositivo Citrix ADC. Consulte Crear y usar certificados SSL en un dispositivo Citrix ADC.

Para obtener más información, consulte Autenticación en el Manual de implementación.

4. Haga clic en **Guardar y exportar script**.

   - **Guardar y exportar script**. Haga clic en el botón para guardar la configuración y exportar un paquete de configuración. Puede cargar un script del paquete en NetScaler Gateway para configurarlo con los ajustes de Citrix Endpoint Management. Para obtener información, consulte "Configurar un NetScaler Gateway local para usarlo con Citrix Endpoint Management" después de estos pasos.

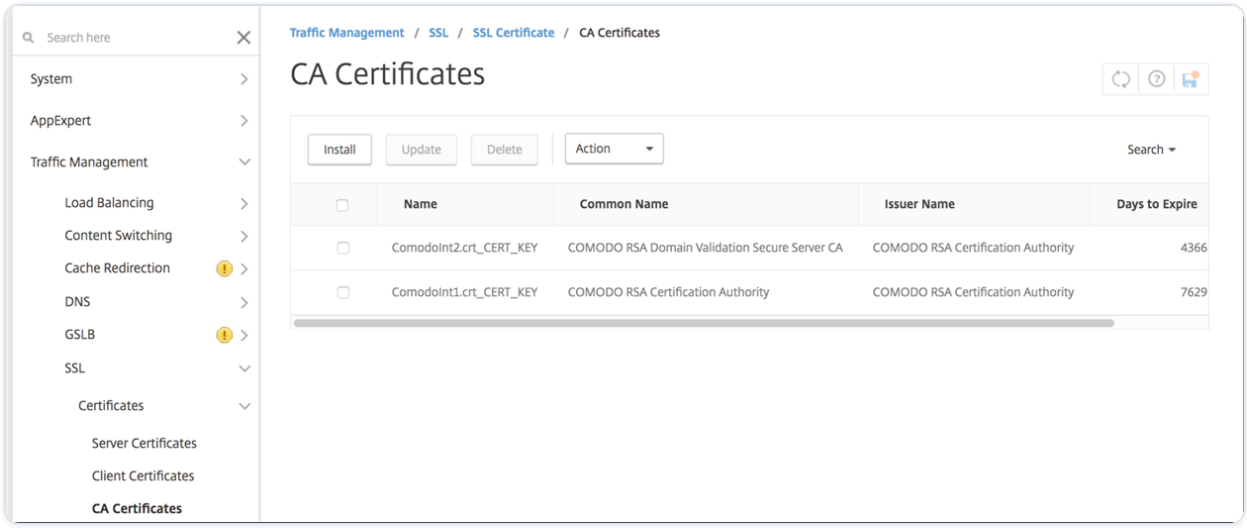
   Ha agregado el nuevo NetScaler Gateway. El mosaico de **NetScaler Gateway** aparece en la página **Configuración**. Para modificar una instancia, haga clic en **Ver más**.

Instalar el script en su entorno

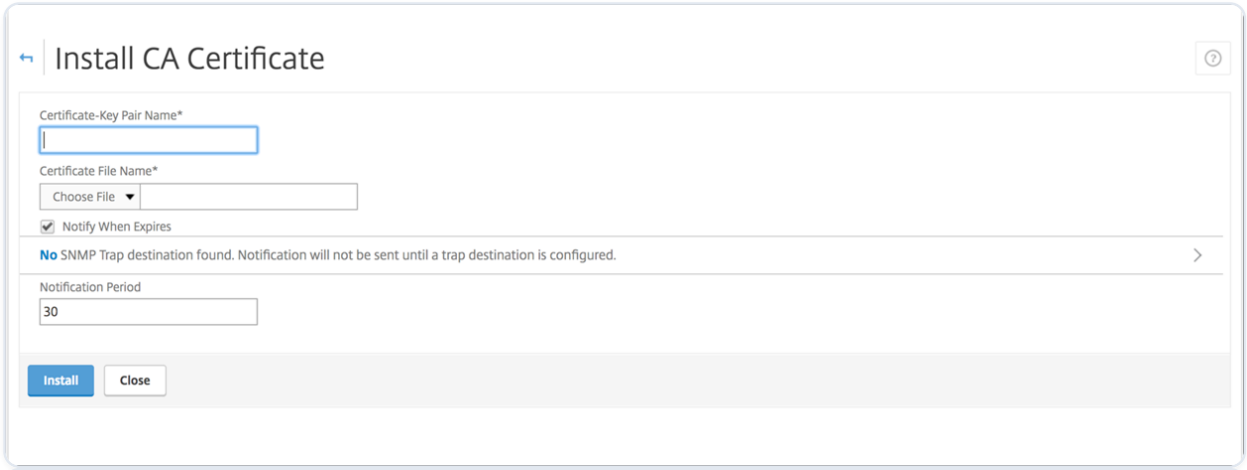
El paquete de scripts incluye lo siguiente.

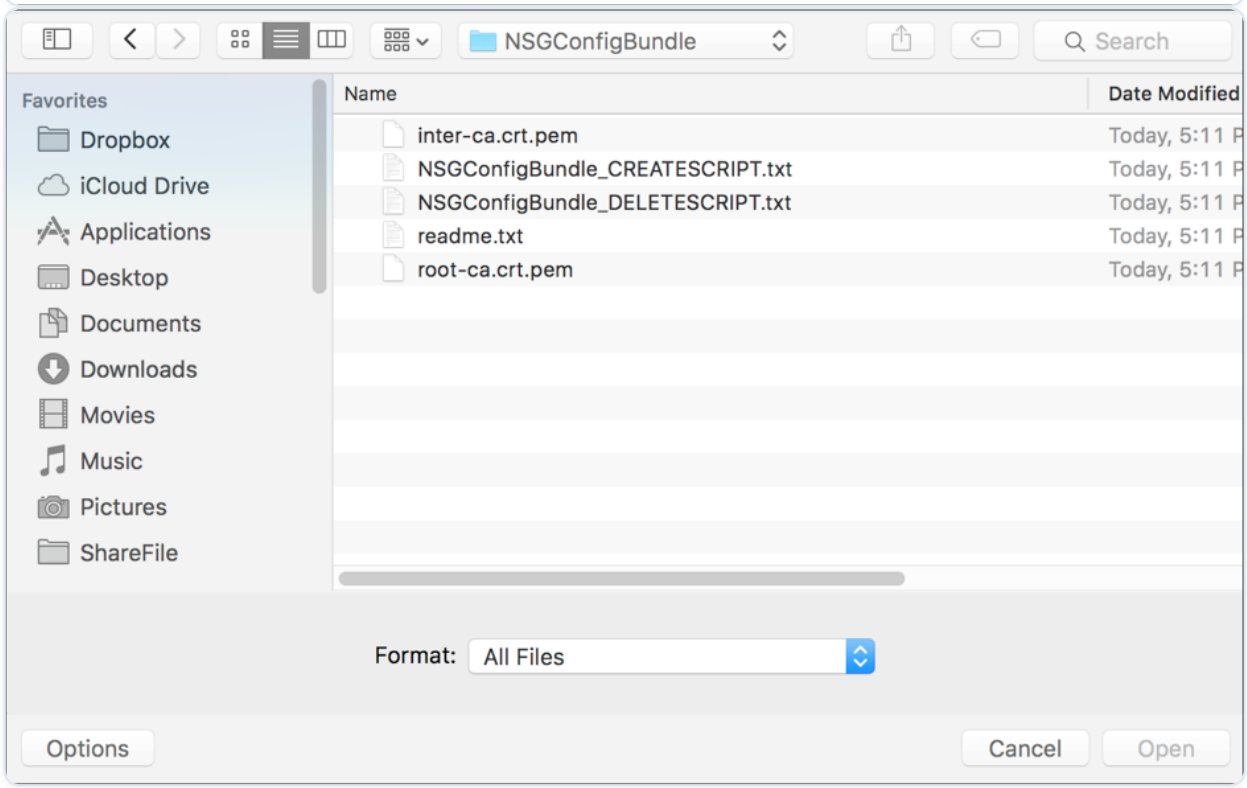
- Archivo Léame con instrucciones detalladas
- Scripts que contienen los comandos de la CLI de NetScaler® utilizados para configurar los componentes necesarios en NetScaler
- Certificado de CA raíz pública y certificado de CA intermedia
- Scripts que contienen los comandos de la CLI de NetScaler utilizados para eliminar la configuración de NetScaler

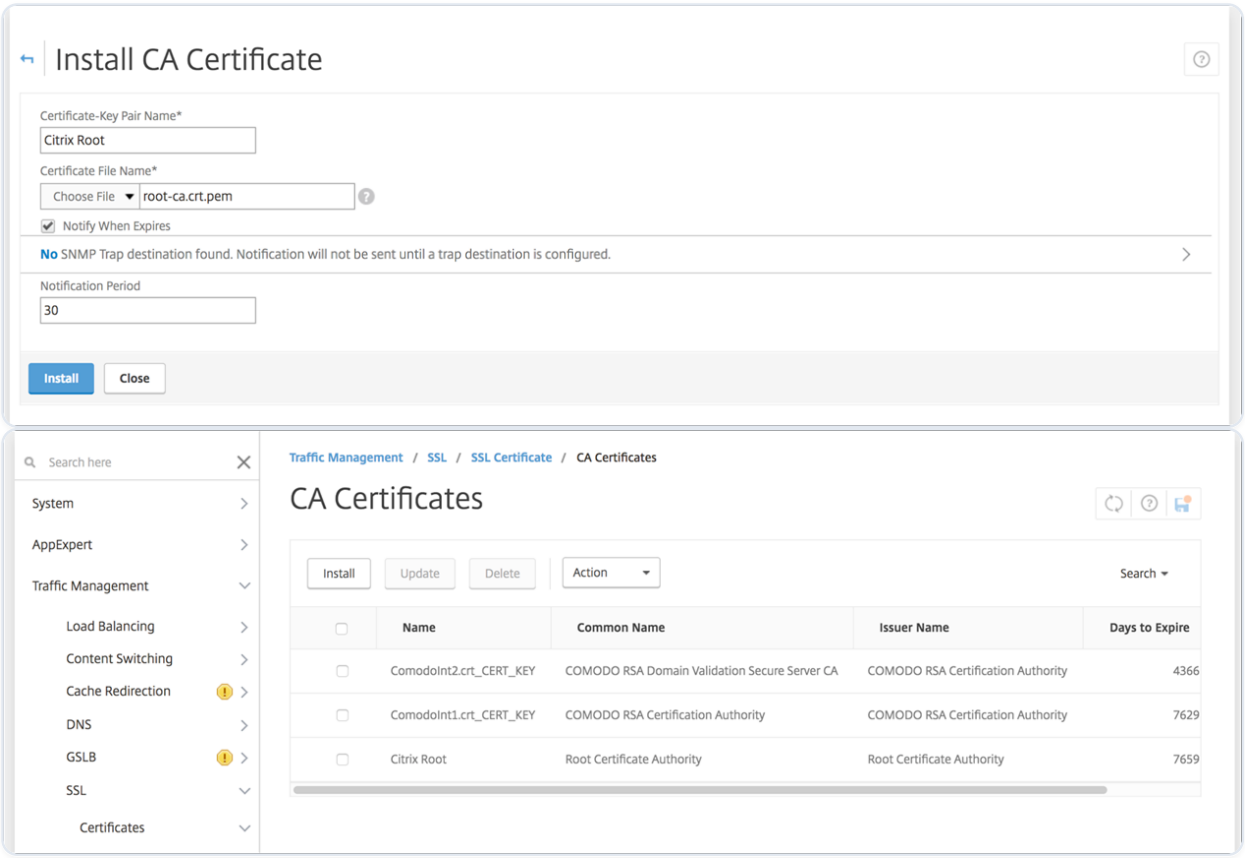
1. Cargue e instale los archivos de certificado (proporcionados en el paquete de scripts) en el dispositivo Citrix ADC en el directorio /nsconfig/ssl/. Consulte Crear y usar certificados SSL en un dispositivo Citrix ADC.



Los siguientes ejemplos muestran cómo instalar el certificado raíz.







Asegúrese de instalar los certificados raíz e intermedio.

2. Edite el script (ConfigureCitrixGatewayScript_Classic.txt o ConfigureCitrixGatewayScript_Advanced.txt) para reemplazar todos los marcadores de posición con los detalles de su entorno.

```
#Important Note: Please update the following placeholders with valid values:
# <NSG_IP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reachable from your devices either directly or via a NAT.
# <PROXY_LB_VIP> -- Virtual IP Address to be assigned to the proxy load-balancer configured on the NetScaler. This IP address must be a private address.
# <LDAP_SVC_USERNAME> -- LDAP Service Account Username.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <SERVER_CERT_NAME> -- Name of the server certificate file on the NetScaler. This certificate is bound to the NetScaler Gateway virtual server.
```

3. Ejecute el script editado en el shell bash de NetScaler, como se describe en el archivo readme incluido en el paquete de scripts. Por ejemplo:

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management Password> batch -f "/var/OfflineNSGConfigtBundle_CREATESCRIPT.txt"
```

```
login as: nsroot
################################################################################
#                                                                              #
#        WARNING: Access to this system is for authorized users only           #
#         Disconnect IMMEDIATELY if you are not an authorized user!            #
#                                                                              #
################################################################################

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

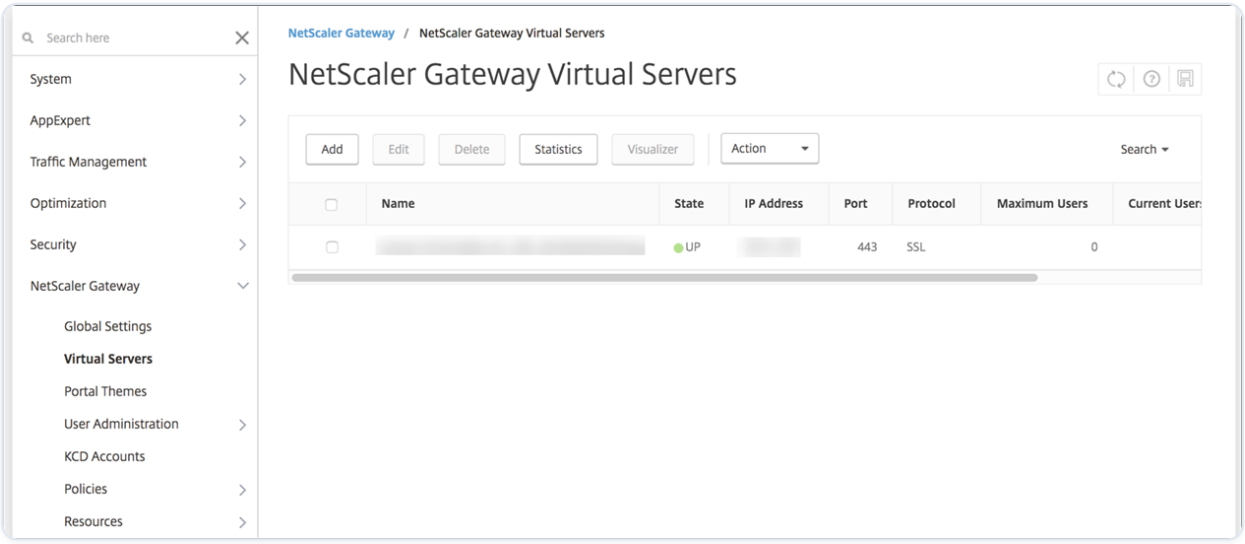
Cuando el script finaliza, aparecen las siguientes líneas.

```
exec: save ns config
 Done
 Done
root@ns#
```

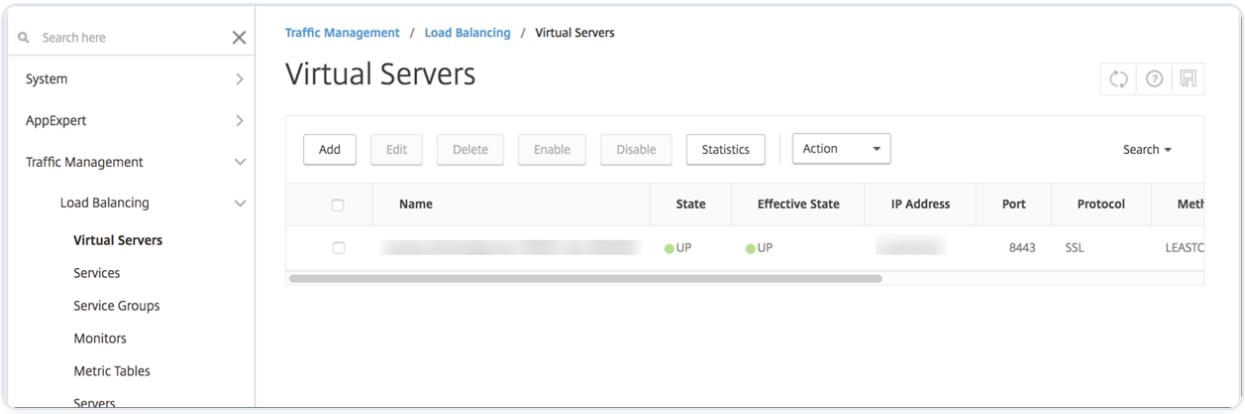
Probar la configuración

Para validar la configuración:

1. Valide que el servidor virtual de NetScaler Gateway muestre un estado de **UP**.



2. Valide que el servidor virtual de equilibrio de carga de proxy muestre un estado de **UP**.



3. Abra un explorador web, conéctese a la URL de NetScaler Gateway e intente autenticarse. Si la autenticación se realiza correctamente, se le redirigirá a un mensaje de "HTTP Status 404 - Not Found".
4. Inscriba un dispositivo y asegúrese de que obtenga la inscripción de MDM y MAM.

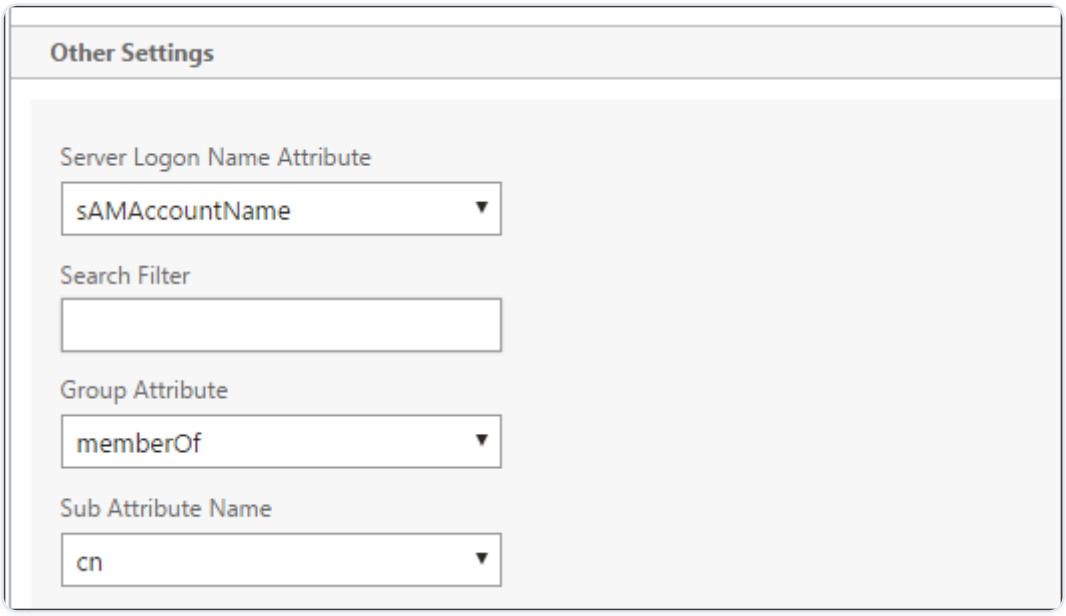
Configurar la autenticación para varios dominios

Si tiene varias instancias de Citrix Endpoint Management, como para entornos de prueba, desarrollo y producción, debe configurar NetScaler Gateway para los entornos adicionales manualmente. (Solo puede usar el asistente de NetScaler para XenMobile una vez).

Configuración de NetScaler Gateway

Para configurar las directivas de autenticación de NetScaler Gateway y una directiva de sesión para un entorno multidominio:

1. En la utilidad de configuración de NetScaler Gateway, en la pestaña **Configuration**, expanda **NetScaler Gateway > Policies > Authentication**.
2. En el panel de navegación, haga clic en **LDAP**.
3. Haga clic para editar el perfil LDAP. Cambie el **Server Logon Name Attribute** a **userPrincipalName** o al atributo que desee usar para las búsquedas. Anote los atributos que especifique. Los proporcionará al configurar los ajustes de LDAP en la consola de Citrix Endpoint Management.

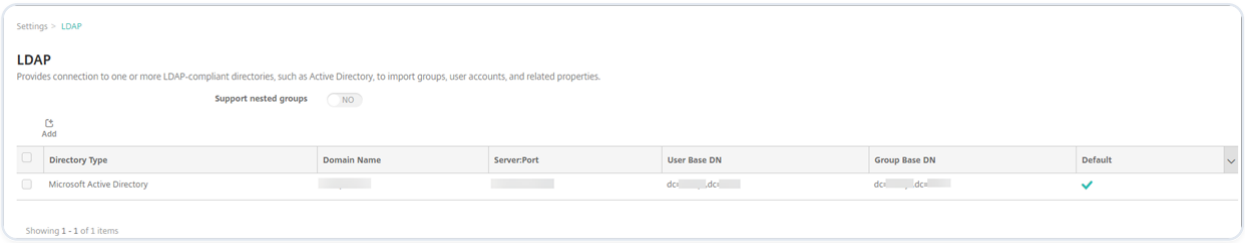


4. Repita esos pasos para cada directiva LDAP. Se requiere una directiva LDAP independiente para cada dominio.
5. En la directiva de sesión vinculada al servidor virtual de NetScaler Gateway, vaya a **Edit session profile > Published Applications**. Asegúrese de que **Single Sign-On Domain** esté en blanco.

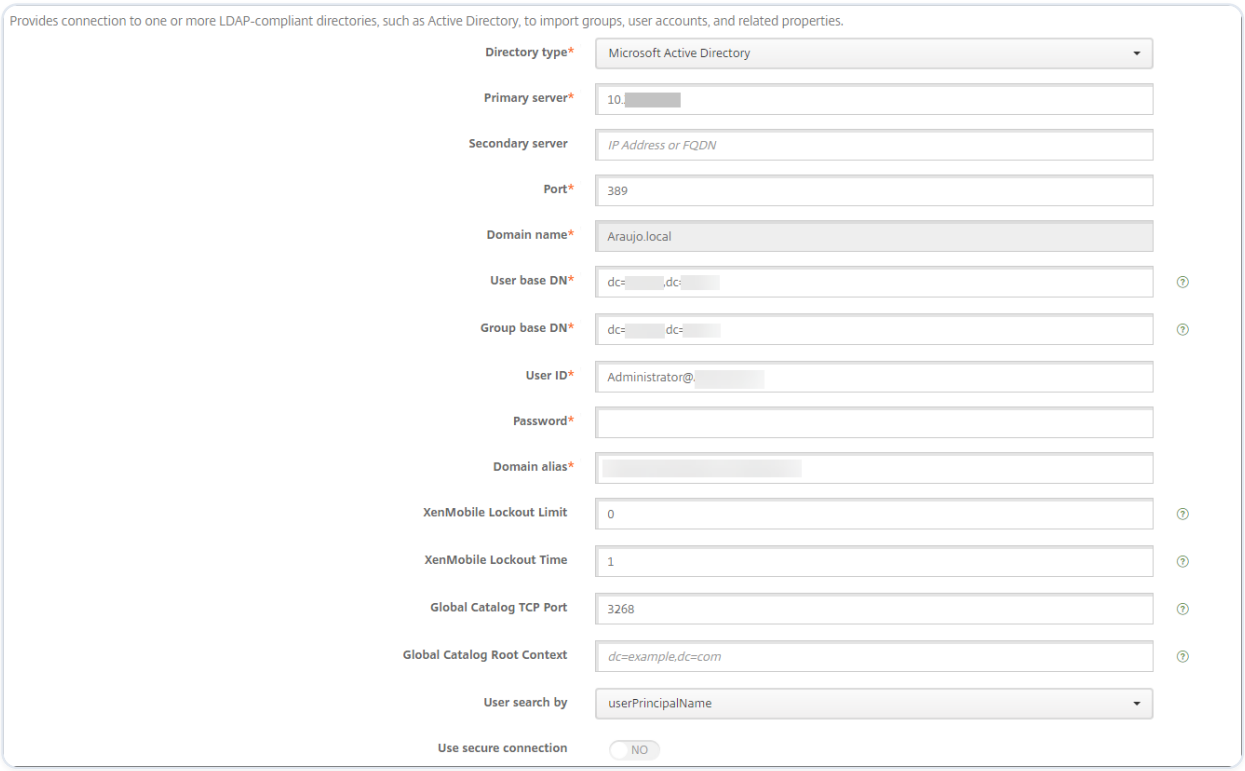
Configuración de Citrix Endpoint Management

Para configurar LDAP de Citrix Endpoint Management para un entorno de varios dominios:

1. En la consola de Citrix Endpoint Management, vaya a **Settings > LDAP** y agregue o edite un directorio.



2. Proporcione la información.
   - En **Domain Alias**, especifique cada dominio que se utilizará para la autenticación de usuarios. Separe los dominios con una coma y no use espacios entre ellos. Por ejemplo: domain1.com,domain2.com,domain3.com
   - Asegúrese de que el campo **User search by** coincida con el **Server Logon Name Attribute** especificado en la directiva LDAP de NetScaler Gateway.



Eliminar solicitudes de conexión entrantes a URL específicas

Si NetScaler Gateway de su entorno está configurado para la descarga SSL, es posible que prefiera que el gateway elimine las solicitudes de conexión entrantes para URL específicas. Si prefiere esa seguridad adicional, póngase en contacto con Operaciones de Citrix Cloud y solicite que permitan su IP a sus centros de datos locales.

Autenticación de dominio o de dominio más token de seguridad

Citrix Endpoint Management admite la autenticación basada en dominio en uno o varios directorios que cumplen con el Protocolo ligero de acceso a directorios (LDAP). Se configura una conexión en Citrix Endpoint Management a uno o varios directorios. Citrix Endpoint Management utiliza la configuración de LDAP para importar grupos, cuentas de usuario y propiedades relacionadas.

> **Importante:**
>
> Citrix Endpoint Management no admite el cambio del modo de autenticación de un tipo a otro después de que los usuarios inscriban dispositivos en Citrix Endpoint Management. Por ejemplo, no se puede cambiar el modo de autenticación de **Autenticación de dominio** a **Dominio + Certificado** después de que los usuarios se hayan inscrito.

Acerca de LDAP

LDAP es un protocolo de aplicación de código abierto e independiente del proveedor para acceder y mantener servicios de información de directorio distribuidos a través de una red de Protocolo de Internet (IP). Los servicios de información de directorio se utilizan para compartir información sobre usuarios, sistemas, redes, servicios y aplicaciones disponibles en toda la red.

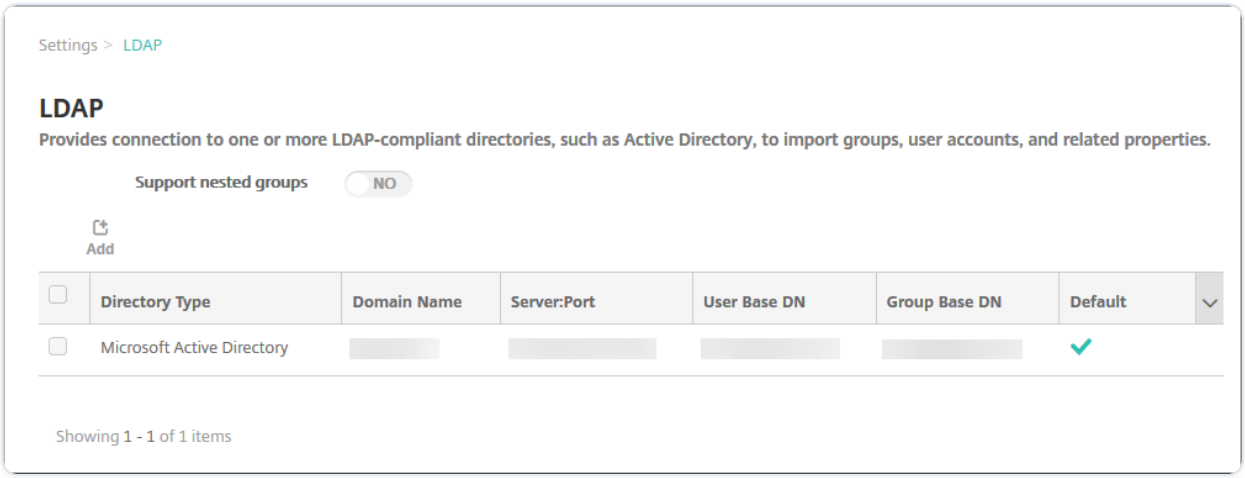
Un uso común de LDAP es proporcionar inicio de sesión único (SSO) para los usuarios, donde una única contraseña (por usuario) se comparte entre muchos servicios. El inicio de sesión único permite a un usuario iniciar sesión una vez en un sitio web de la empresa para acceder de forma autenticada a la intranet corporativa.

Un cliente inicia una sesión LDAP conectándose a un servidor LDAP, conocido como Agente de sistema de directorio (DSA). Luego, el cliente envía una solicitud de operación al servidor, y el servidor responde con la autenticación adecuada.

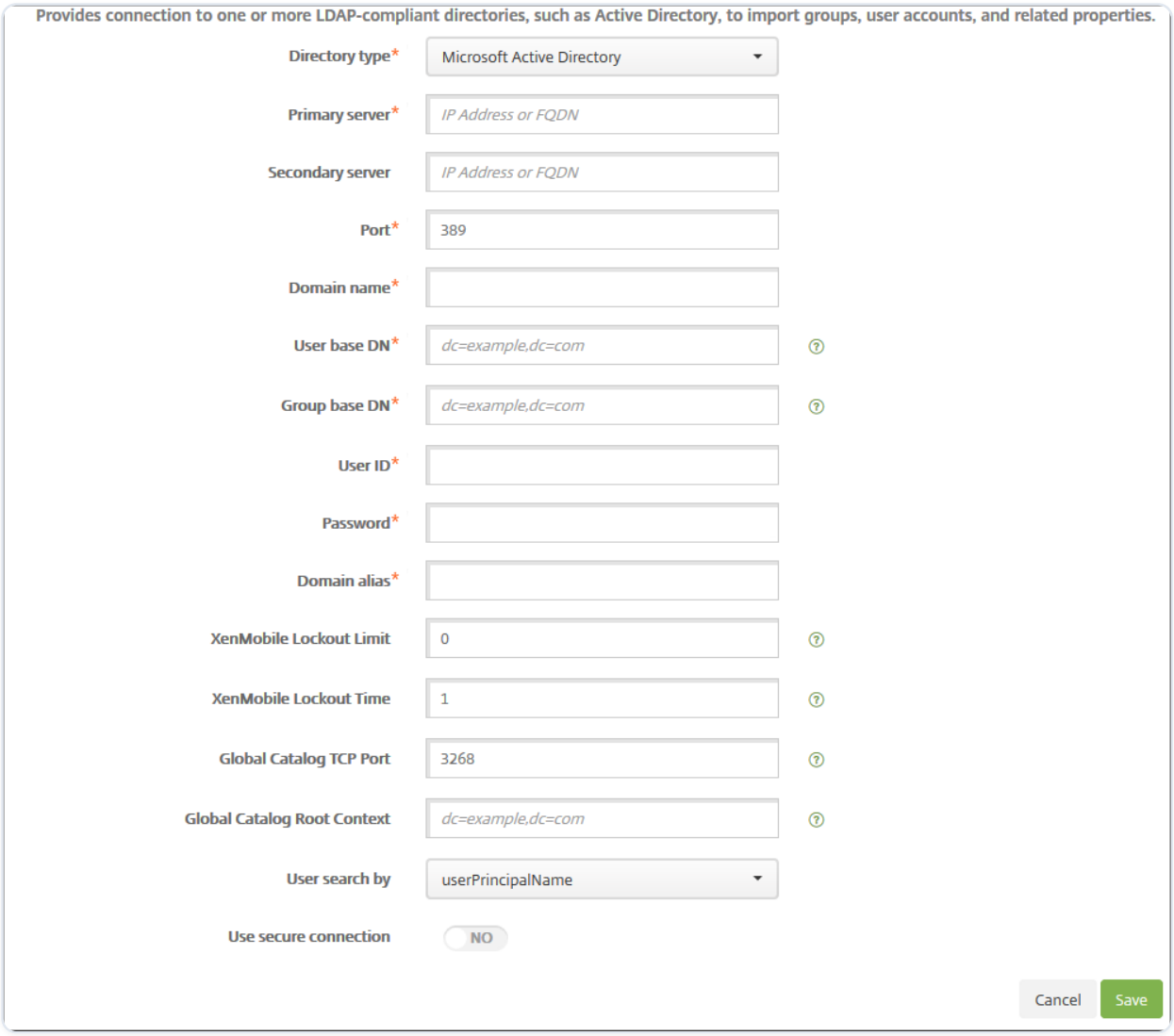
Para agregar o modificar conexiones LDAP en Citrix Endpoint Management

Normalmente, se configuran las conexiones LDAP al incorporarse a Citrix Endpoint Management, como se describe en Para configurar LDAP. Si se incorporó antes de que las pantallas que se muestran en esa sección estuvieran disponibles, utilice la información de esta sección para agregar conexiones LDAP.

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > LDAP**.
2. En **Servidor**, haga clic en **LDAP**. Aparecerá la página **LDAP**.



3. En la página **LDAP**, haga clic en **Agregar** o **Modificar**. Aparecerá la página **Agregar LDAP** o **Modificar LDAP**.



4. Configure estos ajustes:

   - **Tipo de directorio:** Haga clic en el tipo de directorio adecuado en la lista desplegable. El valor predeterminado es **Microsoft Active Directory**.
   - **Servidor principal:** Escriba el servidor principal utilizado para LDAP; puede introducir la dirección IP o el nombre de dominio completo (FQDN).
   - **Servidor secundario:** Opcionalmente, si se ha configurado un servidor secundario, introduzca la dirección IP o el FQDN de este. Este servidor es un servidor de conmutación por error que se utiliza si no se puede acceder al servidor principal.
   - **Puerto:** Escriba el número de puerto utilizado por el servidor LDAP. De forma predeterminada, el número de puerto se establece en **389** para las conexiones LDAP no seguras. Utilice el número de puerto **636** para las conexiones LDAP seguras, **3268** para las conexiones LDAP no seguras de Microsoft o **3269** para las conexiones LDAP seguras de Microsoft.
   - **Nombre de dominio:** Escriba el nombre de dominio.

- **DN base de usuario:** Escriba la ubicación de los usuarios en Active Directory mediante un identificador único. Algunos ejemplos de sintaxis son: `ou=users`, `dc=example` o `dc=com`.
- **DN base de grupo:** Escriba la ubicación de los grupos en Active Directory. Por ejemplo, `cn=users, dc=domain, dc=net`, donde `cn=users` representa el nombre del contenedor de los grupos y `dc` representa el componente de dominio de Active Directory.
- **ID de usuario:** Escriba el ID de usuario asociado a la cuenta de Active Directory.
- **Contraseña:** Escriba la contraseña asociada al usuario.
- **Alias de dominio:** Escriba un alias para el nombre de dominio. Si cambia la configuración de **Alias de dominio** después de la inscripción, los usuarios deben volver a inscribirse.
- **Límite de bloqueo de Citrix Endpoint Management:** Escriba un número entre **0** y **999** para el número de intentos de inicio de sesión fallidos. Un valor de **0** significa que Citrix Endpoint Management nunca bloquea al usuario por intentos de inicio de sesión fallidos. El valor predeterminado es **0**.

  Considere la posibilidad de establecer este límite de bloqueo en un valor inferior al de su directiva de bloqueo de LDAP. Esto ayuda a evitar bloqueos de usuario si Citrix Endpoint Management no puede autenticarse en el servidor LDAP. Por ejemplo, si la directiva de bloqueo de LDAP es de 5 intentos, configure este límite de bloqueo en **4** o menos.
- **Tiempo de bloqueo de Citrix Endpoint Management:** Escriba un número entre **0** y **99999** que represente el número de minutos que un usuario debe esperar después de superar el límite de bloqueo. Un valor de **0** significa que el usuario no se ve obligado a esperar después de un bloqueo. El valor predeterminado es **1**.
- **Puerto TCP del catálogo global:** Escriba el número de puerto TCP del servidor del catálogo global. De forma predeterminada, el número de puerto TCP se establece en **3268**; para las conexiones SSL, utilice el número de puerto **3269**.
- **Contexto raíz del catálogo global:** Opcionalmente, escriba el valor del Contexto raíz global utilizado para habilitar una búsqueda de catálogo global en Active Directory. Esta búsqueda se suma a la búsqueda LDAP estándar, en cualquier dominio sin necesidad de especificar el nombre de dominio real.
- **Búsqueda de usuario por:** Seleccione el formato de nombre de usuario o ID de usuario que Citrix Endpoint Management utiliza para buscar usuarios en este directorio. Los usuarios introducen su nombre de usuario o ID de usuario en este formato al inscribirse. Si cambia la configuración de **Búsqueda de usuario por** después de la inscripción, los usuarios deben volver a inscribirse.

Si elige **userPrincipalName**, los usuarios introducen un nombre principal de usuario (UPN) con este formato:

- `*username*@*domain*`

Si elige **sAMAccountName**, los usuarios introducen un nombre de administrador de cuentas de seguridad (SAM) en uno de estos formatos:

- `*username*@*domain*`
- `*domain\username*`

- **Usar conexión segura:** Seleccione si desea utilizar conexiones seguras. El valor predeterminado es **NO**.

5. Haga clic en **Guardar**.

Para eliminar un directorio compatible con LDAP

1. En la tabla **LDAP**, seleccione el directorio que desea eliminar.

   Puede seleccionar más de una propiedad para eliminar marcando la casilla de verificación junto a cada propiedad.

2. Haga clic en **Eliminar**. Aparece un cuadro de diálogo de confirmación. Vuelva a hacer clic en **Eliminar**.

Configurar la autenticación de dominio más token de seguridad

Puede configurar Citrix Endpoint Management para que exija a los usuarios autenticarse con sus credenciales LDAP más una contraseña de un solo uso, utilizando el protocolo RADIUS.

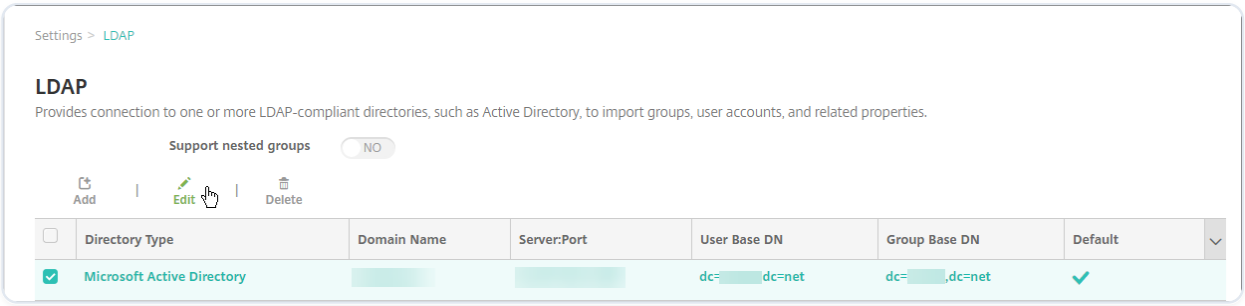
Para una usabilidad óptima, puede combinar esta configuración con el PIN de Citrix y el almacenamiento en caché de contraseñas de Active Directory. Con esa configuración, los usuarios no tienen que introducir sus nombres de usuario y contraseñas LDAP repetidamente. Los usuarios introducen los nombres de usuario y las contraseñas para la inscripción, la caducidad de la contraseña y el bloqueo de la cuenta.

Configurar los ajustes de LDAP

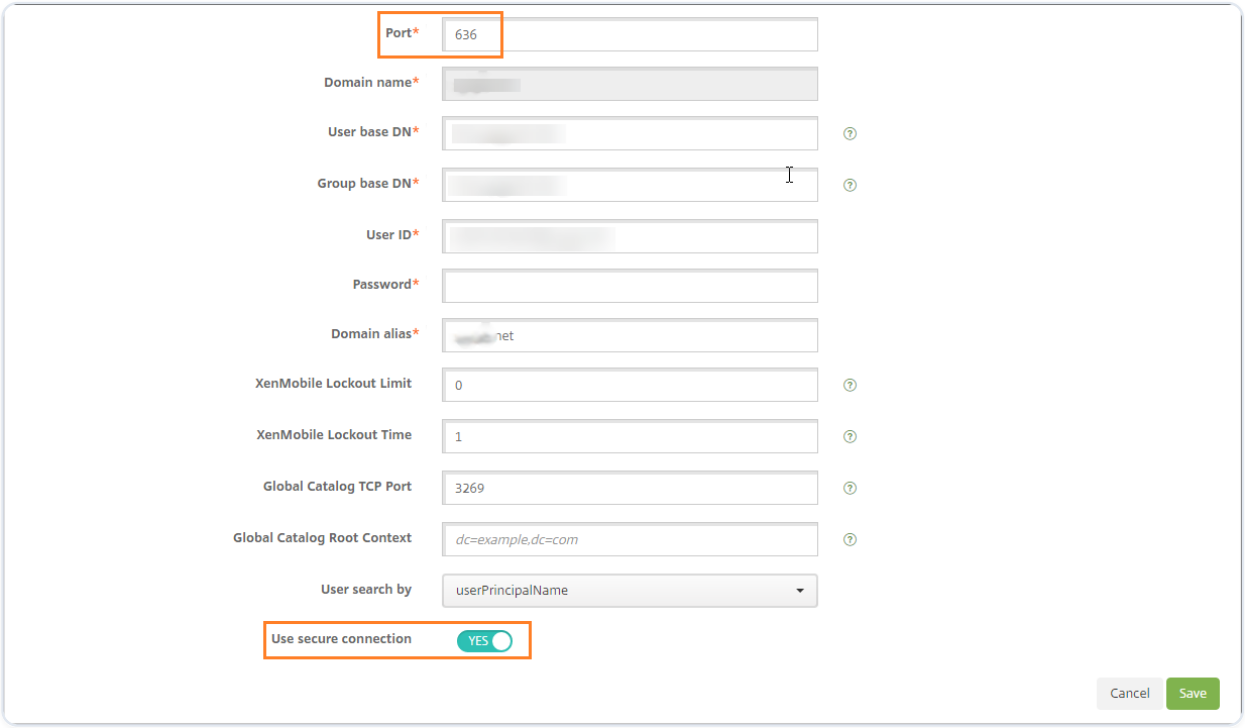
El uso de LDAP para la autenticación requiere que instale un certificado SSL de una entidad de certificación en Citrix Endpoint Management. Para obtener más información, consulte Cargar certificados.

1. En **Configuración**, haga clic en **LDAP**.

2. Seleccione **Microsoft Active Directory** y, a continuación, haga clic en **Editar**.



3. verificar que el puerto sea **636**, que es para conexiones LDAP seguras, o **3269** para conexiones LDAP seguras de Microsoft.
4. Cambie **Usar conexión segura** a **Sí**.



Configurar los ajustes de NetScaler Gateway

Los siguientes pasos asumen que ya ha añadido una instancia de NetScaler Gateway a Citrix Endpoint Management. Para añadir una instancia de NetScaler Gateway, consulte NetScaler Gateway y Citrix Endpoint Management.

1. En **Configuración**, haga clic en **NetScaler Gateway**.
2. Seleccione NetScaler Gateway y, a continuación, haga clic en **Editar**.
3. En **Tipo de inicio de sesión**, seleccione **Dominio y token de seguridad**.

Habilitar el PIN de Citrix y el almacenamiento en caché de contraseñas de usuario

Para habilitar el PIN de Citrix y el almacenamiento en caché de contraseñas de usuario, vaya a **Settings > Client Properties** y seleccione estas casillas de verificación: **Enable Citrix PIN Authentication** y **Enable User Password Caching**. Para obtener más información, consulte Propiedades del cliente.

Configurar NetScaler Gateway para la autenticación de dominio y token de seguridad

Configure los perfiles y las directivas de sesión de NetScaler Gateway para los servidores virtuales que utiliza con Citrix Endpoint Management. Para obtener más información, consulte la documentación de NetScaler Gateway.

Certificado de cliente o certificado más autenticación de dominio

La configuración predeterminada de Citrix Endpoint Management es la autenticación de nombre de usuario y contraseña. Para añadir otra capa de seguridad para la inscripción y el acceso al entorno de Citrix Endpoint Management, considere la posibilidad de utilizar la autenticación basada en certificados. En el entorno de Citrix Endpoint Management, esta configuración es la mejor combinación de seguridad y experiencia de usuario. La autenticación de certificado más dominio ofrece las mejores posibilidades de SSO junto con la seguridad proporcionada por la autenticación de dos factores en NetScaler Gateway.

Para una usabilidad óptima, puede combinar la autenticación de certificado más dominio con el PIN de Citrix y el almacenamiento en caché de contraseñas de Active Directory. Como resultado, los usuarios no tienen que introducir sus nombres de usuario y contraseñas LDAP repetidamente. Los usuarios introducen nombres de usuario y contraseñas para la inscripción, la caducidad de la contraseña y el bloqueo de la cuenta.

> **Importante:**

> Citrix Endpoint Management no admite cambiar el modo de autenticación de autenticación de dominio a otro modo de autenticación después de que los usuarios inscriban dispositivos en Citrix Endpoint Management.

> Si no permite LDAP y utiliza tarjetas inteligentes o métodos similares, la configuración de certificados le permite representar una tarjeta inteligente en Citrix Endpoint Management. Los usuarios se inscriben entonces utilizando un PIN único que Citrix Endpoint Management

> genera para ellos. Una vez que un usuario tiene acceso, Citrix Endpoint Management crea e implementa el certificado utilizado para autenticarse en el entorno de Citrix Endpoint Management.

Puede utilizar el asistente de NetScaler for XenMobile para realizar la configuración necesaria para Citrix Endpoint Management cuando se utiliza la autenticación solo con certificado de NetScaler Gateway o la autenticación de certificado más dominio. Puede ejecutar el asistente de NetScaler for XenMobile una sola vez.

En entornos de alta seguridad, el uso de credenciales LDAP fuera de una organización en redes públicas o inseguras se considera una amenaza de seguridad principal para la organización. Para entornos de alta seguridad, la autenticación de dos factores que utiliza un certificado de cliente y un token de seguridad es una opción. Para obtener más información, consulte Configuración de Citrix Endpoint Management para la autenticación de certificados y tokens de seguridad.

La autenticación de certificado de cliente está disponible para dispositivos inscritos en MAM y MDM+MAM. Para utilizar la autenticación de certificado de cliente para esos dispositivos, debe configurar el servidor de Microsoft, Citrix Endpoint Management y, a continuación, NetScaler Gateway. Siga estos pasos generales, como se describe en este artículo.

En el servidor de Microsoft:

1. Agregue un complemento de certificado a la Consola de administración de Microsoft.
2. Agregue la plantilla a la entidad de certificación (CA).
3. Cree un certificado PFX desde el servidor de CA.

En Citrix Endpoint Management:

1. Cargue el certificado en Citrix Endpoint Management.
2. Crear la entidad PKI para la autenticación basada en certificados.
3. Configurar proveedores de credenciales.
4. Configurar NetScaler Gateway para entregar un certificado de usuario para la autenticación.

Para obtener información sobre la configuración de NetScaler Gateway, consulte estos artículos en la documentación de Citrix ADC:

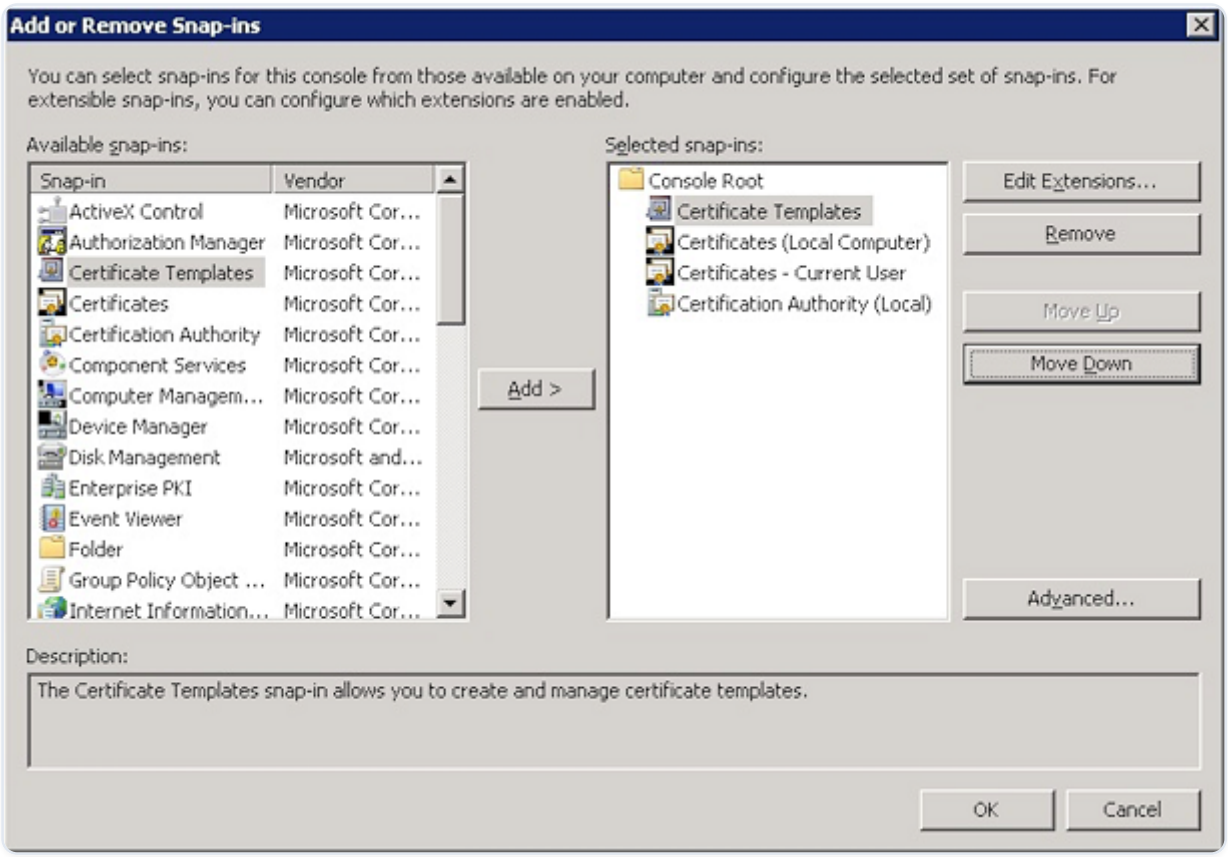
- Autenticación de cliente
- Infraestructura de perfiles SSL
- Configuración y enlace de una directiva de autenticación de certificado de cliente.

Requisitos previos

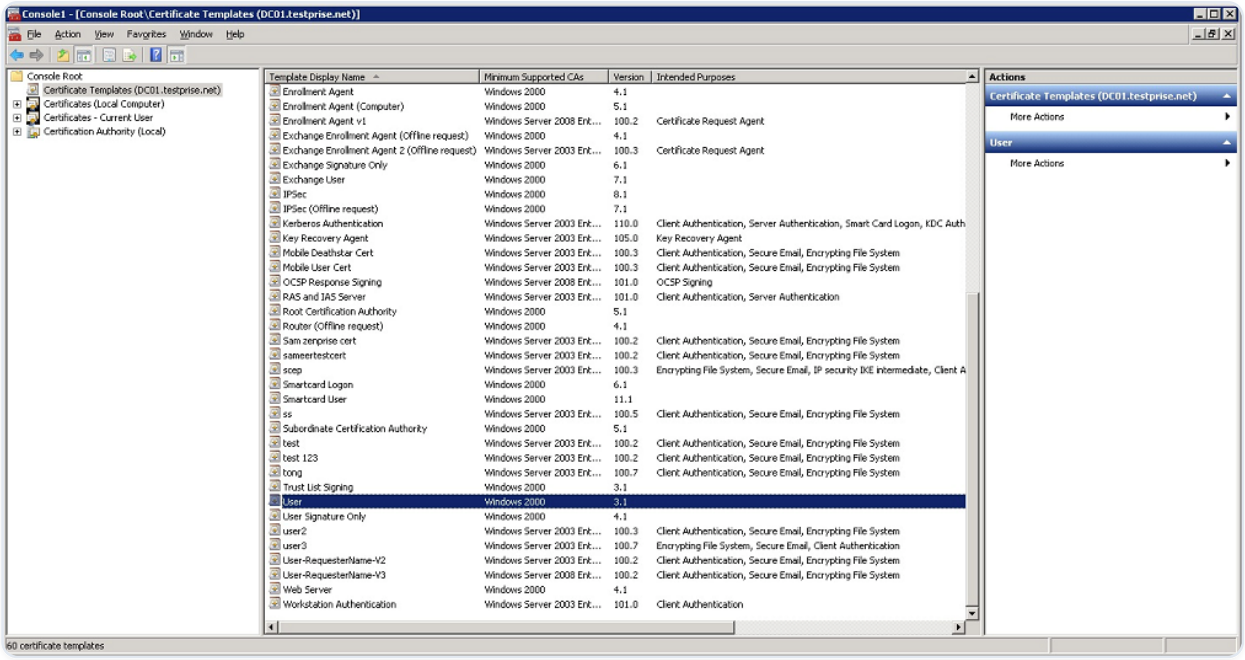
- Al crear una plantilla de entidad de Servicios de certificados de Microsoft, evite posibles problemas de autenticación con los dispositivos inscritos excluyendo los caracteres especiales. Por ejemplo, no utilice estos caracteres en el nombre de la plantilla: `: ! $ () # % + * ~ ? | {} []`
- Para configurar la autenticación basada en certificados para Exchange ActiveSync, consulte la documentación de Microsoft sobre Exchange Server. Configure el sitio del servidor de la entidad de certificación (CA) para que Exchange ActiceSync requiera certificados de cliente.
- Si utiliza certificados de servidor privados para proteger el tráfico de ActiveSync al servidor de Exchange, asegúrese de que los dispositivos móviles tengan todos los certificados raíz/intermedios. De lo contrario, la autenticación basada en certificados fallará durante la configuración del buzón en Citrix Secure Mail. En la consola IIS de Exchange, debe:
  - Agregue un sitio web para el uso de Citrix Endpoint Management con Exchange y vincule el certificado del servidor web.
  - Utilice el puerto 9443.
  - Para ese sitio web, debe agregar dos aplicaciones, una para "Microsoft-Server-ActiveSync" y otra para "EWS". Para ambas aplicaciones, en **Configuración SSL**, seleccione **Requerir SSL**.

Agregar un complemento de certificado a la Consola de administración de Microsoft

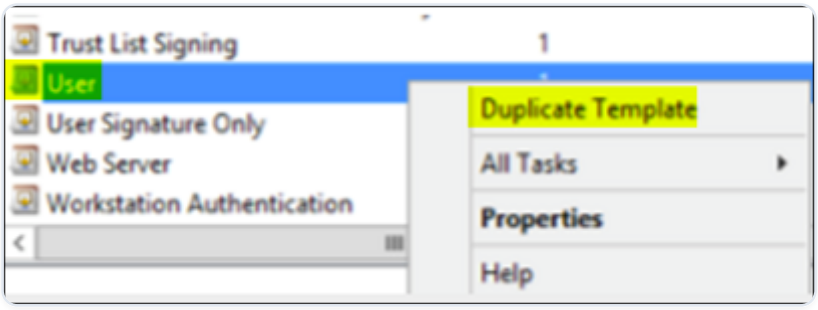
1. Abra la consola y, a continuación, haga clic en **Agregar o quitar complementos**.
2. Agregue los siguientes complementos:
   - Plantillas de certificado
   - Certificados (equipo local)
   - Certificados - Usuario actual
   - Entidad de certificación (local)



3. Expanda **Plantillas de certificado**.



4. Seleccione la plantilla **Usuario** y **Duplicar plantilla**.

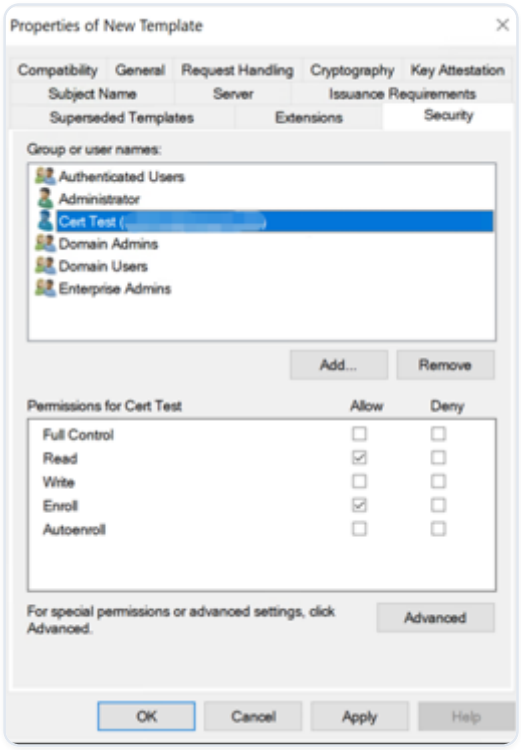


5. Proporcione el nombre para mostrar de la plantilla.

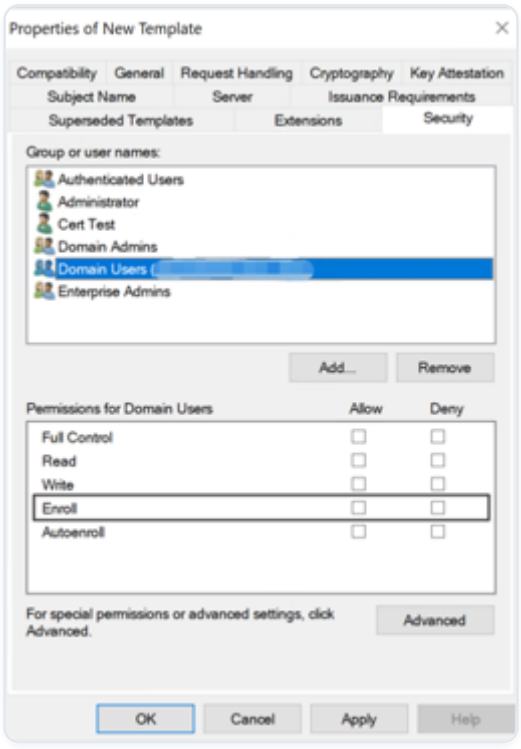
> **Importante:**
>
> No se recomienda seleccionar la opción **Publicar certificado en Active Directory**. Si se selecciona esta opción, se crean certificados de cliente para todos los usuarios de Active Directory, lo que podría saturar la base de datos de Active Directory.

6. Seleccione **Windows 2003 Server** para el tipo de plantilla. En el servidor Windows 2012 R2, en **Compatibilidad**, seleccione **Entidad de certificación** y establezca el destinatario como **Windows 2003**.
7. En **Seguridad**, configure lo siguiente:
   a. Haga clic en **Agregar** y, a continuación, seleccione la cuenta de usuario de AD que Citrix Endpoint Management utiliza para generar certificados.

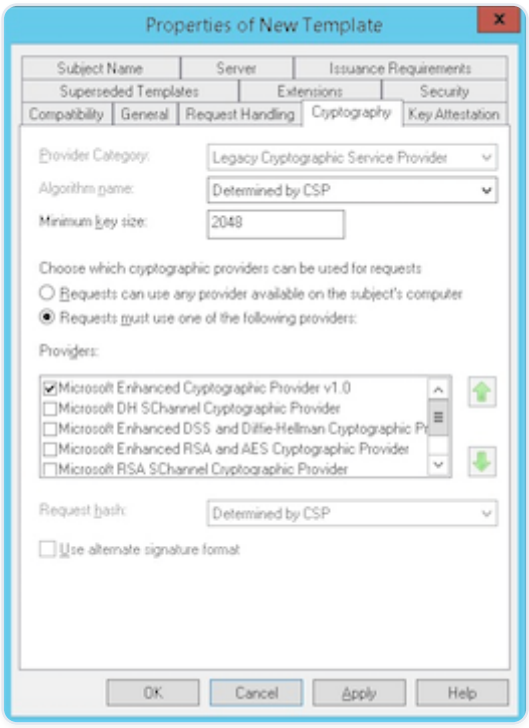
> **Importante:**
>
> Agregue aquí solo el usuario de la cuenta de servicio. Agregue el permiso **Inscribir** solo a esta cuenta de usuario de AD.
>
> Como se describe más adelante en este artículo, se crea un certificado .pfx de usuario mediante la cuenta de servicio. Para obtener más información, consulte Crear un certificado PFX desde el servidor de CA.



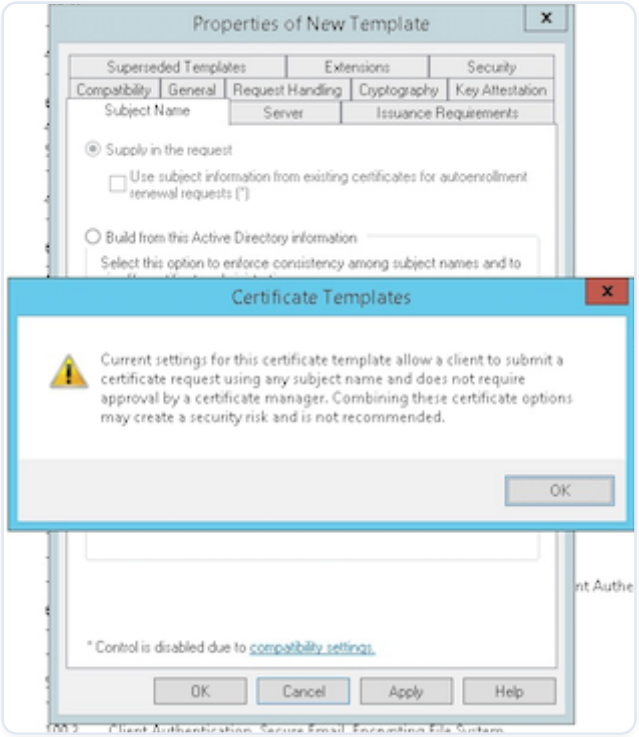
b. Revoque el permiso **Inscribir** de **Usuarios del dominio**.



8. En **Criptografía**, asegúrese de proporcionar el tamaño de clave. Más adelante, introducirá el tamaño de clave durante la configuración de Citrix Endpoint Management.

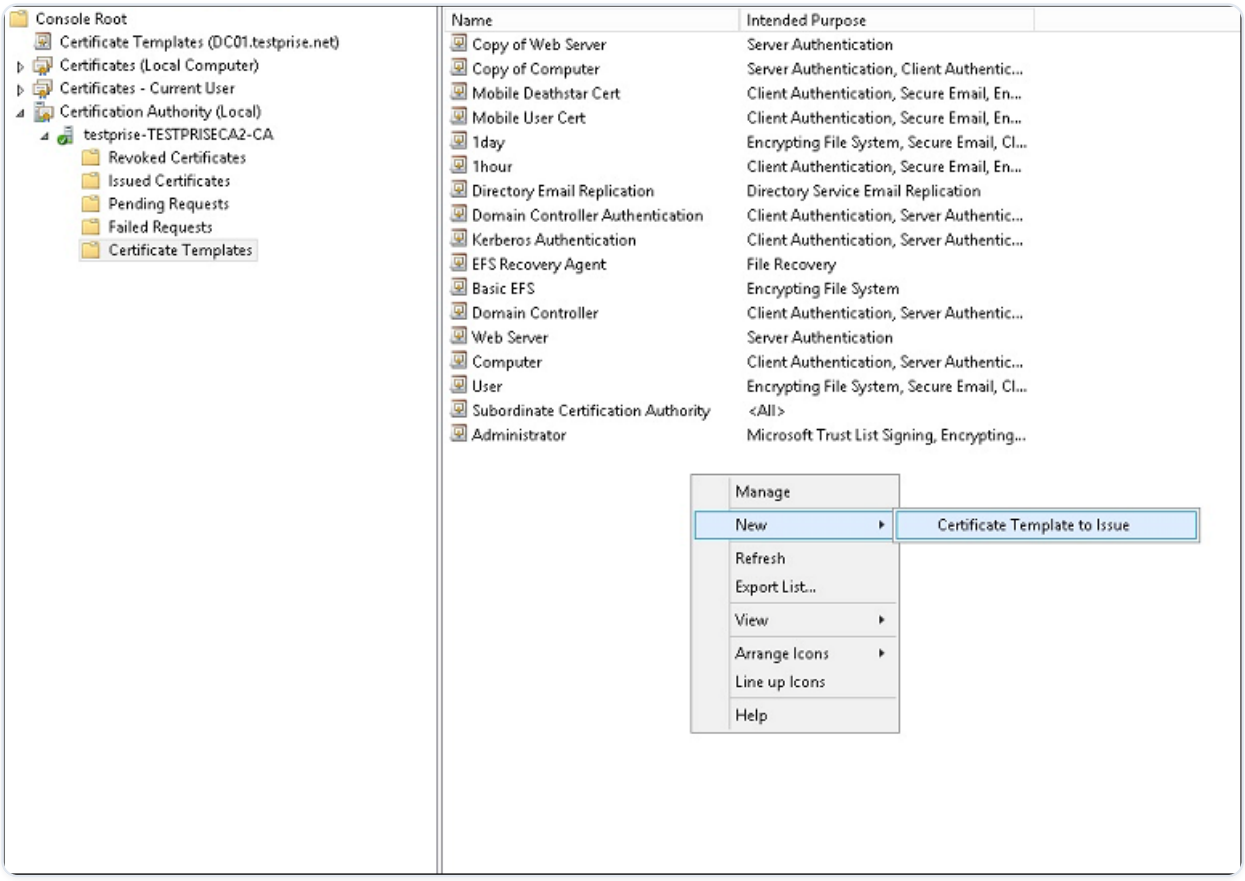


9. En **Nombre del sujeto**, seleccione **Suministrar en la solicitud**. Aplique los cambios y, a continuación, guarde.

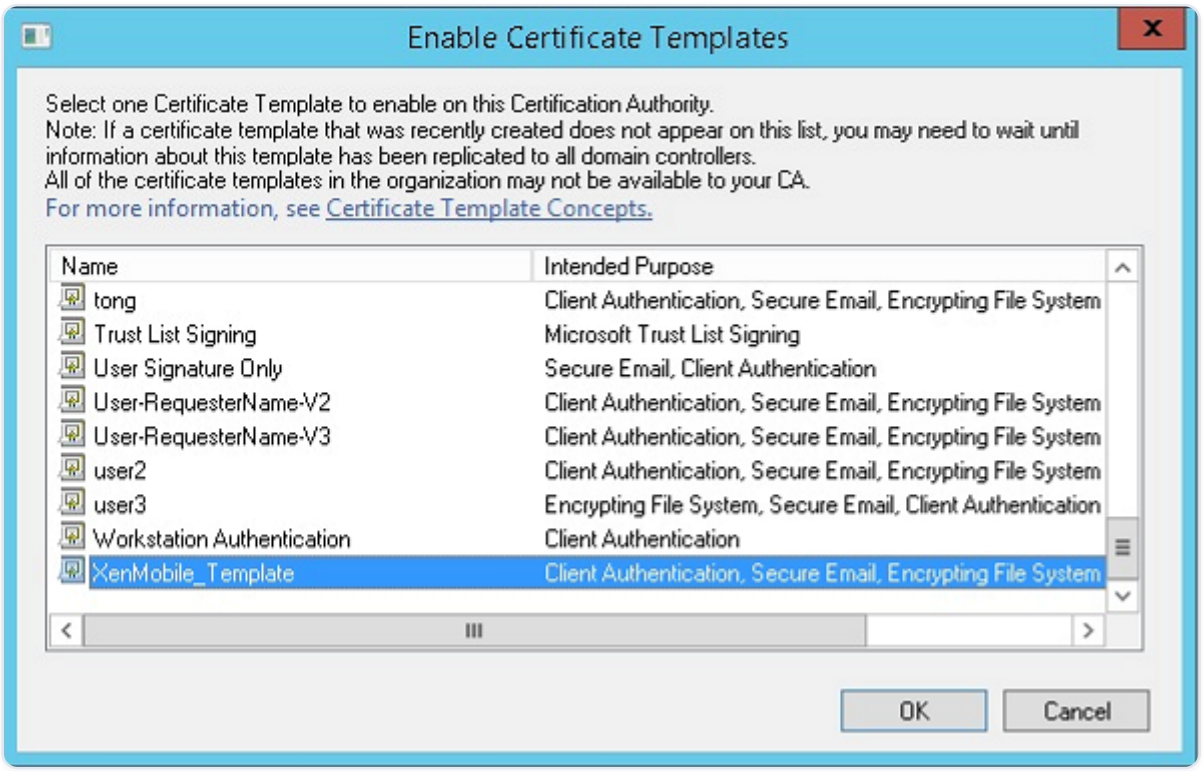


Agregar la plantilla a la entidad de certificación

1. Vaya a **Entidad de certificación** y seleccione **Plantillas de certificado**.
2. Haga clic con el botón derecho en el panel derecho y, a continuación, seleccione **Nuevo > Plantilla de certificado para emitir**.

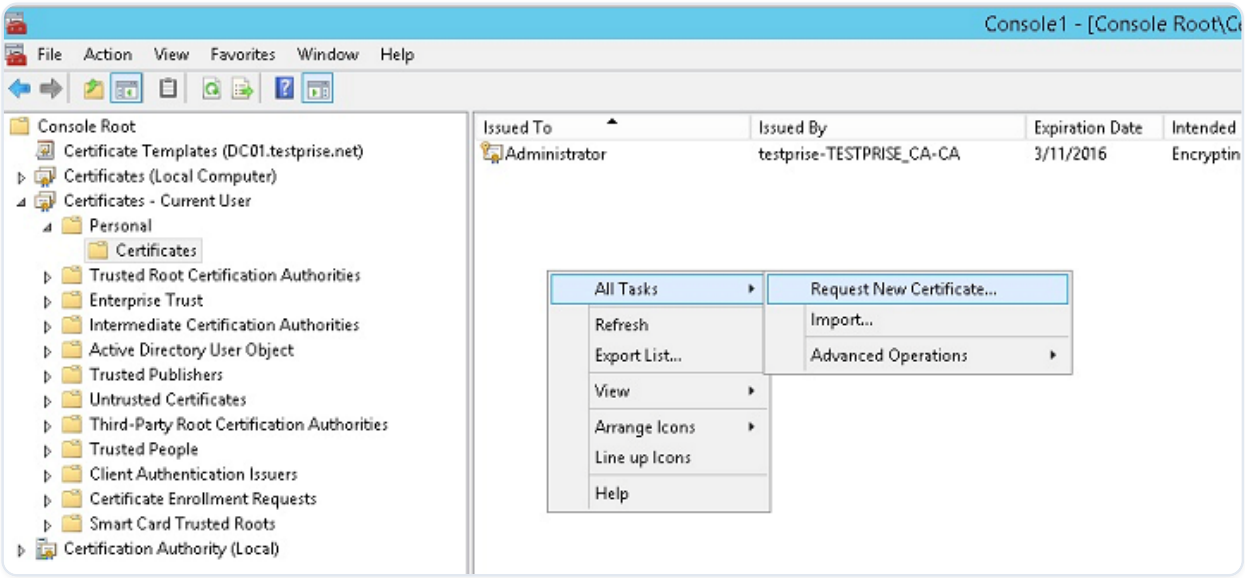


3. Seleccione la plantilla que creó en el paso anterior y, a continuación, haga clic en **OK** para agregarla a la **Certificate Authority**.

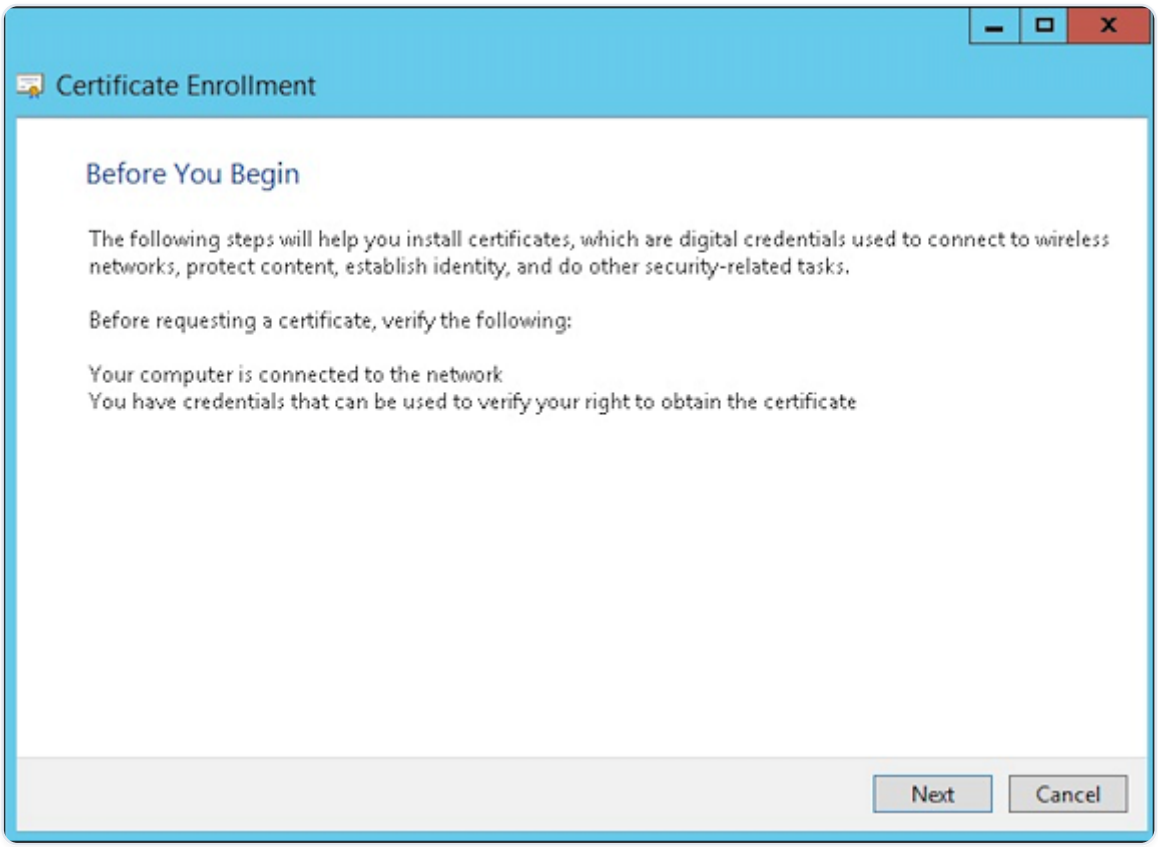


Creación de un certificado PFX desde el servidor de CA

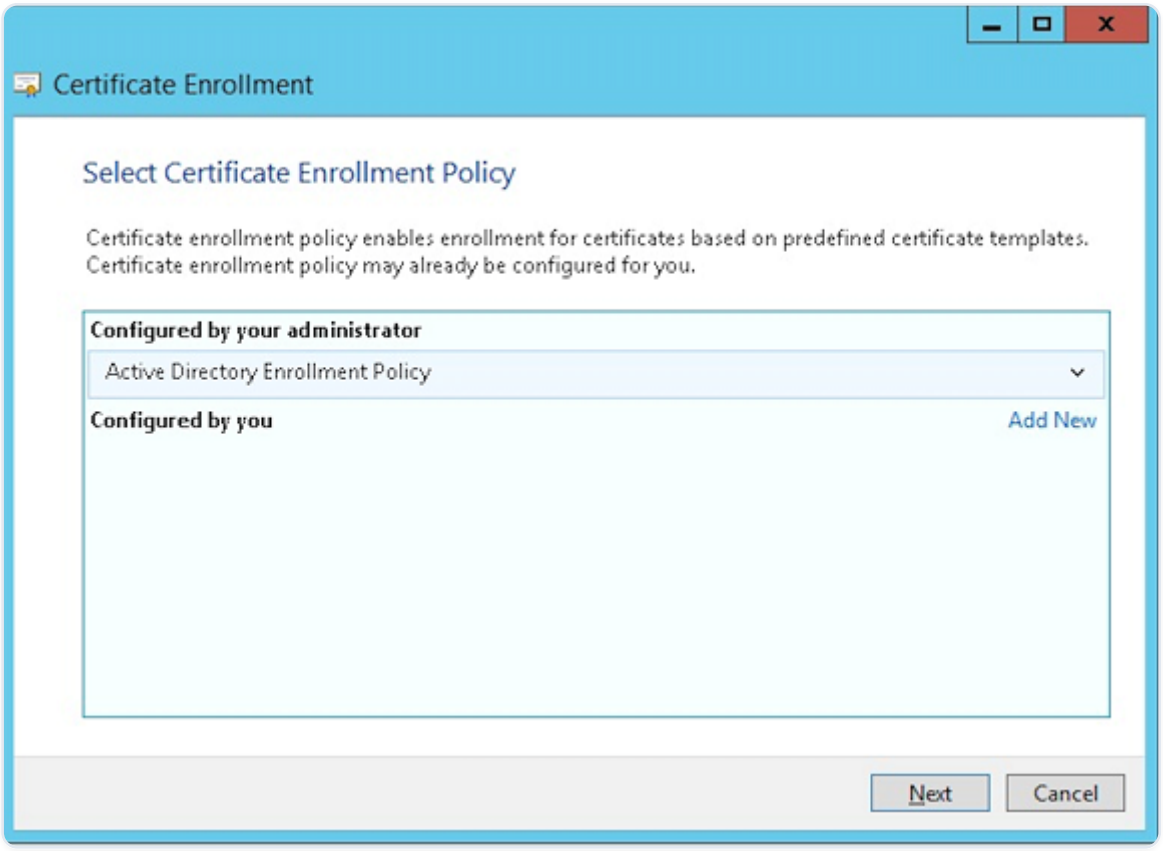
1. Cree un certificado .pfx de usuario mediante la cuenta de servicio con la que inició sesión. El archivo .pfx se carga en Citrix Endpoint Management, que luego solicita un certificado de usuario para los usuarios que inscriben sus dispositivos.
2. En **Current User**, expanda **Certificates**.
3. Haga clic con el botón secundario en el panel derecho y, a continuación, haga clic en **Request New Certificate**.



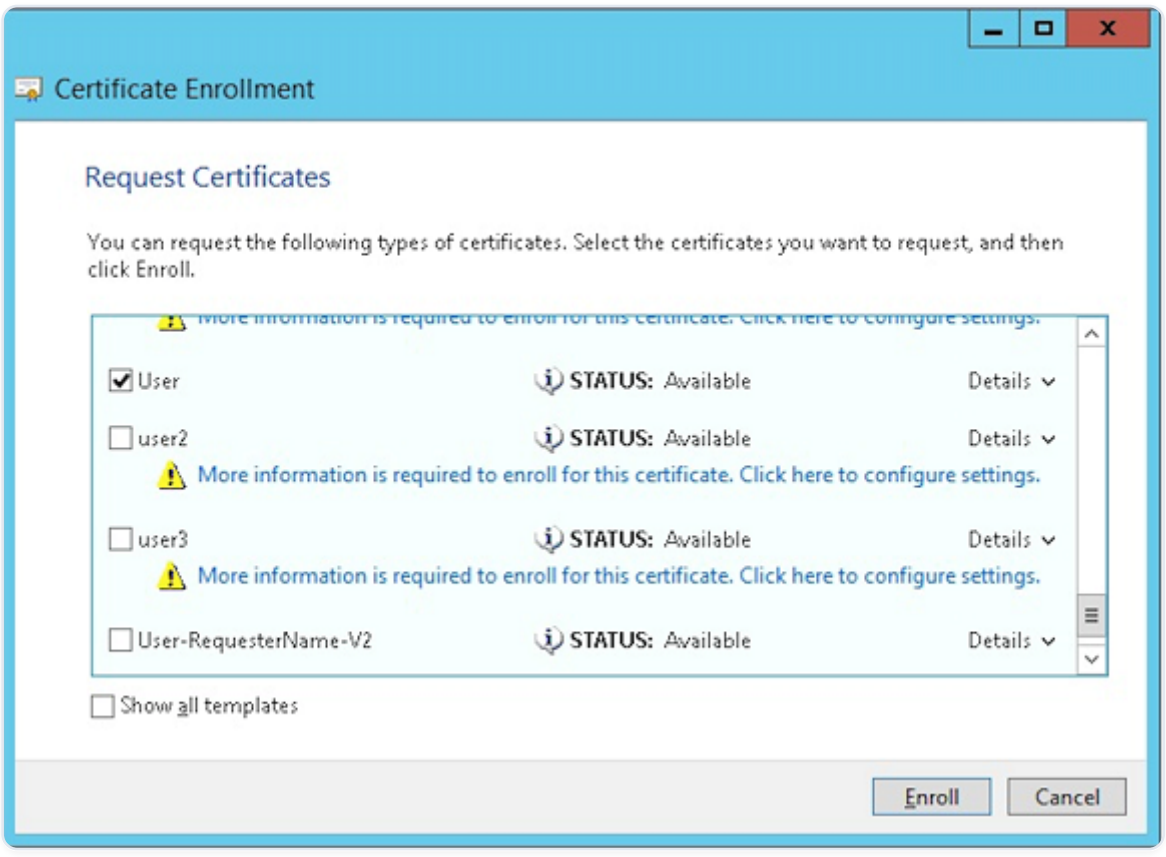
4. Aparece la pantalla **Certificate Enrollment**. Haga clic en **Next**.



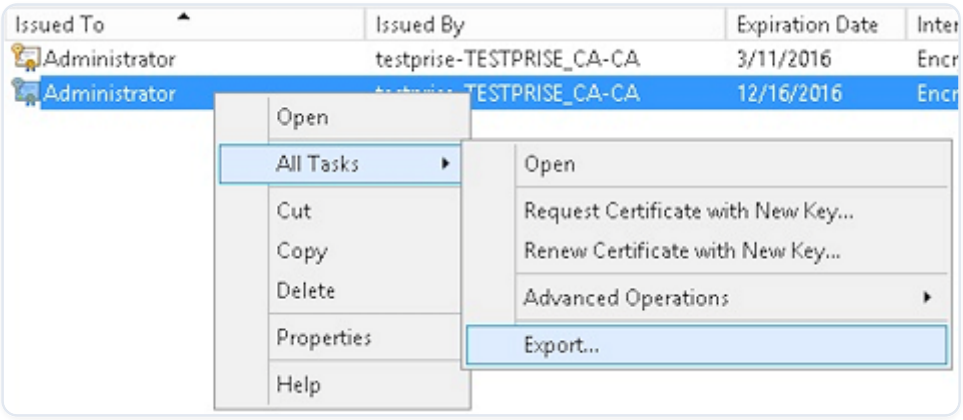
5. Seleccione **Active Directory Enrollment Policy** y, a continuación, haga clic en **Next**.



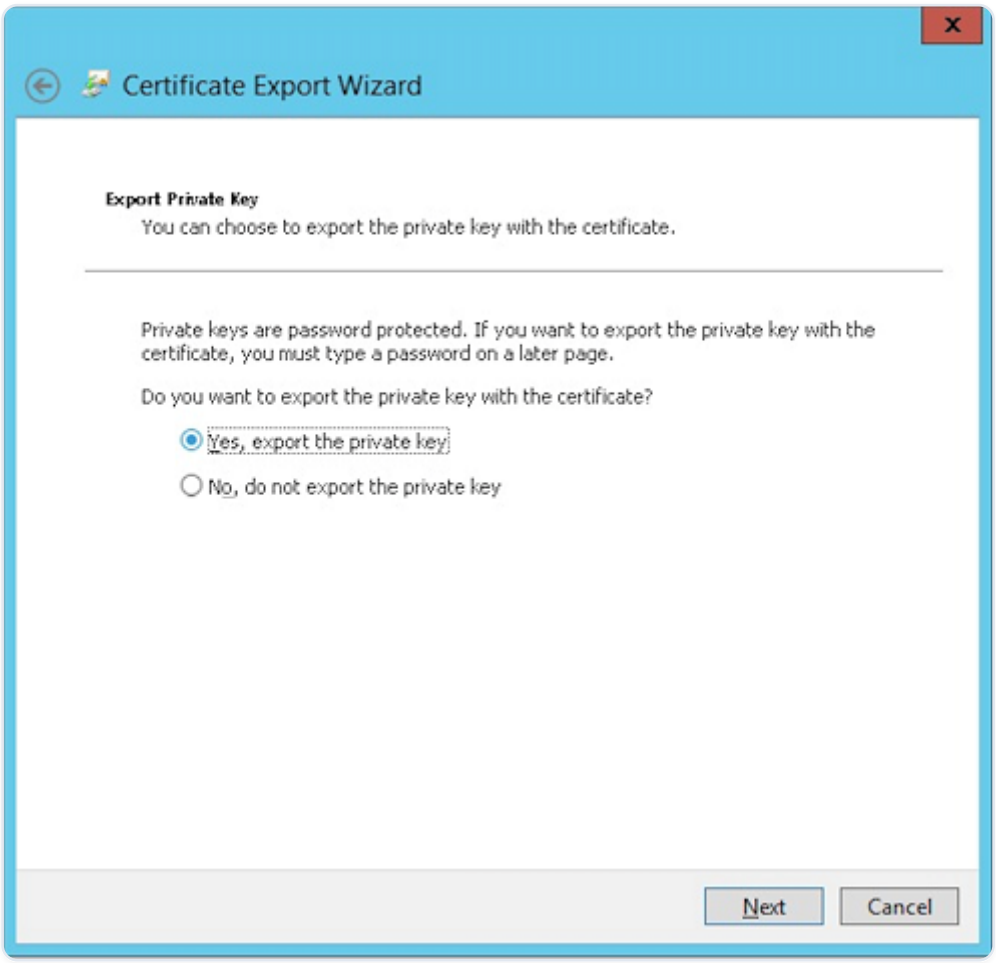
6. Seleccione la plantilla **User** y, a continuación, haga clic en **Enroll**.



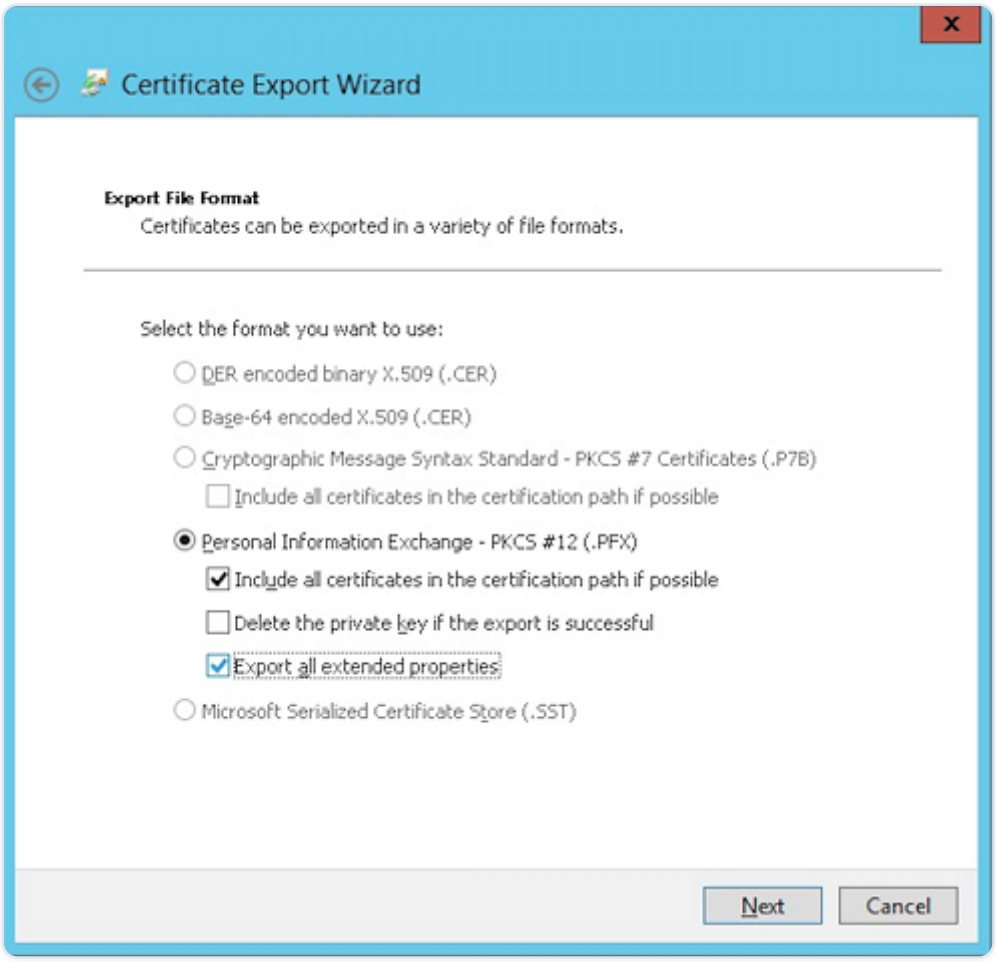
7. Exporte el archivo .pfx que creó en el paso anterior.



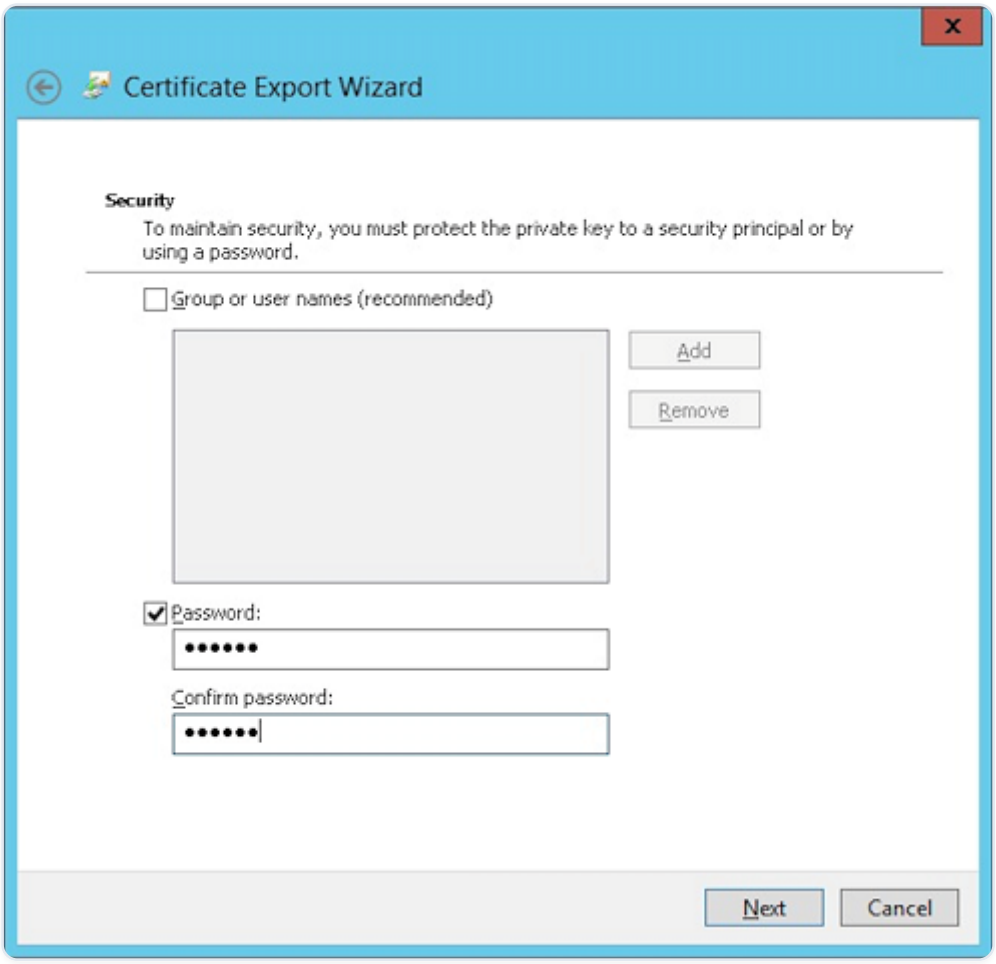
8. Haga clic en **Sí, exportar la clave privada**.



9. Seleccione **Incluir todos los certificados en la ruta de certificación si es posible** y marque la casilla **Exportar todas las propiedades extendidas**.



10. Establezca una contraseña para usar al cargar este certificado en Citrix Endpoint Management.

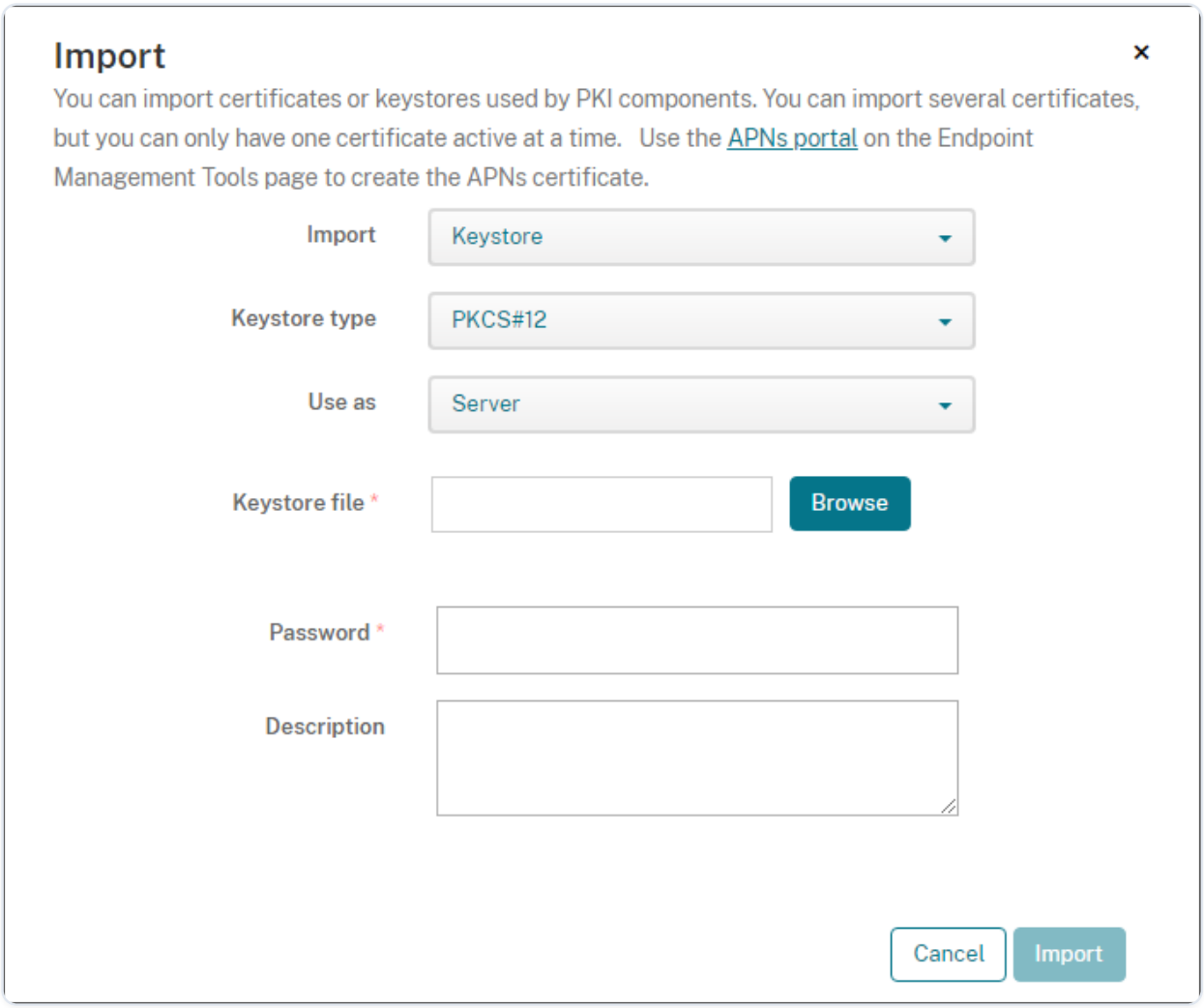


11. Guarde el certificado en su disco duro.

Carga del certificado en Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha. Aparece la pantalla **Configuración**.
2. Haga clic en **Certificados** y, a continuación, en **Importar**.
3. Introduzca los siguientes parámetros:

    - **Importar:** Keystore
    - **Tipo de Keystore:** PKCS #12
    - **Usar como:** Servidor
    - **Archivo de almacén de claves:** Haga clic en Examinar para seleccionar el certificado .pfx que creó.
    - **Contraseña:** Introduzca la contraseña que creó para este certificado.

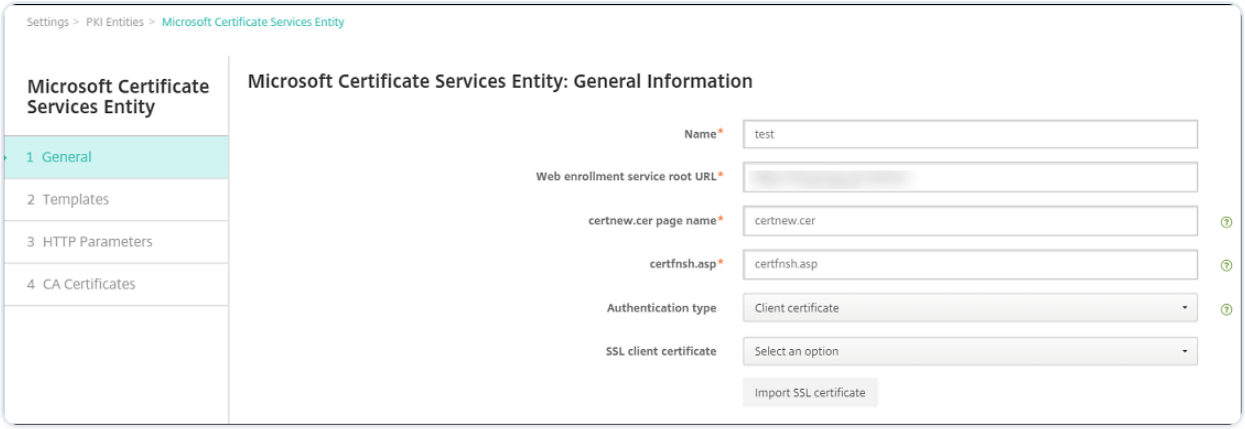


4. Haga clic en **Importar**.
5. verificar que el certificado se haya instalado correctamente. Un certificado instalado correctamente se muestra como un certificado de usuario.

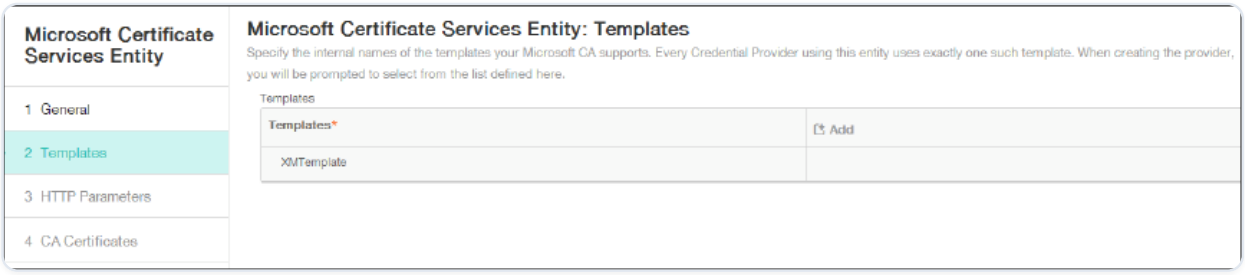
Creación de la entidad PKI para la autenticación basada en certificados

1. En **Parámetros**, vaya a **Más > Administración de certificados > Entidades PKI**.
2. Haga clic en **Agregar** y, a continuación, en **Entidad de servicios de certificados de Microsoft**. Aparece la pantalla **Entidad de servicios de certificados de Microsoft: Información general**.
3. Introduzca los siguientes parámetros:
   - **Nombre:** Escriba cualquier nombre.
   - **URL raíz del servicio de inscripción web:** `https://RootCA-URL/certsrv/` (Asegúrese de agregar la última barra, /, en la ruta de la URL.)
   - **Nombre de la página certnew.cer:** certnew.cer (valor predeterminado)

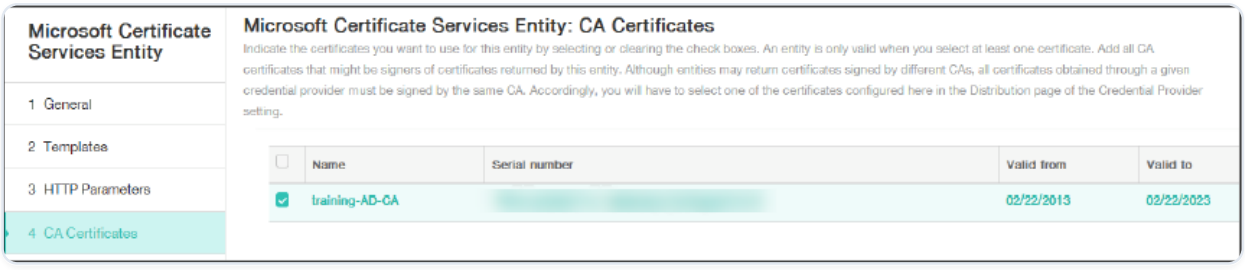
- **certfnsh.asp:** certfnsh.asp (valor predeterminado)
- **Tipo de autenticación:** Certificado de cliente
- **Certificado de cliente SSL:** Seleccione el certificado de usuario que se utilizará para emitir el certificado de cliente de Citrix Endpoint Management. Si no existe ningún certificado, siga el procedimiento de la sección anterior para cargar certificados.



4. En **Plantillas**, añada la plantilla que creó al configurar el certificado de Microsoft. No añada espacios.



5. Omita los parámetros HTTP y, a continuación, haga clic en **Certificados de CA**.
6. Seleccione el nombre de la CA raíz que corresponda a su entorno. Esta CA raíz forma parte de la cadena importada del certificado de cliente de Citrix Endpoint Management.



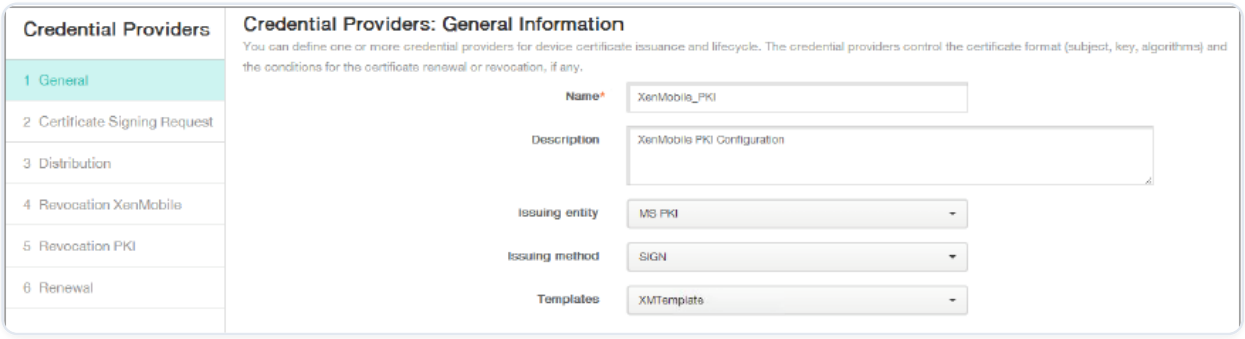
7. Haga clic en **Guardar**.

Configuración de proveedores de credenciales

1. En **Parámetros**, vaya a **Más > Administración de certificados > Proveedores de credenciales**.

2. Haga clic en **Agregar**.
3. En **General**, introduzca los siguientes parámetros:

    - **Nombre:** Escriba cualquier nombre.
    - **Descripción:** Escriba cualquier descripción.
    - **Entidad emisora:** Seleccione la entidad PKI creada anteriormente.
    - **Método de emisión:** SIGN
    - **Plantillas:** Seleccione la plantilla agregada en la entidad PKI.

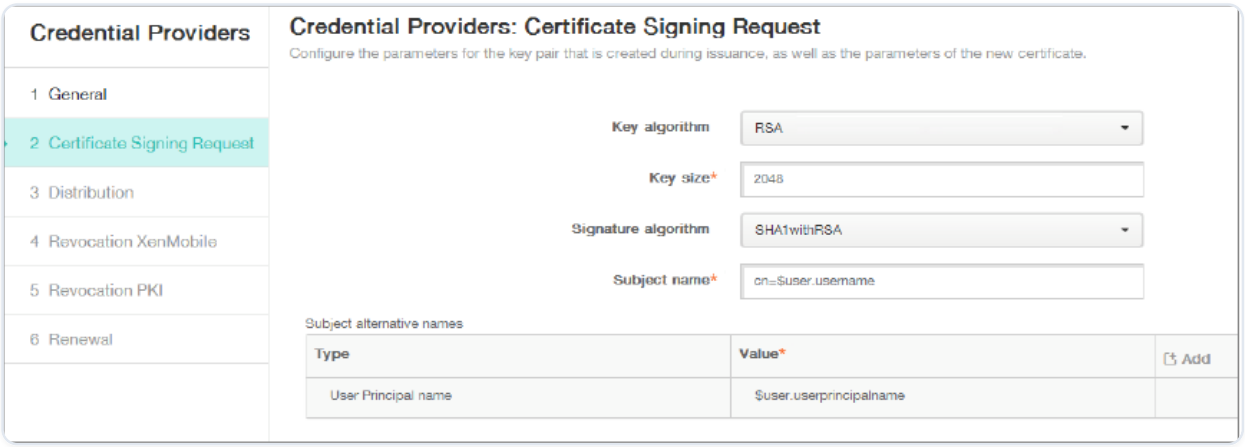


4. Haga clic en **Solicitud de firma de certificado** y, a continuación, introduzca los siguientes parámetros:

    - **Algoritmo de clave:** RSA
    - **Tamaño de clave:** 2048
    - **Algoritmo de firma:** SHA256withRSA
    - **Nombre del sujeto:** `cn=$user.username`

    Para **Nombres alternativos del sujeto**, haga clic en **Agregar** y, a continuación, introduzca los siguientes parámetros:

    - **Tipo:** Nombre principal de usuario
    - **Valor:** `$user.userprincipalname`

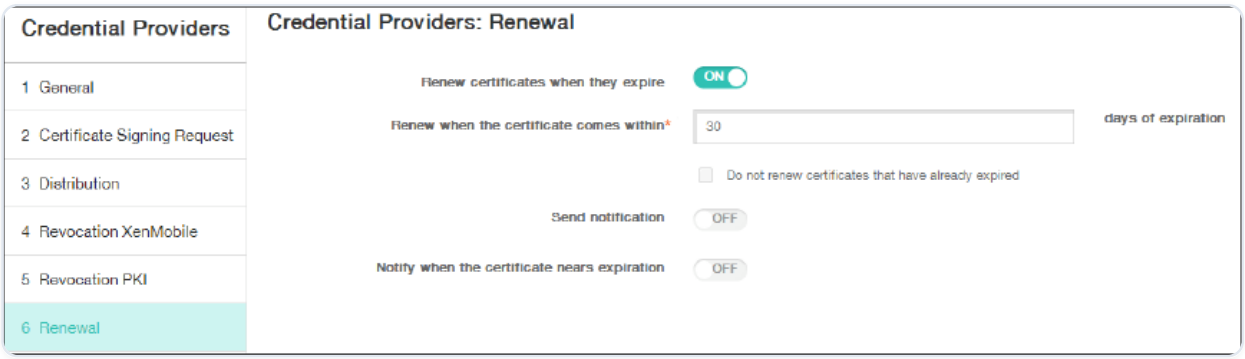


5. Haga clic en **Distribución** e introduzca los siguientes parámetros:

   - **Certificado de CA emisora:** Seleccione la CA emisora que firmó el certificado de cliente de Citrix Endpoint Management.
   - **Seleccionar modo de distribución:** Seleccione **Preferir centralizado: Generación de claves en el servidor**.



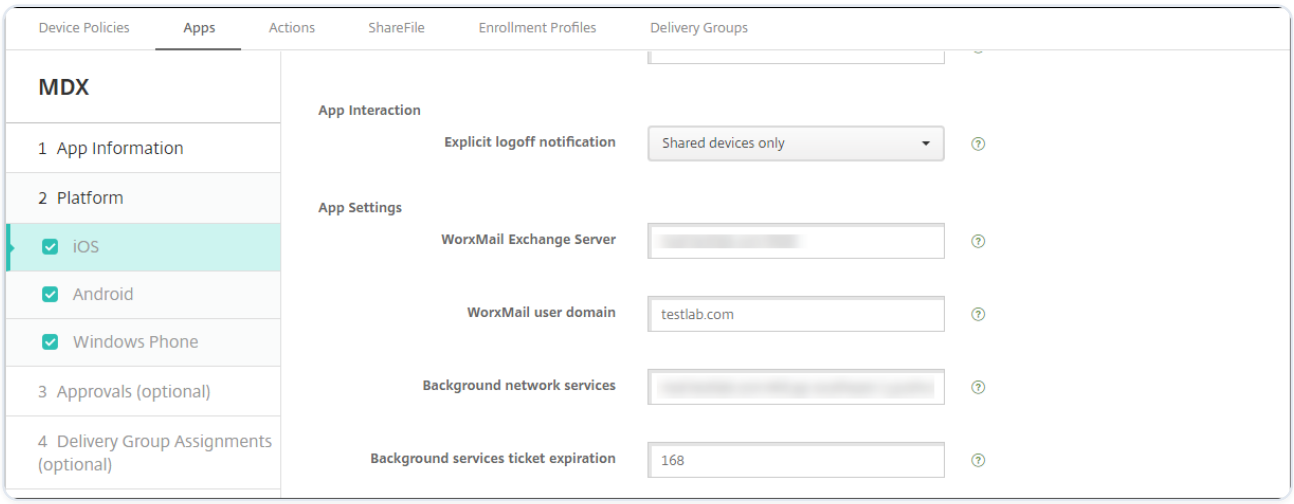
6. Para las dos secciones siguientes, **Revocation Citrix Endpoint Management** y **Revocation PKI**, configure los parámetros según sea necesario. En este ejemplo, se omiten ambas opciones.
7. Haga clic en **Renovación**.
8. Habilite **Renovar certificados cuando caduquen**.
9. Deje todas las demás configuraciones por defecto o cámbielas según sea necesario.



10. Haga clic en **Guardar**.

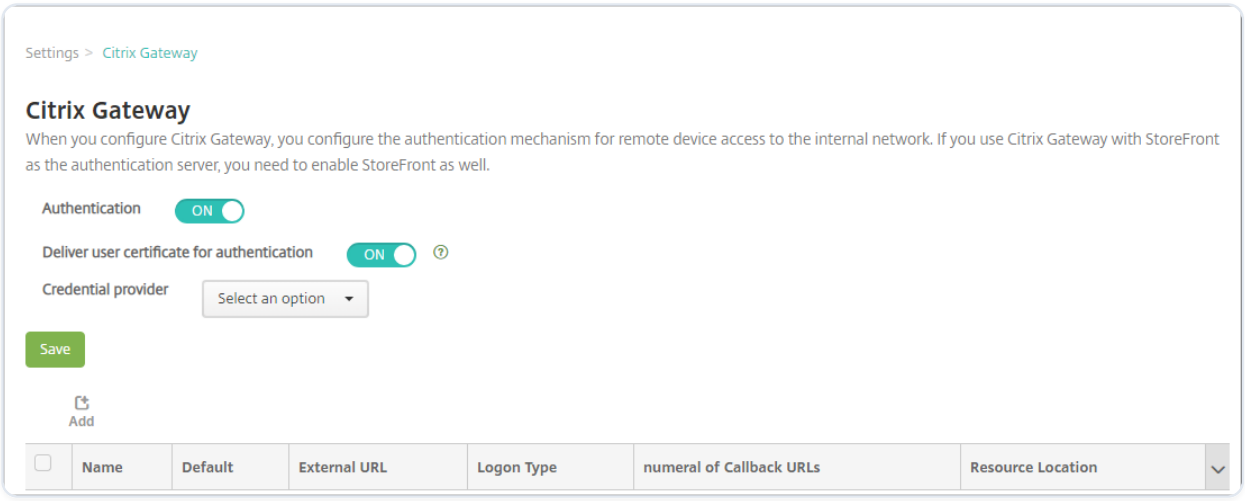
Configuración de Citrix Secure Mail para usar la autenticación basada en certificados

Cuando añada Citrix Secure Mail a Citrix Endpoint Management, asegúrese de configurar los ajustes de Exchange en **Configuración de la aplicación**.

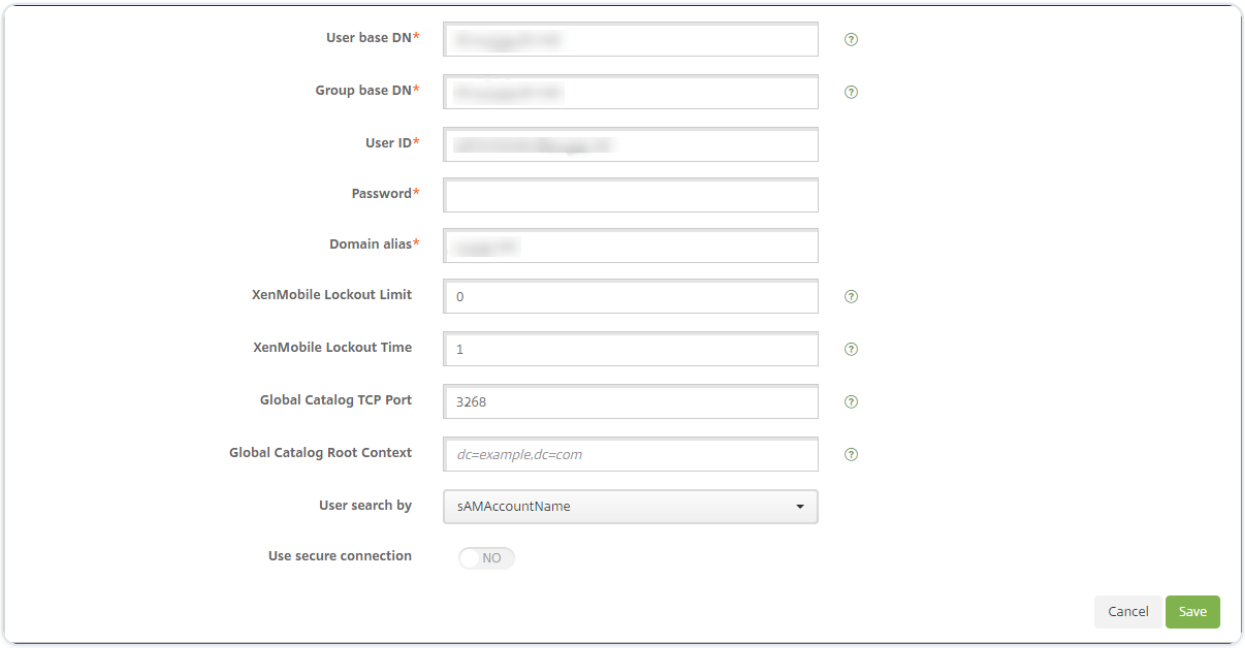


Configuración de la entrega de certificados de NetScaler Gateway en Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha. Aparecerá la pantalla **Configuración**.
2. En **Servidor**, haga clic en **NetScaler Gateway**.
3. Si NetScaler Gateway aún no se ha añadido, haga clic en **Agregar** y especifique la configuración:
    - **Nombre:** Un nombre descriptivo para el dispositivo.
    - **Alias:** Un alias opcional para el dispositivo.
    - **URL externa:** `https://YourCitrixGatewayURL`
    - **Tipo de inicio de sesión:** Seleccione **Certificado y dominio**
    - **Contraseña requerida:** Desactivado
    - **Establecer como predeterminado:** Activado
4. Para **Authentication** y **Deliver user certificate for authentication**, seleccione **On**.



5. Para **Credential Provider**, seleccione un proveedor y, a continuación, haga clic en **Guardar**.
6. Para usar los atributos sAMAccount en los certificados de usuario como alternativa al Nombre principal de usuario (UPN), configure el conector LDAP en Citrix Endpoint Management de la siguiente manera: Vaya a **Settings > LDAP**, seleccione el directorio y haga clic en **Edit**, y seleccione **sAMAccountName** en **User search by**.



Habilitar el PIN de Citrix y el almacenamiento en caché de contraseñas de usuario

Para habilitar el PIN de Citrix y el almacenamiento en caché de contraseñas de usuario, vaya a **Settings > Client Properties** y seleccione estas casillas de verificación: **Enable Citrix PIN Authentication** y **Enable User Password Caching**. Para obtener más información, consulte Client properties.

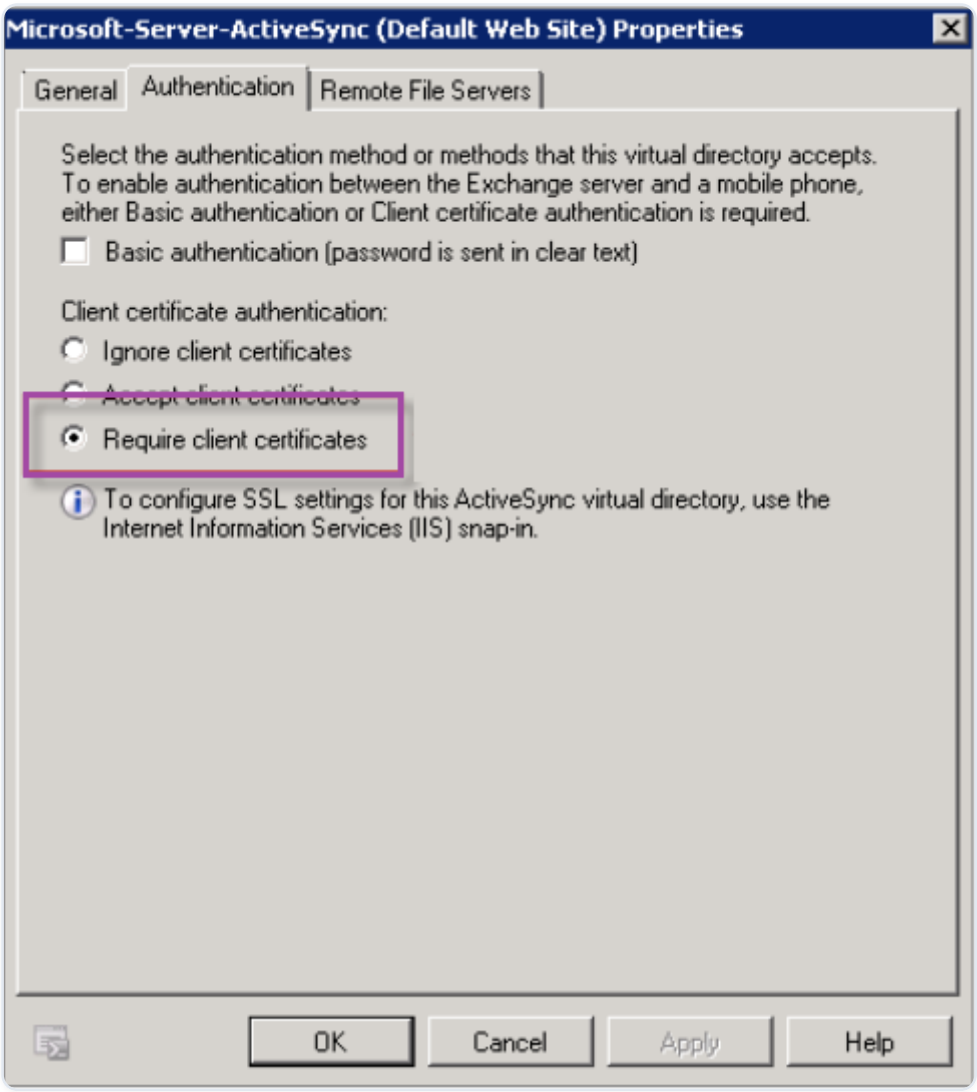
Solución de problemas de la configuración del certificado de cliente

Después de una configuración correcta de la configuración anterior más la configuración de NetScaler Gateway, el flujo de trabajo del usuario es el siguiente:

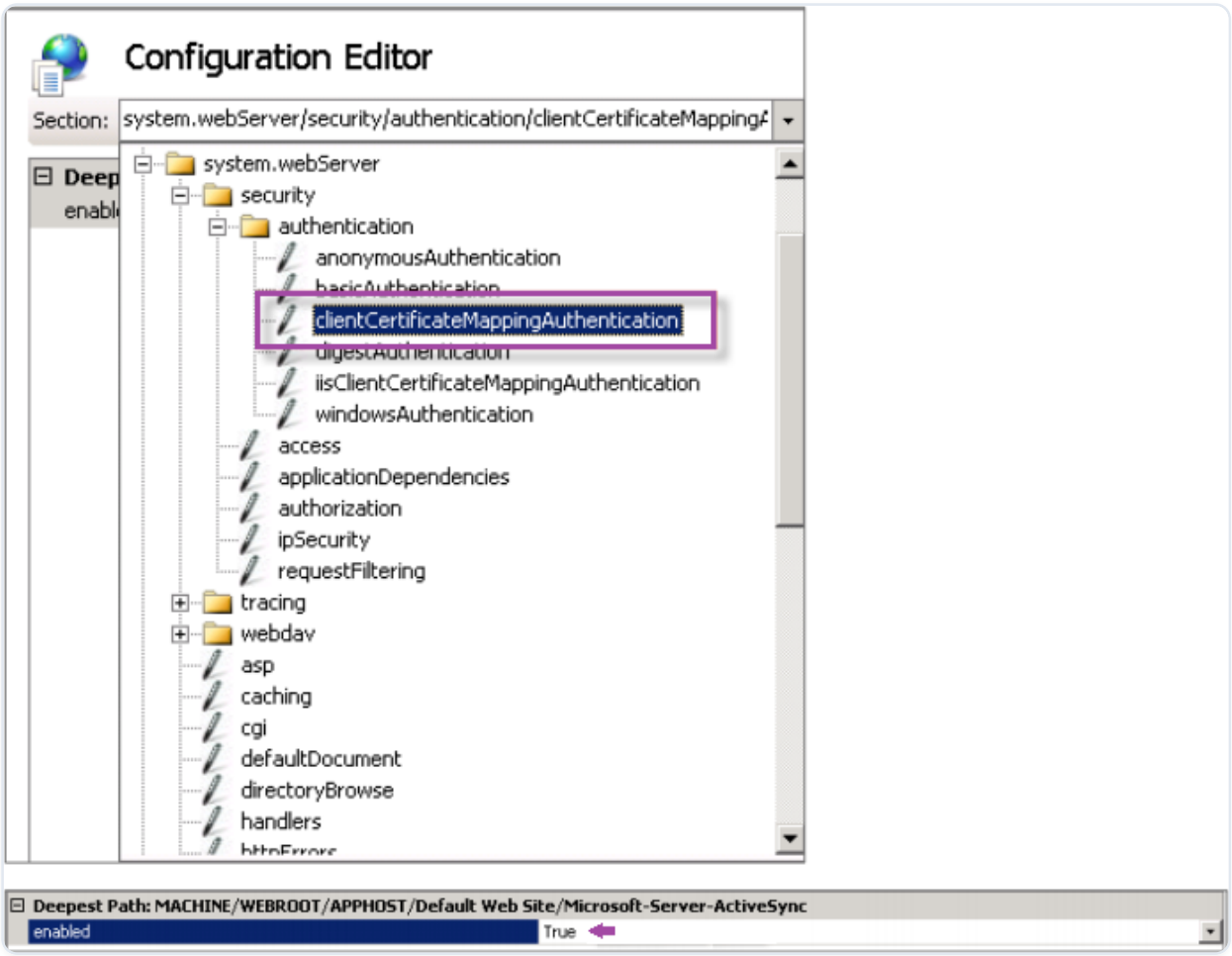
1. Los usuarios inscriben su dispositivo móvil.
2. Citrix Endpoint Management solicita a los usuarios que creen un PIN de Citrix.
3. Los usuarios son redirigidos a la tienda de aplicaciones.
4. Cuando los usuarios inician Citrix Secure Mail, Citrix Endpoint Management no les solicita credenciales de usuario para la configuración del buzón. En su lugar, Citrix Secure Mail solicita el certificado de cliente a Citrix Secure Hub y lo envía al servidor de Microsoft Exchange para su autenticación. Si Citrix Endpoint Management solicita credenciales cuando los usuarios inician Citrix Secure Mail, compruebe su configuración.

Si los usuarios pueden descargar e instalar Citrix Secure Mail, pero durante la configuración del buzón Citrix Secure Mail no logra finalizar la configuración:

1. Si Microsoft Exchange Server ActiveSync utiliza certificados de servidor SSL privados para proteger el tráfico, verificar que los certificados raíz/intermedios estén instalados en el dispositivo móvil.
2. verificar que el tipo de autenticación seleccionado para ActiveSync esté configurado como **Requerir certificados de cliente**.



3. En el servidor de Microsoft Exchange, compruebe el sitio **Microsoft-Server-ActiveSync** para verificar que la autenticación de asignación de certificados de cliente esté habilitada. De forma predeterminada, la autenticación de asignación de certificados de cliente está deshabilitada. La opción se encuentra en **Configuration Editor > Security > Authentication**.



Después de seleccionar **True**, asegúrese de hacer clic en **Apply** para que los cambios surtan efecto.

4. Compruebe la configuración de NetScaler Gateway en la consola de Citrix Endpoint Management: Asegúrese de que **Entregar certificado de usuario para autenticación** esté en **Activado** y que **Proveedor de credenciales** tenga el perfil correcto seleccionado.

Para determinar si el certificado de cliente se entregó a un dispositivo móvil

1. En la consola de Citrix Endpoint Management, vaya a **Administrar > Dispositivos** y seleccione el dispositivo.
2. Haga clic en **Editar** o **Mostrar más**.
3. Vaya a la sección **Grupos de entrega** y busque esta entrada:

   Credenciales de NetScaler Gateway: Credencial solicitada, CertId=

Para validar si la negociación del certificado de cliente está habilitada

1. Ejecute este comando `netsh` para mostrar la configuración del certificado SSL que está vinculada al sitio web de IIS:

`netsh http show sslcert`

2. Si el valor de **Negociar certificado de cliente** es **Deshabilitado**, ejecute el siguiente comando para habilitarlo:

   `netsh http delete sslcert ipport=0.0.0.0:443`

   `netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={app_id} certstorename=store_name verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable`

   Por ejemplo:

   `netsh http add sslcert ipport=0.0.0.0:443 certhash=23498dfsdfhaf98rhkjqf9823rkjhdasf98asfk appid={123asd456jd-a12b-3c45-d678-123456lkjhgf} certstorename=ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable`

Si no puede entregar certificados raíz/intermedios a un dispositivo Windows Phone 8.1 a través de Citrix Endpoint Management:

- Envíe los archivos de certificados raíz/intermedios (.cer) por correo electrónico al dispositivo Windows Phone 8.1 e instálelos directamente.

Si Citrix Secure Mail no se instala correctamente en Windows Phone 8.1, verificar lo siguiente:

- El token de inscripción de la aplicación (archivo .AETX) se entrega a través de Citrix Endpoint Management mediante la política de dispositivo de Enterprise Hub.
- El token de inscripción de la aplicación se creó utilizando el mismo certificado empresarial del proveedor de certificados utilizado para encapsular Citrix Secure Mail y firmar las aplicaciones de Citrix Secure Hub.
- Se utiliza el mismo ID de editor para firmar y encapsular Citrix Secure Hub, Citrix Secure Mail y el token de inscripción de la aplicación.

Entidades PKI

Una configuración de entidad de infraestructura de clave pública (PKI) de Citrix Endpoint Management representa un componente que realiza operaciones PKI reales (emisión, revocación

e información de estado). Estos componentes son internos o externos a Citrix Endpoint Management. Los componentes internos se denominan discrecionales. Los componentes externos forman parte de la infraestructura de su empresa.

Citrix Endpoint Management admite los siguientes tipos de entidades PKI:

- Servicios de certificados de Microsoft
- Autoridades de certificación (CA) discrecionales

Citrix Endpoint Management admite los siguientes servidores CA:

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

> **Nota:**
>
> Windows Servers 2012 R2, 2012 y 2008 R2 ya no son compatibles, ya que han llegado al final de su vida útil. Para obtener más información, consulte la documentación del ciclo de vida de los productos de Microsoft.

Conceptos comunes de PKI

Independientemente de su tipo, cada entidad PKI tiene un subconjunto de las siguientes capacidades:

- **Firmar:** Emisión de un nuevo certificado, basado en una solicitud de firma de certificado (CSR).
- **Obtener:** Recuperación de un certificado y un par de claves existentes.
- **Revocar:** Revocación de un certificado de cliente.

Acerca de los certificados de CA

Cuando configure una entidad PKI, indique a Citrix Endpoint Management qué certificado de CA es el firmante de los certificados emitidos por (o recuperados de) esa entidad. Esa entidad PKI puede devolver certificados (obtenidos o recién firmados) firmados por cualquier número de CA diferentes.

Proporcione el certificado de cada una de estas autoridades como parte de la configuración de la entidad PKI. Para ello, cargue los certificados en Citrix Endpoint Management y, a continuación, haga referencia a ellos en la entidad PKI. Para las CA discrecionales, el certificado es implícitamente el certificado de CA firmante. Para las entidades externas, debe especificar el certificado manualmente.

> **Importante:**
>
> Cuando cree una plantilla de entidad de servicios de certificados de Microsoft, evite posibles problemas de autenticación con los dispositivos inscritos: No utilice caracteres especiales en el nombre de la plantilla. Por ejemplo, no utilice: `! : $ ( ) # % + * ~ ? | { } [ ]`

Servicios de certificados de Microsoft

Citrix Endpoint Management se interconecta con los servicios de certificados de Microsoft a través de su interfaz de inscripción web. Citrix Endpoint Management solo admite la emisión de nuevos certificados a través de esa interfaz. Si la CA de Microsoft genera un certificado de usuario de NetScaler Gateway, NetScaler Gateway admite la renovación y revocación de esos certificados.

Para crear una entidad PKI de CA de Microsoft en Citrix Endpoint Management, debe especificar la URL base de la interfaz web de los servicios de certificados. Si lo desea, utilice la autenticación de cliente SSL para proteger la conexión entre Citrix Endpoint Management y la interfaz web de los servicios de certificados.

Agregar una entidad de servicios de certificados de Microsoft

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha de la consola y, a continuación, haga clic en **Entidades PKI**.
2. En la página **Entidades PKI**, haga clic en **Agregar**.

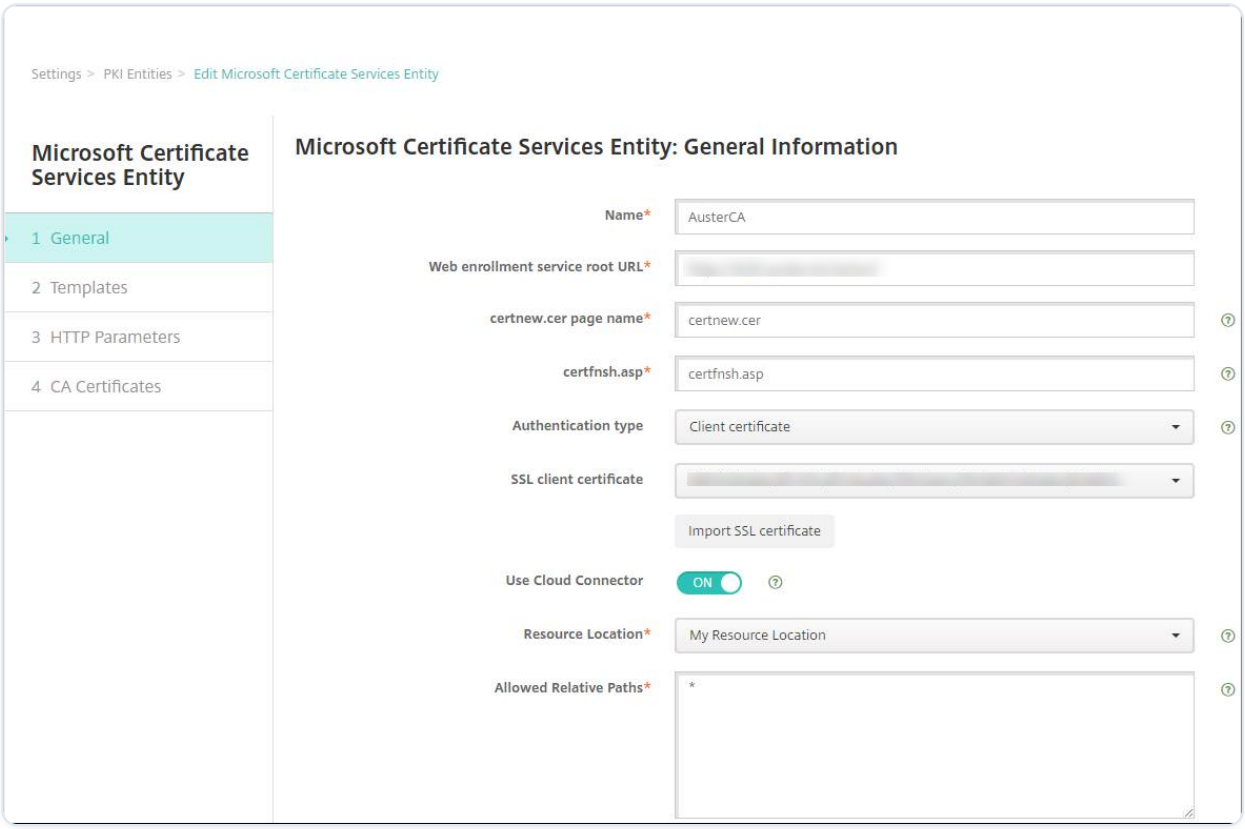
   Aparece un menú de tipos de entidad PKI.
3. Haga clic en **Entidad de servicios de certificados de Microsoft**.

   Aparece la página **Entidad de servicios de certificados de Microsoft: Información general**.
4. En la página **Entidad de servicios de certificados de Microsoft: Información general**, configure estos ajustes:

   - **Nombre:** Escriba un nombre para la nueva entidad, que utilizará más adelante para referirse a ella. Los nombres de las entidades deben ser únicos.

- **URL raíz del servicio de inscripción web:** Escriba la URL base de su servicio de inscripción web de CA de Microsoft. Por ejemplo: `https://192.0.0.1/certsrv/`. La URL puede usar HTTP simple o HTTP a través de SSL.
- **Nombre de la página certnew.cer:** El nombre de la página certnew.cer. Utilice el nombre predeterminado a menos que lo haya cambiado por algún motivo.
- **certfnsh.asp:** El nombre de la página certfnsh.asp. Utilice el nombre predeterminado a menos que lo haya cambiado por algún motivo.
- **Tipo de autenticación:** Elija el método de autenticación que desea utilizar.
  - **Ninguno**
  - **HTTP básico:** Escriba el nombre de usuario y la contraseña necesarios para conectarse.
  - **Certificado de cliente:** Elija el certificado de cliente SSL correcto.
- **Usar Cloud Connector:** Seleccione **Activado** para usar Cloud Connector para las conexiones al servidor PKI. A continuación, especifique una **Ubicación de recursos** y **Rutas relativas permitidas** para la conexión.
  - **Ubicación de recursos:** Elija entre las ubicaciones de recursos definidas en Citrix Cloud Connector.
  - **Rutas relativas permitidas:** Las rutas relativas permitidas para la ubicación de recursos especificada. Especifique una ruta por línea. Puede usar el comodín de asterisco (*).

    Supongamos que la ubicación de recursos es `https://www.ServiceRoot/certsrv`. Para proporcionar acceso a todas las URL de esa ruta, introduzca `/*` en **Rutas relativas permitidas**.



5. Haga clic en **Probar conexión** para asegurarse de que el servidor es accesible. Si no es accesible, aparecerá un mensaje indicando que la conexión falló. Compruebe la configuración.
6. Haga clic en **Siguiente**.

   Aparece la página **Entidad de servicios de certificados de Microsoft: Plantillas**. En esta página, especifica los nombres internos de las plantillas que admite su CA de Microsoft. Al crear proveedores de credenciales, selecciona una plantilla de la lista definida aquí. Cada proveedor de credenciales que utiliza esta entidad usa exactamente una de estas plantillas.

   Para conocer los requisitos de las plantillas de servicios de certificados de Microsoft, consulte la documentación de Microsoft para su versión de Microsoft Server. Citrix Endpoint Management no tiene requisitos para los certificados que distribuye, aparte de los formatos de certificado indicados en Certificados.
7. En la página **Entidad de servicios de certificados de Microsoft: Plantillas**, haga clic en **Agregar**, escriba el nombre de la plantilla y, a continuación, haga clic en **Guardar**. Repita este paso para cada plantilla que desee agregar.
8. Haga clic en **Siguiente**.

   Aparece la página **Entidad de servicios de certificados de Microsoft: Parámetros HTTP**. En esta página, especifica los parámetros personalizados que Citrix Endpoint Management debe agregar a la solicitud HTTP a la interfaz de inscripción web de Microsoft. Los parámetros personalizados solo son útiles para scripts personalizados que se ejecutan en la CA.

9. En la página **Entidad de servicios de certificados de Microsoft: Parámetros HTTP**, haga clic en **Agregar**, escriba el nombre y el valor de los parámetros HTTP que desea agregar y, a continuación, haga clic en **Siguiente**.

   Aparece la página **Entidad de servicios de certificados de Microsoft: Certificados de CA**. En esta página, debe informar a Citrix Endpoint Management de los firmantes de los certificados que el sistema obtiene a través de esta entidad. Cuando se renueve el certificado de su CA, actualícelo en Citrix Endpoint Management. Citrix Endpoint Management aplica el cambio a la entidad de forma transparente.

10. En la página **Entidad de servicios de certificados de Microsoft: Certificados de CA**, seleccione los certificados que desea usar para esta entidad.

11. Haga clic en **Guardar**.

    La entidad aparece en la tabla de entidades PKI.

Lista de revocación de certificados (CRL) de NetScaler Gateway

Citrix Endpoint Management solo admite la lista de revocación de certificados (CRL) para una entidad de certificación de terceros. Si tiene una CA de Microsoft configurada, Citrix Endpoint Management utiliza NetScaler Gateway para administrar la revocación.

Al configurar la autenticación basada en certificados de cliente, considere si configurar el ajuste de la lista de revocación de certificados (CRL) de NetScaler Gateway **Habilitar actualización automática de CRL**. Este paso garantiza que el usuario de un dispositivo en modo solo MAM no pueda autenticarse utilizando un certificado existente en el dispositivo.

Citrix Endpoint Management vuelve a emitir un nuevo certificado, porque no restringe a un usuario la generación de un certificado de usuario después de que se haya revocado uno. Esta configuración aumenta la seguridad de las entidades PKI cuando la CRL comprueba las entidades PKI caducadas.

CA discrecionales

Se crea una CA discrecional cuando se proporciona a Citrix Endpoint Management un certificado de CA y la clave privada asociada. Citrix Endpoint Management gestiona internamente la emisión, revocación e información de estado de los certificados, según los parámetros que especifique.

Al configurar una CA discrecional, puede activar la compatibilidad con el Protocolo de estado de certificados en línea (OCSP) para esa CA. Si habilita la compatibilidad con OCSP, la CA añade la

extensión `id-pe-authorityInfoAccess` a los certificados que emite. La extensión apunta al respondedor OCSP interno de Citrix Endpoint Management en la siguiente ubicación:

`https://<server>/<instance>/ocsp`

Al configurar el servicio OCSP, especifique un certificado de firma OCSP para la entidad discrecional en cuestión. Puede utilizar el propio certificado de CA como firmante. Para evitar la exposición innecesaria de su clave privada de CA (recomendado): Cree un certificado de firma OCSP delegado, firmado por el certificado de CA, e incluya esta extensión: `id-kp-OCSPSigning extendedKeyUsage`.

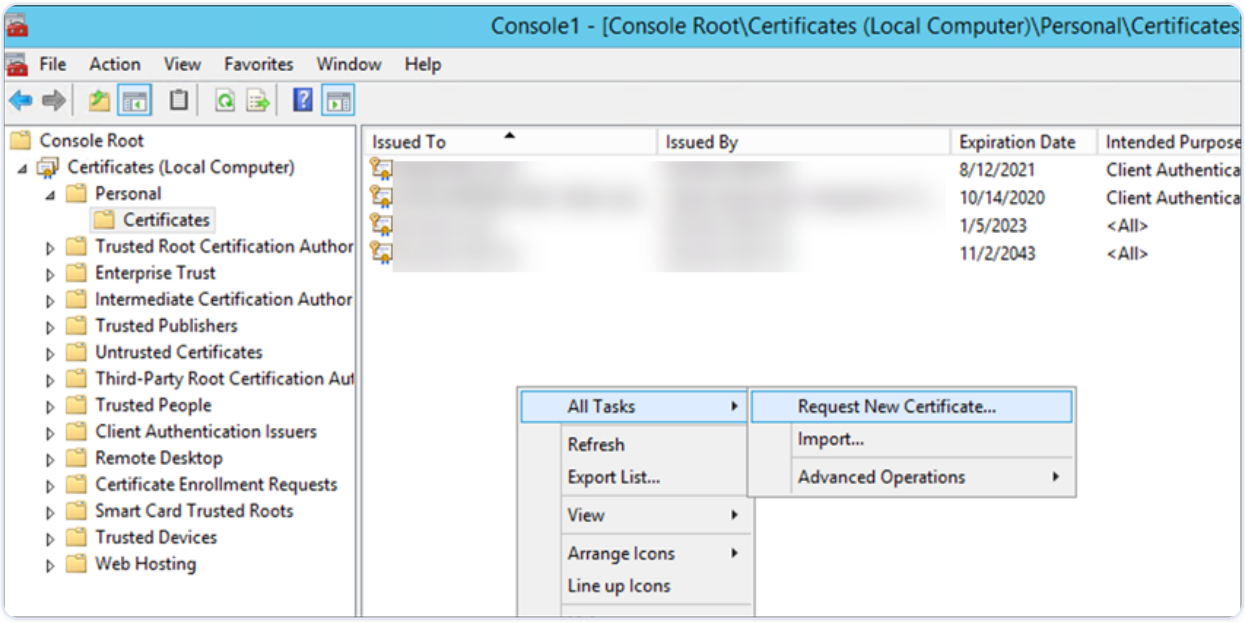
El servicio de respondedor OCSP de Citrix Endpoint Management admite respuestas OCSP básicas y los siguientes algoritmos de hash en las solicitudes:

- SHA-256
- SHA-384
- SHA-512

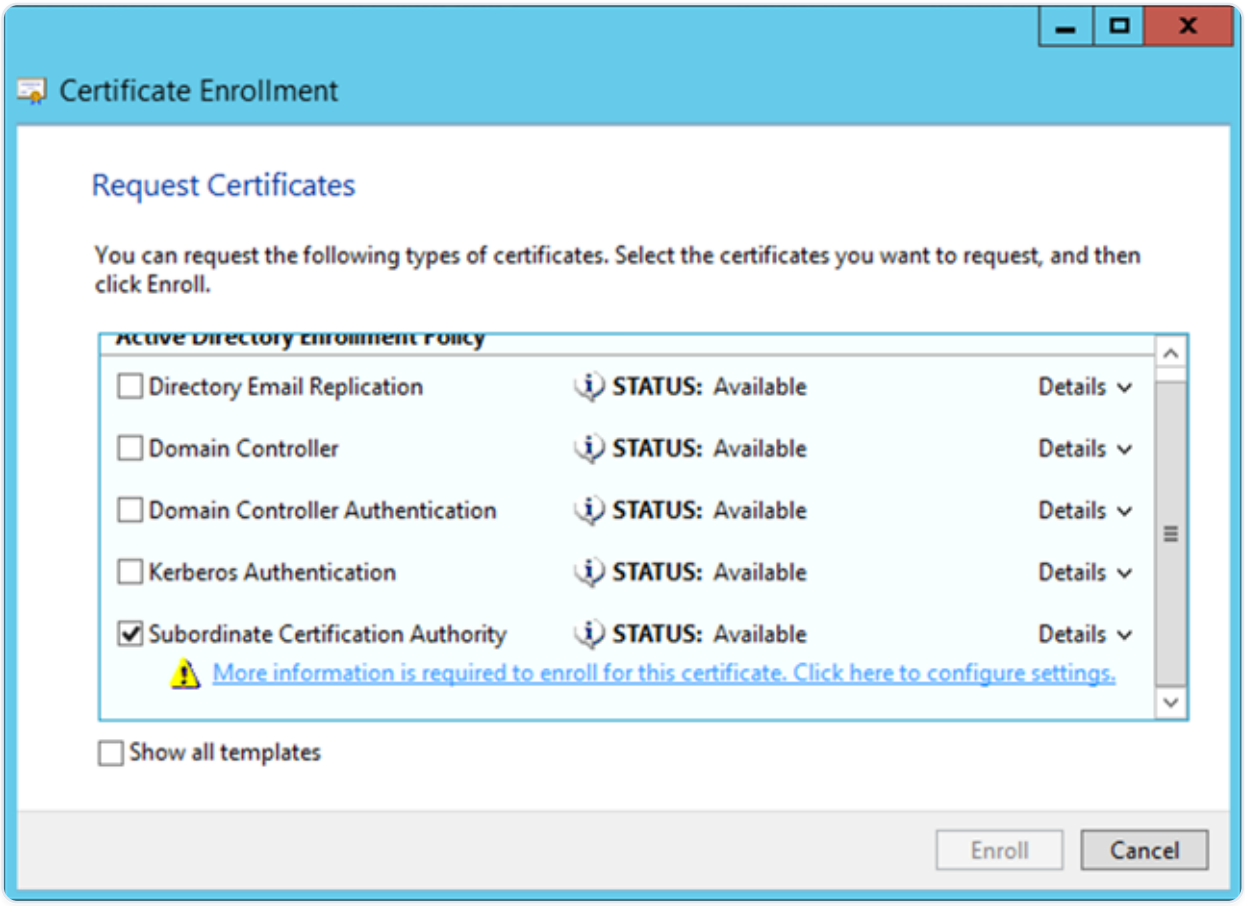
Las respuestas se firman con SHA-256 y el algoritmo de clave del certificado de firma (DSA, RSA o ECDSA).

Generar e importar un certificado para su CA

1. En su servidor, abra la Consola de administración de Microsoft (MMC) con su cuenta de sistema local y abra el complemento de certificados. En el panel de la derecha, haga clic con el botón derecho y, a continuación, haga clic en **Todas las tareas > Solicitar nuevo certificado**.



2. En el asistente que se abre, haga clic en **Siguiente** dos veces. En la lista **Solicitar certificados**, seleccione **Entidad de certificación subordinada** y, a continuación, haga clic en el enlace **Más información**.



3. En la ventana, escriba un **Nombre de sujeto** y un **Nombre alternativo**. Haga clic en **Aceptar**.

   Plantilla de CA subordinada(/en-us/citrix-endpoint-management/media/subordinate-ca-properties.png)

4. Haga clic en **Inscribir** y, a continuación, en **Finalizar**.
5. En la MMC, haga clic con el botón derecho en el certificado que creó. Haga clic en **Todas las tareas > Exportar**. Exporte el certificado como un archivo .pfx con una clave privada. Seleccione la opción **Incluir todos los certificados en la ruta de certificación si es posible**.

   Opciones de certificado(/en-us/citrix-endpoint-management/media/include-all-certificates.png)

6. En la consola de Citrix Endpoint Management, vaya a **Configuración > Certificados**.

   Página de certificados(/en-us/citrix-endpoint-management/media/certificate-loaded-in-console.png)

7. Haga clic en **Importar**. En la ventana que se abre, busque los archivos de certificado y clave privada que exportó anteriormente.

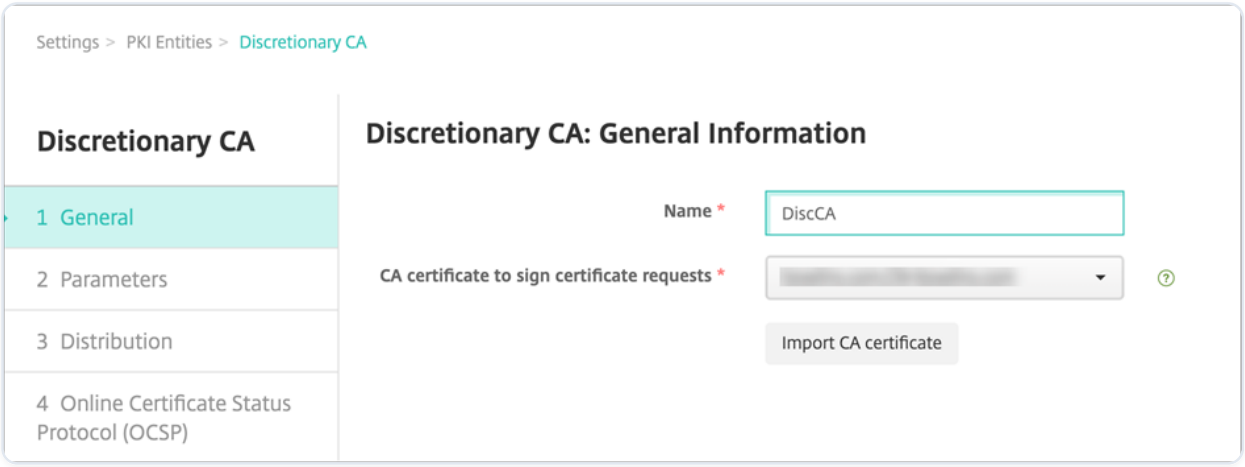
Página de certificados(/en-us/citrix-endpoint-management/media/import-certificate.png)

8. Haga clic en **Importar**. El certificado se añade a la tabla.

Agregar CA discrecionales

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha de la consola y, a continuación, haga clic en **Más > Entidades PKI**.
2. En la página **Entidades PKI**, haga clic en **Agregar**.

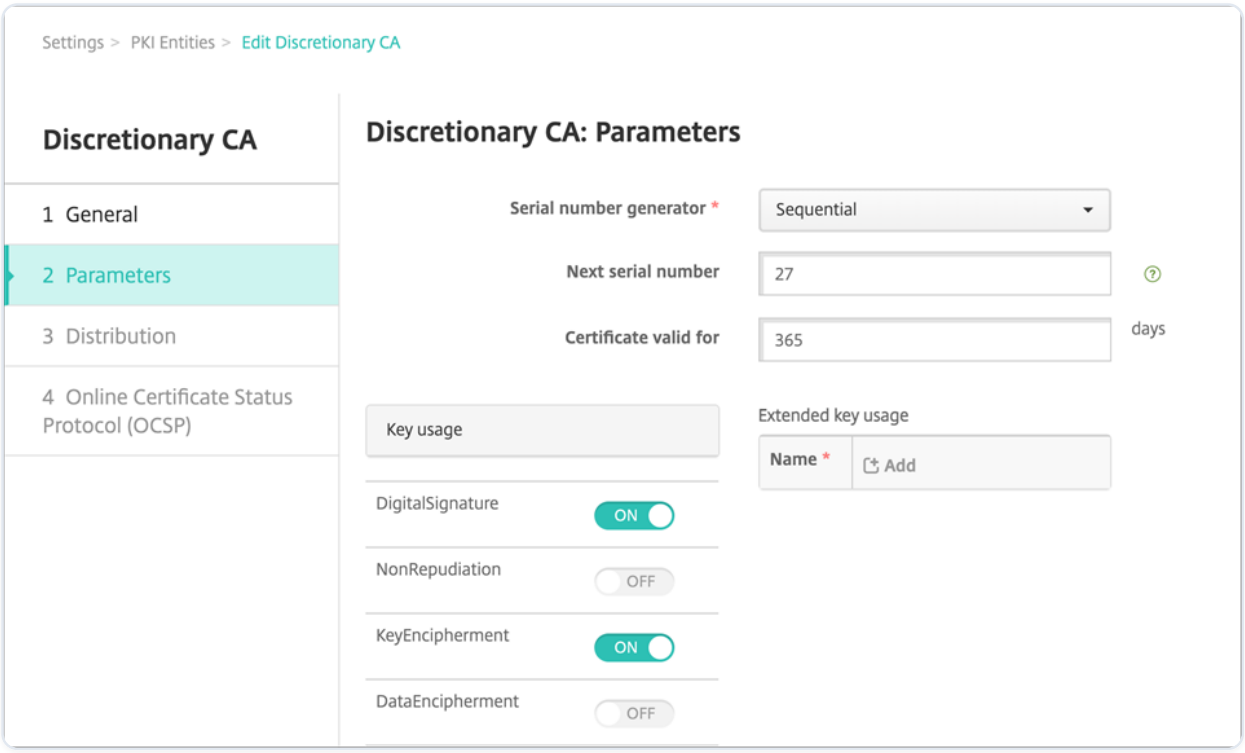
   Tipos de entidades PKI(/en-us/citrix-endpoint-management/media/pki-entities-discretionary-ca.png)
3. Haga clic en **CA discrecional**.



4. En la página **CA discrecional: Información general**, configure lo siguiente:

   - **Nombre:** Escriba un nombre descriptivo para la CA discrecional.
   - **Certificado de CA para firmar solicitudes de certificado:** Haga clic en un certificado para que la CA discrecional lo use para firmar solicitudes de certificado.

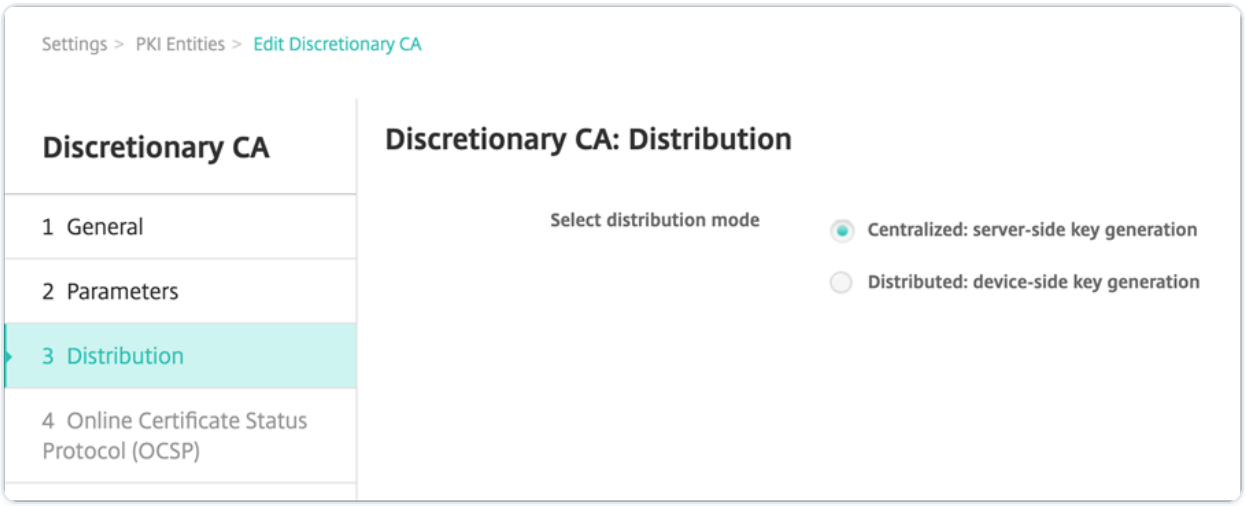
     Esta lista de certificados se genera a partir de los certificados de CA con claves privadas que cargó en Citrix Endpoint Management en **Configurar > Parámetros > Certificados**.
5. Haga clic en **Siguiente**.



6. En la página **CA discrecional: Parámetros**, configure lo siguiente:

   - **Generador de números de serie:** La CA discrecional genera números de serie para los certificados que emite. En esta lista, haga clic en **Secuencial** o **No secuencial** para determinar cómo se generan los números.
   - **Siguiente número de serie:** Escriba un valor para determinar el siguiente número emitido.
   - **Certificado válido durante:** Escriba el número de días durante los que el certificado es válido.
   - **Uso de clave:** Identifique el propósito de los certificados emitidos por la CA discrecional configurando las claves adecuadas en **Activado**. Una vez configurada, la CA se limita a emitir certificados para esos propósitos.
   - **Uso de clave extendido:** Para agregar más parámetros, haga clic en **Agregar**, escriba el nombre de la clave y, a continuación, haga clic en **Guardar**.

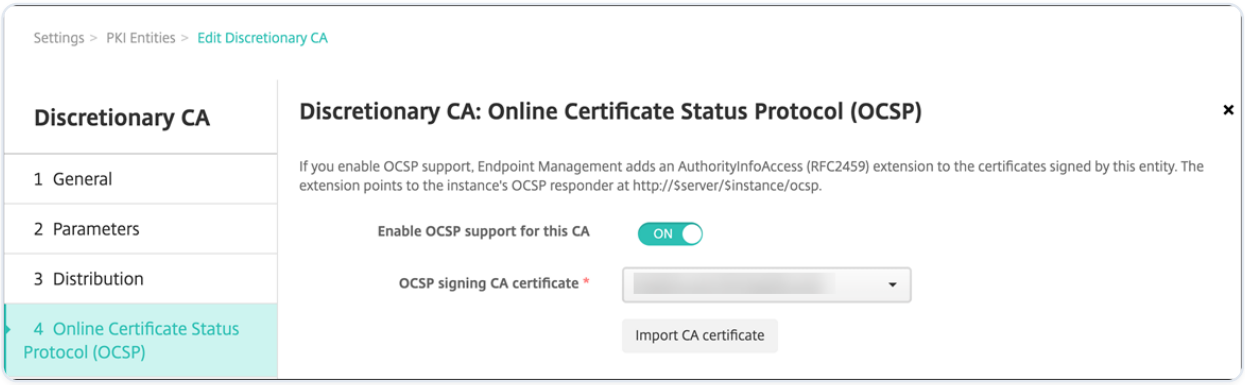
7. Haga clic en **Siguiente**.



8. En la página **CA discrecional: Distribución**, seleccione un modo de distribución:

   - **Centralizado: generación de claves en el servidor**. Citrix® recomienda la opción centralizada. Las claves privadas se generan y almacenan en el servidor y se distribuyen a los dispositivos de usuario.
   - **Distribuido: generación de claves en el dispositivo**. Las claves privadas se generan en los dispositivos de usuario. Este modo distribuido utiliza SCEP y requiere un certificado de cifrado de RA con la extensión **keyUsage keyEncryption** y un certificado de firma de RA con la extensión **keyUsage digitalSignature**. Se puede utilizar el mismo certificado tanto para el cifrado como para la firma.

9. Haga clic en **Siguiente**.



10. En la página **CA discrecional: Protocolo de estado de certificados en línea (OCSP)**, configure lo siguiente:

    - Si quiere agregar una extensión `AuthorityInfoAccess` (RFC2459) a los certificados firmados por esta CA, establezca **Habilitar compatibilidad con OCSP para esta CA** en **Activado**. Esta extensión apunta al respondedor OCSP de la CA en `https://<server>/<instance>/ocsp`.

- Si habilitó la compatibilidad con OCSP, seleccione un certificado de CA de firma de OCSP. Esta lista de certificados se genera a partir de los certificados de CA que cargó en Citrix Endpoint Management.

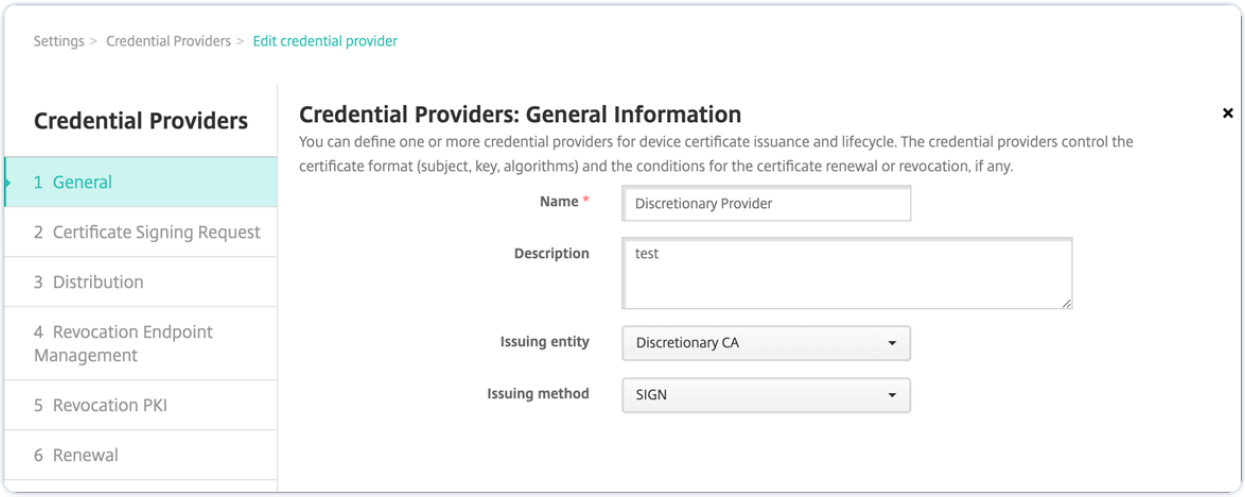
La habilitación de la función le da a Citrix ADC la oportunidad de comprobar el estado de los certificados. Citrix recomienda habilitar esta función.

11. Haga clic en **Guardar**.

    La CA discrecional aparece en la tabla Entidades PKI.

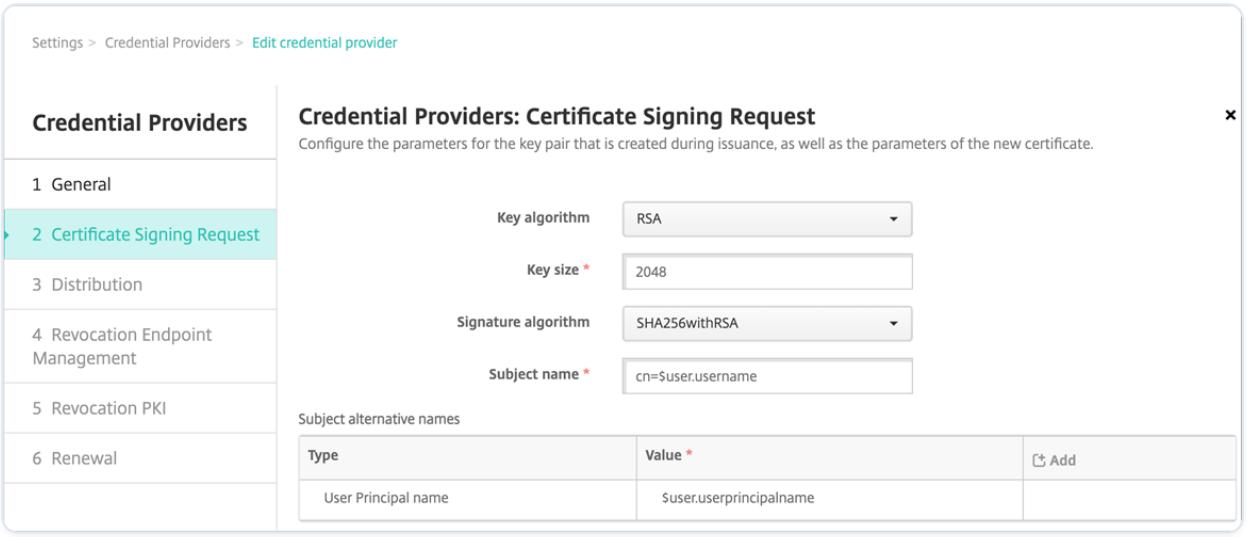
Configurar un proveedor de credenciales

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Proveedor de credenciales** y haga clic en **Agregar**.
2. En la página **Proveedores de credenciales: Información general**, configure lo siguiente:



- **Nombre:** Escriba un nombre único para la nueva configuración del proveedor. Este nombre se utiliza más adelante para identificar la configuración en otras partes de la consola de Citrix Endpoint Management.
- **Descripción:** Describa el proveedor de credenciales. Aunque este campo es opcional, una descripción puede proporcionar detalles útiles sobre este proveedor de credenciales.
- **Entidad emisora:** Seleccione **CA discrecional**.
- **Método de emisión:** Haga clic en **Firmar** o **Obtener** para que sirva como método que el sistema utiliza para obtener certificados de la entidad configurada. Para la autenticación de certificados de cliente, utilice **Firmar**.

3. Haga clic en **Siguiente**. En la página **Proveedores de credenciales: Solicitud de firma de certificado**, configure lo siguiente según la configuración de su certificado:



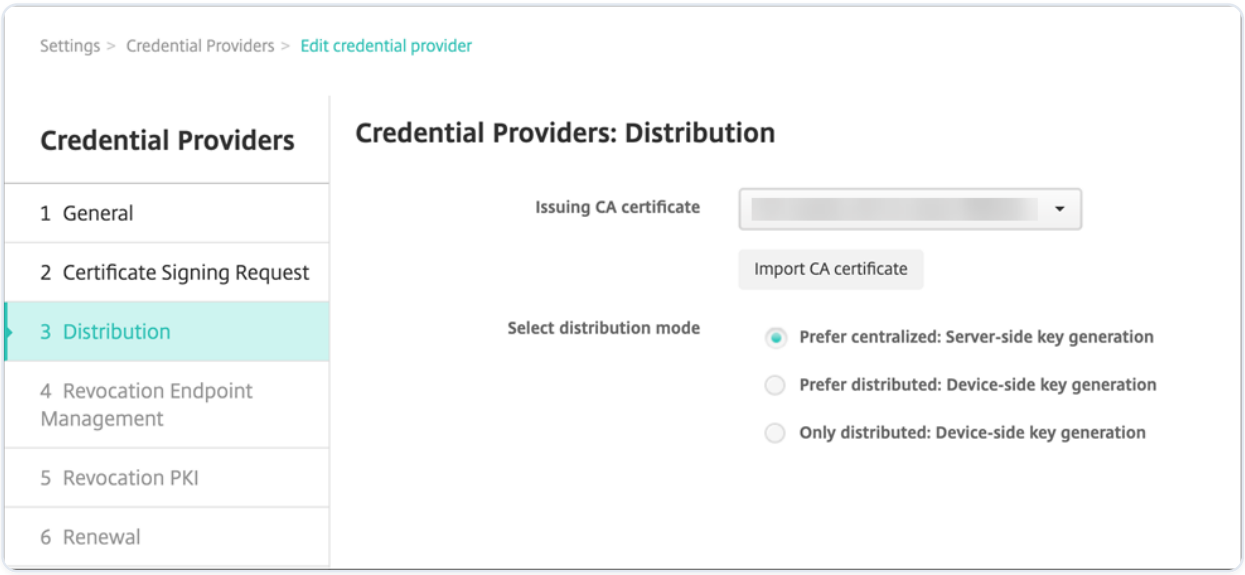
- **Algoritmo de clave:** Elija el algoritmo de clave para el nuevo par de claves. Los valores disponibles son **RSA**, **DSA** y **ECDSA**.
- **Tamaño de clave:** Escriba el tamaño, en bits, del par de claves. Este campo es obligatorio. Citrix recomienda usar **2048** bits.
- **Algoritmo de firma:** Haga clic en un valor para el nuevo certificado. Los valores dependen del algoritmo de clave. Citrix recomienda **SHA256withRSA**.
- **Nombre del sujeto:** Obligatorio. Escriba el nombre distintivo (DN) del nuevo sujeto del certificado. Utilice `CN=${user.username}` para el nombre de usuario o `CN=${user.samaccountname}` para usar el sAMAccountName.
- Para agregar una entrada a la tabla **Nombres alternativos del sujeto**, haga clic en **Agregar**. Seleccione el tipo de nombre alternativo y, a continuación, escriba un valor en la segunda columna.

  Agregue lo siguiente:

  - **Tipo:** Nombre principal de usuario
  - **Valor:** `$user.userprincipalname`

  Al igual que con el nombre del sujeto, puede usar macros de Citrix Endpoint Management en el campo de valor.

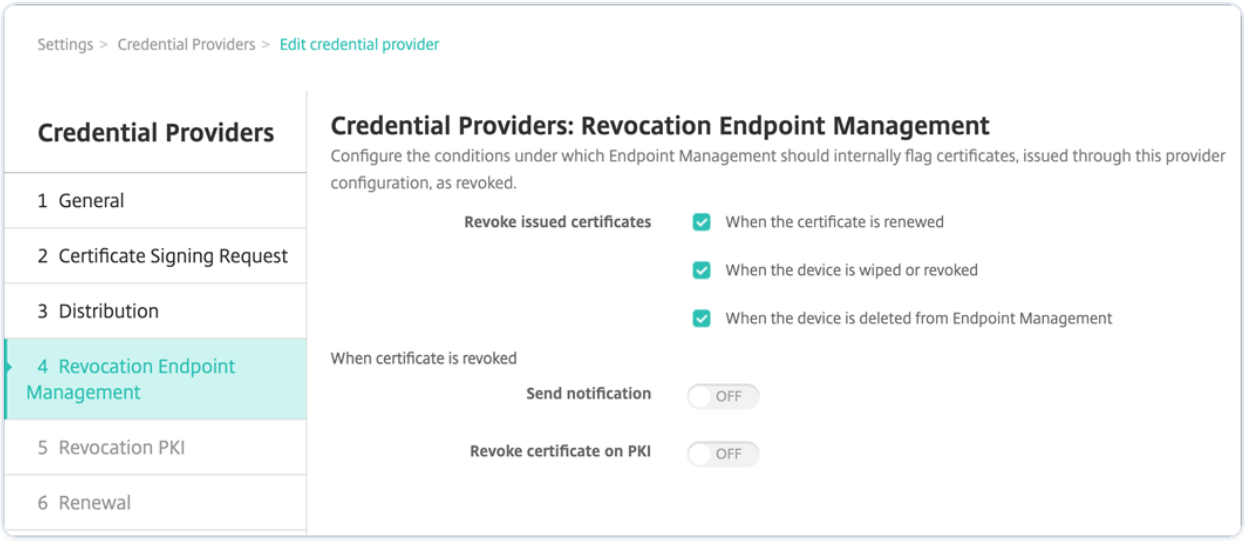
4. Haga clic en **Siguiente**. En la página **Proveedores de credenciales: Distribución**, configure lo siguiente:



- **Certificado de CA emisora:** Seleccione el certificado de CA discrecional que agregó anteriormente.
- **Seleccionar modo de distribución:** Seleccione una de las siguientes formas de generar y distribuir claves:
  - **Preferir centralizado: Generación de claves en el servidor:** Citrix recomienda esta opción centralizada. Es compatible con todas las plataformas compatibles con Citrix Endpoint Management y es necesaria cuando se utiliza la autenticación de NetScaler Gateway. Las claves privadas se generan y almacenan en el servidor y se distribuyen a los dispositivos de usuario.
  - **Preferir distribuido: Generación de claves en el dispositivo:** Las claves privadas se generan y almacenan en los dispositivos de usuario. Este modo distribuido utiliza SCEP y requiere un certificado de cifrado RA con el uso de clave keyUsage keyEncryption y un certificado de firma RA con el uso de clave KeyUsage digitalSignature. Se puede utilizar el mismo certificado tanto para el cifrado como para la firma.
  - **Solo distribuido: Generación de claves en el dispositivo:** Esta opción funciona igual que **Preferir distribuido: Generación de claves en el dispositivo**, excepto que no hay ninguna opción disponible si la generación de claves en el dispositivo falla o no está disponible.

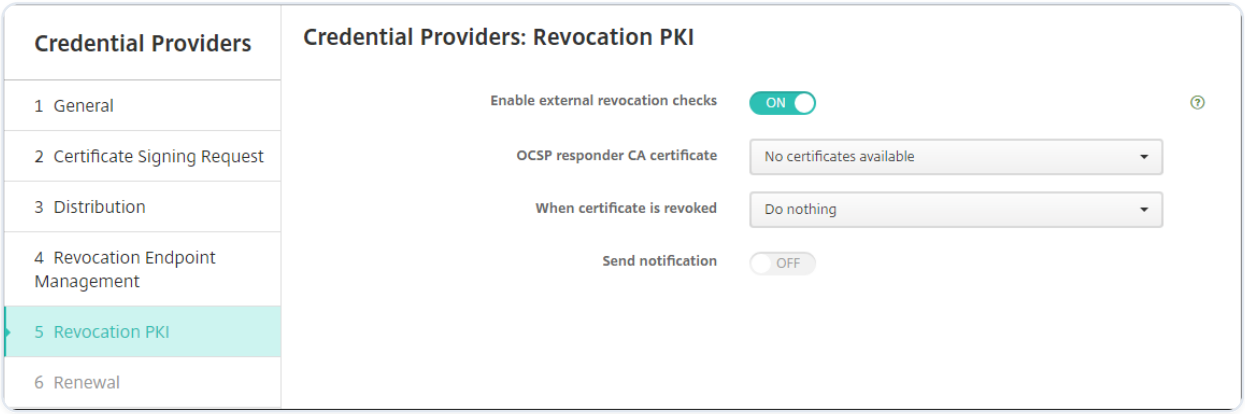
Si seleccionó **Preferir distribuido: Generación de claves en el dispositivo** o **Solo distribuido: Generación de claves en el dispositivo**, haga clic en el certificado de firma RA y en el certificado de cifrado RA. Se puede utilizar el mismo certificado para ambos. Aparecen nuevos campos para estos certificados.

5. Haga clic en **Siguiente**. En la página **Proveedores de credenciales: Revocación de Citrix Endpoint Management**, configure las condiciones bajo las cuales Citrix Endpoint Management marca internamente como revocados los certificados emitidos a través de esta configuración de proveedor. Configure lo siguiente:



   - En **Revocar certificados emitidos**, seleccione una de las opciones que indican cuándo revocar certificados.
   - Para indicar a Citrix Endpoint Management que envíe una notificación cuando se revoque el certificado: Establezca el valor de **Enviar notificación** en **Activado** y elija una plantilla de notificación.
   - **Revocar certificado en PKI** no funciona cuando se utiliza Citrix Endpoint Management como PKI discrecional.

6. Haga clic en **Siguiente**. En la página **Proveedores de credenciales: Revocación de PKI**, identifique las acciones que se deben realizar en la PKI si se revoca el certificado. También tiene la opción de crear un mensaje de notificación. Configure lo siguiente:



   - **Habilitar comprobaciones de revocación externas:** Establezca esta opción en **Activado**. Aparecerán más campos relacionados con la PKI de revocación.

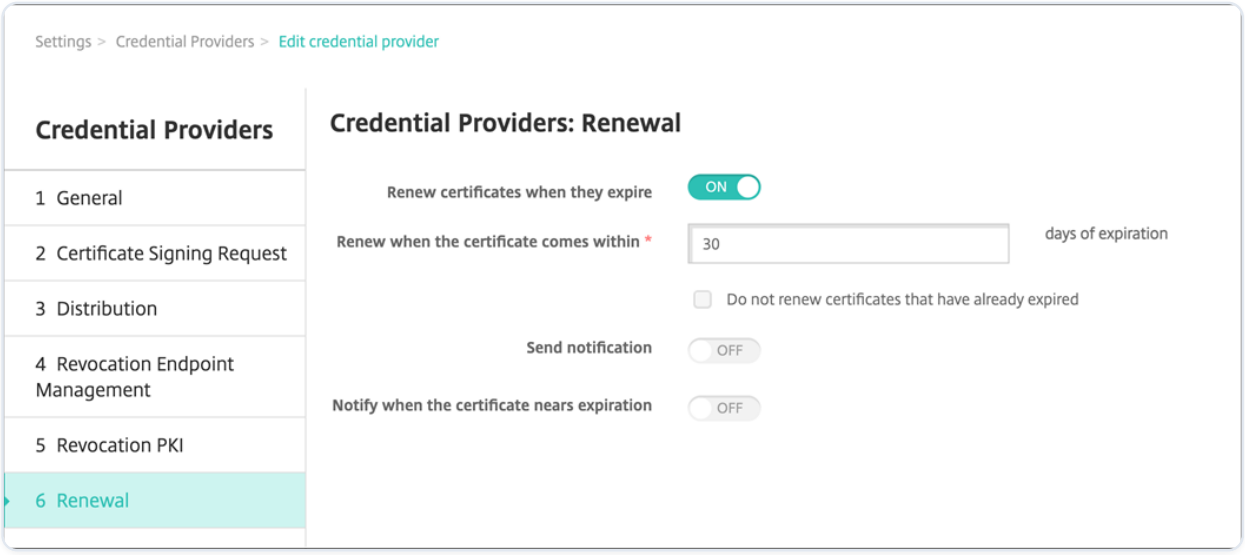
- En la lista **Certificado de CA del respondedor OCSP**, seleccione el nombre distintivo (DN) del sujeto del certificado.

  Puede usar macros de Citrix Endpoint Management para los valores del campo DN. Por ejemplo: `CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation`

- En la lista **Cuando se revoque el certificado**, haga clic en una de las siguientes acciones que se realizarán en la entidad PKI cuando se revoque el certificado:
  - No hacer nada.
  - Renovar el certificado.
  - Revocar y borrar el dispositivo.
- Para indicar a Citrix Endpoint Management que envíe una notificación cuando se revoque el certificado: Establezca el valor de **Enviar notificación** en **Activado**.

  Puede elegir entre dos opciones de notificación:
  - Si selecciona **Seleccionar plantilla de notificación**, puede elegir un mensaje de notificación preescrito que luego podrá personalizar. Estas plantillas se encuentran en la lista Plantilla de notificación.
  - Si selecciona **Introducir detalles de notificación**, puede escribir su propio mensaje de notificación. Además de proporcionar la dirección de correo electrónico del destinatario y el mensaje, puede establecer la frecuencia con la que se envía la notificación.

7. Haga clic en **Siguiente**. En la página **Proveedores de credenciales: Renovación**, configure lo siguiente:



Establezca **Renovar certificados cuando caduquen** en **Activado**. Aparecerán más campos.

- En el campo **Renovar cuando el certificado esté dentro de**, escriba cuántos días antes de la caducidad se debe renovar el certificado.
- Opcionalmente, seleccione **No renovar los certificados que ya hayan caducado**. En este caso, "ya caducado" significa que la fecha `NotAfter` es anterior, no que se haya revocado. Citrix Endpoint Management no renueva los certificados después de que se hayan revocado internamente.

Para indicar a Citrix Endpoint Management que envíe una notificación cuando se haya renovado el certificado: Establezca **Enviar notificación** en **Activado**. Para indicar a Citrix Endpoint Management que envíe una notificación cuando el certificado esté a punto de caducar: Establezca **Notificar cuando el certificado esté a punto de caducar** en **Activado**. Para cualquiera de estas opciones, puede elegir entre dos opciones de notificación:

- **Seleccionar plantilla de notificación:** Seleccione un mensaje de notificación preescrito que podrá personalizar. Estas plantillas se encuentran en la lista de plantillas de notificación.
- **Introducir detalles de la notificación:** Escriba su propio mensaje de notificación. Proporcione la dirección de correo electrónico del destinatario, un mensaje y una frecuencia para enviar la notificación.

8. Haga clic en **Guardar**.

Proveedores de credenciales

Los proveedores de credenciales son las configuraciones de certificado reales que se utilizan en las distintas partes del sistema Citrix Endpoint Management. Los proveedores de credenciales definen las fuentes, los parámetros y los ciclos de vida de los certificados. Esas operaciones se producen tanto si los certificados forman parte de las configuraciones de dispositivos como si son independientes (es decir, se envían tal cual al dispositivo).

La inscripción de dispositivos restringe el ciclo de vida del certificado. Es decir, Citrix Endpoint Management no emite certificados antes de la inscripción, aunque Citrix Endpoint Management podría emitir algunos certificados como parte de la inscripción. Además, los certificados emitidos desde la PKI interna en el contexto de una inscripción se revocan cuando se revoca la inscripción. Una vez que finaliza la relación de administración, no queda ningún certificado válido.

Puede utilizar una configuración de proveedor de credenciales en muchos lugares, de modo que una configuración puede regir cualquier número de certificados al mismo tiempo. La unidad se centra entonces en el recurso de implementación y en la implementación. Por ejemplo, si el

proveedor de credenciales P se implementa en el dispositivo D como parte de la configuración C: La configuración de emisión para P determina el certificado que se implementa en D. Del mismo modo, la configuración de renovación para D se aplica cuando se actualiza C. Y la configuración de revocación para D también se aplica cuando se elimina C o cuando se revoca D.

Según esas reglas, la configuración del proveedor de credenciales en Citrix Endpoint Management determina lo siguiente:

- El origen de los certificados.
- El método en que se obtienen los certificados: Firmar un nuevo certificado o recuperar un certificado y un par de claves existentes.
- Los parámetros para la emisión o recuperación: Por ejemplo, parámetros de solicitud de firma de certificado (CSR), como el tamaño de la clave, el algoritmo de clave y las extensiones de certificado.
- La forma en que se entregan los certificados al dispositivo.
- Condiciones de revocación: Aunque todos los certificados se revocan en Citrix Endpoint Management cuando se interrumpe la relación de administración, la configuración podría especificar una revocación anterior. Por ejemplo, la configuración puede especificar la revocación de un certificado cuando se elimina la configuración de dispositivo asociada. Además, bajo algunas condiciones, la revocación del certificado asociado en Citrix Endpoint Management podría enviarse a la infraestructura de clave pública (PKI) de back-end. Es decir, la revocación de certificados en Citrix Endpoint Management podría causar la revocación de certificados en la PKI.
- Configuración de renovación: Los certificados obtenidos a través de un proveedor de credenciales determinado pueden renovarse automáticamente cuando se acercan a su caducidad. O, independientemente de esa situación, se pueden emitir notificaciones cuando se acerca esa caducidad.

La disponibilidad de las opciones de configuración depende principalmente del tipo de entidad PKI y del método de emisión que seleccione para un proveedor de credenciales.

Método de emisión de certificados

Puede obtener un certificado, lo que se conoce como método de emisión, mediante la firma.

Con este método, la emisión implica crear una nueva clave privada, crear una CSR y enviar la CSR a una entidad de certificación (CA) para su firma. Citrix Endpoint Management admite el

método de firma tanto para entidades de servicios de certificados de MS como para entidades de CA discrecionales.

Un proveedor de credenciales utiliza el método de emisión de firma.

Entrega de certificados

Hay dos modos de entrega de certificados disponibles en Citrix Endpoint Management: centralizado y distribuido. El modo distribuido utiliza el Protocolo simple de inscripción de certificados (SCEP) y solo está disponible en situaciones en las que el cliente admite el protocolo (solo iOS). El modo distribuido es obligatorio en algunas situaciones.

Para que un proveedor de credenciales admita la entrega distribuida (asistida por SCEP), es necesario un paso de configuración especial: la configuración de los certificados de la Autoridad de registro (RA). Los certificados de RA son necesarios porque, si utiliza el protocolo SCEP, Citrix Endpoint Management actúa como un delegado (un registrador) de la autoridad de certificación real. Citrix Endpoint Management debe demostrar al cliente que tiene la autoridad para actuar como tal. Esa autoridad se establece cargando los certificados mencionados anteriormente en Citrix Endpoint Management.

Se requieren dos funciones de certificado distintas (aunque un solo certificado puede cumplir ambos requisitos): firma de RA y cifrado de RA. Las restricciones para estas funciones son las siguientes:

- El certificado de firma de RA debe tener el uso de clave X.509 de firma digital.
- El certificado de cifrado de RA debe tener el uso de clave X.509 de cifrado de clave.

Para configurar los certificados de RA del proveedor de credenciales, cargue los certificados en Citrix Endpoint Management y, a continuación, vincúlelos en el proveedor de credenciales.

Un proveedor de credenciales se considera compatible con la entrega distribuida solo si el proveedor tiene un certificado configurado para las funciones de certificado. Puede configurar cada proveedor de credenciales para que prefiera el modo centralizado, el modo distribuido o para que requiera el modo distribuido. El resultado real depende del contexto: si el contexto no admite el modo distribuido, pero el proveedor de credenciales requiere este modo, la implementación falla. Del mismo modo, si el contexto requiere el modo distribuido, pero el proveedor de credenciales no admite el modo distribuido, la implementación falla. En todos los demás casos, se respeta la configuración preferida.

La siguiente tabla muestra la distribución de SCEP en Citrix Endpoint Management:

CONTEXTO	SCEP ADMITIDO	SCEP REQUERIDO
Servicio de perfiles de iOS	Sí	Sí
Inscripción en la administración de dispositivos móviles (MDM) de iOS	Sí	No
Perfiles de configuración de iOS	Sí	No
Inscripción en SHTP	No	No
Configuración de SHTP	No	No
Inscripción de tabletas Windows	No	No
Configuración de tablet Windows	No, excepto para la directiva de dispositivos de red, que es compatible con las versiones de Windows 10 y Windows 11	No

Revocación de certificados

Existen tres tipos de revocación.

- **Revocación interna:** La revocación interna afecta al estado del certificado tal como lo mantiene Citrix Endpoint Management. Citrix Endpoint Management considera este estado al evaluar un certificado presentado o al proporcionar información de estado OCSP para un certificado. La configuración del proveedor de credenciales determina cómo se ve afectado este estado bajo diversas condiciones. Por ejemplo, el proveedor de credenciales podría especificar que los certificados se marquen como revocados cuando se eliminan del dispositivo.
- **Revocación propagada externamente:** También conocida como Revocación de Citrix Endpoint Management, este tipo de revocación se aplica a los certificados obtenidos de una PKI externa. El certificado se revoca en la PKI cuando Citrix Endpoint Management revoca internamente el certificado, bajo las condiciones definidas por la configuración del proveedor de credenciales.

- **Revocación inducida externamente:** También conocida como Revocación de PKI, este tipo de revocación también se aplica únicamente a los certificados obtenidos de una PKI externa. Cada vez que Citrix Endpoint Management evalúa el estado de un certificado determinado, Citrix Endpoint Management consulta a la PKI sobre dicho estado. Si el certificado está revocado, Citrix Endpoint Management revoca internamente el certificado. Este mecanismo utiliza el protocolo OCSP.

Estos tres tipos no son exclusivos, sino que se aplican conjuntamente. Una revocación externa o un hallazgo independiente pueden causar una revocación interna. Una revocación interna puede afectar potencialmente a una revocación externa.

Renovación de certificados

Una renovación de certificado es la combinación de la revocación del certificado existente y la emisión de otro certificado.

Citrix Endpoint Management intenta primero obtener el nuevo certificado antes de revocar el certificado anterior, para evitar la interrupción del servicio si la emisión falla. Para la entrega distribuida (compatible con SCEP), la revocación también solo ocurre después de que el certificado se haya instalado correctamente en el dispositivo. De lo contrario, la revocación ocurre antes de que el nuevo certificado se envíe al dispositivo. Esa revocación es independiente del éxito o fracaso de la instalación del certificado.

La configuración de revocación requiere que especifique una duración determinada (en días). Cuando el dispositivo se conecta, el servidor verifica si la fecha `NotAfter` del certificado es posterior a la fecha actual, menos la duración especificada. Si el certificado cumple esa condición, Citrix Endpoint Management intenta renovar el certificado.

Crear un proveedor de credenciales

La configuración de un proveedor de credenciales varía principalmente en función de la entidad emisora y el método de emisión que seleccione para el proveedor de credenciales. Puede distinguir entre proveedores de credenciales que utilizan una entidad interna o una entidad externa:

- Una entidad discrecional, que es interna a Citrix Endpoint Management, es una entidad interna. El método de emisión para una entidad discrecional es siempre firmar. Firmar significa que, con cada operación de emisión, Citrix Endpoint Management firma un nuevo par de claves con el certificado de CA seleccionado para la entidad. Si el par de claves se genera en el dispositivo o en el servidor depende del método de distribución que seleccione.

- Una entidad externa, que forma parte de su infraestructura corporativa, incluye Microsoft CA.

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha y, a continuación, haga clic en **Settings > Credential Providers**.
2. En la página **Credential Providers**, haga clic en **Add**.

   Aparece la página **Credential Providers: General Information**.
3. En la página **Credential Providers: General Information**, haga lo siguiente:

   - **Nombre:** Escriba un nombre único para la nueva configuración del proveedor. Este nombre se utiliza más adelante para identificar la configuración en otras partes de la consola de Citrix Endpoint Management.
   - **Descripción:** Describa el proveedor de credenciales. Aunque este campo es opcional, una descripción puede proporcionar detalles útiles sobre este proveedor de credenciales.
   - **Entidad emisora:** Haga clic en la entidad emisora del certificado.
   - **Método de emisión:** Haga clic en **Sign** o **Fetch** para que sirva como método que el sistema utiliza para obtener certificados de la entidad configurada. Para la autenticación de certificados de cliente, utilice **Sign**.
   - Si la lista **Template** está disponible, seleccione la plantilla que agregó en la entidad PKI para el proveedor de credenciales.

     Estas plantillas están disponibles cuando se agregan entidades de servicios de certificados de Microsoft en **Settings > PKI Entities**.
4. Haga clic en **Next**.

   Aparece la página **Credential Providers: Certificate Signing Request**.
5. En la página **Proveedores de credenciales: Solicitud de firma de certificado**, configure lo siguiente según la configuración de su certificado:

   - **Algoritmo de clave:** Elija el algoritmo de clave para el nuevo par de claves. Los valores disponibles son **RSA**, **DSA** y **ECDSA**.
   - **Tamaño de clave:** Escriba el tamaño, en bits, del par de claves. Este campo es obligatorio.

     Los valores permitidos dependen del tipo de clave. Por ejemplo, el tamaño máximo para las claves DSA es de 2048 bits. Para evitar falsos negativos, que dependen del hardware y software subyacentes, Citrix Endpoint Management no impone tamaños de clave. Pruebe siempre las configuraciones del proveedor de credenciales en un entorno de prueba antes de activarlas en producción.

- **Algoritmo de firma:** Haga clic en un valor para el nuevo certificado. Los valores dependen del algoritmo de clave.
- **Nombre del sujeto:** Obligatorio. Escriba el Nombre Distinguido (DN) del nuevo sujeto del certificado. Por ejemplo: `CN=${user.username}, OU=${user.department}, O=${user.companyname},C=${user.c}\endquotation`

  Por ejemplo, para la autenticación de certificados de cliente, utilice esta configuración:

  - **Algoritmo de clave:** RSA
  - **Tamaño de clave:** 2048
  - **Algoritmo de firma:** SHA256withRSA
  - **Nombre del sujeto:** `cn=$user.username`
- Para añadir una entrada a la tabla **Nombres alternativos del sujeto**, haga clic en **Añadir**. Seleccione el tipo de nombre alternativo y, a continuación, escriba un valor en la segunda columna.

  Para la autenticación de certificados de cliente, especifique:

  - **Tipo:** Nombre principal de usuario
  - **Valor:** `$user.userprincipalname`

    Al igual que con el nombre del sujeto, puede usar macros de Citrix Endpoint Management en el campo de valor.

6. Haga clic en **Siguiente**.

   Aparece la página **Proveedores de credenciales: Distribución**.

7. En la página **Proveedores de credenciales: Distribución**, haga lo siguiente:

   - En la lista **Certificado de CA emisor**, haga clic en el certificado de CA ofrecido. Dado que el proveedor de credenciales utiliza una entidad de CA discrecional, el certificado de CA para el proveedor de credenciales es siempre el certificado de CA configurado en la propia entidad. El certificado de CA se presenta aquí para mantener la coherencia con las configuraciones que utilizan entidades externas.
   - En **Seleccionar modo de distribución**, haga clic en una de las siguientes formas de generar y distribuir claves:

     - **Preferir centralizado: Generación de claves en el servidor:** Citrix recomienda esta opción centralizada. Es compatible con todas las plataformas compatibles con Citrix

Endpoint Management y es necesaria cuando se utiliza la autenticación de NetScaler Gateway. Las claves privadas se generan y almacenan en el servidor y se distribuyen a los dispositivos de los usuarios.

- **Preferir distribuido: Generación de claves en el dispositivo:** Las claves privadas se generan y almacenan en los dispositivos de los usuarios. Este modo distribuido utiliza SCEP y requiere un certificado de cifrado de RA con el uso de clave keyEncryption y un certificado de firma de RA con el uso de clave digitalSignature. Se puede usar el mismo certificado para el cifrado y la firma.
- **Solo distribuido: Generación de claves en el dispositivo:** Esta opción funciona igual que Preferir distribuido: Generación de claves en el dispositivo, salvo que, al ser "Solo" en lugar de "Preferir", no hay ninguna opción disponible si la generación de claves en el dispositivo falla o no está disponible.

Si seleccionó **Preferir distribuido: Generación de claves en el dispositivo** o **Solo distribuido: Generación de claves en el dispositivo**, haga clic en el certificado de firma de RA y en el certificado de cifrado de RA. Se puede usar el mismo certificado para ambos. Aparecen nuevos campos para estos certificados.

8. Haga clic en **Siguiente**.

   Aparece la página **Proveedores de credenciales: Revocación de Citrix Endpoint Management**. En esta página, se configuran las condiciones bajo las cuales Citrix Endpoint Management marca internamente como revocados los certificados emitidos a través de esta configuración de proveedor.

9. En la página **Proveedores de credenciales: Revocación de Citrix Endpoint Management**, haga lo siguiente:

   - En **Revocar certificados emitidos**, seleccione una de las opciones que indican cuándo revocar certificados.
   - Para indicar a Citrix Endpoint Management que envíe una notificación cuando se revoque el certificado: Establezca el valor de **Enviar notificación** en **Activado** y elija una plantilla de notificación.
   - Para revocar el certificado en la PKI cuando se revoca el certificado de Citrix Endpoint Management: Establezca **Revocar certificado en PKI** en **Activado** y, en la **Lista de entidades**, haga clic en una plantilla. La Lista de entidades muestra todas las entidades disponibles con capacidades de revocación. Cuando el certificado se revoca de Citrix Endpoint Management, se envía una llamada de revocación a la PKI seleccionada de la Lista de entidades.

10. Haga clic en **Siguiente**.

    Aparece la página **Proveedores de credenciales: PKI de revocación**. En esta página, identifique las acciones que se deben realizar en la PKI si se revoca el certificado. También tiene la opción de crear un mensaje de notificación.

11. En la página **Proveedores de credenciales: PKI de revocación**, haga lo siguiente si quiere revocar certificados de la PKI:

    - Cambie la configuración de **Habilitar comprobaciones de revocación externas** a **Activado**. Aparecen más campos relacionados con la PKI de revocación.
    - En la lista **Certificado de CA del respondedor OCSP**, haga clic en el nombre distintivo (DN) del sujeto del certificado.

      Puede usar macros de Citrix Endpoint Management para los valores de campo de DN. Por ejemplo: `CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation`
    - En la lista **Cuando se revoca el certificado**, haga clic en una de las siguientes acciones que se realizarán en la entidad PKI cuando se revoque el certificado:
      - No hacer nada.
      - Renovar el certificado.
      - Revocar y borrar el dispositivo.
    - Para indicar a Citrix Endpoint Management que envíe una notificación cuando se revoque el certificado: Establezca el valor de **Enviar notificación** en **Activado**.

      Puede elegir entre dos opciones de notificación:
    - Si selecciona **Seleccionar plantilla de notificación**, puede seleccionar un mensaje de notificación preescrito que luego puede personalizar. Estas plantillas se encuentran en la lista Plantilla de notificación.
    - Si selecciona **Introducir detalles de notificación**, puede escribir su propio mensaje de notificación. Además de proporcionar la dirección de correo electrónico del destinatario y el mensaje, puede establecer la frecuencia con la que se envía la notificación.

12. Haga clic en **Siguiente**.

    Aparece la página **Proveedores de credenciales: Renovación**. En esta página, puede configurar Citrix Endpoint Management para que haga lo siguiente:

- Renovar el certificado. Opcionalmente, puede enviar una notificación de renovación y, opcionalmente, excluir de la operación los certificados ya caducados.
- Emitir una notificación para los certificados próximos a caducar (notificación antes de la renovación).

13. En la página **Proveedores de credenciales: Renovación**, haga lo siguiente si quiere renovar los certificados cuando caduquen:

    Establezca **Renovar certificados** cuando caduquen en **Activado**. Aparecen más campos.

    - En el campo **Renovar cuando el certificado esté dentro de**, escriba cuántos días antes de la caducidad se debe renovar el certificado.
    - Opcionalmente, seleccione **No renovar los certificados que ya hayan caducado**. En este caso, "ya caducado" significa que la fecha `NotAfter` es anterior, no que se haya revocado. Citrix Endpoint Management no renueva los certificados después de que se hayan revocado internamente.

    Para indicar a Citrix Endpoint Management que envíe una notificación cuando se haya renovado el certificado: Establezca **Enviar notificación** en **Activado**. Para indicar a Citrix Endpoint Management que envíe una notificación cuando el certificado esté próximo a caducar: Establezca **Notificar cuando el certificado esté próximo a caducar** en **Activado**. Para cualquiera de estas opciones, puede elegir entre dos opciones de notificación:

    - **Seleccionar plantilla de notificación:** Seleccione un mensaje de notificación preescrito que luego podrá personalizar. Estas plantillas se encuentran en la lista de plantillas de notificación.
    - **Introducir detalles de la notificación:** Escriba su propio mensaje de notificación. Proporcione la dirección de correo electrónico del destinatario, un mensaje y una frecuencia para enviar la notificación.

    En el campo **Notificar cuando el certificado esté dentro de**, escriba cuántos días antes de la caducidad del certificado se debe enviar la notificación.

14. Haga clic en **Guardar**.

    El proveedor de credenciales aparece en la tabla de proveedores de credenciales.

Certificados APNs

Para inscribir y administrar dispositivos Apple en Citrix Endpoint Management, debe configurar un certificado del servicio de notificaciones push de Apple (APNs) de Apple. El certificado permite la administración de dispositivos móviles a través de la red push de Apple.

Resumen del flujo de trabajo:

Paso 1: (#create-a-certificate-signing-request) (CSR) mediante cualquiera de estos métodos:

- (#create-a-csr-by-using-keychain-access-on-macos) (recomendado por Citrix®)
- (#create-a-csr-by-using-microsoft-iis)
- (#create-a-csr-by-using-openssl)

Paso 2: Firmar la CSR en las herramientas de Citrix Endpoint Management

Paso 3: (#submit-the-signed-csr-to-apple-to-get-the-apns-certificate)

Paso 4: Con el mismo equipo utilizado en el Paso 1, (#complete-the-csr-and-export-a-pkcs-12-file) :

- (#create-a-pkcs-12-file-by-using-keychain-access-on-macos)
- (#create-a-pkcs-12-file-by-using-microsoft-iis)
- (#create-a-pkcs-12-file-by-using-openssl)

Paso 5: Importar un certificado APNs en Citrix Endpoint Management

Paso 6: (#renew-an-apns-certificate)

Crear una solicitud de firma de certificado

Recomendamos que cree una CSR mediante Acceso a Llaveros en macOS. También puede crear una CSR mediante Microsoft IIS u OpenSSL.

> **Importante:**

> - Para el ID de Apple utilizado para crear el certificado:
>   - El ID de Apple debe ser un ID corporativo y no un ID personal.

    - Anote el ID de Apple que utiliza para crear el certificado.
    - Para renovar el certificado, utilice el mismo nombre de organización y el mismo ID de Apple. El uso de un ID de Apple diferente para renovar el certificado requiere volver a inscribir el dispositivo.

- Si revoca el certificado de forma accidental o intencionada, perderá la capacidad de administrar sus dispositivos.
- Si utilizó el Programa para desarrolladores empresariales de iOS para crear un certificado push del administrador de dispositivos móviles: asegúrese de gestionar cualquier acción para los certificados migrados en el Portal de certificados push de Apple.

Crear una CSR mediante Acceso a Llaveros en macOS

1. En un equipo con macOS, en **Aplicaciones > Utilidades**, inicie la aplicación Acceso a Llaveros.
2. Abra el menú **Acceso a Llaveros** y, a continuación, haga clic en **Asistente para Certificados > Solicitar un certificado a una autoridad de certificación**.
3. El Asistente para Certificados le pide que introduzca la siguiente información:
    - **Dirección de correo electrónico:** Dirección de correo electrónico de la persona o cuenta de rol que administra el certificado.
    - **Nombre común:** Nombre común de la persona o cuenta de rol que administra el certificado.
    - **Dirección de correo electrónico de la CA:** Dirección de correo electrónico de la Autoridad de Certificación.
4. Seleccione las opciones **Guardar en disco** y **Permitirme especificar la información del par de claves** y, a continuación, haga clic en **Continuar**.
5. Introduzca un nombre para el archivo CSR, guarde el archivo en su equipo y, a continuación, haga clic en **Guardar**.
6. Especifique la información del par de claves: Seleccione el **Tamaño de clave** de 2048 bits y el **algoritmo RSA** y, a continuación, haga clic en **Continuar**. El archivo CSR está listo para que lo cargue como parte del proceso de certificado APNs.
7. Haga clic en **Listo** cuando el Asistente de certificados complete el proceso de CSR.
8. Para continuar, Firme el CSR.

Crear un CSR mediante Microsoft IIS

El primer paso para generar una solicitud de certificado APNs es crear una Solicitud de firma de certificado (CSR). Para Windows, genere un CSR mediante Microsoft IIS.

1. Abra Microsoft IIS.
2. Haga doble clic en el icono Certificados de servidor para IIS.
3. En la ventana **Certificados de servidor**, haga clic en **Crear solicitud de certificado**.
4. Escriba la información adecuada del Nombre distintivo (DN). Por ejemplo, puede escribir el nombre de dominio completo (FQDN) de su servidor Citrix Endpoint Management, como `www.domain.com`. A continuación, haga clic en **Siguiente**.
5. Seleccione **Microsoft RSA SChannel Cryptographic Provider** para el Proveedor de servicios criptográficos y **2048** para la longitud de bits y, a continuación, haga clic en **Siguiente**.
6. Introduzca un nombre de archivo y especifique una ubicación para guardar el CSR y, a continuación, haga clic en **Finalizar**.
7. Para continuar, Firme el CSR.

Crear un CSR usando OpenSSL

Si no puede usar un dispositivo macOS o Microsoft IIS para generar un CSR, use OpenSSL. Puede descargar e instalar OpenSSL desde el sitio web de OpenSSL.

1. En el equipo donde instale OpenSSL, ejecute el siguiente comando desde un símbolo del sistema o shell.

   `openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.csr -newkey rsa:2048`

2. Aparece el siguiente mensaje para la información de nombres de certificado. Introduzca la información según se solicite.

   ```
   You are about to be asked to enter information that will be
   incorporated into your certificate request.

   What you are about to enter is what is called a Distinguished Name or a
   DN.

   There are quite a few fields but you can leave some blank

   For some fields there will be a default value,
   ```

```
If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:CA

Locality Name (eg, city) []:RWC

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer

Organizational Unit Name (eg, section) [:Marketing

Common Name (eg, YOUR name) []:John Doe

Email Address []:john.doe@customer.com
```

3. En el siguiente mensaje, introduzca una contraseña para la clave privada del CSR.

```
Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

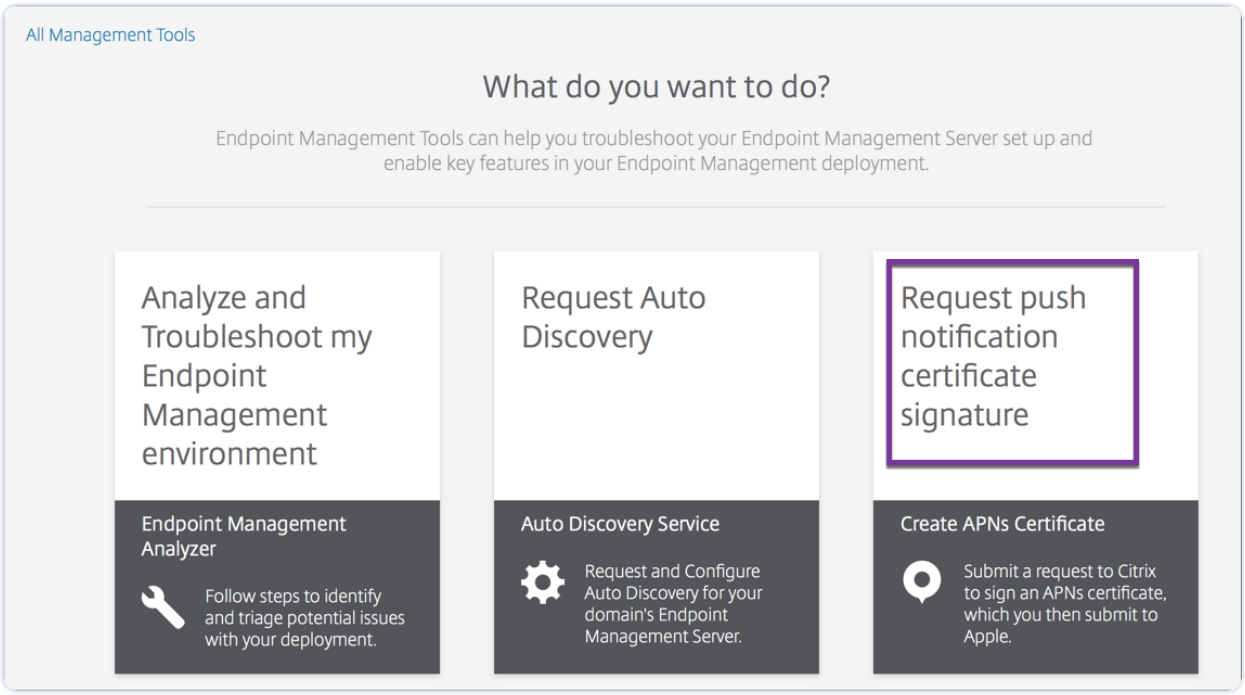
An optional company name []:
```

4. Para continuar, firme el CSR como se describe en la siguiente sección.

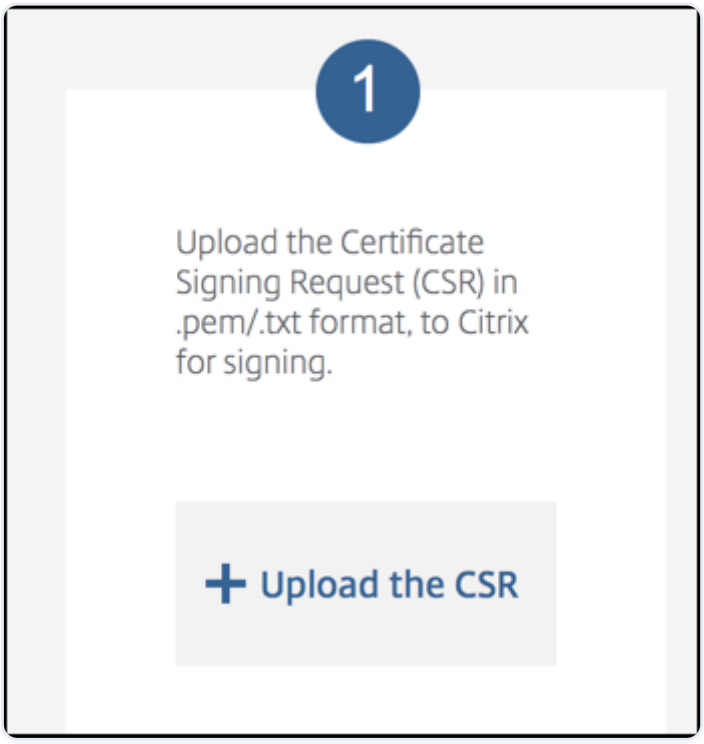
Firmar el CSR

Para usar un certificado con Citrix Endpoint Management, debe enviarlo a Citrix para que lo firme. Citrix firma el CSR con su certificado de firma de Mobile Device Management y devuelve el archivo firmado en formato `.plist`.

1. En su navegador, vaya al sitio web Citrix Endpoint Management Tools y, a continuación, haga clic en **Request push notification certificate signature**.



2. En la página **Creating a new certificate**, haga clic en **Upload the CSR**.



3. Busque y seleccione el certificado.

> **Importante:**
>
> El certificado debe estar en formato .pem/txt. Si es necesario, cambie la extensión del nombre de archivo del certificado a .pem o .txt haciendo clic con el botón derecho y renombrando el archivo.

4. En la página **Citrix Endpoint Management APNs CSR Signing**, haga clic en **Firmar**. El CSR se firma y se guarda automáticamente en su carpeta de descargas configurada.
5. Para continuar, envíe el CSR firmado como se describe en la siguiente sección.

Envíe el CSR firmado a Apple para obtener el certificado APNs

Después de recibir su Solicitud de Firma de Certificado (CSR) firmada de Citrix, envíe el CSR a Apple para obtener el certificado APNs necesario para importar a Citrix Endpoint Management.

> **Nota:**
>
> Algunos usuarios han informado de problemas al iniciar sesión en el Portal de Apple Push. Como alternativa, puede iniciar sesión en el Portal para desarrolladores de Apple. A continuación, puede seguir estos pasos:

1. En un navegador, vaya al Portal de certificados push de Apple.
2. Haga clic en **Crear un certificado**.
3. La primera vez que cree un certificado con Apple: Seleccione la casilla de verificación **He leído y acepto estos términos y condiciones**, y luego haga clic en **Aceptar**.
4. Haga clic en **Elegir archivo**, busque el CSR firmado en su equipo y, a continuación, haga clic en **Cargar**. Un mensaje de confirmación indica que la carga se ha realizado correctamente.
5. Haga clic en **Descargar** para recuperar el certificado .pem.
6. Para continuar, complete el CSR y exporte un archivo PKCS #12 como se describe en la siguiente sección.

Complete el CSR y exporte un archivo PKCS #12

Después de recibir el certificado APNs de Apple, vuelva a Acceso a Llaveros, Microsoft IIS u OpenSSL para exportar el certificado a un archivo PCKS #12.

Un archivo PKCS #12 contiene el archivo de certificado APNS y su clave privada. Los archivos PFX suelen tener la extensión .pfx o .p12. Puede usar archivos .pfx y .p12 indistintamente.

> **Importante:**

> Citrix recomienda guardar o exportar las claves públicas y privadas del sistema local. Necesita las claves para acceder a los certificados APNs y reutilizarlos. Sin las mismas claves, el certificado no es válido y debe repetir todo el proceso de CSR y APNs.

Crear un archivo PKCS #12 mediante Acceso a Llaveros en macOS

> **Importante:**

> Utilice el mismo dispositivo macOS para esta tarea que utilizó para generar la CSR.

1. En el dispositivo, localice el certificado de identidad de producción (.pem) que recibió de Apple.
2. Inicie la aplicación Acceso a Llaveros y vaya a la ficha **Inicio de sesión > Mis certificados**. Arrastre y suelte el certificado de identidad del producto en la ventana abierta.
3. Haga clic en el certificado y expanda la flecha izquierda para verificar que el certificado incluye una clave privada asociada.
4. Para empezar a exportar el certificado a un certificado PCKS #12 (.pfx), elija el certificado y la clave privada, haga clic con el botón derecho y seleccione **Exportar 2 elementos**.
5. Asigne un nombre único al archivo de certificado para usarlo con Citrix Endpoint Management. No incluya espacios en el nombre. A continuación, elija una ubicación de carpeta para el certificado guardado, seleccione el formato de archivo .pfx y haga clic en **Guardar**.
6. Introduzca una contraseña para exportar el certificado. Citrix recomienda utilizar una contraseña única y segura. Además, asegúrese de mantener el certificado y la contraseña a salvo para su uso y referencia posteriores.
7. La aplicación Acceso a Llaveros le pedirá la contraseña de inicio de sesión o el llavero seleccionado. Escriba la contraseña y, a continuación, haga clic en **Aceptar**. El certificado guardado ya está listo para usarse con el servidor de Citrix Endpoint Management.
8. Para continuar, consulte Importar un certificado APNs en Citrix Endpoint Management.

Crear un archivo PKCS #12 mediante Microsoft IIS

> **Importante:**

> Utilice el mismo servidor IIS para esta tarea que utilizó para generar la CSR.

1. Abra Microsoft IIS.
2. Haga clic en el icono **Certificados de servidor**.
3. En la ventana **Certificados de servidor**, haga clic en **Completar solicitud de certificado**.
4. Busque el archivo Certificate.pem de Apple. A continuación, escriba un nombre descriptivo o el nombre del certificado y haga clic en **Aceptar**. No incluya espacios en el nombre.
5. Seleccione el certificado que identificó en el paso 4 y, a continuación, haga clic en **Exportar**.
6. Especifique una ubicación y un nombre de archivo para el certificado .pfx y una contraseña, y, a continuación, haga clic en **Aceptar**.

   Necesita la contraseña del certificado para importarlo en Citrix Endpoint Management.
7. Copie el certificado .pfx en el servidor donde tiene previsto instalar Citrix Endpoint Management.
8. Para continuar, consulte Importar un certificado APNs en Citrix Endpoint Management.

Crear un archivo PKCS #12 mediante OpenSSL

Si utiliza OpenSSL para crear una CSR, también puede usar OpenSSL para crear un certificado APNs .pfx.

1. En un símbolo del sistema o shell, ejecute el siguiente comando. `Customer.privatekey.pem` es la clave privada de su CSR. `APNs_Certificate.pem` es el certificado que acaba de recibir de Apple.

   ```
   openssl pkcs12 -export -in APNs_Certificate.pem -inkey
   Customer.privatekey.pem -out apns_identity.pfx
   ```
2. Introduzca una contraseña para el archivo de certificado .pfx. Recuerde esta contraseña porque la volverá a usar cuando cargue el certificado en Citrix Endpoint Management.
3. Anote la ubicación del archivo de certificado .pfx. A continuación, copie el archivo en el servidor de Citrix Endpoint Management para poder usar la consola para cargarlo.
4. Para continuar, importe un certificado APNs en Citrix Endpoint Management, tal como se describe en la siguiente sección.

Importar un certificado APNs en Citrix Endpoint Management

Después de recibir el nuevo certificado APNs: importe el certificado APNs en Citrix Endpoint Management para agregarlo por primera vez o para reemplazar un certificado.

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Certificados**.

2. Haga clic en **Importar > Almacén de claves**.
3. En **Usar como**, elija **APNs**.
4. Busque el archivo .pfx o .p12 en su equipo.
5. Introduzca una contraseña y, a continuación, haga clic en **Importar**.

Para obtener más información sobre los certificados en Citrix Endpoint Management, consulte Certificados y autenticación.

Renovar un certificado APNs

> **Importante:**
>
> Si utiliza un ID de Apple diferente para el proceso de renovación, debe volver a inscribir los dispositivos de usuario.

> Para renovar un certificado APNs, siga los pasos para crear un certificado y, a continuación, vaya al Portal de certificados push de Apple. Utilice ese portal para cargar el nuevo certificado. Después de iniciar sesión, aparecerá su certificado existente o un certificado importado de su cuenta anterior de Apple Developers.

En el Portal de certificados, la única diferencia al renovar el certificado es que hace clic en **Renovar**. Debe tener una cuenta de desarrollador en el Portal de certificados para acceder al sitio. Para renovar su certificado, use el mismo nombre de organización y Apple ID.

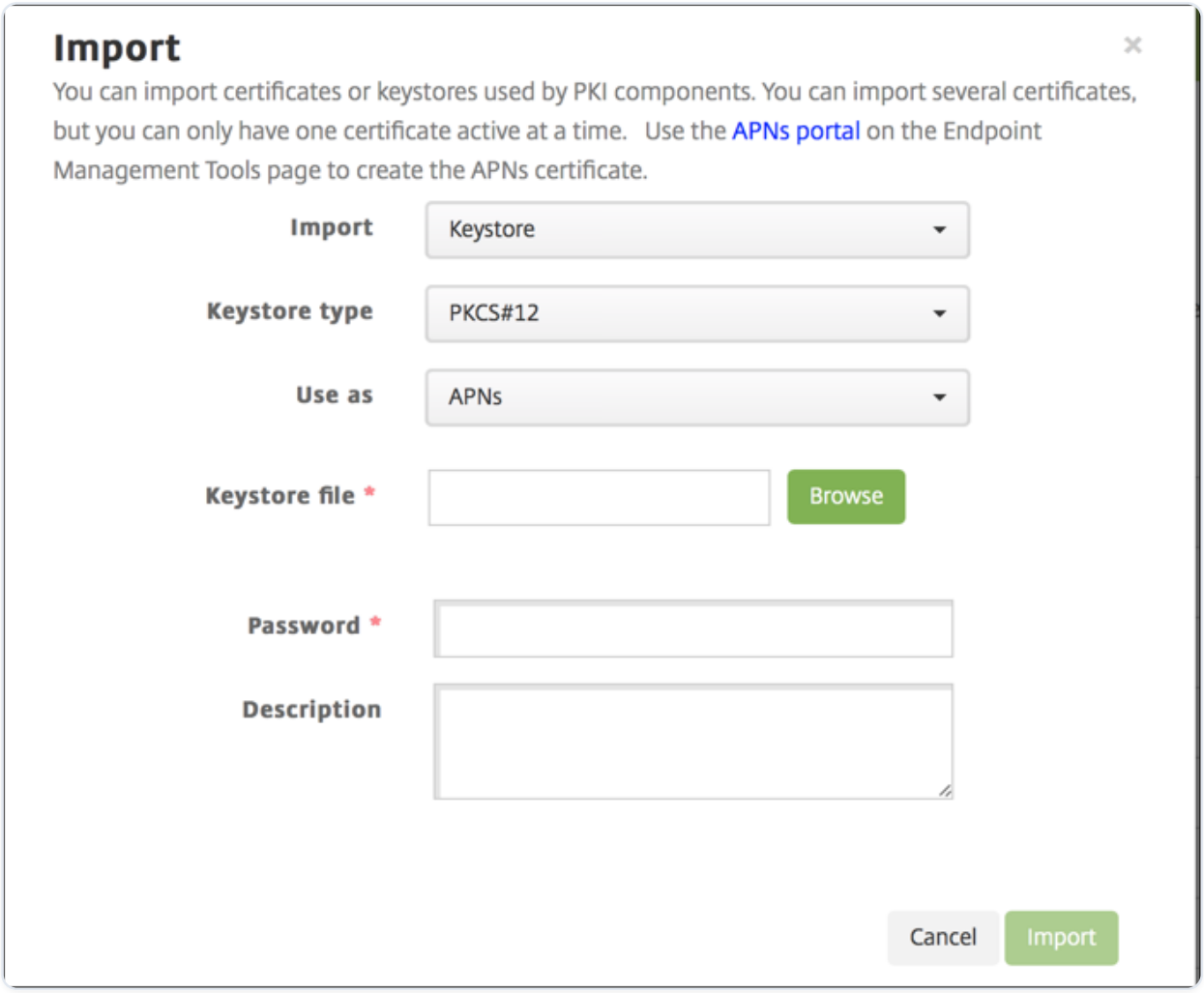
Para determinar cuándo caduca su certificado APNs, en la consola de Citrix Endpoint Management, vaya a **Parámetros > Certificados**. Si el certificado caduca, no lo revoque.

1. Genere una CSR con Microsoft IIS, Acceso a Llaveros (macOS) u OpenSSL. Para obtener más información sobre cómo generar una CSR, consulte Crear una solicitud de firma de certificado.
2. En su explorador, vaya a Citrix Endpoint Management Tools. A continuación, haga clic en **Solicitar firma de certificado de notificación push**.
3. Haga clic en **+ Cargar la CSR**.
4. En el cuadro de diálogo, vaya a la CSR, haga clic en **Abrir** y haga clic en **Firmar**.
5. Cuando reciba un archivo `.plist`, guárdelo.
6. En el título del paso 3, haga clic en **Apple Push Certificates Portal** e inicie sesión.

7. Seleccione el certificado que desea renovar y, a continuación, haga clic en **Renovar**.
8. Cargue el archivo `.plist`. Recibirá un archivo .pem como resultado. Guarde el archivo .pem.
9. Con ese archivo .pem, complete la CSR (según el método que utilizó para crear la CSR en el Paso 1).
10. Exporte el certificado como un archivo .pfx.

En la consola de Citrix Endpoint Management, importe el archivo .pfx y complete la configuración de la siguiente manera:

1. Vaya a **Parámetros > Certificados > Importar**.
2. En el **menú Importar**, elija **Almacén de claves**.
3. En el menú **Tipo de almacén de claves**, elija **PKCS #12**.
4. En **Usar como**, elija **APNs**.



5. En **Archivo de almacén de claves**, haga clic en **Examinar** y vaya al archivo.
6. En **Contraseña**, escriba la contraseña del certificado.

7. Escriba una **Descripción** opcional.
8. Haga clic en **Importar**.

Citrix Endpoint Management le redirige de nuevo a la página **Certificados**. Los campos **Nombre**, **Estado**, **Válido desde** y **Válido hasta** se actualizan.

SAML para inicio de sesión único con Citrix Files

> **Descargo de responsabilidad:**

> Esta función quedará obsoleta si ShareFile (ahora Progress) deja de ofrecer soporte.

> Puede configurar Citrix Endpoint Management y ShareFile para usar el Lenguaje de marcado de aserción de seguridad (SAML) a fin de proporcionar acceso de inicio de sesión único (SSO) a las aplicaciones móviles de Citrix Files. Esta funcionalidad incluye:

- Aplicaciones de Citrix Files habilitadas para MAM SDK o encapsuladas mediante MDX Toolkit
- Clientes de Citrix Files no encapsulados, como el sitio web, el complemento de Outlook o los clientes de sincronización
- **Para las aplicaciones encapsuladas de Citrix Files:** Los usuarios que inician sesión en Citrix Files se redirigen a Citrix Secure Hub para la autenticación de usuarios y para adquirir un token SAML. Después de una autenticación correcta, la aplicación móvil de Citrix Files envía el token SAML a ShareFile. Después del inicio de sesión inicial, los usuarios pueden acceder a la aplicación móvil de Citrix Files a través de SSO. También pueden adjuntar documentos de ShareFile a los correos de Citrix Secure Mail sin iniciar sesión cada vez.
- **Para los clientes de Citrix Files no encapsulados:** Los usuarios que inician sesión en Citrix Files mediante un explorador web u otro cliente de Citrix Files se redirigen a Citrix Endpoint Management. Citrix Endpoint Management autentica a los usuarios, quienes luego adquieren un token SAML que se envía a ShareFile. Después del inicio de sesión inicial, los usuarios pueden acceder a los clientes de Citrix Files a través de SSO sin iniciar sesión cada vez.

Para usar Citrix Endpoint Management como proveedor de identidades (IdP) SAML para ShareFile, debe configurar Citrix Endpoint Management para su uso con cuentas de empresa, como se describe en este artículo. O bien, puede configurar Citrix Endpoint Management para que funcione solo con conectores de zona de almacenamiento. Para obtener más información, consulte Uso de ShareFile con Citrix Endpoint Management.

Para ver un diagrama de arquitectura de referencia detallado, consulte Arquitectura.

Requisitos previos

Complete los siguientes requisitos previos antes de poder configurar el SSO con Citrix Endpoint Management y las aplicaciones de Citrix Files:

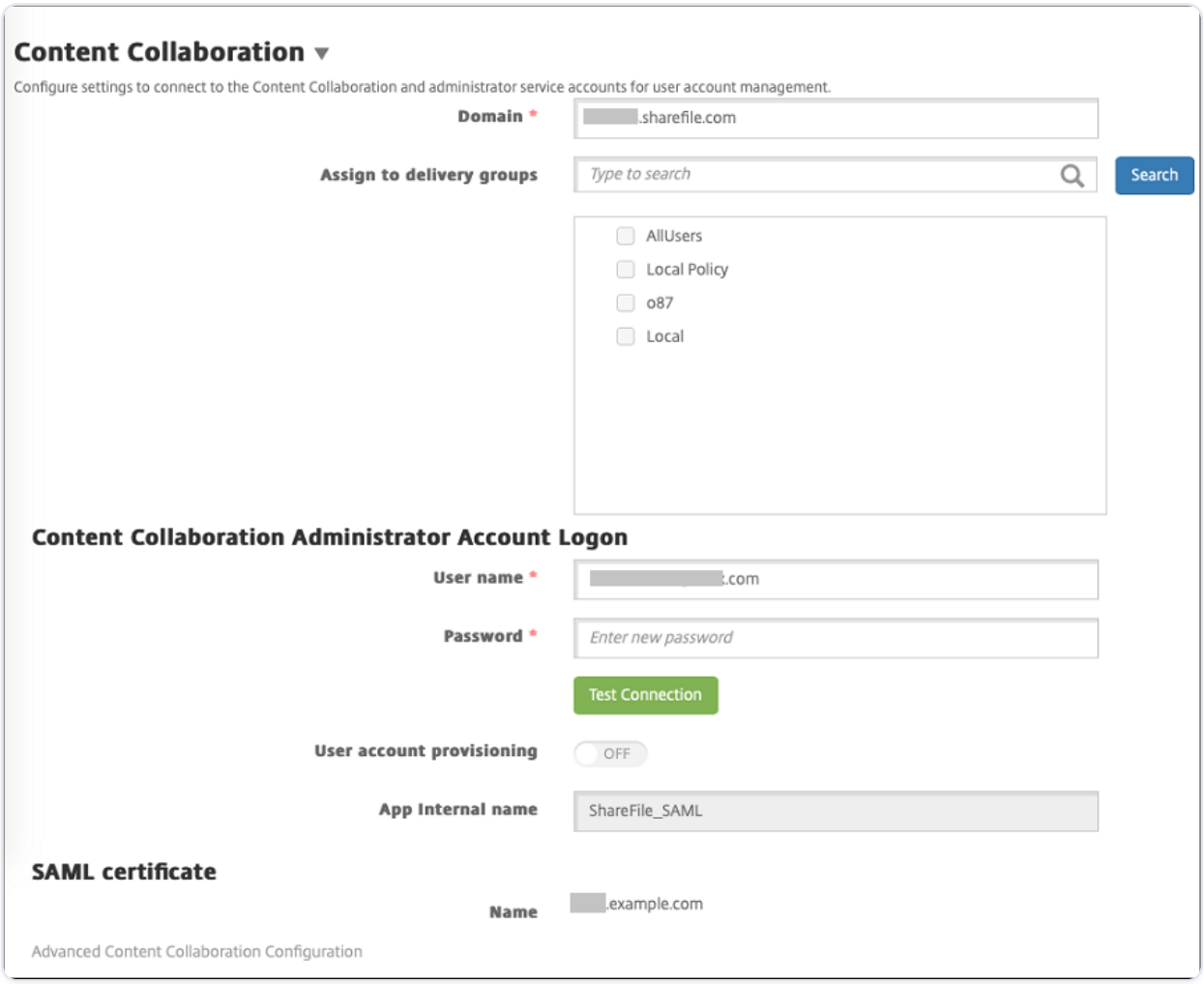
- El MAM SDK o una versión compatible de MDX Toolkit (para aplicaciones móviles de Citrix Files).

  Para obtener más información, consulte Compatibilidad de Citrix Endpoint Management.
- Una versión compatible de las aplicaciones móviles de Citrix Files y Citrix Secure Hub.
- Cuenta de administrador de ShareFile.
- Conectividad verificada entre Citrix Endpoint Management y ShareFile.

Configurar el acceso a ShareFile

Antes de configurar SAML para ShareFile, proporcione la información de acceso a ShareFile de la siguiente manera:

1. En la consola web de Citrix Endpoint Management, haga clic en **Configurar > ShareFile**. Aparece la página de configuración de **ShareFile**.



2. Configure estos ajustes:

   - **Dominio:** Escriba el nombre de su subdominio de ShareFile. Por ejemplo: `example.sharefile.com`.
   - **Asignar a grupos de entrega:** Seleccione o busque los grupos de entrega que desea que puedan usar SSO con ShareFile.
   - **Inicio de sesión de la cuenta de administrador de ShareFile**
   - **Nombre de usuario:** Escriba el nombre de usuario del administrador de ShareFile. Este usuario debe tener privilegios de administrador.
   - **Contraseña:** Escriba la contraseña del administrador de ShareFile.
   - **Aprovisionamiento de cuentas de usuario:** Deje esta configuración deshabilitada. Utilice la herramienta de administración de usuarios de ShareFile para el aprovisionamiento de usuarios. Consulte Aprovisionar cuentas de usuario y grupos de distribución.

3. Haga clic en **Probar conexión** para verificar que el nombre de usuario y la contraseña de la cuenta de administrador de ShareFile se autentican en la cuenta de ShareFile especificada.
4. Haga clic en **Guardar**.

- Citrix Endpoint Management se sincroniza con ShareFile y actualiza la configuración de ShareFile **ID de emisor/entidad de ShareFile** y **URL de inicio de sesión**.
- La página **Configurar > ShareFile** muestra el **Nombre interno de la aplicación**. Necesita ese nombre para completar los pasos descritos más adelante en (#modify-the-citrix-filescom-sso-settings).

Configurar SAML para aplicaciones MDX de Citrix Files encapsuladas

No es necesario usar NetScaler Gateway para la configuración de inicio de sesión único con aplicaciones de Citrix Files preparadas con el SDK de MAM. Para configurar el acceso para clientes de Citrix Files no encapsulados, como el sitio web, el complemento de Outlook o los clientes de sincronización, consulte Configurar NetScaler Gateway para otros clientes de Citrix Files.

Para configurar SAML para aplicaciones MDX de Citrix Files encapsuladas:

1. Descargue ShareFile para clientes de Citrix Endpoint Management. Consulte Descargas de herramientas/aplicaciones de ShareFile.
2. Prepare la aplicación móvil Citrix Files con el SDK de MAM. Para obtener más información, consulte la Descripción general del SDK de MAM.
3. En la consola de Citrix Endpoint Management, cargue la aplicación móvil Citrix Files preparada. Para obtener información sobre cómo cargar aplicaciones MDX, consulte Para agregar una aplicación MDX a Citrix Endpoint Management.
4. verificar la configuración de SAML: Inicie sesión en ShareFile con el nombre de usuario y la contraseña de administrador que configuró anteriormente.
5. verificar que ShareFile y Citrix Endpoint Management estén configurados para la misma zona horaria. Asegúrese de que Citrix Endpoint Management muestre la hora correcta para la zona horaria configurada. De lo contrario, el SSO podría fallar.

Validar la aplicación móvil Citrix Files

1. En el dispositivo del usuario, instale y configure Citrix Secure Hub.
2. Desde la tienda de aplicaciones, descargue e instale la aplicación móvil Citrix Files.
3. Inicie la aplicación móvil Citrix Files. Citrix Files se inicia sin solicitar nombre de usuario ni contraseña.

Validar con Citrix Secure Mail

1. En el dispositivo del usuario, si aún no se ha hecho, instale y configure Citrix Secure Hub.

2. Desde la tienda de aplicaciones, descargue, instale y configure Citrix Secure Mail.
3. Abra un nuevo formulario de correo electrónico y, a continuación, toque **Adjuntar desde ShareFile**. Los archivos disponibles para adjuntar al correo electrónico se muestran sin solicitar un nombre de usuario o contraseña.

Configurar NetScaler Gateway para otros clientes de Citrix Files

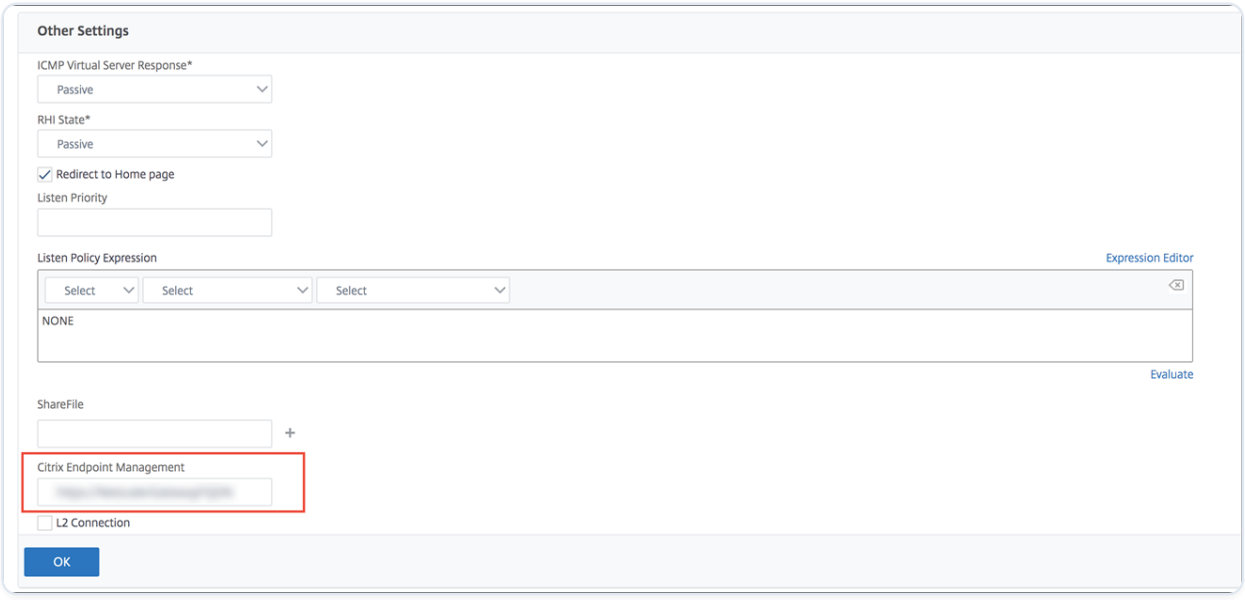
Para configurar el acceso para clientes de Citrix Files no encapsulados, como el sitio web, el complemento de Outlook o los clientes de sincronización: Configure NetScaler Gateway para que admita el uso de Citrix Endpoint Management como proveedor de identidades SAML de la siguiente manera.

- Inhabilitar la redirección de la página de inicio.
- Cree una directiva y un perfil de sesión de Citrix Files.
- Configure las directivas en el servidor virtual de NetScaler Gateway.

Inhabilitar la redirección de la página de inicio

Inhabilite el comportamiento predeterminado para las solicitudes que llegan a través de la ruta / cginfra. Esa acción permite a los usuarios ver la URL interna solicitada originalmente en lugar de la página de inicio configurada.

1. Edite la configuración del servidor virtual de NetScaler Gateway que se utiliza para los inicios de sesión de Citrix Endpoint Management. En NetScaler Gateway, vaya a **Other Settings** y, a continuación, desactive la casilla de verificación **Redirect to Home Page**.



2. En **ShareFile** (ahora llamado ShareFile), escriba el nombre del servidor interno y el número de puerto de Citrix Endpoint Management.

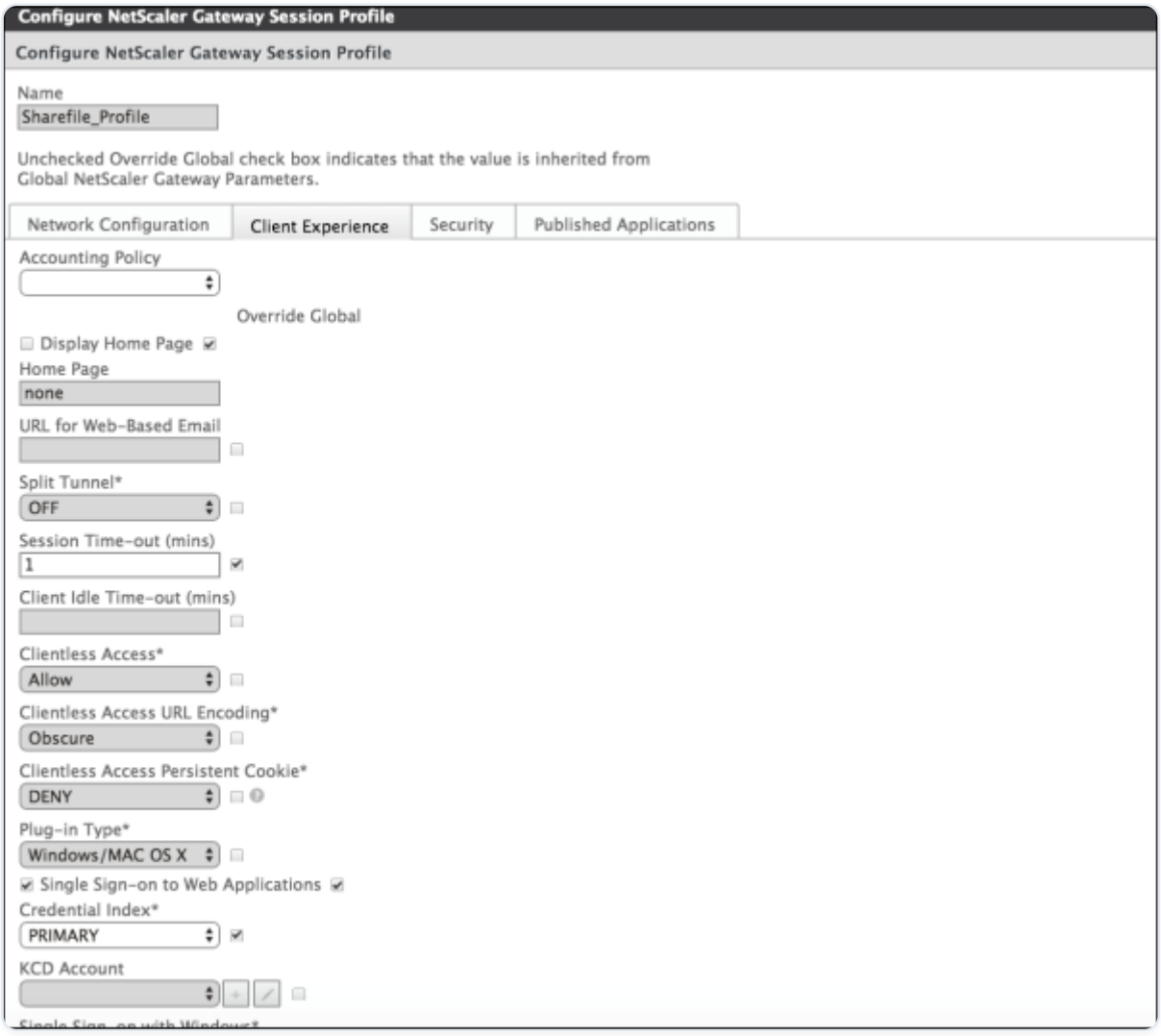
3. En **Citrix Endpoint Management**, escriba la URL de Citrix Endpoint Management.

   Esta configuración autoriza las solicitudes a la URL que introdujo a través de la ruta /cginfra.

Crear una directiva de sesión y un perfil de solicitud de Citrix Files

Configure estos ajustes para crear una directiva de sesión y un perfil de solicitud de Citrix Files:

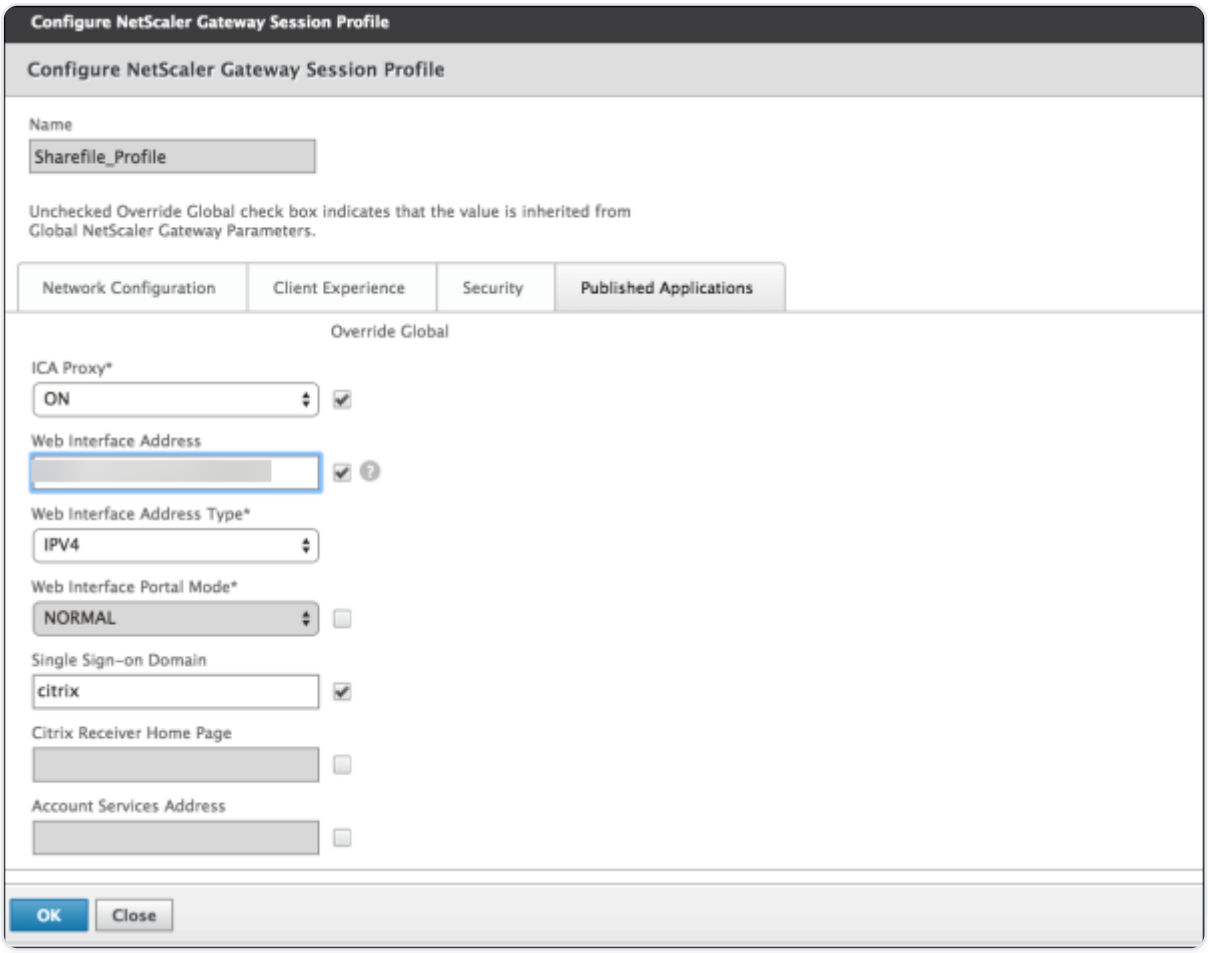
1. En la utilidad de configuración de NetScaler Gateway, en el panel de navegación izquierdo, haga clic en **NetScaler Gateway > Policies > Session**.
2. Cree una directiva de sesión. En la ficha **Policies**, haga clic en **Add**.
3. En el campo **Name**, escriba **ShareFile_Policy**.
4. Cree una acción haciendo clic en el botón **+**. Aparece la página **Create NetScaler® Gateway Session Profile**.



Configure estos ajustes:

- **Name:** Escriba **ShareFile_Profile**.

- Haga clic en la ficha **Client Experience** y, a continuación, configure estos ajustes:
  - **Home Page:** Escriba **none**.
  - **Session Time-out (mins):** Escriba **1**.
  - **Single Sign-on to Web Applications:** Seleccione este ajuste.
  - **Credential Index:** Haga clic en **PRIMARY**.
- Haga clic en la ficha **Published Applications**.

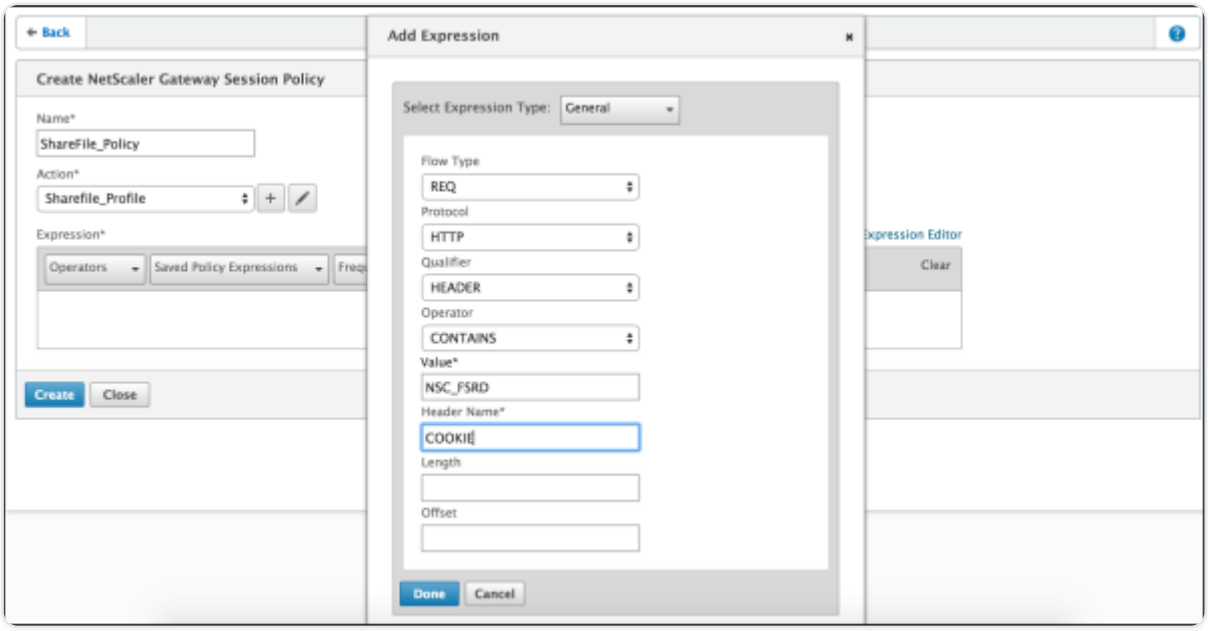


Configure estos ajustes:

- **Proxy de ICA®:** Haga clic en **Activar**.
- **Dirección de la interfaz web:** Escriba la URL de su servidor de Citrix Endpoint Management.
- **Dominio de inicio de sesión único:** Escriba el nombre de su dominio de Active Directory.

  Al configurar el perfil de sesión de NetScaler Gateway, el sufijo de dominio para el **Dominio de inicio de sesión único** debe coincidir con el alias de dominio de Citrix Endpoint Management definido en LDAP.

5. Haga clic en **Crear** para definir el perfil de sesión.
6. Haga clic en **Editor de expresiones**.



Configure estos ajustes:

- **Valor:** Escriba **NSC_FSRD**.
- **Nombre del encabezado:** Escriba **COOKIE**.

7. Haga clic en **Crear** y, a continuación, en **Cerrar**.

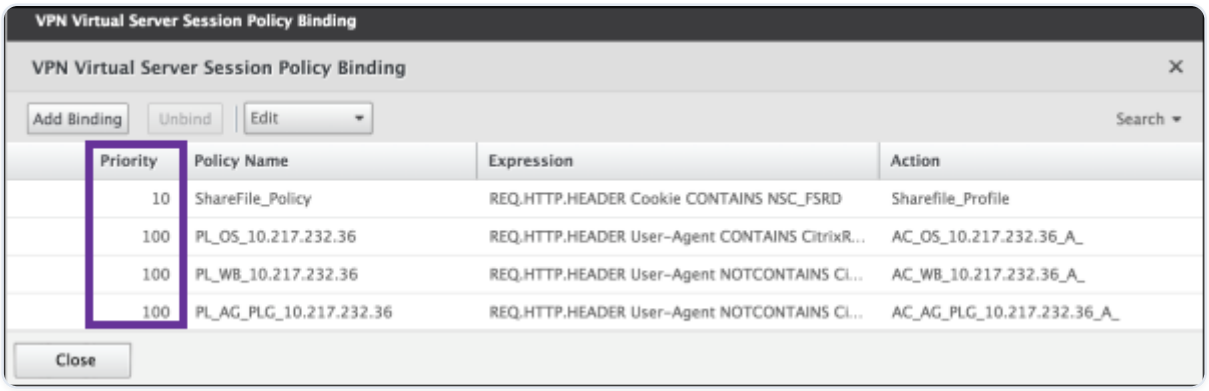


Configurar directivas en el servidor virtual de NetScaler Gateway

Configure estos ajustes en el servidor virtual de NetScaler Gateway.

1. En la utilidad de configuración de NetScaler Gateway, en el panel de navegación izquierdo, haga clic en **NetScaler Gateway > Virtual Servers**.
2. En el panel de **Detalles**, haga clic en su servidor virtual de NetScaler Gateway.
3. Haga clic en **Editar**.

4. Haga clic en **Configured policies > Session policies** y, a continuación, haga clic en **Add binding**.
5. Seleccione **ShareFile_Policy**.
6. Edite el número de **Priority** generado automáticamente para la directiva seleccionada para que tenga la prioridad más alta (el número más pequeño) en relación con cualquier otra directiva de la lista. Por ejemplo:



7. Haga clic en **Done** y, a continuación, guarde la configuración en ejecución de NetScaler Gateway.

Modificar la configuración de SSO de Citrix Files.com

Realice los siguientes cambios para las aplicaciones de Citrix Files MDX y no MDX.

> **Importante:**

> Se añade un nuevo número al nombre interno de la aplicación:

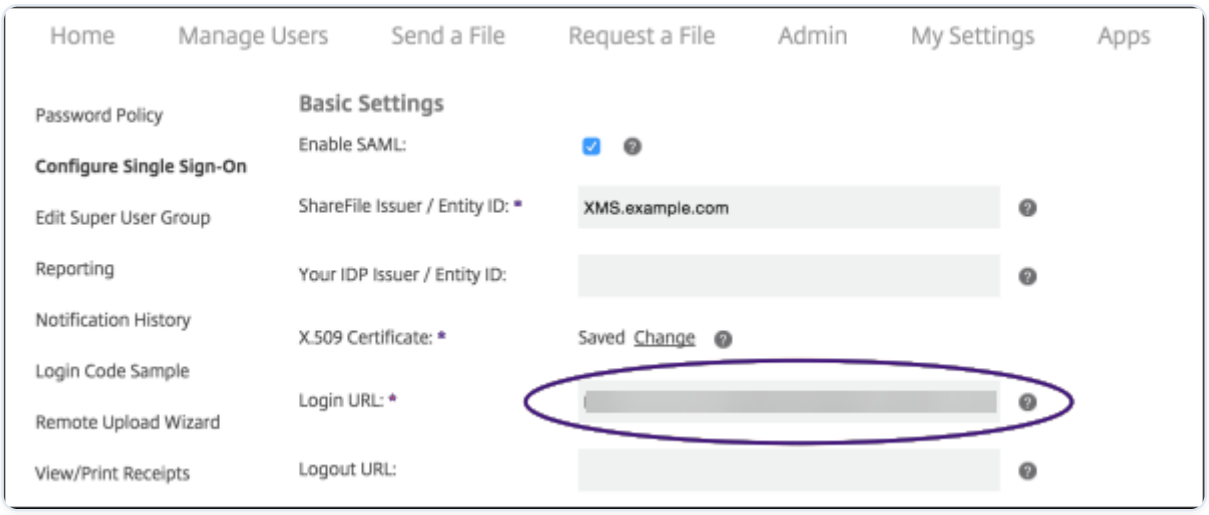
> - Cada vez que edite o vuelva a crear la aplicación Citrix Files
> - Cada vez que cambie la configuración de ShareFile en Citrix Endpoint Management

> Como resultado, también debe actualizar la URL de inicio de sesión en el sitio web de Citrix Files para que muestre el nombre de aplicación actualizado.

1. Inicie sesión en su cuenta de ShareFile (`https://<subdomain>.sharefile.com`) como administrador de ShareFile.
2. En la interfaz web de ShareFile, haga clic en **Admin** y, a continuación, seleccione **Configurar inicio de sesión único**.

3. Edite la **URL de inicio de sesión** de la siguiente manera:

   Aquí tiene un ejemplo de **URL de inicio de sesión** antes de las modificaciones: `https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`.



   - Inserte el FQDN externo del servidor virtual de NetScaler Gateway más **/cginfra/https/** delante del FQDN del servidor de Citrix Endpoint Management y, a continuación, agregue **8443** después del FQDN de Citrix Endpoint Management.

     Aquí tiene un ejemplo de una URL editada: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`

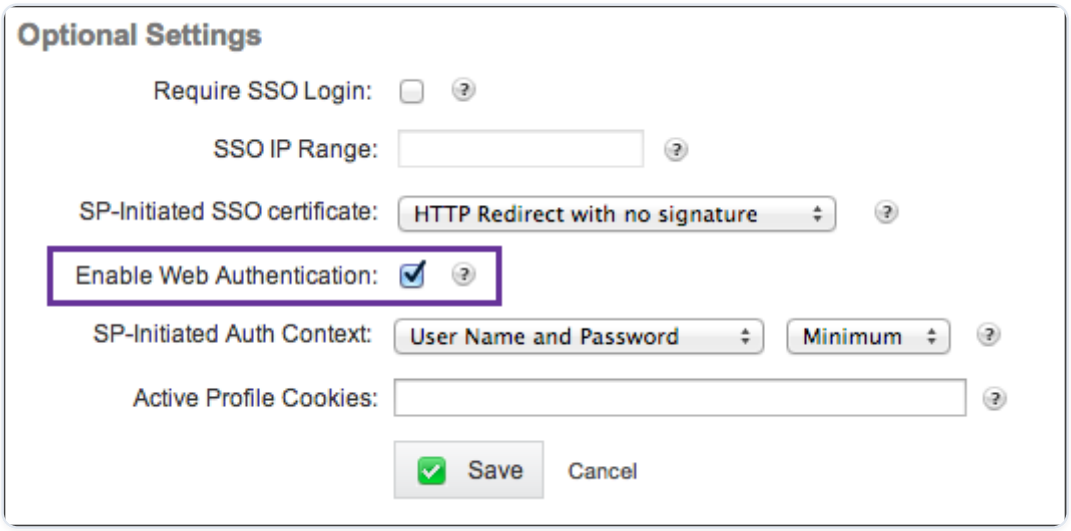
   - Cambie el parámetro `&app=ShareFile_SAML_SP` por el nombre interno de la aplicación Citrix Files. El nombre interno es `ShareFile_SAML` de forma predeterminada. Sin embargo, cada vez que cambia la configuración, se añade un número al nombre interno (`ShareFile_SAML_2`, `ShareFile_SAML_3`, etc.). Puede consultar el **nombre interno de la aplicación** en la página **Configurar > ShareFile**.

     Aquí tiene un ejemplo de una URL editada: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

   - Agregue `&nssso=true` al final de la URL.

     Aquí tiene un ejemplo de la URL final: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`.

4. En **Configuración opcional**, seleccione la casilla de verificación **Habilitar autenticación web**.



Validar la configuración

Realice lo siguiente para validar la configuración.

1. Dirija su explorador a `https://<subdomain>sharefile.com/saml/login`.

   Se le redirige al formulario de inicio de sesión de NetScaler Gateway. Si no se le redirige, verificar la configuración anterior.

2. Introduzca el nombre de usuario y la contraseña del entorno de NetScaler Gateway y Citrix Endpoint Management que configuró.

   Aparecen sus carpetas de Citrix Files en `<subdomain>.sharefile.com`. Si no ve sus carpetas de Citrix Files, asegúrese de haber introducido las credenciales de inicio de sesión correctas.

Autenticación con Azure Active Directory a través de Citrix Cloud

Citrix Endpoint Management admite la autenticación con credenciales de Azure Active Directory (Azure AD) a través de Citrix Cloud. Este método de autenticación solo está disponible para los usuarios que se inscriben en MDM a través de Citrix Secure Hub.

Para usar Citrix Secure Hub con MDM+MAM, configure Citrix Endpoint Management para que use NetScaler Gateway para la inscripción de MAM. Para obtener más información, consulte NetScaler Gateway y Citrix Endpoint Management.

Citrix Endpoint Management utiliza el servicio Citrix Cloud, identidad de Citrix, para federarse con Azure Active Directory. Citrix recomienda utilizar el proveedor de identidades de Citrix en lugar de una conexión directa a Azure Active Directory.

Citrix Endpoint Management admite la autenticación con Azure AD para las siguientes plataformas:

- Dispositivos iOS y macOS no inscritos en Apple Business Manager o Apple School Manager
- Dispositivos iOS y macOS inscritos en Apple Business Manager
- Dispositivos Android Enterprise (versión preliminar), para modos BYOD y totalmente administrados

La autenticación con Azure AD a través de Citrix Cloud tiene estas limitaciones:

- No está disponible para las cuentas locales de Citrix Endpoint Management.
- No admite la autenticación a través de Azure AD para invitaciones de inscripción. Si envía a los usuarios una invitación de inscripción que tiene una URL de inscripción, los usuarios se autentican a través de LDAP en lugar de Azure AD.

Requisitos previos

> **Nota:**
>
> Azure Active Directory Standalone no es compatible; se requiere un Active Directory local para la integración con Citrix Endpoint Management.

- Credenciales de usuario de Azure Active Directory.
- Los grupos de usuarios en Active Directory deben coincidir con los grupos de usuarios en Azure Active Directory.
- Los nombres de usuario y las direcciones de correo electrónico en Active Directory deben coincidir con los nombres de usuario y las direcciones de correo electrónico en Azure Active Directory.
- Cuenta de Citrix Cloud, con Citrix Cloud Connector instalado para la sincronización del servicio de directorio.
- NetScaler Gateway. Citrix recomienda habilitar la autenticación basada en certificados o Azure AD para una experiencia completa de inicio de sesión único. Si utiliza la autenticación LDAP en NetScaler Gateway para el registro de MAM, los usuarios finales experimentarán un doble

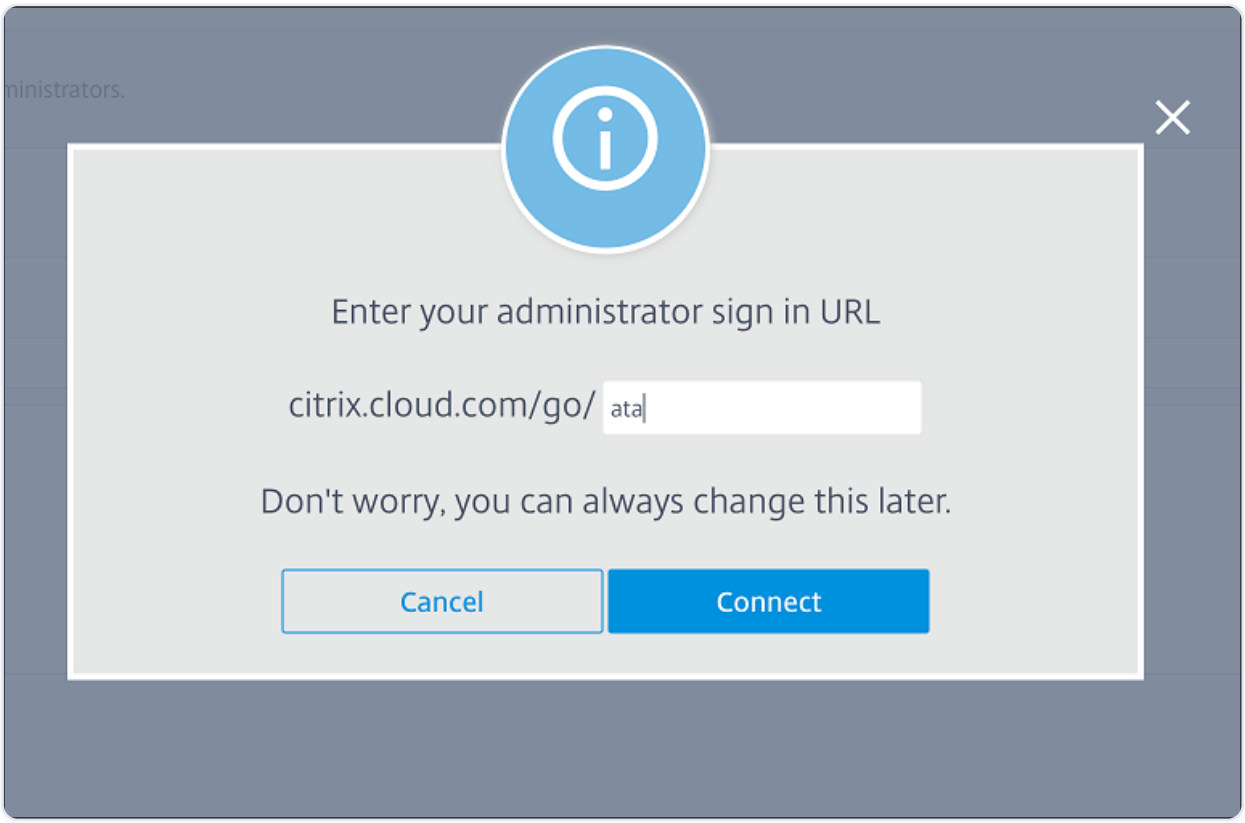
aviso de autenticación durante la inscripción. Para obtener más información, consulte Autenticación de certificado de cliente o certificado más dominio.

- En el perfil de inscripción para Android Enterprise, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Desactivado**. Si los usuarios rechazan la administración de dispositivos, no podrán inscribirse utilizando un proveedor de identidades para autenticarse. Para obtener más información, consulte Seguridad de la inscripción.

Configurar Citrix Cloud para usar Azure Active Directory como proveedor de identidades

Para configurar este servicio para su uso con Citrix Secure Hub, configure Azure Active Directory en Citrix Cloud.

1. Vaya a https://citrix.cloud.com e inicie sesión en su cuenta de Citrix Cloud.
2. Desde el menú de Citrix Cloud, vaya a la página **Administración de identidades y accesos** y conéctese a Azure Active Directory.
3. Escriba la URL de inicio de sesión de su administrador y, a continuación, haga clic en **Conectar**.



4. Después de iniciar sesión, su cuenta de Azure Active Directory se conecta a Citrix Cloud. La página **Administración de identidades y accesos > Autenticación** muestra qué cuentas usar para iniciar sesión en sus cuentas de Citrix Cloud y Azure AD.

5. Para habilitar la autenticación con Azure AD para los usuarios que se inscriben a través de Citrix Secure Hub, en **Configuración de Workspace > Autenticación**, seleccione **Azure Active Directory**. Una vez completada la configuración, puede inscribir los dispositivos de los usuarios a través de Citrix Secure Hub.

Configurar la identidad de Citrix como el tipo de IdP para Citrix Endpoint Management

Esta configuración se aplica solo a los usuarios que se inscriben a través de Citrix Secure Hub. Después de configurar Azure Active Directory en Citrix Cloud, configure Citrix Endpoint Management de la siguiente manera.

1. En la consola de Citrix Endpoint Management, vaya a **Configuración > Proveedor de identidades (IDP)** y, a continuación, haga clic en **Agregar**.
2. En la página **Proveedor de identidades (IDP)**, configure lo siguiente:

    - **Nombre de IDP:** Escriba un nombre único para identificar la conexión de IDP que está creando.
    - **Tipo de IDP:** Elija **Plataforma de identidades de Citrix**.
    - **Dominio de autenticación:** Elija **Azure Active Directory**. Este dominio corresponde al dominio del proveedor de identidades en la página **Configuración de Workspace > Autenticación** de Citrix Cloud.

3. Haga clic en **Siguiente**. En la página **Uso de notificaciones de IDP**, configure lo siguiente:

    - **Tipo de identificador de usuario:** De forma predeterminada, este campo está establecido en **userPrincipalName**. Asegúrese de configurar todos los usuarios con el mismo identificador tanto en su Active Directory local como en Azure Active Directory. Citrix Endpoint Management utiliza este identificador para asignar usuarios del proveedor de identidades a usuarios de Active Directory local.
    - **Cadena de identificador de usuario:** Este campo se rellena automáticamente.

4. Haga clic en **Siguiente**, revise la página **Resumen** y, a continuación, haga clic en **Guardar**.

    Los usuarios de Citrix Secure Hub, la consola de Citrix Endpoint Management y el portal de autoayuda ahora pueden iniciar sesión con sus credenciales de Azure Active Directory. Los usuarios de Citrix Secure Hub unidos a un dominio pueden usar Citrix Secure Hub para iniciar sesión con sus credenciales de Azure AD. Citrix Secure Hub utiliza la autenticación de certificados de cliente para dispositivos MAM.

Flujo de autenticación de Citrix Secure Hub

Citrix Endpoint Management utiliza el siguiente flujo para autenticar a los usuarios con Azure AD como IDP en dispositivos inscritos a través de Citrix Secure Hub:

1. Un usuario inicia Citrix Secure Hub.
2. Citrix Secure Hub pasa la solicitud de autenticación a la identidad de Citrix, que pasa la solicitud a Azure Active Directory.
3. El usuario escribe su nombre de usuario y contraseña de Azure Active Directory.
4. Azure Active Directory valida al usuario y envía un código a la identidad de Citrix.
5. La identidad de Citrix envía el código a Citrix Secure Hub, que envía el código al servidor de Citrix Endpoint Management.
6. Citrix Endpoint Management obtiene un token de ID mediante el código y el secreto, y luego valida la información del usuario que se encuentra en el token de ID. Citrix Endpoint Management devuelve un ID de sesión.

Autenticación con administración basada en grupos de Azure Active Directory

Citrix Endpoint Management ahora admite la autenticación de identidad basada en grupos para acceder a sus servicios a través de Azure Active Directory (AAD). Esta actualización garantiza que los administradores puedan gestionar el acceso a nivel de grupo utilizando la pertenencia a grupos de AAD, lo que ofrece flexibilidad y seguridad mejorada. El mecanismo de inicio de sesión heredado de Citrix Identity sigue estando disponible como alternativa.

Mejoras clave

- **Integración de grupos de Azure AD**: Los administradores ahora pueden gestionar el acceso de los usuarios a los servicios de CEM aprovechando los grupos de Azure AD. Esto simplifica la gestión de permisos y permite controles de acceso basados en grupos.
- **Autenticación de inicio de sesión de Citrix Endpoint Management con grupos de Azure AD**: Los usuarios pueden autenticarse a través de grupos de Azure AD, lo que proporciona una integración perfecta con la infraestructura de identidad organizacional existente.
- **Compatibilidad con Citrix Identity heredado**: El inicio de sesión de Citrix Identity sigue estando disponible, lo que garantiza que los usuarios puedan realizar la transición a su propio ritmo.

Marcas de funciones

- **Marca de función de Citrix Cloud™**: `fullAccessGroups` – Esta función está habilitada de forma predeterminada para permitir el acceso completo a los grupos.
- **Marca de función de Citrix Endpoint Management**: `cc.group.based.admin` – Habilita la funcionalidad de administración basada en grupos en Citrix Endpoint Management.

Requisitos previos

- Azure AD está configurado en el portal de Citrix Cloud.
- La URL de inicio de sesión de administrador para Citrix Cloud debe configurarse para acceder a Citrix Endpoint Management a través de grupos de Azure AD.

Pasos de configuración

1. Inicie sesión en el portal de Azure y acceda a Azure Active Directory.
2. Vaya a Usuarios y seleccione Crear nuevo usuario.
3. Navegue a Grupos, haga clic en Nuevo grupo y añada el usuario recién creado como miembro de este grupo.
4. Inicie sesión en Citrix Cloud utilizando credenciales de administrador para iniciar sesión.
5. Navegue a Identidad y administración de acceso, asigne permisos completos o personalizados al nuevo grupo de Azure AD.
6. El usuario del grupo de Azure AD ahora puede iniciar sesión en Citrix Endpoint Management™ utilizando la URL de inicio de sesión de administrador.

Autenticación con Azure Active Directory a través de NetScaler Gateway para la inscripción de MAM

Citrix Endpoint Management admite la autenticación con credenciales de Azure Active Directory (Azure AD) a través de NetScaler Gateway. Este método de autenticación solo está disponible para los usuarios que se inscriben en MAM a través de Citrix Secure Hub.

Requisitos previos

Para configurar Citrix Endpoint Management para que utilice Azure AD a través de NetScaler Gateway como proveedor de identidades (IdP) para los dispositivos inscritos en MAM, asegúrese de que se cumplen los siguientes requisitos previos:

- Configure Citrix Endpoint Management con Azure AD a través de Citrix Cloud como IdP para dispositivos inscritos en MDM. Para obtener más información sobre cómo configurar Azure AD para MDM, consulte Autenticación con Azure Active Directory a través de Citrix Cloud.
- Conecte Azure AD a Citrix Cloud. Para obtener más información, consulte Conectar Azure Active Directory a Citrix Cloud.
- Habilite las siguientes marcas de función relevantes según la plataforma, respectivamente:
  - iOS:
    - iOS-V3Form-MAM
    - iOS-SAMLAuth-MAM
  - Android:
    - Android-V3Form-MAM
    - Android-SAMLAuth-MAM

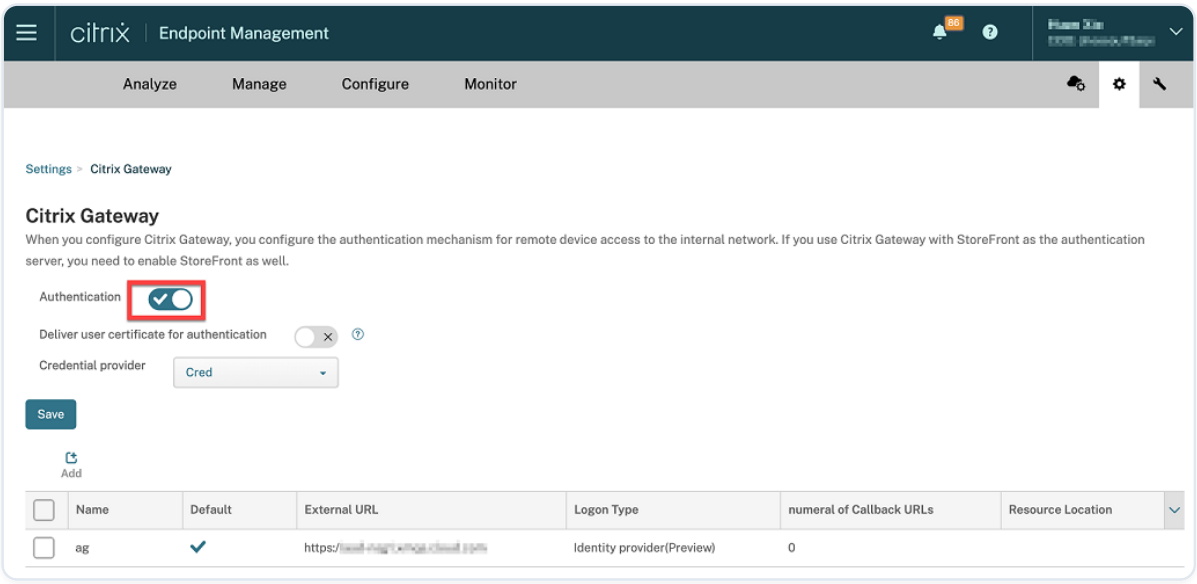
> **Nota:**
>
> Para habilitar esta función, póngase en contacto con su equipo de soporte.

- Para Android, habilite **Android Enterprise**.

> **Nota:**
>
> Esta función no se ha probado ni verificado en el modo heredado de Administrador de dispositivos Android (DA). Este modo no es compatible.

Configurar Azure AD para MAM como IdP

1. Configure NetScaler Gateway en Citrix Endpoint Management de la siguiente manera:
   a. Inicie sesión en la consola de Citrix Endpoint Management y, a continuación, haga clic en el icono **Configuración** ⚙.
   b. Haga clic en **NetScaler Gateway** en **Servidor**.
   c. Habilite el botón de alternancia **Autenticación**.



   d. Asegúrese de que el **Tipo de inicio de sesión** de la puerta de enlace sea el *proveedor de identidades*.

   e. Haga clic en **Guardar**.

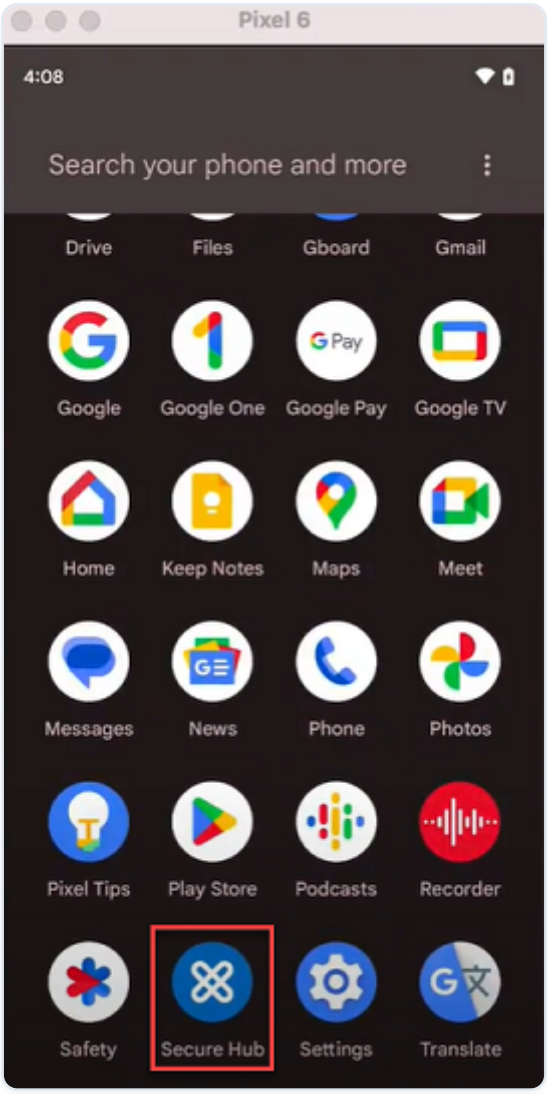
2. Configure Azure AD como IdP de SAML mediante Configurar Azure AD como IdP de SAML.
3. Configure NetScaler ADC como SP de SAML mediante la directiva avanzada con Configurar NetScaler ADC como proveedor de servicios (SP) SAML.
4. Cree un servidor virtual AAA mediante Para configurar un servidor virtual de autenticación mediante la GUI.
5. Configure el servidor virtual AAA mediante Configurar el servidor virtual de autenticación.
6. Cree y configure el perfil de autenticación mediante Perfiles de autenticación.
7. Vincule el perfil de autenticación con el servidor virtual de Gateway y guarde todas las configuraciones.

Ahora, Azure AD se agrega como proveedor de identidades para los dispositivos inscritos en MAM y puede autenticarlos mediante Azure AD.

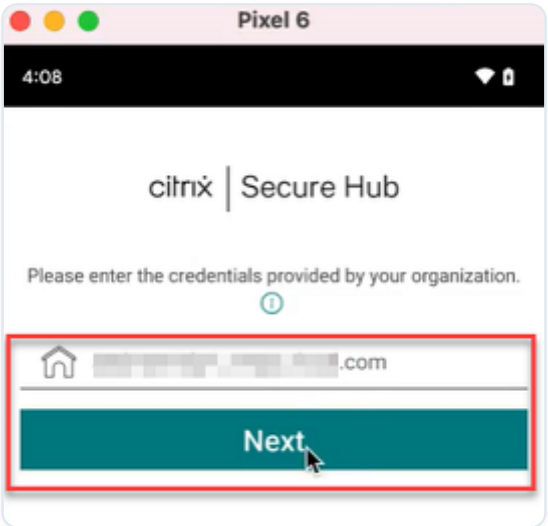
Comportamiento esperado

El siguiente ejemplo utiliza un dispositivo Android:

1. En su dispositivo móvil, abra la aplicación Citrix Secure Hub.

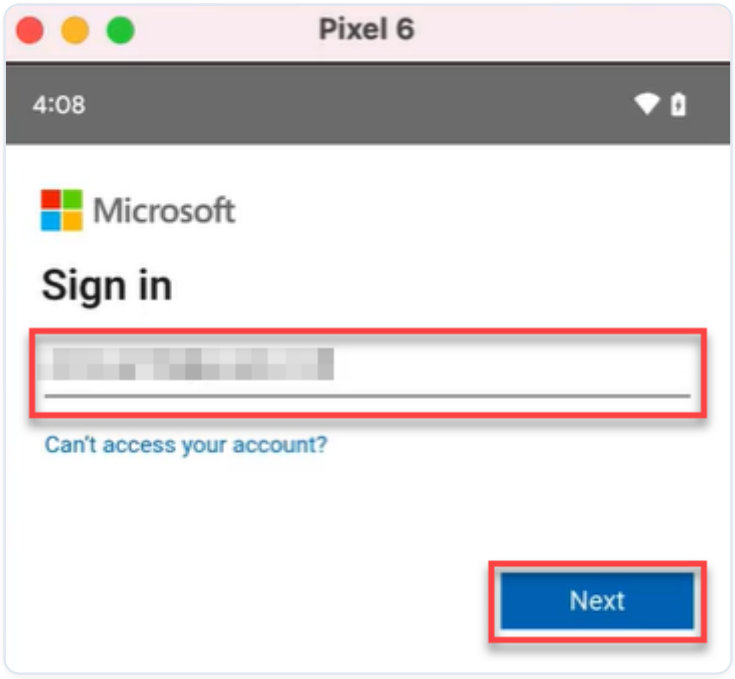


2. Proporcione los permisos necesarios.
3. En la página de inicio de sesión, introduzca las credenciales proporcionadas por su organización y, a continuación, toque **Siguiente**.

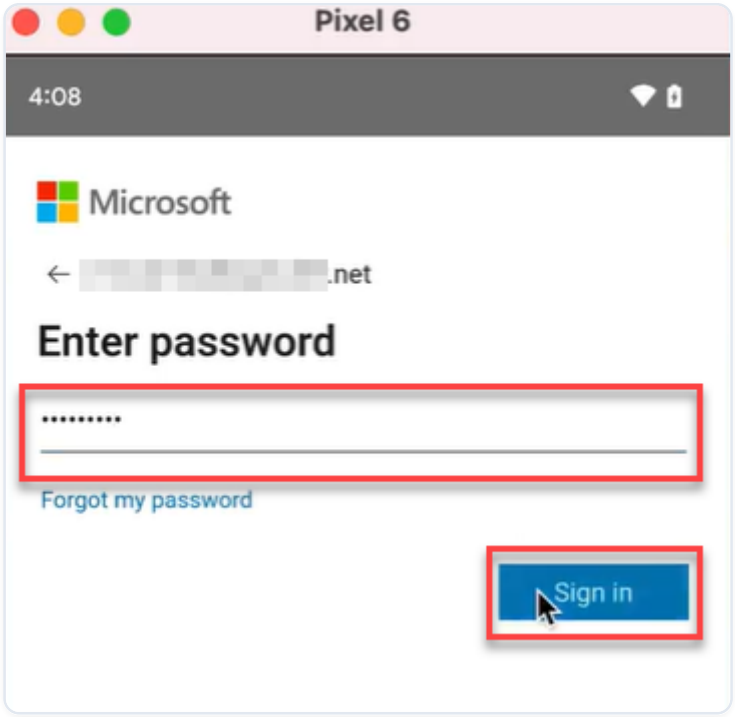


Se le redirige a la página de inicio de sesión de Microsoft.

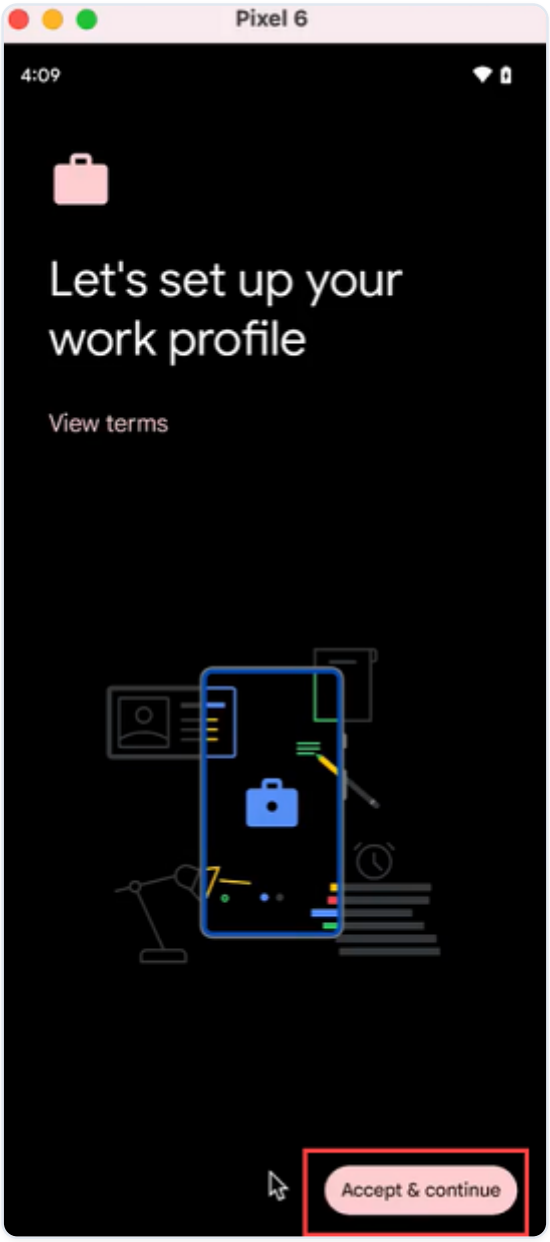
4. En la página de inicio de sesión de Microsoft, introduzca su ID de correo electrónico y, a continuación, toque **Siguiente**.



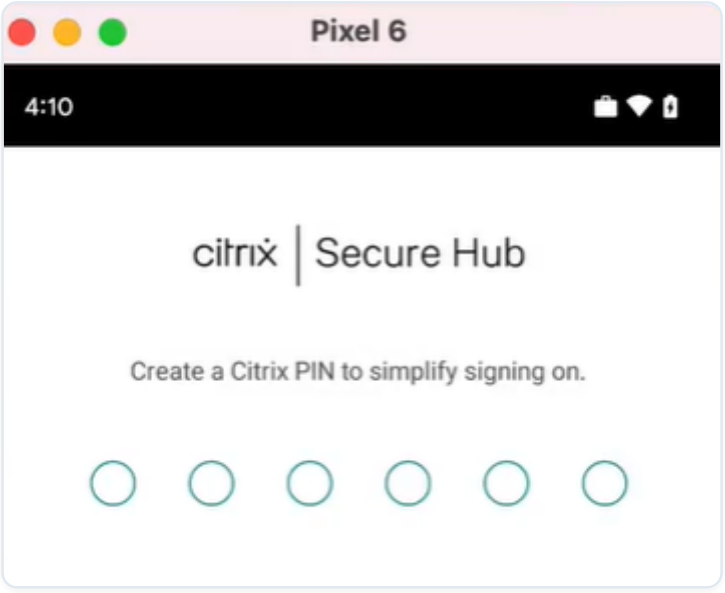
5. Introduzca la contraseña y, a continuación, toque **Iniciar sesión**.



6. En la página de **Configurar su perfil de trabajo**, toque **Aceptar y continuar**.



7. Cree el PIN para la aplicación Citrix Secure Hub y confírmelo.



Se le redirige correctamente a la página de inicio de Citrix Secure Hub.

Autenticación con Okta a través de Citrix Cloud

Citrix Endpoint Management admite la autenticación con credenciales de Okta a través de Citrix Cloud. Este método de autenticación solo está disponible para los usuarios que se inscriben en MDM a través de Citrix Secure Hub.

Los dispositivos que se inscriben en MAM no pueden autenticarse con credenciales de Okta a través de Citrix Cloud. Para usar Citrix Secure Hub con MDM+MAM, configure Citrix Endpoint Management para que use NetScaler Gateway para la inscripción en MAM. Para obtener más información, consulte NetScaler Gateway y Citrix Endpoint Management.

Citrix Endpoint Management utiliza el servicio Citrix Cloud, Citrix Identity, para federarse con Okta. Citrix recomienda utilizar el proveedor de identidades de Citrix en lugar de una conexión directa a Okta.

Citrix Endpoint Management admite la autenticación con Okta para las siguientes plataformas:

- Dispositivos iOS y macOS no inscritos en Apple Business Manager o Apple School Manager
- Dispositivos iOS y macOS inscritos en Apple Business Manager
- Dispositivos Android Enterprise (versión preliminar), para los modos BYOD y totalmente administrado

La autenticación con Okta a través de Citrix Cloud tiene estas limitaciones:

- No está disponible para las cuentas locales de Citrix Endpoint Management.
- No admite la autenticación a través de Okta para las invitaciones de inscripción. Si envía a los usuarios una invitación de inscripción que tiene una URL de inscripción, los usuarios se autentican a través de LDAP en lugar de Okta.

Requisitos previos

- Credenciales de usuario de Okta
- Los grupos de usuarios en Active Directory deben coincidir con los grupos de usuarios en Okta.
- Los nombres de usuario y las direcciones de correo electrónico en el directorio activo deben coincidir con los nombres de usuario y las direcciones de correo electrónico en Okta.

- Cuenta de Citrix Cloud con Citrix Cloud Connector instalado para la sincronización del servicio de directorio.
- NetScaler Gateway. Citrix recomienda habilitar la autenticación basada en certificados para una experiencia completa de inicio de sesión único. Si utiliza la autenticación LDAP en NetScaler Gateway para el registro de MAM, los usuarios finales experimentarán una doble solicitud de autenticación durante la inscripción. Para obtener más información, consulte Autenticación de certificado de cliente o certificado más dominio.
- En el perfil de inscripción para Android Enterprise, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Desactivado**. Si los usuarios rechazan la administración de dispositivos, no podrán inscribirse utilizando un proveedor de identidades para autenticarse. Para obtener más información, consulte Seguridad de la inscripción.

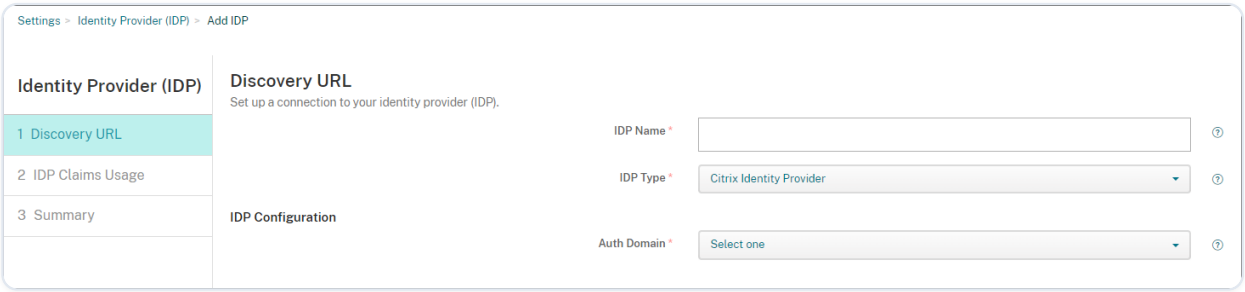
Configurar Citrix Cloud para usar Okta como proveedor de identidades

Para configurar Okta en Citrix Cloud, consulte Conectar Okta como proveedor de identidades a Citrix Cloud.

Configurar la identidad de Citrix como el tipo de IdP para Citrix Endpoint Management

Esta configuración se aplica solo a los usuarios que se inscriben a través de Citrix Secure Hub. Después de configurar Azure Active Directory en Citrix Cloud, configure Citrix Endpoint Management de la siguiente manera:

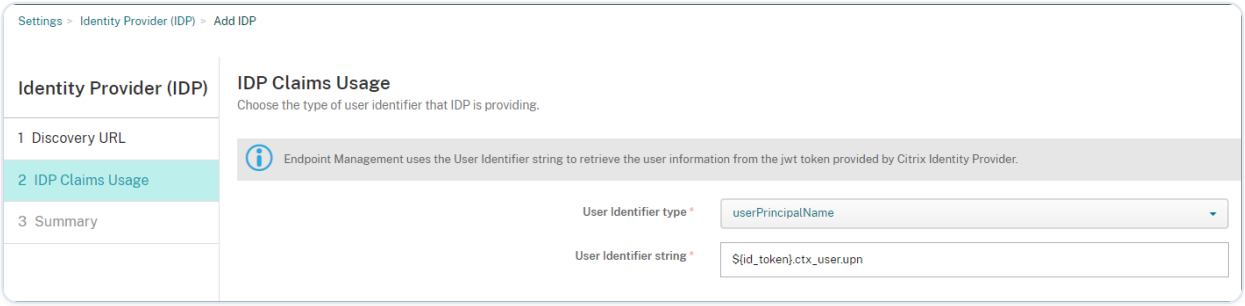
1. En la consola de Citrix Endpoint Management, vaya a **Configuración > Proveedor de identidades (IDP)** y, a continuación, haga clic en **Agregar**.
2. En la página **Proveedor de identidades (IDP)**, configure lo siguiente:



- **Nombre de IdP:** Escriba un nombre único para identificar la conexión de IdP que está creando.
- **Tipo de IdP:** Elija **Proveedor de identidades de Citrix**.

- **Dominio de autenticación:** Elija el dominio de Citrix Cloud. Si no está seguro de cuál elegir, su dominio aparece en la página **Administración de identidades y accesos > Autenticación** de Citrix Cloud.

3. Haga clic en **Siguiente**. En la página **Uso de notificaciones de IdP**, configure lo siguiente:



- **Tipo de identificador de usuario:** Este campo se establece en **userPrincipalName**. Asegúrese de configurar a todos los usuarios con el mismo identificador en su Active Directory local y en Okta. Citrix Endpoint Management utiliza este identificador para asignar usuarios del proveedor de identidades a usuarios de Active Directory local.
- **Cadena de identificador de usuario:** Este campo se rellena automáticamente.

Después de esta configuración, los usuarios de Citrix Secure Hub que están unidos a un dominio pueden usar Citrix Secure Hub para iniciar sesión con sus credenciales de Okta. Citrix Secure Hub utiliza la autenticación de certificados de cliente para los dispositivos MAM.

Flujo de autenticación de Citrix Secure Hub

Citrix Endpoint Management utiliza el siguiente flujo para autenticar a los usuarios con Okta como IdP en dispositivos inscritos a través de Citrix Secure Hub:

1. Un usuario inicia Citrix Secure Hub.
2. Citrix Secure Hub pasa la solicitud de autenticación a la identidad de Citrix, que pasa la solicitud a Okta.
3. El usuario escribe su nombre de usuario y contraseña.
4. Okta valida al usuario y envía un código a la identidad de Citrix.
5. La identidad de Citrix envía el código a Citrix Secure Hub, que envía el código al servidor de Citrix Endpoint Management.
6. Citrix Endpoint Management obtiene un token de ID mediante el código y el secreto, y luego valida la información del usuario que se encuentra en el token de ID. Citrix Endpoint Management devuelve un ID de sesión.

Autenticación con Okta a través de NetScaler Gateway para la inscripción de MAM

Citrix Endpoint Management admite la autenticación con credenciales de Okta a través de NetScaler Gateway. Este método de autenticación solo está disponible para los usuarios que se inscriben en MAM a través de Citrix Secure Hub.

Requisitos previos

Para configurar Citrix Endpoint Management para que utilice Okta a través de NetScaler Gateway como proveedor de identidades (IdP) para los dispositivos inscritos con MAM, asegúrese de que se cumplen los siguientes requisitos previos:

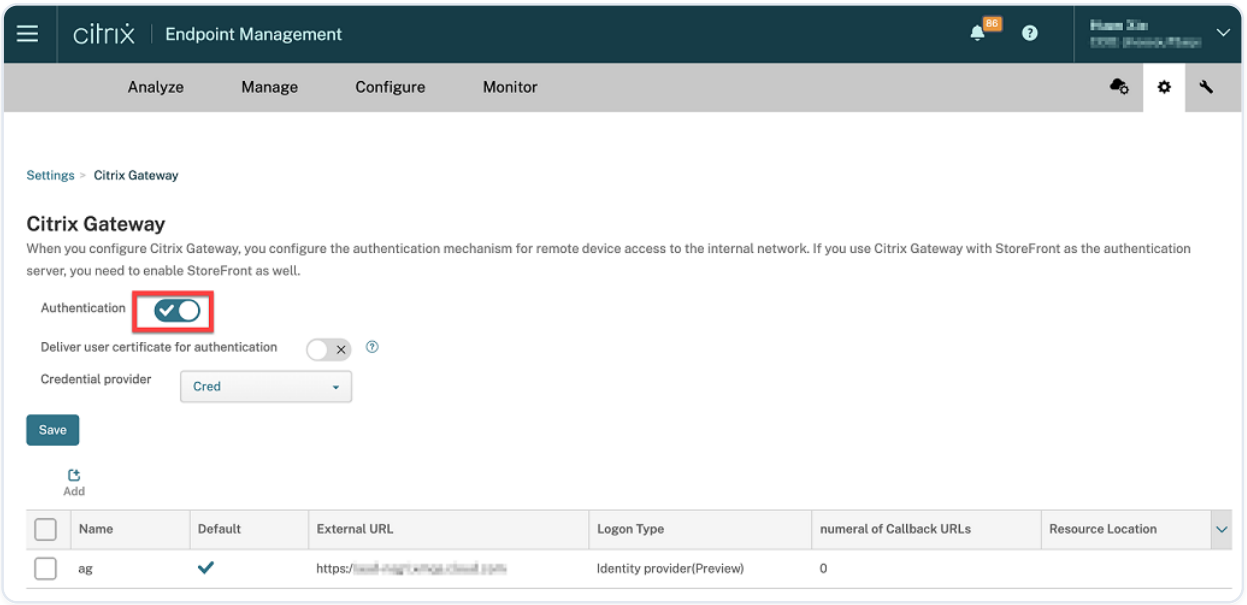
- Configure Citrix Endpoint Management con Okta a través de Citrix Cloud como IdP para dispositivos inscritos con MDM. Para obtener más información sobre la configuración de Okta para MDM, consulte Autenticación con Okta a través de Citrix Cloud.
- Habilite las siguientes marcas de funciones relevantes según la plataforma, respectivamente:
  - iOS:
    - iOS-V3Form-MAM
    - iOS-SAMLAuth-MAM
  - Android:
    - Android-V3Form-MAM
    - Android-SAMLAuth-MAM

> **Nota:**
>
> Para habilitar esta función, póngase en contacto con su equipo de soporte.

- Descargue e instale la última versión de Citrix Secure Hub.
- Asegúrese de que el servicio de Okta esté disponible para su organización y de que los usuarios y grupos relevantes se hayan creado o importado a Okta.

Configurar NetScaler Gateway en Citrix Endpoint Management

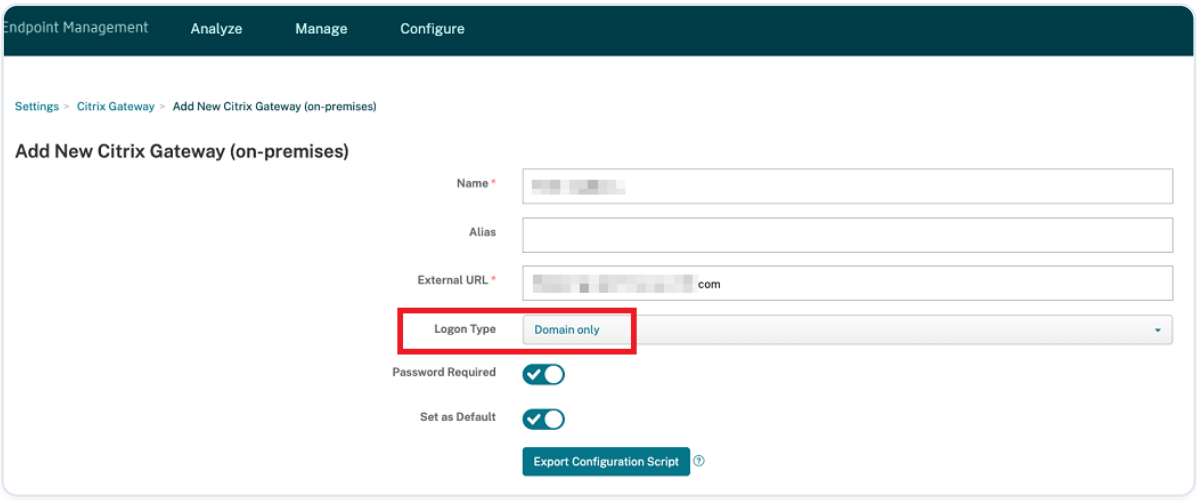
1. Inicie sesión en la consola de Citrix Endpoint Management y, a continuación, haga clic en el icono **Configuración** .
2. Haga clic en **NetScaler Gateway** en **Servidor**.
3. Habilite el botón de alternancia **Autenticación**.



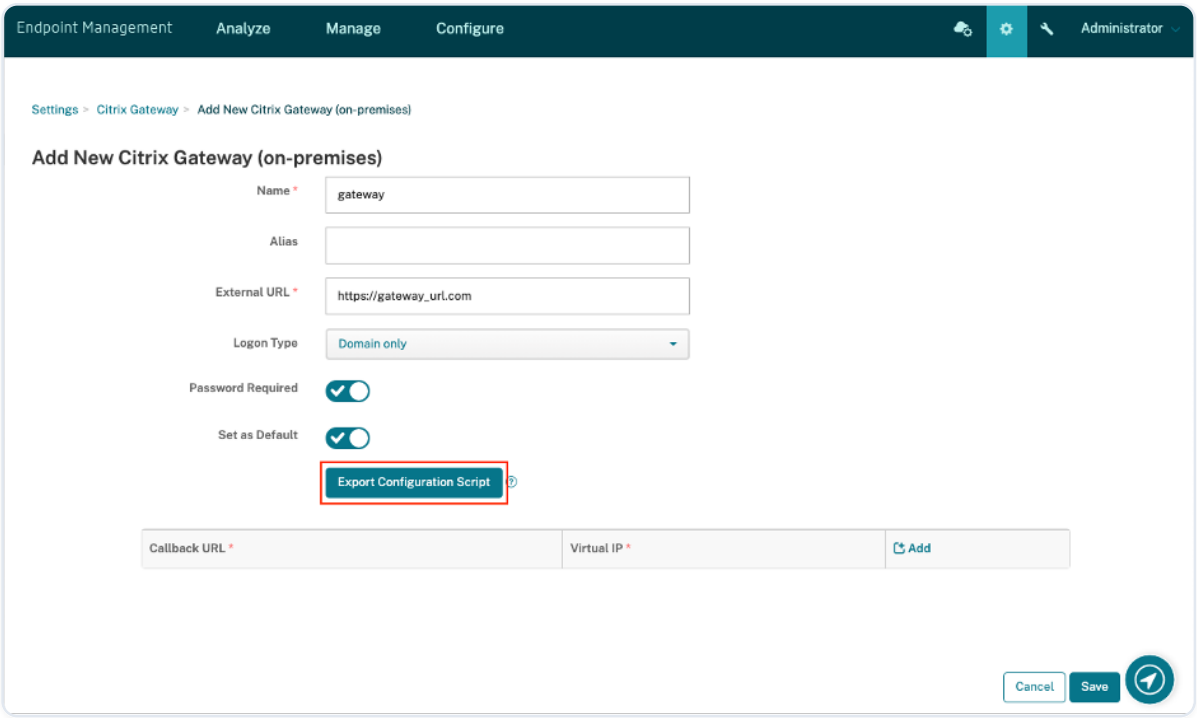
4. Asegúrese de que el **Tipo de inicio de sesión** de la puerta de enlace sea el *Proveedor de identidades*.
5. Haga clic en **Guardar**.

Preparar NetScaler Gateway local

1. Si no tiene un NetScaler Gateway local configurado para Citrix Endpoint Management, siga estos pasos:
    a. En la consola de Citrix Endpoint Management, haga clic en el icono **Configuración** .
    b. Haga clic en **NetScaler Gateway** en **Servidor**.
    c. Haga clic en **Modificar**.
    d. Haga clic en el menú desplegable **Tipo de inicio de sesión** y seleccione *Solo dominio*.

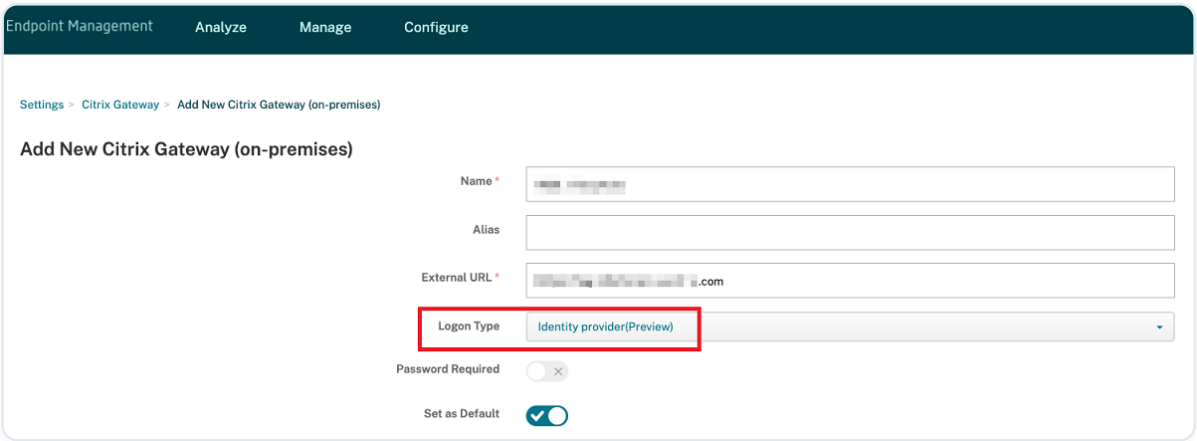


e. Haga clic en **Export Configuration Script**.



Se descarga el **Export Configuration Script**.

f. Haga clic en el menú desplegable **Logon Type** y seleccione *Identity provider*.



g. Haga clic en **Save**.

h. Abra el archivo zip descargado y extraiga los archivos de él.

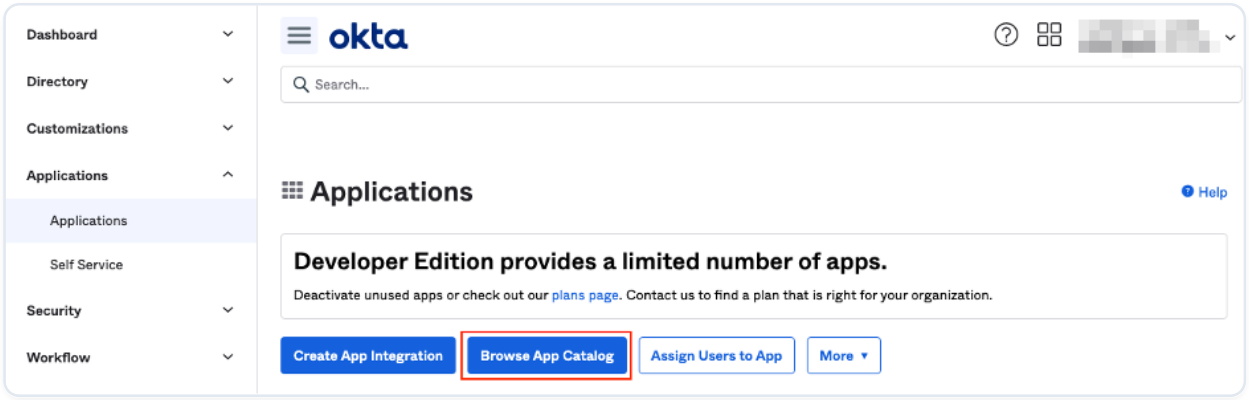
i. Ejecute los scripts en los archivos .txt extraídos para preparar el NetScaler Gateway local.



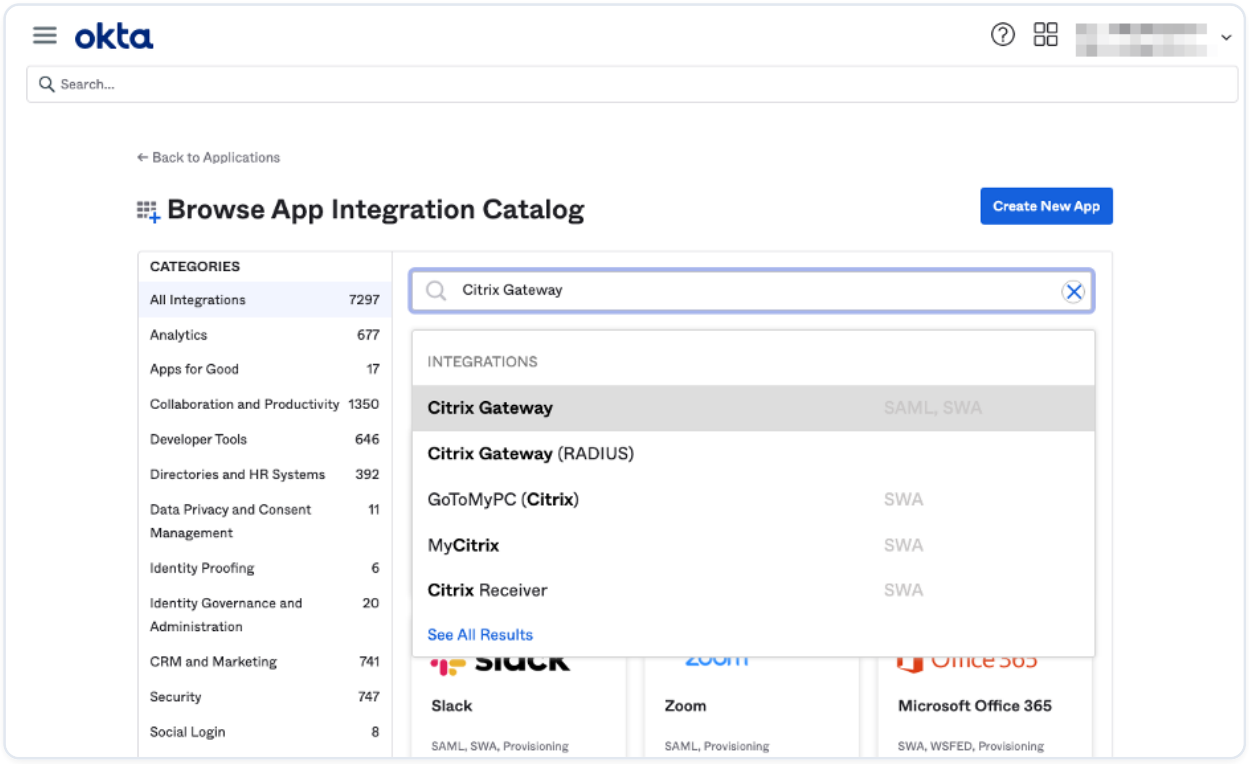
2. Inicie sesión en la consola de administración de Citrix ADC y, a continuación, vaya a **NetScaler Gateway** > **Virtual Servers**.
3. Haga clic en el gateway relevante para su configuración de Citrix Endpoint Management.
4. Desvincule cualquier política de autenticación existente en el NetScaler Gateway local.

Configurar Okta

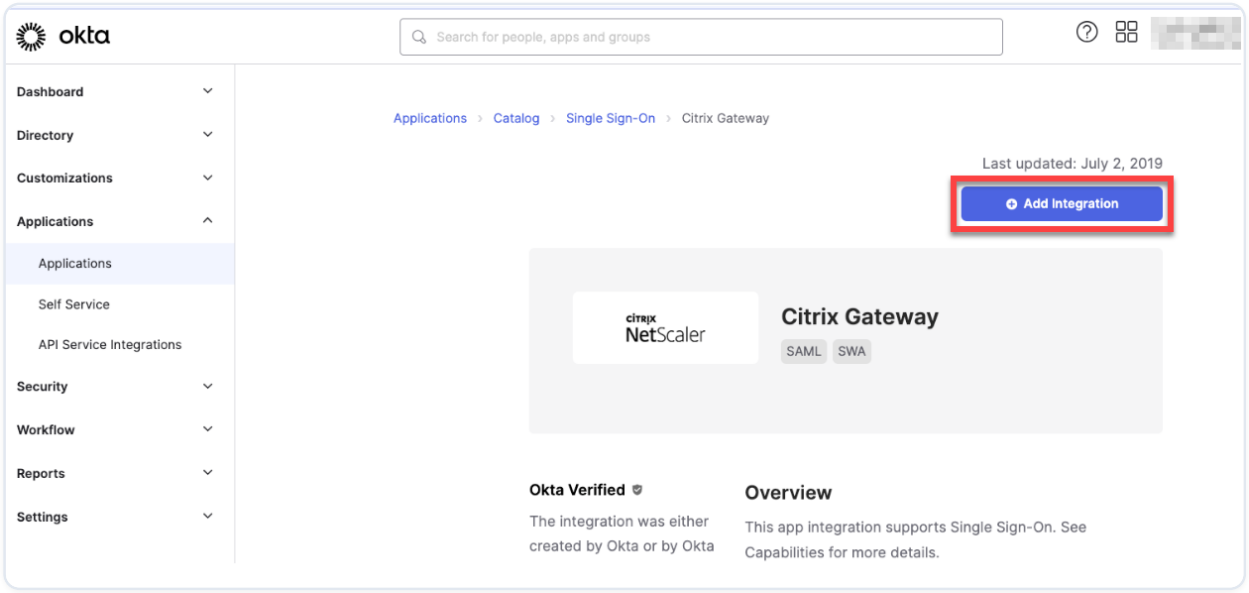
1. Inicie sesión en Okta como administrador.
2. Haga clic en **Applications** > **Applications** > **Browse App Catalog**.



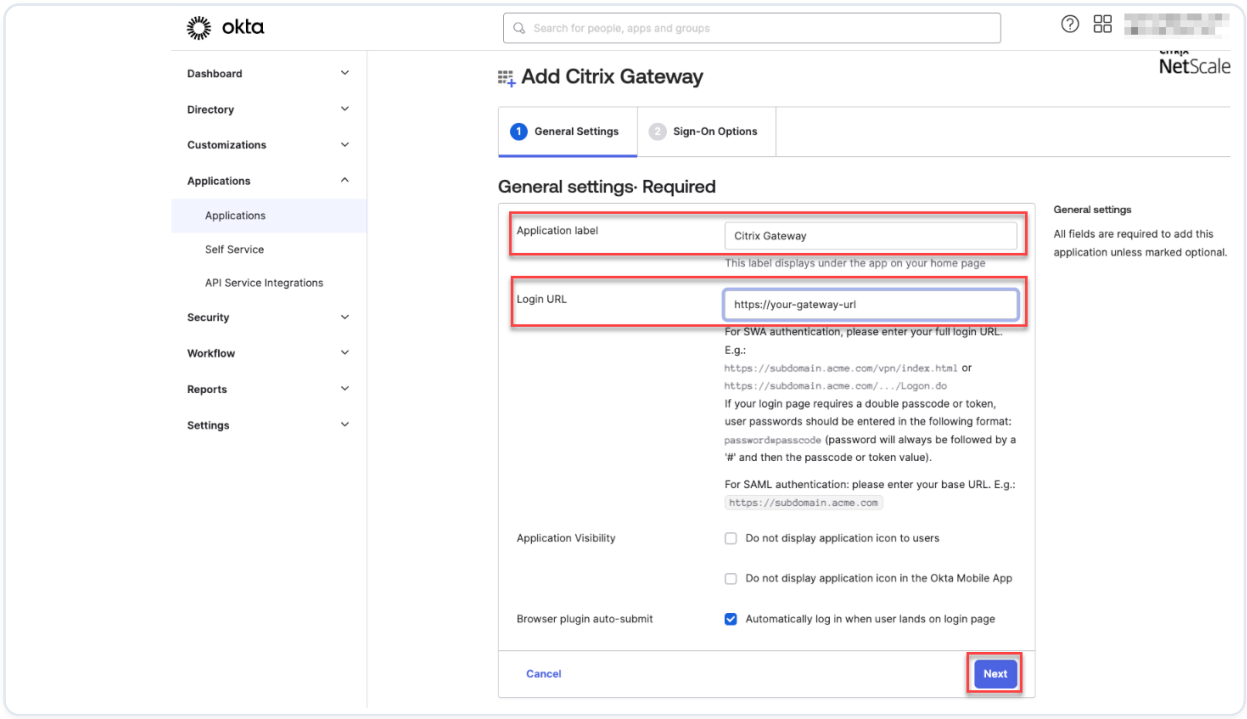
3. Escriba **NetScaler Gateway** en la barra de búsqueda en **Browse App Integration Catalog** y, a continuación, seleccione **NetScaler Gateway (SAML, SWA)**.



4. Haga clic en **Add Integration**.



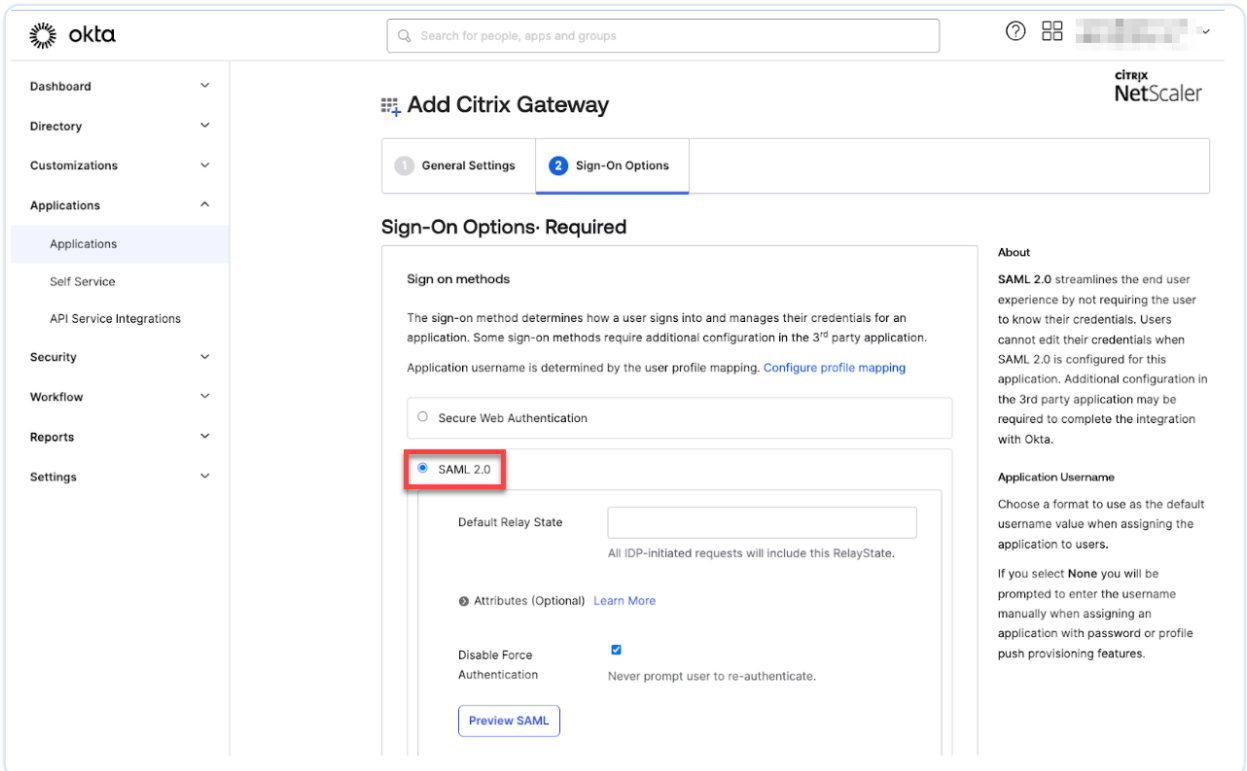
5. Introduzca el nombre correspondiente en el campo **Application label**.
6. Introduzca la URL del servidor virtual de la puerta de enlace en el campo **Login URL** y, a continuación, haga clic en **Next**.



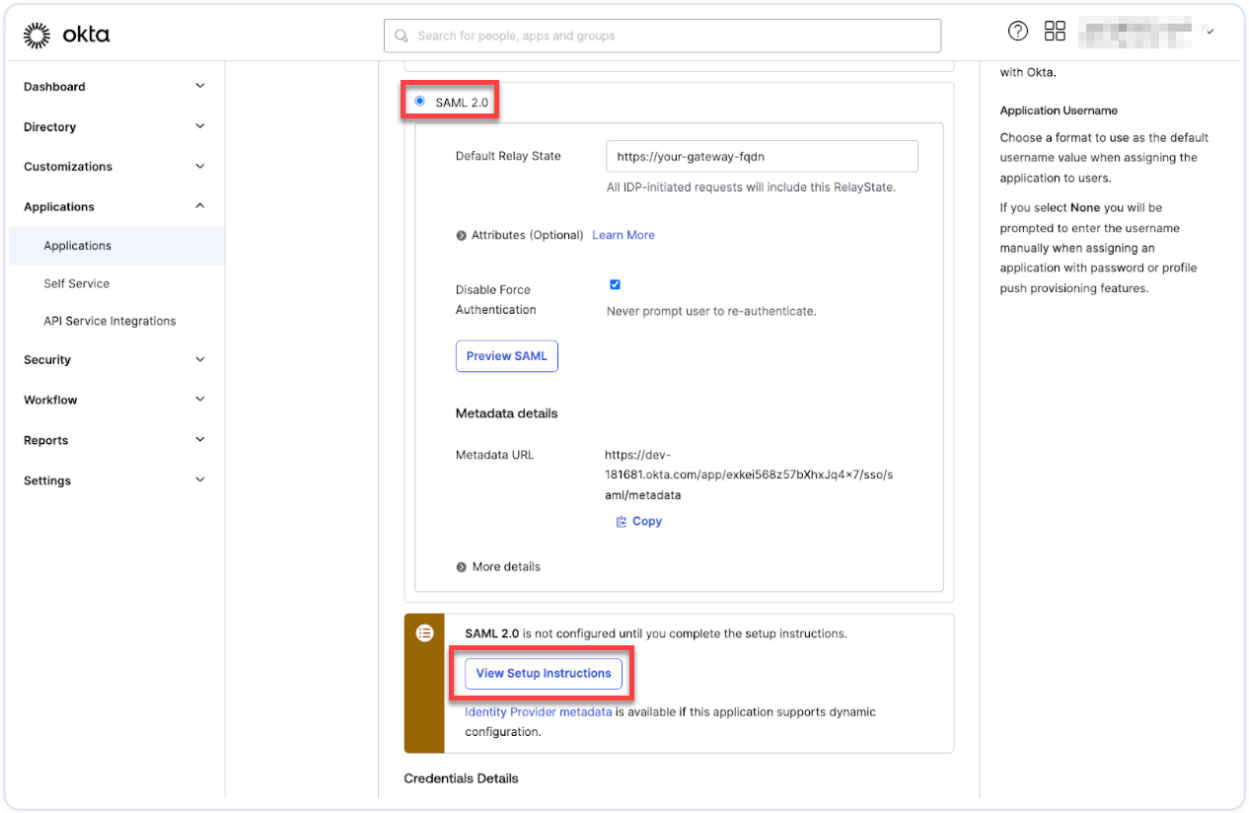
Nota:

La URL introducida en el campo **Login URL** debe ser la misma que la URL de NetScaler Gateway para la configuración de Citrix Endpoint Management.

7. En **Sign-On Options Required** > **Sign on methods**, seleccione **SAML 2.0**.



8. Haga clic en **View Setup Instructions** y siga las instrucciones proporcionadas en la página para crear la directiva SAML en la consola de administración de la puerta de enlace local de Citrix®.



Nota:

- Después de instalar el certificado de CA al configurar NetScaler Gateway versiones 11.1 o posteriores, cree una acción SAML. Para crear una acción SAML, vaya a **Security** > **AAA - Application Traffic** > **Policies** > **Authentication** > **Advanced Policies** > **Actions** > **SAML Actions**. Haga clic en **Add** y rellene la información tal como se proporciona en la página anterior. No siga la navegación proporcionada en la página, es decir, **Netscaler Gateway** > **Policies** > **Authentication** > **SAML** > **Servers**.
- Además, no siga los pasos proporcionados para crear la política SAML, ya que esos pasos utilizan la política clásica. Ahora estamos utilizando la política avanzada. Realice el siguiente paso 9 para crear una política SAML mediante una política avanzada.

9. Cree una política SAML correspondiente para la acción SAML y vincule la política al servidor virtual de autenticación de la siguiente manera:

    a. Vaya a **Seguridad** > **Tráfico de aplicaciones AAA** > **Directivas** > **Autenticación** > **Directivas avanzadas** y haga clic en **Agregar**.

    b. En la página Crear política de autenticación, proporcione los siguientes detalles:

        - **Nombre**: especifique un nombre para la política SAML.
        - **Tipo de acción**: seleccione *SAML* como tipo de acción de autenticación.
        - **Acción**: seleccione el perfil de servidor SAML con el que vincular la política SAML.
        - **Expresión**: muestra el nombre de la regla o expresión que utiliza la política SAML para determinar si el usuario debe autenticarse con el servidor SAML. En el cuadro de texto, establezca el valor **rule** = `true` para que la política SAML surta efecto y se ejecute la acción SAML correspondiente.

    c. Vincule la política SAML al servidor virtual VPN y vincule el servidor virtual VPN al servidor virtual de autenticación mediante un perfil de autenticación. Para obtener más información sobre el procedimiento de vinculación, consulte Vincular la política de autenticación.

10. Cree un servidor virtual AAA mediante Para configurar un servidor virtual de autenticación mediante la GUI.
11. Configure el servidor virtual AAA mediante Configurar el servidor virtual de autenticación.
12. Cree y configure el perfil de autenticación mediante Perfiles de autenticación.
13. Vincule el perfil de autenticación con el servidor virtual de Gateway y guarde todas las configuraciones.
14. Después de crear la política SAML en la consola de administración de Citrix Gateway local, haga clic en Listo.

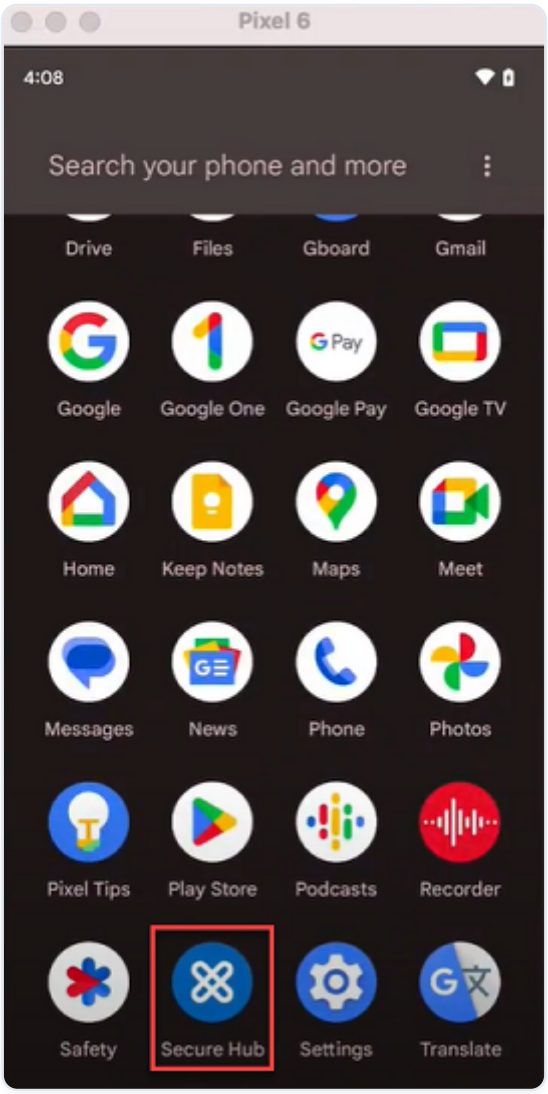
    Ahora, puede ver dos aplicaciones para la integración de Citrix Endpoint Management, es decir, una aplicación web para Citrix Cloud y una aplicación SAML para la autenticación MAM de Citrix Endpoint Management.
15. Asigne los usuarios y grupos relevantes a la aplicación SAML que creó.

Ahora, Okta se añade como proveedor de identidades para los dispositivos inscritos con MAM y puede autenticarlos usando Okta.

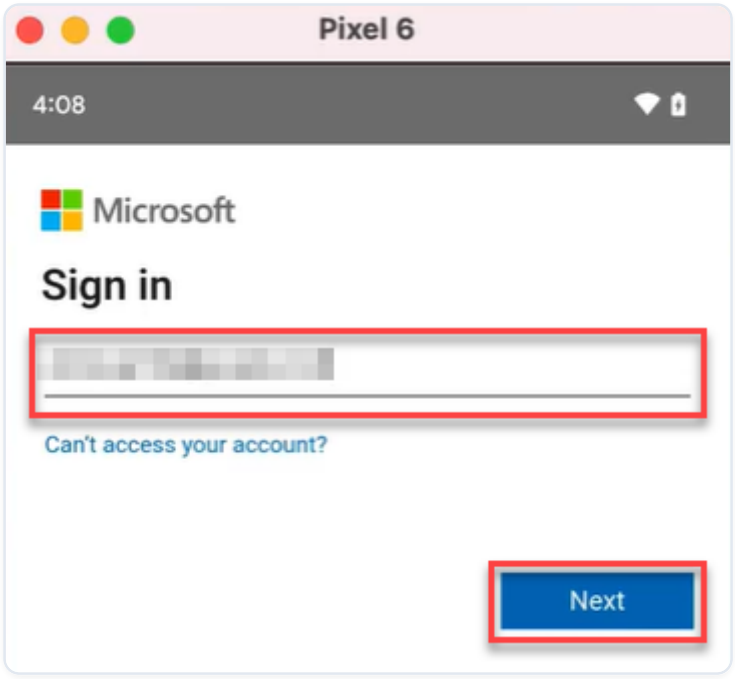
Comportamiento esperado

El siguiente ejemplo utiliza un dispositivo Android:

1. En su dispositivo móvil, abra la aplicación Citrix Secure Hub.

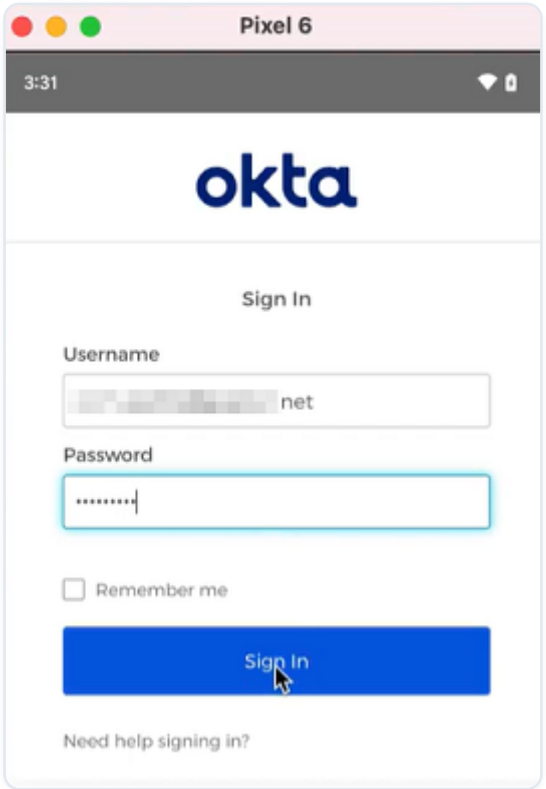


2. Proporcione los permisos necesarios.
3. En la página de inicio de sesión, introduzca las credenciales proporcionadas por su organización y, a continuación, toque **Siguiente**.

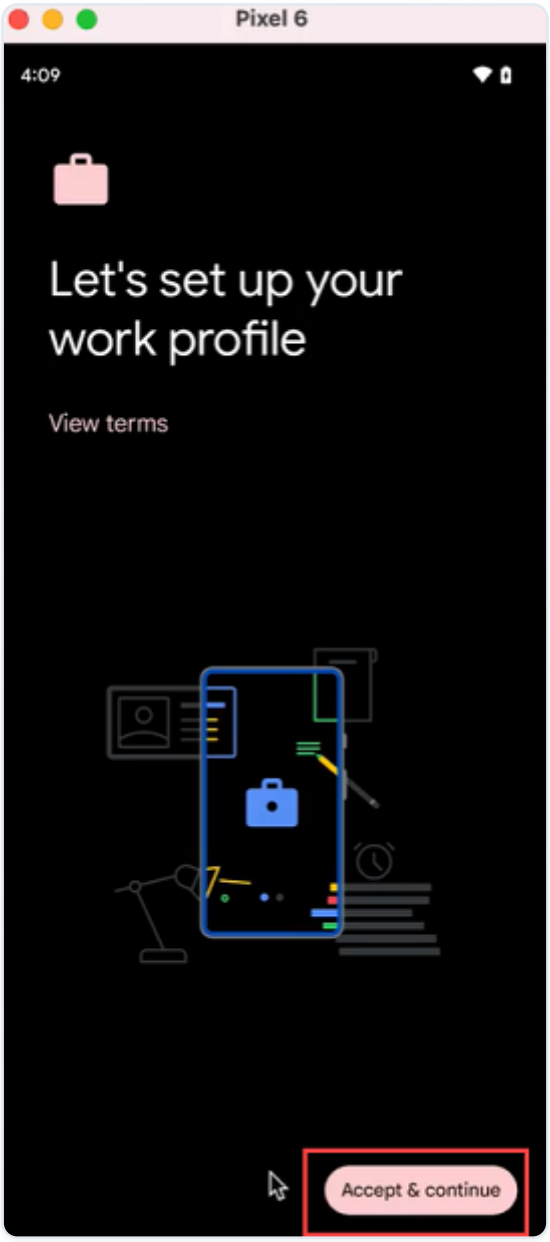


Se le redirige a la página de inicio de sesión de Okta.

4. En la página de inicio de sesión de Okta, introduzca sus credenciales y, a continuación, toque **Iniciar sesión**.



5. En la página **Configurar su perfil de trabajo**, toque **Aceptar y continuar**.



6. Cree el PIN para la aplicación Citrix Secure Hub y confírmelo.

   Pin de Citrix Secure Hub(/en-us/citrix-endpoint-management/media/citrix-secure-hub-create-pin.png)

   Se le redirige correctamente a la página de inicio de Citrix Secure Hub.

Autenticación con un NetScaler Gateway local a través de Citrix Cloud

Citrix Endpoint Management admite la autenticación con un NetScaler Gateway local a través de Citrix Cloud. Este método de autenticación solo está disponible para los usuarios que se inscriben en MDM a través de Citrix Secure Hub.

Los dispositivos que se inscriben en MAM no pueden autenticarse con credenciales de NetScaler Gateway local a través de Citrix Cloud. Para usar Citrix Secure Hub con MDM+MAM, configure Citrix Endpoint Management para que use NetScaler Gateway para la inscripción de MAM. Para obtener más información, consulte NetScaler Gateway y Citrix Endpoint Management.

Citrix Endpoint Management admite la autenticación con un NetScaler Gateway local a través de Citrix Cloud para las siguientes plataformas:

- Dispositivos iOS
- Dispositivos Android Enterprise, para los modos BYOD y totalmente administrado

Nota:

Citrix Endpoint Management no admite la autenticación con un NetScaler Gateway local a través de Citrix Cloud para las invitaciones de inscripción. Si envía a los usuarios una invitación de inscripción que tiene una URL de inscripción, los usuarios se autentican a través de LDAP en lugar de un NetScaler Gateway local como proveedor de identidades.

Se recomienda habilitar la autenticación basada en certificados para una experiencia completa de inicio de sesión único. Si utiliza la autenticación LDAP en NetScaler Gateway para el registro de MAM, los usuarios finales experimentarán un doble mensaje de autenticación durante la inscripción. Para obtener más información, consulte Autenticación de certificado de cliente o de certificado más dominio.

Requisitos previos

- NetScaler Gateway. Citrix recomienda habilitar la autenticación basada en certificados para una experiencia completa de inicio de sesión único. Si utiliza la autenticación LDAP en NetScaler Gateway para el registro de MAM, los usuarios finales experimentarán un doble mensaje de autenticación durante la inscripción. Para obtener más información, consulte Autenticación de certificado de cliente o de certificado más dominio.
- Cuenta de Citrix Cloud con Citrix Cloud Connector instalado para la sincronización del servicio de directorio.
- Citrix Secure Hub 20.5.0 y versiones posteriores.

Configurar Citrix Cloud para usar NetScaler Gateway como proveedor de identidades

Para configurar la autenticación de NetScaler Gateway en Citrix Cloud, consulte Conectar un NetScaler Gateway local como proveedor de identidades a Citrix Cloud.

Configurar el proveedor de identidades de Citrix como el tipo de IdP para Citrix Endpoint Management

Esta configuración se aplica solo a los usuarios que se inscriben a través de Citrix Secure Hub. Después de configurar NetScaler Gateway en Citrix Cloud, configure Citrix Endpoint Management de la siguiente manera.

1. En la consola de Citrix Endpoint Management, vaya a **Configuración > Proveedor de identidades (IdP)** y, a continuación, haga clic en **Agregar**.
2. En la página **Proveedor de identidades (IdP)**, configure lo siguiente:
   - **Nombre del IdP:** Escriba un nombre único para identificar la conexión del IdP que está creando.
   - **Tipo de IdP:** Elija **Proveedor de identidades de Citrix**.
   - **Dominio de autenticación:** Elija **NetScaler Gateway**. Este dominio corresponde a su dominio de proveedor de identidades en la página **Configuración del espacio de trabajo > Autenticación** de Citrix Cloud.
3. Haga clic en **Siguiente**. En la página **Uso de notificaciones del IdP**, configure lo siguiente:
   - **Tipo de identificador de usuario:** De forma predeterminada, este campo se establece en **userPrincipalName**.
   - **Cadena de identificador de usuario:** Este campo se rellena automáticamente.
4. Haga clic en **Siguiente**, revise la página **Resumen** y, a continuación, haga clic en **Guardar**.

   Ahora puede inscribir dispositivos de usuario a través de Citrix Secure Hub utilizando un NetScaler Gateway local como proveedor de identidades.

Flujo de autenticación de Citrix Secure Hub

Citrix Endpoint Management utiliza el siguiente flujo para autenticar a los usuarios con un NetScaler Gateway local como IdP en dispositivos inscritos a través de Citrix Secure Hub:

1. Un usuario inicia Citrix Secure Hub.

2. Citrix Secure Hub pasa la solicitud de autenticación a la identidad de Citrix, que pasa la solicitud a un NetScaler Gateway local.
3. El usuario escribe su nombre de usuario y contraseña.
4. Un NetScaler Gateway local valida al usuario y envía un código a la identidad de Citrix.
5. La identidad de Citrix envía el código a Citrix Secure Hub, que envía el código al servidor de Citrix Endpoint Management.
6. Citrix Endpoint Management obtiene un token de ID mediante el código y el secreto, y luego valida la información del usuario que se encuentra en el token de ID. Citrix Endpoint Management devuelve un ID de sesión.

Autenticación nFactor

La autenticación nFactor le permite usar todos los modos de autenticación actualmente posibles con NetScaler cuando utiliza Citrix Secure Hub. Mejora la seguridad de una aplicación al requerir que los usuarios proporcionen más pruebas de identidad para obtener acceso. Para obtener más información sobre la autenticación nFactor, consulte Autenticación nFactor.

Además, para obtener más información sobre los diferentes métodos de autenticación y autorización y cómo configurarlos, consulte Autenticación y autorización.

Citrix Endpoint Management admite los siguientes tipos de autenticación con la autenticación nFactor:

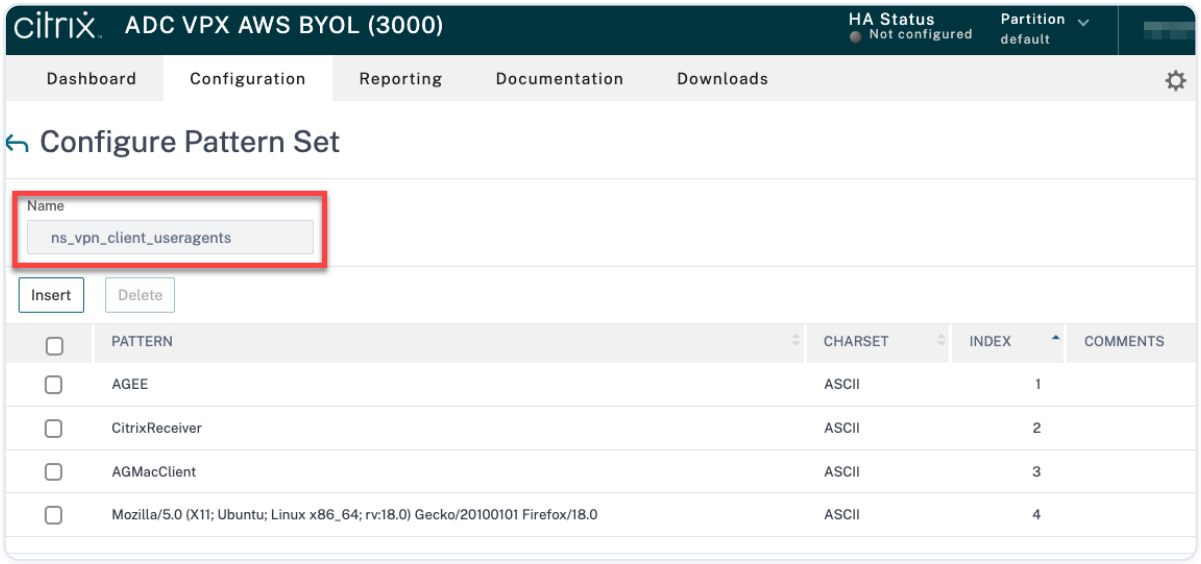
- Local
- Protocolo ligero de acceso a directorios (LDAP)
- RADIUS
- SAML
- Autenticación de certificado de cliente

Requisitos previos

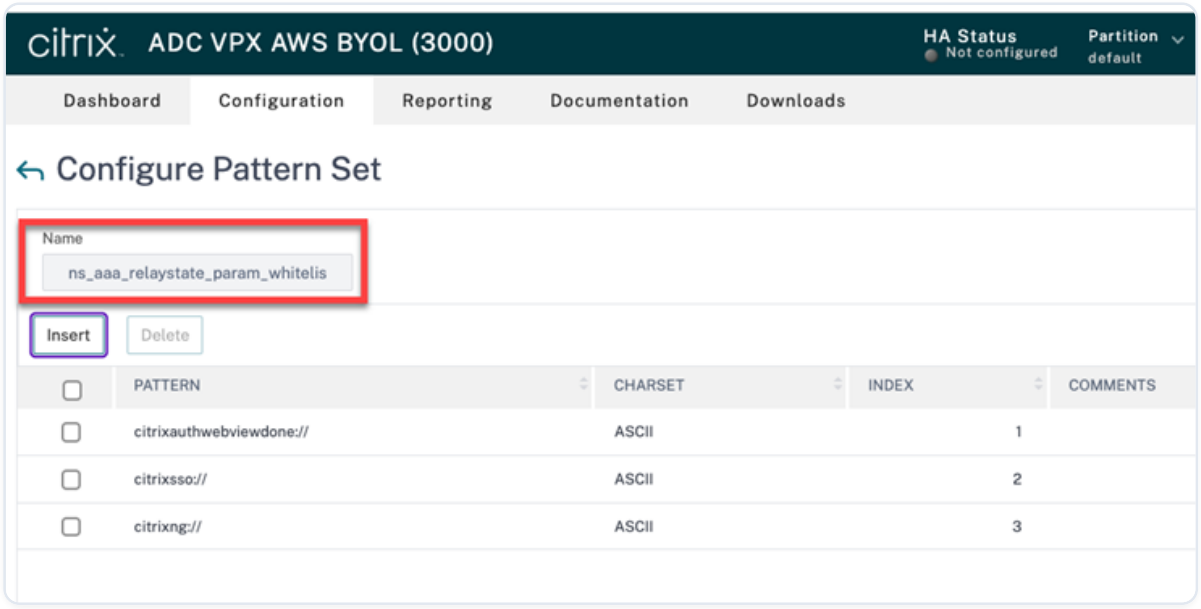
Para configurar Citrix Endpoint Management para que utilice la autenticación nFactor, asegúrese de que se cumplen los siguientes requisitos previos:

- Asegúrese de que está utilizando NetScaler 13.0 o posterior.
- Asegúrese de haber configurado los siguientes ajustes del conjunto de patrones en NetScaler® para sus dispositivos Android e iOS:

- Ns_vpn_client_useragents



- Ns_aaa_relaystate_param_whitelist



- Asegúrese de haber instalado la última versión de Citrix Secure Hub desde Apple o Google Play.
- Asegúrese de que está utilizando la directiva de autenticación avanzada en NetScaler Gateway.
- Asegúrese de establecer la propiedad de cliente **ENABLE_MAM_NFACTOR_SSO** como **True** tanto para entornos locales como en la nube. Para obtener más información sobre la propiedad **ENABLE_MAM_NFACTOR_SSO**, consulte Referencia de propiedades de cliente.

> **Nota:**

> Si la propiedad de cliente **Enable nFactor SSO** está establecida en **False**, asegúrese de que las directivas de autenticación clásicas estén vinculadas a NetScaler Gateway.

Configurar la autenticación nFactor

Configure la autenticación nFactor para Citrix Endpoint Management en función de cómo esté configurado su NetScaler Gateway, de la siguiente manera:

- Citrix Endpoint Management ya está configurado con NetScaler Gateway mediante la directiva de autenticación clásica. Para obtener más información, consulte Actualizar la directiva clásica a la directiva de autenticación avanzada en el NetScaler Gateway existente.
- Configuración de Citrix Endpoint Management con NetScaler Gateway mediante la directiva de autenticación avanzada. Para obtener más información, consulte Configurar la configuración de NetScaler Gateway mediante la directiva avanzada.

Actualizar la directiva clásica a la directiva de autenticación avanzada en el NetScaler Gateway existente

Si su Citrix Endpoint Management ya está configurado mediante la directiva de autenticación clásica en NetScaler Gateway, debe actualizar la directiva de autenticación clásica a la directiva de autenticación avanzada mediante uno de los siguientes métodos:

- Cree una directiva de autenticación avanzada y cambie la configuración de la puerta de enlace para usar la directiva de autenticación avanzada. Para obtener más información, consulte Directivas de autenticación.
- Actualice la directiva de autenticación clásica a la directiva de autenticación avanzada. Para obtener más información, consulte Conversión de expresiones de directiva mediante la herramienta NSPEPI.

Configure la configuración de NetScaler Gateway mediante la política avanzada

Para configurar la autenticación nFactor para Citrix Endpoint Management en NetScaler Gateway mediante la política de autenticación avanzada, consulte Configurar la autenticación nFactor.

> **Nota:**
>
> - Puede elegir el tipo de autenticación relevante entre los tipos de autenticación admitidos.

- Si utiliza el tipo de autenticación SAML, puede configurar SAML mediante MAM IdP utilizando uno de los siguientes métodos:
  - Para configurar mediante Azure Active Directory, consulte Autenticación con Azure Active Directory a través de NetScaler Gateway para la inscripción de MAM.
  - Para configurar mediante Okta, consulte Autenticación con Okta a través de NetScaler Gateway para la inscripción de MAM.

Cuentas de usuario, roles e inscripción

Las tareas de configuración de usuarios se realizan en la consola de Citrix Endpoint Management, en la ficha **Administrar** y en la página **Configuración**. A menos que se indique lo contrario, los pasos para las siguientes tareas se proporcionan en este artículo.

- Modo de seguridad de inscripción e invitaciones
    - En **Configuración > Inscripción**, configure hasta siete modos de seguridad de inscripción y envíe invitaciones de inscripción. Cada modo de seguridad de inscripción tiene su propio nivel de seguridad y el número de pasos que los usuarios deben seguir para inscribir sus dispositivos.
- Roles para cuentas de usuario y grupos
    - En **Configuración > Control de acceso basado en roles**, asigne roles predefinidos, o conjuntos de permisos, a usuarios y grupos. Estos permisos controlan el nivel de acceso que tienen los usuarios a las funciones del sistema. Para obtener más información, consulte Configurar roles con RBAC.
    - En **Configuración > Plantillas de notificación**, cree o actualice las plantillas de notificación que se usarán en acciones automatizadas, inscripciones y mensajes de notificación estándar enviados a los usuarios. Configure las plantillas de notificación para enviar mensajes a través de dos canales diferentes: Citrix Secure Hub o SMTP. Para obtener más información, consulte: Crear y actualizar plantillas de notificación.
- Cuentas de usuario y grupos:
    - En **Administrar > Usuarios**, puede agregar cuentas de usuario locales manualmente o usar un archivo de aprovisionamiento .csv para importar las cuentas y administrar grupos locales. Sin embargo, la mayoría de las implementaciones de Citrix Endpoint Management se conectan a LDAP para obtener información de usuarios y grupos. Puede que prefiera crear cuentas de usuario localmente en casos de uso como los siguientes:
        - En entornos, como el minorista, donde los dispositivos se comparten en lugar de dedicarse a usuarios individuales.
        - Si utiliza un directorio no compatible, como Novell eDirectory.

    - En **Configuración > Flujos de trabajo**, use flujos de trabajo para administrar la creación y eliminación de cuentas de usuario.

Acerca de las cuentas de usuario

Una cuenta de usuario de Citrix Endpoint Management es para un usuario local, de Active Directory o de la nube.

- **Usuarios de la nube:** Un usuario de la nube es una cuenta de usuario especial que Citrix Cloud crea cuando se agrega un administrador a su cuenta de cliente de Citrix Cloud. Una cuenta de usuario de la nube utiliza el mismo nombre de usuario que la cuenta de administrador en Citrix Cloud y, por defecto, tiene el rol de administrador. La cuenta de usuario de la nube proporciona inicio de sesión único y realiza otras funciones administrativas.

  Para añadir administradores a una cuenta de Citrix Cloud, consulte Invitar a nuevos administradores.

Para usuarios de la nube:

- Puede cambiar los roles y las propiedades de usuario de los usuarios de la nube a través de la consola de Citrix Cloud. Consulte Administrar administradores de Citrix Cloud.
- Para cambiar la contraseña, consulte Administradores.
- Para eliminar un usuario de la nube, en Citrix Cloud, vaya a **Administración de identidades y accesos > Administradores**. Haga clic en los puntos suspensivos al final de la fila del usuario y, a continuación, seleccione **Eliminar administrador**.
- No puede añadir usuarios de la nube a un grupo local.

Configurar modos de seguridad de inscripción

Configure un modo de seguridad de inscripción de dispositivos para especificar un nivel de seguridad y una plantilla de notificación para la inscripción de dispositivos en Citrix Endpoint Management.

Citrix Endpoint Management ofrece seis modos de seguridad de inscripción, cada uno con su propio nivel de seguridad y los pasos que los usuarios deben seguir para inscribir sus dispositivos. Los modos de seguridad de inscripción se configuran en la consola de Citrix Endpoint Management desde la página **Administrar > Invitaciones de inscripción**. Para obtener más información, consulte Invitaciones de inscripción.

Nota:

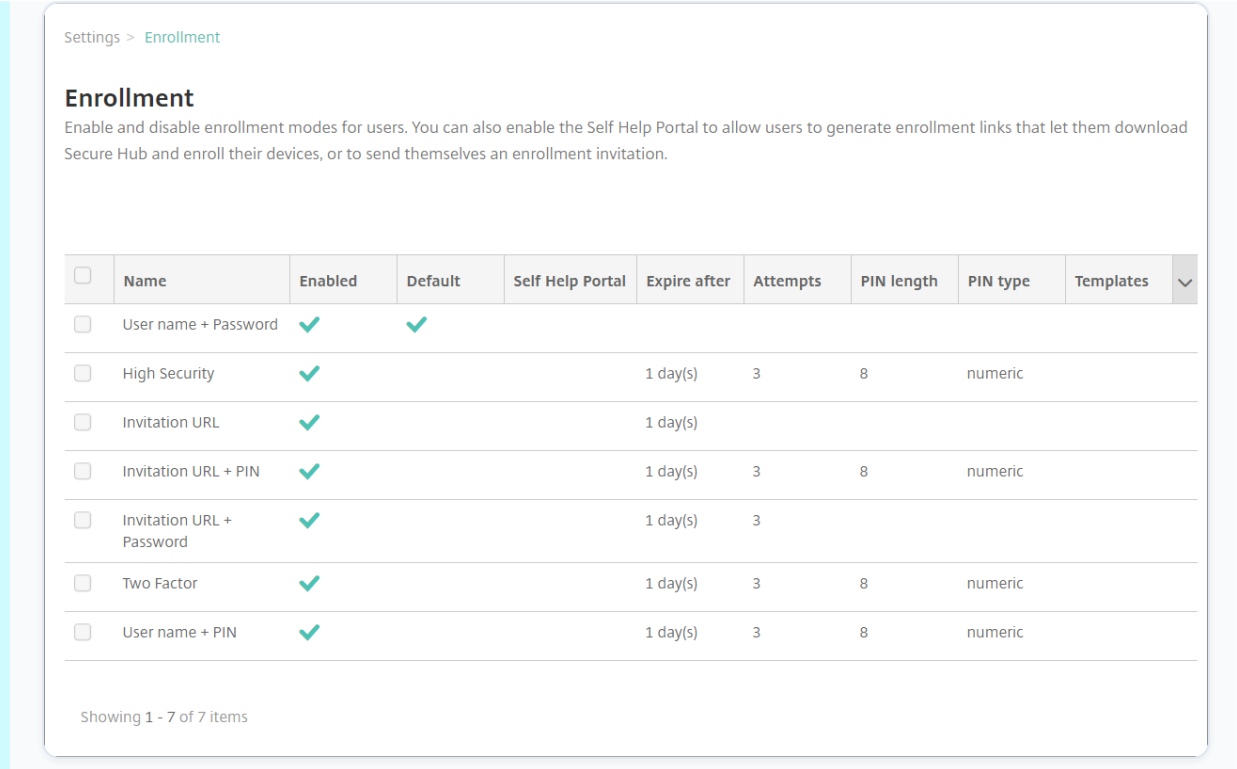
Si tiene previsto utilizar plantillas de notificación personalizadas, debe configurarlas antes de configurar los modos de seguridad de inscripción. Para obtener más información sobre las plantillas de notificación, consulte Crear o actualizar plantillas de notificación.

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha de la consola. Aparece la página **Configuración**.
2. Haga clic en **Inscripción**. Aparece la página **Inscripción**. Contiene una tabla con todos los modos de seguridad de inscripción disponibles. De forma predeterminada, todos los modos de seguridad de inscripción están habilitados.
3. Seleccione cualquier modo de seguridad de inscripción de la lista para editarlo. A continuación, establezca el modo como predeterminado o desactive el modo.

   Seleccione la casilla de verificación junto a un modo de seguridad de inscripción para ver el menú de opciones. O bien, haga clic en cualquier otro lugar de la lista para ver el menú de opciones en el lado derecho de la lista.

   Consejo:

   Al editar el modo de seguridad de inscripción, puede especificar una fecha límite de caducidad después de la cual los usuarios no podrán inscribir sus dispositivos. Para obtener información, consulte Para editar un modo de seguridad de inscripción en este artículo. El valor aparece en las páginas de configuración de invitación de inscripción de usuarios y grupos.



Tiene las siguientes opciones de modo de seguridad de inscripción según su plataforma:

- Nombre de usuario + Contraseña
- URL de invitación
- URL de invitación + PIN
- URL de invitación + Contraseña
- Dos factores
- Nombre de usuario + PIN

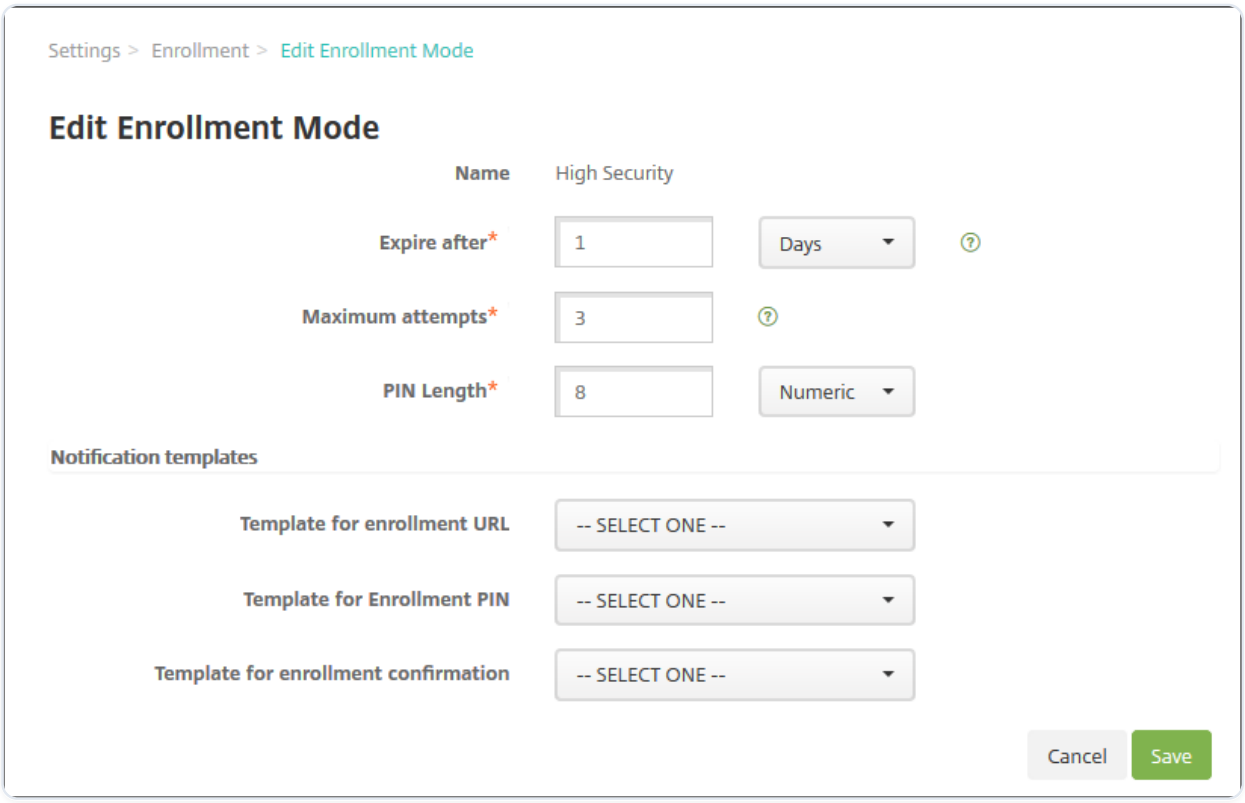
Para obtener información sobre los modos de seguridad de inscripción específicos de la plataforma, consulte Modos de seguridad de inscripción por plataforma.

Puede usar las invitaciones de inscripción como una forma eficaz de restringir la capacidad de inscripción a usuarios o grupos específicos. Para enviar invitaciones de inscripción, solo puede usar los modos de seguridad de inscripción **URL de invitación**, **URL de invitación + PIN** o **URL de invitación + Contraseña**. Para los dispositivos que se inscriben con **Nombre de usuario + Contraseña**, **Autenticación de dos factores** o **Nombre de usuario + PIN**, los usuarios deben introducir manualmente sus credenciales en Citrix Secure Hub.

Puede usar invitaciones de inscripción con PIN de un solo uso (a veces también llamado OTP) como solución de autenticación de dos factores. Las invitaciones de inscripción con PIN de un solo uso controlan la cantidad de dispositivos que un usuario puede inscribir. Las invitaciones OTP no están disponibles para dispositivos Windows.

Para editar un modo de seguridad de inscripción

1. En la lista **Inscripción**, seleccione un modo de seguridad de inscripción y, a continuación, haga clic en **Editar**. Aparece la página **Editar modo de inscripción**. Según el modo que seleccione, es posible que vea diferentes opciones.



2. Cambie la siguiente información según corresponda:

   - **Caduca después de:** Escriba una fecha límite de caducidad después de la cual los usuarios no podrán inscribir sus dispositivos. Este valor aparece en las páginas de configuración de invitación de inscripción de usuarios y grupos.

     Escriba **0** para evitar que la invitación caduque.
   - **Días:** Haga clic en **Días** u **Horas** en la lista desplegable para que se corresponda con la fecha límite de caducidad que introdujo en **Caduca después de**.
   - **Intentos máximos:** Escriba el número de intentos de inscripción que un usuario puede realizar antes de ser bloqueado del proceso de inscripción. Este valor aparece en las páginas de configuración de invitación de inscripción de usuarios y grupos.

     Escriba **0** para permitir intentos ilimitados.
   - **Longitud del PIN:** Escriba un número para establecer la longitud del PIN generado.
   - **Numérico:** Haga clic en **Numérico** o **Alfanumérico** en la lista desplegable para el tipo de PIN.

- **Plantillas de notificación:**
  - **Plantilla para URL de inscripción:** Haga clic en una plantilla de la lista desplegable para usarla para la URL de inscripción. Por ejemplo, la plantilla de invitación de inscripción envía un correo electrónico a los usuarios. Para obtener más información sobre las plantillas de notificación, consulte (/es-es/citrix-endpoint-management/users/notifications.html#create-and-update-notification-templates).
  - **Plantilla para PIN de inscripción:** Haga clic en una plantilla de la lista desplegable para usarla para el PIN de inscripción.
  - **Plantilla para confirmación de inscripción:** Haga clic en una plantilla de la lista desplegable para usarla para informar a un usuario de que se ha inscrito correctamente.

3. Haga clic en **Guardar**.

Para establecer un modo de seguridad de inscripción como predeterminado

El modo de seguridad de inscripción predeterminado se utiliza para todas las solicitudes de inscripción de dispositivos, a menos que seleccione un modo de seguridad de inscripción diferente. Si no se establece ningún modo de seguridad de inscripción como predeterminado, debe crear una solicitud de inscripción para cada inscripción de dispositivo.

1. Si el modo de seguridad de inscripción que quiere usar como predeterminado no está habilitado, selecciónelo y haga clic en **Habilitar**. Los únicos modos de seguridad de inscripción que puede usar como predeterminados son **Nombre de usuario + Contraseña**, **Doble factor** o **Nombre de usuario + PIN**.
2. Seleccione el modo de seguridad de inscripción y haga clic en **Predeterminado**. El modo seleccionado ahora es el predeterminado. Si cualquier otro modo de seguridad de inscripción estaba establecido como predeterminado, ese modo deja de serlo.

Para inhabilitar un modo de seguridad de inscripción

Al inhabilitar un modo de seguridad de inscripción, este deja de estar disponible, tanto para las invitaciones de inscripción de grupos como en el portal de autoayuda. Puede cambiar la forma en que permite a los usuarios inscribir sus dispositivos inhabilitando un modo de seguridad de inscripción y habilitando otro.

1. Seleccione un modo de seguridad de inscripción.

No puede inhabilitar el modo de seguridad de inscripción predeterminado. Si quiere inhabilitar el modo de seguridad de inscripción predeterminado, primero debe quitar su estado predeterminado.

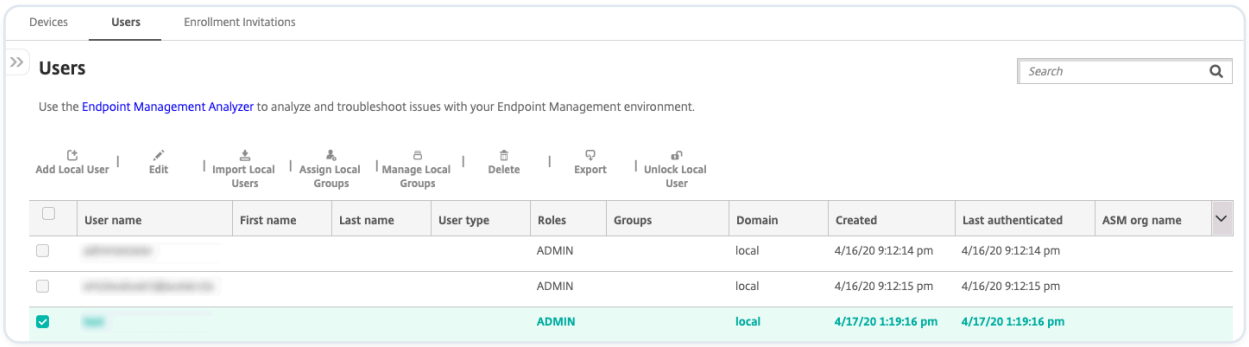
2. Haga clic en **Inhabilitar**. El modo de seguridad de inscripción ya no está habilitado.

Agregar, modificar, desbloquear o eliminar cuentas de usuario locales

Puede agregar cuentas de usuario locales a Citrix Endpoint Management manualmente o puede usar un archivo de aprovisionamiento para importar las cuentas. Para conocer los pasos para importar cuentas de usuario desde un archivo de aprovisionamiento, consulte Importar cuentas de usuario.

Todos los administradores de Citrix Cloud se crean como administradores de Citrix Endpoint Management. Si crea un administrador de Citrix Cloud con acceso personalizado, asegúrese de que el acceso incluya Citrix Endpoint Management. Para obtener información sobre cómo agregar administradores de Citrix Cloud, consulte Agregar administradores.

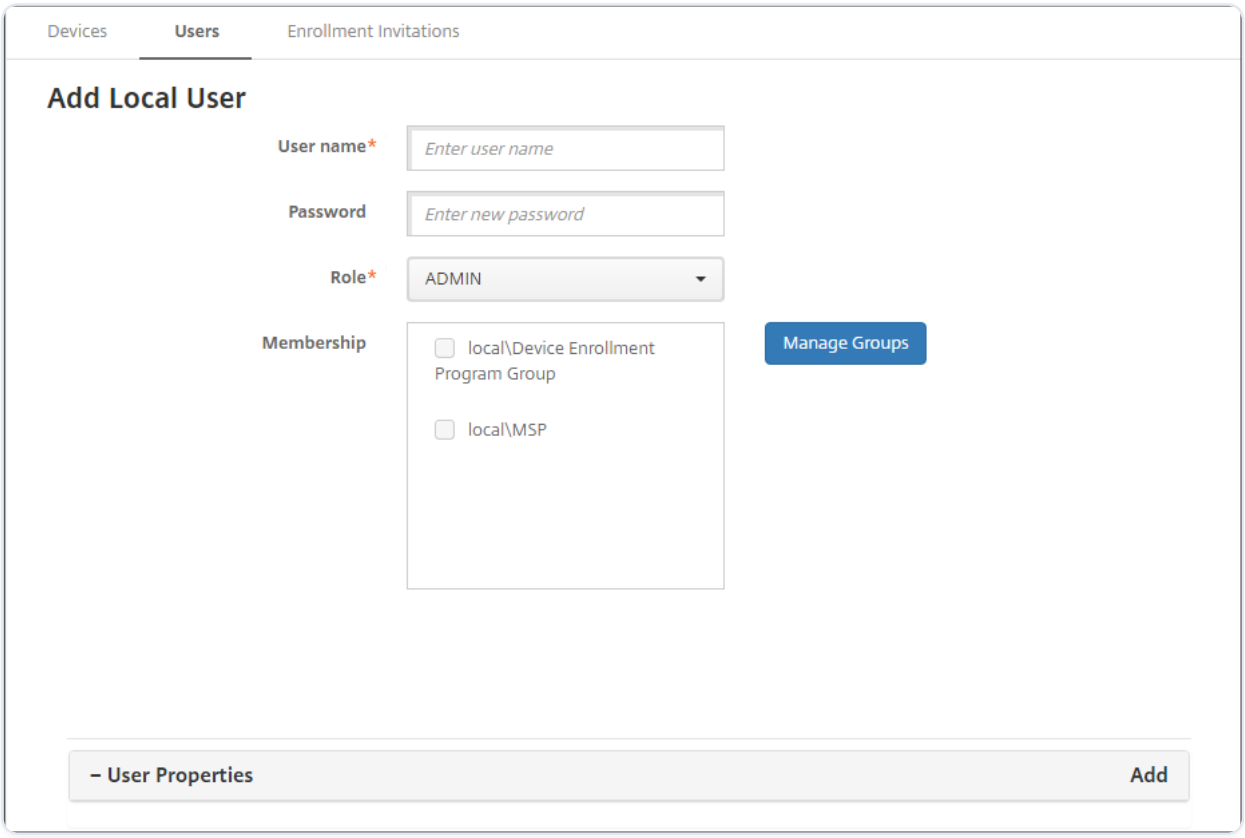
1. En la consola de Citrix Endpoint Management, haga clic en **Administrar > Usuarios**. Aparecerá la página **Usuarios**.



2. Haga clic en **Mostrar filtro** para filtrar la lista.

Para agregar una cuenta de usuario local

1. En la página **Usuarios**, haga clic en **Agregar usuario local**. Aparecerá la página **Agregar usuario local**.



2. Configure estos ajustes:

- **Nombre de usuario:** Escriba el nombre, un campo obligatorio. Puede incluir lo siguiente en los nombres: espacios, letras mayúsculas y letras minúsculas.
- **Contraseña:** Escriba una contraseña de usuario opcional. La contraseña debe tener al menos 14 caracteres y cumplir todos los criterios siguientes:
  - Incluir al menos dos números
  - Incluir al menos una letra mayúscula y una minúscula
  - Incluir al menos un carácter especial
  - No incluya palabras de diccionario ni palabras restringidas, como su nombre de usuario de Citrix® o su dirección de correo electrónico
  - No incluya más de tres caracteres secuenciales y repetidos o patrones de teclado, como 1111, 1234 o asdf
- **Rol:** Haga clic en el rol de usuario en la lista desplegable. Para obtener más información sobre los roles, consulte Configurar roles con RBAC. Las opciones posibles son:
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT

    - USER

- **Pertenencia:** Haga clic en el grupo o grupos de la lista desplegable a los que desea añadir el usuario.
- **Propiedades de usuario:** Agregue propiedades de usuario opcionales. Para cada propiedad de usuario que desee agregar, haga clic en **Agregar** y realice lo siguiente:

    - **Propiedades de usuario:** Haga clic en una propiedad de la lista desplegable y, a continuación, escriba el atributo de la propiedad de usuario en el campo junto a la propiedad.
    - Haga clic en **Listo** para guardar la propiedad de usuario o haga clic en **Cancelar**.

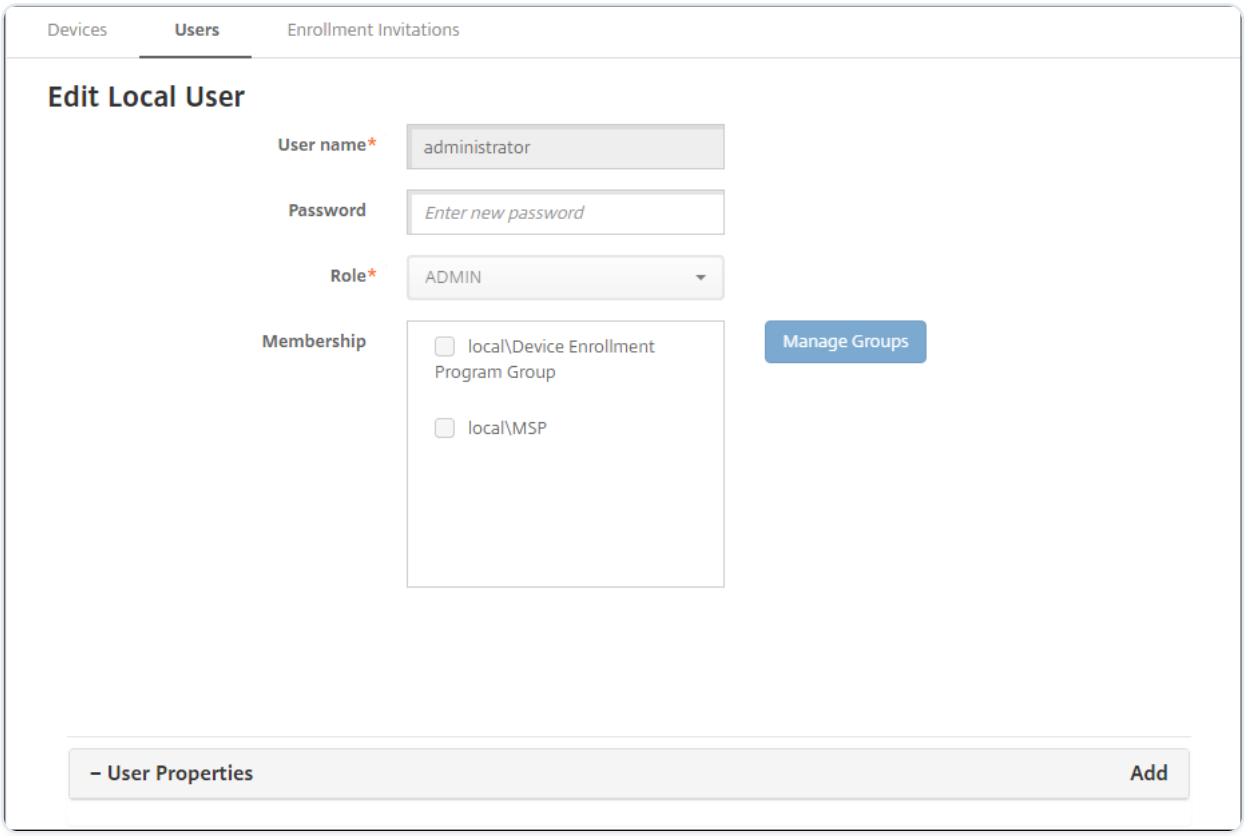
  Para eliminar una propiedad de usuario existente, coloque el puntero sobre la línea que contiene la propiedad y, a continuación, haga clic en la **X** del lado derecho. La propiedad se elimina inmediatamente.

  Para modificar una propiedad de usuario existente, haga clic en la propiedad y realice los cambios. Haga clic en **Listo** para guardar la entrada modificada o en **Cancelar** para dejar la entrada sin cambios.

3. Haga clic en **Guardar**. Después de crear un usuario, el campo **Tipo de usuario** de una cuenta de usuario local permanece vacío.

Para modificar una cuenta de usuario local

1. En la página **Usuarios**, en la lista de usuarios, haga clic para seleccionar un usuario y, a continuación, haga clic en **Modificar**. Aparece la página **Modificar usuario local**.



2. Modifique la siguiente información según corresponda:

- **Nombre de usuario:** No puede cambiar el nombre de usuario.
- **Contraseña:** Cambie o agregue una contraseña de usuario.
- **Rol:** Haga clic en el rol de usuario de la lista desplegable.
- **Pertenencia:** Haga clic en el grupo o grupos de la lista desplegable a los que desea agregar o modificar la cuenta de usuario. Para quitar la cuenta de usuario de un grupo, desactive la casilla de verificación junto al nombre del grupo.
- **Propiedades de usuario:** Realice una de las siguientes acciones:
  - Para cada propiedad de usuario que desee cambiar, haga clic en la propiedad y realice los cambios. Haga clic en **Listo** para guardar la lista modificada o en **Cancelar** para dejar la lista sin cambios.
  - Para cada propiedad de usuario que desee añadir, haga clic en **Añadir** y realice lo siguiente:
    - **Propiedades de usuario:** Haga clic en una propiedad de la lista desplegable y, a continuación, escriba el atributo de la propiedad de usuario en el campo junto a la propiedad.
    - Haga clic en **Listo** para guardar la propiedad de usuario o haga clic en **Cancelar**.

- Para cada propiedad de usuario existente que desee eliminar, pase el ratón por encima de la línea que contiene la propiedad y, a continuación, haga clic en la **X** del lado derecho. La propiedad se elimina inmediatamente.

3. Haga clic en **Guardar** para guardar los cambios o haga clic en **Cancelar** para dejar al usuario sin cambios.

Para desbloquear una cuenta de usuario local

Una cuenta de usuario local se bloquea según estas propiedades del servidor:

- `local.user.account.lockout.time`
- `local.user.account.lockout.limit`

  Para obtener más información, consulte Definiciones de propiedades del servidor.

Cuando una cuenta de usuario local se bloquea, puede desbloquearla desde la consola de Citrix Endpoint Management.

1. En la página **Usuarios**, en la lista de cuentas de usuario, haga clic para seleccionar una cuenta de usuario.
2. Haga clic en **Desbloquear usuario**. Aparece un cuadro de diálogo de confirmación.
3. Haga clic en **Desbloquear** para desbloquear la cuenta de usuario o haga clic en **Cancelar** para dejar al usuario sin cambios.

No puede abrir un usuario de Active Directory desde la consola de Citrix Endpoint Management. Un usuario de Active Directory bloqueado debe ponerse en contacto con el servicio de asistencia de Active Directory para restablecer la contraseña.

Para eliminar una cuenta de usuario local

1. En la página **Usuarios**, en la lista de cuentas de usuario, haga clic para seleccionar una cuenta de usuario.

   Puede seleccionar más de una cuenta de usuario para eliminar marcando la casilla de verificación junto a cada cuenta de usuario.
2. Haga clic en **Eliminar**. Aparece un cuadro de diálogo de confirmación.
3. Haga clic en **Eliminar** para eliminar la cuenta de usuario o haga clic en **Cancelar**.

Para eliminar usuarios de Active Directory

Para eliminar uno o varios usuarios de Active Directory a la vez, seleccione los usuarios y haga clic en **Eliminar**.

Si un usuario que elimina tiene dispositivos inscritos y desea volver a inscribir esos dispositivos, elimine los dispositivos antes de volver a inscribirlos. Para eliminar un dispositivo, vaya a **Administrar > Dispositivos**, seleccione el dispositivo y, a continuación, haga clic en **Eliminar**.

Importar cuentas de usuario

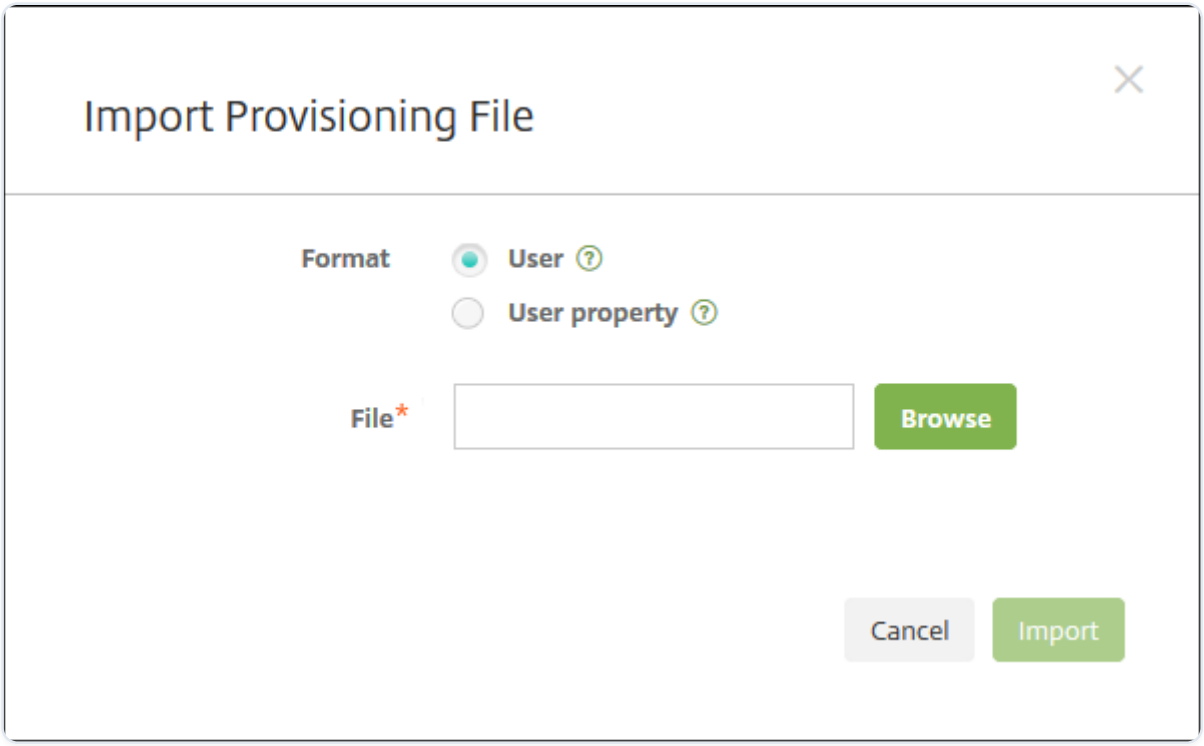
Puede importar cuentas de usuario locales y propiedades desde un archivo .csv denominado archivo de aprovisionamiento, que puede crear manualmente. Para obtener más información sobre el formato de los archivos de aprovisionamiento, consulte Formatos de archivo de aprovisionamiento.

Nota:

- Para los usuarios locales, utilice el nombre de dominio junto con el nombre de usuario en el archivo de importación. Por ejemplo, especifique `username@domain`. Si el usuario local que crea o importa es para un dominio administrado en Citrix Endpoint Management, el usuario no puede inscribirse utilizando las credenciales LDAP correspondientes.
- Si importa cuentas de usuario al directorio de usuarios interno de Citrix Endpoint Management, inhabilite el dominio predeterminado para acelerar el proceso de importación. Tenga en cuenta que la inhabilitación del dominio afecta a las inscripciones. Vuelva a habilitar el dominio predeterminado una vez completada la importación de usuarios internos.
- Los usuarios locales pueden tener el formato de nombre principal de usuario (UPN). Sin embargo, Citrix recomienda que no utilice el dominio administrado. Por ejemplo, si example.com está administrado, no cree un usuario local con este formato UPN: user@example.com.

Después de preparar un archivo de aprovisionamiento, siga estos pasos para importarlo a Citrix Endpoint Management.

1. En la consola de Citrix Endpoint Management, haga clic en **Administrar > Usuarios**. Aparecerá la página **Usuarios**.
2. Haga clic en **Importar usuarios locales**. Aparecerá el cuadro de diálogo **Importar archivo de aprovisionamiento**.



3. Seleccione **Usuario** o **Propiedad** para el formato del archivo de aprovisionamiento que va a importar.
4. Seleccione el archivo de aprovisionamiento que desea utilizar haciendo clic en **Examinar** y, a continuación, navegando hasta la ubicación del archivo.
5. Haga clic en **Importar**.

Formatos de archivo de aprovisionamiento

Puede crear un archivo de aprovisionamiento y utilizarlo para importar cuentas de usuario y propiedades a Citrix Endpoint Management. Utilice uno de los siguientes formatos para un archivo de aprovisionamiento:

- **Campos del archivo de aprovisionamiento de usuarios:** `user;password;role;group1;group2`
- **Campos del archivo de aprovisionamiento de atributos de usuario:** `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

Nota:

- Separe los campos dentro del archivo de aprovisionamiento con un punto y coma (;). Si parte de un campo tiene un punto y coma, escápelo con una barra invertida (\). Por ejemplo, escriba la propiedad **propertyV; test;1;2** como **propertyV\;test\;1\;2** en el archivo de aprovisionamiento.
- Los valores válidos para **Rol** son los roles predefinidos USER, ADMIN, SUPPORT y DEVICE_PROVISIONING, además de cualquier otro rol que haya definido.
- Utilice el carácter de punto (.) como separador para crear una jerarquía de grupos. No utilice un punto en los nombres de los grupos.
- Utilice minúsculas para los atributos de propiedad en los archivos de aprovisionamiento de atributos. La base de datos distingue entre mayúsculas y minúsculas.

Ejemplo de contenido de aprovisionamiento de usuarios

La entrada `user01;pwd\ \;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` significa:

- **Usuario:** user01
- **Contraseña:** pwd; 01
- **Rol:** USER
- **Grupos:**
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

Como otro ejemplo, `AUser0;1.password;USER;ActiveDirectory.test.net` significa:

- **Usuario:** AUser0
- **Contraseña:** 1.password
- **Rol:** USER
- **Grupo:** ActiveDirectory.test.net

Ejemplo de contenido de aprovisionamiento de atributos de usuario

La entrada `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` significa:

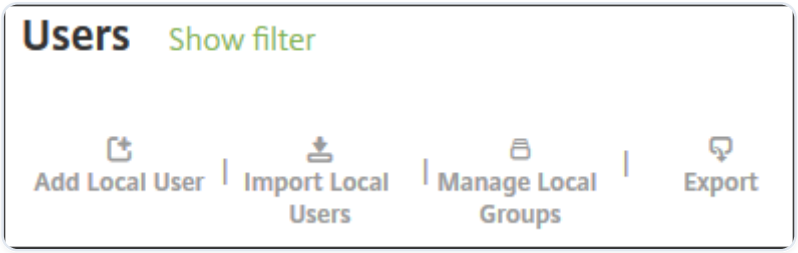
- **Usuario:** user01
- **Propiedad 1**
  - **nombre:** propertyN
  - **valor:** propertyV;test;1;2
- **Propiedad 2:**
  - **nombre:** prop 2
  - **valor:** prop2 value

Agregar o quitar grupos

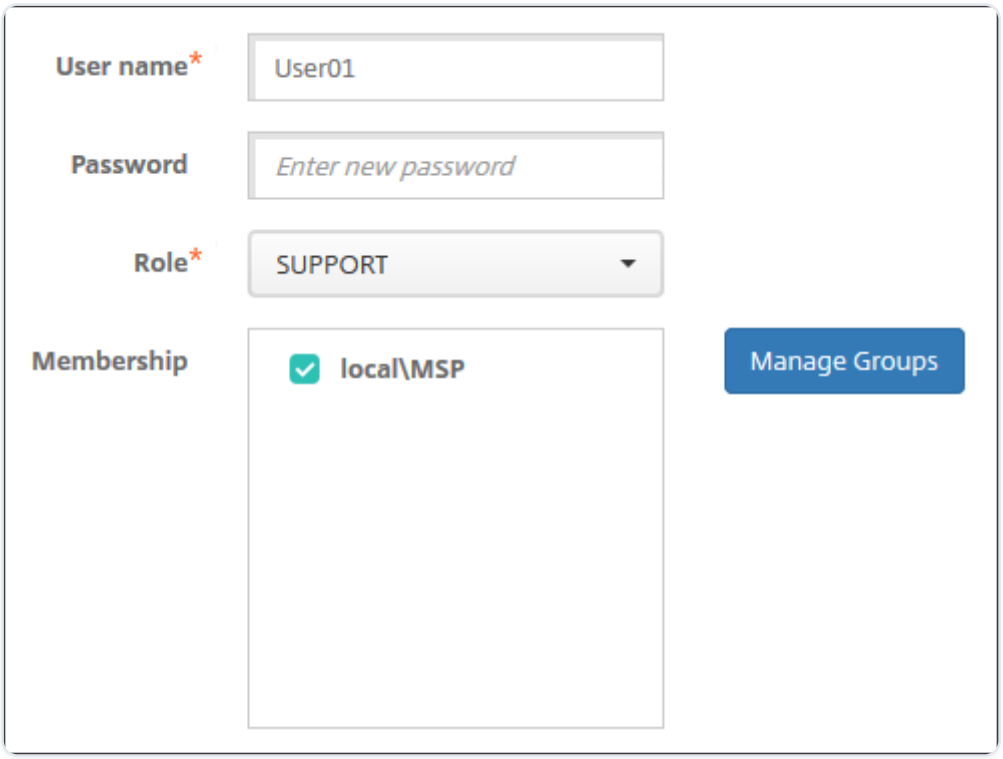
Los grupos se administran en el cuadro de diálogo **Administrar grupos** de la consola de Citrix Endpoint Management en estas páginas: **Usuarios**, **Agregar usuario local** o **Modificar usuario local**. No hay ningún comando para modificar grupos.

Para agregar un grupo local

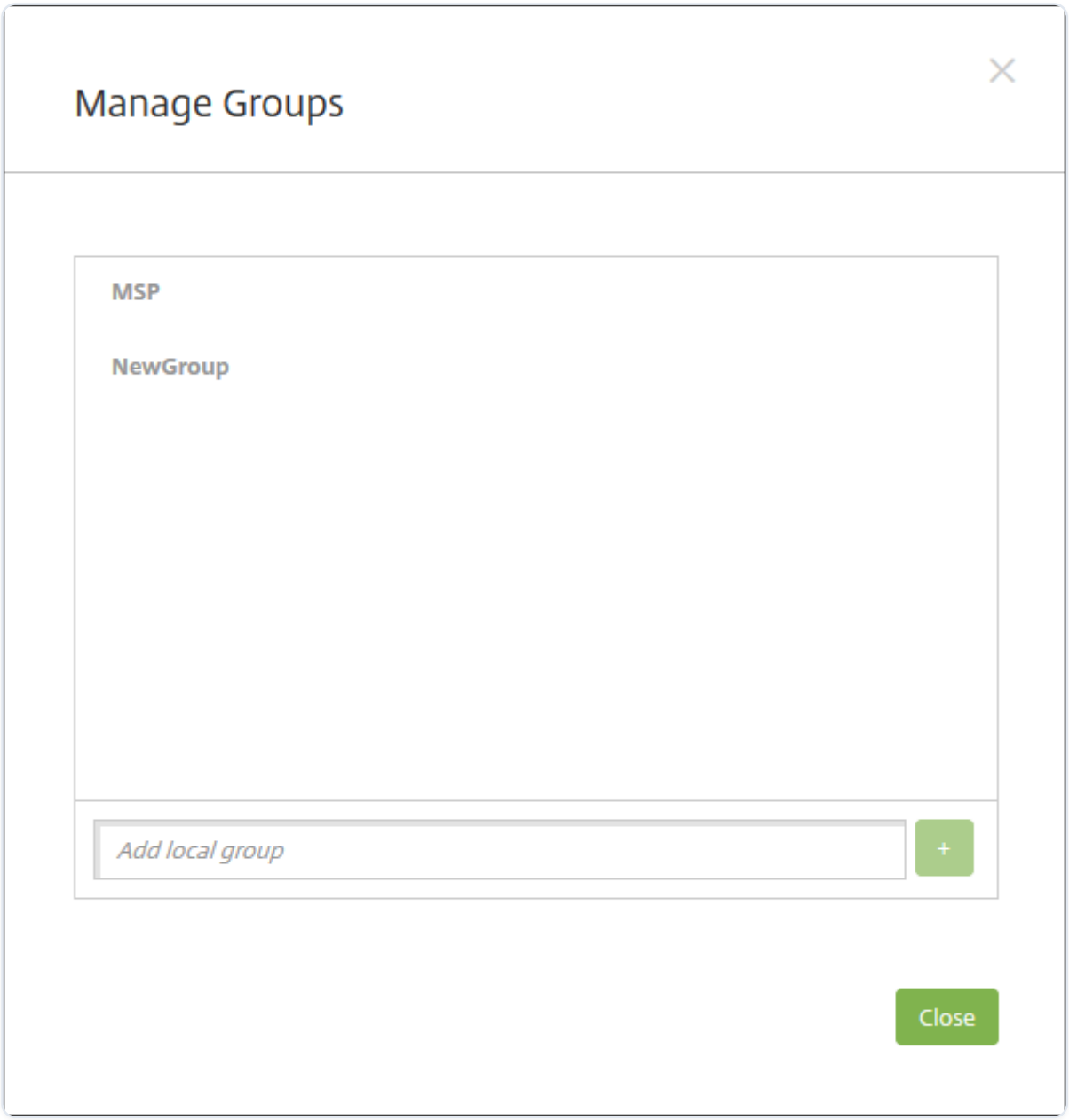
1. Realice una de las siguientes acciones:
   - En la página **Usuarios**, haga clic en **Administrar grupos locales**.



   - En la página **Agregar usuario local** o en la página **Modificar usuario local**, haga clic en **Administrar grupos**.



Aparece el cuadro de diálogo **Administrar grupo**.



2. Debajo de la lista de grupos, escriba un nuevo nombre de grupo y, a continuación, haga clic en el signo más (**+**). El grupo de usuarios se agrega a la lista.
3. Haga clic en **Cerrar**.

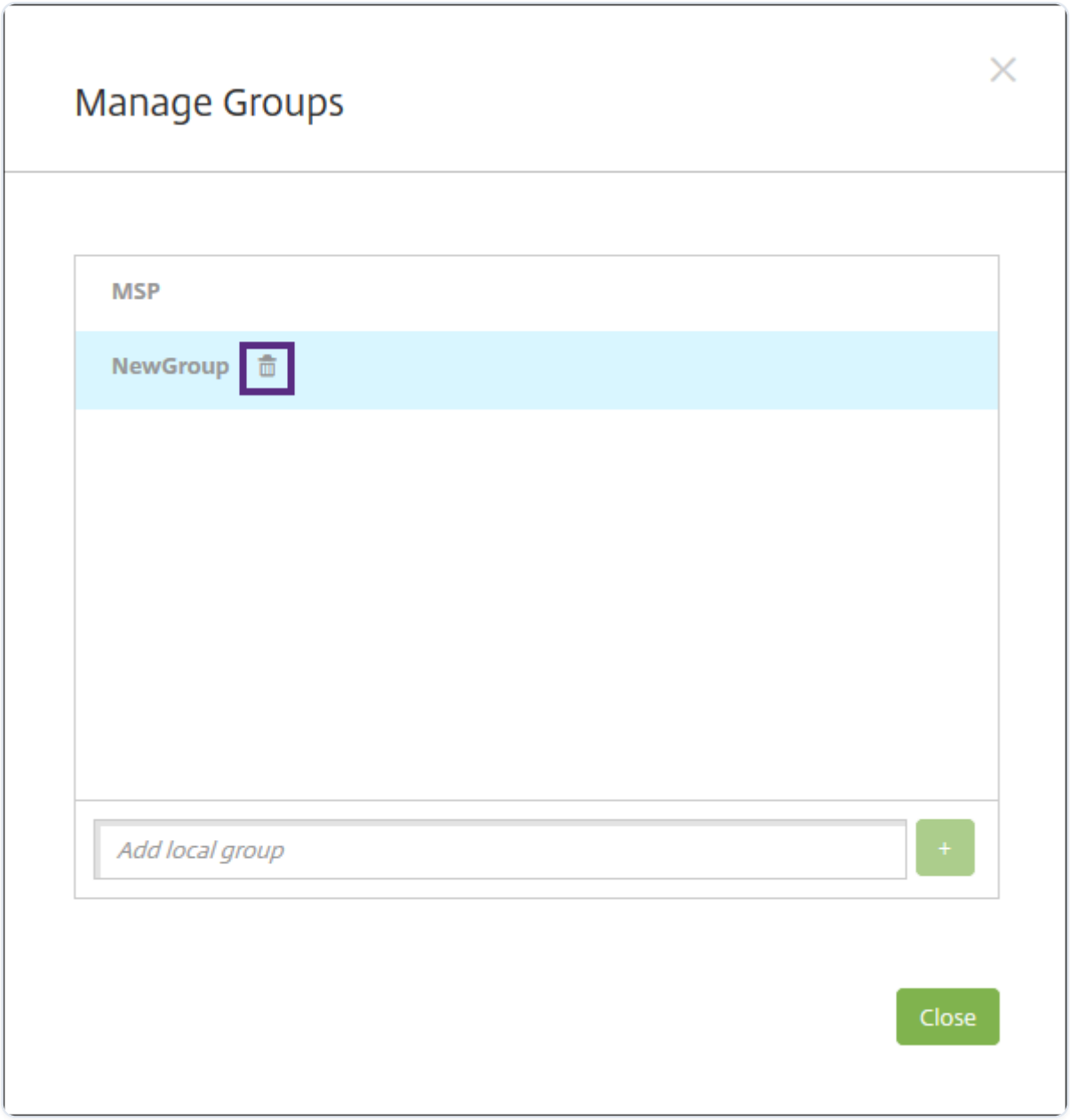
Para eliminar un grupo

La eliminación de un grupo no afecta a las cuentas de usuario. En su lugar, la eliminación de un grupo solo elimina la asociación del usuario con ese grupo. Los usuarios también pierden el acceso a las aplicaciones o perfiles proporcionados por los grupos de entrega asociados a ese grupo. Sin embargo, cualquier otra asociación de grupo permanece intacta. Si los usuarios no están asociados a ningún otro grupo local, se asocian en el nivel superior.

1. Realice una de las siguientes acciones:

- En la página **Usuarios**, haga clic en **Administrar grupos locales**.
- En la página **Agregar usuario local** o en la página **Modificar usuario local**, haga clic en **Administrar grupos**.

Aparece el cuadro de diálogo **Administrar grupos**.



2. En el cuadro de diálogo **Administrar grupos**, haga clic en el grupo que desea eliminar.
3. Haga clic en el icono de la papelera a la derecha del nombre del grupo. Aparece un cuadro de diálogo de confirmación.
4. Haga clic en **Eliminar** para confirmar la operación y eliminar el grupo.

> **Importante:**

> No puede deshacer esta operación.

5. En el cuadro de diálogo **Administrar grupos**, haga clic en **Cerrar**.

Crear y administrar flujos de trabajo

Puede usar flujos de trabajo para administrar la creación y eliminación de cuentas de usuario. Antes de crear un flujo de trabajo, identifique a las personas de su organización que tienen autoridad para aprobar las solicitudes de cuentas de usuario. Luego, use la plantilla de flujo de trabajo para crear y aprobar solicitudes de cuentas de usuario.

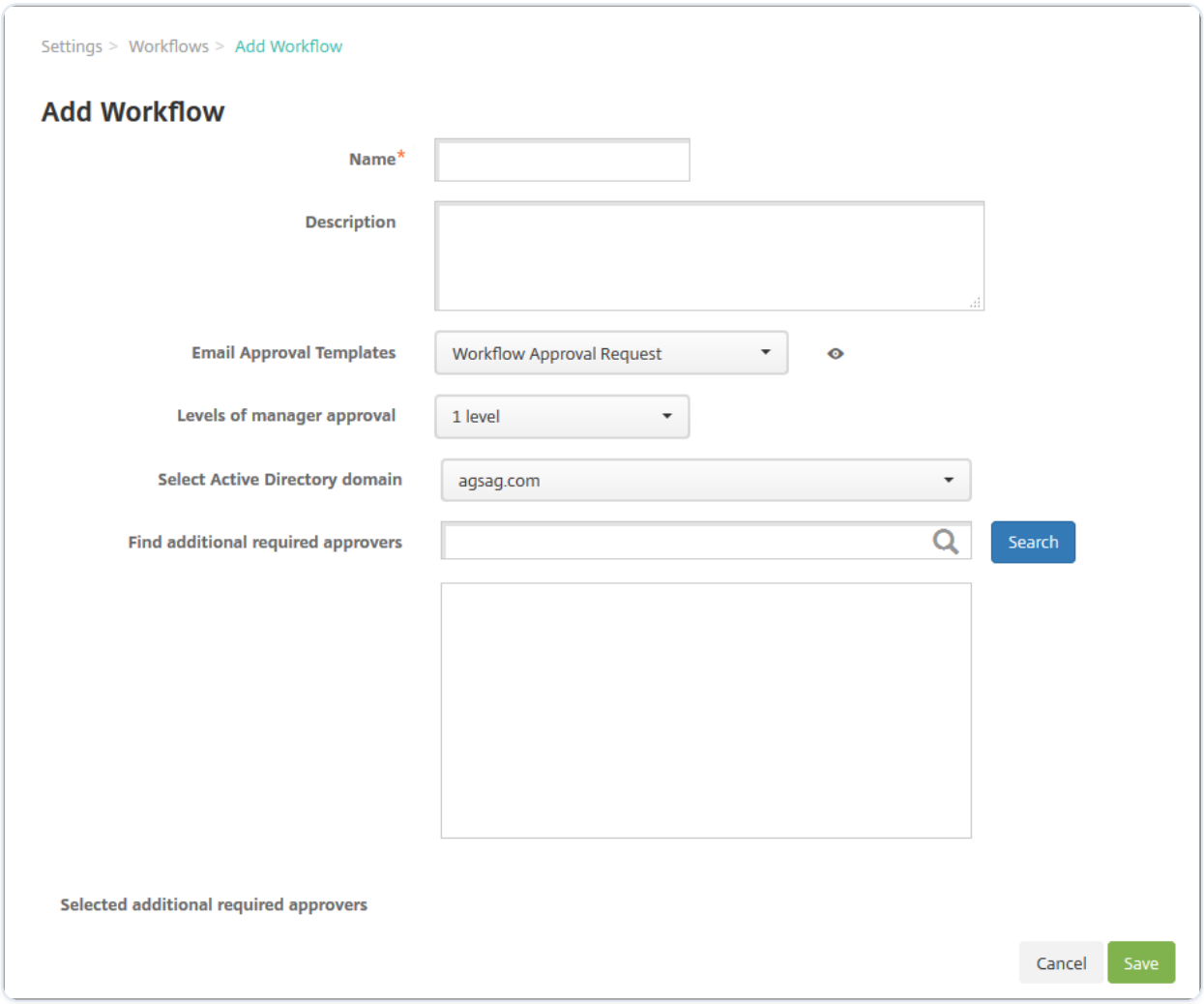
Cuando configura Citrix Endpoint Management por primera vez, configura los ajustes de correo electrónico del flujo de trabajo, que deben establecerse antes de poder usar los flujos de trabajo. Puede cambiar los ajustes de correo electrónico del flujo de trabajo en cualquier momento. Estos ajustes incluyen el servidor de correo electrónico, el puerto, la dirección de correo electrónico y si la solicitud para crear la cuenta de usuario requiere aprobación.

Puede configurar flujos de trabajo en dos lugares de Citrix Endpoint Management:

- En la página **Parámetros > Flujos de trabajo** de la consola de Citrix Endpoint Management. En la página **Flujos de trabajo**, puede configurar varios flujos de trabajo para usarlos con las configuraciones de aplicaciones. Cuando configura flujos de trabajo en la página Flujos de trabajo, puede seleccionar el flujo de trabajo al configurar la aplicación.
- Cuando configure un conector de aplicación en la aplicación, proporcione un nombre de flujo de trabajo y, a continuación, configure las personas que aprobarán la solicitud de cuenta de usuario. Consulte Agregar aplicaciones.

Puede asignar hasta tres niveles para la aprobación de cuentas de usuario por parte del administrador. Si necesita que otras personas aprueben la cuenta de usuario, puede buscarlas y seleccionarlas por su nombre o dirección de correo electrónico. Cuando Citrix Endpoint Management encuentra a la persona, la agrega al flujo de trabajo. Todas las personas del flujo de trabajo reciben correos electrónicos para aprobar o denegar la nueva cuenta de usuario.

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha de la consola. Aparece la página **Parámetros**.
2. Haga clic en **Flujos de trabajo**. Aparece la página **Flujos de trabajo**.
3. Haga clic en **Agregar**. Aparece la página **Agregar flujo de trabajo**.



4. Configure los siguientes parámetros:

- **Nombre:** Escriba un nombre único para el flujo de trabajo.
- **Descripción:** Opcionalmente, escriba una descripción para el flujo de trabajo.
- **Plantillas de aprobación de correo electrónico:** En la lista, seleccione la plantilla de aprobación de correo electrónico que se va a asignar. Las plantillas de correo electrónico se crean en la sección **Plantillas de notificación** en **Configuración** de la consola de Citrix Endpoint Management. Al hacer clic en el icono del ojo a la derecha de este campo, verá una vista previa de la plantilla que está configurando.
- **Niveles de aprobación del administrador:** En la lista, seleccione el número de niveles de aprobación del administrador necesarios para este flujo de trabajo. El valor predeterminado es **1 nivel**. Las opciones posibles son:
  - No es necesario
  - 1 nivel
  - 2 niveles

    - 3 niveles

- **Seleccionar dominio de Active Directory:** En la lista, seleccione el dominio de Active Directory apropiado que se utilizará para el flujo de trabajo.
- **Buscar aprobadores adicionales obligatorios:** Escriba un nombre en el campo de búsqueda y, a continuación, haga clic en **Buscar**. Los nombres provienen de Active Directory.
- Cuando el nombre aparezca en el campo, marque la casilla de verificación junto al nombre. El nombre y la dirección de correo electrónico aparecerán en la lista **Aprobadores adicionales obligatorios seleccionados**.

    - Para quitar un nombre de la lista, realice una de las siguientes acciones:

        - Haga clic en **Buscar** para ver una lista de todos los usuarios del dominio seleccionado.
        - Escriba un nombre completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Buscar** para limitar los resultados de la búsqueda.
        - Las personas de la lista **Aprobadores adicionales obligatorios seleccionados** tienen marcas de verificación junto a su nombre en la lista de resultados de búsqueda. Desplácese por la lista y desactive la casilla de verificación junto a cada nombre que desee eliminar.

5. Haga clic en **Guardar**. El flujo de trabajo creado aparece en la página **Flujos de trabajo**.

Después de crear el flujo de trabajo, puede ver sus detalles, las aplicaciones asociadas a él o eliminarlo. No puede editar un flujo de trabajo después de crearlo. Si necesita uno con diferentes niveles de aprobación o aprobadores, cree otro.

Para ver los detalles y eliminar un flujo de trabajo

1. En la página **Flujos de trabajo**, en la lista de flujos de trabajo existentes, seleccione un flujo de trabajo específico. Para ello, haga clic en la fila de la tabla o seleccione la casilla de verificación junto al flujo de trabajo.
2. Para eliminar un flujo de trabajo, haga clic en **Eliminar**. Aparece un cuadro de diálogo de confirmación. Vuelva a hacer clic en **Eliminar**.

> **Importante:**

> No puede deshacer esta operación.

Perfiles de inscripción

Un perfil de inscripción especifica lo siguiente:

- Opciones de inscripción de administración de dispositivos para dispositivos Android, iOS y Windows.
- Opciones de inscripción de administración de aplicaciones para dispositivos Android e iOS.
- Otras opciones de inscripción:
  - Si se debe limitar el número de dispositivos que un usuario puede inscribir.

    Si se alcanza el límite de dispositivos, un mensaje de error informa al usuario de que ha superado el límite de registro de dispositivos.
  - Si se debe permitir que un usuario rechace la administración de dispositivos.

Puede usar perfiles de inscripción para combinar varios casos de uso y rutas de migración de dispositivos en una única consola de Citrix Endpoint Management. Algunos casos de uso incluyen:

- Administración de dispositivos móviles (solo MDM)
- MDM+Administración de aplicaciones móviles (MAM)
- Solo MAM
- Inscripciones de propiedad corporativa
- Inscripción BYOD (la capacidad de no participar en la inscripción MDM)
- Migración de inscripciones de Administrador de dispositivos Android a inscripciones de Android Enterprise (totalmente administrado, perfil de trabajo, dispositivo dedicado)
- Inscripción automática de dispositivos Windows 10 y Windows 11 a través de la aplicación Citrix Workspace para Windows (vista previa)

Si su sitio actual es solo MDM y quiere agregar MAM, debe configurar un NetScaler Gateway. Para obtener más información, consulte Requisitos de NetScaler Gateway.

Al crear un grupo de entrega, puede usar el perfil de inscripción predeterminado llamado Global o especificar un perfil de inscripción diferente.

Las funciones del perfil de inscripción por plataforma incluyen las siguientes.

- **Para dispositivos Android:** Se especifica el modo de administración y de propietario del dispositivo. Por ejemplo: Dispositivo propiedad de la empresa, totalmente administrado con perfil de trabajo y perfil de trabajo BYOD.

  Los dispositivos nuevos se inscriben en Android Enterprise de forma predeterminada. Puede optar por administrar los dispositivos mediante el modo de administrador de dispositivos Android (DA) heredado. Los dispositivos nuevos también se inscriben en la administración de aplicaciones de forma predeterminada.

  Para obtener información sobre cómo especificar el nivel de seguridad y los pasos de inscripción necesarios, consulte Cuentas de usuario, roles e inscripción.
- **Para dispositivos iOS:** Se especifica el tipo de administración de dispositivos: **Inscripción de usuario de Apple**, **Inscripción de dispositivos Apple** o **No administrar dispositivos**. Este modo de **Inscripción de usuario de Apple** está disponible como vista previa pública. Para habilitar esta función, póngase en contacto con su equipo de soporte.

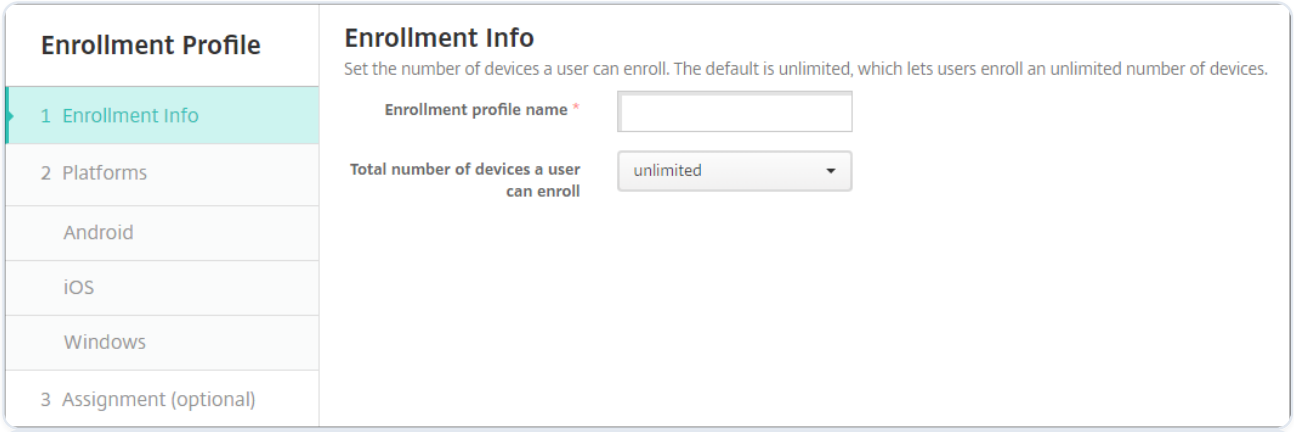
  Si selecciona Inscripción de usuario de Apple, puede optar por usar un dominio personalizado para los ID de Apple administrados y configurar ese dominio.

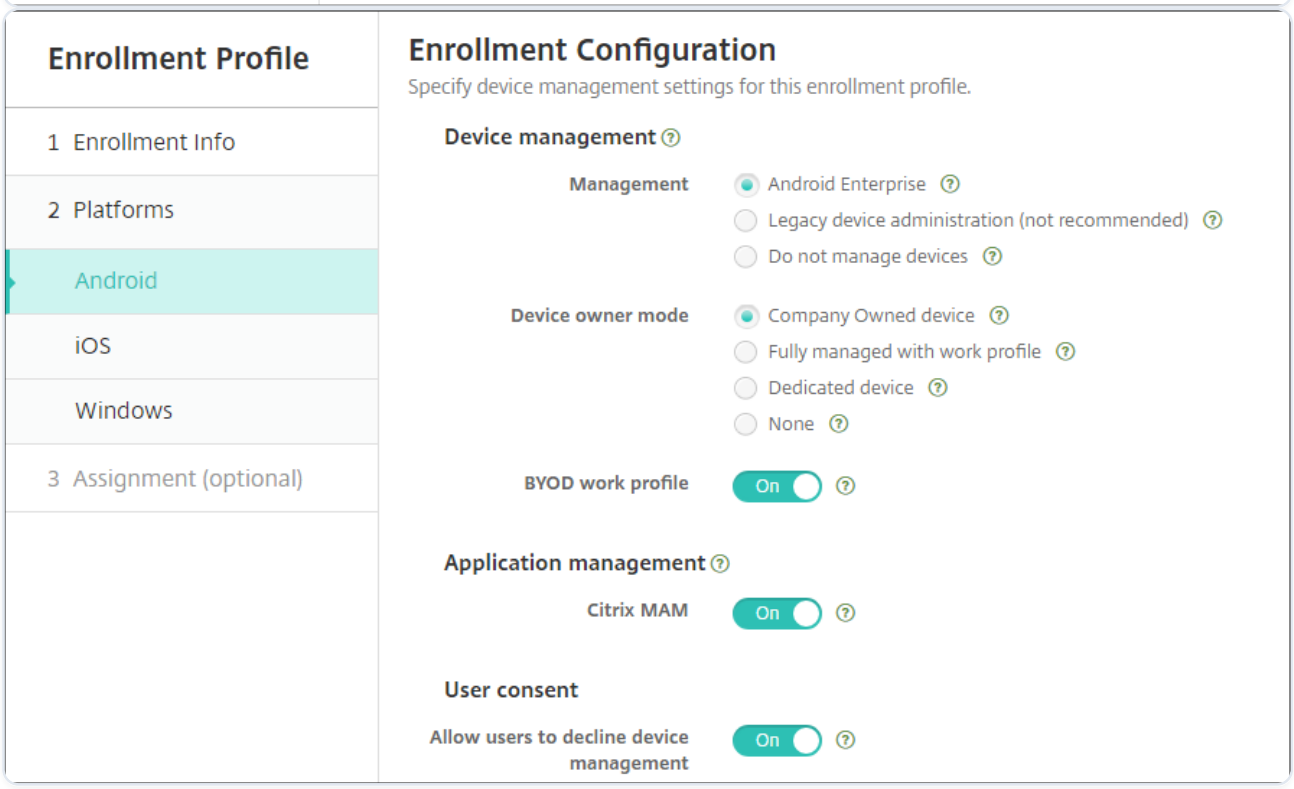
  Los dispositivos nuevos se inscriben en la administración de dispositivos Apple de forma predeterminada. Los dispositivos nuevos también se inscriben en la administración de aplicaciones de forma predeterminada.
- **Para dispositivos Windows 10 y Windows 11:** Se especifica si se debe usar la administración de dispositivos Citrix® para Windows. Los dispositivos nuevos se inscriben en la administración de dispositivos de forma predeterminada.

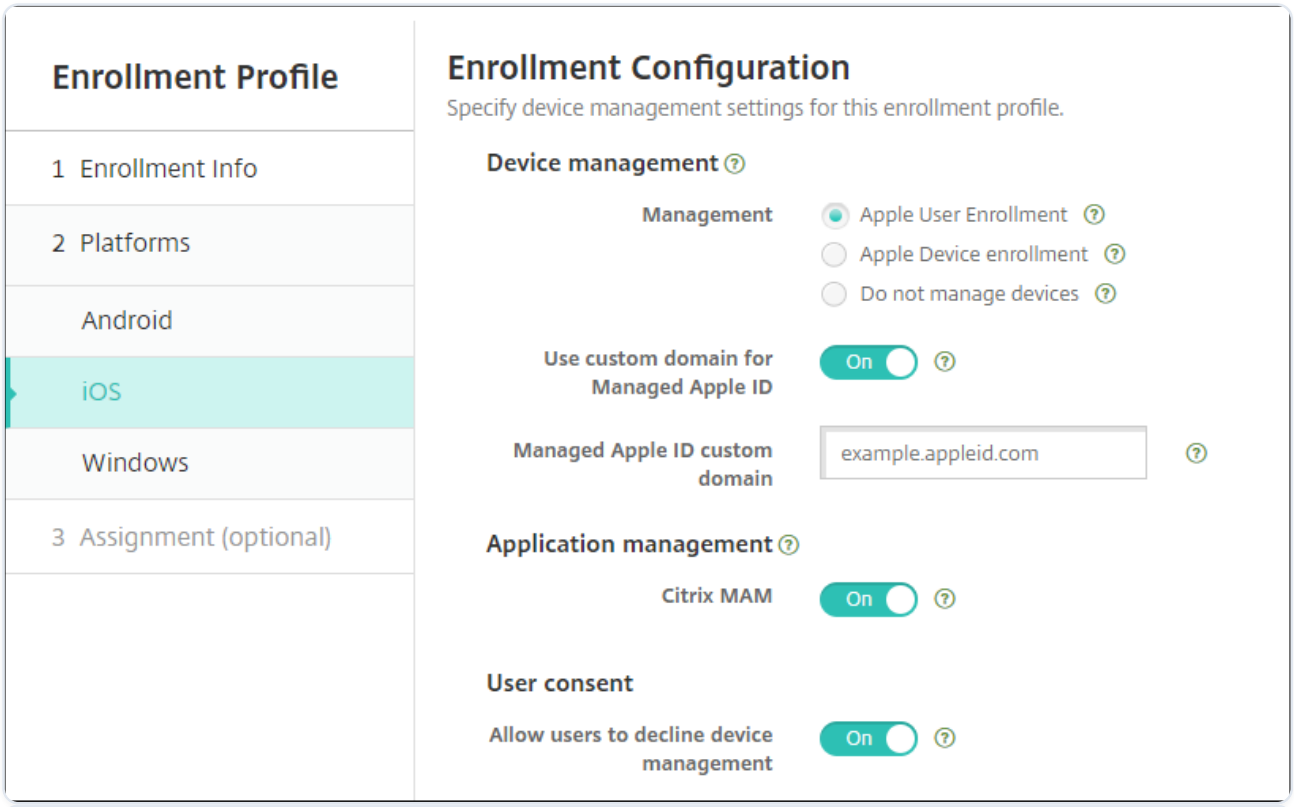
Perfil de inscripción global

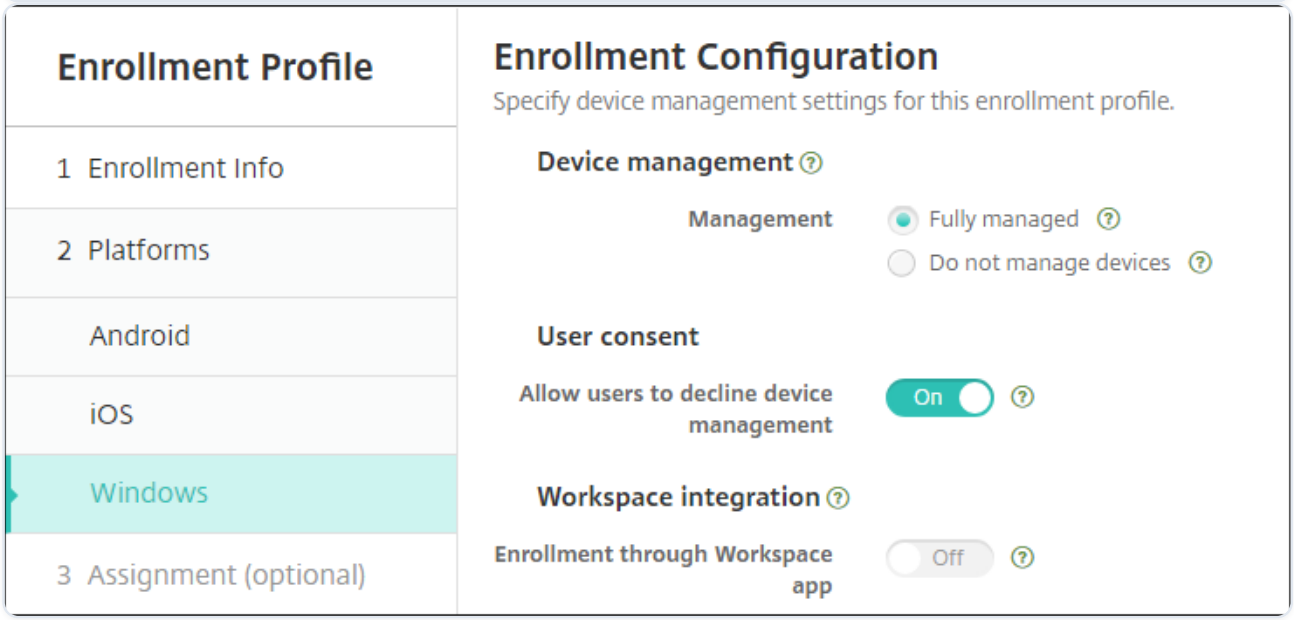
El perfil de inscripción predeterminado se llama Global. El perfil Global es útil para realizar pruebas hasta que tenga la oportunidad de crear perfiles de inscripción.

Si se incorpora a Citrix Endpoint Management 20.2.1 o posterior, el perfil de inscripción Global tiene configuraciones predefinidas. Las siguientes capturas de pantalla muestran la configuración predeterminada para el perfil de inscripción Global. Las implementaciones solo de MAM muestran un subconjunto de estas opciones.


Enrollment Profile
1 Enrollment Info
2 Platforms
Android
iOS
Windows
3 Assignment (optional)
Enrollment Info
Set the number of devices a user can enroll. The default is unlimited, which lets users enroll an unlimited number of devices.
Enrollment profile name *
Total number of devices a user can enroll
unlimited


Enrollment Profile
1 Enrollment Info
2 Platforms
Android
iOS
Windows
3 Assignment (optional)
Enrollment Configuration
Specify device management settings for this enrollment profile.
Device management
Management
Android Enterprise
Legacy device administration (not recommended)
Do not manage devices
Device owner mode
Company Owned device
Fully managed with work profile
Dedicated device
None
BYOD work profile
On
Application management
Citrix MAM
On
User consent
Allow users to decline device management
On





Perfiles de inscripción, grupos de entrega e inscripción

Los perfiles de inscripción y los grupos de entrega interactúan de la siguiente manera:

- Puede adjuntar un perfil de inscripción a uno o varios grupos de entrega.
- Si un usuario pertenece a varios grupos de entrega que tienen diferentes perfiles de inscripción, el nombre del grupo de entrega determina el perfil de inscripción utilizado. Citrix Endpoint Management selecciona el grupo de entrega que aparece en último lugar en una lista alfabética de grupos de entrega. Por ejemplo, supongamos que tiene lo siguiente:

  - Dos perfiles de inscripción, denominados "EP1" y "EP2".
  - Dos grupos de entrega, denominados "DG1" y "DG2".
  - "DG1" está asociado a "EP1".
  - "DG2" está asociado a "EP2".

  Si el usuario que se inscribe está en los grupos de entrega "DG1" y "DG2", Citrix Endpoint Management utiliza el perfil de inscripción "EP2" para determinar el tipo de inscripción del usuario.

- El orden de implementación se aplica solo a los dispositivos de un grupo de entrega que tiene un perfil de inscripción configurado para MDM (administración de dispositivos).
- Después de que un dispositivo se inscribe, algunos cambios en un perfil de inscripción requieren una nueva inscripción:
  - Cambiar la configuración para degradar un dispositivo de la inscripción MDM+MAM a MAM o MDM. Una degradación puede ocurrir al actualizar un perfil de inscripción o mover un dispositivo a un grupo de entrega diferente.
  - Adición de MAM a un perfil de inscripción configurado para MDM.
  - Adición de MDM a un perfil de inscripción configurado para MAM.
- Cambiar a un perfil de inscripción diferente no afecta a los dispositivos inscritos existentes. Sin embargo, los usuarios deben anular la inscripción y volver a inscribir esos dispositivos para que los cambios surtan efecto.

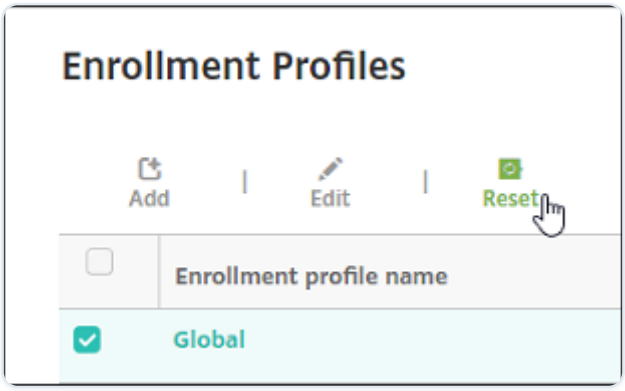
Para crear un perfil de inscripción

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Perfiles de inscripción**.
2. En la página **Información de inscripción**, escriba un nombre descriptivo para el perfil. De forma predeterminada, un usuario puede inscribir un número ilimitado de dispositivos. Seleccione un valor para limitar el número de dispositivos por usuario. El límite se aplica a la suma de dispositivos Android, iOS y Windows administrados por MAM o MDM que un usuario inscribe.
3. Complete las páginas de la plataforma. Para obtener información sobre la configuración de inscripción específica de las plataformas, consulte:
   - Android Enterprise: Crear perfiles de inscripción
   - iOS: Métodos de inscripción admitidos
   - Windows de escritorio y tableta: Métodos de inscripción admitidos

4. En la página **Asignaciones**, adjunte uno o varios grupos de entrega al perfil de inscripción.

   Un usuario puede pertenecer a varios grupos de entrega que tienen diferentes perfiles de inscripción. En ese caso, el nombre del grupo de entrega determina el perfil de inscripción utilizado. Citrix Endpoint Management selecciona el grupo de entrega que aparece en último lugar en una lista alfabética de grupos de entrega. Para crear grupos de entrega, vaya a **Configurar > Grupos de entrega**.

Una lista de sus perfiles de inscripción aparece en la página **Configurar > Perfiles de inscripción**. Para editar el perfil global o restablecerlo a la configuración predeterminada original, seleccione la fila del perfil global y haga clic en **Restablecer**. No se puede eliminar el perfil global.



Notificaciones

Puede usar las notificaciones en Citrix Endpoint Management para los siguientes fines:

- Para comunicarse con grupos de usuarios seleccionados para varias funciones relacionadas con el sistema. También puede dirigir estas notificaciones a determinados usuarios. Por ejemplo, todos los usuarios con dispositivos iOS, usuarios cuyos dispositivos no cumplen las normas, usuarios con dispositivos propiedad de los empleados, etc.
- Para inscribir a los usuarios y sus dispositivos
- Para notificar automáticamente a los usuarios (mediante acciones automatizadas) cuando se cumplen determinadas condiciones. Por ejemplo:
  - Cuando un dispositivo de usuario está a punto de ser bloqueado del dominio corporativo debido a un problema de cumplimiento
  - Cuando un dispositivo ha sido liberado (jailbreak) o rooteado

Para obtener más información sobre las acciones automatizadas, consulte Acciones automatizadas.

Para enviar notificaciones con Citrix Endpoint Management, debe configurar una puerta de enlace y un servidor de notificaciones. Puede configurar un servidor de notificaciones en Citrix Endpoint Management para configurar servidores SMTP. Esos servidores envían notificaciones por correo electrónico a los usuarios. Puede usar las notificaciones para enviar mensajes a través de SMTP.

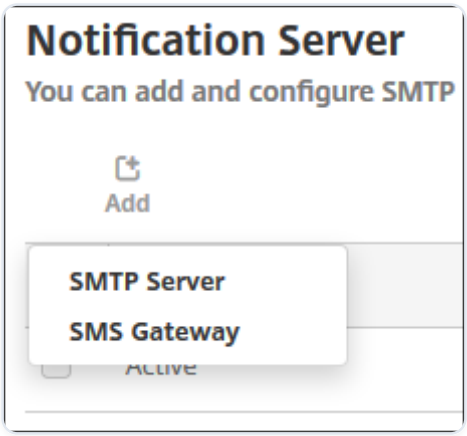
- SMTP es un protocolo orientado a la conexión y basado en texto en el que un remitente de correo se comunica con un receptor de correo. El remitente de correo emite cadenas de comandos y proporciona los datos necesarios, normalmente a través de una conexión TCP. Las sesiones SMTP consisten en comandos originados por un cliente SMTP (la persona que envía el mensaje) y las respuestas correspondientes del servidor SMTP.

Requisitos previos

- Configure el servidor de notificaciones SMTP para enviar mensajes a los usuarios. Si el servidor está alojado en un servidor interno, póngase en contacto con el administrador del sistema para obtener información de configuración. Si el servidor es un servicio de correo electrónico alojado, busque la información de configuración adecuada en el sitio web del proveedor de servicios.
- Solo puede usar un servidor SMTP activo. Este canal de comunicación solo permite una configuración activa.
- Abra el puerto 25 desde Citrix Endpoint Management en la DMZ de su red para que apunte de nuevo al servidor SMTP de su red interna. Esto permite que Citrix Endpoint Management envíe notificaciones correctamente.

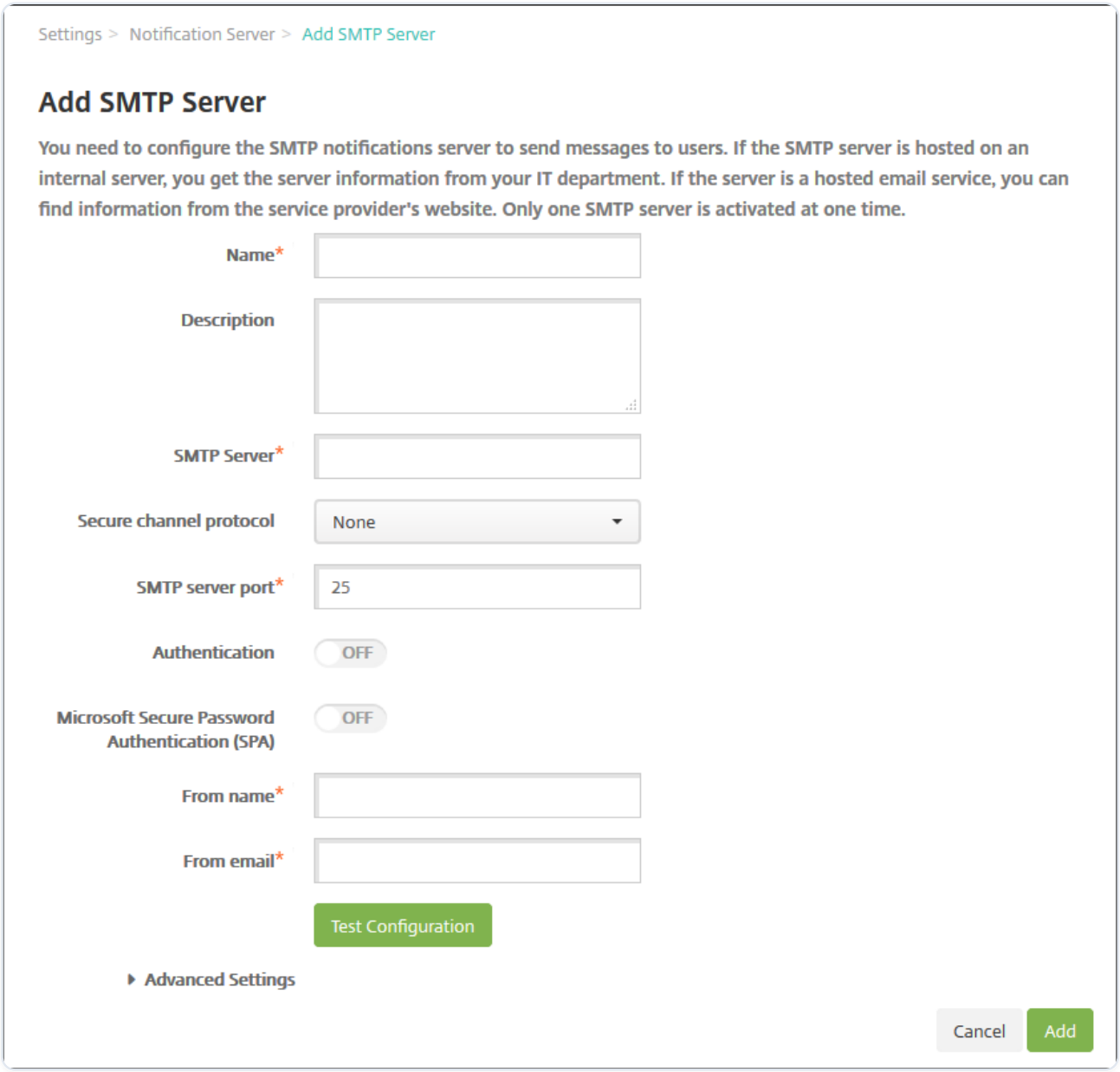
Configurar un servidor SMTP

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha de la consola. Aparece la página de **Configuración**.
2. En **Notificaciones**, haga clic en **Servidor de notificaciones**. Aparece la página **Servidor de notificaciones**.
3. Haga clic en **Agregar**. Aparece un menú con opciones para configurar un servidor SMTP.



- Para agregar un servidor SMTP, haga clic en **Servidor SMTP** y, a continuación, consulte Agregar un servidor SMTP para ver los pasos para configurar este ajuste.

Agregar un servidor SMTP



1. Configure estos ajustes:

   - **Nombre:** Escriba el nombre asociado a esta cuenta de servidor SMTP.
   - **Descripción:** Opcionalmente, introduzca una descripción del servidor.
   - **Servidor SMTP:** Escriba el nombre de host del servidor. Especifique un nombre de dominio completo (FQDN) o una dirección IP.
   - **Protocolo de canal seguro:** Haga clic en **SSL**, **TLS** o **Ninguno** en la lista desplegable para el protocolo de canal seguro utilizado por el servidor (si el servidor está configurado para usar autenticación segura). El valor predeterminado es **Ninguno**.
   - **Puerto del servidor SMTP:** Escriba el puerto utilizado por el servidor SMTP. De forma predeterminada, el puerto está configurado en 25. Si las conexiones SMTP utilizan el protocolo de canal seguro SSL, configure el puerto en 465.
   - **Autenticación:** Seleccione **Activado** o **Desactivado**. El valor predeterminado es **Desactivado**.
   - Si habilita la **Autenticación**, configure estos ajustes:
     - **Nombre de usuario:** Escriba el nombre de usuario para la autenticación
     - **Contraseña:** Escriba la contraseña del usuario de autenticación.

   > **Importante:**
   >
   > Para usar OAuth con Microsoft Exchange Online, primero debe registrar su aplicación en Microsoft Entra ID. Después del registro, habilite **Autenticación** y **Microsoft Exchange Online OAuth 2.0**.

   - Si habilita **Autenticación** y **Microsoft Exchange Online OAuth 2.0**, configure los siguientes ajustes:
     - **Nombre de usuario:** Escriba el nombre de usuario para la autenticación.
     - **ID de inquilino:** Escriba el ID de inquilino de su directorio de Microsoft Entra ID.
     - **ID de cliente:** Escriba el ID de cliente (aplicación) de su aplicación registrada. Puede encontrarlo en Azure portal > su aplicación registrada > **ID de aplicación (cliente)**.
     - **Secreto de cliente:** Escriba el secreto de cliente de su aplicación registrada. Puede encontrarlo en Azure portal > su aplicación registrada > **Certificados y secretos**.

- **Autenticación de contraseña segura de Microsoft (SPA):** Si el servidor SMTP utiliza SPA, haga clic en **Activado**. El valor predeterminado es **Desactivado**.
- **Nombre del remitente:** Escriba el nombre que se muestra en el cuadro **De** cuando un cliente recibe un correo electrónico de notificación de este servidor. Por ejemplo, TI corporativa.
- **Correo electrónico del remitente:** Escriba la dirección de correo electrónico que se utiliza si un destinatario de correo electrónico responde a la notificación enviada por el servidor SMTP.

2. Haga clic en **Probar configuración** para enviar una notificación de correo electrónico de prueba.
3. Expanda **Configuración avanzada** y, a continuación, configure estos ajustes:
   - **Número de reintentos de SMTP:** Escriba el número de veces que se debe reintentar un mensaje fallido enviado desde el servidor SMTP. El valor predeterminado es 5.
   - **Tiempo de espera de SMTP:** Escriba la duración de la espera (en segundos) al enviar una solicitud SMTP. Aumente este valor si el envío de mensajes falla continuamente debido a tiempos de espera agotados. Tenga precaución al disminuir este valor para evitar aumentar el número de mensajes con tiempo de espera agotado y no entregados. El valor predeterminado es de 30 segundos.
   - **Número máximo de destinatarios SMTP:** Escriba el número máximo de destinatarios por mensaje de correo electrónico enviado por el servidor SMTP. El valor predeterminado es 100.
4. Haga clic en **Agregar**.

Crear y actualizar plantillas de notificación

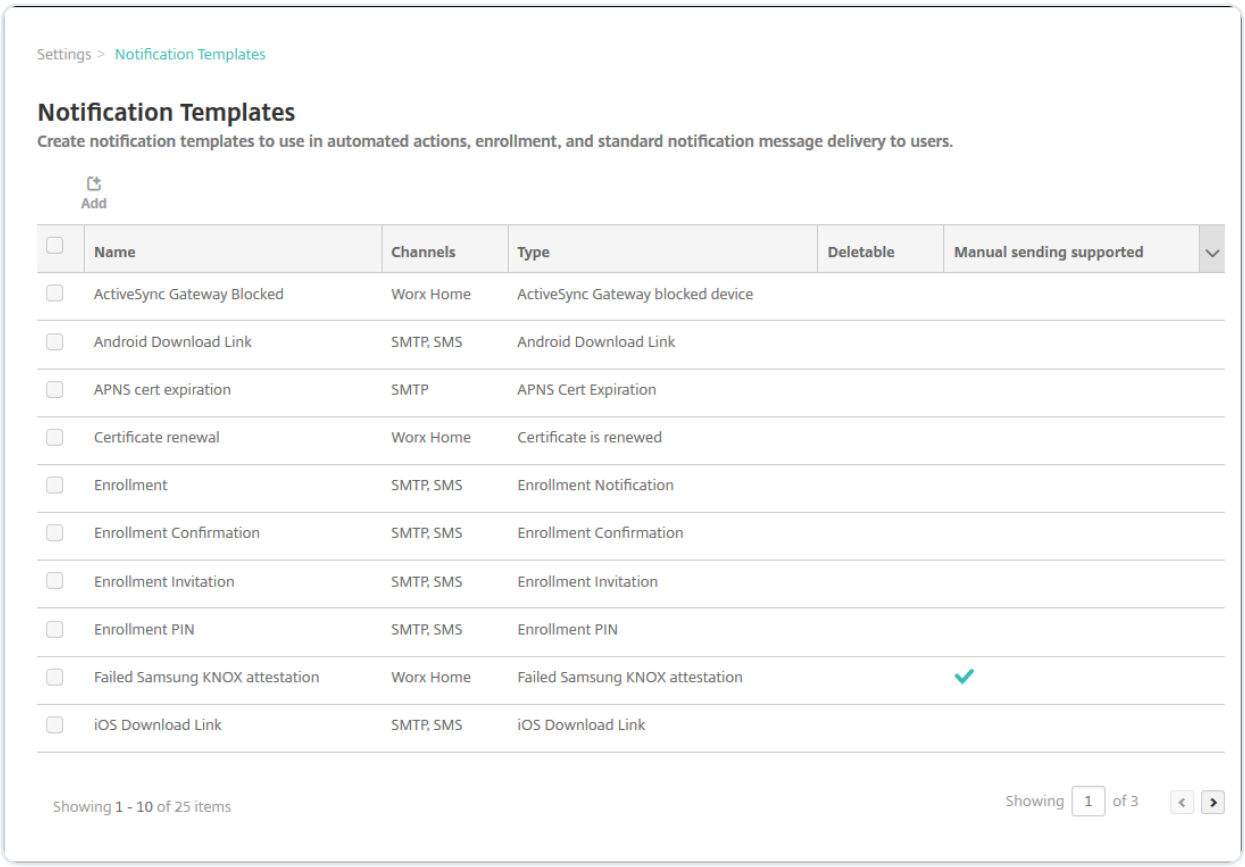
Puede crear o actualizar plantillas de notificación en Citrix Endpoint Management para utilizarlas en acciones automatizadas, inscripciones y mensajes de notificación estándar enviados a los usuarios. Las plantillas de notificación se configuran para enviar mensajes a través de dos canales diferentes: Citrix Secure Hub o SMTP.

Citrix Endpoint Management incluye muchas plantillas de notificación predefinidas. Las plantillas reflejan los distintos tipos de eventos a los que Citrix Endpoint Management responde automáticamente para cada dispositivo del sistema.

> **Nota:**

> Si tiene previsto utilizar canales SMTP para enviar notificaciones a los usuarios, debe configurar los canales antes de poder activarlos. Citrix Endpoint Management le pedirá que configure los canales al agregar plantillas de notificación si aún no están configurados.

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha de la consola. Aparecerá la página **Configuración**.
2. Haga clic en **Plantillas de notificación**. Aparecerá la página **Plantillas de notificación**.



Agregar una plantilla de notificación

1. Haga clic en **Agregar**. Si no hay ningún servidor SMTP configurado, aparecerá un mensaje sobre el uso de las notificaciones SMTP. Puede optar por configurar los servidores SMTP ahora o configurarlos más tarde.

   Si elige configurar los ajustes del servidor SMTP ahora, se le redirigirá a la página **Servidor de notificaciones** en la página **Configuración**. Después de configurar los canales que desea utilizar, puede volver a la página **Plantilla de notificación** para seguir agregando o modificando plantillas de notificación.

   > **Importante:**

> Si elige configurar los ajustes del servidor SMTP más tarde, no podrá activar esos canales al añadir o editar una plantilla de notificación. Como resultado, esos canales no estarán disponibles para enviar notificaciones a los usuarios.

2. Configure estos ajustes:

   - **Nombre:** Escriba un nombre descriptivo para la plantilla.
   - **Descripción:** Escriba una descripción para la plantilla.
   - **Tipo:** Haga clic en el tipo de notificación en la lista desplegable. Solo aparecen los canales admitidos para el tipo seleccionado. Solo se permite una plantilla de caducidad de certificado APNS, que es una plantilla predefinida. No puede añadir una plantilla de este tipo.

   > **Nota:**
   >
   > Para algunos tipos de plantilla, la frase "Envío manual admitido" aparece debajo del tipo. Esos tipos de plantilla están disponibles en la lista **Notificaciones** del **Panel de control** y en la página **Dispositivos**. Desde esas ubicaciones, puede enviar manualmente la notificación a los usuarios. El envío manual no está disponible en ninguna plantilla que utilice las siguientes macros en el campo Asunto o Mensaje de cualquier canal:

   - ${outofcompliance.reason(whitelist_blacklist_apps_name)}
   - ${outofcompliance.reason(smg_block)}

     > **Nota:**
     >
     > La consola de Citrix Endpoint Management incluye los términos "lista negra" y "lista blanca". Cambiaremos esos términos en una próxima versión a "lista de bloqueo" y "lista de permitidos".

3. En **Canales**, configure la información de cada canal que se utilizará con esta notificación. Puede elegir cualquier canal o todos. Los canales que elija dependen de cómo desee enviar las notificaciones:

- Si elige **Citrix Secure Hub**, solo los dispositivos iOS y Android recibirán las notificaciones, que aparecerán en la bandeja de notificaciones del dispositivo.
- Si elige **SMTP**, los usuarios que se inscribieron con su dirección de correo electrónico recibirán el mensaje.

Citrix Secure Hub:

- **Activar:** Haga clic para habilitar el canal de notificaciones.
- **Mensaje:** Escriba el mensaje que se enviará al usuario. Este campo es obligatorio si utiliza Citrix Secure Hub. Para obtener información sobre el uso de macros en un mensaje, consulte Macros.
- **Archivo de sonido:** En la lista, haga clic en el sonido de notificación que el usuario oye cuando se recibe la notificación.

SMTP:

- **Activar:** Haga clic para habilitar el canal de notificaciones.

  Puede activar la notificación SMTP solo después de configurar el servidor SMTP.
- **Remitente:** Escriba un remitente opcional para la notificación, que puede ser un nombre, una dirección de correo electrónico o ambos.
- **Destinatario:** Este campo tiene una macro predefinida para todas las notificaciones, excepto las Ad Hoc, para asegurarse de que las notificaciones se envían a la dirección de destinatario SMTP correcta. Citrix recomienda no modificar las macros en las plantillas. Puede añadir más destinatarios (como un administrador corporativo) añadiendo sus direcciones en este campo. Utilice un punto y coma (;) para separar las macros y otras direcciones. Para enviar notificaciones Ad Hoc, puede introducir destinatarios específicos o seleccionar dispositivos desde la página **Administrar > Dispositivos** y enviar notificaciones desde allí. Para obtener más información, consulte Dispositivos.
- **Asunto:** Escriba un asunto descriptivo para la notificación. Este campo es obligatorio.
- **Mensaje:** Escriba el mensaje que se enviará al usuario. Para obtener información sobre el uso de macros en un mensaje, consulte Macros.

4. Haga clic en **Agregar**. Cuando todos los canales están configurados correctamente, aparecen en este orden en la página **Plantillas de notificación**: SMTP y Citrix Secure Hub. Los canales que no están configurados correctamente aparecen después de los canales configurados correctamente.

Editar una plantilla de notificación

1. Seleccione una plantilla de notificación. Aparece la página de edición específica de esa plantilla. Puede editar la plantilla, excepto el campo **Tipo**, y activar o desactivar canales.
2. Haga clic en **Guardar**.

Eliminar una plantilla de notificación

Solo puede eliminar las plantillas de notificación que haya añadido. No puede eliminar las plantillas de notificación predefinidas.

1. Seleccione una plantilla de notificación existente.
2. Haga clic en **Eliminar**. Aparece un cuadro de diálogo de confirmación.
3. Haga clic en **Eliminar** para eliminar la plantilla de notificación o haga clic en **Cancelar** para anular la eliminación de la plantilla de notificación.

Configurar roles con RBAC

La función de control de acceso basado en roles (RBAC) de Citrix Endpoint Management le permite asignar roles a usuarios y grupos. Los roles son conjuntos de permisos que controlan el nivel de acceso que tienen los usuarios a las funciones del sistema.

Citrix Endpoint Management incluye los siguientes roles de usuario predeterminados. Puede usar los roles predeterminados como plantillas que puede personalizar para crear sus propios roles de usuario.

- **Administrador:** Concede acceso total al sistema.
- **Usuario:** Permite a los usuarios inscribir dispositivos y acceder al portal de autoayuda.

Puede usar la función RBAC en Citrix Endpoint Management para:

- Crear y modificar roles de usuario.
- Asignar roles a grupos de usuarios locales y a grupos de Active Directory (AD).
- Asignar roles a los administradores en Citrix Cloud a través de **Administración de identidades y accesos > Administradores**. Consulte (#add-roles-to-citrix-cloud-administrators).

Usar la función RBAC

Puede asignar roles a usuarios locales, a administradores de la nube (en Citrix Cloud) y a grupos de usuarios locales y grupos de Active Directory.

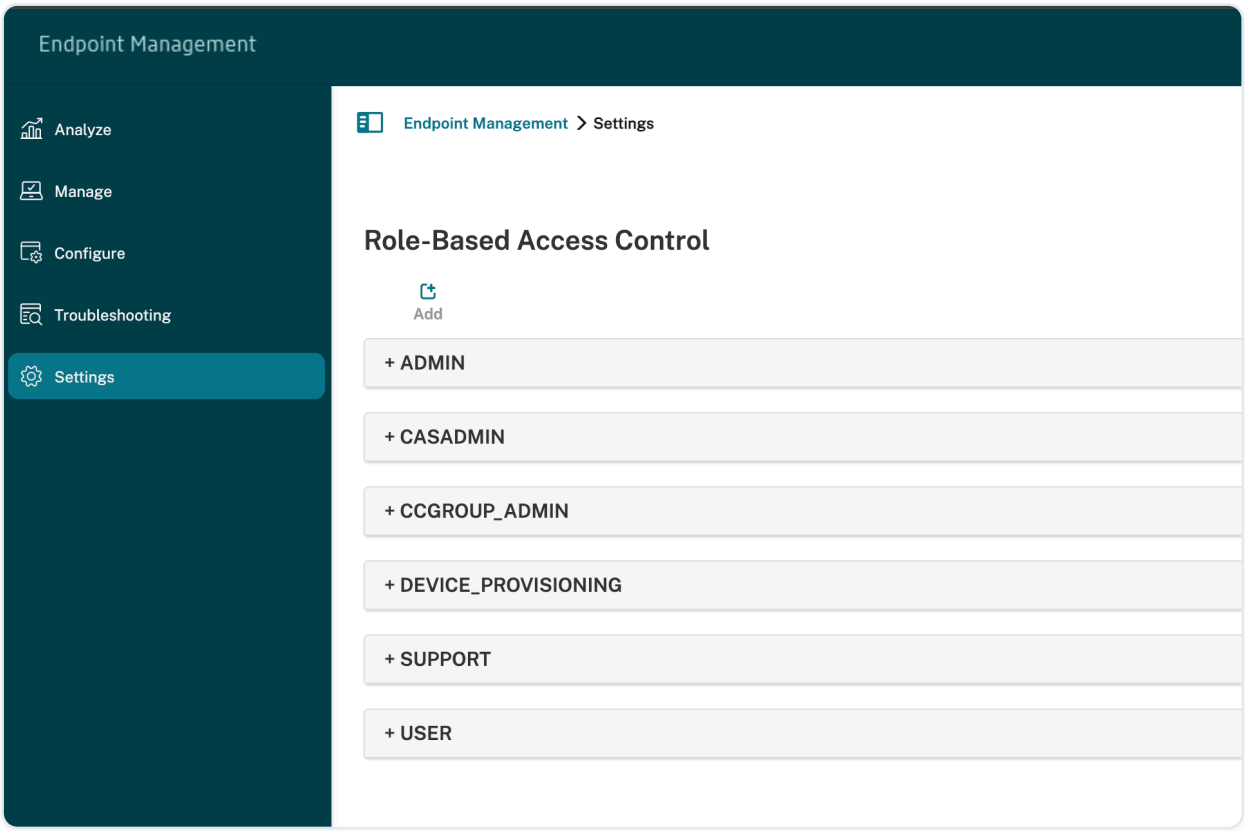
- **Usuarios locales:** Asigne roles a los usuarios locales mediante **Administrar > Usuarios**. Solo puede asignar un rol a los usuarios locales. Para cambiar los roles, puede modificar manualmente la cuenta de usuario. O bien, puede crear un grupo para usuarios locales y asignar un rol a ese grupo.
- **Administradores de la nube:** Un administrador de la nube es una cuenta de usuario especial que Citrix Cloud crea cuando se agrega un administrador a su cuenta de cliente de Citrix Cloud. Una cuenta de administrador de la nube utiliza el mismo nombre de usuario que la cuenta de administrador en Citrix Cloud. Cree roles RBAC en la consola de Citrix Endpoint Management y asigne roles a estos usuarios a través de **Administración de identidades y accesos > Administradores** en Citrix Cloud.
- **Grupos de Active Directory:** Todos los usuarios de un grupo de Active Directory tienen los mismos permisos. Si un usuario pertenece a varios grupos de Active Directory, todos los permisos se fusionan para definir los permisos de ese usuario. Por ejemplo, supongamos que los usuarios de ADGroupA pueden localizar dispositivos de gerentes y los usuarios de ADGroupB pueden borrar dispositivos de empleados. Un usuario que pertenece a ambos grupos puede localizar y borrar los dispositivos de gerentes y empleados. Si un usuario pertenece a grupos con permisos en conflicto, prevalecen los permisos permitidos.

Para obtener más información, consulte Acerca de las cuentas de usuario.

Crear o editar roles

1. En la consola de Citrix Endpoint Management, para acceder a la página **Configuración**, haga clic en el icono de engranaje de la esquina superior derecha.
2. Haga clic en **Control de acceso basado en roles**. La página **Control de acceso basado en roles** muestra los roles de usuario predeterminados y los roles que haya agregado.

   Haga clic en el signo más (+) junto a un rol para ver todos los permisos de ese rol.



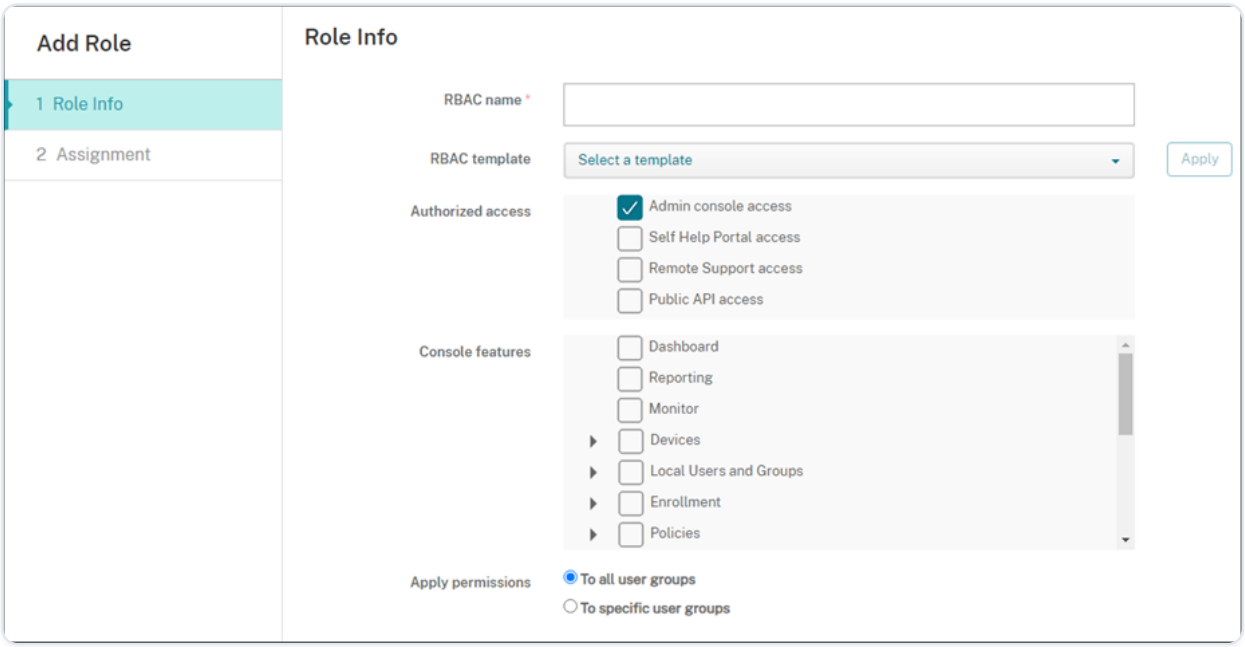
3. Para agregar un rol, haga clic en **Agregar**. O, para editar un rol, haga clic en el lápiz a la derecha de un rol existente.

> **Nota:**
>
> Puede eliminar un rol haciendo clic en el icono de la papelera a la derecha de un rol que haya definido. No puede eliminar los roles de usuario predeterminados.

4. En la página **Agregar rol**, introduzca la siguiente información:

   - **Nombre de RBAC:** Introduzca un nombre descriptivo para el nuevo rol de usuario. No puede cambiar el nombre de un rol existente.
   - **Plantilla de RBAC:** Opcionalmente, seleccione una plantilla como punto de partida para el nuevo rol. (Al editar un rol, no puede seleccionar ni cambiar plantillas). Las plantillas de RBAC son los roles de usuario predeterminados que definen el acceso a las funciones del sistema.

   Haga clic en el botón **Aplicar** para rellenar las casillas de verificación **Acceso autorizado** y **Funciones de la consola**. Citrix Endpoint Management rellena esos campos con el acceso predefinido y los permisos de funciones para la plantilla seleccionada.



5. Para personalizar el rol, seleccione o desactive las casillas de verificación en **Acceso autorizado** y **Funciones de la consola**.

   Haga clic en el triángulo junto a una función de la consola para mostrar y seleccionar los permisos específicos de esa función. Al hacer clic en la casilla de verificación de nivel superior no se seleccionan los permisos individuales. Seleccione las opciones individuales después de expandir el permiso de nivel superior.

6. **Aplicar permisos:** Haga clic en **A grupos de usuarios específicos** para aplicar permisos a los grupos que seleccione.

   Por ejemplo, si un administrador de RBAC tiene permiso para el grupo de usuarios de Active Directory:

   - El administrador solo puede acceder a la información de los usuarios que están en el grupo de Active Directory.
   - El administrador no puede ver ningún otro usuario local o de AD. El administrador puede ver a los usuarios que son miembros de grupos secundarios de cualquiera de esos grupos.
   - El administrador puede enviar invitaciones a:
     - Los grupos de permisos y sus grupos secundarios
     - Los usuarios que son miembros de grupos de permisos y sus grupos secundarios

   Configuración de RBAC de Citrix Endpoint Management(/en-us/citrix-endpoint-management/media/rbac-apply-permissions.png)

7. Haga clic en **Siguiente** e introduzca la siguiente información para asignar el rol a los grupos de usuarios.

   Configuración de RBAC de Citrix Endpoint Management(/en-us/citrix-endpoint-management/media/rbac-assignment-page.png)

   - **Seleccionar dominio:** En la lista, seleccione un dominio.
   - **Buscar grupos de usuarios:** Haga clic en **Buscar** para ver una lista de todos los grupos disponibles. Escriba un nombre de grupo completo o parcial para acotar la búsqueda.
   - **Incluir grupos de usuarios:** En la lista que aparece, seleccione los grupos de usuarios a los que desea asignar el rol.

8. Haga clic en **Guardar**.

Agregar roles a los administradores de Citrix Cloud

En lugar de asignar roles RBAC a los administradores de Citrix Cloud a través de la consola de Citrix Endpoint Management, asigne los roles desde la consola de Citrix Cloud.

1. En la consola de Citrix Cloud, vaya a **Administración de identidades y accesos > Administradores**.
2. Seleccione un proveedor de identidades y, a continuación, escriba una dirección de correo electrónico para añadir un administrador. Haga clic en **Invitar**.

   Haga clic en los **...** al final de una fila de administrador existente para editar esos permisos.
3. Haga clic en **Acceso personalizado**. Al asignar permisos al administrador, puede seleccionar los roles RBAC creados en la consola de Citrix Endpoint Management.

   Roles RBAC en Citrix Cloud(/en-us/citrix-endpoint-management/media/rbac-roles-citrix-cloud.png)
4. Haga clic en **Enviar invitación** para enviar una invitación a un nuevo administrador o haga clic en **Guardar** para terminar de editar un administrador.

Roles predefinidos

Cada rol RBAC predefinido tiene ciertos permisos de acceso y funciones asociados. Las tablas siguientes describen cada uno de los permisos para el rol de administrador y para el rol de usuario. No puede eliminar ni editar los roles predefinidos.

- Para obtener una lista completa de los permisos predeterminados para cada rol integrado, descargue Valores predeterminados de control de acceso basado en roles

- Para obtener información sobre las cuentas de usuario de Citrix Endpoint Management, consulte Acerca de las cuentas de usuario.

Importante:

En el permiso Configuración, el permiso RBAC otorga a los usuarios administradores acceso completo, incluida la capacidad de asignar sus propios permisos. Conceda este acceso solo a los usuarios a los que desee dar la capacidad de manipular todo en el sistema de Citrix Endpoint Management.

Rol de administrador

El rol de administrador predefinido proporciona acceso específico en Citrix Endpoint Management. De forma predeterminada, **Acceso autorizado** (excepto el portal de autoayuda), **Funciones de la consola** y **Aplicar permisos** están habilitados.

Puede cambiar el rol de los usuarios locales a los que se asigna el rol de administrador mediante **Administrar > Usuarios**. Para los usuarios de la nube que tienen el rol de administrador, utilice la consola de Citrix Cloud para cambiar el rol. De forma predeterminada, los usuarios de la nube y locales con el rol de administrador tienen acceso total.

Acceso autorizado para administradores

Acceso a la consola de administración	Los administradores pueden acceder a todas las funciones de la consola de Citrix Endpoint Management.
Acceso al portal de autoayuda	De forma predeterminada, los administradores no pueden acceder al portal de autoayuda. (Los usuarios con el rol de usuario solo pueden acceder al portal de autoayuda).
Acceso a asistencia remota	Los administradores pueden acceder a la función de asistencia remota.
Acceso a la API pública	Los administradores pueden acceder a la API pública para realizar acciones mediante programación que están disponibles en la consola de Citrix Endpoint Management. Las acciones incluyen la administración de

	certificados, aplicaciones, dispositivos, grupos de entrega y usuarios locales.

Funciones de la consola para administradores

Los administradores tienen acceso sin restricciones a la consola de Citrix Endpoint Management.

Panel	El **Panel** es la primera página que ven los administradores después de iniciar sesión en la consola de Citrix Endpoint Management. El **Panel** muestra información básica sobre notificaciones y dispositivos.
Informes	La página **Analyze > Reporting** proporciona informes predefinidos que le permiten analizar las implementaciones de sus aplicaciones y dispositivos.
Dispositivos	La página **Manage > Devices** es donde se administran los dispositivos de usuario. Puede agregar dispositivos individuales en la página o importar un archivo de aprovisionamiento de dispositivos para agregar varios dispositivos a la vez.
Usuarios y grupos locales	La página **Manage > Users** es donde puede agregar, modificar o eliminar usuarios y grupos de usuarios locales.
Inscripción	La página **Manage > Enrollment Invitations** es donde se administra cómo se invita a los usuarios a inscribir sus dispositivos en Citrix Endpoint Management.
Directivas	La página **Configure > Device Policies** es donde se administran las directivas de dispositivos, como VPN y red.
Aplicación	La página **Configure > Apps** es donde se administran las diversas aplicaciones que los usuarios pueden instalar en sus dispositivos.

Contenido multimedia	La página **Configure > Media** es donde se administran los diversos contenidos multimedia que los usuarios pueden instalar en sus dispositivos.
Acción	La página **Configure > Actions** es donde se administran las respuestas a los eventos de activación.
Grupo de entrega	La página **Configurar > Grupos de entrega** es donde se administran los grupos de entrega y los recursos asociados a ellos.
Perfil de inscripción	La página **Configurar > Perfiles de inscripción** es donde se especifica cómo los usuarios pueden inscribir sus dispositivos.
Alexa para empresas	La página **Configuración** es donde se administran los perfiles de Alexa para empresas.
Configuración	La página **Configuración** es donde se administran los ajustes del sistema, como las propiedades de cliente y servidor, los certificados y los proveedores de credenciales. **Importante:** Estos ajustes incluyen el permiso RBAC. El permiso RBAC otorga a los administradores acceso total, incluida la capacidad de asignar sus propios permisos. Conceda este acceso solo a los usuarios a los que desee dar la capacidad de manipular todo en el sistema Citrix Endpoint Management.
Soporte	La página **Solución de problemas y soporte** es donde se realizan actividades de solución de problemas, como ejecutar diagnósticos y generar registros.

RESTRICCIONES DE DISPOSITIVOS PARA ADMINISTRADORES

Los administradores acceden a las funciones del dispositivo a través de la consola estableciendo restricciones de dispositivos, configurando y enviando notificaciones a los dispositivos, administrando aplicaciones en los dispositivos, etc.

Borrar dispositivo por completo	Borrar todos los datos y aplicaciones de un dispositivo, incluidas las tarjetas de memoria si el dispositivo tiene una.
Borrar restricción	Eliminar una o más restricciones de dispositivo.
Borrado selectivo de dispositivo	Borrar todos los datos y aplicaciones corporativos de un dispositivo, dejando los datos y aplicaciones personales intactos.
Ver ubicaciones	Ver la ubicación y establecer restricciones geográficas en un dispositivo. Incluye: Localizar dispositivo, Rastrear dispositivo.
Bloquear dispositivo	Bloquear un dispositivo de forma remota para que los usuarios no puedan usarlo.
Desbloquear dispositivo	Desbloquear un dispositivo de forma remota para que los usuarios puedan usarlo.
Bloquear contenedor	Bloquear de forma remota el contenedor corporativo en un dispositivo.
Desbloquear contenedor	Desbloquear de forma remota el contenedor corporativo en un dispositivo.
Restablecer contraseña del contenedor	Restablecer la contraseña del contenedor corporativo.
Habilitar ASM/Omitir bloqueo de activación	Almacene un código de omisión en un dispositivo iOS supervisado cuando el Bloqueo de activación esté habilitado. Para borrar el dispositivo, use este código para borrar el Bloqueo de activación automáticamente.

Obtener usuarios residentes	Enumere los usuarios que tienen cuentas activas en el dispositivo actual. Esta acción fuerza una sincronización entre el dispositivo y la consola de Citrix Endpoint Management.
Cerrar sesión de usuario residente	Forzar el cierre de sesión del usuario actual.
Eliminar usuario residente	Eliminar la sesión actual de un usuario específico. El usuario puede iniciar sesión de nuevo.
Hacer sonar el dispositivo	Hacer sonar un dispositivo Windows de forma remota a todo volumen durante 5 minutos.
Reiniciar el dispositivo	Reiniciar dispositivos Windows desde la consola de Citrix Endpoint Management.
Implementar en el dispositivo	Enviar aplicaciones, notificaciones, restricciones y otros recursos a un dispositivo.
Editar dispositivo	Cambiar la configuración del dispositivo.
Notificación al dispositivo	Enviar una notificación a un dispositivo.
Agregar/Eliminar dispositivo	Agregar o quitar dispositivos de Citrix Endpoint Management.
Importación de dispositivos	Importar un grupo de dispositivos de un archivo a Citrix Endpoint Management.
Exportar tabla de dispositivos	Recopilar información del dispositivo de la página Dispositivo y exportarla a un archivo .csv.
Revocar dispositivo	Prohibir que un dispositivo se conecte a Citrix Endpoint Management.
Bloqueo de apps	Denegar el acceso a todas las aplicaciones de un dispositivo. En Android, esta restricción impide que los usuarios inicien sesión en Citrix Endpoint Management. En iOS, los usuarios

	pueden iniciar sesión, pero no pueden acceder a las aplicaciones.
Borrado de apps	En Android, esta restricción elimina la cuenta de Citrix Endpoint Management del usuario. En iOS, esta restricción elimina la clave de cifrado necesaria para que los usuarios accedan a las funciones de Citrix Endpoint Management.
Ver inventario de software	Ver qué software está instalado en un dispositivo.
Solicitar duplicación de AirPlay	Solicitar el inicio de la transmisión de AirPlay.
Detener duplicación de AirPlay	Detener la transmisión de AirPlay.
Habilitar modo perdido	En la página **Administrar > Dispositivos**, puede poner un dispositivo supervisado en modo perdido para bloquearlo en la pantalla de bloqueo. A continuación, puede localizar el dispositivo cuando se pierda o sea robado.
Deshabilitar modo perdido	En la página **Administrar > Dispositivos**, puede deshabilitar el modo perdido para un dispositivo que esté configurado en modo perdido.
Actualizar SO del dispositivo	Puede implementar una directiva de actualización del SO del dispositivo en los dispositivos.
Apagar dispositivo	Apagar dispositivos iOS desde la consola de Citrix Endpoint Management.
Reiniciar dispositivo	Reiniciar dispositivos iOS desde la consola de Citrix Endpoint Management.
Renovar certificado de inscripción de dispositivos	Renovar un certificado de CA de dispositivo.

USUARIOS Y GRUPOS LOCALES

Los administradores gestionan los usuarios locales y los grupos de usuarios locales en la página **Administrar > Usuarios** de Citrix Endpoint Management.

Agregar usuarios locales
Eliminar usuarios locales
Modificar usuarios locales
Importar usuarios locales
Exportar usuarios locales
Grupos de usuarios locales
Obtener ID de bloqueo de usuario local
Eliminar bloqueo de usuario local

INSCRIPCIÓN

Los administradores pueden agregar y eliminar invitaciones de inscripción, enviar notificaciones a los usuarios y exportar la tabla de inscripción a un archivo .csv.

Añadir/Eliminar inscripción	Añadir o eliminar una invitación de inscripción a un usuario o a un grupo de usuarios.
Notificar al usuario	Enviar una invitación de inscripción a un usuario o grupo de usuarios.
Exportar tabla de invitaciones de inscripción	Recopilar información de inscripción de la página de Inscripción y exportarla a un archivo .csv.

DIRECTIVAS

Añadir/Eliminar directiva	Añadir o eliminar una directiva de dispositivo o aplicación.

Editar directiva	Cambiar una directiva de dispositivo o aplicación.
Cargar directiva	Cargar una directiva de dispositivo o aplicación.
Clonar directiva	Copiar una directiva de dispositivo o aplicación.
Deshabilitar política	Deshabilita una política de aplicaciones existente.
Exportar política	Recopile información de la política de dispositivos de la página Directivas de dispositivos y expórtela a un archivo .csv.
Asignar política	Asigne una política de dispositivos a uno o varios grupos de entrega.

APLICACIÓN

Los administradores gestionan las aplicaciones en la página **Configurar > Aplicaciones** de Citrix Endpoint Management.

Agregar/eliminar aplicación de tienda de aplicaciones o aplicación empresarial	Agregue o elimine una aplicación de tienda de aplicaciones pública o una aplicación empresarial (no habilitada para MDX).
Editar aplicación de tienda de aplicaciones o aplicación empresarial	Cambie una aplicación de tienda de aplicaciones pública o una aplicación empresarial (no habilitada para MDX).
Agregar/eliminar aplicación MDX, web y SaaS	Agregue o elimine una aplicación habilitada para MDX, una aplicación de su red interna (aplicación web) o una aplicación de una red pública (SaaS) en Citrix Endpoint Management.
Editar aplicación MDX, web y SaaS	Cambiar una aplicación habilitada para MDX, una aplicación de su red interna (aplicación

	web) o una aplicación de una red pública (SaaS) a Citrix Endpoint Management.
Añadir/Eliminar categoría	Añadir o eliminar una categoría en la que pueden aparecer aplicaciones en la tienda de aplicaciones.
Asignar aplicación pública/empresarial a un grupo de entrega	Asignar una aplicación de la tienda de aplicaciones pública o una aplicación habilitada para MDX a un grupo de entrega para su implementación.
Asignar aplicación MDX/WebLink/SaaS a un grupo de entrega	Asignar a un grupo de entrega una aplicación habilitada para MDX, que no requiere inicio de sesión único (WebLink) o que es de una red pública (SaaS).
Exportar tabla de aplicaciones	Recopilar información de la aplicación de la página Aplicación y exportarla a un archivo .csv.

CONTENIDO MULTIMEDIA

Administrar contenido multimedia de una tienda de aplicaciones pública o una licencia de compra por volumen.

Añadir/Eliminar libros de la tienda de aplicaciones o empresariales
Asignar libros públicos/empresariales a un grupo de entrega
Editar libros de la tienda de aplicaciones o empresariales

ACCIÓN

Añadir/eliminar acción	Añadir o eliminar una acción definida por un desencadenador y su respuesta asociada. Un desencadenador es un evento, una propiedad de dispositivo o usuario, o el nombre de una aplicación instalada.

Modificar acción	Cambiar una acción definida por un desencadenador y su respuesta asociada. Un desencadenador es un evento, una propiedad de dispositivo o usuario, o el nombre de una aplicación instalada.
Asignar acción a grupo de entrega	Asignar una acción a un grupo de entrega para su implementación en los dispositivos de los usuarios.
Exportar acción	Recopilar información de acciones de la página Acciones y exportarla a un archivo .csv.

GRUPO DE ENTREGA

Los administradores gestionan los grupos de entrega desde la página **Configurar > Grupos de entrega**.

Añadir/eliminar grupo de entrega	Crear o eliminar un grupo de entrega, lo que añade usuarios especificados y directivas, aplicaciones y acciones opcionales.
Modificar grupo de entrega	Cambiar un grupo de entrega existente, lo que modifica usuarios y directivas, aplicaciones y acciones opcionales.
Implementar grupo de entrega	Hacer que el grupo de entrega esté disponible para su uso.
Exportar grupo de entrega	Recopilar información del grupo de entrega de la página Grupo de entrega y exportarla a un archivo .csv.

PERFIL DE INSCRIPCIÓN

Administrar perfiles de inscripción.

Agregar/eliminar perfil de inscripción
Editar perfil de inscripción

Asignar perfil de inscripción a grupo de entrega

ALEXA PARA EMPRESAS

Administrar perfiles de Alexa for Business.

Agregar/eliminar/editar salas
Agregar/eliminar/editar perfiles de sala
Agregar/eliminar/editar grupos de habilidades

CONFIGURACIÓN PARA ADMINISTRADORES

Los administradores configuran varios ajustes en las páginas de **Configuración**.

RBAC	Asignación de RBAC. **Importante:** Este permiso otorga a los administradores acceso total, incluida la capacidad de asignar sus propios permisos. Conceda este acceso solo a los usuarios a quienes pretenda otorgar la capacidad de manipular todo en el sistema Citrix Endpoint Management.
LDAP	Administrar uno o varios directorios compatibles con LDAP, como Active Directory, para importar grupos, cuentas de usuario y propiedades relacionadas.
Inscripción	Habilitar modos de seguridad de inscripción para usuarios y el Portal de autoayuda.
Gestión de versiones	Ver la versión instalada actual. Incluye: Actualización de gestión de versiones
Certificados	Editar certificado APNS
Plantillas de notificación	Crear plantillas de notificación para usar en acciones automatizadas, inscripción y entrega

	de mensajes de notificación estándar a los usuarios.
Flujos de trabajo	Administrar la creación, aprobación y eliminación de cuentas de usuario para usar con configuraciones de aplicaciones.
Proveedores de credenciales	Agregue uno o varios proveedores de credenciales autorizados para emitir certificados de dispositivo. Los proveedores de credenciales controlan el formato del certificado y las condiciones para renovar o revocar el certificado.
Entidades PKI	Administre entidades de infraestructura de clave pública (genéricas, de Microsoft Certificate Services o CA discrecional).
Probar conexión PKI	Utilice el botón **Probar conexión** de la página **Configuración > Entidades PKI** para asegurarse de que el servidor es accesible.
Propiedades del cliente	Administre varias propiedades en los dispositivos de los usuarios, como el tipo de código de acceso, la seguridad y la caducidad.
Soporte al cliente	Configure las formas en que los usuarios pueden ponerse en contacto con sus servicios de soporte (correo electrónico, teléfono o correo electrónico de ticket de soporte).
Personalización de marca del cliente	Cree un nombre de tienda personalizado y vistas de tienda predeterminadas para la tienda de aplicaciones. Agregue un logotipo personalizado que aparece en la tienda de aplicaciones o en Citrix Secure Hub.
Puerta de enlace SMS del operador	Configure puertas de enlace SMS del operador para configurar las notificaciones que Citrix Endpoint Management envía a través de las puertas de enlace SMS del operador.

Servidor de notificaciones	Configure un servidor de puerta de enlace SMTP para enviar un correo electrónico a los usuarios.
ActiveSync Gateway	Administrar el acceso de los usuarios a usuarios y dispositivos mediante reglas y propiedades.
Google Chrome	Configure Citrix Endpoint Management para que se comunique con su cuenta de Google Workspace.
Programa de implementación de Apple	Agregue una cuenta del Programa de implementación de Apple a Citrix Endpoint Management.
Inscripción de dispositivos con Apple Configurator	Configure los ajustes de Apple Configurator en la consola de Citrix Endpoint Management.
Configuración de iOS/compra por volumen	Agregue cuentas de compra por volumen de Apple.
NetScaler Gateway	Configure los ajustes de NetScaler Gateway (ahora renombrado NetScaler Gateway) en Citrix Endpoint Management.
Control de acceso a la red	Establezca las condiciones que determinan que un dispositivo no cumple las normas para que no pueda acceder a la red.
Propiedades del servidor	Añadir o modificar propiedades del servidor. Requiere reiniciar Citrix Endpoint Management en todos los nodos.
Aplicaciones y escritorios virtuales	Permitir a los usuarios añadir Citrix Virtual Apps y Desktops a través de la aplicación Citrix Workspace.
Citrix Files	Cuando se utiliza Citrix Endpoint Management con cuentas Enterprise: Configure los ajustes para conectarse a las cuentas de servicio de ShareFile y de administrador para la gestión de cuentas de usuario. Requiere un dominio

	de Citrix Files existente y credenciales de administrador. Cuando se utiliza Citrix Endpoint Management con conectores de zona de almacenamiento: Configure Citrix Endpoint Management para que apunte a recursos compartidos de red y ubicaciones de SharePoint definidos en los conectores de zona de almacenamiento.
Android Enterprise	Configure los ajustes del servidor de Android Enterprise.
Proveedor de identidades (IdP)	Configure un proveedor de identidades.
Herramientas de Citrix Endpoint Management	Acceda a la página Herramientas de Citrix Endpoint Management.
Inscripción masiva de Windows	Configure los ajustes de inscripción masiva de Windows.

SOPORTE

Los administradores pueden realizar varias tareas de soporte.

Comprobaciones de conectividad de NetScaler® Gateway	Realice varias comprobaciones de conectividad para NetScaler Gateway por dirección IP. Requiere un nombre de usuario y una contraseña.
Comprobaciones de conectividad de Citrix Endpoint Management	Realice comprobaciones de conectividad para las funciones seleccionadas de Citrix Endpoint Management, como la base de datos, DNS y Google Plan.
Documentación de productos de Citrix	Acceda al sitio de documentación pública de Citrix Endpoint Management.
Centro de conocimiento de Citrix	Acceda al sitio de soporte de Citrix para buscar artículos de la base de conocimientos.
Registros	Ver y descargar archivos de registro.

Macros	Rellene los datos de propiedades de usuario o dispositivo en el campo de texto de una plantilla de perfil, directiva, notificación o inscripción. Configure una única directiva, impleméntela en una gran base de usuarios y haga que aparezcan valores específicos del usuario para cada usuario de destino.
Configuración de PKI	Importe y exporte información de configuración de PKI.
Utilidad de firma de APNS	Enviar una solicitud de certificados de firma de Apple Push Network (APNs), o cargar un certificado APNs de Citrix Secure Mail para iOS.
Citrix Insight Services	Cargar registros en Citrix Insight Services (CIS) para obtener ayuda con diversos problemas.
Estado del conector de NetScaler Gateway del dispositivo para Exchange ActiveSync	Consultar Citrix Endpoint Management para conocer el estado de un dispositivo enviado al conector para Exchange ActiveSync. La consulta se basa en el ID de ActiveSync del dispositivo.

Restringir el acceso a grupos

Los usuarios administradores pueden aplicar permisos a todos los grupos de usuarios.

Funciones de la consola para el aprovisionamiento de dispositivos

Los usuarios de aprovisionamiento de dispositivos tienen el siguiente acceso restringido a la consola de Citrix Endpoint Management. De forma predeterminada, cada una de las siguientes funciones está habilitada.

RESTRICCIONES DE DISPOSITIVOS

Editar dispositivo	Cambiar la configuración del dispositivo.
Agregar/Eliminar dispositivo	Agregar o eliminar dispositivos de Citrix Endpoint Management.

Configuración para el aprovisionamiento de dispositivos

Los usuarios de aprovisionamiento de dispositivos pueden acceder a la página de **Configuración**, pero no tienen derecho a configurar las funciones.

Rol de usuario

Los usuarios con el rol de usuario tienen el siguiente acceso limitado a Citrix Endpoint Management.

Acceso autorizado para usuarios

Portal de autoayuda	Proporcionar a los usuarios acceso solo al Portal de autoayuda en Citrix Endpoint Management.

Funciones de consola para usuarios

Los usuarios tienen el siguiente acceso restringido a la consola de Citrix Endpoint Management.

ACCESO RESTRINGIDO A DISPOSITIVOS PARA USUARIOS

Borrar dispositivo por completo	Borrar todos los datos y aplicaciones de un dispositivo, incluidas las tarjetas de memoria si el dispositivo tiene una.
Borrar dispositivo de forma selectiva	Borrar todos los datos y aplicaciones corporativos de un dispositivo, dejando los datos y aplicaciones personales en su lugar.
Ver ubicaciones	Ver la ubicación de un dispositivo y establecer restricciones geográficas en él. Incluido: Localizar dispositivo, Ver la ubicación de un dispositivo, Rastrear dispositivo, Rastrear la ubicación del dispositivo a lo largo del tiempo
Bloquear dispositivo	Bloquear un dispositivo de forma remota para que no se pueda usar.
Desbloquear dispositivo	Desbloquear un dispositivo de forma remota para que se pueda usar.

Bloquear contenedor	Bloquear de forma remota el contenedor corporativo en un dispositivo.
Desbloquear contenedor	Desbloquear de forma remota el contenedor corporativo en un dispositivo.
Restablecer contraseña del contenedor	Restablecer la contraseña del contenedor corporativo.
Habilitar ASM/Omitir bloqueo de activación	Almacene un código de omisión en un dispositivo iOS supervisado cuando el Bloqueo de activación esté habilitado. Para borrar el dispositivo, use este código para borrar automáticamente el Bloqueo de activación.
Obtener usuarios residentes	Enumerar los usuarios que tienen cuentas activas en el dispositivo actual. Esta acción fuerza una sincronización entre el dispositivo y la consola de Citrix Endpoint Management.
Cerrar sesión de usuario residente	Forzar el cierre de sesión del usuario actual.
Eliminar usuario residente	Eliminar la sesión actual de un usuario específico. El usuario puede iniciar sesión de nuevo.
Hace sonar el dispositivo	Hacer sonar un dispositivo Windows de forma remota a todo volumen durante 5 minutos.
Reiniciar el dispositivo	Reiniciar un dispositivo Windows.
Bloqueo de apps	Denegar el acceso a todas las aplicaciones de un dispositivo. En Android, los usuarios no pueden iniciar sesión en Citrix Endpoint Management. En iOS, los usuarios pueden iniciar sesión, pero no pueden acceder a las aplicaciones.
Borrado de apps	En Android, esta restricción elimina la cuenta de Citrix Endpoint Management del usuario. En iOS, esta restricción elimina la clave de cifrado necesaria para que los usuarios

	accedan a las funciones de Citrix Endpoint Management.
Ver inventario de software	Ver qué software está instalado en un dispositivo.

RESTRICCIONES DE INSCRIPCIÓN PARA USUARIOS

Añadir/Eliminar inscripción	Añadir o eliminar una invitación de inscripción a un usuario o a un grupo de usuarios.
Notificar al usuario	Enviar una invitación de inscripción a un usuario o grupo de usuarios.

Restringir el acceso a grupos para todos los roles

Para los roles predeterminados, este permiso está establecido de forma predeterminada y se puede aplicar a todos los grupos de usuarios. No se puede editar el rol.

Licencias

Para obtener información sobre el uso de licencias de Citrix®, consulte:

- Supervisar el uso activo y las licencias de los servicios en la nube
- Supervisar el uso activo y las licencias de Citrix Endpoint Management

Administración de dispositivos

Citrix Endpoint Management puede aprovisionar, administrar, proteger e inventariar una amplia gama de tipos de dispositivos desde una única consola de administración.

- Utilice un conjunto común de directivas de dispositivo para administrar los dispositivos compatibles. Para ver rápidamente las directivas de dispositivo disponibles por plataforma:

  a. Vaya a la consola de Citrix Endpoint Management y, a continuación, a **Configurar > Directivas de dispositivo**.

  b. Haga clic en **Agregar** y, a continuación, seleccione las plataformas que quiere ver.

  Para obtener más información, consulte Filtrar la lista de directivas de dispositivo agregadas.

- Proteja la información empresarial con una seguridad estricta para la identidad, los dispositivos corporativos y BYO, las aplicaciones, los datos y la red. Especifique la identidad de usuario que se utilizará para autenticarse en los dispositivos. Configure cómo mantener separados los datos empresariales y personales en los dispositivos.
- Entregue cualquier aplicación a los usuarios finales, sea cual sea el dispositivo o el sistema operativo. Proteja su información a nivel de aplicación y proporcione una administración de aplicaciones móviles de nivel empresarial.
- Utilice los controles de aprovisionamiento y configuración para configurar los dispositivos. Esos controles incluyen la inscripción de dispositivos, la aplicación de directivas y los privilegios de acceso.
- Utilice los controles de seguridad y cumplimiento para crear una base de seguridad personalizada con desencadenadores accionables. Por ejemplo, bloquee, borre o notifique a un dispositivo que infrinja los estándares de cumplimiento definidos.
- Utilice los controles de actualización del sistema operativo para evitar o forzar las actualizaciones del sistema operativo. Esta función es fundamental para la prevención de la pérdida de datos frente a vulnerabilidades específicas del sistema operativo.

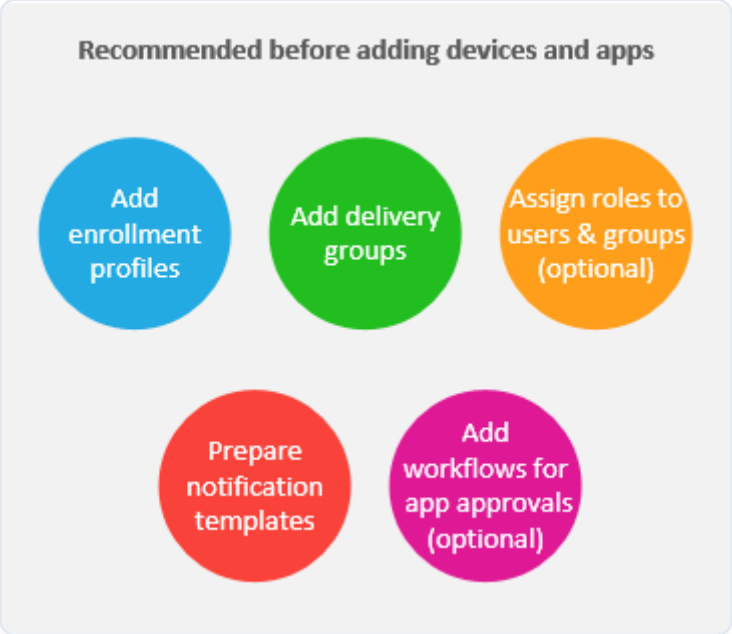
Para acceder a los artículos sobre cada plataforma compatible, expanda la sección "Administración de dispositivos" en la lista de contenidos. Esos artículos proporcionan detalles

específicos de cada plataforma de dispositivo. El resto de este artículo describe cómo realizar tareas generales de administración de dispositivos.

Flujos de trabajo de administración de dispositivos

Los diagramas de flujo de esta sección proporcionan una secuencia sugerida para las tareas de administración de dispositivos.

1. **Requisitos previos recomendados para agregar dispositivos y aplicaciones:** Realizar la siguiente configuración con antelación le permite configurar dispositivos y aplicaciones sin interrupciones.



Consulte:

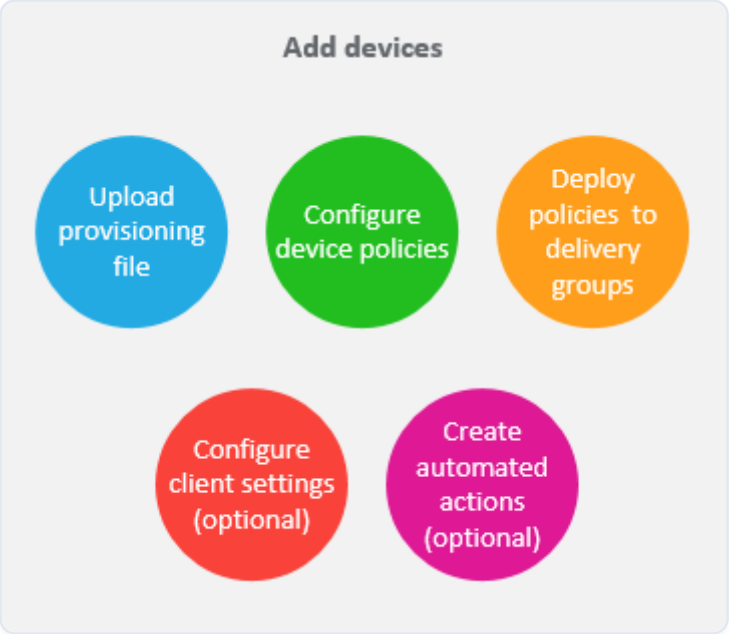
Implementar recursos

Configurar roles con RBAC

Crear y actualizar plantillas de notificación

Crear y administrar flujos de trabajo

2. **Añadir dispositivos:**



Consulte:

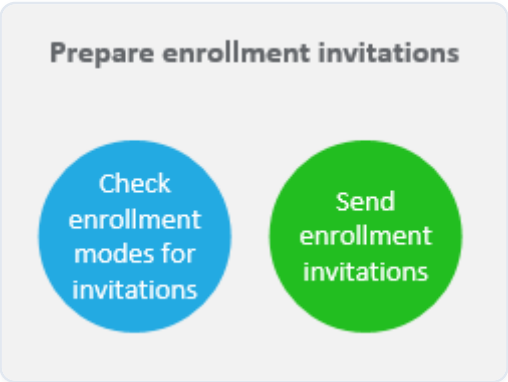
Preparar la inscripción de dispositivos y la entrega de recursos

Directivas de dispositivo

Implementar en grupos de entrega

Acciones automatizadas

3. **Preparar invitaciones de inscripción:** Puede enviar invitaciones de inscripción a usuarios con dispositivos iOS, iPadOS, macOS, Android Enterprise y Android heredados. Haga lo siguiente si tiene previsto utilizar invitaciones de inscripción.

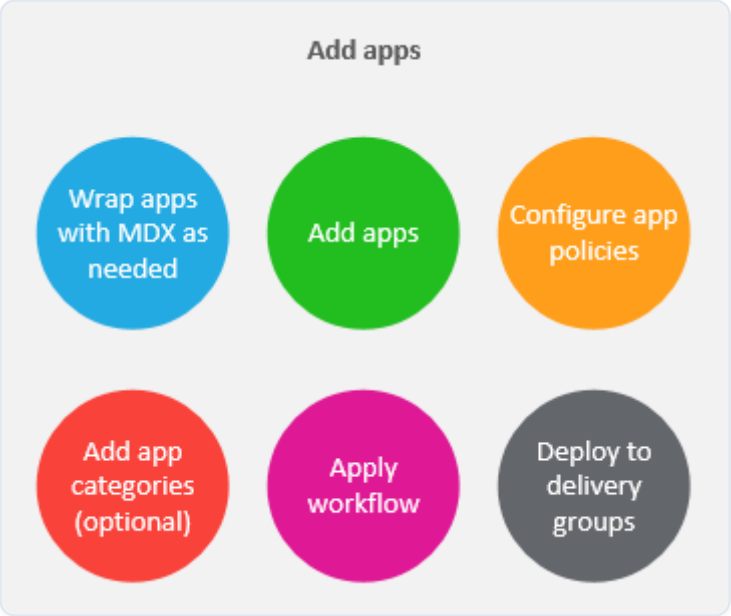


Ver:

Configurar modos de seguridad de inscripción

Enviar una notificación a los dispositivos

4. **Agregar aplicaciones:**



Ver:

SDK de MAM

Agregar aplicaciones

Acerca de las categorías de aplicaciones

Aplicar flujos de trabajo

Implementar en grupos de entrega

5. **Realizar la administración continua de dispositivos y aplicaciones:** Además de usar el panel de Citrix Endpoint Management, le recomendamos que revise el contenido de Novedades de cada versión. Novedades proporciona información sobre cualquier acción necesaria, como la configuración de nuevas directivas de dispositivos.



Ver:

Supervisar y ofrecer soporte

Informes

Acciones de seguridad

¿Novedades?

Directivas de dispositivo

Invitaciones de inscripción

Para administrar los dispositivos de usuario de forma remota y segura, se inscriben los dispositivos de usuario en Citrix Endpoint Management. El software cliente de Citrix Endpoint Management se instala en el dispositivo de usuario y se autentica la identidad del usuario. A continuación, se instalan Citrix Endpoint Management y el perfil de usuario. Para obtener detalles sobre la inscripción en las plataformas de dispositivos compatibles, consulte los artículos sobre dispositivos en esta sección.

En la consola de Citrix Endpoint Management:

- Puede enviar una invitación de inscripción a los usuarios con dispositivos iOS, iPadOS, macOS, Android Enterprise y Android heredado. Las invitaciones de inscripción no están disponibles para dispositivos Windows.

- Puede enviar una URL de invitación a los usuarios con dispositivos iOS, iPadOS, Android Enterprise o Android heredado. Las URL de invitación no están disponibles para dispositivos Windows.

Las invitaciones de inscripción se envían de la siguiente manera:

- Si los usuarios de Active Directory tienen una dirección de correo electrónico en Active Directory, reciben la invitación. Los usuarios locales reciben la invitación en el correo electrónico especificado en las propiedades de usuario.

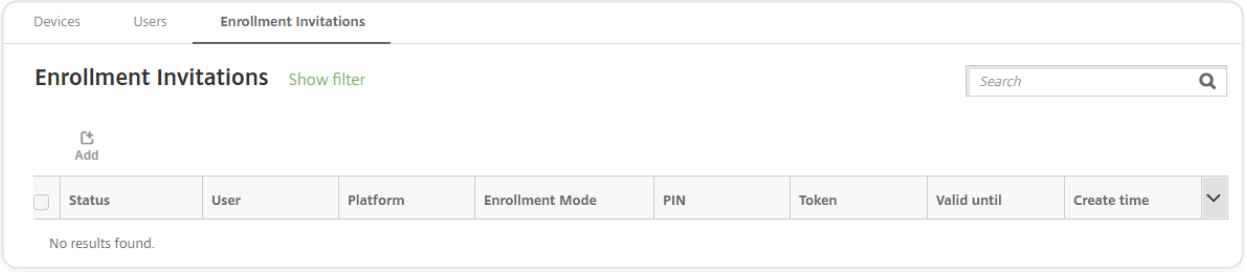
Después de que los usuarios se inscriben, sus dispositivos aparecen como administrados en **Administrar > Dispositivos**. El estado de la URL de invitación se muestra como **Canjeada**.

Requisitos previos

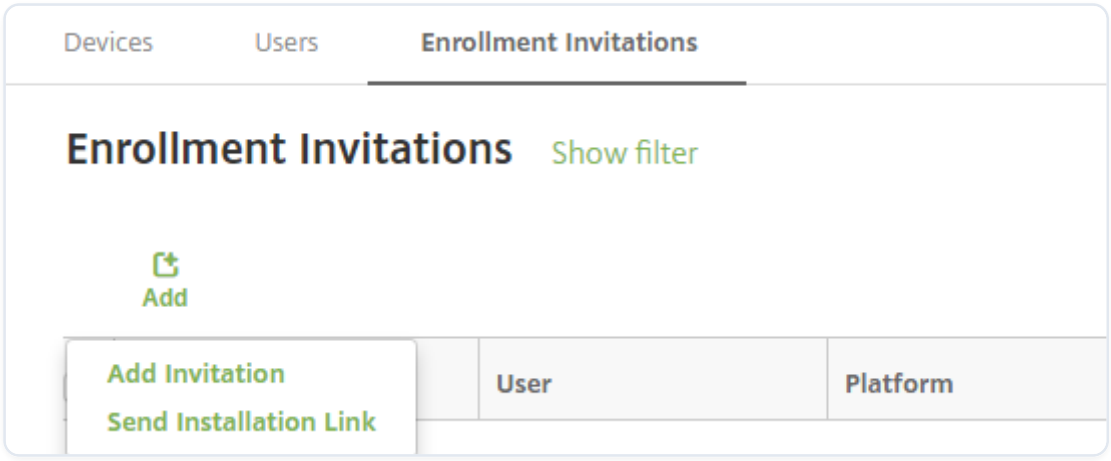
- LDAP configurado
- Si utiliza grupos locales y usuarios locales:
  - Uno o varios grupos locales.
  - Usuarios locales asignados a grupos locales.
  - Los grupos de entrega están asociados a grupos locales.
- Si utiliza Active Directory:
  - Los grupos de entrega están asociados a grupos de Active Directory.

Crear una invitación de inscripción

1. En la consola de Citrix Endpoint Management, haga clic en **Administrar > Invitaciones de inscripción**. Aparecerá la página **Invitaciones de inscripción**.



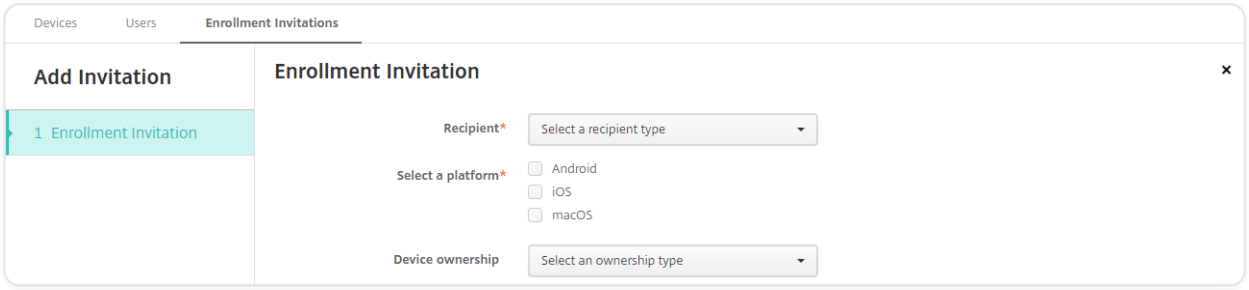
2. Haga clic en **Agregar**. Aparecerá un menú de opciones de inscripción.



- Para enviar una invitación de inscripción a un usuario o grupo, haga clic en **Agregar invitación**.
- Para enviar un enlace de instalación de inscripción a una lista de destinatarios a través de SMTP, haga clic en **Enviar enlace de instalación**.

El envío de invitaciones de inscripción y enlaces de instalación se describe después de estos pasos.

3. Haga clic en **Agregar invitación**. Aparecerá la pantalla **Invitación de inscripción**.



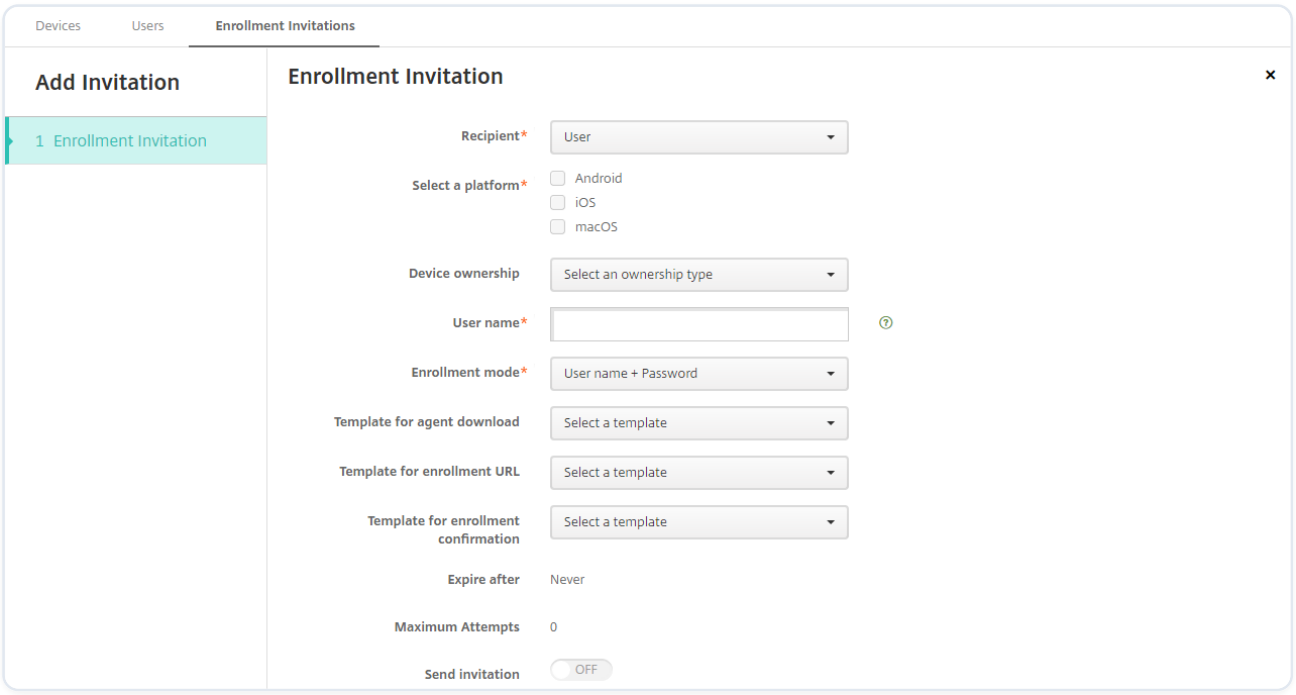
4. Configure estos ajustes:

   - **Destinatario:** Elija **Grupo** o **Usuario**.
   - **Seleccionar una plataforma:** Si **Destinatario** es **Grupo**, se seleccionan todas las plataformas. Puede cambiar la selección de la plataforma. Si **Destinatario** es **Usuario**, no se selecciona ninguna plataforma. Seleccione una plataforma.

     Para crear una invitación de inscripción para dispositivos Android Enterprise, seleccione **Android**.
   - **Propiedad del dispositivo:** Seleccione **Corporativo** o **Empleado**.

   Aparecen los ajustes para usuarios o grupos, como se describe en las siguientes secciones.

Para enviar una invitación de inscripción a un usuario



1. Configure estos ajustes de **Usuario**:

   - **Nombre de usuario:** Escriba un nombre de usuario. El usuario debe existir en Citrix Endpoint Management como usuario local o de Active Directory. Si el usuario es local, configure la propiedad de correo electrónico del usuario para poder enviarle notificaciones. Si el usuario está en Active Directory, siempre que LDAP esté configurado.
   - **Número de teléfono:** Este ajuste no aparece si selecciona más de una plataforma o si selecciona solo macOS. Opcionalmente, escriba el número de teléfono del usuario.
   - **Operador:** Este ajuste no aparece si selecciona más de una plataforma o si selecciona solo macOS. Elija un operador para asociarlo al número de teléfono del usuario.
   - **Modo de inscripción:** Elija el modo de seguridad de inscripción para los usuarios. El valor predeterminado es **Nombre de usuario + Contraseña**. Algunas de las siguientes opciones no están disponibles para todas las plataformas:

     - **Nombre de usuario + Contraseña**
     - **URL de invitación**
     - **URL de invitación + PIN**
     - **URL de invitación + Contraseña**
     - **Doble factor**
     - **Nombre de usuario + PIN**

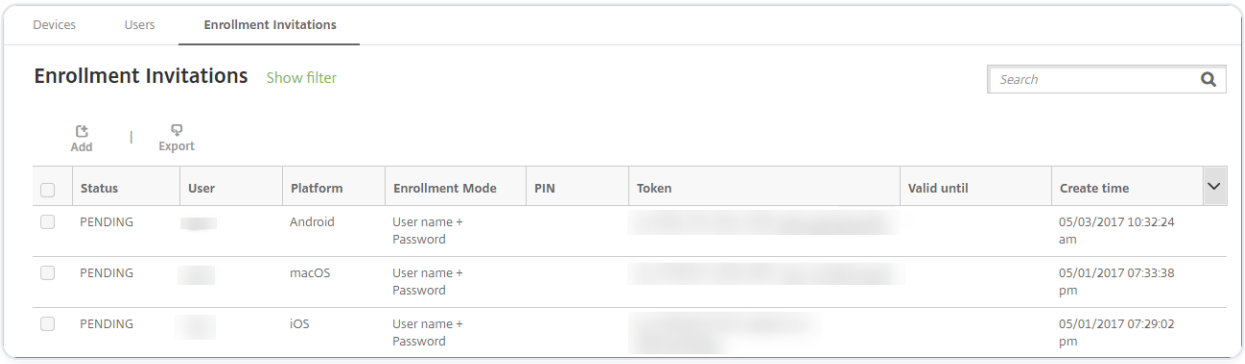
Hemos dejado de dar soporte al modo de inscripción de **Alta seguridad**. Para enviar invitaciones de inscripción, solo puede usar los modos de seguridad de inscripción **URL de invitación**, **URL de invitación + PIN** o **URL de invitación + Contraseña**. Para los dispositivos que se inscriben con **Nombre de usuario + Contraseña**, **Doble factor** o **Nombre de usuario + PIN**, los usuarios deben descargar Citrix Secure Hub e introducir manualmente sus credenciales.

Para obtener más información, consulte Modos de seguridad de inscripción por plataforma. Un PIN para la inscripción también se denomina PIN de un solo uso. Dichos PIN solo son válidos cuando el usuario se inscribe.

> **Nota:**
>
> Cuando selecciona cualquier modo de seguridad de inscripción que incluya un PIN, aparece el campo **Plantilla para el PIN de inscripción**. Haga clic en **PIN de inscripción**.

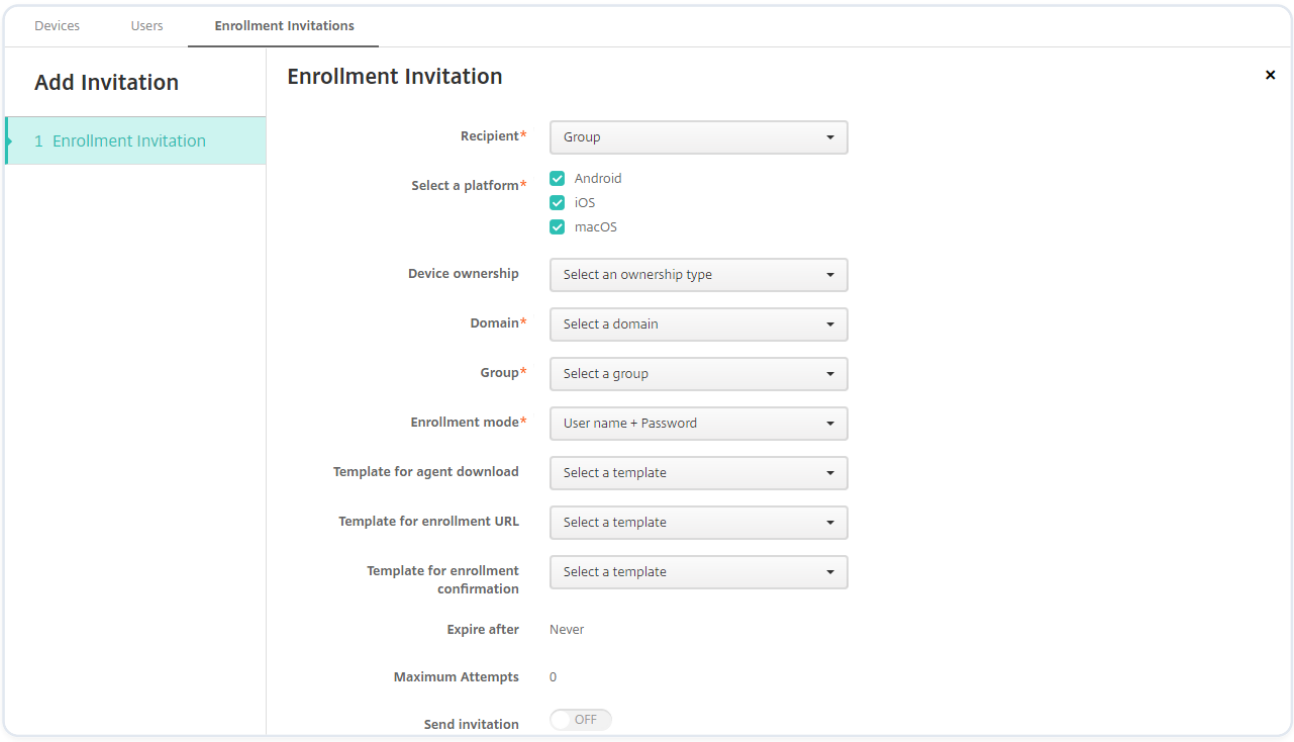
- **Plantilla para la descarga del agente:** Elija la plantilla de enlace de descarga denominada **Enlace de descarga**. Esa plantilla es para todas las plataformas compatibles.
- **Plantilla para la URL de inscripción:** Elija **Invitación de inscripción**.
- **Plantilla para la confirmación de inscripción:** Elija **Confirmación de inscripción**.
- **Caduca después de:** Este campo se establece al configurar el modo de seguridad de inscripción e indica cuándo caduca la inscripción. Para obtener más información sobre cómo configurar los modos de seguridad de inscripción, consulte Configurar modos de seguridad de inscripción.
- **Intentos máximos:** Este campo se establece al configurar el modo de seguridad de inscripción e indica el número máximo de veces que se produce el proceso de inscripción.
- **Enviar invitación:** Seleccione **Activado** para enviar la invitación inmediatamente. Seleccione **Desactivado** para agregar la invitación a la tabla de la página **Invitaciones de inscripción**, pero sin enviarla.

2. Haga clic en **Guardar y enviar** si ha activado **Enviar invitación**. De lo contrario, haga clic en **Guardar**. La invitación aparece en la tabla de la página **Invitaciones de inscripción**.



Para enviar una invitación de inscripción a un grupo

La siguiente figura muestra la configuración para configurar una invitación de inscripción a un grupo.



1. Configure estos ajustes:

   - **Dominio:** Elija el dominio del grupo que recibirá la invitación.
   - **Grupo:** Elija el grupo que recibirá la invitación. Citrix Endpoint Management obtiene la lista de usuarios de Active Directory. La lista incluye usuarios cuyos nombres tienen caracteres especiales.
   - **Modo de inscripción:** Elija cómo desea que se inscriban los usuarios del grupo. El valor predeterminado es **Nombre de usuario + Contraseña**. Algunas de las siguientes opciones no están disponibles para todas las plataformas:

     - **Nombre de usuario + Contraseña**

- **URL de invitación**
- **URL de invitación + PIN**
- **URL de invitación + Contraseña**
- **Doble factor**
- **Nombre de usuario + PIN**

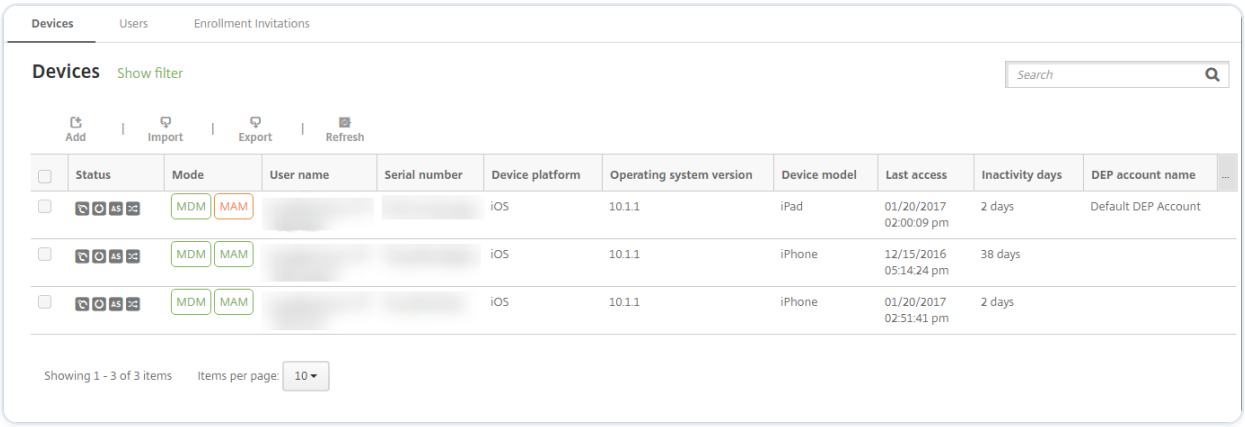
Hemos dejado de admitir el modo de inscripción de **Alta seguridad**. Para enviar invitaciones de inscripción, solo puede usar los modos de seguridad de inscripción **URL de invitación**, **URL de invitación + PIN** o **URL de invitación + Contraseña**. Para los dispositivos que se inscriben con **Nombre de usuario + Contraseña**, **Doble factor** o **Nombre de usuario + PIN**, los usuarios deben descargar Citrix Secure Hub e introducir manualmente sus credenciales.

Solo aparecen los modos de seguridad de inscripción válidos para cada una de las plataformas seleccionadas. Para obtener más información, consulte Modos de seguridad de inscripción por plataforma.

> **Nota:**
>
> Cuando selecciona cualquier modo de seguridad de inscripción que incluya un PIN, aparece el campo **Plantilla para PIN de inscripción**. Haga clic en **PIN de inscripción**.

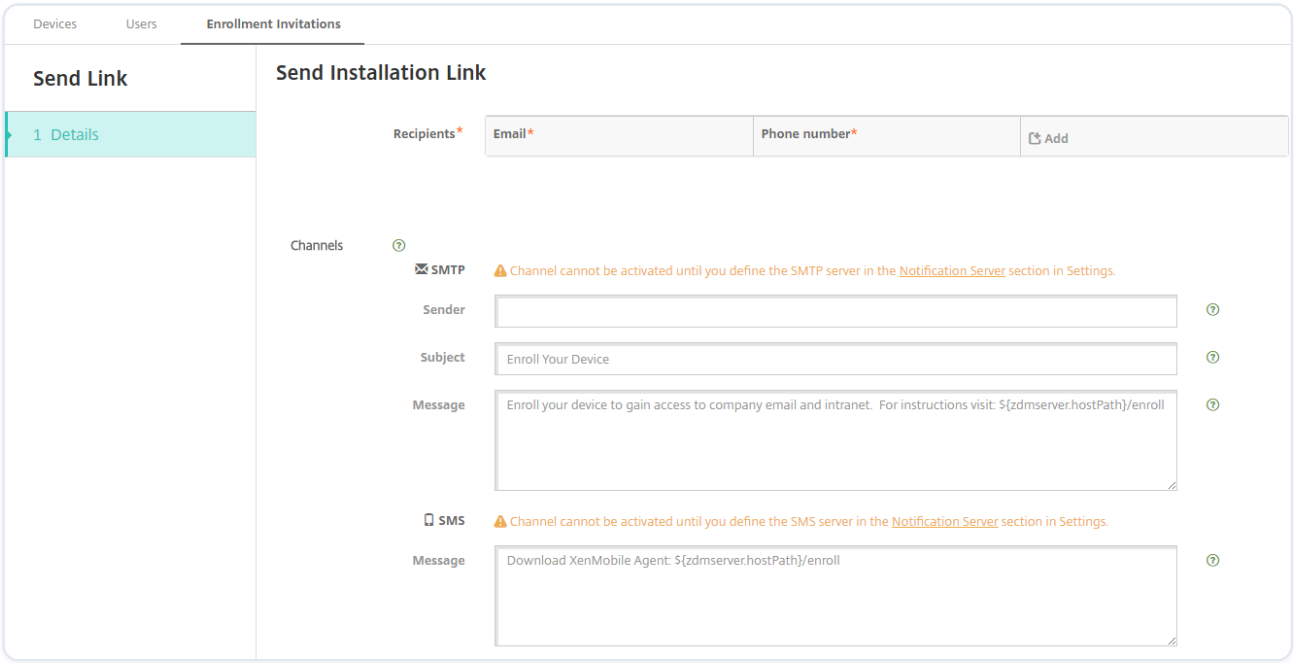
- **Plantilla para descarga del agente:** Elija la plantilla de enlace de descarga denominada **Enlace de descarga**. Esa plantilla es para todas las plataformas compatibles.
- **Plantilla para URL de inscripción:** Elija **Invitación de inscripción**.
- **Plantilla para confirmación de inscripción:** Elija **Confirmación de inscripción**.
- **Caduca después de:** Este campo se establece al configurar el modo de seguridad de inscripción e indica cuándo caduca la inscripción. Para obtener más información sobre la configuración de los modos de seguridad de inscripción, consulte Configurar modos de seguridad de inscripción.
- **Intentos máximos:** Este campo se establece al configurar el modo de seguridad de inscripción e indica el número máximo de veces que se produce el proceso de inscripción.
- **Enviar invitación:** Seleccione **Activado** para enviar la invitación inmediatamente. Seleccione **Desactivado** para agregar la invitación a la tabla de la página **Invitaciones de inscripción**, pero sin enviarla.

2. Haga clic en **Guardar y enviar** si habilitó **Enviar invitación**. De lo contrario, haga clic en **Guardar**. La invitación aparece en la tabla de la página **Invitación de inscripción**.



Para enviar un enlace de instalación

Antes de poder enviar un enlace de instalación de inscripción, debe configurar los canales (SMTP) en el servidor de notificaciones desde la página **Configuración**. Para obtener más información, consulte Notificaciones



1. Configure estos ajustes y, a continuación, haga clic en **Guardar**.

    - **Destinatario:** Para cada destinatario que desee añadir, haga clic en **Añadir** y, a continuación, haga lo siguiente:

        - **Correo electrónico:** Escriba la dirección de correo electrónico del destinatario. Este campo es obligatorio.

- **Número de teléfono:** Escriba el número de teléfono del destinatario. Este campo es obligatorio.

> **Nota:**
>
> Para eliminar un destinatario, sitúe el cursor sobre la línea con el listado y, a continuación, haga clic en el icono de la papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Eliminar** para eliminar el listado o en **Cancelar** para mantenerlo.

> Para modificar un destinatario, sitúe el cursor sobre la línea con el listado. A continuación, haga clic en el icono del lápiz situado a la derecha. Actualice el listado y, a continuación, haga clic en **Guardar** para guardar el listado modificado o en **Cancelar** para dejar el listado sin cambios.

- **Canales:** Seleccione un canal para enviar el enlace de instalación de la inscripción. Puede enviar notificaciones a través de **SMTP**. Estos canales no se pueden activar hasta que configure los ajustes del servidor en la página **Configuración** de **Servidor de notificaciones**. Para obtener más información, consulte Notificaciones.
- **SMTP:** Configure estos ajustes opcionales. Si no escribe nada en estos campos, se utilizarán los valores predeterminados especificados en la plantilla de notificación configurada para la plataforma seleccionada:
  - **Remitente:** Escriba un remitente opcional.
  - **Asunto:** Escriba un asunto opcional para el mensaje. Por ejemplo, "Inscriba su dispositivo".
  - **Mensaje:** Escriba un mensaje opcional para enviar al destinatario. Por ejemplo, "Inscriba su dispositivo para obtener acceso a las aplicaciones y el correo electrónico de la organización".

2. Haga clic en **Enviar**.

> **Nota:**
>
> Si su entorno utiliza sAMAccountName: Después de que los usuarios reciban la invitación y hagan clic en el enlace, deben modificar el nombre de usuario para

> completar la autenticación. El nombre de usuario aparece en el formato `sAMAccountName@domainname.com`. Los usuarios deben eliminar la parte `@domainname.com`.

Modos de seguridad de inscripción por plataforma

La siguiente tabla muestra los modos de seguridad que puede usar para inscribir dispositivos de usuario. En la tabla, **Sí** indica qué plataformas de dispositivos admiten modos de inscripción y administración específicos con diferentes perfiles de inscripción.

MODO DE SEGURIDAD DE INSCRIPCIÓN DE MDM	MODO DE SEGURIDAD DE INSCRIPCIÓN DE MAM EN NETSCALER GATEWAY	MODOS DE ADMINISTRACIÓN	ADMITEN DIFERENTES PERFILES DE INSCRIPCIÓN	ANDROID (HEREDADO)	ANDROID ENTERPRISE	IOS (MODO DE INSCRIPCIÓN DE USUARIO)	IOS	MACOS	WINDOWS
Azure AD y Okta como proveedores de identidades a través de Citrix	Certificado de cliente	MDM+MAM o MDM	Sí	Sí	Sí	Sí	Sí	No	No

MODO DE SEGURIDAD DE INSCRIPCIÓN DE MDM	MODO DE SEGURIDAD DE INSCRIPCIÓN DE MAM EN NETSCALER GATEWAY	MODOS DE ADMINISTRACIÓN	ADMITEN DIFERENTES PERFILES DE INSCRIPCIÓN	ANDROID (HEREDADO)	ANDROID ENTERPRISE	IOS (MODO DE INSCRIPCIÓN DE USUARIO)	IOS	MACOS	WINDOWS
Cloud									
Nombre de usuario + Contraseña	LDAP, LDAP + certificado de cliente y solo certificado de cliente	MDM+MAM, MDM o MAM (el modo solo MAM no admite certificados de cliente en NetScaler Gateway)	Sí	Sí	Sí	Sí	Sí	Sí	Sí

MODO DE SEGURIDAD DE INSCRIPCIÓN DE MDM	MODO DE SEGURIDAD DE INSCRIPCIÓN DE MAM EN NETSCALER GATEWAY	MODOS DE ADMINISTRACIÓN	ADMITEN DIFERENTES PERFILES DE INSCRIPCIÓN	ANDROID (HEREDADO)	ANDROID ENTERPRISE	IOS (MODO DE INSCRIPCIÓN DE USUARIO)	IOS	MACOS	WINDOWS
URL de invitación	Certificado de cliente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	No	No
URL de invitación + PIN	Certificado de cliente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	No	No
URL de invitación + Contraseña	LDAP, LDAP + certificado de cliente y solo certificado de	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	No	No

MODO DE SEGURIDAD DE INSCRIPCIÓN DE MDM	MODO DE SEGURIDAD DE INSCRIPCIÓN DE MAM EN NETSCALER GATEWAY	MODOS DE ADMINISTRACIÓN	ADMITEN DIFERENTES PERFILES DE INSCRIPCIÓN	ANDROID (HEREDADO)	ANDROID ENTERPRISE	IOS (MODO DE INSCRIPCIÓN DE USUARIO)	IOS	MACOS	WINDOWS
	cliente								
Autenticación de dos factores (nombre de usuario + contraseña + PIN)	LDAP, LDAP + certificado de cliente y solo certificado de cliente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	Sí	No
Nombre de usuar	Certificado de cliente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	Sí	No

MODO DE SEGURIDAD DE INSCRIPCIÓN DE MDM	MODO DE SEGURIDAD DE INSCRIPCIÓN DE MAMEN NETSCALER GATEWAY	MODOS DE ADMINISTRACIÓN	ADMITEN DIFERENTES PERFILES DE INSCRIPCIÓN	ANDROID (HEREDADO)	ANDROID ENTERPRISE	IOS (MODO DE INSCRIPCIÓN DE USUARIO)	IOS	MACOS	WINDOWS
io + PIN									

A continuación se describe cómo se comportan los modos de seguridad de inscripción en dispositivos iOS, Android y Android Enterprise:

- **Nombre de usuario + Contraseña** (predeterminado)
    - Envía al usuario una única notificación que contiene una URL de inscripción. Cuando el usuario hace clic en la URL, se abre Citrix Secure Hub. A continuación, el usuario escribe un nombre de usuario y una contraseña para inscribir el dispositivo en Citrix Endpoint Management.
- **URL de invitación**
    - Envía al usuario una única notificación que contiene una URL de inscripción. Cuando el usuario hace clic en la URL, se abre Citrix Secure Hub. Aparecen el nombre del servidor de Citrix Endpoint Management y el botón **Sí, inscribir**. El usuario toca **Sí, inscribir** para inscribir el dispositivo en Citrix Endpoint Management.
- **URL de invitación + PIN**
    - Envía al usuario los siguientes correos electrónicos:
        - Un correo electrónico con una URL de inscripción, que permite al usuario inscribir el dispositivo en Citrix Endpoint Management a través de Citrix Secure Hub.

        - Un correo electrónico con un PIN de un solo uso que el usuario debe escribir al inscribir el dispositivo, junto con la contraseña de Active Directory (o local) del usuario.

    - Con este modo, el usuario se inscribe solo usando la URL de inscripción en la notificación. Si el usuario pierde la invitación de notificación, no puede inscribirse. Sin embargo, puede enviar otra invitación.

- **URL de invitación + Contraseña**

    - Envía al usuario una única notificación que contiene una URL de inscripción. Cuando el usuario hace clic en la URL, se abre Citrix Secure Hub. Aparece el nombre del servidor de Citrix Endpoint Management, junto con un campo que permite al usuario escribir una contraseña.

- **Doble factor**

    - Envía al usuario una única notificación que contiene una URL de inscripción y un PIN de un solo uso. Cuando el usuario hace clic en la URL, se abre Citrix Secure Hub. Aparece el nombre del servidor de Citrix Endpoint Management, junto con dos campos que permiten al usuario escribir una contraseña y el PIN.

- **Nombre de usuario + PIN**

    - Envía al usuario los siguientes correos electrónicos:

        - Un correo electrónico con una URL de inscripción, que permite al usuario descargar e instalar Citrix Secure Hub. Una vez abierto Citrix Secure Hub, se le pide al usuario que escriba un nombre de usuario y una contraseña para inscribir el dispositivo en Citrix Endpoint Management.
        - Un correo electrónico con un PIN de un solo uso que el usuario debe escribir al inscribir el dispositivo, junto con la contraseña de Active Directory (o local) del usuario.

    - Si el usuario pierde la invitación de notificación, no puede inscribirse. Sin embargo, puede enviar otra invitación.

A continuación, se describe cómo se comportan los modos de seguridad de inscripción en los dispositivos macOS:

- **Nombre de usuario + Contraseña**

    - Envía al usuario una única notificación que contiene una URL de inscripción. Cuando el usuario hace clic en la URL, se abre el navegador Safari. Aparece una página de inicio de

sesión que le pide al usuario que escriba un nombre de usuario y una contraseña para inscribir el dispositivo en Citrix Endpoint Management.

- **Doble factor**
  - Envía al usuario una única notificación que contiene una URL de inscripción y un PIN de un solo uso. Cuando el usuario hace clic en la URL, se abre el navegador Safari. Aparece una página de inicio de sesión que muestra dos campos que permiten al usuario escribir una contraseña y el PIN.
- **Nombre de usuario + PIN**
  - Envía al usuario los siguientes correos electrónicos:
    - Un correo electrónico con una URL de inscripción. Cuando el usuario hace clic en la URL, se abre el navegador Safari. Aparece una página de inicio de sesión que solicita al usuario que escriba un nombre de usuario y una contraseña para inscribir el dispositivo en Citrix Endpoint Management.
    - Un correo electrónico con un PIN de un solo uso que el usuario debe escribir al inscribir el dispositivo, junto con la contraseña de Active Directory (o local) del usuario.
  - Si el usuario pierde la invitación de notificación, no podrá inscribirse. Sin embargo, puede enviar otra invitación.

No puede enviar invitaciones de inscripción a dispositivos Windows. Los usuarios de Windows se inscriben directamente a través de sus dispositivos. Para obtener información sobre cómo inscribir dispositivos Windows, consulte Dispositivos Windows.

Acciones de seguridad

Las acciones de seguridad de dispositivos y aplicaciones se realizan desde la página **Administrar > Dispositivos**. Las acciones de dispositivos incluyen revocar, bloquear, desbloquear y borrar. Las acciones de seguridad de aplicaciones incluyen bloqueo de aplicaciones y borrado de aplicaciones.

- **Omisión de Bloqueo de activación:** Elimina el Bloqueo de activación de los dispositivos iOS supervisados antes de la activación del dispositivo. Este comando no requiere el ID de Apple personal ni la contraseña de un usuario.
- **Bloqueo de aplicaciones:** Deniega el acceso a todas las aplicaciones de un dispositivo. En Android, después de un bloqueo de aplicaciones, los usuarios no pueden iniciar sesión en

Citrix Endpoint Management. En iOS, los usuarios pueden iniciar sesión, pero no pueden acceder a ninguna aplicación.

- **Borrado de aplicaciones:** Elimina la cuenta de usuario de Citrix Secure Hub y anula la inscripción del dispositivo. Los usuarios no pueden volver a inscribirse hasta que utilice la acción **Deshacer borrado de aplicaciones**.
- **Bloqueo de activación del programa de implementación de ASM:** Crea un código de omisión de Bloqueo de activación para dispositivos iOS inscritos en Apple School Manager.
- **Renovación de certificados:** Para los dispositivos iOS, macOS y Android compatibles, la acción de seguridad Renovación de certificados inicia la renovación de certificados. La próxima vez que los dispositivos se conecten a Citrix Endpoint Management, el servidor de Citrix Endpoint Management emitirá nuevos certificados de dispositivo basados en la nueva autoridad de certificación.
- **Borrar restricciones:** En los dispositivos iOS supervisados, este comando permite a Citrix Endpoint Management borrar la contraseña de restricciones y la configuración de restricciones configuradas por el usuario.
- **Habilitar/deshabilitar Modo perdido:** Pone un dispositivo iOS supervisado en Modo perdido y le envía un mensaje, un número de teléfono y una nota al pie para mostrar. La segunda vez que envíe este comando, el dispositivo saldrá del Modo perdido.
- **Enable tracking:** On Android or iOS devices, this command allows Citrix Endpoint Management to poll the location of specific devices at a frequency you define. To view device coordinates and location on a map, go to **Manage > Devices**, select a device, and then click **Edit**. The device info is on the **General** tab under **Security**. Use **Enable tracking** to track the device continuously. Citrix Secure Hub reports the location periodically when the device is running.
- **Borrado completo:** Borra inmediatamente todos los datos y aplicaciones de un dispositivo, incluidas las tarjetas de memoria. Los dispositivos borrados permanecen en la lista de dispositivos de la página **Administrar > Dispositivos** con fines de auditoría. Puede eliminar un dispositivo borrado de la lista de dispositivos.
    - Para dispositivos Android, esta solicitud también puede incluir la opción de borrar tarjetas de memoria.
    - Para dispositivos Android Enterprise totalmente administrados con un perfil de trabajo (dispositivos COPE), puede realizar un borrado completo después de que un borrado selectivo elimine el perfil de trabajo.

- Para dispositivos iOS y macOS, el borrado se produce inmediatamente, incluso si el dispositivo está bloqueado.

  Para dispositivos iOS 11 y iPadOS 12 (versión mínima): Al confirmar el borrado completo, puede optar por conservar el plan de datos móviles en el dispositivo.

  For iOS 11.3 devices (minimum version): When you confirm the full wipe, you prevent iOS devices from doing proximity setup. When setting up a new iOS device, users can normally use an already configured iOS device to set up their own. You can block proximity setup on devices that are Citrix Endpoint Management managed and have been wiped.

  Para dispositivos iOS 17 (versión mínima): Al confirmar el borrado completo, el dispositivo borra automáticamente todos los datos del usuario, se conecta a la red Wi-Fi especificada y se vuelve a inscribir en el servidor MDM utilizando el perfil de inscripción proporcionado.
- Si el usuario del dispositivo apaga el dispositivo antes de que se elimine el contenido de la tarjeta de memoria, el usuario aún podría tener acceso a los datos del dispositivo.
- Puede cancelar la solicitud de borrado hasta que la solicitud se envíe al dispositivo.

- **Localizar:** Localiza un dispositivo e informa de la ubicación del dispositivo, incluido un mapa, en la página **Administrar > Dispositivos**, en **Detalles del dispositivo > General**. Localizar es una acción única. Utilice **Localizar** para mostrar la ubicación actual del dispositivo en el momento en que realiza la acción. Para rastrear continuamente el dispositivo durante un período, utilice **Habilitar seguimiento**.

  - Al aplicar esta acción a dispositivos Android (excepto Android Enterprise) o a dispositivos Android Enterprise (propiedad de la empresa o BYOD), tenga en cuenta el siguiente comportamiento:

    - **Localizar** requiere que el usuario otorgue permiso de ubicación durante la inscripción. El usuario puede optar por no otorgar permiso de ubicación. Si el usuario no otorga el permiso durante la inscripción, Citrix Endpoint Management vuelve a solicitar permiso de ubicación al enviar el comando **Localizar**.

  - Al aplicar esta función a dispositivos iOS o Android Enterprise, tenga en cuenta las siguientes limitaciones:

    - Para dispositivos Android Enterprise, esta solicitud falla a menos que la política de dispositivo de ubicación haya establecido el modo de ubicación del dispositivo en **Alta precisión** o **Ahorro de batería**.

    - Para dispositivos iOS, el comando solo se ejecuta correctamente si los dispositivos están en modo perdido de MDM.

- **Bloquear:** Bloquea un dispositivo de forma remota. Un bloqueo es útil si un dispositivo es robado y debe bloquearse. Citrix Endpoint Management genera entonces un código PIN y lo establece en el dispositivo. Para acceder al dispositivo, el usuario escribe el código PIN. Utilice **Cancelar bloqueo** para quitar el bloqueo de la consola de Citrix Endpoint Management.
- **Bloquear y restablecer contraseña:** Bloquea un dispositivo de forma remota y restablece la contraseña.
    - No compatible con dispositivos que:
        - están inscritos en Android Enterprise en modo de perfil de trabajo y
        - ejecutan versiones de Android anteriores a Android 7.0
    - En dispositivos inscritos en Android Enterprise en modo de perfil de trabajo y que ejecutan Android 7.0 o posterior:
        - La contraseña bloquea el perfil de trabajo. El dispositivo no está bloqueado.
        - Si no se envía una contraseña, o la contraseña enviada no cumple los requisitos y el perfil de trabajo no tiene una contraseña: El dispositivo está bloqueado.
        - Si no se envía una contraseña, o la contraseña enviada no cumple los requisitos, pero el perfil de trabajo tiene una contraseña: El perfil de trabajo está bloqueado, pero el dispositivo no está bloqueado.

> **Nota:**
>
> La funcionalidad de restablecimiento de contraseña solo es compatible con dispositivos BYOD Samsung y el administrador de la consola debe tener permisos `DEVICE_ACTION_CONTAINER_PASSWORD_RESET`.

- **Notificar (Sonar):** Reproduce un sonido en los dispositivos.

> **Nota:**
>
> Esta funcionalidad solo es compatible con dispositivos iOS.

- **Reiniciar:** Reinicia los dispositivos Windows 10 y Windows 11. Para tabletas y PC con Windows, aparece un mensaje sobre el reinicio pendiente. El reinicio se produce en cinco minutos.
- **Solicitar/Detener Duplicación de AirPlay:** Inicia y detiene la duplicación de AirPlay en dispositivos iOS supervisados.
- **Reiniciar/Apagar:** Reinicia o apaga inmediatamente los dispositivos supervisados.

> **Nota:**
>
> Esta funcionalidad solo es compatible con dispositivos iOS.

- **Revocar:** Impide que un dispositivo se conecte a Citrix Endpoint Management.
- **Revocar/Autorizar:** Realiza las mismas acciones que un Borrado selectivo. Después de la revocación, puede volver a autorizar el dispositivo para volver a inscribirlo.
- **Sonar:** Si el dispositivo está en Modo Perdido, Sonar reproduce un sonido en un dispositivo iOS supervisado. El sonido se reproduce hasta que se quita el dispositivo del Modo Perdido o el usuario desactiva el sonido.
- **Rotar clave de recuperación personal:** Si ha habilitado la directiva de dispositivo FileVault, esta acción genera una nueva clave de recuperación personal y reemplaza la clave antigua por esta nueva clave. Puede cancelar esta solicitud mientras la solicitud aún esté pendiente. Para ello, haga clic en **Cancelar rotación de clave de recuperación personal**.
- **Borrado selectivo:** Borra todos los datos y aplicaciones corporativos de un dispositivo, dejando los datos y aplicaciones personales en su lugar. Después de un borrado selectivo, use la acción **Autorizar** para volver a autorizar el dispositivo y que un usuario pueda volver a inscribirlo. Los dispositivos borrados permanecen en la lista de dispositivos en la página **Administrar > Dispositivos** con fines de auditoría. Puede eliminar un dispositivo borrado de la lista de dispositivos.
    - El borrado selectivo de un dispositivo Android no desconectar el dispositivo de Device Manager y de la red corporativa. Para evitar que el dispositivo acceda a Device Manager, también debe revocar los certificados del dispositivo.
    - El borrado selectivo de un dispositivo Android también revoca el dispositivo. Puede volver a inscribir el dispositivo solo después de volver a autorizarlo o de eliminarlo de la consola.
    - Para dispositivos Android Enterprise totalmente administrados con un perfil de trabajo (dispositivos COPE), puede realizar un borrado completo después de que un borrado

selectivo elimine el perfil de trabajo. O bien, puede volver a inscribir el dispositivo con el mismo nombre de usuario. Volver a inscribir el dispositivo recrea el perfil de trabajo.

- Para dispositivos iOS y macOS, este comando elimina cualquier perfil instalado a través de MDM.
- Un borrado selectivo en un dispositivo Windows también elimina el contenido de la carpeta de perfil de cualquier usuario que haya iniciado sesión actualmente. Un borrado selectivo no elimina ningún clip web que entregue a los usuarios a través de una configuración. Para eliminar los clips web, los usuarios deben anular manualmente la inscripción de sus dispositivos. No puede volver a inscribir un dispositivo borrado selectivamente.

- **Desbloquear:** Borra el código de acceso enviado al dispositivo cuando estaba bloqueado. Este comando no abre el dispositivo.

En **Administrar > Dispositivos**, la página **Detalles del dispositivo** también enumera las propiedades de seguridad del dispositivo. Esas propiedades incluyen ID seguro, Bloquear dispositivo, Omisión de bloqueo de activación y otra información para el tipo de plataforma. El campo **Borrado completo del dispositivo** incluye el código PIN del usuario. El usuario debe introducir ese código después de borrar el dispositivo. Si el usuario olvida el código, puede buscarlo aquí.

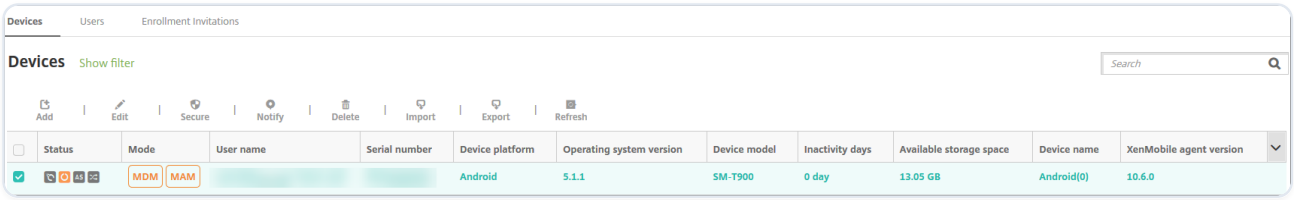
Puede automatizar algunas acciones. Para obtener más información, consulte Acciones automatizadas.

Eliminar un dispositivo de la consola de Citrix Endpoint Management

> **Importante:**

> Cuando se elimina un dispositivo de la consola de Citrix Endpoint Management, las aplicaciones y los datos administrados permanecen en el dispositivo. Para eliminar las aplicaciones y los datos administrados del dispositivo, consulte "Eliminar un dispositivo" más adelante en este artículo.

> Para eliminar un dispositivo de la consola de Citrix Endpoint Management, vaya a **Administrar > Dispositivos**, seleccione un dispositivo administrado y, a continuación, haga clic en **Eliminar**.



Borrar un dispositivo de forma selectiva

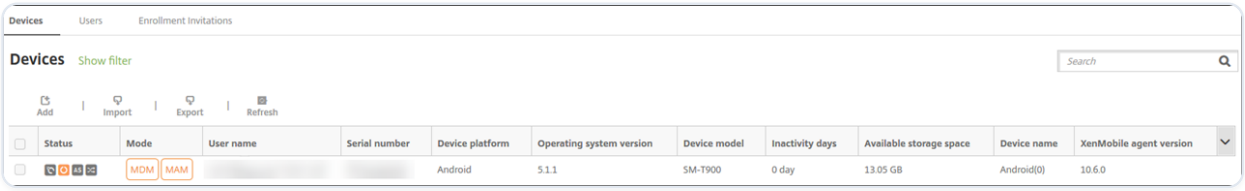
1. Vaya a **Administrar > Dispositivos**, seleccione un dispositivo administrado y, a continuación, haga clic en **Proteger**.
2. En **Acciones de seguridad**, haga clic en **Borrado selectivo**.
3. Solo para dispositivos Android, desconectar el dispositivo de la red corporativa: Después de borrar el dispositivo, en **Acciones de seguridad**, haga clic en **Revocar**.

   Para retirar una solicitud de borrado selectivo antes de que se produzca el borrado, en **Acciones de seguridad**, haga clic en **Cancelar borrado selectivo**.

Eliminar un dispositivo

Este procedimiento elimina las aplicaciones y los datos administrados del dispositivo y elimina el dispositivo de la lista de Dispositivos en la consola de Citrix Endpoint Management. Puede usar la API REST pública de Citrix Endpoint Management para eliminar dispositivos de forma masiva.

1. Vaya a **Administrar > Dispositivos**, seleccione un dispositivo administrado y, a continuación, haga clic en **Proteger**.
2. Haga clic en **Borrado selectivo**. Cuando se le solicite, haga clic en **Realizar borrado selectivo**.
3. Para verificar que el comando de borrado se realizó correctamente, actualice **Administrar > Dispositivos**. En la columna **Modo**, el color ámbar para MDM y MAM indica que el comando de borrado se realizó correctamente.



4. En **Administrar > Dispositivos**, seleccione el dispositivo y, a continuación, haga clic en **Eliminar**. Cuando se le solicite, haga clic en **Eliminar** de nuevo.

Bloquear, desbloquear, borrar o recuperar aplicaciones

1. Vaya a **Administrar > Dispositivos**, seleccione un dispositivo administrado y, a continuación, haga clic en **Proteger**.
2. En **Acciones de seguridad**, haga clic en la acción de la aplicación.

   También puede usar el cuadro **Acciones de seguridad** para comprobar el estado del dispositivo de un usuario cuya cuenta está inhabilitada o eliminada de Active Directory. La presencia de las acciones Desbloquear aplicación o Recuperar aplicación indica que las aplicaciones están bloqueadas o borradas.

Borrado y recuperación de aplicaciones

1. Vaya a **Administrar > Dispositivos**. Seleccione un dispositivo.
2. Borrado de apps
   - Haga clic en **Proteger > Borrar aplicación**. Aparece un cuadro de diálogo con el siguiente mensaje: **¿Está seguro de que desea borrar las aplicaciones de este dispositivo?** Haga clic en **Borrar aplicación**.
3. Recuperación de apps
   - Haga clic en **Proteger > Recuperar aplicación**. Aparece un cuadro de diálogo con el siguiente mensaje: **¿Está seguro de que desea recuperar las aplicaciones de este dispositivo?** Haga clic en **Recuperar aplicación del dispositivo**.
4. Vuelva a inscribir el dispositivo como el mismo usuario, en el mismo modo.
5. Inicie una aplicación MDX desde la página **Mis aplicaciones**.
6. Inicie Citrix Secure Hub.

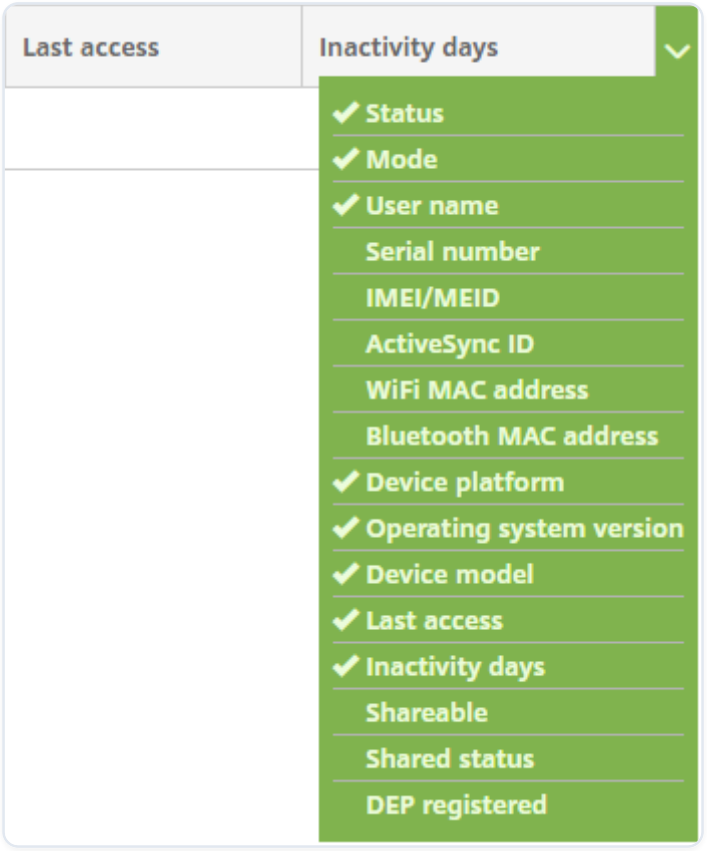
Obtener información sobre los dispositivos

La base de datos de Citrix Endpoint Management almacena una lista de dispositivos móviles. Para rellenar la consola de Citrix Endpoint Management con sus dispositivos, puede agregarlos manualmente o importar una lista de dispositivos desde un archivo. Para obtener más información sobre los formatos de archivo de aprovisionamiento de dispositivos, consulte Formatos de archivo de aprovisionamiento de dispositivos más adelante en este artículo.

La página **Administrar > Dispositivos** de la consola de Citrix Endpoint Management enumera cada dispositivo y la siguiente información:

- **Estado:** Los iconos indican si el dispositivo tiene jailbreak, si está administrado, si ActiveSync Gateway está disponible y el estado de implementación.
- **Modo:** Indica el modo del dispositivo, como MDM o MDM+MAM.
- Otra información sobre el dispositivo, como **Nombre de usuario**, **Plataforma del dispositivo**, **Último acceso** y **Días de inactividad**. Esos encabezados son los que se muestran de forma predeterminada.

Para personalizar la tabla **Dispositivos**, haga clic en la flecha hacia abajo del último encabezado. A continuación, seleccione los encabezados adicionales que desea ver en la tabla o desactive cualquier encabezado para eliminarlos.

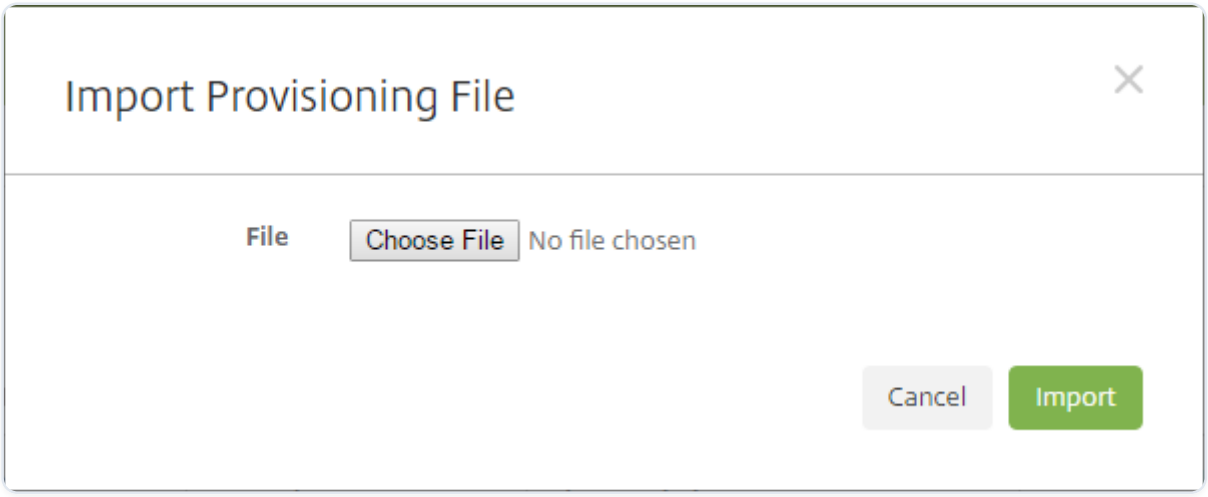


Puede agregar dispositivos manualmente, importar dispositivos desde un archivo de aprovisionamiento de dispositivos, editar los detalles del dispositivo, personalizar las propiedades de usuario de Active Directory, realizar acciones de seguridad y enviar notificaciones a los dispositivos. También puede exportar todos los datos de la tabla de dispositivos a un archivo .csv para crear un informe personalizado. El servidor exporta todos los atributos del dispositivo. Si aplica filtros, Citrix Endpoint Management los utiliza al crear el archivo .csv.

Importar dispositivos desde un archivo de aprovisionamiento

Puede importar un archivo proporcionado por operadores de telefonía móvil o fabricantes de dispositivos, o puede crear su propio archivo de aprovisionamiento de dispositivos. Para obtener más información, consulte Formatos de archivo de aprovisionamiento de dispositivos más adelante en este artículo.

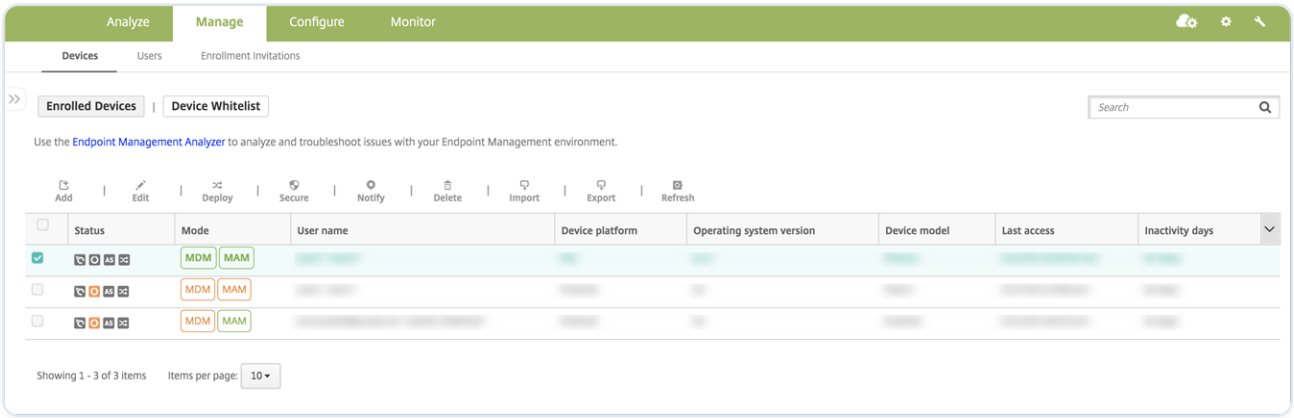
1. Vaya a **Administrar > Dispositivos** y, a continuación, haga clic en **Importar**. Aparecerá el cuadro de diálogo **Importar archivo de aprovisionamiento**.



2. Haga clic en **Elegir archivo** y, a continuación, vaya al archivo que quiere importar.
3. Haga clic en **Importar**. La tabla **Dispositivos** muestra el archivo importado.
4. Para modificar la información del dispositivo, selecciónelo y haga clic en **Modificar**. Para obtener información sobre las páginas de **Detalles del dispositivo**, consulte Obtener información sobre los dispositivos.

Implementar en un dispositivo

Puede forzar a uno o varios dispositivos a conectarse con Citrix Endpoint Management. Los dispositivos seleccionados reciben los recursos inmediatamente sin esperar a la siguiente comprobación programada.

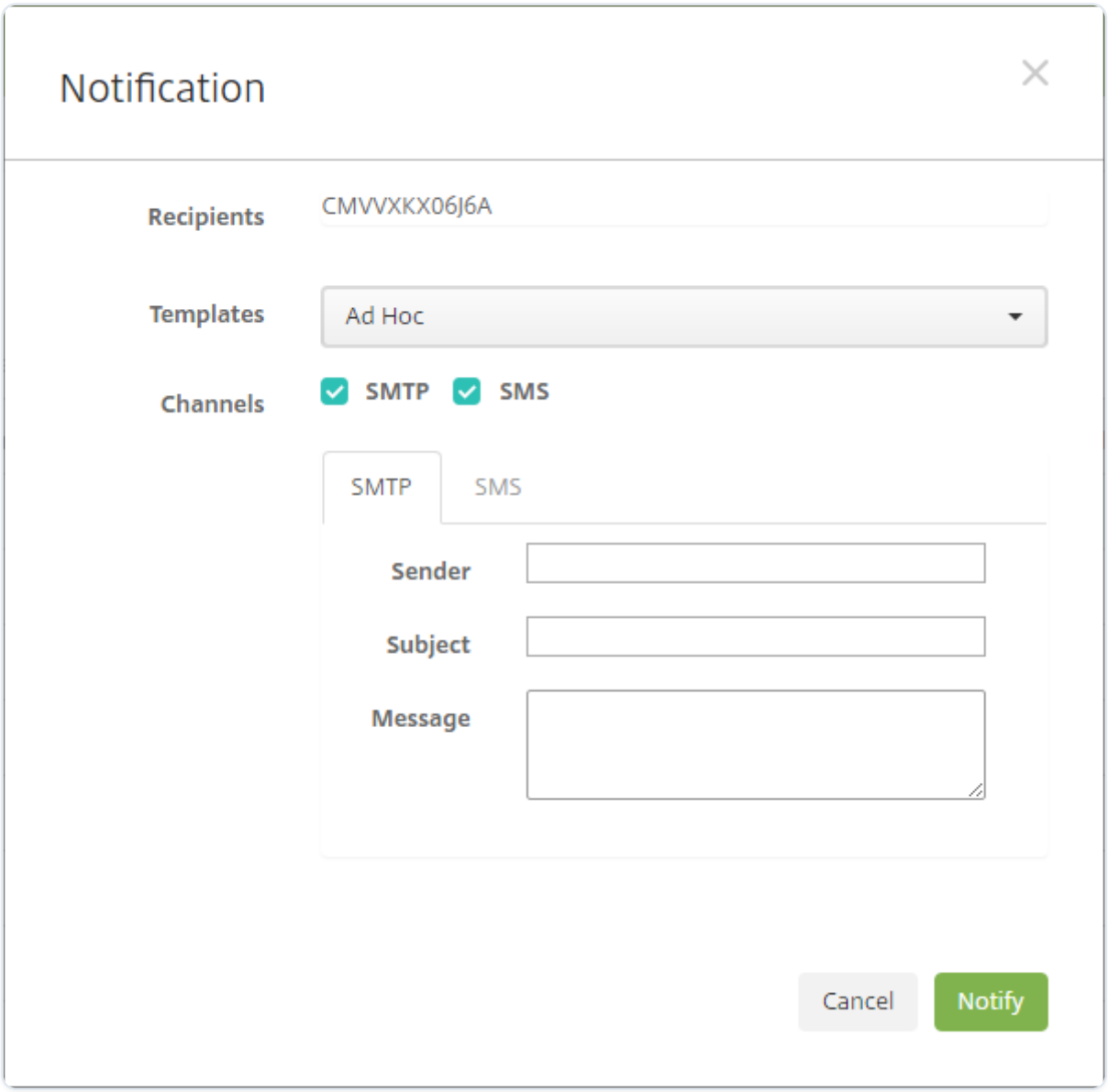


1. Vaya a **Administrar > Dispositivos**, seleccione un dispositivo administrado por MDM o MDM+MAM y, a continuación, haga clic en **Implementar**.
2. En el cuadro de diálogo, haga clic en **Implementar** para confirmar la acción.

Enviar una notificación a los dispositivos

Puede enviar notificaciones a los dispositivos desde la página Dispositivos. Para obtener más información sobre las notificaciones, consulte Notificaciones.

1. En la página **Administrar > Dispositivos**, elija el dispositivo o los dispositivos a los que quiere enviar una notificación.
2. Haga clic en **Notificar**. Aparece el cuadro de diálogo **Notificación**. El campo **Destinatarios** muestra todos los dispositivos que recibirán la notificación.



3. Configure estos ajustes:

   - **Plantillas:** Haga clic en el tipo de notificación que desea enviar en la lista desplegable. Para cada plantilla, excepto **Ad Hoc**, los campos **Asunto** y **Mensaje** muestran el texto configurado para la plantilla que elija.
   - **Canales:** Seleccione cómo enviar el mensaje. El valor predeterminado es **SMTP**. Haga clic en las pestañas para ver el formato del mensaje de cada canal.
   - **Remitente:** Introduzca un remitente opcional.
   - **Asunto:** Introduzca un asunto para un mensaje **Ad Hoc**.
   - **Mensaje:** Introduzca el mensaje para un mensaje **Ad Hoc**.

4. Haga clic en **Notificar**.

Exportar la tabla Dispositivos

1. Filtre la tabla **Dispositivos** según lo que desee que aparezca en el archivo de exportación.
2. Haga clic en el botón **Exportar** encima de la tabla **Dispositivos**. Citrix Endpoint Management extrae la información de la tabla **Dispositivos** filtrada y la convierte a un archivo .csv.
3. Cuando se le solicite, abra o guarde el archivo .csv.

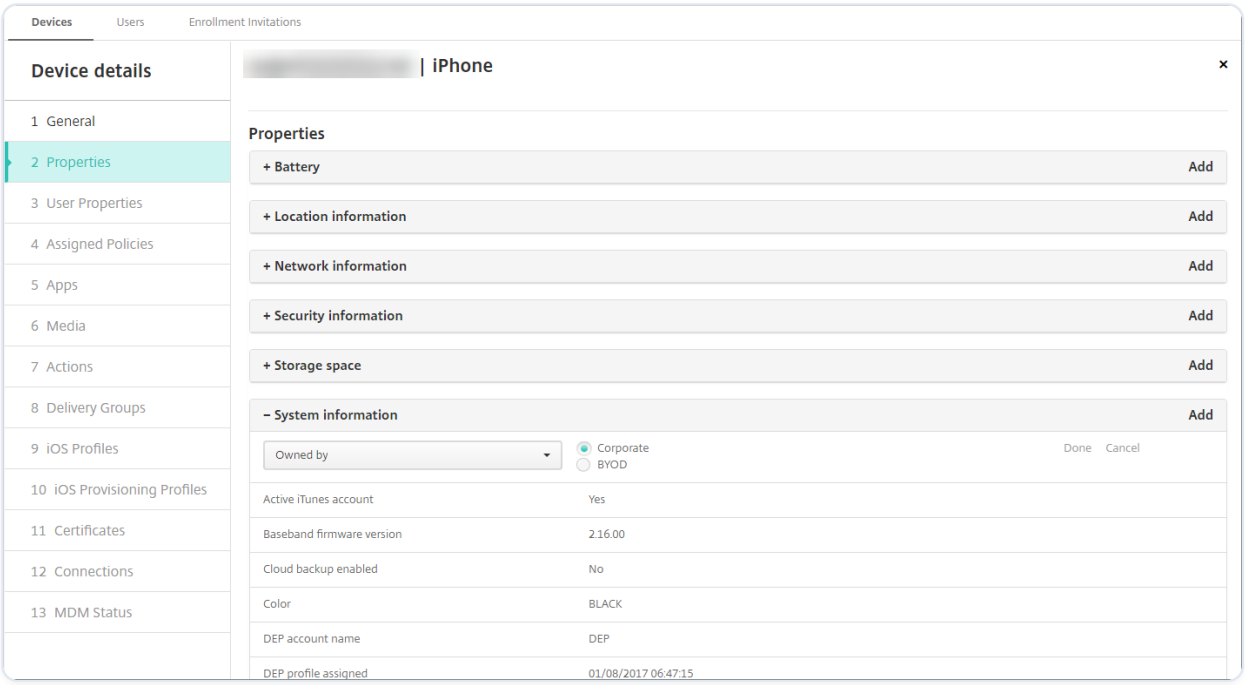
Etiquetar dispositivos de usuario manualmente

Puede etiquetar manualmente un dispositivo en Citrix Endpoint Management de las siguientes maneras:

- Durante el proceso de inscripción basado en invitación.
- Durante el proceso de inscripción del portal de autoservicio.
- Agregando la propiedad del dispositivo como una propiedad del dispositivo

Tiene la opción de etiquetar el dispositivo como propiedad de la empresa o del empleado. Al usar el Portal de autoayuda para auto-inscribir un dispositivo, puede etiquetar el dispositivo como propiedad de la empresa o del empleado. También puede etiquetar un dispositivo manualmente, de la siguiente manera.

1. Agregue una propiedad al dispositivo desde la ficha **Dispositivos** en la consola de Citrix Endpoint Management.
2. Agregue la propiedad denominada **Propiedad de** y elija **Empresa** o **BYOD** (propiedad del empleado).



Personalizar atributos de usuario de Active Directory

Puede personalizar ciertos atributos de usuario de Active Directory para definir a qué atributos puede acceder Citrix Endpoint Management para crear una cuenta de usuario.

Para ver la lista de atributos, agregue la propiedad de servidor `optional.user.identity.attributes` como clave personalizada en **Parámetros > Propiedades del servidor**. En el campo **Valores**, puede quitar y restaurar más tarde los atributos de usuario opcionales de Active Directory que Citrix Endpoint Management proporciona de forma predeterminada. Para obtener más información, consulte Propiedades del servidor.

Después de editar la lista de valores predeterminados y guardar los cambios, puede ver los atributos de usuario de Active Directory actualizados en **Administrar > Dispositivos > Propiedades de usuario**. Citrix Endpoint Management actualiza la consola después de que el usuario inicia sesión en el dispositivo o durante la siguiente comprobación programada del dispositivo. Si comete un error ortográfico o agrega un valor no admitido, Citrix Endpoint Management ignora los cambios.

Quitar los atributos de usuario opcionales de Active Directory puede afectar a las siguientes funcionalidades:

- **Aprovisionamiento de la cuenta de usuario:** Si quita los valores de nombre y apellido, Citrix Endpoint Management no puede aprovisionar la cuenta de usuario para ShareFile y Salesforce.

- **Invitaciones de inscripción:** Si quita los detalles de correo electrónico o teléfono móvil del usuario, el usuario no puede recibir una invitación de inscripción.
- **Acciones de notificación de dispositivos:** Si quita los detalles de correo electrónico del usuario, el usuario no puede recibir las notificaciones a través de SMTP.
- **Inicio de sesión único en Citrix Secure Mail:** Si quita el valor del nombre para mostrar, el usuario no puede iniciar sesión en Citrix Secure Mail mediante el inicio de sesión único.
- **Propiedades de usuario y reglas de implementación:** Si quita cualquiera de los atributos opcionales que utiliza para configurar las propiedades de usuario y las reglas de implementación, puede afectar a las configuraciones existentes.
- **Acciones:** Si quita cualquiera de los atributos opcionales que utiliza para establecer una acción automatizada en **Configurar > Acciones**, puede afectar a las configuraciones existentes.
- **Informes personalizados:** Si elimina alguno de los atributos opcionales que utiliza en los informes personalizados, puede afectar a las configuraciones existentes.

Buscar dispositivos

Para una búsqueda rápida, el ámbito de búsqueda predeterminado incluye las siguientes propiedades del dispositivo:

- Número de serie
- IMEI
- Dirección MAC de Wi-Fi
- Dirección MAC de Bluetooth
- ID de Active Sync
- Nombre de usuario

Puede configurar el ámbito de búsqueda mediante una propiedad de servidor **include.device.properties.during.search**, que de forma predeterminada es **false**. Para incluir todas las propiedades del dispositivo en una búsqueda de dispositivos, vaya a **Parámetros > Propiedades del servidor** y cambie la configuración a **true**.

Formatos de archivo de aprovisionamiento de dispositivos

Muchos operadores de telefonía móvil o fabricantes de dispositivos proporcionan listas de dispositivos móviles autorizados. Puede usar estas listas para evitar tener que introducir

manualmente una larga lista de dispositivos móviles. Citrix Endpoint Management admite un formato de archivo de importación común a estos tipos de dispositivos compatibles: Android, iOS y Windows.

Un archivo de aprovisionamiento que cree manualmente debe tener el siguiente formato:

`SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propert`
`propertyNameN;propertyValueN`

Tenga en cuenta lo siguiente:

- Para conocer los valores válidos de cada propiedad, consulte el PDF Nombres y valores de las propiedades de los dispositivos
- Utilice el juego de caracteres UTF-8.
- Utilice un punto y coma (;) para separar los campos dentro del archivo de aprovisionamiento. Si parte de un campo tiene un punto y coma, escápelo con una barra invertida (\\).

  Por ejemplo, para esta propiedad:

  `propertyV;test;1;2`

  Escápelo de la siguiente manera:

  `propertyV\;test\;1\;2`
- El número de serie es obligatorio para los dispositivos iOS porque el número de serie es el identificador del dispositivo iOS.
- Para otras plataformas de dispositivos, debe incluir el número de serie o el IMEI.
- Los valores válidos para **OperatingSystemFamily** son **WINDOWS**, **ANDROID** o **iOS**.

Ejemplo de archivo de aprovisionamiento de dispositivos:

```
`1050BF3F51730108161006551059039l;15244201625379901;WINDOWS;propertyN;prop
ertyV\;test\;1\;2;prop 2

2050BF3F51730108161006551059039l;25244201625379902;ANDROID;propertyN;prope
rtyV$*&&éééétest

3050BF3F51730108161006551059039l;35244201625379903;iOS;test;

4050BF3F51730108161006551059039l;;iOS;test;
```

```
;55244201625379903;ANDROID;test.testé;value;`
```

Cada línea del archivo describe un dispositivo. La primera entrada de esa muestra significa lo siguiente:

- SerialNumber: `1050BF3F5173010816100655105903 91`
- IMEI: `15244201625379901`
- OperatingSystemFamily: `WINDOWS`
- Nombre de la propiedad: `propertyN`
- Valor de la propiedad: `propertyV\;test\;1\;2;prop 2`

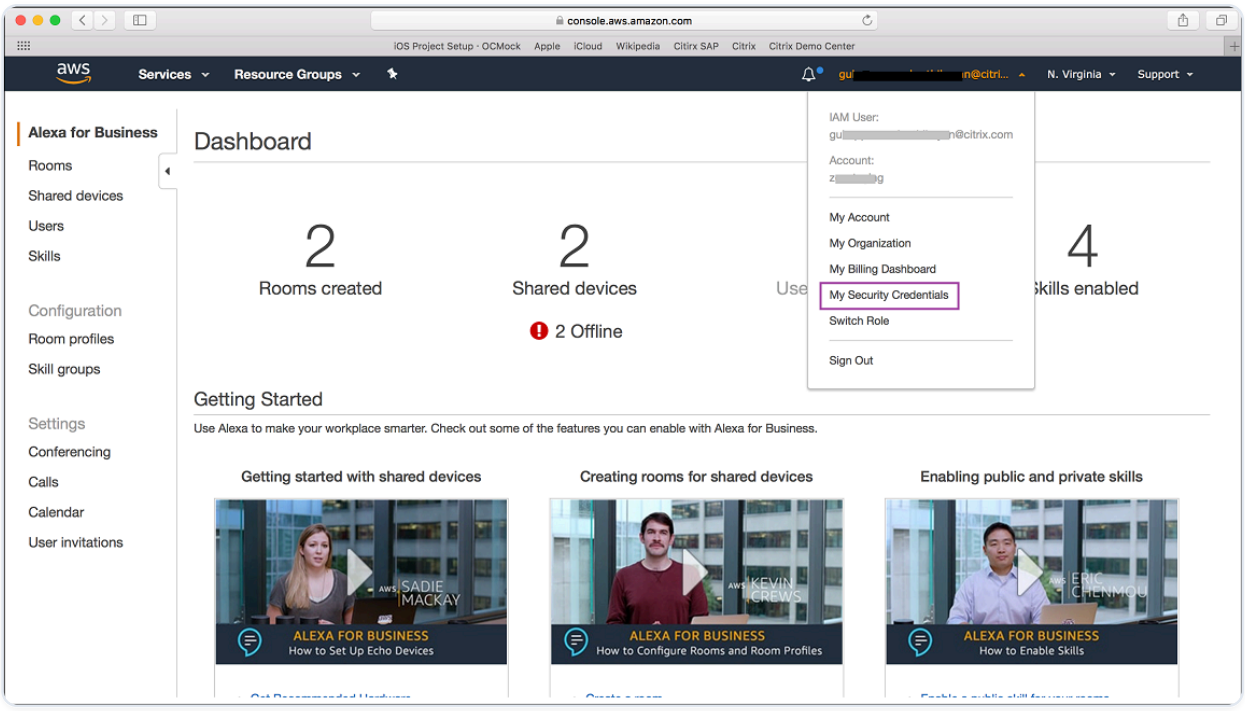
Alexa para empresas

El servicio Alexa for Business de Amazon Web Services (AWS) le permite gestionar un gran número de dispositivos compatibles con Alexa para usos empresariales, como la asistencia en salas de conferencias. Citrix Endpoint Management le permite configurar y gestionar estos dispositivos en la consola de Citrix Endpoint Management. Citrix Endpoint Management no implementa directivas directamente en los dispositivos Alexa. En su lugar, Citrix Endpoint Management actualiza los servicios de AWS y AWS entrega las configuraciones a los dispositivos Alexa.

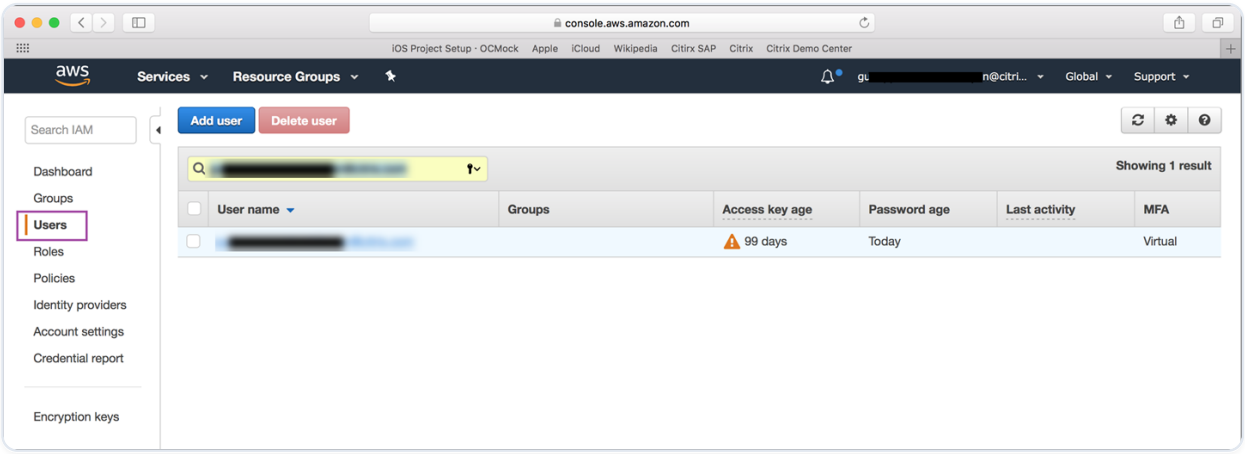
Para obtener información sobre el uso de Alexa for Business, consulte la Guía de administración de Alexa for Business.

Autenticar su cuenta de AWS en Citrix Endpoint Management

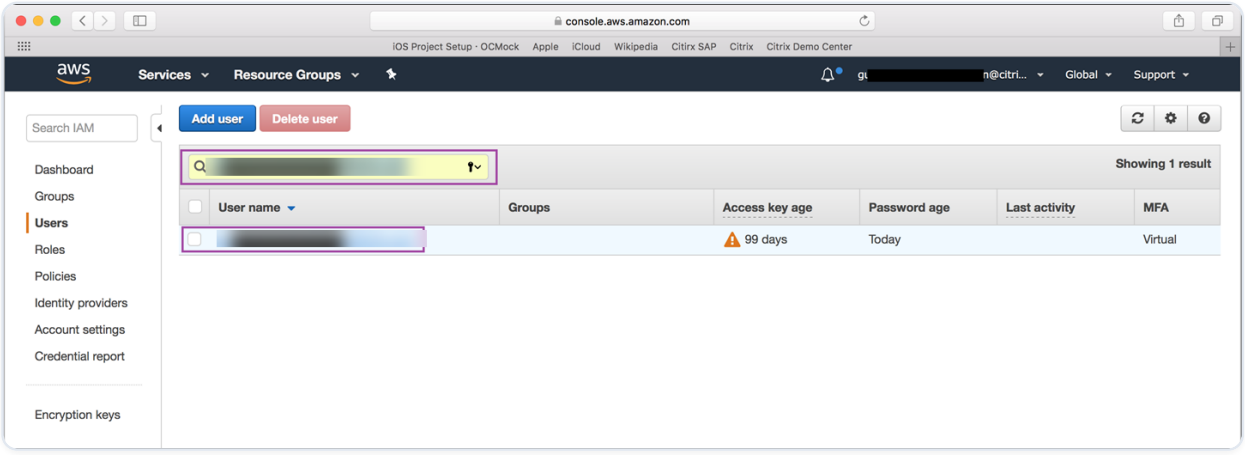
1. Para obtener las credenciales de su cuenta de AWS, inicie sesión en la consola de AWS y seleccione **Mis credenciales de seguridad** en el menú de usuario.



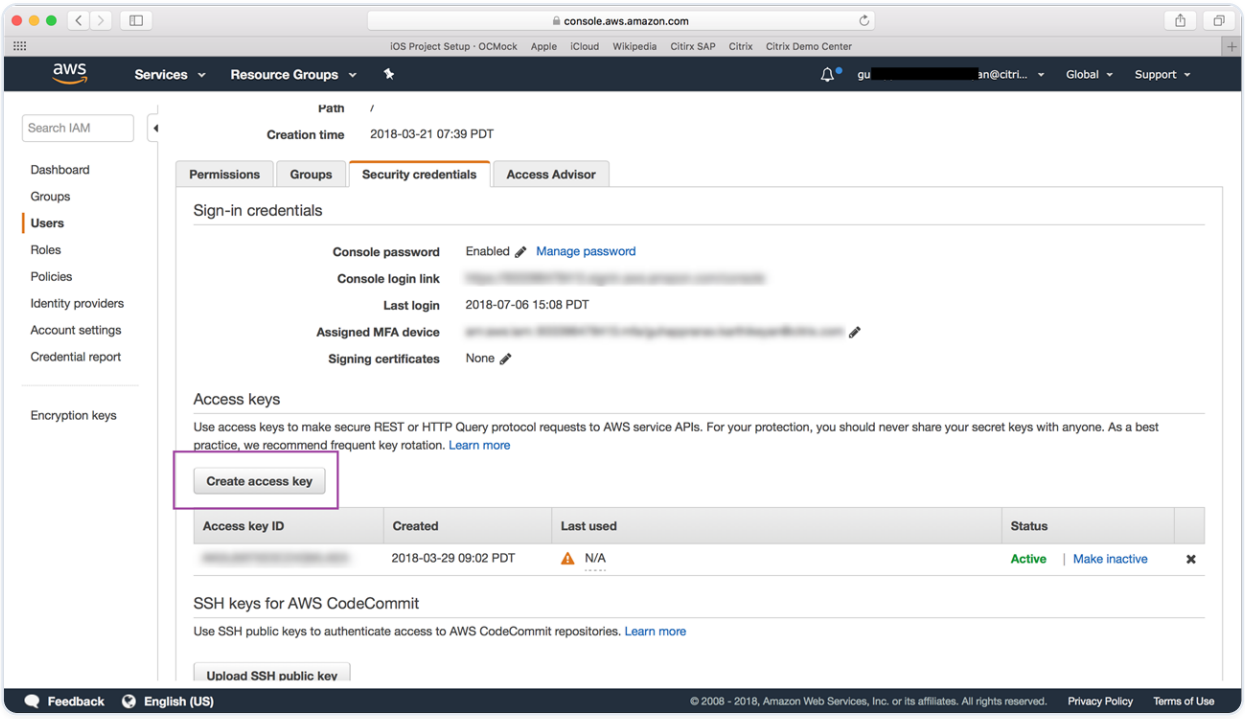
2. Seleccione **Usuarios** en el panel izquierdo.



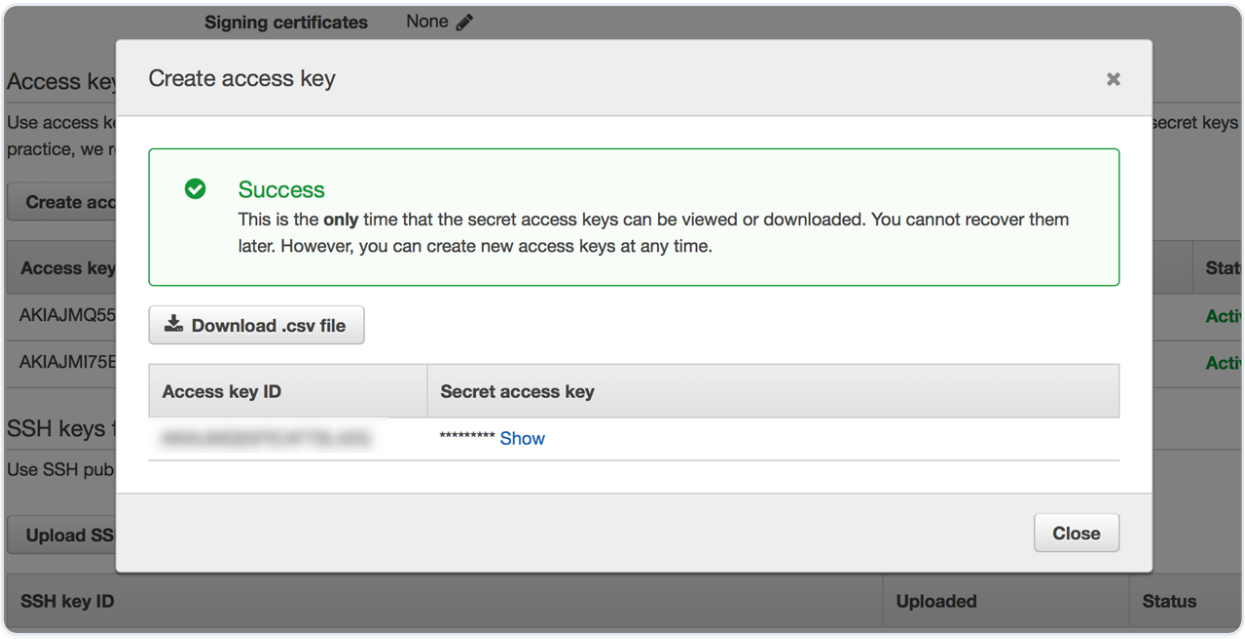
3. Busque su nombre de usuario y, a continuación, selecciónelo.



4. En la ficha **Credenciales de seguridad**, haga clic en **Crear clave de acceso** para generar su ID de clave de acceso y su clave de acceso secreta.

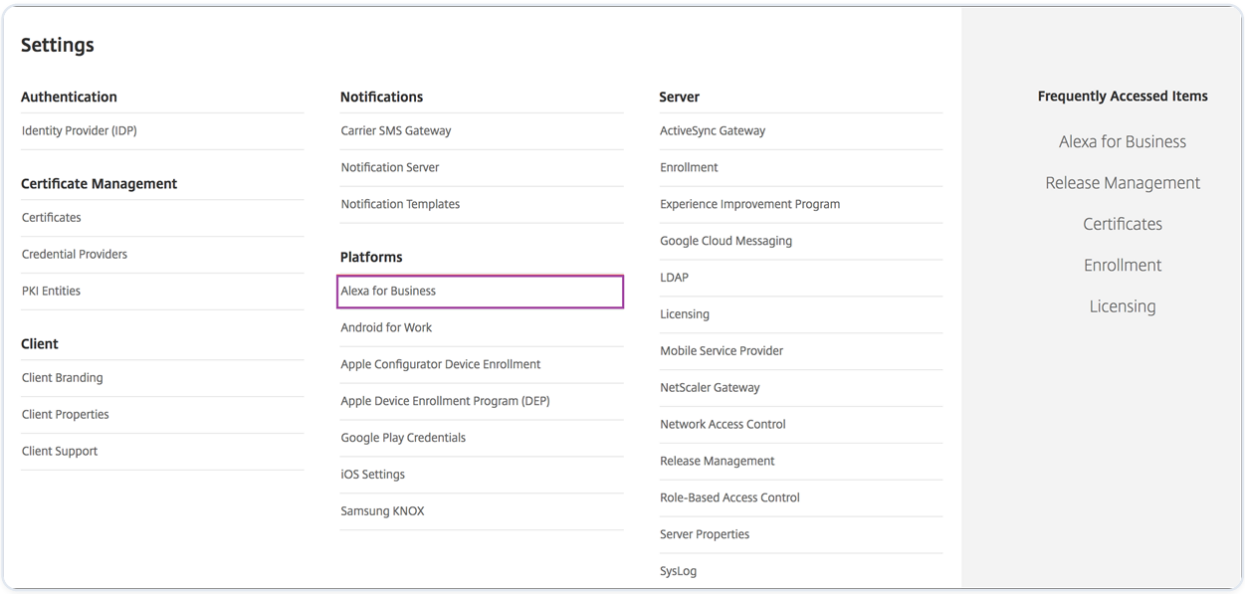


5. Descargue el ID de clave de acceso y la clave de acceso secreta. Guárdelos o anótelos.

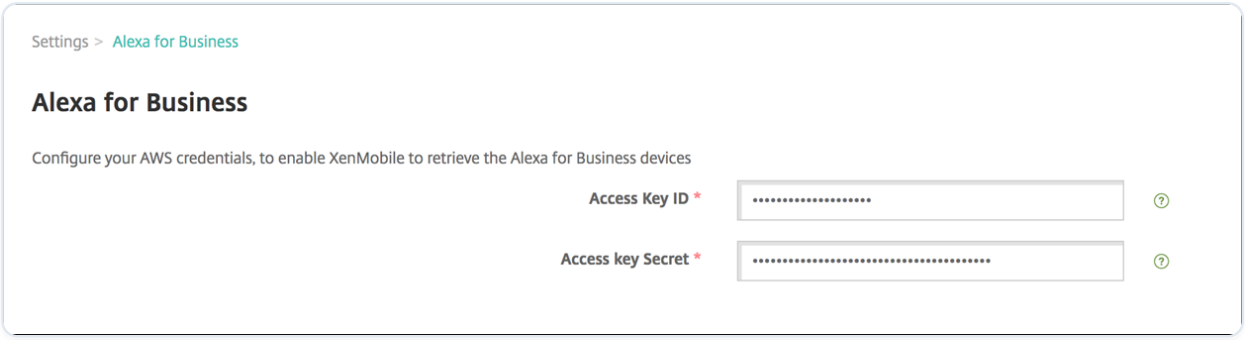


6. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje para ir a **Configuración**.

7. En **Plataformas**, seleccione **Alexa for Business**.



8. Introduzca su ID de clave de acceso y su clave de acceso secreta. Haga clic en **Guardar**.



Configurar Alexa for Business en Citrix Endpoint Management

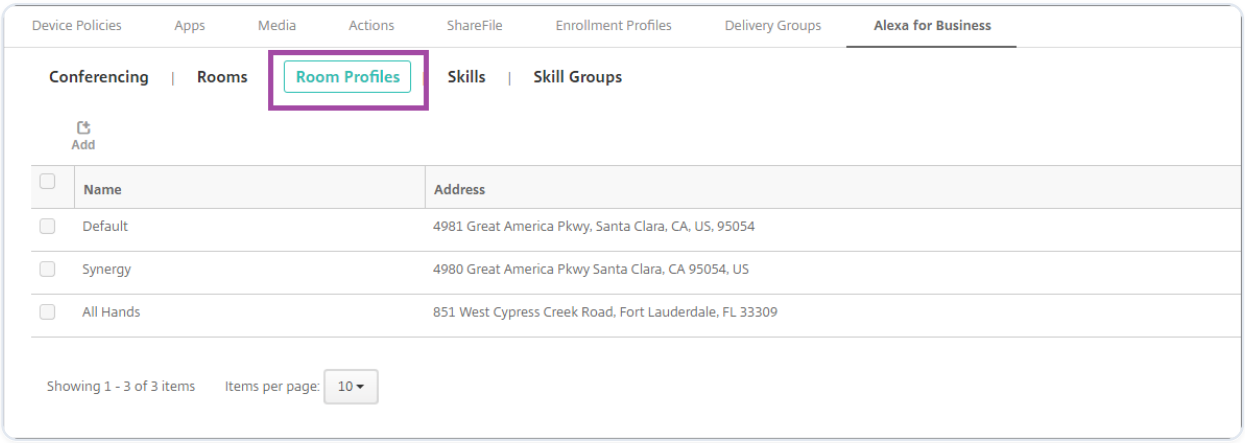
Citrix Endpoint Management le permite configurar:

- Perfiles de sala de configuraciones que se aplican a las salas que tienen dispositivos Alexa
- Salas que representan las salas físicas que tienen los dispositivos
- Grupos de habilidades que asigna a salas o dispositivos
- Habilidades de Alexa de la tienda de habilidades de Alexa que se pueden añadir a grupos de habilidades
- Funciones de conferencia que le permiten elegir un proveedor de conferencias y controlar cómo las personas programan y se unen a las reuniones en sus salas

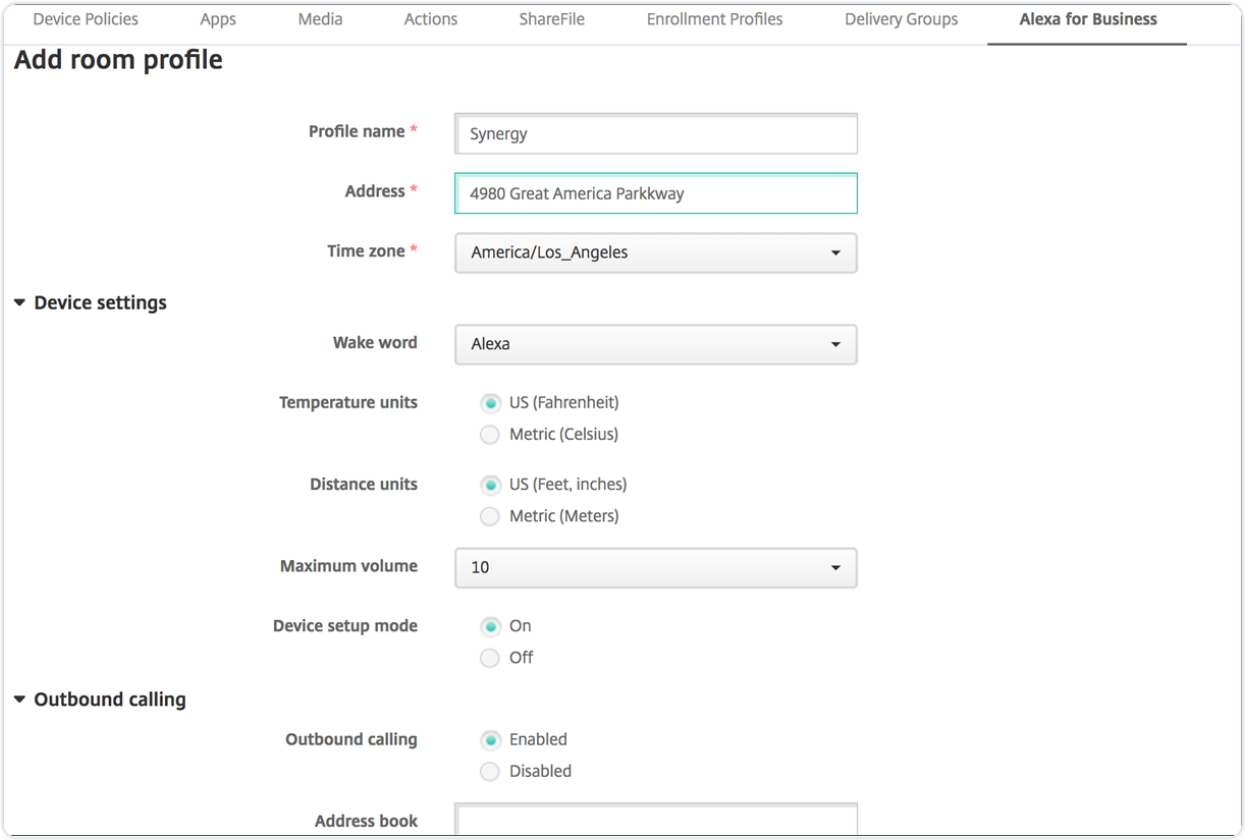
Configurar perfiles de sala

Un perfil de sala es un conjunto de configuraciones comunes que se pueden aplicar a un conjunto de salas que tienen dispositivos Alexa. Puede agregar, modificar y eliminar perfiles de sala.

1. En la consola de Citrix Endpoint Management, seleccione **Configurar > Alexa para empresas > Perfiles de sala**. Aparece la lista de perfiles de sala disponibles.



2. Para agregar un perfil de sala, haga clic en **Agregar**. Para modificar un perfil de sala, seleccione el perfil de sala que quiere modificar y haga clic en **Modificar**.
3. Introduzca la configuración del perfil de sala:



- **Nombre del perfil:** Escriba el nombre del perfil.
- **Dirección:** Escriba la dirección física (calle) del edificio donde se encuentran las salas que tienen los dispositivos Alexa.
- **Zona horaria:** Elija la zona horaria del lugar.
- **Palabra de activación:** Elija la palabra de activación a la que responden los dispositivos Alexa.

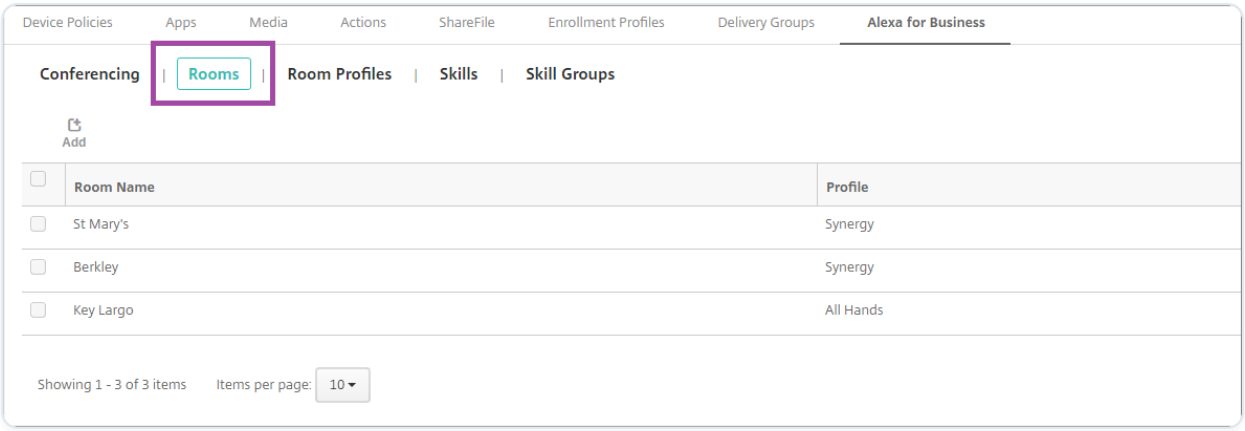
- **Unidades de temperatura:** Seleccione las unidades en las que los dispositivos Alexa informan de la temperatura.
- **Unidades de distancia:** Seleccione las unidades en las que los dispositivos Alexa informan de la distancia.
- **Volumen máximo:** Elija la configuración de volumen máximo para Alexa.
- **Modo de configuración del dispositivo:** Seleccione si los dispositivos Alexa se pueden reconfigurar forzándolos al modo de configuración del dispositivo.
- **Llamadas salientes:** Habilite o deshabilite la capacidad de llamadas salientes de los dispositivos Alexa.
- **Libreta de direcciones:** Configure la libreta de direcciones para los dispositivos Alexa.

4. Haga clic en **Guardar**.

Configurar salas

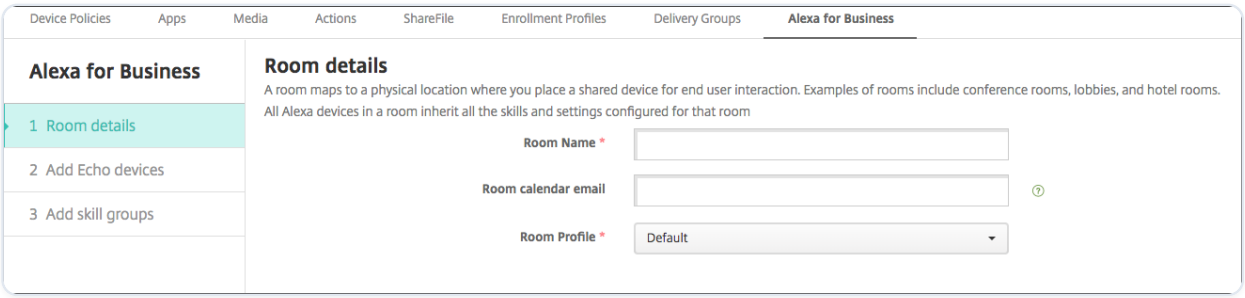
Las salas que configure en la consola de Citrix Endpoint Management representan las salas de conferencias físicas, salas de reuniones y otras salas del edificio. Al configurar una sala, asocia un dispositivo Alexa a la sala y añade un grupo de habilidades al dispositivo. Puede añadir, editar y eliminar salas.

1. En la consola de Citrix Endpoint Management, seleccione **Configurar > Alexa for Business > Salas**. Aparece la lista de salas disponibles.



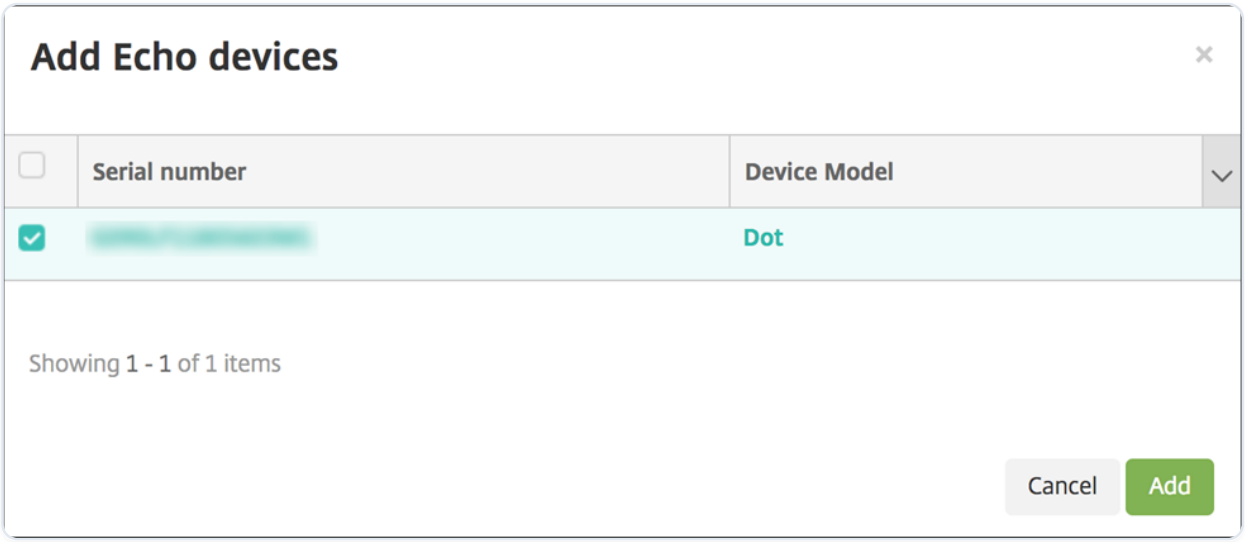
2. Para añadir una sala, haga clic en **Añadir**. Para editar una sala, seleccione la sala que desea editar y haga clic en **Editar**.

3. Introduzca esta configuración de sala:

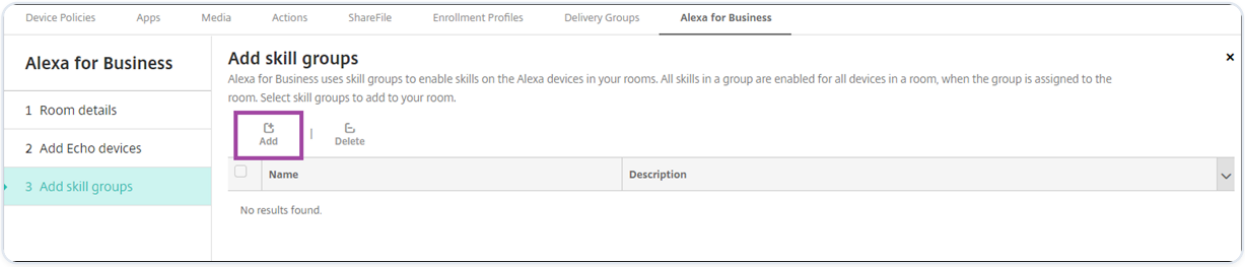


   - **Nombre de la sala:** Escriba el nombre de la sala de conferencias, sala de reuniones u otra sala.
   - **Correo electrónico del calendario de la sala:** Escriba la dirección de correo electrónico del calendario de la sala.
   - **Perfil de la sala:** Elija el nombre de la configuración del perfil de la sala.

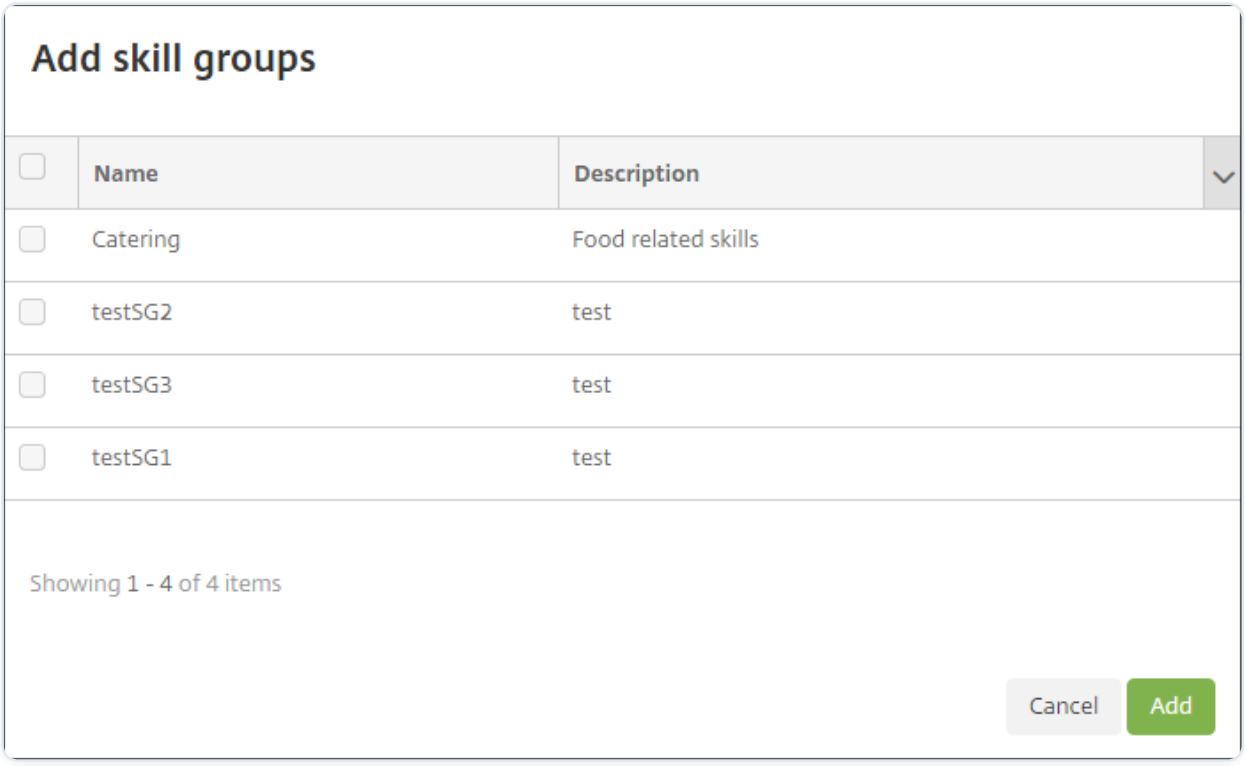
4. Haga clic en **Siguiente**.
5. Para asociar un dispositivo Alexa a la sala, haga clic en **Añadir**.
6. Seleccione un dispositivo y haga clic en **Agregar**. El dispositivo seleccionado aparece en la página **Agregar dispositivos Echo**.



7. Haga clic en **Siguiente**.
8. Para agregar grupos de habilidades a los dispositivos Alexa de la sala, haga clic en **Agregar**.



9. Seleccione los grupos de habilidades que quiere agregar a los dispositivos Alexa de la sala. Haga clic en **Agregar**. Los grupos de habilidades seleccionados aparecen en la página **Agregar grupos de habilidades**.

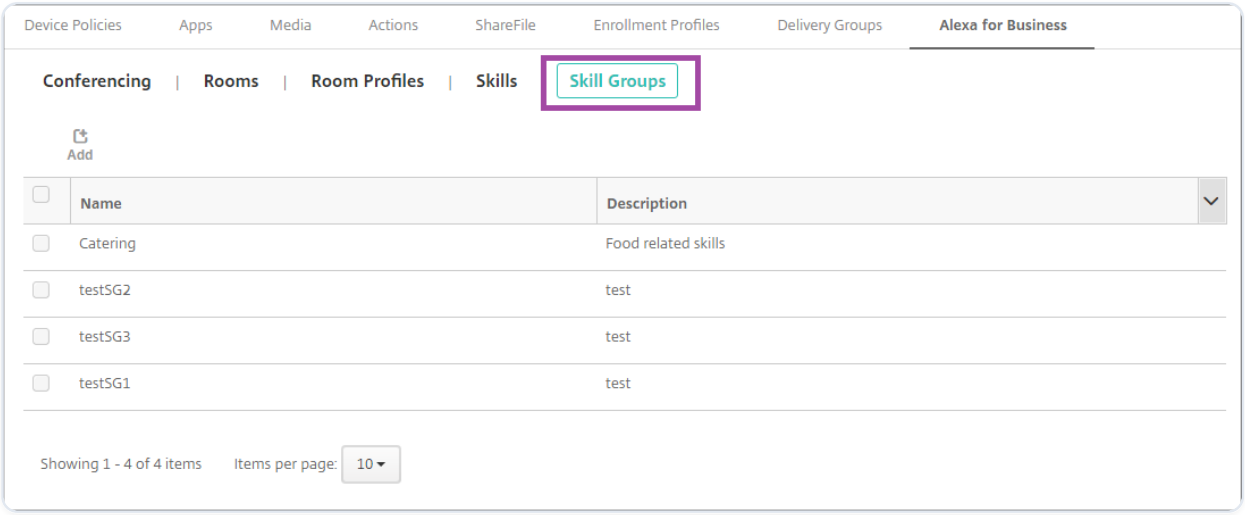


10. Haga clic en **Guardar**.

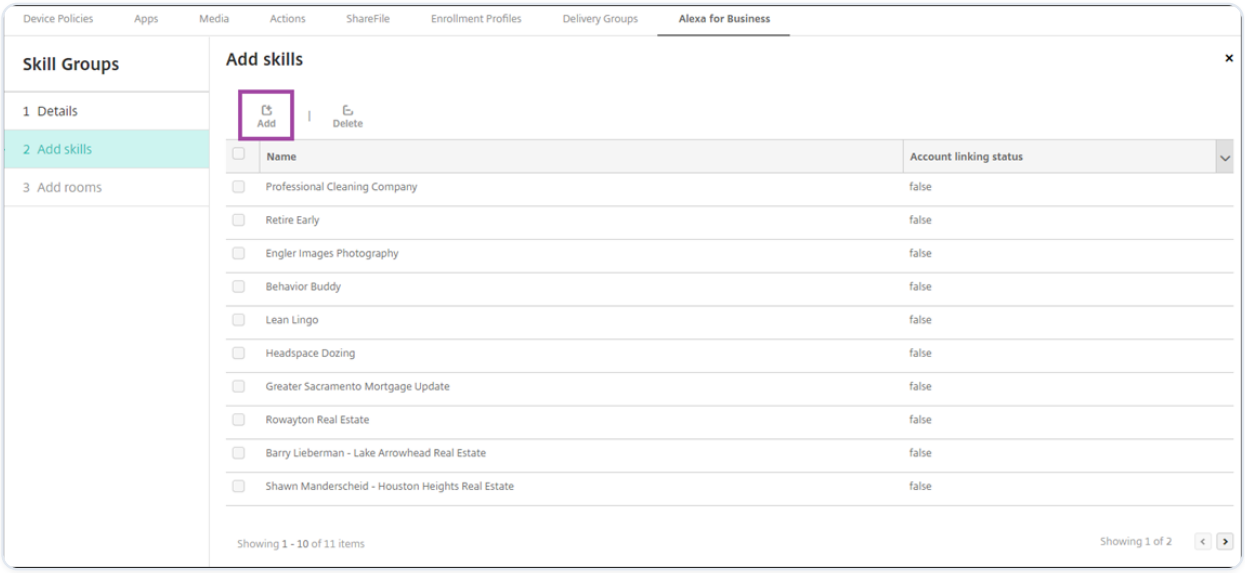
Configurar grupos de habilidades

Los grupos de habilidades son colecciones de habilidades que se pueden aplicar a una sala. Puede crear un grupo de habilidades y luego asignarlo a una sala. Las habilidades le permiten usar un dispositivo Alexa para hacer cosas como iniciar y finalizar una reunión en línea o revisar una lista de elementos de la agenda. Puede agregar, modificar y eliminar grupos de habilidades.

1. En la consola de Citrix Endpoint Management, seleccione **Configurar > Alexa for Business > Grupos de habilidades**. Aparece la lista de grupos de habilidades disponibles.

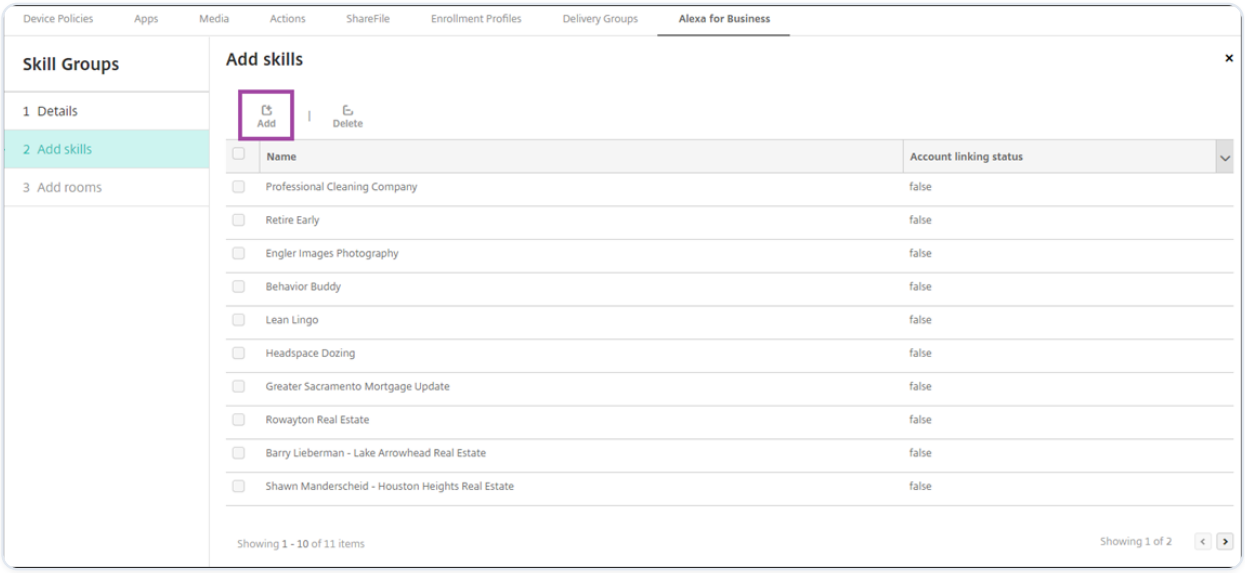


2. Para agregar un grupo de habilidades, haga clic en **Agregar**. Para modificar un grupo de habilidades, seleccione el grupo de habilidades que quiere modificar y haga clic en **Modificar**.
3. Introduzca esta configuración de grupo de habilidades:

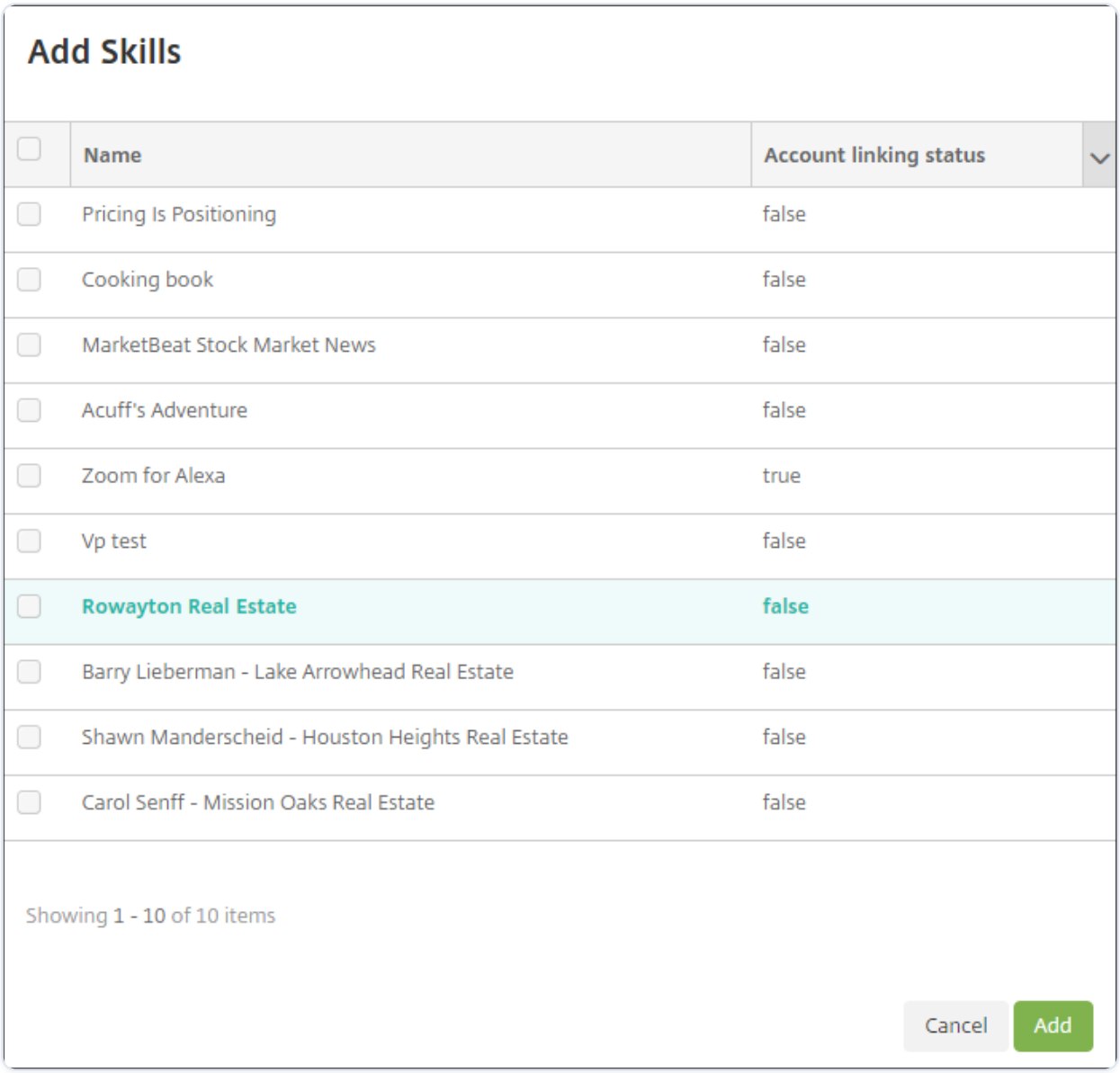


   - **Nombre:** Escriba el nombre del grupo de habilidades.
   - **Descripción:** Escriba una breve descripción del grupo de habilidades.

4. Haga clic en **Siguiente**.
5. Para agregar habilidades al grupo de habilidades, haga clic en **Agregar**.

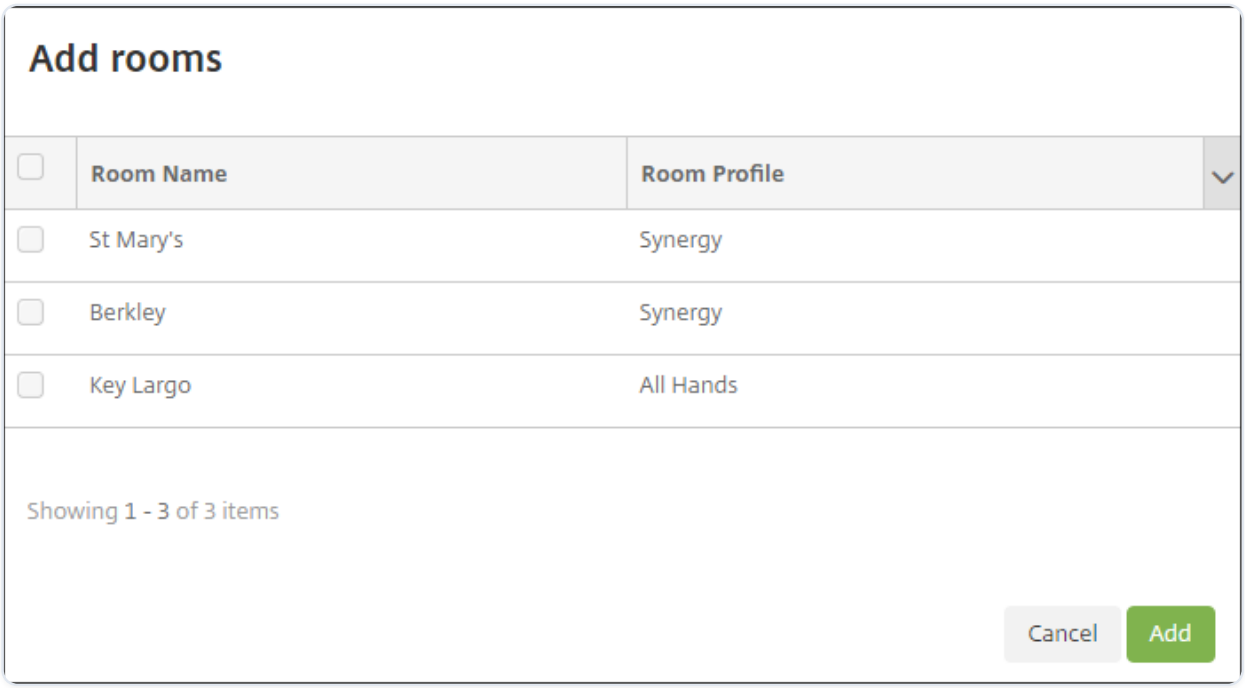


6. Seleccione las habilidades que quiere incluir en el grupo de habilidades y haga clic en **Agregar**. Las habilidades seleccionadas aparecen en la página **Agregar habilidades**.



7. Para añadir el grupo de habilidades a los dispositivos Alexa en las salas que especifique, haga clic en **Añadir**. (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-room-to-group1.png)

8. Seleccione las salas.



9. Haga clic en **Guardar**.

Hacer que las habilidades estén disponibles para los grupos de habilidades

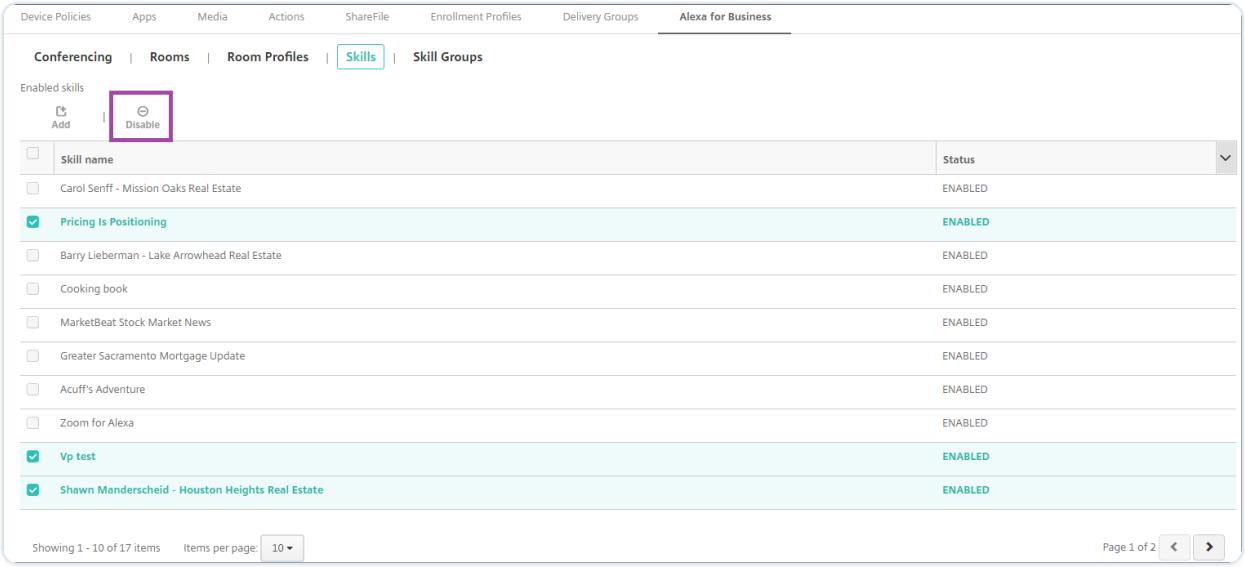
Usted configura la lista de habilidades de Alexa disponibles para ser incluidas en grupos de habilidades en su organización de Alexa for Business. Estas habilidades provienen de la tienda pública de habilidades de Alexa o de habilidades privadas publicadas en su organización.

Añadir habilidades a su organización

1. En la consola de Citrix Endpoint Management, seleccione **Configurar > Alexa for Business > Habilidades**. Aparece la lista de habilidades habilitadas. (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill1.png)
2. Para añadir una habilidad, haga clic en **Añadir**.
3. Para ver más habilidades de Alexa, seleccione una categoría y haga clic en **Mostrar más**. Al hacer clic en **Mostrar más** se añaden hasta 10 habilidades más a la lista de habilidades disponibles para añadir a su organización. Vuelva a hacer clic en **Mostrar más** para añadir más habilidades. (/en-us/citrix-endpoint-management/media/configure-alexa-for-business-skill5.png)
4. Seleccione las habilidades que desea añadir a su organización.
5. Haga clic en **Guardar**.

Eliminar habilidades de su organización

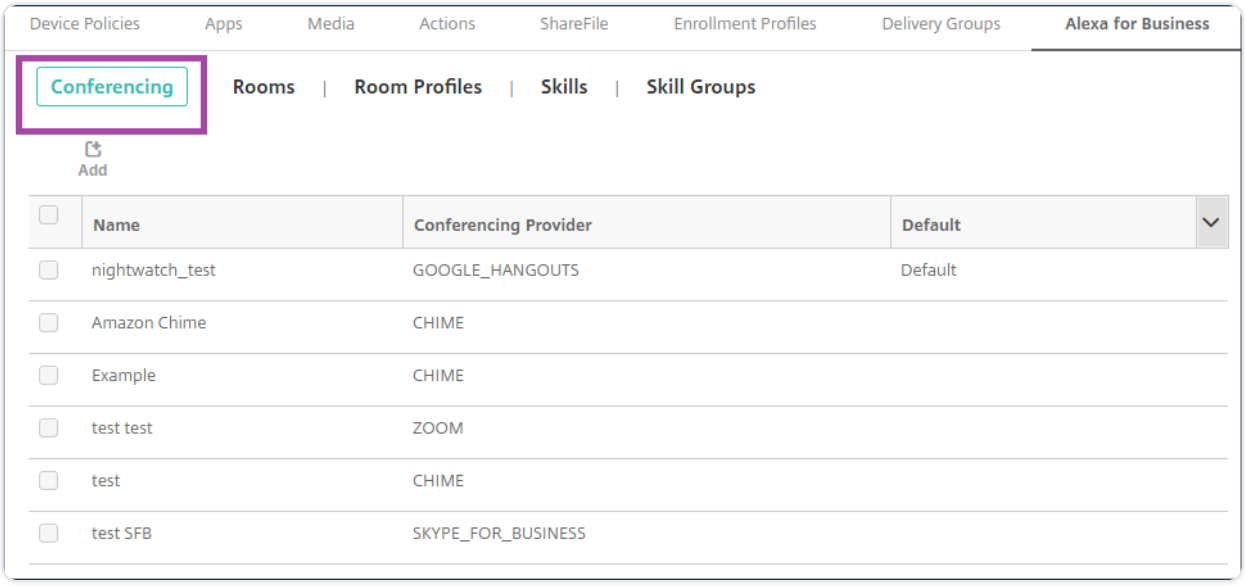
1. En la consola de Citrix Endpoint Management, seleccione **Configurar > Alexa for Business > Habilidades**. Aparece la lista de habilidades habilitadas.
2. Seleccione las habilidades que desea eliminar de su organización.
3. Haga clic en **Deshabilitar**.



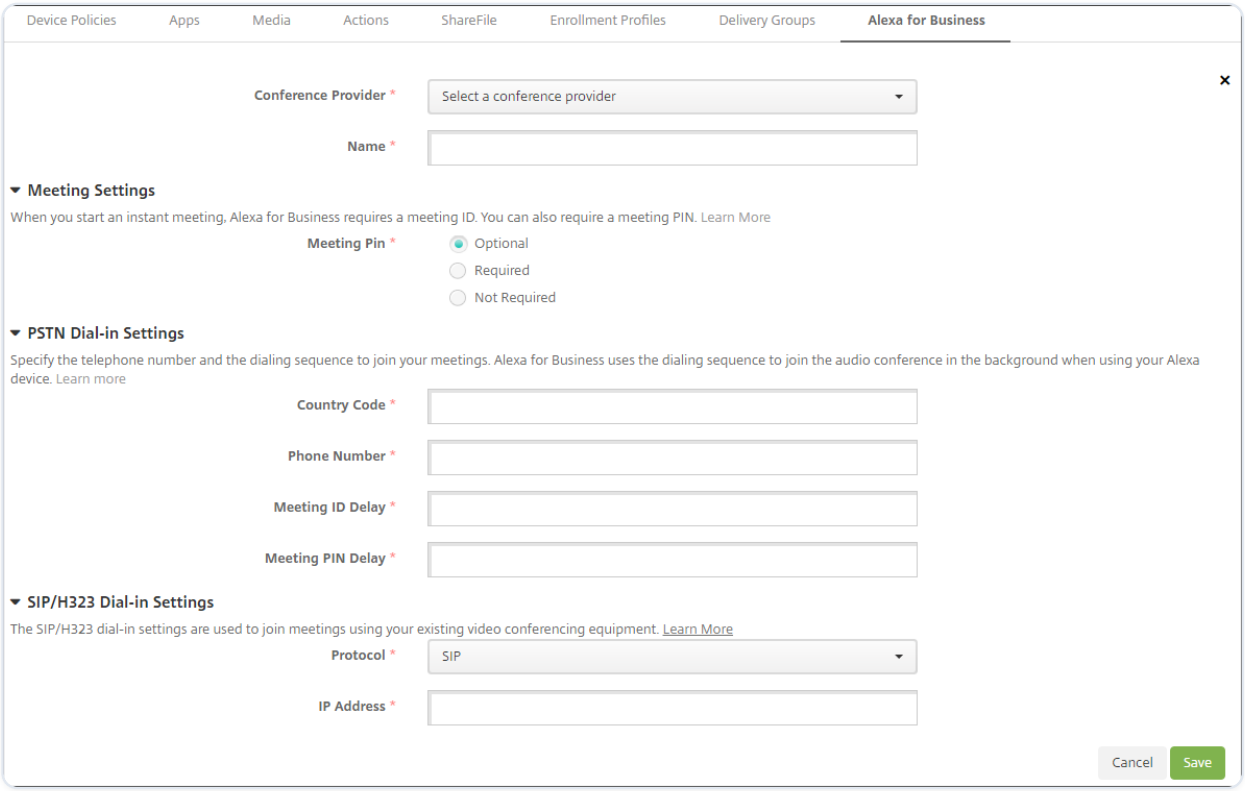
Configurar conferencias

Las funciones de conferencia le permiten configurar proveedores de conferencias, como Google Hangout o Amazon Chime, que controlan cómo las personas se unen a las conferencias en salas que tienen dispositivos Alexa. Puede agregar, editar y eliminar proveedores de conferencias. También puede establecer un proveedor de conferencias predeterminado.

1. En la consola de Citrix Endpoint Management, seleccione **Configurar > Alexa for Business > Conferencias**. Aparecerá la lista de perfiles de sala disponibles.



2. Para agregar un proveedor de conferencias, haga clic en **Agregar**. Para editar un proveedor de conferencias, seleccione el perfil de sala que desea editar y haga clic en **Editar**.
3. Introduzca la configuración del perfil de sala:



- **Proveedor de conferencias:** Seleccione un proveedor de conferencias de la lista.
- **Nombre:** Escriba el nombre que desea dar al proveedor de conferencias.
- **PIN de la reunión:** Especifique si se requiere un PIN para unirse a la reunión.
- **Configuración de marcación PSTN**
  - **Código de país:** Escriba el código de país.
  - **Número de teléfono:** Escriba el número de teléfono.
  - **Retraso del ID de la reunión:** Especifique el número de segundos antes de que se envíe el ID de la reunión.
  - **Retraso del PIN de la reunión:** Especifique el número de segundos antes de que se envíe el PIN.
- **Configuración de marcación SIP/H323** La configuración de marcación SIP/H323 se utiliza para unirse a reuniones utilizando su equipo de videoconferencia existente.
  - **Protocolo:** Seleccione un protocolo.
  - **Dirección IP:** Escriba la dirección IP.

4. Haga clic en **Guardar**.

Si configura más de un proveedor de conferencias, establezca el proveedor predeterminado.

1. En la consola de Citrix Endpoint Management, seleccione **Configurar > Alexa for Business > Conferencias**. Aparece la lista de perfiles de sala disponibles.
2. Seleccione el proveedor de conferencias que quiera establecer como predeterminado.
3. Haga clic en **Establecer como predeterminado**.

Android

Migrar de la administración de dispositivos a Android Enterprise

Este artículo aborda consideraciones y recomendaciones para migrar de la administración de dispositivos Android heredada a Android Enterprise. Google está dejando de usar la API de administración de dispositivos Android. Esa API admitía aplicaciones empresariales en dispositivos Android. Android Enterprise es la solución de administración moderna recomendada por Google y Citrix.

Citrix Endpoint Management está cambiando a Android Enterprise como método de inscripción predeterminado para dispositivos Android. Una vez que Google deje de usar las API, la inscripción fallará para los dispositivos Android Q en modo de administración de dispositivos.

Android Enterprise incluye compatibilidad con los modos de dispositivo totalmente administrado y perfil de trabajo. La publicación de Google, Android Enterprise Migration Bluebook, explica en detalle las diferencias entre la administración de dispositivos heredada y Android Enterprise. Le recomendamos que lea la información de migración de Google.

También le recomendamos que consulte el artículo de Citrix Tech Zone, Migration from Android Device Administrator to Android Enterprise with Citrix Endpoint Management.

Impacto de la desaprobación de la administración de dispositivos

Google ha dejado de usar las API de administrador de dispositivos y no las admitirá a partir de November 2, 2020. Estas API no funcionarán en dispositivos con Android 10+ después de que actualicemos Citrix Secure Hub para que apunte al nivel 29 de la API de Android:

- **Deshabilitar cámara:** Controla el acceso a las cámaras del dispositivo.
- **Funciones de bloqueo de pantalla:** Controla las funciones relacionadas con el bloqueo del dispositivo, como la biometría y los patrones.

- **Caducar contraseña:** Obliga a los usuarios a cambiar su contraseña después de un período de tiempo configurable.
- **Limitar contraseña:** Establece requisitos de contraseña restrictivos.

Requisitos y recomendaciones

- Si puede actualizar un dispositivo a Android 10+, debe inscribir ese dispositivo en Android Enterprise.
    - Debe inscribir los dispositivos Android 11 en Android Enterprise.
    - A partir de September 2020, para dispositivos Android 10: Citrix no admite nuevas inscripciones ni reinscripciones de dispositivos en el modo de administración de dispositivos. Los dispositivos ya inscritos seguirán funcionando hasta November 2, 2020, como se indica en la sección anterior.
- Para los dispositivos que ejecutan Android 9 y versiones anteriores, admitimos el modo de administración de dispositivos heredado. Sin embargo, recomendamos migrar esos dispositivos a Android Enterprise lo antes posible.
- Para los dispositivos nuevos o existentes inscritos en el modo solo MAM de Citrix, no es necesario realizar ninguna acción. Las API de Google obsoletas no tienen ningún impacto en los dispositivos en modo solo MAM. Sin embargo, con el paso al cifrado de plataforma, recomendamos encarecidamente pasar del modo solo MAM al modo de perfil de trabajo de Android Enterprise (BYOD). El modo de perfil de trabajo proporciona funcionalidad MAM, pero en un contenedor en el dispositivo.

Análisis

La fase de análisis de la migración consta de:

- Comprender su configuración heredada de Android
- Documentar su configuración heredada para poder asignar las características heredadas a las características de Android Enterprise

Análisis recomendado

1. Evaluar Android Enterprise en Citrix Endpoint Management: Totalmente administrado, totalmente administrado con perfil de trabajo, dispositivo dedicado, perfil de trabajo (BYOD).
2. Analizar las características actuales de administración de dispositivos frente a Android Enterprise.
3. Documentar sus casos de uso de administración de dispositivos.

Para documentar sus casos de uso de administración de dispositivos:

1. Cree una hoja de cálculo y enumere los grupos de directivas actuales en su consola de Citrix Endpoint Management.
2. Cree casos de uso separados basados en los grupos de directivas existentes.
3. Para cada caso de uso, documente lo siguiente:
    - Nombre
    - Propietario de la empresa
    - Modelo de identidad de usuario
    - Requisitos del dispositivo
        - Seguridad
        - Administración
        - Usabilidad
    - Inventario de dispositivos
        - Marca y modelo
        - Versión del SO
    - Aplicaciones
4. Para cada aplicación, enumere:
    - Nombre de la app
    - Nombre del paquete
    - Método de alojamiento
    - Si la aplicación es pública o privada
    - Si la aplicación es obligatoria (verdadero/falso)

Asignación de requisitos

Según el análisis completado, determine los requisitos de las funciones de Android Enterprise.

Asignación de requisitos recomendada

1. Determine el modo de administración y el método de inscripción:

- Perfil de trabajo (BYOD): Requiere reinscripción. No es necesario restablecer la configuración de fábrica.
- Totalmente administrado: Requiere restablecimiento de fábrica. Inscriba los dispositivos mediante código QR, comunicación de campo cercano (NFC), identificador de controlador de directivas de dispositivo (DPC), cero contacto.

2. Cree una estrategia de migración de aplicaciones.
3. Asigne los requisitos de los casos de uso a las funciones de Android Enterprise. Documente la función para cada requisito de dispositivo que más se ajuste al requisito y su versión de Android correspondiente.
4. Determine el sistema operativo Android mínimo según los requisitos de las funciones (7.0, 8.0, 9.0).
5. Elija un modelo de identidad:
   - Recomendado: Cuenta de Google Play administrada
   - Utilice las cuentas de Google Workspace solo si es cliente de Google Cloud Identity
6. Cree una estrategia de dispositivos:
   - Ninguna acción: Si los dispositivos cumplen el nivel mínimo de sistema operativo
   - Actualizar: Si los dispositivos son compatibles y se pueden actualizar al SO compatible
   - Reemplazar: Si los dispositivos no se pueden actualizar al nivel de SO compatible

Estrategia de migración de aplicaciones recomendada

Una vez que haya completado la asignación de requisitos, mueva las aplicaciones de la plataforma Android a la plataforma Android Enterprise. Para obtener más información sobre la publicación de aplicaciones, consulte Agregar aplicaciones.

- Aplicaciones de la tienda pública

  a. Seleccione las aplicaciones que desea migrar y, a continuación, edítelas para borrar la configuración de Google Play y seleccione **Android Enterprise** como plataforma.
  b. Seleccione el grupo de entrega. Si una aplicación es obligatoria, muévala a la lista de **Aplicaciones requeridas** del grupo de entrega.

  Después de guardar una aplicación, esta aparece en Google Play Store. Si tiene un perfil de trabajo, las aplicaciones aparecen en Google Play Store en el perfil de trabajo.

- Aplicaciones privadas (empresariales)

Las aplicaciones privadas se desarrollan internamente o por un desarrollador externo. Le recomendamos que publique aplicaciones privadas mediante Google Play.

a. Seleccione las aplicaciones que desea migrar y, a continuación, edítelas para seleccionar **Android Enterprise** como plataforma.
b. Cargue el archivo APK y, a continuación, configure los ajustes de la aplicación.
c. Publique la aplicación en el grupo de entrega requerido.

- Aplicaciones MDX

a. Seleccione las aplicaciones que desea migrar y, a continuación, edítelas para seleccionar **Android Enterprise** como plataforma.
b. Cargue el archivo MDX. Pase por el proceso de aprobación de la aplicación.
c. Seleccione las directivas MDX.

Para las aplicaciones MDX de Enterprise, recomendamos cambiarlas a aplicaciones encapsuladas en modo MDX SDK:

  - Opción 1: Aloje el APK en Google Play con una cuenta de desarrollador asignada de forma privada a su organización. Publique el archivo MDX en Citrix Endpoint Management.
  - Opción 2: Publique la aplicación desde Citrix Endpoint Management como una aplicación empresarial. Publique el APK en Citrix Endpoint Management y seleccione la plataforma **Android Enterprise** para el archivo MDX.

Migración de directivas de dispositivos Citrix

Para las directivas disponibles tanto para **Android (DA heredado)** como para las plataformas de **Android Enterprise**: Edite la directiva y seleccione la plataforma **Android Enterprise**.

- Para Android Enterprise, tenga en cuenta el método de inscripción de dispositivos. Algunas opciones de directiva solo están disponibles para dispositivos en modo de perfil de trabajo o en modo totalmente administrado. Consulte Configurar directivas de dispositivos y aplicaciones de Android Enterprise.
- Si utiliza la directiva de dispositivos de Exchange para dispositivos DA heredados, cree una directiva de dispositivos de configuración administrada en su lugar para configurar los ajustes de correo electrónico.
- Para asegurarse de que dirige una directiva a los dispositivos previstos (Android Enterprise frente a DA heredado), añada una regla de implementación a la directiva. Por ejemplo, para la plataforma DA heredada, utilice esta regla de implementación:

```
Limit by known device property name Android Enterprise

Enabled Device? Isn’t equal to true
```

Esa regla de implementación comprueba si el dispositivo NO está habilitado para Android Enterprise y entrega la directiva junto con las aplicaciones a los dispositivos habilitados para DA heredado.

Prueba de concepto

Después de migrar las aplicaciones a Android Enterprise, puede configurar una prueba de migración para verificar que las funciones funcionan según lo previsto.

Configuración recomendada de la prueba de concepto

1. Configure la infraestructura de implementación:
    - Crear un grupo de entrega para sus pruebas de Android Enterprise.
    - Configurar Android Enterprise en Citrix Endpoint Management.
2. Configurar aplicaciones de usuario.
3. Configurar las funciones de Android Enterprise.
4. Asignar directivas al grupo de entrega de Android Enterprise.
5. Probar y confirmar las funciones.
6. Completar un tutorial de configuración de dispositivos para cada caso de uso.
7. Documentar los pasos de configuración del usuario.

Implementación

Ahora puede implementar su configuración de Android Enterprise y preparar a sus usuarios para la migración.

Estrategia de implementación recomendada

La estrategia de implementación recomendada de Citrix es probar todos sus sistemas de producción para Android Enterprise y, a continuación, completar la migración de dispositivos más adelante.

- En este escenario, los usuarios siguen utilizando dispositivos heredados con su configuración actual. Usted configura nuevos dispositivos para la administración de Android Enterprise.
- Migre los dispositivos existentes solo cuando sea necesaria una actualización o un reemplazo.

- Migre los dispositivos existentes a la administración de Android Enterprise al final de su ciclo de vida habitual. O bien, migre esos dispositivos cuando necesiten ser reemplazados debido a pérdida o rotura.

Android Enterprise

Android Enterprise es un conjunto de herramientas y servicios proporcionados por Google como solución de administración empresarial para dispositivos Android. Con Android Enterprise:

- Utiliza Citrix Endpoint Management para administrar dispositivos Android propiedad de la empresa y dispositivos personales (BYOD).
- Puede administrar todo el dispositivo o un perfil independiente en el dispositivo. El perfil independiente aísla las cuentas, aplicaciones y datos empresariales de las cuentas, aplicaciones y datos personales.
- También puede administrar dispositivos dedicados a un solo uso, como la gestión de inventario. Para obtener una descripción general de Google sobre lo que puede hacer Android Enterprise, consulte Administración de Android Enterprise.

Recursos:

- Para obtener una lista de términos y definiciones relacionados con Android Enterprise, consulte el artículo de la guía para desarrolladores de Google Android Enterprise, Terminología de Android Enterprise. Google actualiza estos términos con frecuencia.
- Para obtener una lista de los sistemas operativos Android compatibles con Citrix Endpoint Management, consulte Sistemas operativos de dispositivos compatibles.
- Para obtener información sobre las conexiones salientes que debe tener en cuenta al configurar entornos de red para Android Enterprise, consulte el artículo de soporte de Google, Requisitos de red de Android Enterprise.
- Para obtener información sobre la implementación de Android Enterprise, consulte Implementar recursos).

Primeros pasos con Android Enterprise

> **Importante:**

> El modo de administración de dispositivos ya no es compatible. Si sus usuarios tienen dispositivos en modo de administración de dispositivos, consulte Migrar de la administración de dispositivos a Android Enterprise. Una vez que sus dispositivos se hayan migrado a

Android Enterprise, siga los pasos siguientes para configurar los dispositivos Android Enterprise.



Configuración única

1. Cree una cuenta de Google Play administrada.

   Consulte Uso de Google Play administrado con Citrix Endpoint Management y Requisitos.

2. Vincule su cuenta de Google Play a Citrix Endpoint Management.

   Consulte Conectar Citrix Endpoint Management a Google Play.

3. Planifique cómo quiere administrar los dispositivos.

   Consulte Escenarios y perfiles de implementación de dispositivos.

4. Planifique la seguridad de la inscripción para los dispositivos de usuario.

   Consulte Seguridad de la inscripción.

5. Prepárese para entregar aplicaciones habilitadas para MDX.

   Utilice el SDK de MAM para desarrollar aplicaciones. O, si no está listo para la transición al nuevo SDK, utilice el MDX Toolkit basado en línea de comandos para encapsular las aplicaciones.

   Consulte Información general del SDK de MAM.

En este punto, está preparado para configurar sus dispositivos Android Enterprise con directivas de aplicaciones y dispositivos, perfiles de inscripción y aplicaciones. Consulte la siguiente sección para obtener orientación.

Configurar dispositivos

1. Cree grupos de entrega.

   Controle quién obtiene qué recursos y cuándo los obtiene. Consulte Implementar recursos.

   Dejamos de entregar aplicaciones publicadas para la plataforma DA heredada a los dispositivos inscritos en Android Enterprise. Para los dispositivos Android Enterprise, publique aplicaciones para la plataforma Android Enterprise. Para seguir publicando aplicaciones DA heredadas en dispositivos en modo DA, cree un grupo de entrega independiente para esas aplicaciones. Consulte Obsoleto.
2. Agregue aplicaciones. Puede aprobar las aplicaciones en Google Play directamente desde la consola de Citrix Endpoint Management.

   Consulte el artículo de soporte de Google, Administrar aplicaciones en su organización.
3. Cree perfiles de inscripción.

   Especifique las opciones de inscripción de administración de dispositivos y aplicaciones. Consulte Escenarios y perfiles de implementación de dispositivos y Crear perfiles de inscripción.

   - Cuando implementa una aplicación de la tienda de aplicaciones pública de Android Enterprise en un usuario de dispositivo Android, ese usuario se inscribe automáticamente en Android Enterprise.
   - La inscripción sin contacto le permite configurar los dispositivos para que se inscriban automáticamente cuando se encienden por primera vez. Consulte Inscripción sin contacto.
4. Configure las directivas de dispositivos y aplicaciones.

Equilibre la seguridad empresarial con la privacidad y la experiencia del usuario. Consulte Configurar directivas de dispositivos y aplicaciones de Android Enterprise.

5. Distribuya aplicaciones.

   Utiliza Google Play administrado para agregar, comprar y aprobar aplicaciones para su implementación en el espacio de trabajo de Android Enterprise en un dispositivo. Los usuarios solo pueden instalar aplicaciones de Google Play administrado que usted ponga a su disposición.

   Consulte:

   - Distribuir aplicaciones de Android Enterprise
   - Directiva de configuraciones administradas
   - Directiva de permisos de aplicaciones

6. Configure acciones de seguridad para supervisar y garantizar el cumplimiento.

   Consulte Acciones de seguridad.

Uso de Google Play administrado con Citrix Endpoint Management

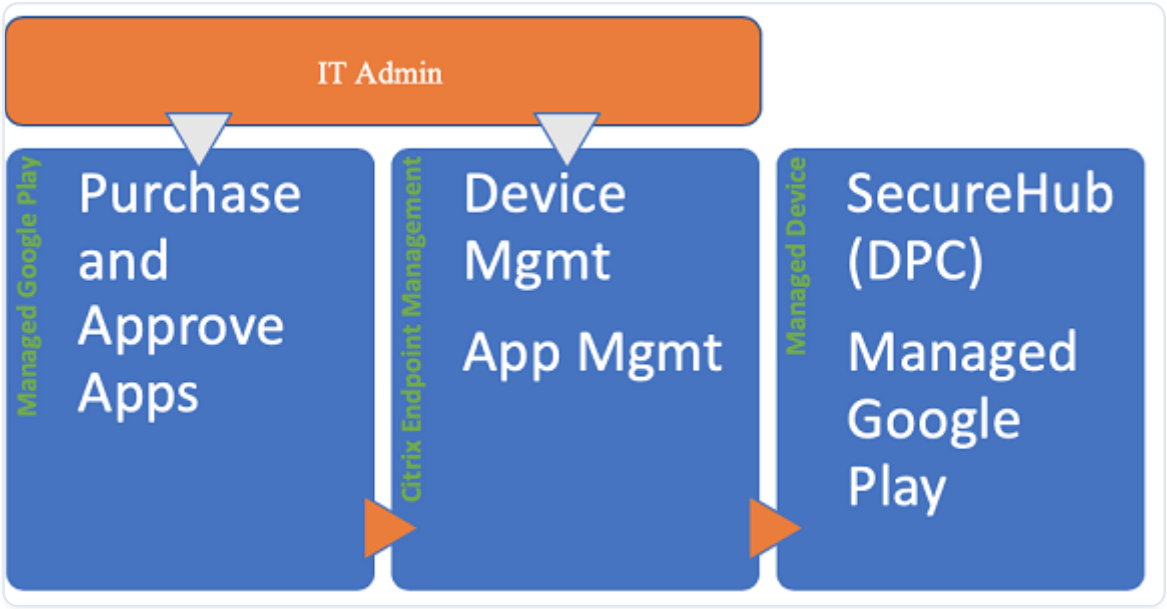
Al integrar Citrix Endpoint Management con Google Play administrado para usar Android Enterprise, se crea una empresa. Google define una empresa como la vinculación entre la organización y su solución de administración de dispositivos móviles empresariales (EMM). Todos los usuarios y dispositivos que la organización administra a través de su solución pertenecen a su empresa.

Una empresa para Android Enterprise tiene tres componentes: una solución EMM, una aplicación de controlador de directivas de dispositivo (DPC) y una plataforma de aplicaciones empresariales de Google. Cuando se integra Citrix Endpoint Management con Android Enterprise, la solución completa tiene estos componentes:

- **Citrix Endpoint Management:** El EMM de Citrix. Citrix Endpoint Management es la solución unificada de Citrix Endpoint Management para un espacio de trabajo digital seguro. Citrix Endpoint Management proporciona los medios para que los administradores de TI administren dispositivos y aplicaciones para sus organizaciones.
- **Citrix Secure Hub:** La aplicación DPC de Citrix. Citrix Secure Hub es la plataforma de lanzamiento de Citrix Endpoint Management. Citrix Secure Hub aplica directivas en el dispositivo.

- **Google Play administrado:** Una plataforma de aplicaciones empresariales de Google que se integra con Citrix Endpoint Management. La API EMM de Google Play establece directivas de aplicaciones y distribuye aplicaciones.

Esta ilustración muestra cómo los administradores interactúan con estos componentes y cómo los componentes interactúan entre sí:



Nota:

Puede usar Google Play administrado o Google Workspace (anteriormente G Suite) para registrar Citrix como su proveedor de EMM. Este artículo trata sobre el uso de Android Enterprise con Google Play administrado. Si su organización utiliza Google Workspace para proporcionar acceso a las aplicaciones, puede usarlo con Android Enterprise. Consulte Android Enterprise heredado para clientes de Google Workspace.

Cuando utiliza Google Play administrado, aprovisione cuentas de Google Play administradas para dispositivos y usuarios finales. Las cuentas de Google Play administradas proporcionan acceso a Google Play administrado, lo que permite a los usuarios instalar y usar las aplicaciones que usted pone a su disposición. Si su organización utiliza un servicio de identidad de terceros, puede vincular las cuentas de Google Play administradas con sus cuentas de identidad existentes.

Debido a que este tipo de empresa no está vinculado a un dominio, puede crear más de una empresa para una sola organización. Por ejemplo, cada departamento o región dentro de una

organización puede inscribirse como una empresa diferente. El uso de diferentes empresas le permite administrar conjuntos separados de dispositivos y aplicaciones.

Para los administradores de Citrix Endpoint Management, Google Play administrado combina la experiencia del usuario y las funciones de la tienda de aplicaciones de Google Play con un conjunto de funciones de administración diseñadas para empresas. Utiliza Google Play administrado para agregar, comprar y aprobar aplicaciones para su implementación en el espacio de trabajo de Android Enterprise en un dispositivo. Puede usar Google Play para implementar aplicaciones públicas, aplicaciones privadas y aplicaciones de terceros.

Para los usuarios de dispositivos administrados, Google Play administrado es la tienda de aplicaciones empresariales. Los usuarios pueden buscar aplicaciones, ver los detalles de las aplicaciones e instalarlas. A diferencia de la versión pública de Google Play, los usuarios solo pueden instalar aplicaciones de Google Play administrado que usted ponga a su disposición.

Escenarios y perfiles de implementación de dispositivos

Los escenarios de implementación de dispositivos se refieren a quién es el propietario de los dispositivos que implementa y cómo los administra. Los perfiles de dispositivo se refieren a cómo el DPC administra y aplica las directivas en los dispositivos.

Un perfil de trabajo aísla las cuentas, aplicaciones y datos empresariales de las cuentas, aplicaciones y datos personales. Los perfiles de trabajo y los perfiles personales están separados a nivel del sistema operativo. Para obtener más información sobre los perfiles de trabajo, consulte ¿Qué es un perfil de trabajo?.

> **Importante:**
>
> Cuando los dispositivos Android Enterprise se actualizan a Android 11, Google migra los dispositivos administrados como «totalmente administrados con un perfil de trabajo» a una nueva experiencia de perfil de trabajo con seguridad mejorada. El nuevo modo de inscripción se denomina «perfil de trabajo en dispositivos propiedad de la empresa». Para obtener más información, consulte Cambios futuros para la administración completa con perfil de trabajo de Android Enterprise. Para dispositivos Android 12, consulte Mejoras de seguridad y privacidad para el perfil de trabajo.

ADMINISTRACIÓN DE DISPOSITIVOS	CASOS DE USO	PERFIL DE TRABAJO	PERFIL PERSONAL	NOTAS
Dispositivos propiedad de la empresa (totalmente administrados)	Dispositivos propiedad de la empresa destinados únicamente al uso laboral	No	No	Solo para dispositivos nuevos o restablecidos de fábrica. Consulte Aprovisionamiento de dispositivos Android Enterprise totalmente administrados.
Totalmente administrado con un perfil de trabajo / Perfil de trabajo en dispositivos propiedad de la empresa	Dispositivos propiedad de la empresa destinados al uso laboral y personal	Sí	Sí. En estos dispositivos se ejecutan dos copias del DPC: Una administra el dispositivo en modo de propietario del dispositivo y la otra administra el perfil de trabajo en modo de propietario del perfil. Puede aplicar directivas independientes al dispositivo y al perfil de trabajo.	Consulte Aprovisionamiento de dispositivos Android Enterprise totalmente administrados con un perfil de trabajo o perfil de trabajo en dispositivos propiedad de la empresa.

ADMINISTRACIÓN DE DISPOSITIVOS	CASOS DE USO	PERFIL DE TRABAJO	PERFIL PERSONAL	NOTAS
Dispositivos dedicados*	Dispositivos propiedad de la empresa configurados para un único caso de uso, como la señalización digital o la impresión de billetes	No	No	Consulte Aprovisionamiento de dispositivos Android Enterprise dedicados.
Perfil de trabajo BYOD**	Dispositivos personales inscritos con administración de perfiles de trabajo (también conocido como modo de propietario del perfil)	Sí	Sí. El DPC administra solo el perfil de trabajo, no todo el dispositivo.	Estos dispositivos no necesitan ser nuevos ni restablecidos de fábrica. Consulte Aprovisionamiento de dispositivos con perfil de trabajo de Android Enterprise.

* Los usuarios pueden compartir un dispositivo dedicado. Cuando un usuario inicia sesión en una aplicación en un dispositivo dedicado, el estado de su trabajo está con la aplicación, no con el dispositivo.

** Citrix Endpoint Management no admite dispositivos Zebra en modo de perfil de trabajo BYOD. Citrix Endpoint Management admite dispositivos Zebra como dispositivos totalmente administrados mediante Android Enterprise.

Seguridad de la inscripción

Los perfiles de inscripción determinan si los dispositivos Android se inscriben en MAM, MDM o MDM+MAM, con la opción de que los usuarios puedan optar por no participar en MDM.

Para obtener información sobre cómo especificar el nivel de seguridad y los pasos de inscripción necesarios, consulte Cuentas de usuario, roles e inscripción.

Citrix Endpoint Management admite los siguientes métodos de autenticación para dispositivos Android inscritos en MDM o MDM+MAM. Para obtener información, consulte los siguientes artículos:

- Autenticación de dominio o de dominio más token de seguridad
- Certificado de cliente o certificado más autenticación de dominio
- Proveedores de identidades:
  - Autenticación con Azure Active Directory a través de Citrix Cloud (Vista previa)
  - Autenticación con Okta a través de Citrix Cloud (Vista previa)

Un método de autenticación poco utilizado es un certificado de cliente más un token de seguridad. Para obtener información, consulte `<https://support.citrix.com/article/CTX215200>`.

Requisitos

Antes de empezar a usar Android Enterprise, necesita:

- Cuentas y credenciales:
  - Para configurar Android Enterprise con Google Play administrado, una cuenta de Google corporativa
  - Para descargar los archivos MDX más recientes, una cuenta de cliente de Citrix®
- Firebase Cloud Messaging (FCM) y una directiva de dispositivo de programación de conexiones configurada para Citrix Endpoint Management. Consulte (/es-es/citrix-endpoint-management/device-management/android/firebase-cloud-messaging.html)Firebase Cloud Messaging y (/es-es/citrix-endpoint-management/policies/connection-scheduling-policy.html)Directiva de dispositivo de programación de conexiones.

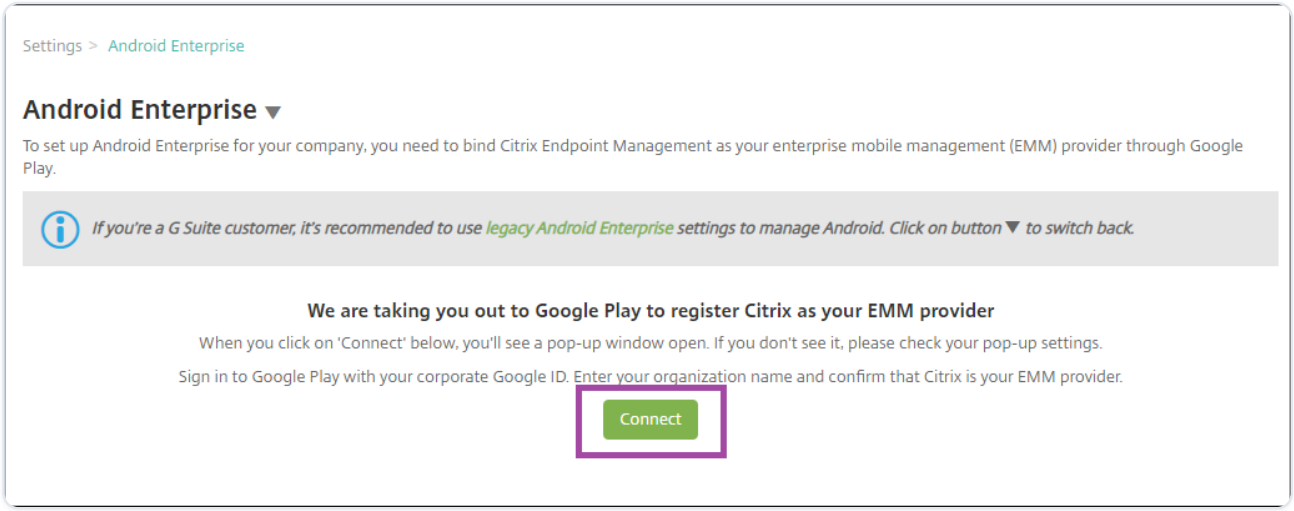
Conectar Citrix Endpoint Management a Google Play

Para configurar Android Enterprise para su organización, registre Citrix como su proveedor de EMM a través de Google Play administrado. Esa configuración conecta Google Play administrado

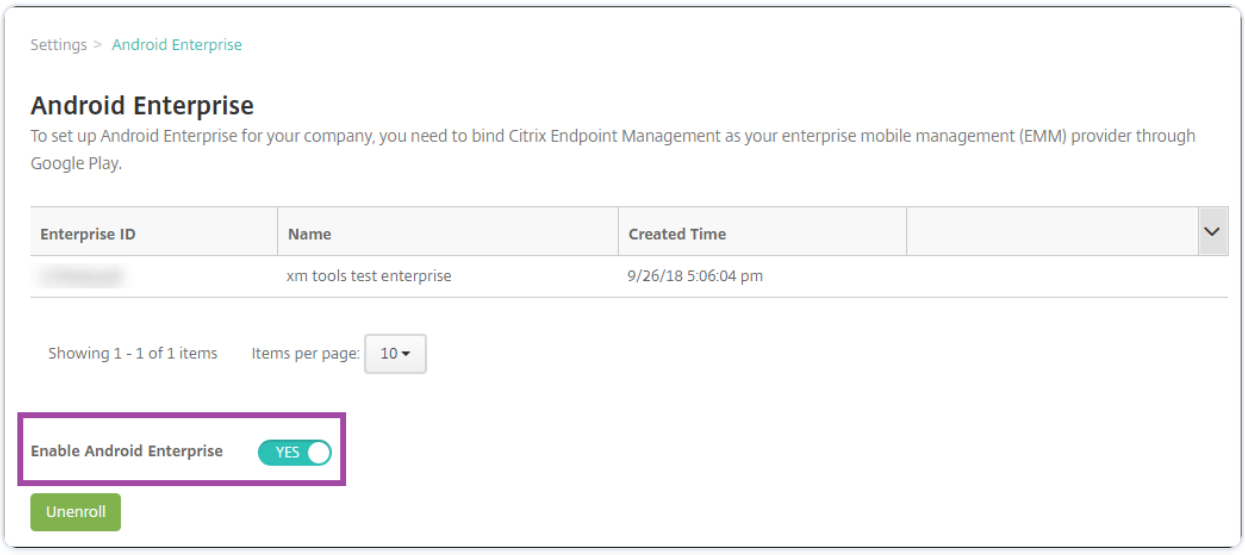
con Citrix Endpoint Management y crea una empresa para Android Enterprise en Citrix Endpoint Management.

Necesita una cuenta de Google corporativa para iniciar sesión en Google Play.

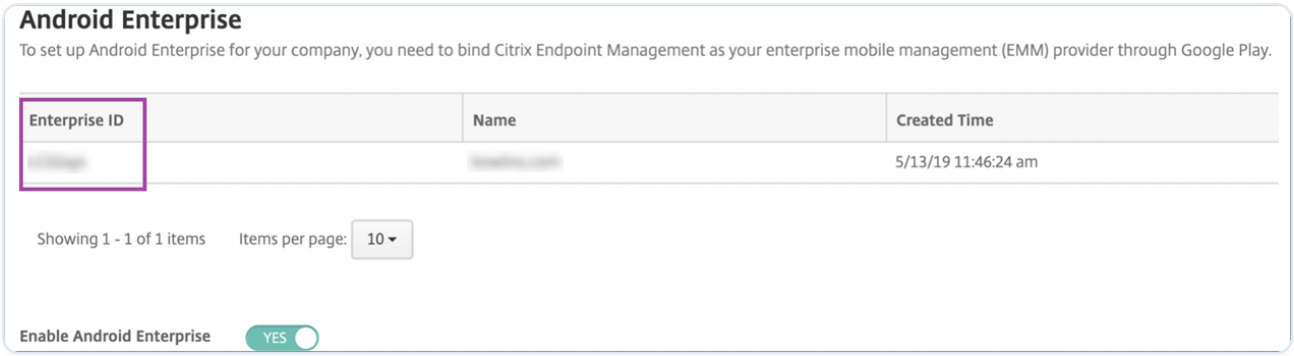
1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Android Enterprise**.
2. Haga clic en **Conectar**. Se abre Google Play.



1. Inicie sesión en Google Play con las credenciales de su cuenta de Google corporativa. Introduzca el nombre de su organización y confirme que Citrix es su proveedor de EMM.
2. Se agrega un ID de empresa para Android Enterprise. Para habilitar Android Enterprise, deslice **Habilitar Android Enterprise** a **Sí**.



Su ID de empresa aparece en la consola de Citrix Endpoint Management.



Su entorno está conectado a Google y está listo para administrar los dispositivos. Ahora puede proporcionar aplicaciones a los usuarios.

Citrix Endpoint Management puede proporcionar a los usuarios aplicaciones de productividad móvil de Citrix, aplicaciones MDX, aplicaciones de tiendas de aplicaciones públicas, aplicaciones web y SaaS, aplicaciones empresariales y enlaces web. Para obtener más información sobre cómo proporcionar estos tipos de aplicaciones a los usuarios, consulte Distribuir aplicaciones de Android Enterprise.

La siguiente sección muestra cómo proporcionar aplicaciones de productividad móvil.

Proporcionar aplicaciones de productividad móvil de Citrix a usuarios de Android Enterprise

Para proporcionar aplicaciones de productividad móvil de Citrix a usuarios de Android Enterprise, se requieren estos pasos.

1. Publique las aplicaciones como aplicaciones MDX. Consulte Configurar aplicaciones como aplicaciones MDX.
2. Configure las reglas para los desafíos de seguridad que sus usuarios utilizan para acceder a los perfiles de trabajo en sus dispositivos. Consulte Configurar la directiva de desafío de seguridad.

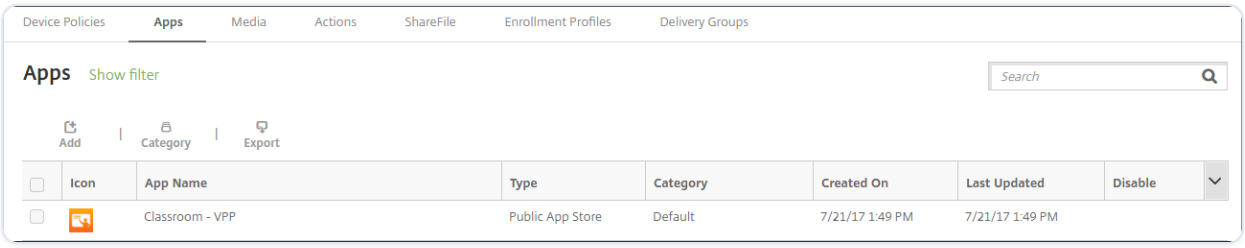
Las aplicaciones que publique están disponibles para los dispositivos inscritos en su empresa de Android Enterprise.

> **Nota:**
>
> Cuando implementa una aplicación de tienda de aplicaciones pública de Android Enterprise en un usuario de Android, ese usuario se inscribe automáticamente en Android Enterprise.

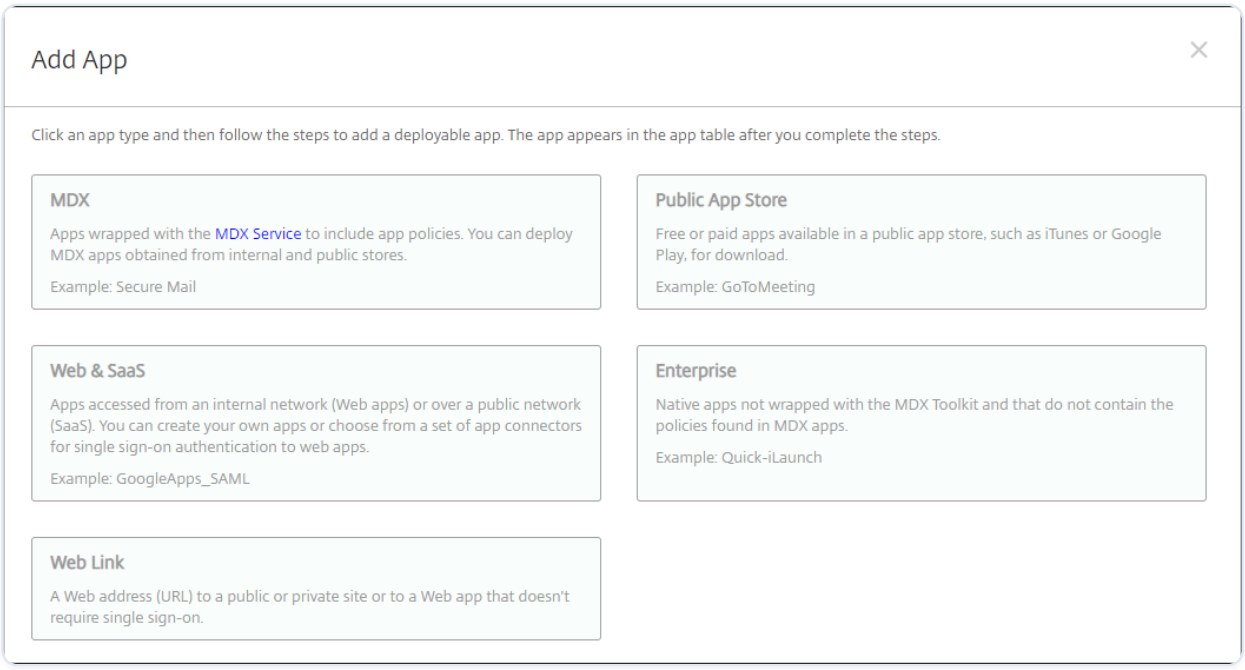
Configurar aplicaciones como aplicaciones MDX

Para configurar una aplicación de productividad de Citrix como una aplicación MDX para Android Enterprise:

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones**. Aparecerá la página **Aplicaciones**.



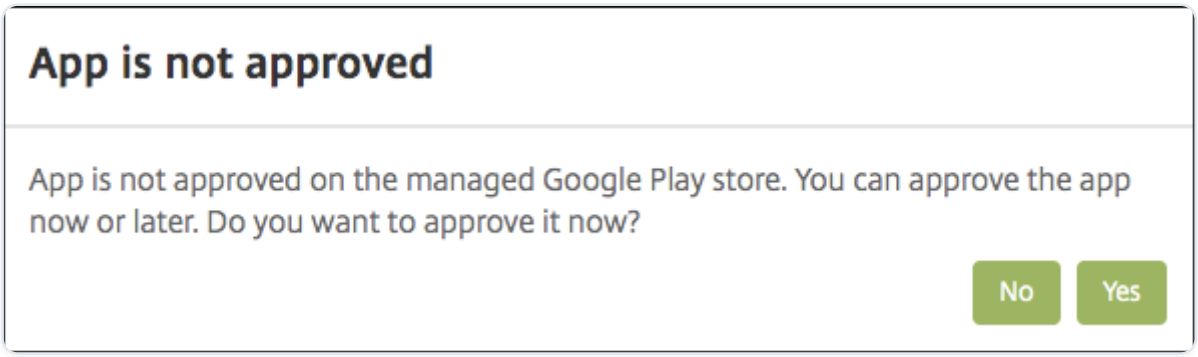
2. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.



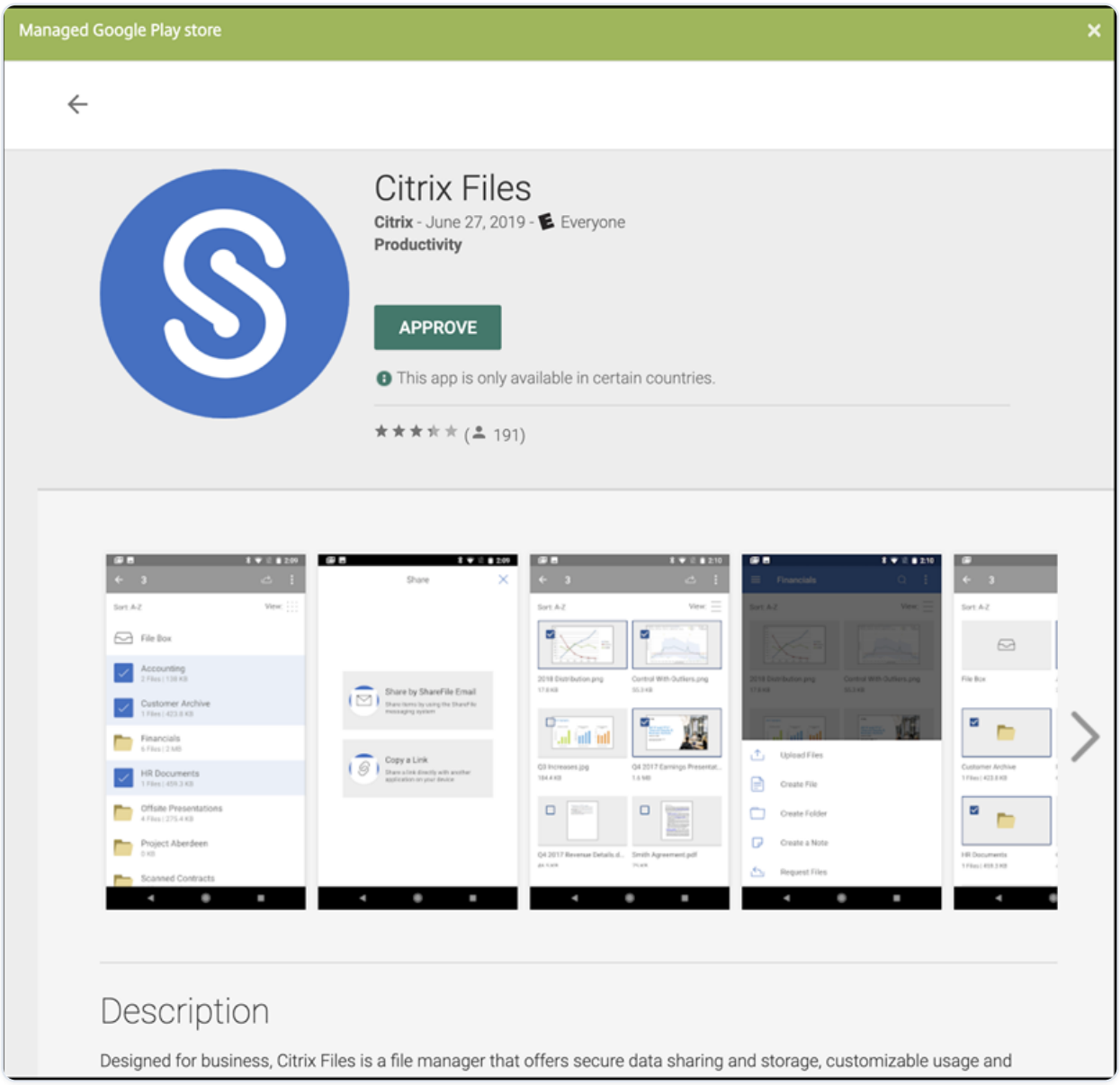
3. Haga clic en **MDX**. Aparece la página **Información de la aplicación**.
4. En el lado izquierdo de la página, seleccione **Android Enterprise** como plataforma.
5. En la página **Información de la aplicación**, escriba la siguiente información:

   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre aparece en **Nombre de la aplicación** en la tabla **Aplicaciones**.
   - **Descripción:** Escriba una descripción opcional de la aplicación.
   - **Categoría de la aplicación:** Opcionalmente, en la lista, haga clic en la categoría a la que desea agregar la aplicación. Para obtener más información sobre las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.

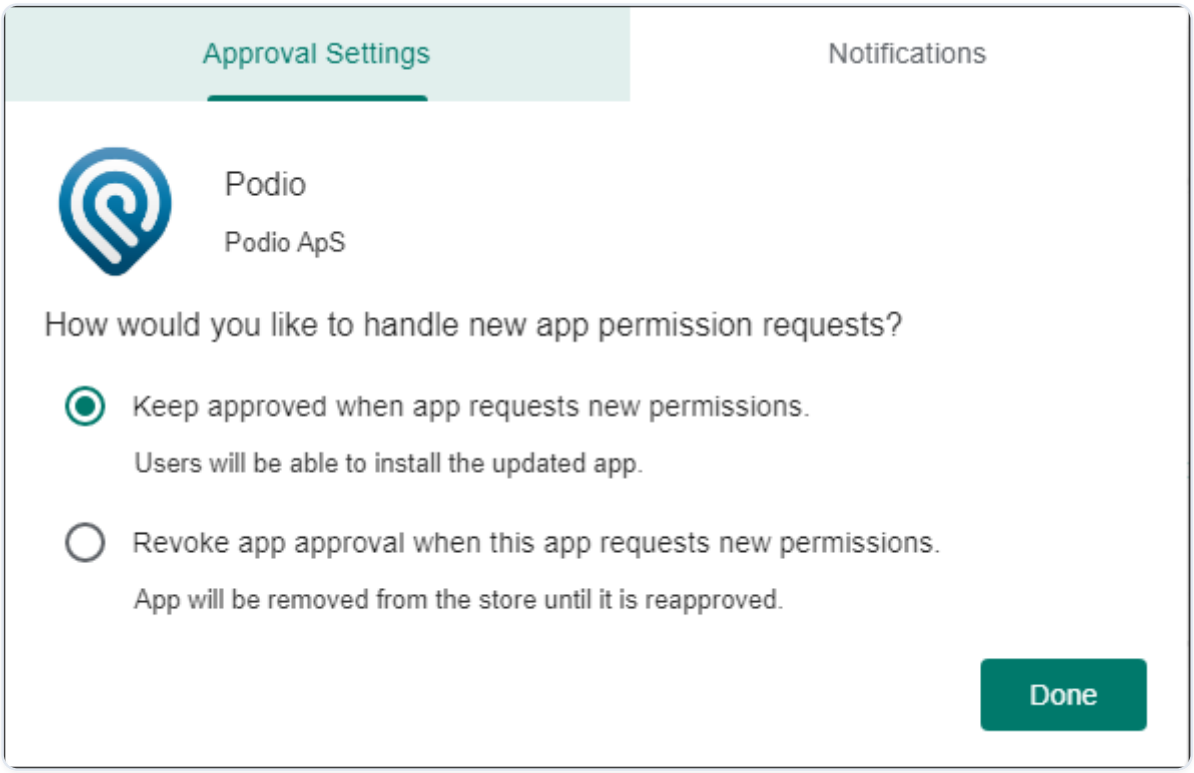
6. Haga clic en **Siguiente**. Aparece la página **Aplicación MDX de Android Enterprise**.
7. Haga clic en **Cargar** y vaya a la ubicación de los archivos .mdx de la aplicación. Seleccione el archivo y haga clic en **Abrir**.
8. La interfaz de usuario le notifica si la aplicación adjunta requiere aprobación de la tienda administrada de Google Play. Para aprobar la aplicación sin salir de la consola de Citrix Endpoint Management, haga clic en **Sí**.



9. Cuando se abra la página de la tienda administrada de Google Play, haga clic en **Aprobar**.



10. Haga clic en **Aprobar** de nuevo.
11. Seleccione **Mantener aprobada cuando la aplicación solicite nuevos permisos**. Haga clic en **Guardar**.

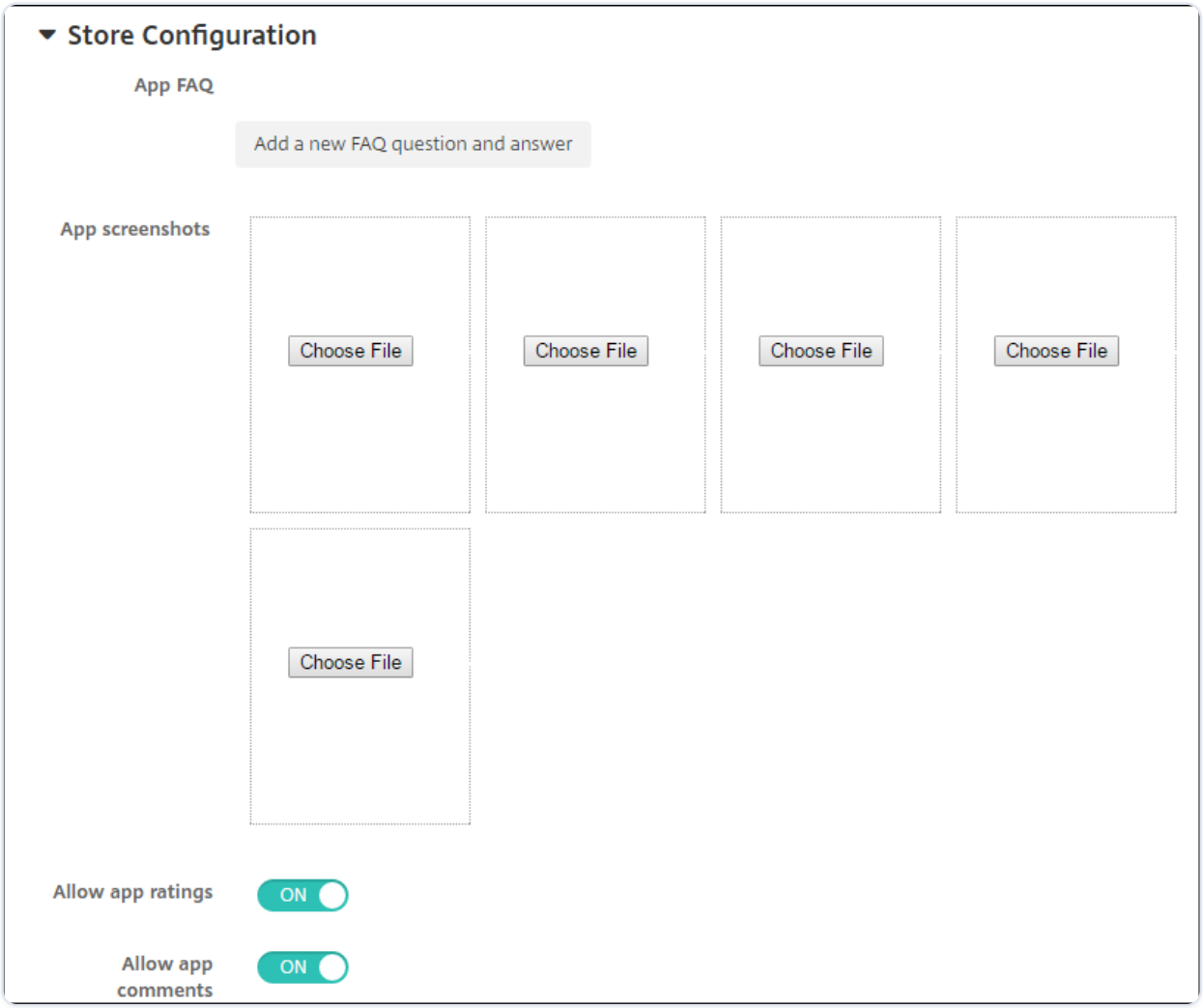


12. Cuando la aplicación se aprueba y se guarda, aparecen más configuraciones en la página. Configure estas opciones:

    - **Nombre de archivo:** Escriba el nombre de archivo asociado a la aplicación.
    - **Descripción de la aplicación:** Escriba una descripción para la aplicación.
    - **Pista de producto:** Especifique la pista de producto que quiere enviar a los dispositivos de los usuarios. Si tiene una pista diseñada para pruebas, puede seleccionarla y asignarla a sus usuarios. El valor predeterminado es Producción.
    - **Versión de la aplicación:** Opcionalmente, escriba el número de versión de la aplicación.
    - **ID de paquete:** La URL de la aplicación en la tienda Google Play.
    - **Versión mínima del SO:** Opcionalmente, escriba la versión más antigua del sistema operativo que el dispositivo puede ejecutar para usar la aplicación.
    - **Versión máxima del SO:** Opcionalmente, escriba la versión más reciente del sistema operativo que el dispositivo debe ejecutar para usar la aplicación.
    - **Dispositivos excluidos:** Opcionalmente, escriba el fabricante o los modelos de dispositivos que no pueden ejecutar la aplicación.

13. Configure las **directivas MDX**. Para obtener más información sobre las directivas de aplicaciones para aplicaciones MDX, consulte Directivas MDX de un vistazo y Información general del SDK de MAM.

14. Configure las reglas de implementación. Para obtener información, consulte Implementar recursos.
15. Expanda **Configuración de la tienda**. Esta configuración no se aplica a las aplicaciones de Android Enterprise, que solo aparecen en Google Play administrado.

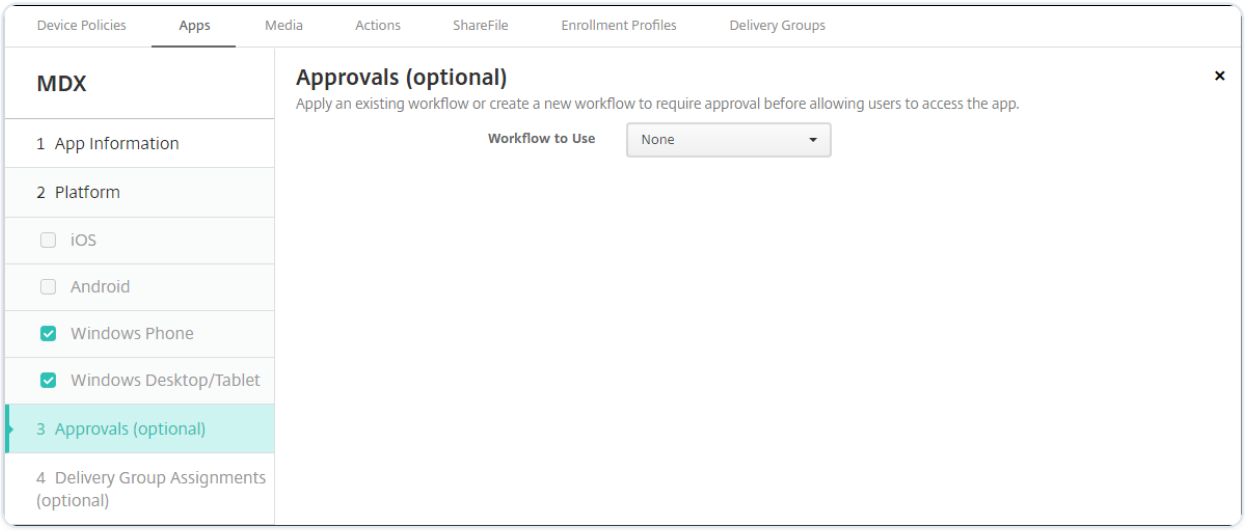


Opcionalmente, puede agregar una sección de preguntas frecuentes para la aplicación o capturas de pantalla que aparecen en la tienda de aplicaciones. También puede configurar si los usuarios pueden calificar o comentar la aplicación.

- Configure los siguientes ajustes:
  - **Preguntas frecuentes de la aplicación:** Añada preguntas y respuestas frecuentes para la aplicación.
  - **Capturas de pantalla de la aplicación:** Añada capturas de pantalla para ayudar a clasificar la aplicación en la tienda de aplicaciones. El gráfico que cargue debe ser un PNG. No puede cargar una imagen GIF o JPEG.
  - **Permitir valoraciones de la aplicación:** Seleccione si permite que un usuario valore la aplicación. El valor predeterminado es **Activado**. **Permitir comentarios de la**

aplicación: Seleccione si permite que los usuarios comenten sobre la aplicación seleccionada. El valor predeterminado es **Activado**.

16. Haga clic en **Siguiente**. Aparece la página **Aprobaciones**.



Utiliza flujos de trabajo cuando necesita aprobación al crear cuentas de usuario. Si no desea configurar flujos de trabajo de aprobación, puede saltar al Paso 15.

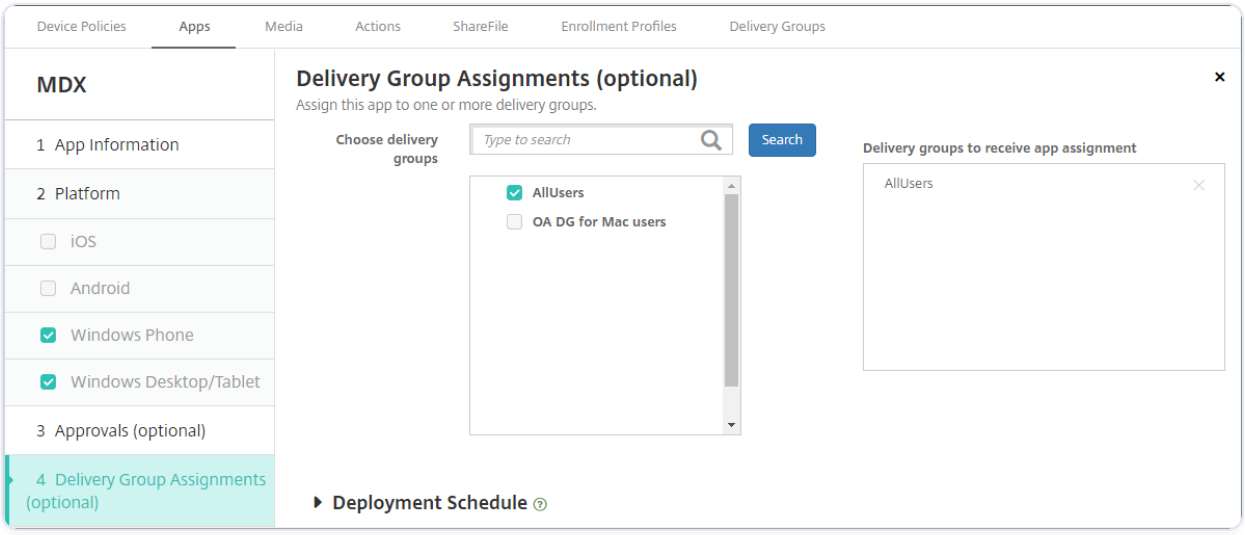
Configure los siguientes ajustes para asignar o crear un flujo de trabajo:

- **Flujo de trabajo a utilizar:** Haga clic en un flujo de trabajo existente en la lista desplegable o haga clic en **Crear un nuevo flujo de trabajo**. El valor predeterminado es **Ninguno**.
- Si selecciona **Crear un nuevo flujo de trabajo**, configure los siguientes ajustes. Para obtener más información, consulte Crear y administrar flujos de trabajo.
- **Nombre:** Escriba un nombre único para el flujo de trabajo.
- **Descripción:** Opcionalmente, escriba una descripción para el flujo de trabajo.
- **Plantillas de aprobación de correo electrónico:** En la lista, seleccione la plantilla de aprobación de correo electrónico que se va a asignar. Al hacer clic en el icono del ojo a la derecha de este campo, aparece un cuadro de diálogo donde puede previsualizar la plantilla.
- **Niveles de aprobación del administrador:** En la lista, seleccione el número de niveles de aprobación del administrador necesarios para este flujo de trabajo. El valor predeterminado es 1 nivel. Las opciones posibles son:
  - No es necesario
  - 1 nivel

- 2 niveles
- 3 niveles

- **Seleccionar dominio de Active Directory:** En la lista, seleccione el dominio de Active Directory adecuado que se utilizará para el flujo de trabajo.
- **Buscar aprobadores adicionales obligatorios:** Escriba el nombre de la persona adicional obligatoria en el campo de búsqueda y, a continuación, haga clic en **Buscar**. Los nombres provienen de Active Directory.
- Cuando el nombre aparezca en el campo, marque la casilla junto al nombre. El nombre y la dirección de correo electrónico aparecen en la lista de **Aprobadores adicionales obligatorios seleccionados**.
  - Para eliminar a una persona de la lista de **Aprobadores adicionales obligatorios seleccionados**, realice una de las siguientes acciones:
    - Haga clic en **Buscar** para ver una lista de todas las personas del dominio seleccionado.
    - Escriba un nombre completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Buscar** para limitar los resultados de la búsqueda.
    - Las personas de la lista de **Aprobadores adicionales obligatorios seleccionados** tienen marcas de verificación junto a su nombre en la lista de resultados de búsqueda. Desplácese por la lista y desmarque la casilla junto a cada nombre que desee eliminar.

17. Haga clic en **Siguiente**. Aparece la página **Asignación de grupos de entrega**.



18. Junto a **Elegir grupos de entrega**, escriba para buscar un grupo de entrega o seleccione uno o varios grupos de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega que recibirán la asignación de la aplicación**.
19. Expanda **Programación de implementación** y, a continuación, configure los siguientes ajustes:

    - Junto a **Implementar**, haga clic en **Activado** para programar la implementación o en **Desactivado** para evitarla. La opción predeterminada es **Activado**.
    - Junto a Programación de la implementación, haga clic en **Ahora** o en **Más tarde**. La opción predeterminada es **Ahora**.
    - Si hace clic en **Más tarde**, haga clic en el icono del calendario y, a continuación, seleccione la fecha y la hora de la implementación.
    - Junto a **Condición de implementación**, haga clic en **En cada conexión** o en **Solo si la implementación anterior ha fallado**. La opción predeterminada es **En cada conexión**.
    - Junto a **Implementar para conexión permanente**, asegúrese de que la opción **Desactivado** esté seleccionada. La opción predeterminada es **Desactivado**. Las conexiones permanentes no están disponibles para Android Enterprise para los clientes que empezaron a usar Citrix Endpoint Management con la versión 10.18.19 o posterior. No recomendamos las conexiones para los clientes que empezaron a usar Citrix Endpoint Management antes de la versión 10.18.19.

      Esta opción se aplica cuando ha configurado la clave de implementación en segundo plano de la programación en **Parámetros > Propiedades del servidor**.

      La programación de la implementación que configure es la misma para todas las plataformas. Cualquier cambio que realice se aplica a todas las plataformas, excepto a **Implementar para conexión permanente**.

20. Haga clic en **Guardar**.

Repita los pasos para cada aplicación de productividad móvil.

Configurar la directiva de desafío de seguridad

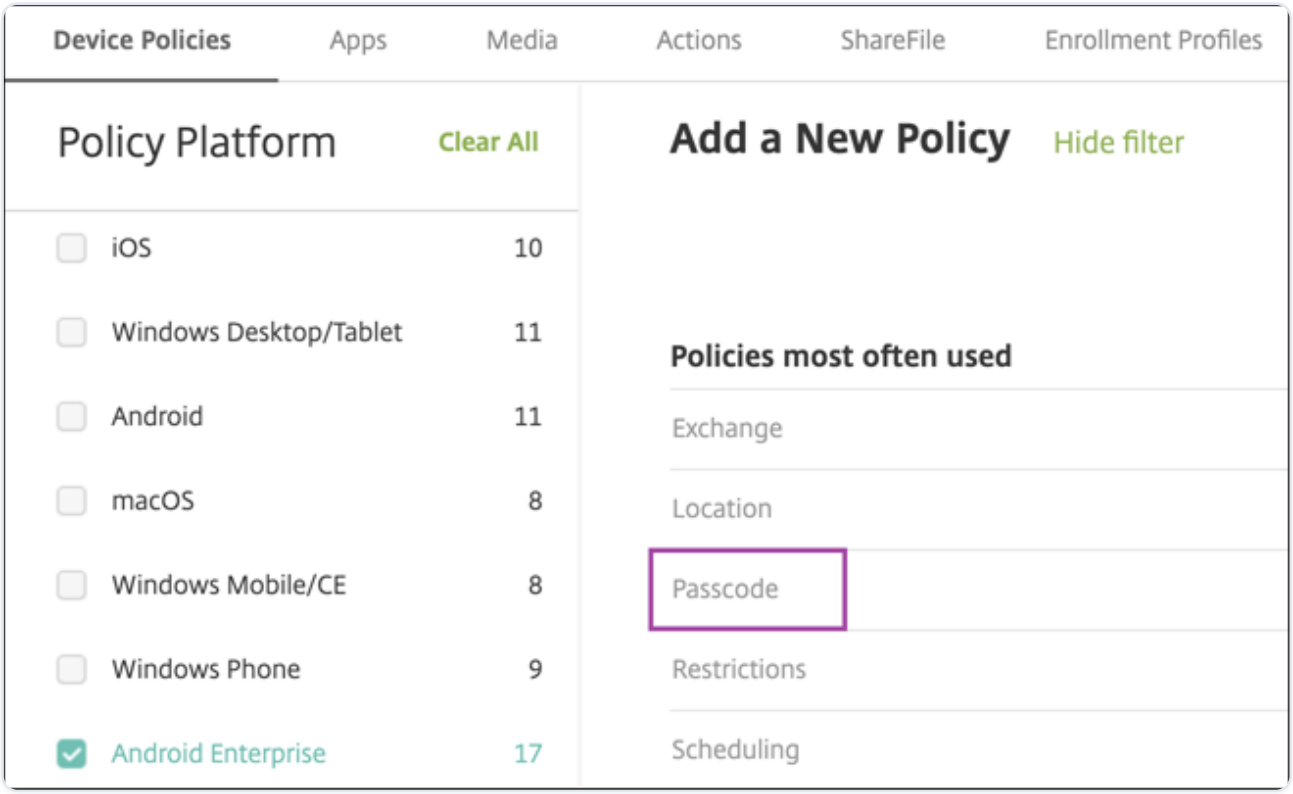
La directiva de dispositivo de código de acceso de Citrix Endpoint Management configura las reglas de desafío de seguridad. Los desafíos aparecen cuando los usuarios acceden a sus dispositivos o a los perfiles de trabajo de Android Enterprise en sus dispositivos. Un desafío de seguridad puede ser un código de acceso o un reconocimiento biométrico. Para obtener más

información sobre la directiva de código de acceso, consulte Directiva de dispositivo de código de acceso.

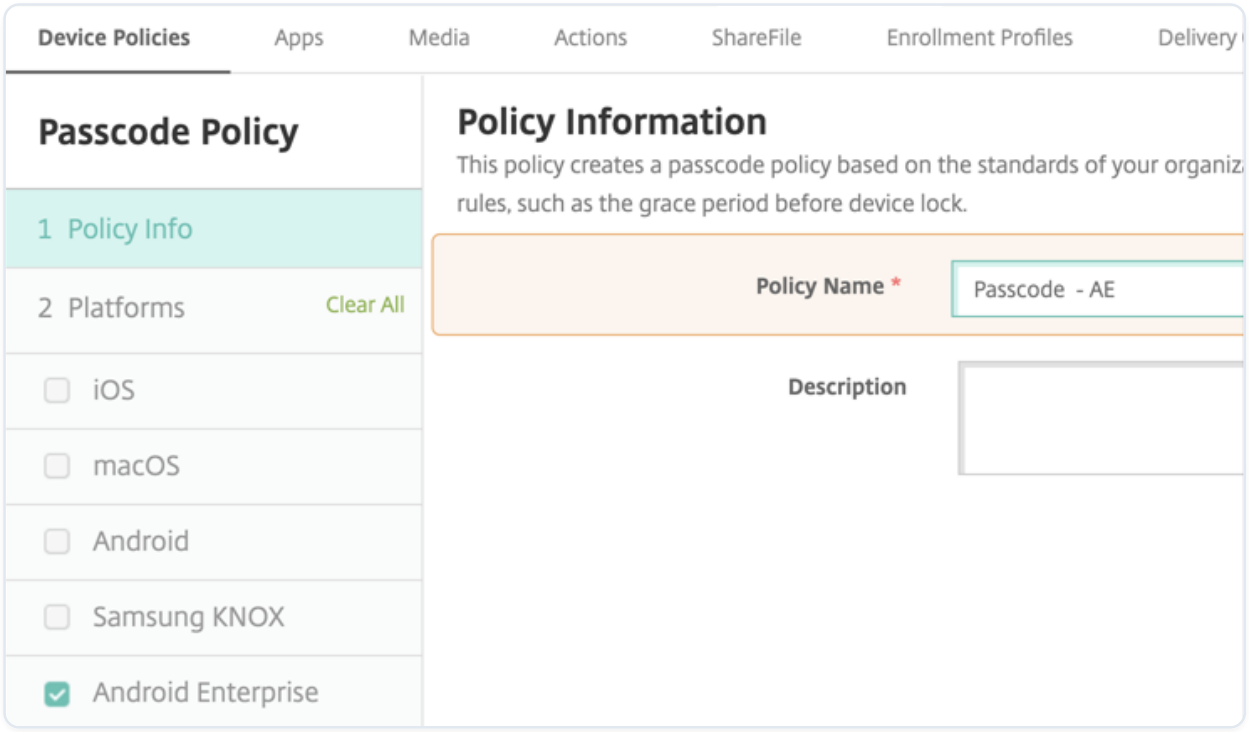
- Si su implementación de Android Enterprise incluye dispositivos BYOD, configure la directiva de código de acceso para el perfil de trabajo.
- Si su implementación incluye dispositivos propiedad de la empresa y totalmente administrados, configure la directiva de código de acceso para el propio dispositivo.
- Si su implementación incluye ambos tipos de dispositivos, configure ambos tipos de directiva de código de acceso.

Para configurar la directiva de código de acceso:

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Directivas de dispositivo**.
2. Haga clic en **Agregar**.
3. Haga clic en **Mostrar filtro** para mostrar el panel de **Plataforma de directivas**. En el panel de **Plataforma de directivas**, seleccione **Android Enterprise**.
4. Haga clic en **Código de acceso** en el panel derecho.



1. Introduzca un **Nombre de directiva**. Haga clic en **Siguiente**.



2. Configure la configuración de la directiva de código de acceso.
    - Establezca **Código de acceso del dispositivo requerido** en **Activado** para ver la configuración disponible para los desafíos de seguridad del propio dispositivo.
    - Establezca **Desafío de seguridad del perfil de trabajo** en **Activado** para ver la configuración disponible para los desafíos de seguridad del perfil de trabajo.
3. Haga clic en **Siguiente**.
4. Asigne la directiva a uno o varios grupos de entrega.
5. Haga clic en **Guardar**.

Creación de perfiles de inscripción

Los perfiles de inscripción controlan cómo se inscriben los dispositivos Android si Android Enterprise está habilitado para su implementación de Citrix Endpoint Management. Cuando crea un perfil de inscripción para inscribir dispositivos Android Enterprise, puede configurar el perfil de inscripción para inscribir dispositivos nuevos y restablecidos de fábrica como:

- Dispositivos totalmente administrados
- Dispositivos dedicados
- Dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos corporativos

También puede configurar cada uno de estos perfiles de inscripción de Android Enterprise para inscribir dispositivos Android BYOD como dispositivos con perfil de trabajo.

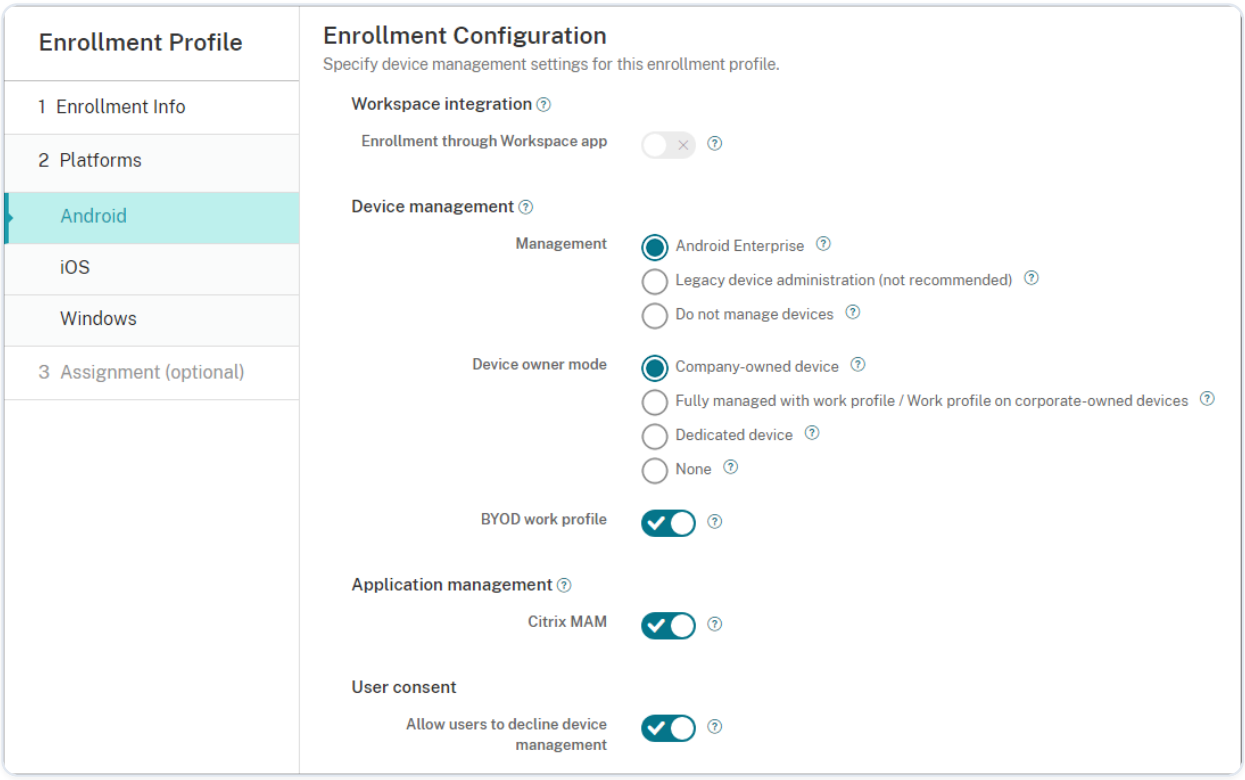
Si Android Enterprise está habilitado para su implementación de Citrix Endpoint Management, todos los dispositivos Android recién inscritos o reinscritos se inscriben como dispositivos Android Enterprise. De forma predeterminada, el perfil de inscripción global inscribe los dispositivos Android nuevos y restablecidos de fábrica como dispositivos totalmente administrados e inscribe los dispositivos Android BYOD como perfil de trabajo en dispositivos corporativos.

Al crear perfiles de inscripción, les asigna grupos de entrega. Si un usuario pertenece a varios grupos de entrega que tienen diferentes perfiles de inscripción, el nombre del grupo de entrega determina el perfil de inscripción utilizado. Citrix Endpoint Management selecciona el grupo de entrega que aparece en último lugar en una lista alfabética de grupos de entrega. Para obtener más información, consulte Perfiles de inscripción.

Agregar un perfil de inscripción para dispositivos totalmente administrados

El perfil de inscripción global inscribe dispositivos totalmente administrados de forma predeterminada, pero puede crear más perfiles de inscripción para inscribir dispositivos totalmente administrados.

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Perfiles de inscripción**.
2. Para agregar un perfil de inscripción, haga clic en **Agregar**. En la página Información de inscripción, escriba un nombre para el perfil de inscripción.
3. Establezca el número de dispositivos que los miembros con este perfil pueden inscribir.
4. Seleccione **Android** en **Plataformas** o haga clic en **Siguiente**. Aparece la página Configuración de inscripción.
5. Establezca **Administración** en **Android Enterprise**.
6. Establezca **Modo de propietario del dispositivo** en **Dispositivo corporativo**.



7. **Perfil de trabajo BYOD** le permite configurar el perfil de inscripción para inscribir dispositivos BYOD como dispositivos con perfil de trabajo. Los dispositivos nuevos y restablecidos de fábrica se inscriben como dispositivos totalmente administrados. Establezca **Perfil de trabajo BYOD** en **Activado** para permitir la inscripción de dispositivos BYOD como dispositivos con perfil de trabajo. Establezca **Perfil de trabajo BYOD** en **Desactivado** para restringir la inscripción a dispositivos totalmente administrados. El valor predeterminado es **Activado**.
8. Elija si desea inscribir dispositivos en Citrix MAM.
9. Si establece **Perfil de trabajo BYOD** en **Activado**, configure el consentimiento del usuario. Para permitir que los usuarios de dispositivos con perfil de trabajo BYOD rechacen la administración de dispositivos al inscribirlos, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Activado**.

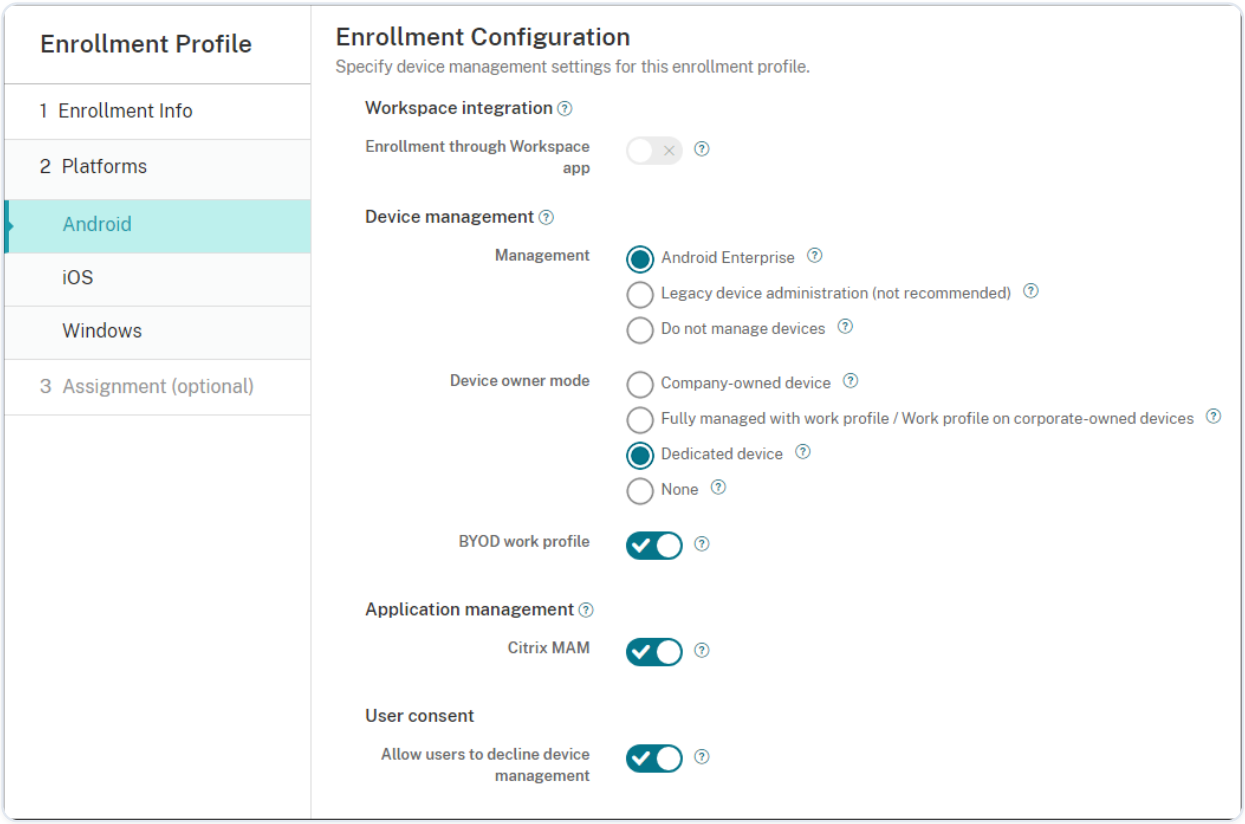
   Si **Perfil de trabajo BYOD** está establecido en **Activado**, el valor predeterminado de **Permitir a los usuarios rechazar la administración de dispositivos** es **Activado**. Si **Perfil de trabajo BYOD** está establecido en **Desactivado**, entonces **Permitir a los usuarios rechazar la administración de dispositivos** está inhabilitado.
10. Seleccione **Asignación (opciones)**. Aparece la pantalla Asignación de grupos de entrega.
11. Elija el grupo de entrega o los grupos de entrega que tienen los administradores que inscriben dispositivos totalmente administrados. A continuación, haga clic en **Guardar**.

    Aparece la página Perfil de inscripción con el perfil que ha agregado.

Agregar un perfil de inscripción de dispositivos dedicados

Cuando su implementación de Citrix Endpoint Management incluye dispositivos dedicados, un único administrador de Citrix Endpoint Management o un pequeño grupo de administradores inscriben muchos dispositivos dedicados. Para asegurarse de que estos administradores puedan inscribir todos los dispositivos necesarios, cree un perfil de inscripción para ellos con un número ilimitado de dispositivos permitidos por usuario.

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Perfiles de inscripción**.
2. Para agregar un perfil de inscripción, haga clic en **Agregar**. En la página Información de inscripción, escriba un nombre para el perfil de inscripción. Establezca en **Ilimitado** el número de dispositivos que los miembros con este perfil pueden inscribir.
3. Seleccione **Android** en **Plataformas** o haga clic en **Siguiente**. Aparece la página Configuración de inscripción.
4. Establezca **Administración** en **Android Enterprise**.
5. Establezca **Modo de propietario del dispositivo** en **Dispositivo dedicado**.



6. **Perfil de trabajo BYOD** le permite configurar el perfil de inscripción para inscribir dispositivos BYOD como dispositivos con perfil de trabajo. Los dispositivos nuevos y restablecidos de fábrica se inscriben como dispositivos dedicados. Establezca **Perfil de trabajo BYOD** en **Activado** para permitir la inscripción de dispositivos BYOD como dispositivos con perfil de

trabajo. Establezca **Perfil de trabajo BYOD** en **Desactivado** para restringir la inscripción a dispositivos propiedad de la empresa. El valor predeterminado es **Activado**.

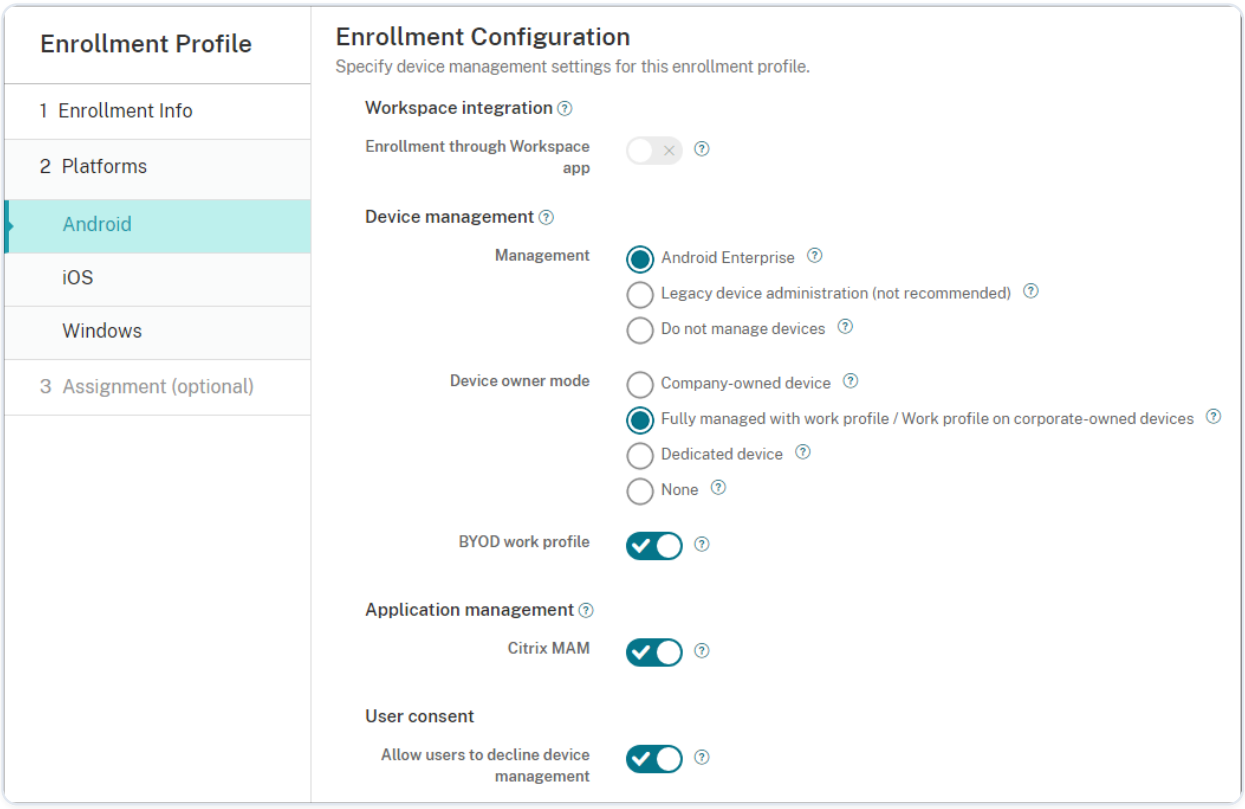
7. Elija si desea inscribir dispositivos en Citrix MAM.
8. Si establece **Perfil de trabajo BYOD** en **Activado**, configure el consentimiento del usuario. Para permitir que los usuarios de dispositivos con perfil de trabajo BYOD rechacen la administración de dispositivos al inscribirlos, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Activado**.

   Si **Perfil de trabajo BYOD** está establecido en **Activado**, el valor predeterminado de **Permitir a los usuarios rechazar la administración de dispositivos** es **Activado**. Si **Perfil de trabajo BYOD** está establecido en **Desactivado**, entonces **Permitir a los usuarios rechazar la administración de dispositivos** está inhabilitado.
9. Seleccione **Asignación (opciones)**. Aparece la pantalla Asignación de grupos de entrega.
10. Elija el grupo o los grupos de entrega que tienen los administradores que inscriben los dispositivos dedicados. A continuación, haga clic en **Guardar**.

    Aparece la página Perfil de inscripción con el perfil que ha agregado.

Agregar un perfil de inscripción para dispositivos totalmente administrados con un perfil de trabajo / perfil de trabajo en dispositivos propiedad de la empresa

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Perfiles de inscripción**.
2. Para agregar un perfil de inscripción, haga clic en **Agregar**. En la página Información de inscripción, escriba un nombre para el perfil de inscripción.
3. Establezca el número de dispositivos que los miembros con este perfil pueden inscribir.
4. Seleccione **Android** en **Plataformas** o haga clic en **Siguiente**. Aparece la página Configuración de inscripción.
5. Establezca **Administración** en **Android Enterprise**. Establezca **Modo de propietario del dispositivo** en **Totalmente administrado con perfil de trabajo / Perfil de trabajo en dispositivos propiedad de la empresa**.



6. **Perfil de trabajo BYOD** le permite configurar el perfil de inscripción para inscribir dispositivos BYOD como dispositivos con perfil de trabajo. Los dispositivos nuevos y restablecidos de fábrica se inscriben como dispositivos totalmente administrados con un perfil de trabajo. Establezca **Perfil de trabajo BYOD** en **Activado** para permitir la inscripción de dispositivos BYOD como dispositivos con perfil de trabajo. Establezca **Perfil de trabajo BYOD** en **Desactivado** para restringir la inscripción a dispositivos dedicados. El valor predeterminado es **Desactivado**.
7. Elija si desea inscribir dispositivos en Citrix MAM.
8. Si establece **Perfil de trabajo BYOD** en **Activado**, configure el consentimiento del usuario. Para permitir que los usuarios de dispositivos con perfil de trabajo BYOD rechacen la administración de dispositivos al inscribir sus dispositivos, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Activado**.

   Si **Perfil de trabajo BYOD** está establecido en **Activado**, el valor predeterminado de **Permitir a los usuarios rechazar la administración de dispositivos** es **Activado**. Si **Perfil de trabajo BYOD** está establecido en **Desactivado**, entonces **Permitir a los usuarios rechazar la administración de dispositivos** está inhabilitado.
9. Seleccione **Asignación (opciones)**. Aparece la pantalla Asignación de grupos de entrega.
10. Elija el grupo de entrega o los grupos de entrega que tienen los administradores que inscriben dispositivos totalmente administrados con un perfil de trabajo. A continuación, haga clic en **Guardar**.

Aparece la página Perfil de inscripción con el perfil que ha agregado.

Agregar un perfil de inscripción para dispositivos heredados

Google dejó de usar el modo de administrador de dispositivos para la administración de dispositivos. Google recomienda a los clientes que administren todos los dispositivos Android en modo de propietario del dispositivo o en modo de propietario del perfil. (Consulte Retirada del administrador de dispositivos en las guías para desarrolladores de Google Android Enterprise).

Para admitir este cambio:

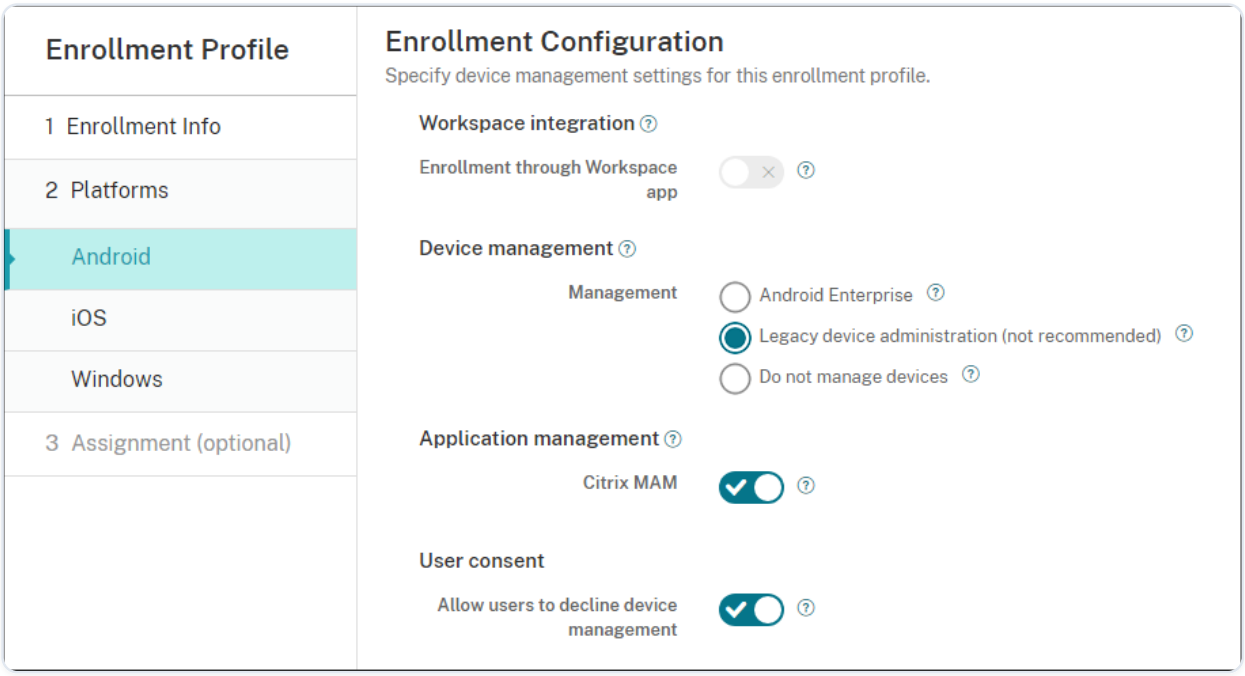
- Citrix convirtió Android Enterprise en la opción de inscripción predeterminada para los dispositivos Android.
- Si Android Enterprise está habilitado para su implementación de Citrix Endpoint Management, todos los dispositivos Android recién inscritos o reinscritos se inscriben como dispositivos Android Enterprise.

Es posible que su organización no esté lista para comenzar a administrar dispositivos Android heredados mediante Android Enterprise. En ese caso, puede seguir administrándolos en modo de administrador de dispositivos. Para los dispositivos ya inscritos en modo de administrador de dispositivos, Citrix Endpoint Management continúa administrándolos en modo de administrador de dispositivos.

Cree un perfil de inscripción para dispositivos heredados para permitir que las nuevas inscripciones de dispositivos Android utilicen el modo de administrador de dispositivos.

Para crear un perfil de inscripción para dispositivos heredados:

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Perfiles de inscripción**.
2. Para agregar un perfil de inscripción, haga clic en **Agregar**. En la página Información de inscripción, escriba un nombre para el perfil de inscripción.
3. Establezca el número de dispositivos que los miembros con este perfil pueden inscribir.
4. Seleccione **Android** en **Plataformas** o haga clic en **Siguiente**. Aparece la página Configuración de inscripción.
5. Establezca **Administración** en **Administración de dispositivos heredados (no recomendado)**. Haga clic en **Siguiente**.



6. Elija si quiere inscribir dispositivos en Citrix MAM.
7. Para permitir que los usuarios rechacen la administración de dispositivos al inscribir sus dispositivos, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Activado**. El valor predeterminado es **Activado**.
8. Seleccione **Asignación (opciones)**. Aparece la pantalla Asignación de grupos de entrega.
9. Elija el grupo de entrega o los grupos de entrega que tienen los administradores que inscriben los dispositivos dedicados. A continuación, haga clic en **Guardar**.

Aparece la página Perfil de inscripción con el perfil que ha agregado.

Para seguir administrando dispositivos heredados en el modo de administrador de dispositivos, inscríbalos o reinscríbalos con este perfil. Los dispositivos de administrador de dispositivos se inscriben de forma similar a los dispositivos de perfil de trabajo, haciendo que los usuarios descarguen Citrix Secure Hub y proporcionando una URL de servidor de inscripción.

Aprovisionamiento de dispositivos con perfil de trabajo de Android Enterprise

Los dispositivos con perfil de trabajo de Android Enterprise se inscriben en modo de propietario de perfil. Estos dispositivos no necesitan ser nuevos ni restablecerse de fábrica. Los dispositivos BYOD se inscriben como dispositivos con perfil de trabajo. La experiencia de inscripción es similar a la inscripción de Android en Citrix Endpoint Management. Los usuarios descargan Citrix Secure Hub de Google Play e inscriben sus dispositivos.

De forma predeterminada, las opciones **Depuración USB y Orígenes desconocidos** se deshabilitan en un dispositivo al inscribirlo en Android Enterprise como dispositivo con perfil de trabajo.

Al inscribir dispositivos en Android Enterprise como dispositivos con perfil de trabajo, vaya siempre a Google Play. Desde allí, habilite Citrix Secure Hub para que aparezca en el perfil personal del usuario.

Aprovisionamiento de dispositivos totalmente administrados de Android Enterprise

Puede inscribir dispositivos totalmente administrados en la implementación que configuró en las secciones anteriores. Los dispositivos totalmente administrados son dispositivos propiedad de la empresa y se inscriben en modo de propietario del dispositivo. Solo los dispositivos nuevos o restablecidos de fábrica se pueden inscribir en modo de propietario del dispositivo.

Puede inscribir dispositivos en modo de propietario del dispositivo mediante cualquiera de estos métodos de inscripción:

- **Token de identificador de DPC:** Con este método de inscripción, los usuarios introducen los caracteres `afw#xenmobile` al configurar el dispositivo. `afw#xenmobile` es el token de identificador de DPC de Citrix. Este token identifica el dispositivo como administrado por Citrix Endpoint Management y descarga Citrix Secure Hub de Google Play Store. Consulte Inscribir dispositivos mediante el token de identificador de DPC de Citrix.
- **Toque NFC (comunicación de campo cercano):** El método de inscripción por toque NFC transfiere datos entre dos dispositivos mediante comunicación de campo cercano. Bluetooth, Wi-Fi y otros modos de comunicación están inhabilitados en un dispositivo nuevo o restablecido de fábrica. NFC es el único protocolo de comunicación que el dispositivo puede usar en este estado. Consulte Inscribir dispositivos con toque NFC.
- **Código QR:** La inscripción con código QR se puede usar para inscribir una flota distribuida de dispositivos que no admiten NFC, como las tabletas. El método de inscripción con código QR configura el modo de perfil del dispositivo escaneando un código QR desde el asistente de configuración. Consulte Inscribir dispositivos mediante un código QR.
- **Zero-touch:** La inscripción Zero-touch le permite configurar los dispositivos para que se inscriban automáticamente cuando se encienden por primera vez. La inscripción Zero-touch es compatible con algunos dispositivos Android que ejecutan Android 9.0 o posterior. Consulte Inscripción Zero-touch.
- **Cuentas de Google:** Los usuarios introducen sus credenciales de la cuenta de Google para iniciar el proceso de aprovisionamiento. Esta opción es para empresas que utilizan Google Workspace.

Inscribir dispositivos mediante el token de identificador de DPC de Citrix

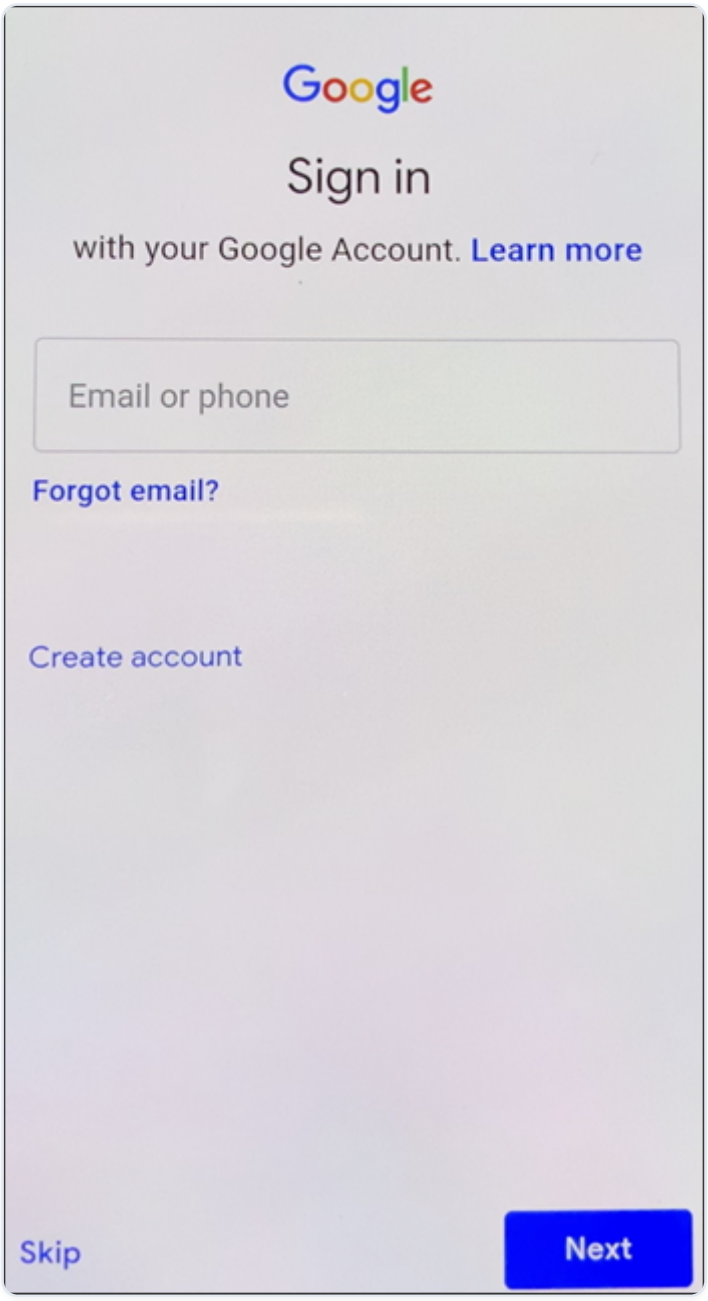
Los usuarios introducen `afw#xenmobile` cuando se les pide que introduzcan una cuenta de Google después de encender dispositivos nuevos o restablecidos de fábrica para la configuración inicial. Esta acción descarga e instala Citrix Secure Hub. A continuación, los usuarios siguen las indicaciones de configuración de Citrix Secure Hub para completar la inscripción.

REQUISITOS DEL SISTEMA

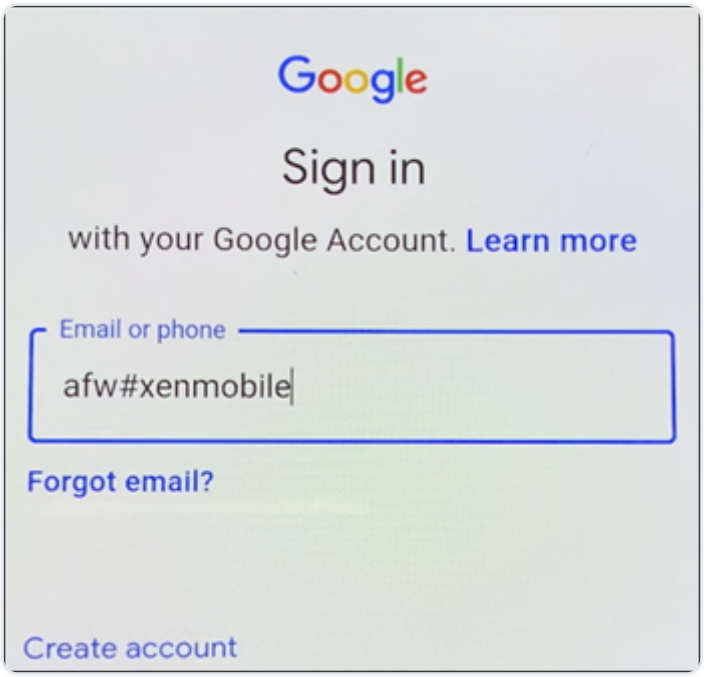
- Compatible con todos los dispositivos Android que ejecutan el sistema operativo Android.

PARA INSCRIBIR EL DISPOSITIVO

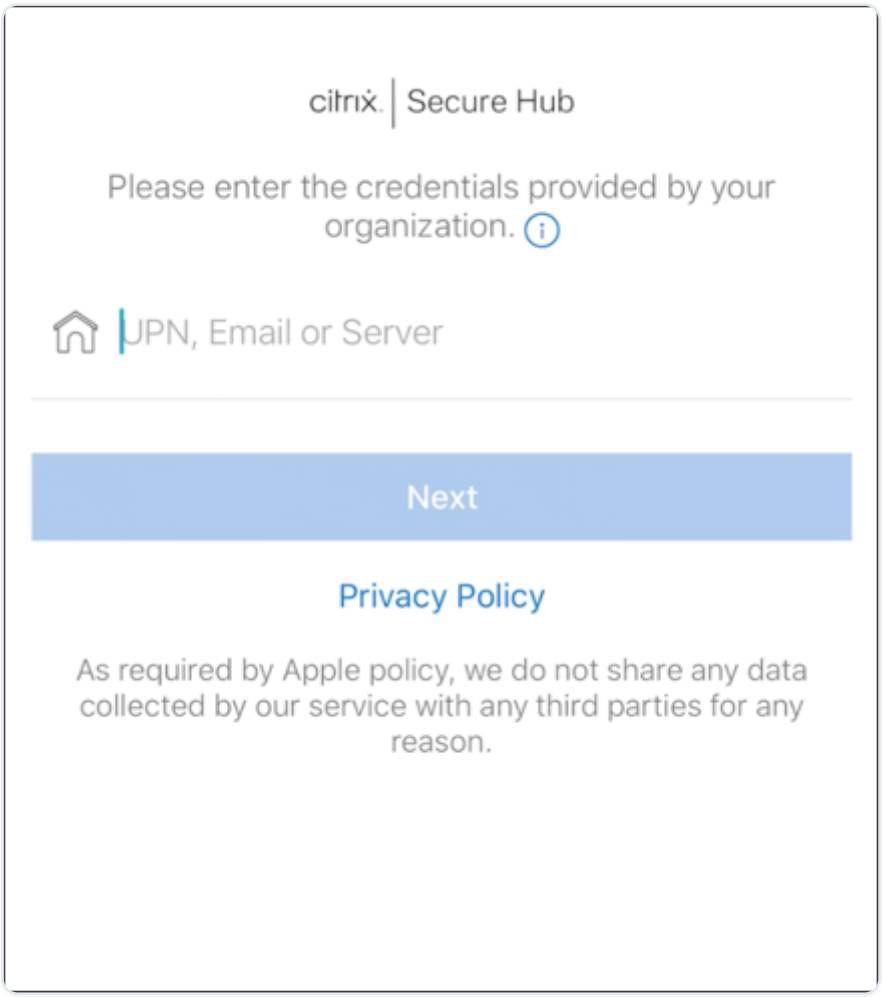
1. Encienda un dispositivo nuevo o restablecido de fábrica.
2. La configuración inicial del dispositivo se carga y solicita una cuenta de Google. Si el dispositivo carga la pantalla de inicio del dispositivo, compruebe la barra de notificaciones para ver una notificación de **Finalizar configuración**.



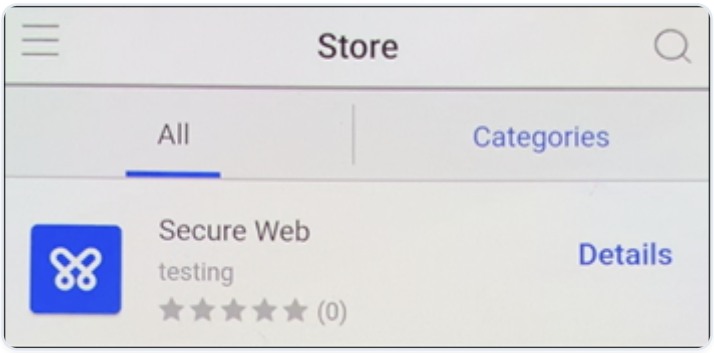
3. Introduzca `afw#xenmobile` en el campo **Correo electrónico o teléfono**.



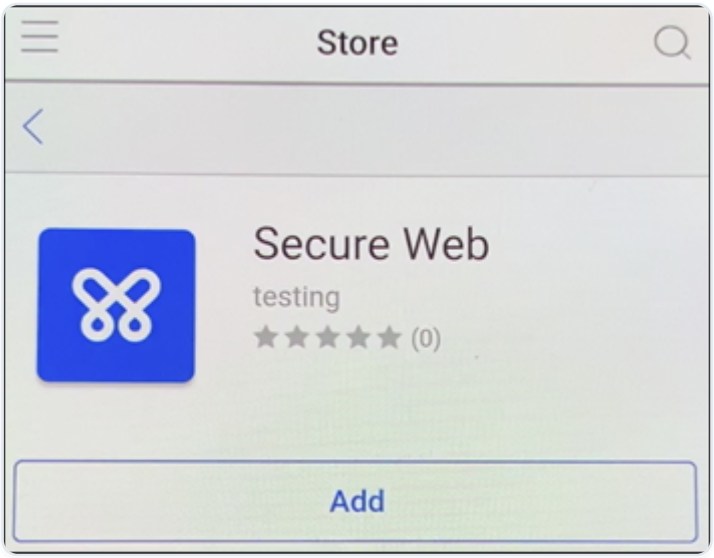
4. Toque **Instalar** en la pantalla de Android Enterprise que le pide que instale Citrix Secure Hub.
5. Toque **Instalar** en la pantalla del instalador de Citrix Secure Hub.
6. Toque **Permitir** para todas las solicitudes de permisos de aplicaciones.
7. Toque **Aceptar y continuar** para instalar Citrix Secure Hub y permitirle administrar el dispositivo.
8. Citrix Secure Hub ya está instalado y en la pantalla de inscripción predeterminada. En este ejemplo, AutoDiscovery no está configurado. Si lo está, el usuario puede introducir su nombre de usuario/correo electrónico y se le puede encontrar un servidor. En su lugar, introduzca la URL de inscripción para el entorno y toque **Siguiente**.



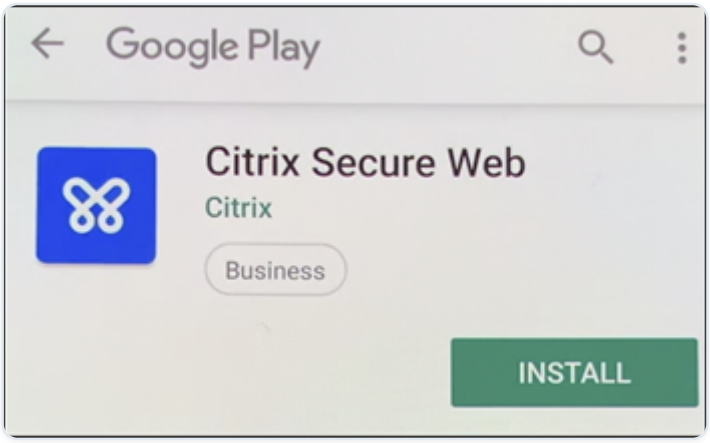
9. La configuración predeterminada de Citrix Endpoint Management permite a los usuarios elegir si utilizan MAM o MDM+MAM. Si se le solicita de esta manera, toque **Sí, inscribir** para elegir MDM+MAM.
10. Introduzca la dirección de correo electrónico y la contraseña del usuario, y luego toque **Siguiente**.
11. Se le pide al usuario que configure un código de acceso del dispositivo. Toque **Establecer** e introduzca un código de acceso.
12. Se le pide al usuario que configure un método de desbloqueo del perfil de trabajo. Para este ejemplo, toque **Contraseña**, toque **PIN** e introduzca un PIN.
13. El dispositivo se encuentra ahora en la pantalla de inicio **Mis aplicaciones** de Citrix Secure Hub. Toque **Agregar aplicaciones de la tienda**.
14. Para agregar Citrix Secure Web, toque **Citrix Secure Web**.



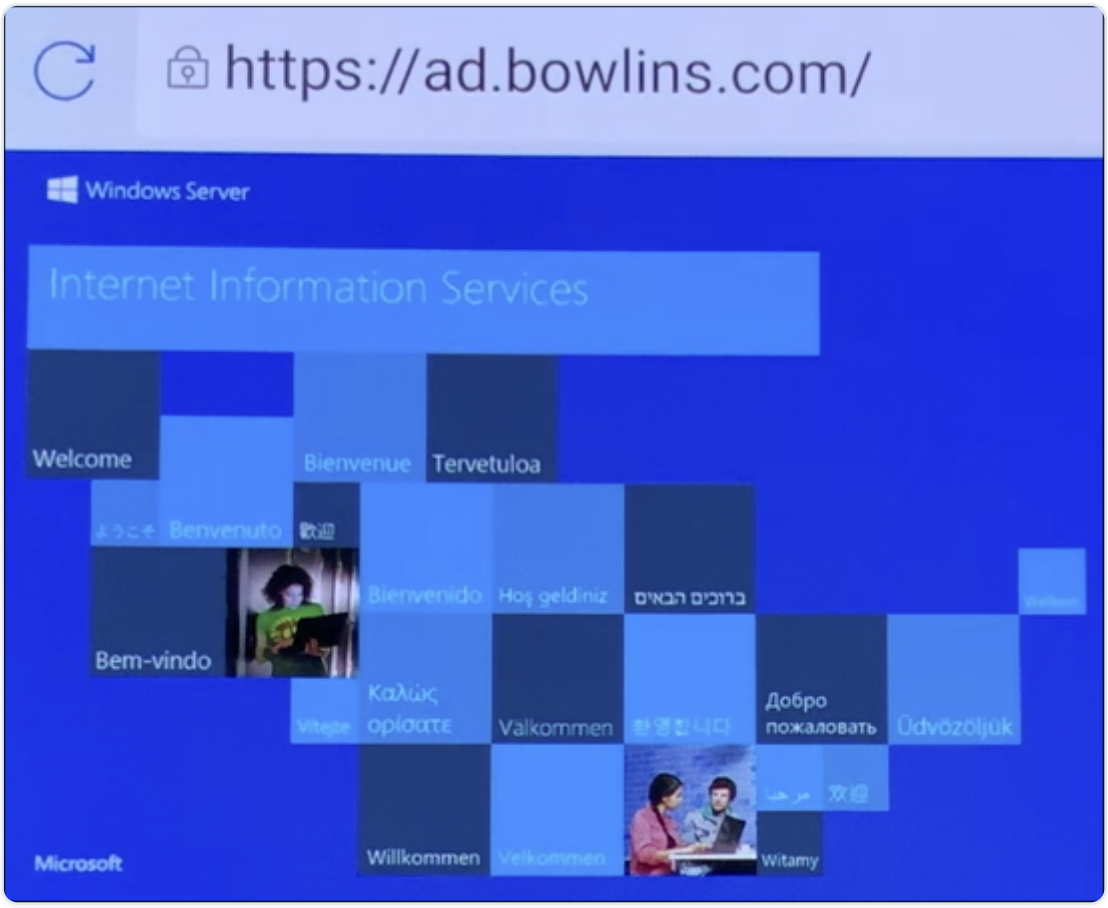
15. Pulse **Añadir**.



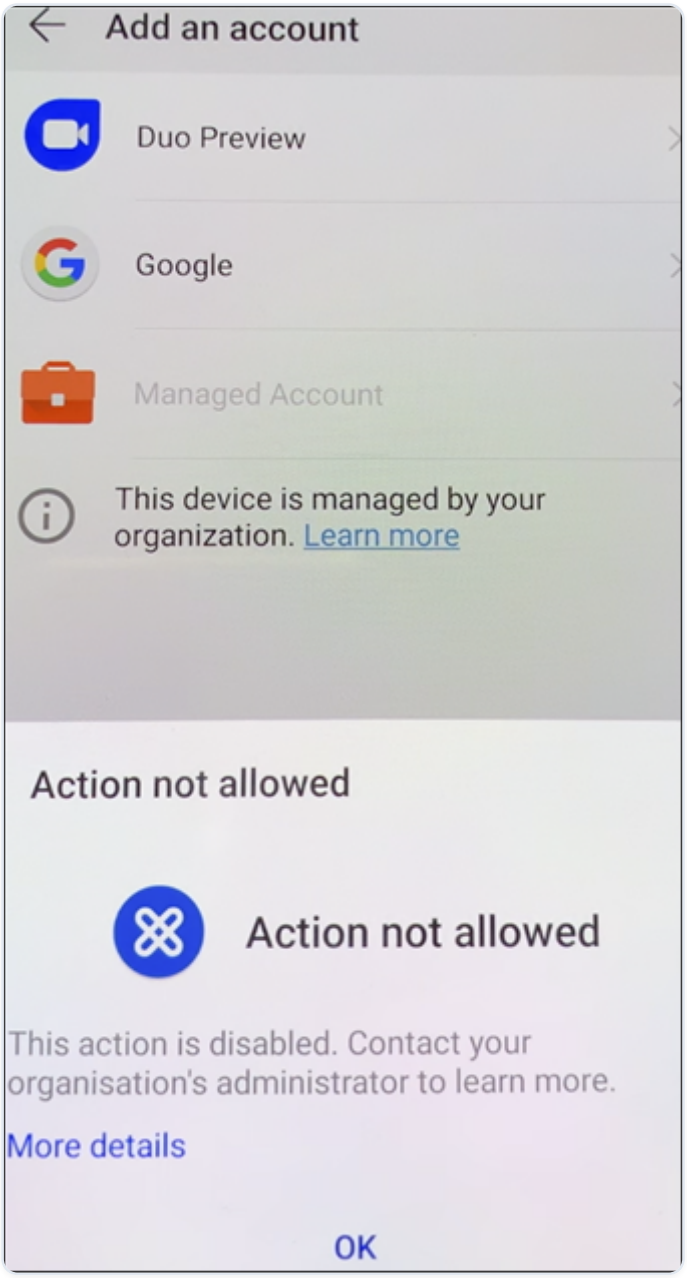
16. Citrix Secure Hub dirige al usuario a Google Play Store para instalar Citrix Secure Web. Pulse **Instalar**.



17. Una vez instalado Citrix Secure Web, pulse **Abrir**. Introduzca una URL de un sitio interno en la barra de direcciones y verificar que la página se carga.



18. Vaya a **Configuración > Cuentas** en el dispositivo. Observe que la **Cuenta administrada** no se puede modificar. Las opciones de desarrollador para compartir pantalla o la depuración remota también están bloqueadas.



Inscripción de dispositivos con NFC bump

Para inscribir un dispositivo como dispositivo totalmente administrado mediante NFC bumps se necesitan dos dispositivos: uno que se haya restablecido a la configuración de fábrica y otro que ejecute la herramienta de aprovisionamiento de Citrix Endpoint Management.

REQUISITOS DEL SISTEMA Y REQUISITOS PREVIOS

- Dispositivos Android compatibles.
- Un dispositivo nuevo o restablecido de fábrica con la función NFC, aprovisionado para Android Enterprise como dispositivo totalmente administrado. Consulte la sección sobre Aprovisionamiento de dispositivos Android Enterprise totalmente administrados.

- Otro dispositivo con la función NFC, que ejecute la herramienta de aprovisionamiento configurada. La herramienta de aprovisionamiento está disponible en Citrix Secure Hub o en la página de descargas de Citrix.

Cada dispositivo puede tener un solo perfil de Android Enterprise. En este caso, el perfil es para un Citrix Secure Hub administrado. Intentar añadir una segunda aplicación DPC elimina el Citrix Secure Hub instalado.

DATOS TRANSFERIDOS MEDIANTE EL TOQUE NFC

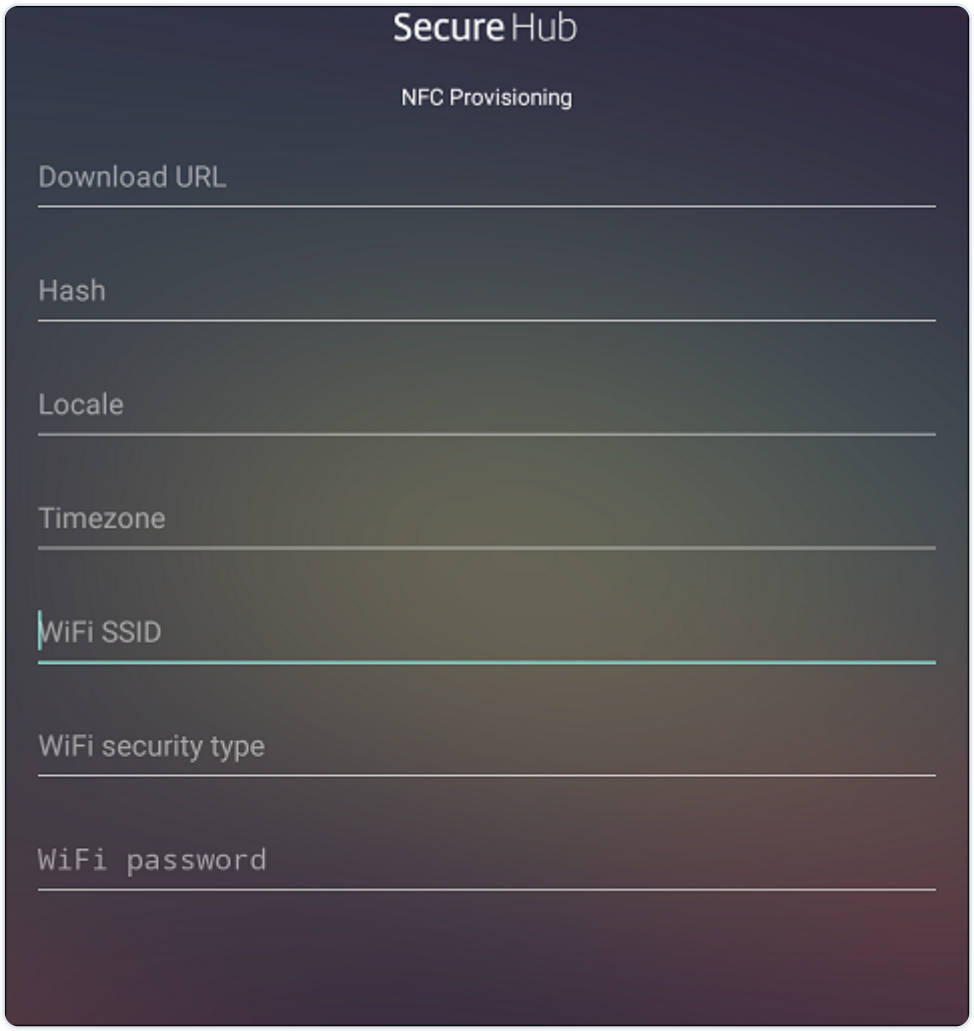
El aprovisionamiento de un dispositivo restablecido de fábrica requiere que envíe los siguientes datos mediante un toque NFC para iniciar Android Enterprise:

- Nombre del paquete de la aplicación DPC que actúa como propietario del dispositivo (en este caso, Citrix Secure Hub).
- Ubicación de intranet/internet desde la que el dispositivo puede descargar la aplicación DPC.
- Hash SHA-256 de la aplicación DPC para verificar si la descarga se ha realizado correctamente.
- Detalles de conexión Wi-Fi para que un dispositivo restablecido de fábrica pueda conectarse y descargar la aplicación DPC. Nota: Android ya no es compatible con Wi-Fi 802.1x para este paso.
- Zona horaria del dispositivo (opcional).
- Ubicación geográfica del dispositivo (opcional).

Cuando los dos dispositivos se tocan, los datos de la Herramienta de aprovisionamiento se envían al dispositivo restablecido de fábrica. Esos datos se utilizan luego para descargar Citrix Secure Hub con la configuración de administrador. Si no introduce los valores de zona horaria y ubicación, Android configura automáticamente los valores en el nuevo dispositivo.

CONFIGURACIÓN DE LA HERRAMIENTA DE APROVISIONAMIENTO DE CITRIX ENDPOINT MANAGEMENT

Antes de realizar un toque NFC, debe configurar la Herramienta de aprovisionamiento. Esta configuración se transfiere luego al dispositivo restablecido de fábrica durante el toque NFC.



Puede introducir datos en los campos obligatorios o rellenarlos mediante un archivo de texto. Los pasos del siguiente procedimiento describen cómo configurar el archivo de texto con descripciones para cada campo. La aplicación no guarda la información después de introducirla, por lo que es posible que desee crear un archivo de texto para conservar la información para uso futuro.

Para configurar la Herramienta de aprovisionamiento mediante un archivo de texto

Asigne el nombre nfcprovisioning.txt al archivo y colóquelo en la carpeta `/sdcard/` de la tarjeta SD del dispositivo. La aplicación podrá leer el archivo de texto y rellenar los valores.

El archivo de texto debe contener los siguientes datos:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

Esta línea es la ubicación de intranet/internet de la aplicación del proveedor de EMM. Después de que el dispositivo restablecido de fábrica se conecte a la red Wi-Fi tras el toque NFC, el dispositivo debe tener acceso a esta ubicación para la descarga. La URL es una URL normal, sin necesidad de formato especial.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>`

Esta línea es la suma de comprobación (checksum) de la aplicación del proveedor de EMM. Esta suma de comprobación se utiliza para verificar que la descarga se ha realizado correctamente. Los pasos para obtener la suma de comprobación se explican más adelante en este artículo.

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

Esta línea es el SSID de la red Wi-Fi conectada del dispositivo en el que se ejecuta la herramienta de aprovisionamiento.

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

Los valores admitidos son WEP y WPA2. Si la red Wi-Fi no está protegida, este campo debe estar vacío.

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

Si la red Wi-Fi no está protegida, este campo debe estar vacío.

`android.app.extra.PROVISIONING_LOCALE=<locale>`

Introduzca los códigos de idioma y país. Los códigos de idioma son códigos ISO de idioma de dos letras en minúscula (como en) según lo definido por ISO 639-1. Los códigos de país son códigos ISO de país de dos letras en mayúscula (como US) según lo definido por ISO 3166-1. Por ejemplo, escriba en_US para el inglés hablado en Estados Unidos. Si no introduce ningún código, el país y el idioma se rellenan automáticamente.

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

La zona horaria en la que se ejecuta el dispositivo. Escriba el nombre de la base de datos del área/ubicación. Por ejemplo, escriba **America/Los_Angeles** para la hora del Pacífico. Si no escribe un nombre, la zona horaria se rellena automáticamente.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

Estos datos no son necesarios, porque el valor está codificado en la aplicación como Citrix Secure Hub. Se menciona aquí solo por motivos de exhaustividad.

Si hay una red Wi-Fi protegida con WPA2, un archivo nfcprovisioning.txt completado podría tener el siguiente aspecto:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk`

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name`

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2`

`android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere`

`android.app.extra.PROVISIONING_LOCALE=en_US`

`android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles`

Si hay una red Wi-Fi sin protección, un archivo nfcprovisioning.txt completado podría tener el siguiente aspecto:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk`

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name`

`android.app.extra.PROVISIONING_LOCALE=en_US`

`android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles`

PARA OBTENER LA SUMA DE COMPROBACIÓN DE CITRIX SECURE HUB

La suma de comprobación de Citrix Secure Hub es un valor constante: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`. Para descargar un archivo APK de Citrix Secure Hub, utilice el siguiente enlace de Google Play Store: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

PARA OBTENER LA SUMA DE COMPROBACIÓN DE UNA APLICACIÓN

Requisitos previos:

- La herramienta **apksigner** de Android SDK Build Tools
- Línea de comandos de OpenSSL

Para obtener la suma de comprobación de cualquier aplicación, siga estos pasos:

1. Descargue el archivo APK de la aplicación desde Google Play Store.
2. En la línea de comandos de OpenSSL, vaya a la herramienta **apksigner**: `android-sdk/build-tools/<version>/apksigner` y escriba lo siguiente:

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{(?
<=SHA-256 digest:) .*}'  | xxd -r -p | openssl base64 | tr -d '=' | tr
-- '+/=' '-_'
```

El comando devuelve una suma de comprobación válida.

3. Para generar el código QR, introduzca la suma de comprobación en el campo `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM`. Por ejemplo:

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",


"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUth
eu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?
identifier=xenmobile",

  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"

   }

}
```

BIBLIOTECAS UTILIZADAS

La herramienta de aprovisionamiento utiliza las siguientes bibliotecas en su código fuente:

- Biblioteca v7 `appcompat`, biblioteca Design Support y biblioteca v7 palette support de Google bajo licencia Apache 2.0

  Para obtener información, consulte Guía de funciones de la biblioteca de soporte.

- Butter Knife de Jake Wharton bajo licencia Apache 2.0

Inscribir dispositivos mediante un código QR

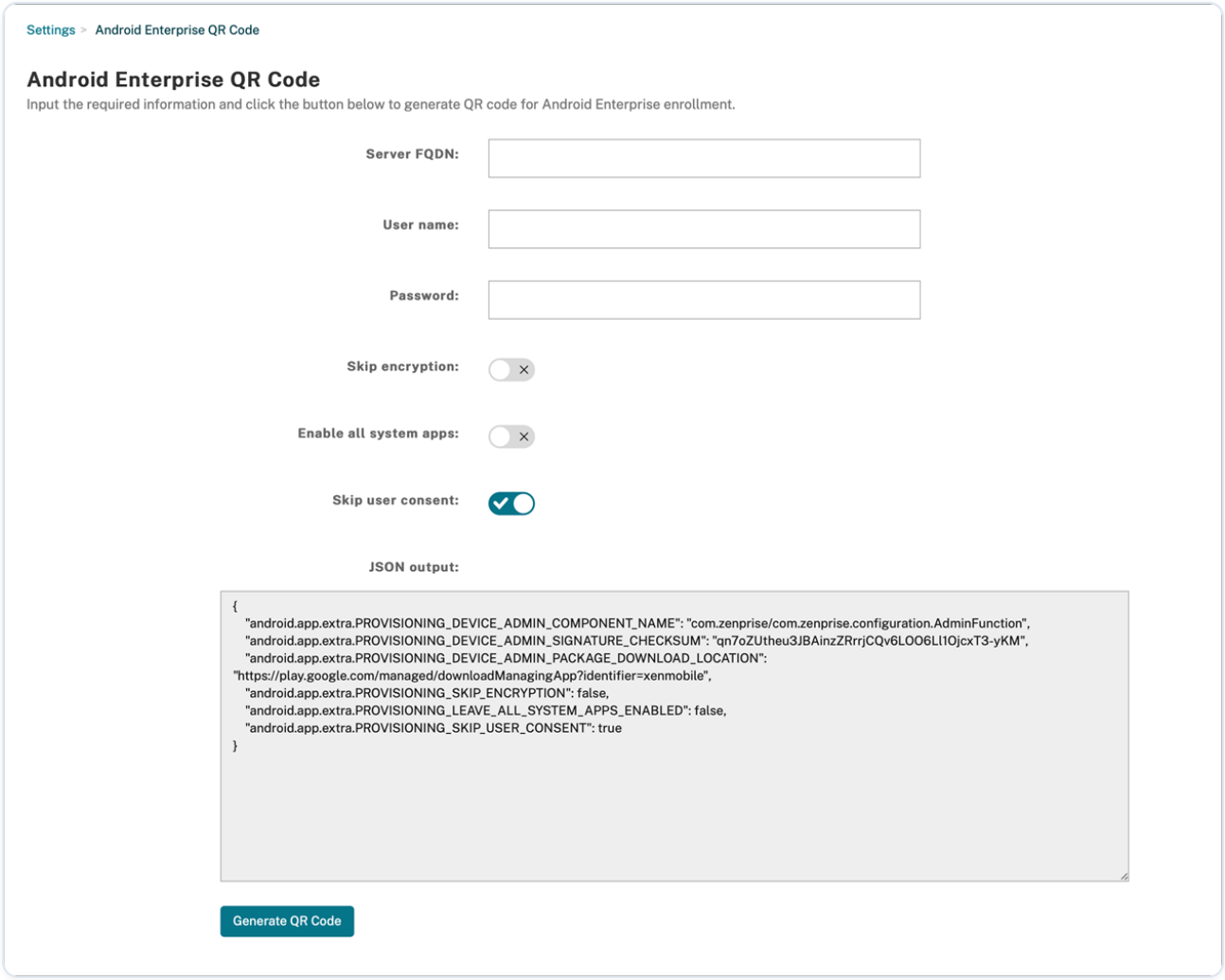
Los usuarios pueden inscribir un dispositivo totalmente administrado mediante el código QR que usted genere para ellos.

REQUISITOS DEL SISTEMA

Dispositivos Android con Android 7.0 o posterior.

CREAR UN CÓDIGO QR

Usted genera un código QR especificando la información de inscripción según sea necesario. Después de generar un código QR, guárdelo localmente. Citrix Endpoint Management no lo almacena.



1. Vaya a **Parámetros > Código QR de Android Enterprise**.
2. Si es necesario, especifique la siguiente información de inscripción:
    - **FQDN del servidor:** Escriba el FQDN del servidor de Citrix Endpoint Management (por ejemplo, `example.cem.cloud.com`). Este campo es opcional. Si lo deja vacío, los usuarios deben rellenar esta información al inscribirse.

- **Nombre de usuario:** Escriba el nombre de usuario utilizado para la inscripción. Si tiene previsto distribuir el código QR a más de un usuario, le recomendamos dejar este campo vacío. Configurar un código QR con un nombre de usuario y una contraseña es útil para inscribir dispositivos de quiosco. Si deja el campo vacío, los usuarios deben rellenar esta información al inscribirse.
- **Contraseña:** Escriba la contraseña asociada al nombre de usuario que ha introducido. Si deja el campo vacío, los usuarios deben rellenar esta información al inscribirse.
- **Omitir cifrado:** Si está en **Activado**, el dispositivo no se cifra durante la inscripción. El valor predeterminado es **Desactivado**.
- **Habilitar todas las aplicaciones del sistema:** Si está **Activado**, permite el acceso a todas las aplicaciones del sistema en el dispositivo. El valor predeterminado es **Desactivado**.
- **Omitir consentimiento del usuario:** Si está **Desactivado**, los usuarios pueden optar por no participar en la administración de dispositivos. El valor predeterminado es **Desactivado**.

El cuadro **Salida JSON** muestra el contenido JSON que corresponde a la información que especificó.

3. Para agregar más información de inscripción, edite el contenido JSON en el cuadro **Salida JSON**.
4. Haga clic en **Generar código QR**. El código QR aparece a la derecha de la salida JSON.
5. Haga clic con el botón derecho en la imagen del código QR y guárdela.
6. Envíe la imagen a los usuarios para la inscripción de dispositivos.

Un dispositivo restablecido de fábrica escanea este código QR para inscribirse como un dispositivo totalmente administrado.

PARA INSCRIBIR EL DISPOSITIVO

Después de encender un dispositivo nuevo o restablecido de fábrica:

1. Toque la pantalla seis veces en la pantalla de bienvenida para iniciar el flujo de inscripción con código QR.
2. Cuando se le solicite, conéctese a una red Wi-Fi. La ubicación de descarga de Citrix Secure Hub en el código QR es accesible a través de esta red Wi-Fi.

   Una vez que el dispositivo se conecta correctamente a la red Wi-Fi, descarga un lector de códigos QR de Google e inicia la cámara.
3. Apunte la cámara al código QR para escanear el código.

Android descarga Citrix Secure Hub desde la ubicación de descarga en el código QR, valida la firma del certificado de firma, instala Citrix Secure Hub y lo establece como propietario del dispositivo.

Para obtener más información, consulte esta guía de Google para desarrolladores de Android EMM: `<https://developers.google.com/android/work/prov-devices#qr_code_method>`.

Inscripción Zero-touch

La inscripción Zero-touch le permite configurar dispositivos para que se aprovisionen como dispositivos totalmente administrados cuando se encienden por primera vez.

Su distribuidor de dispositivos crea una cuenta para usted en el portal Zero-touch de Android, una herramienta en línea que le permite aplicar configuraciones a los dispositivos. Con el portal Zero-touch de Android, cree una o varias configuraciones de inscripción Zero-touch y aplíquelas a los dispositivos asignados a su cuenta. Cuando los usuarios encienden estos dispositivos, se inscriben automáticamente en Citrix Endpoint Management. La configuración asignada al dispositivo define su proceso de inscripción automática.

REQUISITOS DEL SISTEMA

- La compatibilidad con la inscripción Zero-touch comienza con Android 9.0.

DISPOSITIVOS E INFORMACIÓN DE LA CUENTA DE SU DISTRIBUIDOR

- Los dispositivos aptos para la inscripción Zero-touch se compran a un distribuidor empresarial o a un socio de Google. Para obtener una lista de los socios Zero-touch de Android Enterprise, consulte el sitio web de Android.
- Una cuenta del portal Zero-touch de Android Enterprise, creada por su distribuidor.
- Información de inicio de sesión de la cuenta del portal Zero-touch de Android Enterprise, proporcionada por su distribuidor.

CREAR UNA CONFIGURACIÓN ZERO-TOUCH

Al crear una configuración Zero-touch, incluya un JSON personalizado para especificar los detalles de la configuración.

Utilice este JSON para configurar el dispositivo para que se inscriba en el servidor de Citrix Endpoint Management que especifique. Reemplace la URL de su servidor por 'URL' en este ejemplo.

```
{

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

  {

        "serverURL":"URL"

   }

}
```

Puede utilizar un JSON opcional con más parámetros para personalizar aún más su configuración. Este ejemplo especifica el servidor de Citrix Endpoint Management y el nombre de usuario y la contraseña que los dispositivos que utilizan esta configuración usan para iniciar sesión en el servidor.

```
{

   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

     {

         "serverURL":"URL",

         "xm_username":"username",

         "xm_password":"password"

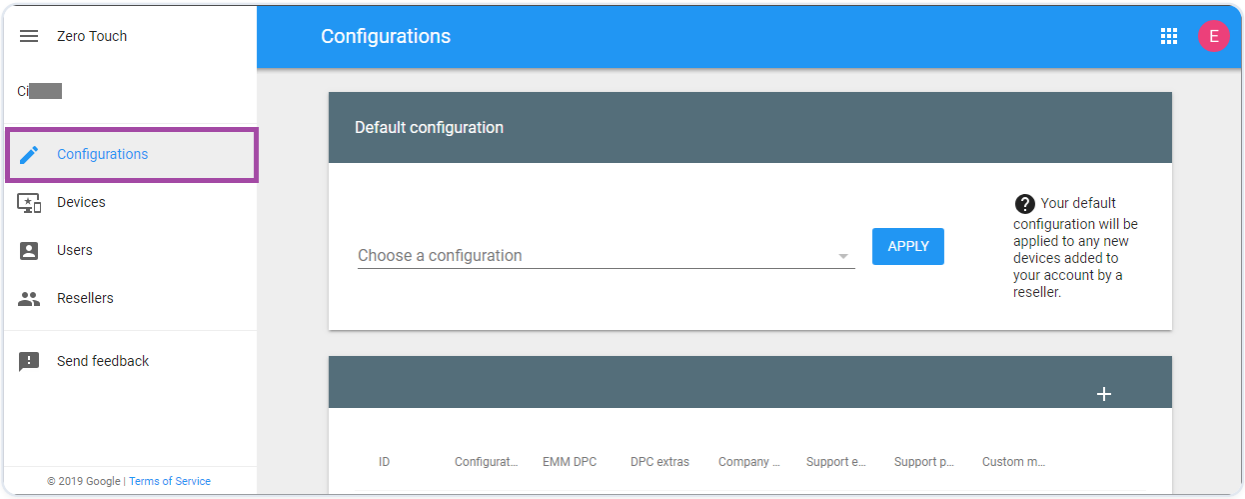
     }

       }
```

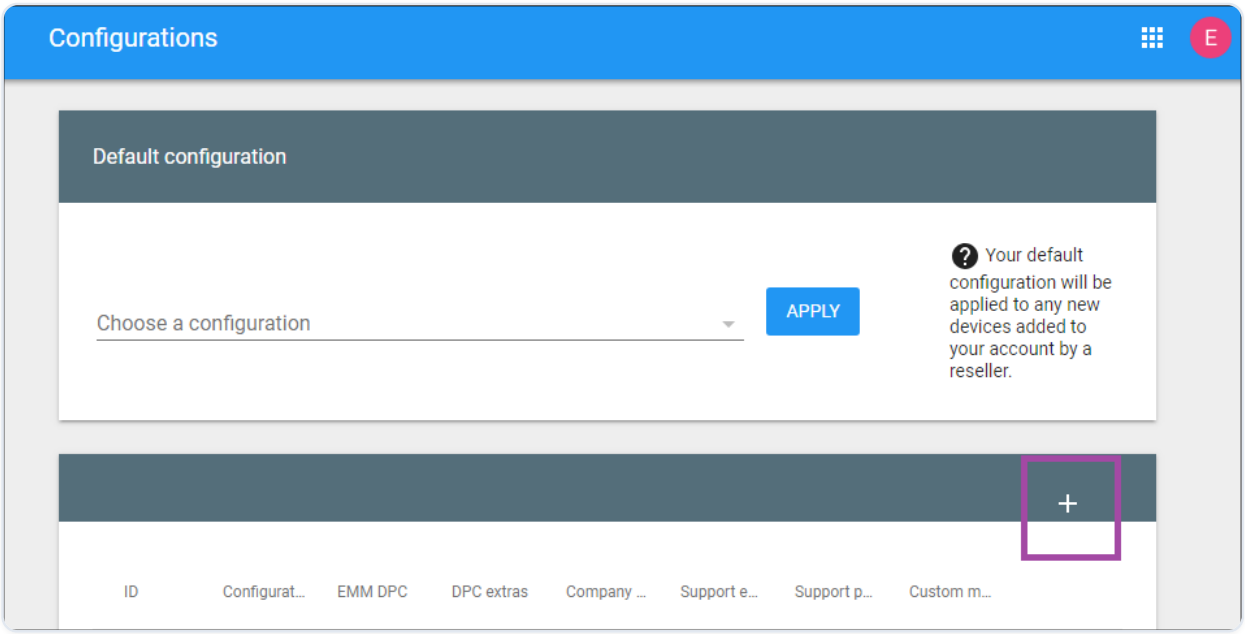
Importante:

Para inscribir dispositivos en el perfil de trabajo en el modo de dispositivos propiedad de la empresa, añada `{"desiredProvisioningMode": "managedProfile"}` al JSON personalizado en `PROVISIONING_ADMIN_EXTRAS_BUNDLE`.

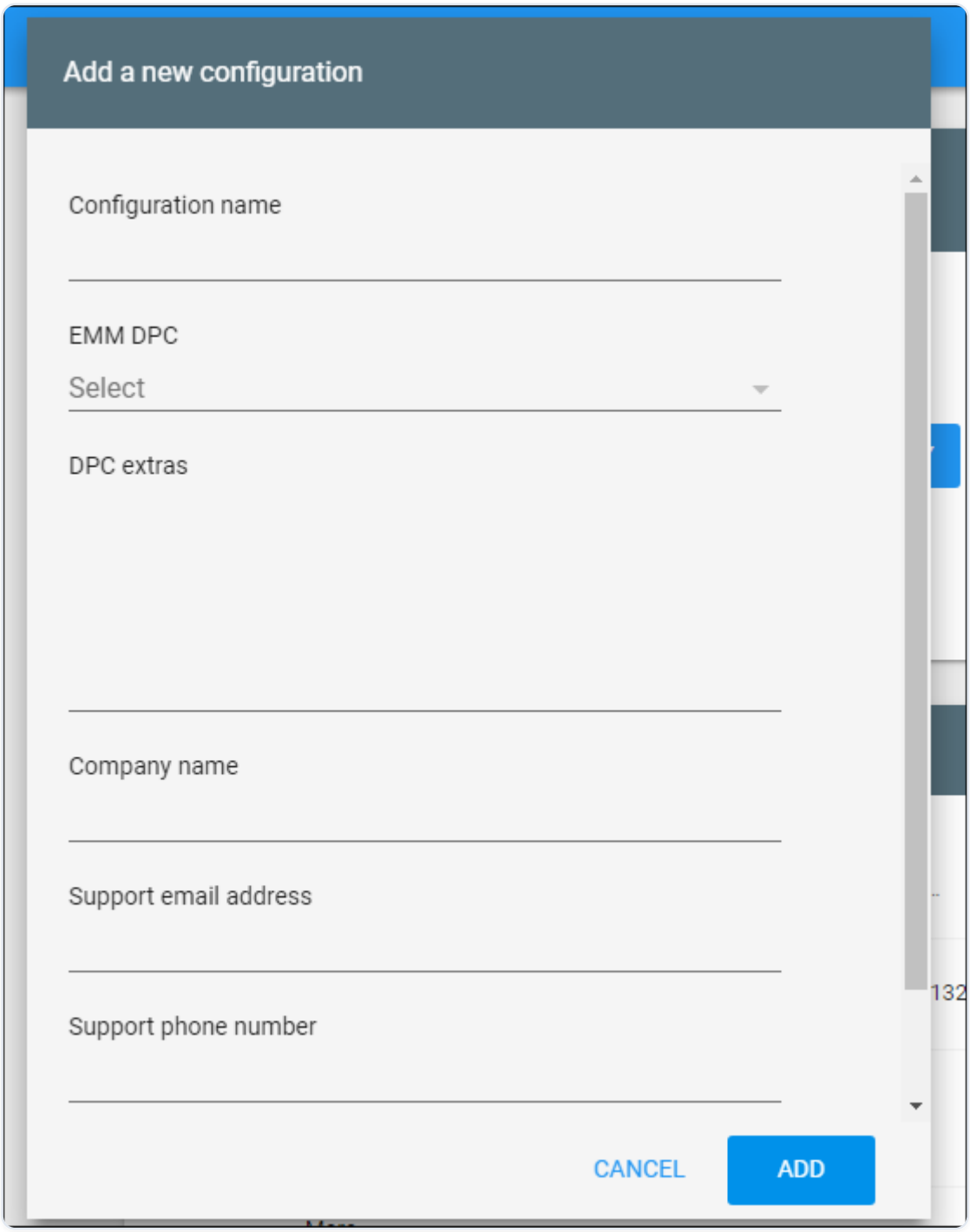
1. Vaya al portal de Android zero-touch en https://partner.android.com/zerotouch. Inicie sesión con la información de la cuenta de su distribuidor de dispositivos zero-touch.
2. Haga clic en **Configuración**.



3. Haga clic en **+** encima de la tabla de configuración.



4. Introduzca la información de su configuración en la ventana de configuración que aparece.



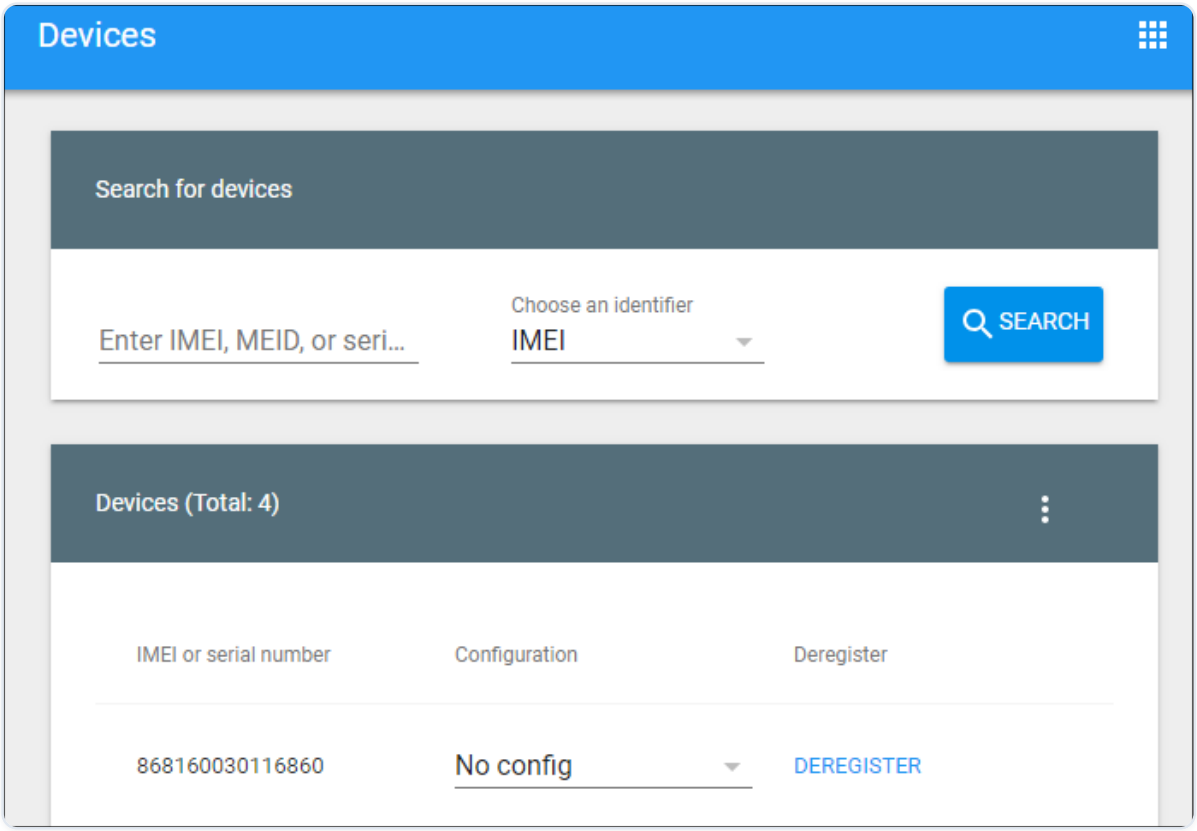
- **Nombre de la configuración:** Escriba el nombre que elija para esta configuración.
- **EMM DPC:** Elija **Citrix Secure Hub**.
- **Extras de DPC:** Pegue su texto JSON personalizado en este campo.
- **Nombre de la empresa:** Escriba el nombre que desea que aparezca en sus dispositivos Android Enterprise zero-touch durante el aprovisionamiento del dispositivo.

- **Dirección de correo electrónico de soporte:** Escriba una dirección de correo electrónico a la que sus usuarios puedan contactar para obtener ayuda. Esta dirección aparece en sus dispositivos Android Enterprise zero-touch antes del aprovisionamiento del dispositivo.
- **Número de teléfono de soporte:** Escriba un número de teléfono al que sus usuarios puedan contactar para obtener ayuda. Este número de teléfono aparece en sus dispositivos Android Enterprise zero-touch antes del aprovisionamiento del dispositivo.
- **Mensaje personalizado:** Opcionalmente, añada una o dos frases para ayudar a sus usuarios a ponerse en contacto con usted o para darles más detalles sobre lo que le está sucediendo a su dispositivo. Este mensaje personalizado aparece en sus dispositivos Android Enterprise zero-touch antes del aprovisionamiento del dispositivo.

5. Haga clic en **Agregar**.
6. Para crear más configuraciones, repita los pasos 2 a 4.
7. Para aplicar una configuración a un dispositivo:

   a. En el portal Android zero-touch, haga clic en **Dispositivos**.

   b. Busque el dispositivo en la lista de dispositivos y elija la configuración que quiere asignarle.



   c. Haga clic en **Actualizar**.

Puede aplicar una configuración a muchos dispositivos mediante un archivo CSV.

Para obtener información sobre cómo aplicar una configuración a muchos dispositivos, consulte Inscripción Zero-touch para administradores de TI. Este tema de Android Enterprise contiene más información sobre cómo administrar configuraciones y aplicarlas a los dispositivos.

Aprovisionamiento de dispositivos Android Enterprise dedicados

Los dispositivos Android Enterprise dedicados son dispositivos totalmente administrados que se dedican a cumplir un único caso de uso. Estos dispositivos se restringen a una aplicación o a un pequeño conjunto de aplicaciones necesarias para realizar las tareas requeridas para este caso de uso. También se impide que los usuarios habiliten otras aplicaciones o realicen otras acciones en el dispositivo.

Inscriba los dispositivos dedicados mediante cualquiera de los métodos de inscripción utilizados para otros dispositivos totalmente administrados, como se describe en Aprovisionamiento de dispositivos Android Enterprise totalmente administrados. El aprovisionamiento de dispositivos dedicados requiere más configuración antes de la inscripción.

Para aprovisionar dispositivos dedicados:

- Agregue un perfil de inscripción para los administradores de Citrix Endpoint Management a los que permita inscribir dispositivos dedicados en su implementación de Citrix Endpoint Management. Consulte Crear perfiles de inscripción.
- Para permitir que un dispositivo dedicado acceda a las aplicaciones, agréguelas a la lista de permitidos.
- Opcionalmente, configure la aplicación permitida para que admita el modo de bloqueo de tareas. Cuando una aplicación está en modo de bloqueo de tareas, la aplicación se fija a la pantalla del dispositivo cuando el usuario la abre. No aparece ningún botón de Inicio y el botón Atrás está inhabilitado. El usuario sale de la aplicación mediante una acción programada en la aplicación, como cerrar sesión.
- Inscriba cada dispositivo en el perfil de inscripción que agregó.

Requisitos del sistema

- La compatibilidad con la inscripción de dispositivos dedicados comienza con Android 6.0.

Permitir aplicaciones y establecer el modo de tarea bloqueada

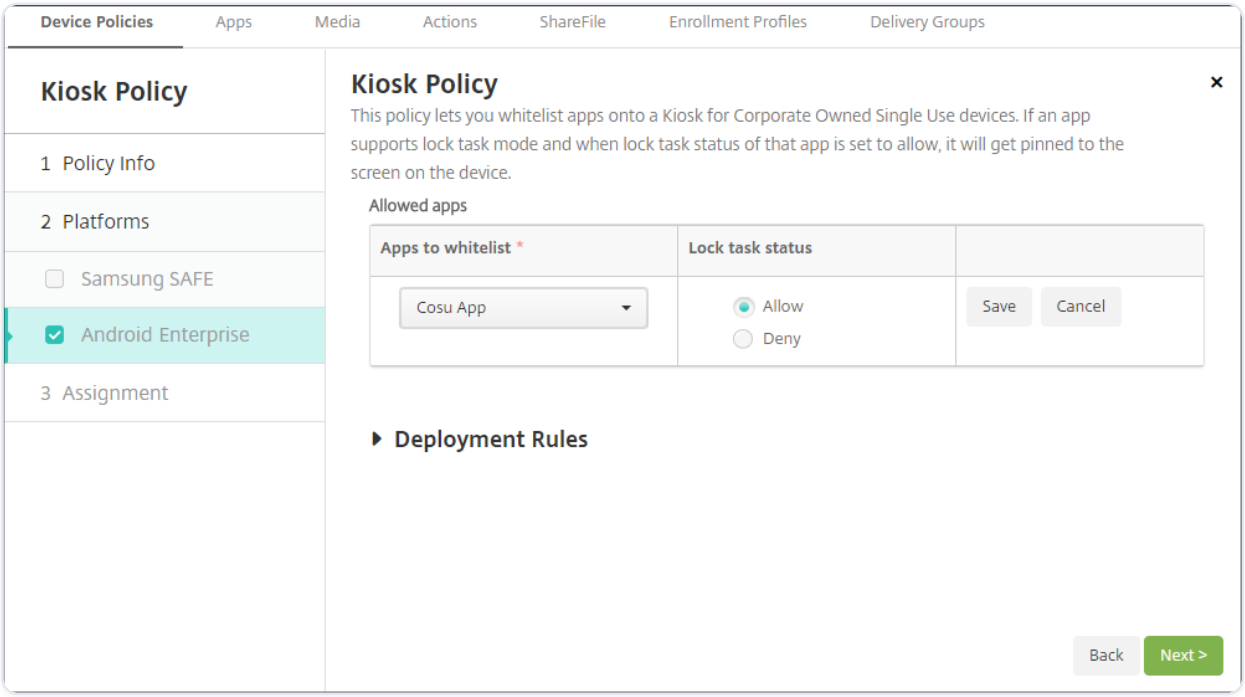
La directiva de dispositivo Quiosco le permite permitir aplicaciones y establecer el modo de tarea bloqueada. De forma predeterminada, Citrix Secure Hub y los servicios de Google Play están en la lista de permitidos.

Para agregar la directiva Quiosco:

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Directivas de dispositivo**. Aparece la página **Directivas de dispositivo**.
2. Haga clic en **Agregar**. Aparece el cuadro de diálogo **Agregar nueva directiva**.
3. Expanda **Más** y, a continuación, en Seguridad, haga clic en **Quiosco**. Aparece la página **Directiva de quiosco**.
4. En Plataformas, seleccione **Android Enterprise**. Desactive las demás plataformas.
5. En el panel Información de la directiva, escriba el **Nombre de la directiva** y una **Descripción** opcional.
6. Haga clic en **Siguiente** y, a continuación, en **Agregar**.
7. Para permitir una aplicación y permitir o denegar el modo de tarea bloqueada para esa aplicación:

   Seleccione la aplicación que quiere permitir de la lista.

   Elija **Permitir** para configurar la aplicación para que se fije en la pantalla del dispositivo cuando el usuario la inicie. Elija **Denegar** para configurar la aplicación para que no se fije. El valor predeterminado es **Permitir**.



8. Haga clic en **Guardar**.
9. Para permitir otra aplicación y permitir o denegar el modo de tarea bloqueada para esa aplicación, haga clic en **Agregar**.
10. Configure las reglas de implementación y elija los grupos de entrega. Para obtener más información, consulte Directivas de dispositivo.

Aprovisionamiento de dispositivos Android Enterprise totalmente administrados con un perfil de trabajo o un perfil de trabajo en dispositivos propiedad de la empresa

Los dispositivos con Android 9.0-10.x se inscriben como «totalmente administrados con un perfil de trabajo». A partir de Android 11 o posterior, los dispositivos se inscriben como «perfil de trabajo en dispositivos propiedad de la empresa». Todos estos dispositivos son propiedad de la empresa y se utilizan tanto para fines laborales como personales. Su organización administra todo el dispositivo. Puede aplicar un conjunto de directivas al dispositivo y un conjunto de directivas diferente al perfil de trabajo.

En la consola de Citrix Endpoint Management, los dispositivos totalmente administrados con un perfil de trabajo aparecen con estos términos:

- La propiedad del dispositivo es «Corporativa».
- El tipo de instalación de Android Enterprise del dispositivo es «Propietario corporativo habilitado personalmente».

Requisitos del sistema

- La compatibilidad con la inscripción de dispositivos totalmente administrados con perfiles de trabajo comienza con Android 9.0.

Para inscribir el dispositivo

Los dispositivos nuevos y restablecidos de fábrica se inscriben como dispositivos totalmente administrados con un perfil de trabajo. Esos dispositivos utilizan cualquiera de los métodos de inscripción utilizados para otros dispositivos totalmente administrados, como se describe en Aprovisionamiento de dispositivos Android Enterprise totalmente administrados. Los dispositivos con Android 11 pueden inscribirse en el modo de perfil de trabajo en dispositivos propiedad de la empresa mediante el código QR o los métodos de inscripción sin contacto descritos en esa sección.

> **Importante:**

> Al inscribir dispositivos en el modo de perfil de trabajo en dispositivos propiedad de la empresa mediante el método de código QR, agregue lo siguiente a la salida JSON, encima del campo `serverURL`: `"desiredProvisioningMode": "managedProfile",`

JSON output

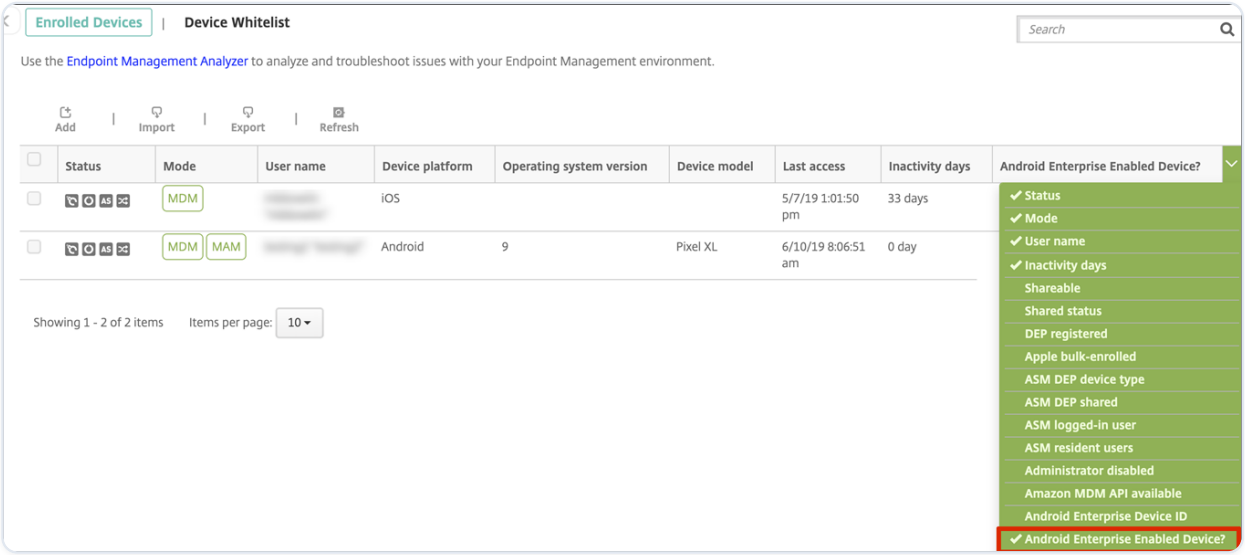

```
{
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
    "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?identifier=xenmobile",
    "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
    "android.app.extra.PROVISIONING_LEAVE_ALL_SYSTEM_APPS_ENABLED": false,
    "android.app.extra.PROVISIONING_SKIP_USER_CONSENT": true,
    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
        "desiredProvisioningMode": "managedProfile",
        "serverURL": "https://testServer.xmqa.cloud.com",
        "username": "username",
        "password": "password"
    }
```


Los dispositivos que no son nuevos o no se han restablecido de fábrica se inscriben como dispositivos con perfil de trabajo, tal como se describe en Aprovisionamiento de dispositivos Android Enterprise con perfil de trabajo.

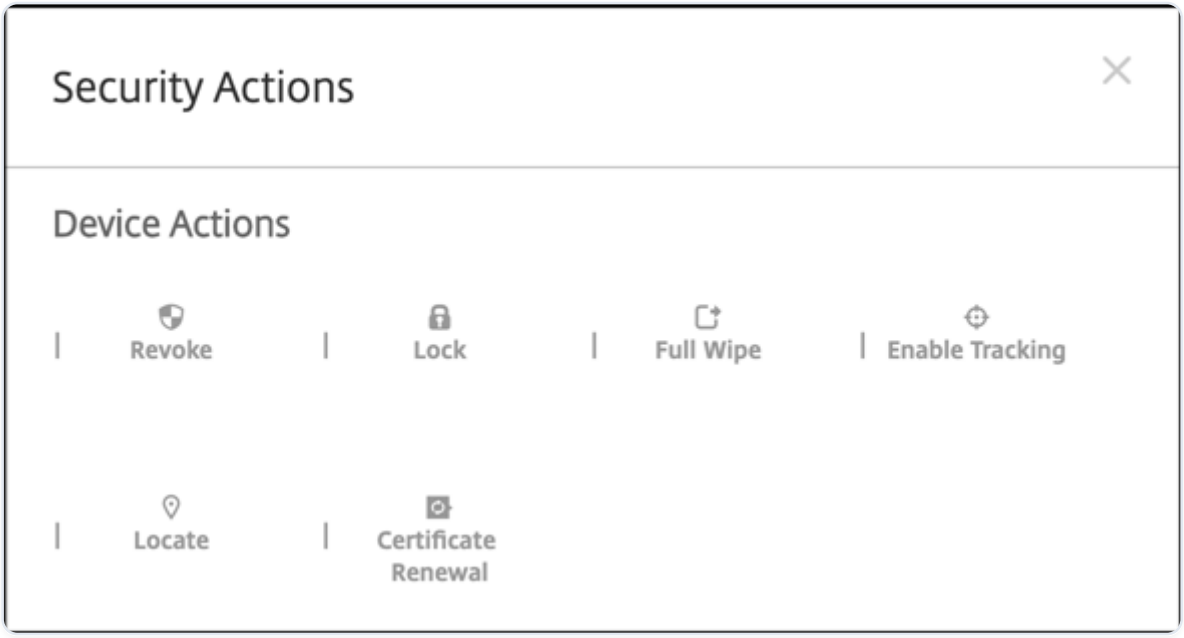
Visualización de dispositivos Android Enterprise en la consola de Citrix Endpoint Management

Para ver dispositivos Android Enterprise totalmente administrados, dispositivos dedicados y dispositivos totalmente administrados con un perfil de trabajo:

1. En la consola de Citrix Endpoint Management, vaya a **Administrar > Dispositivos**.
2. Agregue la columna **¿Dispositivo Android Enterprise habilitado?** haciendo clic en el menú del borde derecho de la tabla.



3. Para ver las acciones de seguridad disponibles, seleccione un dispositivo totalmente administrado y haga clic en **Proteger**. Cuando el dispositivo está totalmente administrado, la acción **Borrado completo** está disponible, pero **Borrado selectivo** no lo está. Esa diferencia se debe a que el dispositivo solo permite aplicaciones de la tienda Google Play administrada. No hay una opción para que el usuario instale aplicaciones de la tienda pública. Su organización administra todo el contenido del dispositivo.



Configurar directivas de dispositivos y aplicaciones de Android Enterprise

Para obtener una descripción general de las directivas controladas tanto a nivel de dispositivo como de aplicación, consulte Directivas de dispositivo y directivas MDX compatibles con Android Enterprise.

Qué saber sobre las directivas:

- **Restricciones de dispositivo:** Decenas de restricciones de dispositivo le permiten controlar funciones como:
  - Uso de la cámara del dispositivo
  - Uso de copiar y pegar entre perfiles de trabajo y personales
- **VPN por aplicación:** Utilice la directiva de dispositivo de configuraciones administradas para configurar perfiles VPN para Android Enterprise.
- **Directiva de correo electrónico:** Recomendamos utilizar la directiva de dispositivo de configuraciones administradas para configurar aplicaciones.

Directivas de dispositivo

Esta tabla enumera todas las directivas de dispositivo disponibles para los dispositivos Android Enterprise.

Importante:

Para los dispositivos que se inscriben en Android Enterprise y usan aplicaciones MDX: Puede controlar algunas configuraciones a través de MDX y Android Enterprise. Use la configuración de política menos restrictiva para MDX y controle la política a través de Android Enterprise.

Permisos de aplicaciones	Inventario de aplicaciones	Desinstalación de aplicaciones
Actualizar automáticamente las aplicaciones administradas	Programación de conexiones	Credenciales
XML personalizado	Opciones de Citrix Endpoint Management	Archivos
Administración de bloqueo de pantalla	Kiosco	Configuración del iniciador
Ubicación	Configuraciones administradas	Red
Actualización del SO	Código de acceso	Restricciones

Directivas de dispositivo para dispositivos totalmente administrados con perfil de trabajo (dispositivos COPE)

Para los dispositivos totalmente administrados con perfiles de trabajo, puede usar algunas directivas de dispositivo para aplicar configuraciones separadas a todo el dispositivo y al perfil de trabajo. Puede usar otras directivas de dispositivo para aplicar configuraciones solo a todo el dispositivo o solo al perfil de trabajo de los dispositivos totalmente administrados con perfiles de trabajo. Para los dispositivos inscritos en el modo de perfil de trabajo en dispositivos corporativos, las directivas se aplican solo al perfil de trabajo y no a todo el dispositivo.

DIRECTIVA	SE APLICA A
Permisos de aplicación	Perfil de trabajo
Inventario de aplicaciones	Perfil de trabajo
Desinstalación de aplicaciones	Perfil de trabajo
Actualizar automáticamente las aplicaciones administradas	Perfil de trabajo
Programación de conexiones	Perfil de trabajo
Credenciales	Perfil de trabajo
XML personalizado	N/D
Opciones de Citrix Endpoint Management	Perfil de trabajo
Archivos	Perfil de trabajo
Administración de bloqueo de pantalla	Dispositivo y perfil de trabajo
Kiosco	N/D
Configuración del iniciador	Dispositivo y perfil de trabajo
Ubicación	Dispositivo (solo modo de ubicación)
Configuraciones administradas	Perfil de trabajo
Red	Dispositivo
Actualización del SO	N/D
Código de acceso	Dispositivo y perfil de trabajo
Restricciones	Dispositivo y perfil de trabajo (cree directivas separadas para el dispositivo y el perfil de trabajo)
VPN	N/A

Consulte también Políticas de dispositivo y políticas MDX admitidas para Android Enterprise y Información general del SDK de MAM.

Acciones de seguridad

Android Enterprise admite las siguientes acciones de seguridad. Para obtener una descripción de cada acción de seguridad, consulte Acciones de seguridad.

ACCIÓN DE SEGURIDAD	PERFIL DE TRABAJO	TOTALMENTE ADMINISTRADO
Renovación de certificado	Sí	Sí
Borrado completo	Sí (después de un borrado selectivo)	Sí
Localizar	Sí	Sí
Bloquear	Sí	Sí
Bloquear y restablecer contraseña	No	Sí
Notificar (Sonar)	Sí	Sí
Revocar	Sí	Sí
Borrado selectivo	Sí	Sí

Notas sobre las acciones de seguridad

- La acción de seguridad de localización falla a menos que la directiva de dispositivo de Ubicación establezca el modo de ubicación del dispositivo en **Alta precisión** o **Ahorro de batería**. Consulte Directiva de dispositivo de Ubicación.
- En dispositivos con perfil de trabajo que ejecutan versiones de Android anteriores a Android 9.0:
  - La acción de bloquear y restablecer contraseña no es compatible.
- En dispositivos con perfil de trabajo con Android 9.0 o posterior:
  - El código de acceso enviado bloquea el perfil de trabajo. El dispositivo en sí no se bloquea.
  - Si no se establece ningún código de acceso en el perfil de trabajo:

    - Si no se envía ningún código de acceso, o el código de acceso enviado no cumple los requisitos: El dispositivo se bloquea.
  - Si se establece un código de acceso en el perfil de trabajo:
    - Si no se envía ningún código de acceso, o el código de acceso enviado no cumple los requisitos: El perfil de trabajo se bloquea, pero el dispositivo en sí no se bloquea.

Anular la inscripción de una empresa de Android Enterprise

Si ya no desea utilizar su empresa de Android Enterprise, puede anular la inscripción de la empresa.

> **Advertencia:**
>
> Después de anular la inscripción de una empresa, las aplicaciones de Android Enterprise en los dispositivos ya inscritos a través de ella vuelven a sus estados predeterminados. Google ya no administra los dispositivos. Si se inscribe en una nueva empresa de Android Enterprise, debe aprobar las aplicaciones para la nueva organización desde Google Play administrado. A continuación, puede actualizar las aplicaciones desde la consola de Citrix Endpoint Management.

> Una vez que se anula la inscripción de la empresa de Android Enterprise:

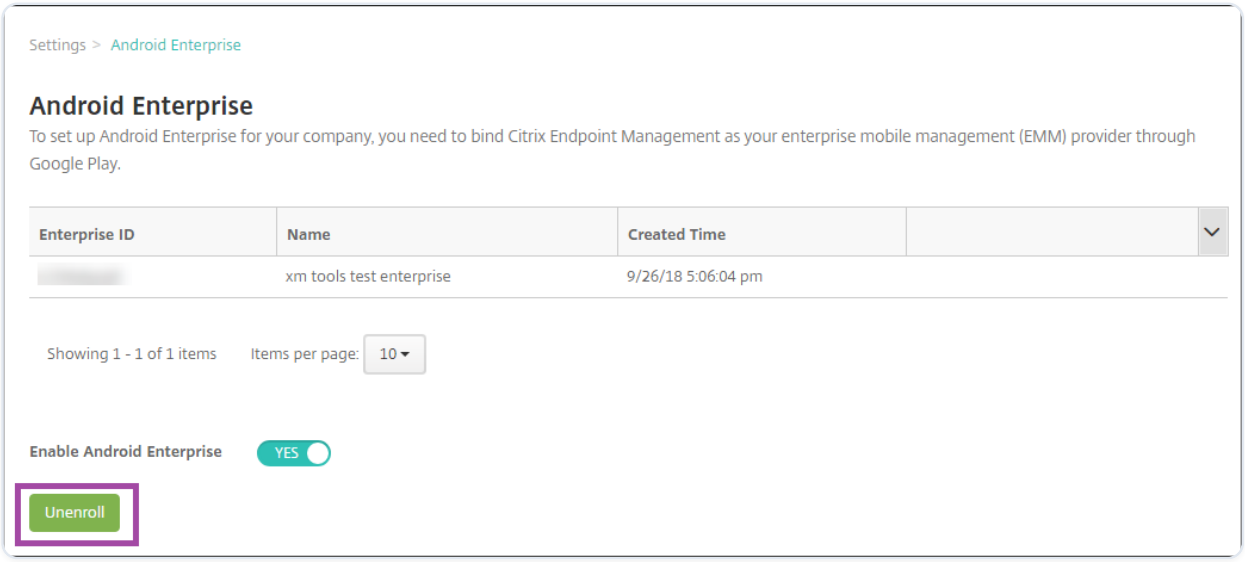
- Los dispositivos y usuarios inscritos a través de la empresa tienen las aplicaciones de Android Enterprise restablecidas a su estado predeterminado. Las directivas de configuraciones administradas aplicadas anteriormente ya no afectan a las operaciones.
- Citrix Endpoint Management administra los dispositivos inscritos a través de la empresa. Desde la perspectiva de Google, esos dispositivos no están administrados. No puede añadir nuevas aplicaciones de Android Enterprise. No puede aplicar directivas de configuraciones administradas. Puede aplicar otras directivas, como Programación, Contraseña y Restricciones, a estos dispositivos.
- Si intenta inscribir dispositivos en Android Enterprise, se inscriben como dispositivos Android, no como dispositivos Android Enterprise.

Anule la inscripción de una empresa de Android Enterprise mediante la consola del servidor de Citrix Endpoint Management y las herramientas de Citrix Endpoint Management.

Al realizar esta tarea, Citrix Endpoint Management abre una ventana emergente de Herramientas. Antes de empezar, asegúrese de que su explorador tenga permiso para abrir ventanas emergentes. Algunos exploradores, como Google Chrome, requieren que desactive el bloqueo de elementos emergentes y añada la dirección del sitio de Citrix Endpoint Management a la lista de elementos emergentes permitidos.

Para anular la inscripción de una empresa de Android Enterprise:

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje de la esquina superior derecha. Aparece la página Configuración.
2. En la página Configuración, haga clic en **Android Enterprise**.
3. Haga clic en **Anular inscripción**.



Distribuir aplicaciones de Android Enterprise

Citrix Endpoint Management administra las aplicaciones implementadas en los dispositivos. Puede organizar e implementar los siguientes tipos de aplicaciones de Android Enterprise.

- **Aplicaciones de tiendas de aplicaciones administradas:** Estas aplicaciones incluyen aplicaciones gratuitas disponibles en Google Play Store administrado. Por ejemplo, GoToMeeting.
- **MDX:** Aplicaciones preparadas con el SDK de MAM o empaquetadas con el MDX Toolkit. Estas aplicaciones incluyen directivas MDX. Puede obtener aplicaciones MDX de fuentes internas y tiendas públicas. Implemente las aplicaciones de productividad móvil de Citrix como aplicaciones MDX.

- **Empresa:** Aplicaciones privadas que desarrolla u obtiene de otra fuente. Proporciona estas aplicaciones a sus usuarios a través de Google Play Store administrado. Google Play Store administrado es la tienda de aplicaciones empresariales de Google.
- **Aplicaciones privadas habilitadas para MDX:** Aplicaciones empresariales preparadas con el SDK de MAM o empaquetadas con el MDX Toolkit.

Puede agregar aplicaciones empresariales y aplicaciones privadas habilitadas para MDX de dos maneras diferentes.

- Agregue las aplicaciones a la consola de Citrix Endpoint Management como aplicaciones empresariales, como se describe en las secciones Aplicaciones empresariales y Aplicaciones privadas habilitadas para MDX de este artículo.
- Publique las aplicaciones directamente en Google Play Store administrado con su cuenta de desarrollador de Google. Luego, agregue las aplicaciones a la consola de Citrix Endpoint Management como aplicaciones de tiendas de aplicaciones administradas. Consulte Aplicaciones de tiendas de aplicaciones administradas.

Si publica aplicaciones con su cuenta de desarrollador de Google y luego cambia a usar la consola de Citrix Endpoint Management, la propiedad de las aplicaciones difiere. En este caso, debe administrar sus aplicaciones en ambas ubicaciones. Citrix recomienda agregar sus aplicaciones utilizando un método u otro.

Si necesita eliminar aplicaciones autoadministradas de Google Play Store administrado, abra un ticket con Google. Los desarrolladores pueden deshabilitar, pero no eliminar, aplicaciones de Google Play Store administrado.

Las siguientes secciones proporcionan información más detallada sobre la configuración de aplicaciones de Android Enterprise. Para obtener información sobre la distribución de aplicaciones, consulte Agregar aplicaciones. Ese artículo incluye:

- Los flujos de trabajo generales para agregar aplicaciones web y SaaS o enlaces web
- El flujo de trabajo de aplicaciones requerido para aplicaciones empresariales y de tiendas públicas
- Cómo entregar aplicaciones empresariales desde la Red de entrega de contenido (CDN) de Citrix para aplicaciones empresariales

Aplicaciones de la tienda de aplicaciones administradas

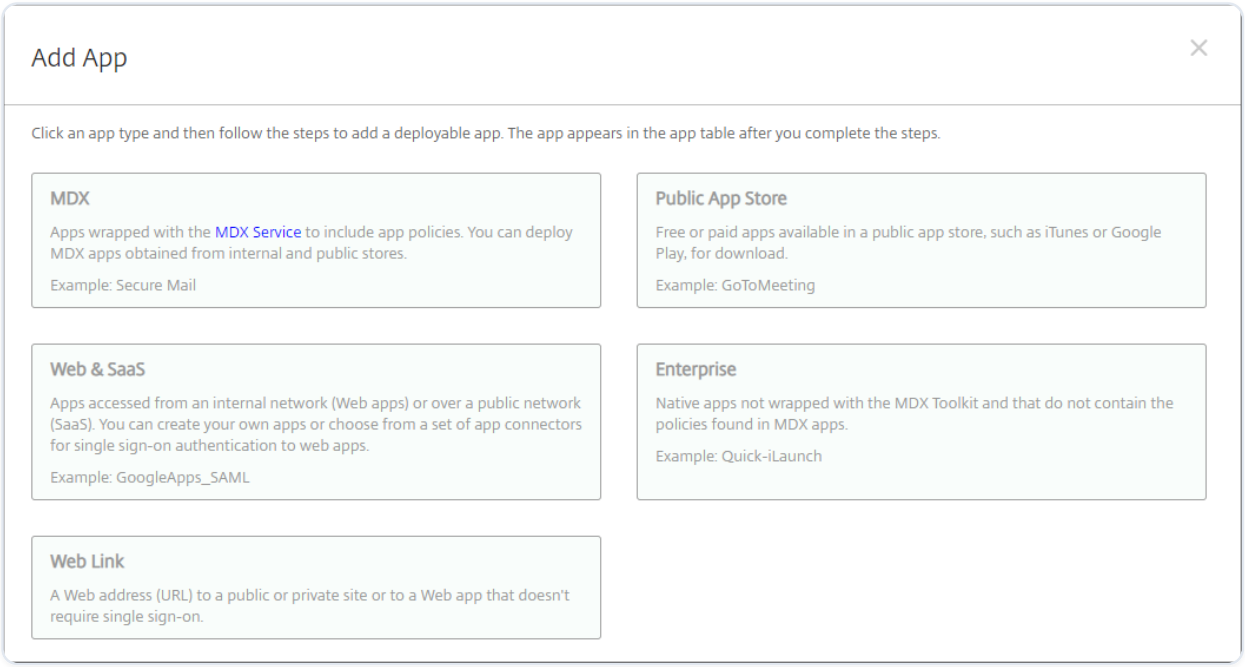
Puede agregar aplicaciones gratuitas disponibles en Google Play Store administrado a Citrix Endpoint Management.

Nota:

Para que todas las aplicaciones de Google Play Store sean accesibles desde Google Play administrado, utilice la propiedad de servidor **Acceder a todas las aplicaciones en Google Play Store administrado**. Consulte Propiedades del servidor. Establecer esta propiedad en **true** permite a todos los usuarios de Android Enterprise acceder a las aplicaciones públicas de Google Play Store. A continuación, puede utilizar la directiva de dispositivo Restricciones para controlar el acceso a estas aplicaciones.

Paso 1: Agregar y configurar aplicaciones

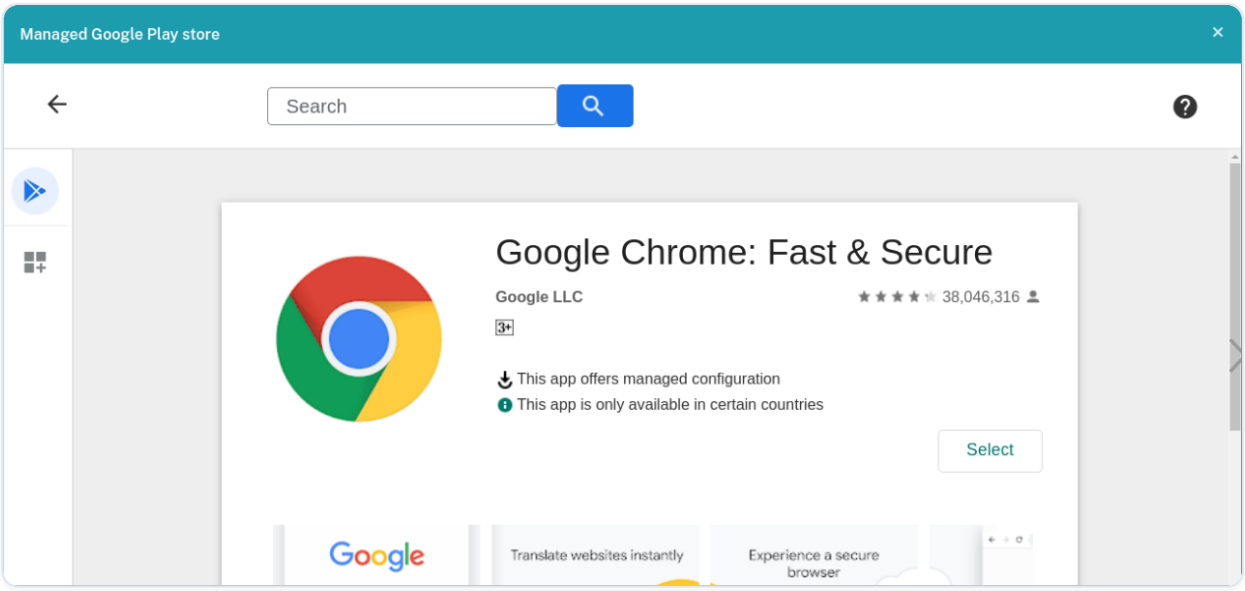
1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar**.
2. Haga clic en **Tienda de aplicaciones pública**.



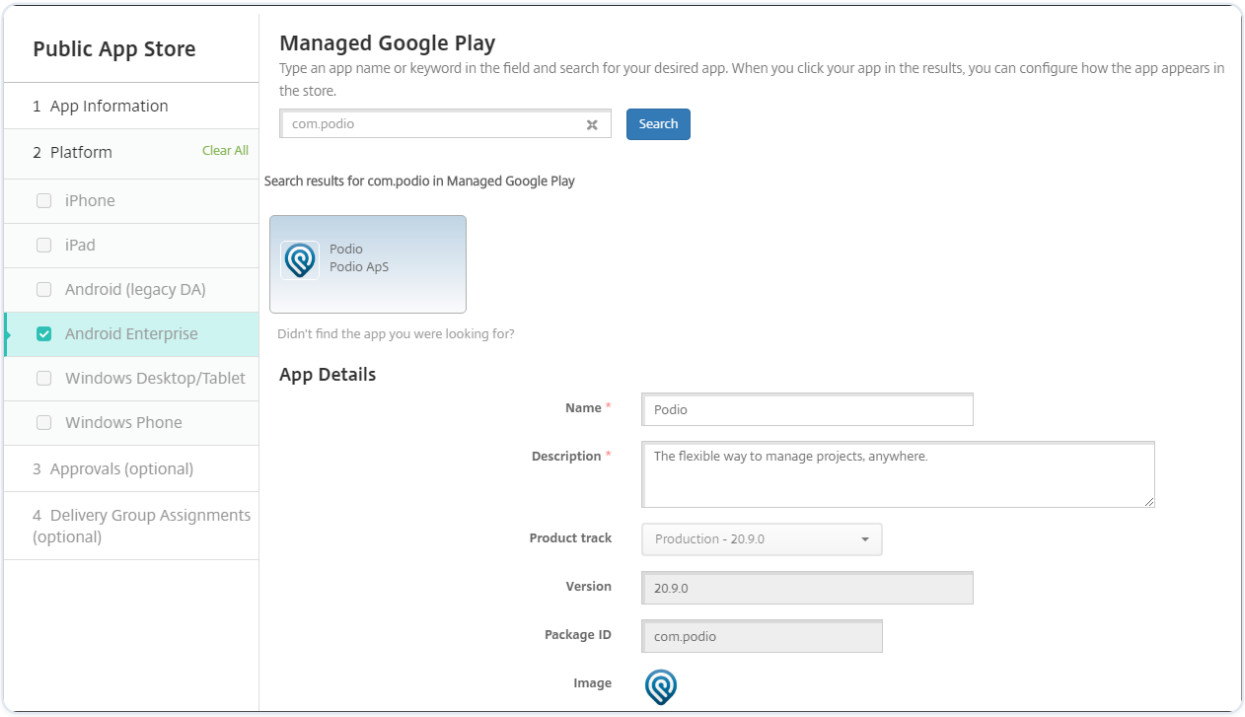
3. En el panel **Información de la aplicación**, escriba la siguiente información:
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. El nombre aparece en **Nombre de la aplicación** en la tabla **Aplicaciones**.
   - **Descripción:** Escriba una descripción opcional de la aplicación.
4. Seleccione **Android Enterprise** como plataforma.
5. Escriba el nombre de la aplicación o el ID del paquete en el cuadro de búsqueda y haga clic en **Buscar**. Puede localizar el ID del paquete en Google Play Store. El ID se encuentra en la URL

de la aplicación. Por ejemplo, `com.Slack` es el ID del paquete en `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`.

6. Aparecen las aplicaciones que coinciden con los criterios de búsqueda. Haga clic en la aplicación deseada y, a continuación, haga clic en **Seleccionar**.



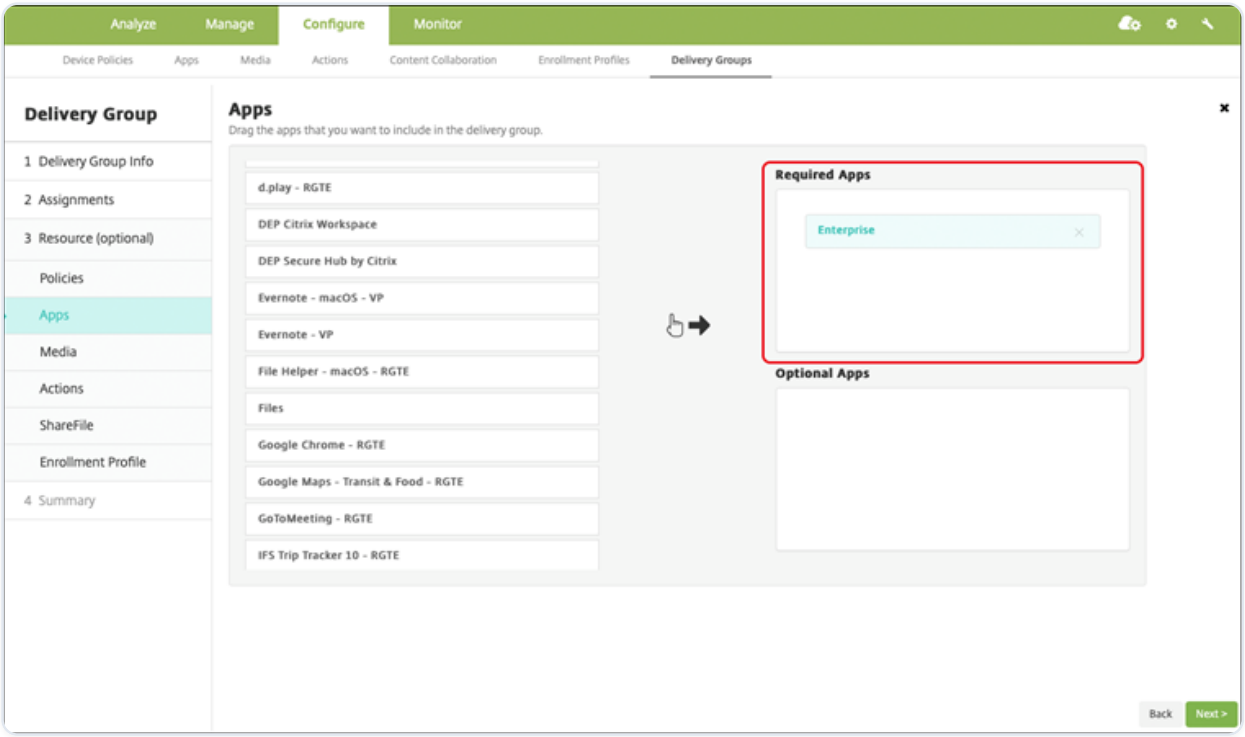
7. Haga clic en **Seleccionar** de nuevo.
8. Haga clic en el icono de la aplicación y configure el **Nombre** y la **Descripción** de la aplicación.



9. Asigne los grupos de entrega a la aplicación y haga clic en **Guardar**. Para obtener más información, consulte Implementar recursos.

Paso 2: Configurar la implementación de aplicaciones

1. Vaya a **Configurar > Grupos de entrega** y seleccione el grupo de entrega que configuró. Haga clic en **Modificar**.
2. En la sección **Aplicaciones**, arrastre las aplicaciones deseadas al cuadro **Aplicaciones obligatorias**.



3. En la página **Resumen**, haga clic en **Guardar**.
4. En la página **Grupos de entrega**, seleccione el grupo de entrega y haga clic en **Implementar**.

Aplicaciones MDX

Agregue archivos MDX a Citrix Endpoint Management y configure los detalles de la aplicación y la configuración de directivas. Para configurar las aplicaciones de productividad móvil de Citrix para Android Enterprise, agréguelas como aplicaciones MDX. Para obtener información sobre las directivas de aplicación disponibles para cada tipo de plataforma de dispositivo, consulte:

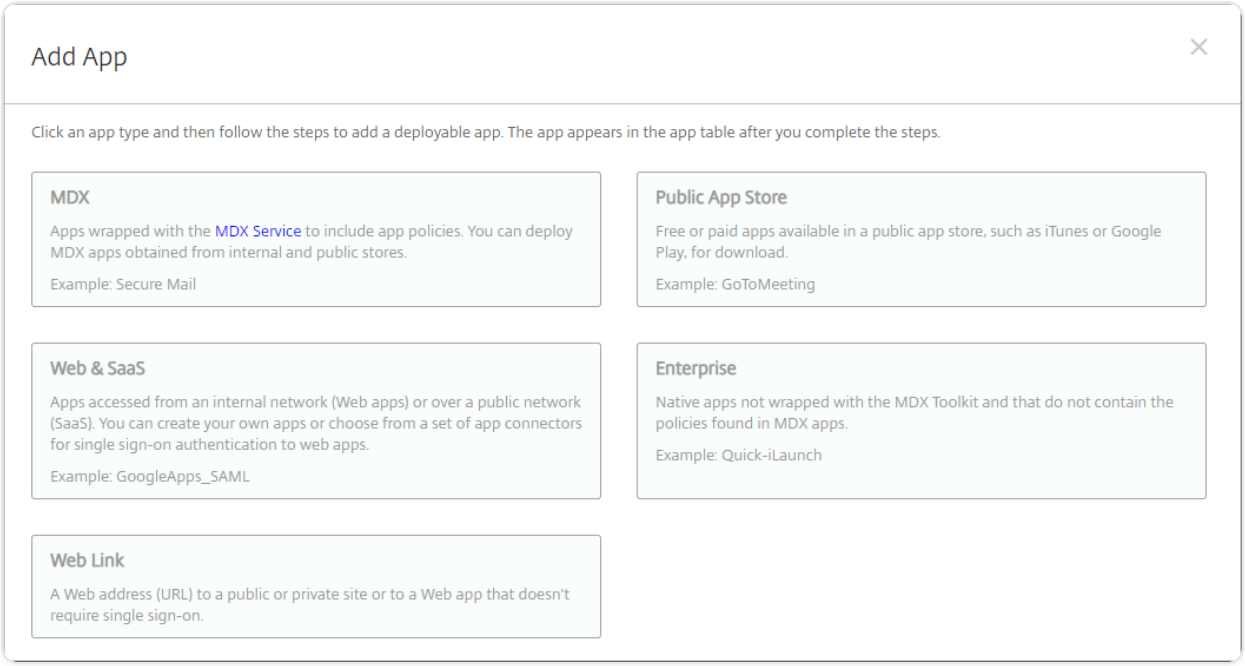
- Información general sobre el SDK de MAM
- Directivas MDX de un vistazo

Paso 1: Agregar y configurar aplicaciones

1. Para las aplicaciones de productividad móvil de Citrix, descargue los archivos MDX de la tienda pública: Vaya a `<https://www.citrix.com/downloads>`. Vaya a **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.

   Para otros tipos de aplicaciones MDX, obtenga el archivo MDX.

2. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones**. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.

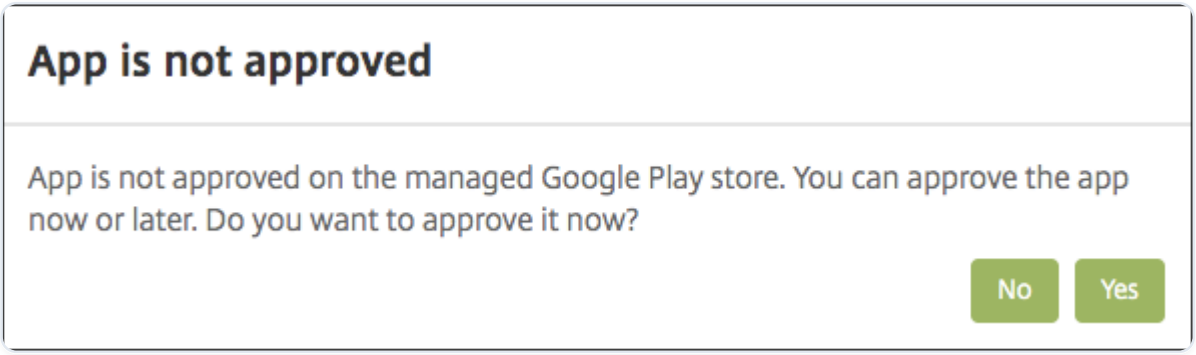


3. Haga clic en **MDX**. Aparecerá la página **Información de la aplicación MDX**. En el panel **Información de la aplicación**, escriba la siguiente información:

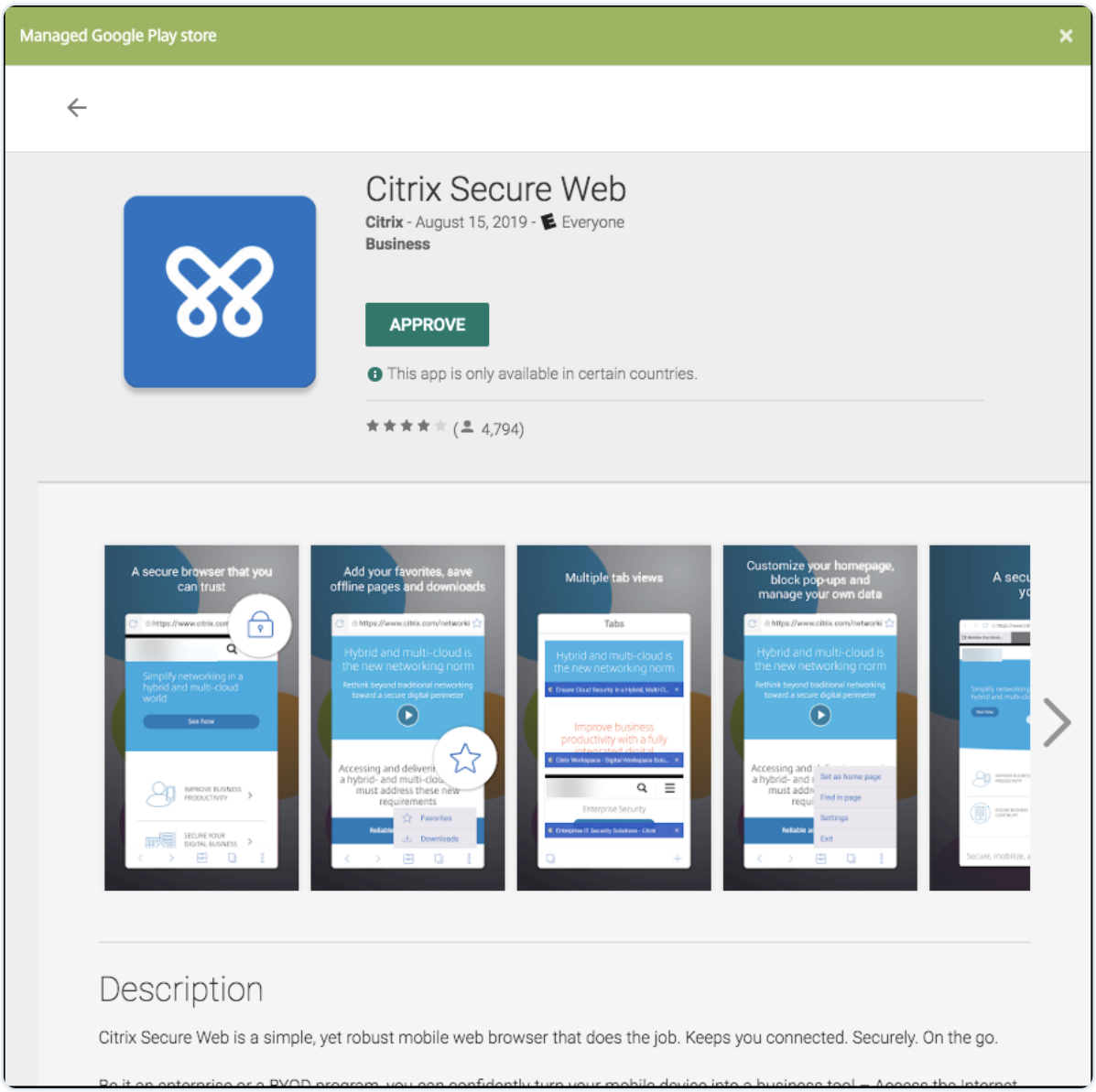
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. El nombre aparece en **Nombre de la aplicación** en la tabla **Aplicaciones**.
   - **Descripción:** Escriba una descripción opcional de la aplicación.

4. Seleccione **Android Enterprise** como plataforma.
5. Haga clic en **Cargar** y vaya al archivo MDX. Android Enterprise solo admite aplicaciones preparadas con el SDK de MAM o MDX Toolkit.

   - La interfaz de usuario le notifica si la aplicación adjunta requiere aprobación de Google Play Store administrado. Para aprobar la aplicación sin salir de la consola de Citrix Endpoint Management, haga clic en **Sí**.



Una vez que se abra Google Play Store administrado, siga las instrucciones para aprobar y guardar la aplicación.



Cuando agregue la aplicación correctamente, aparecerá la página **Detalles de la aplicación**.

6. Configure estos ajustes:

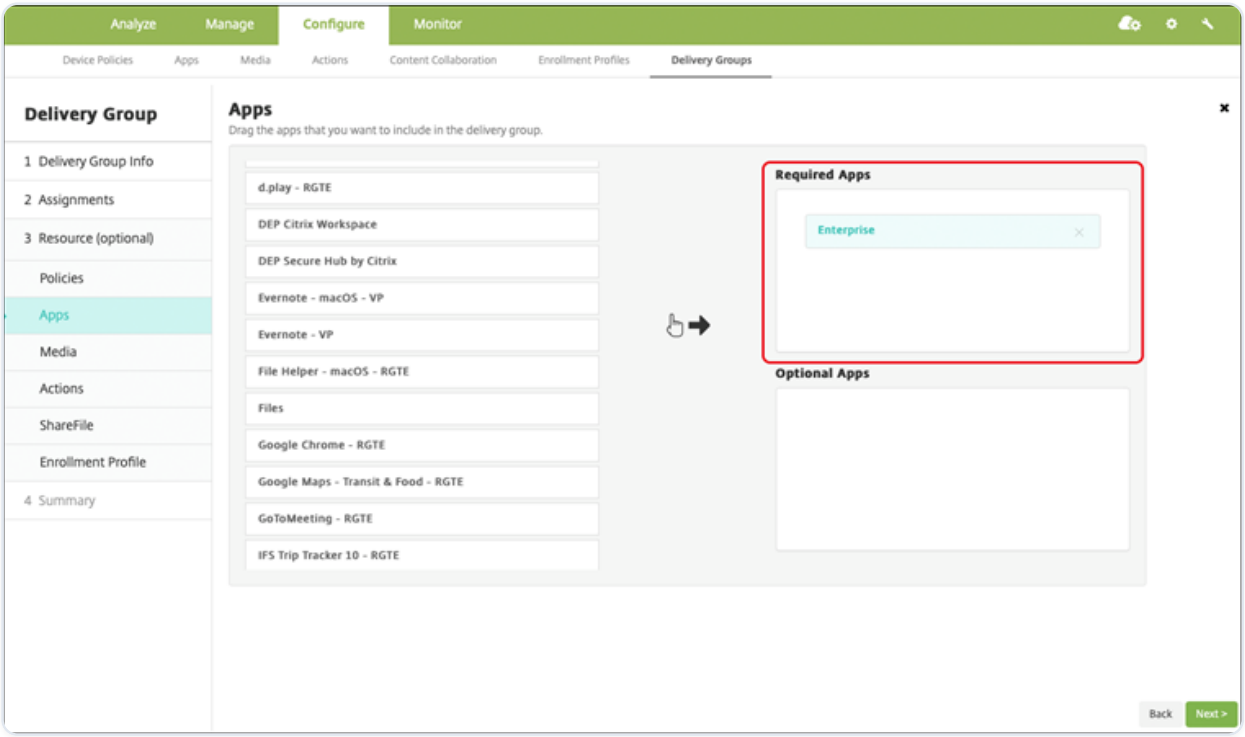
- **Nombre de archivo:** Escriba el nombre de archivo asociado a la aplicación.
- **Descripción de la aplicación:** Escriba una descripción para la aplicación.
- **Versión de la aplicación:** Opcionalmente, escriba el número de versión de la aplicación.
- **ID del paquete:** Escriba el ID del paquete de la aplicación obtenido de Google Play Store administrado.
- **Versión mínima del SO:** Opcionalmente, escriba la versión más antigua del sistema operativo que el dispositivo puede ejecutar para usar la aplicación.

- **Versión máxima del SO:** Opcionalmente, escriba la versión más reciente del sistema operativo que el dispositivo debe ejecutar para usar la aplicación.
- **Dispositivos excluidos:** Opcionalmente, escriba el fabricante o los modelos de dispositivos que no pueden ejecutar la aplicación.

7. Configure las **directivas MDX**. Las directivas MDX varían según la plataforma e incluyen opciones para áreas de directivas, como la autenticación, la seguridad del dispositivo y las restricciones de aplicaciones. En la consola, cada una de las directivas tiene una información sobre herramientas que la describe. Para obtener información sobre las directivas de aplicaciones disponibles para cada tipo de plataforma de dispositivo, consulte:
   - Información general sobre el SDK de MAM
   - Directivas MDX de un vistazo
8. Configure las reglas de implementación y la configuración de la tienda.
9. Asigne los grupos de entrega a la aplicación y haga clic en **Guardar**. Para obtener más información, consulte Implementar recursos.

Paso 2: Configurar la implementación de la aplicación

1. Vaya a **Configurar > Grupos de entrega** y seleccione el grupo de entrega que configuró. Haga clic en **Modificar**.
2. En la sección **Aplicaciones**, arrastre las aplicaciones deseadas al cuadro **Aplicaciones requeridas**.



3. En la página **Resumen**, haga clic en **Guardar**.
4. En la página **Grupos de entrega**, seleccione el grupo de entrega y haga clic en **Implementar**.

Aplicaciones empresariales

Las aplicaciones empresariales representan aplicaciones privadas que no están preparadas con el SDK de MAM o el kit de herramientas MDX. Usted mismo desarrolla estas aplicaciones o las obtiene directamente de otras fuentes. Para agregar una aplicación empresarial, necesita el archivo APK asociado a la aplicación. Asegúrese de seguir las Prácticas recomendadas para aplicaciones privadas de Google.

Vea este vídeo para obtener más información:

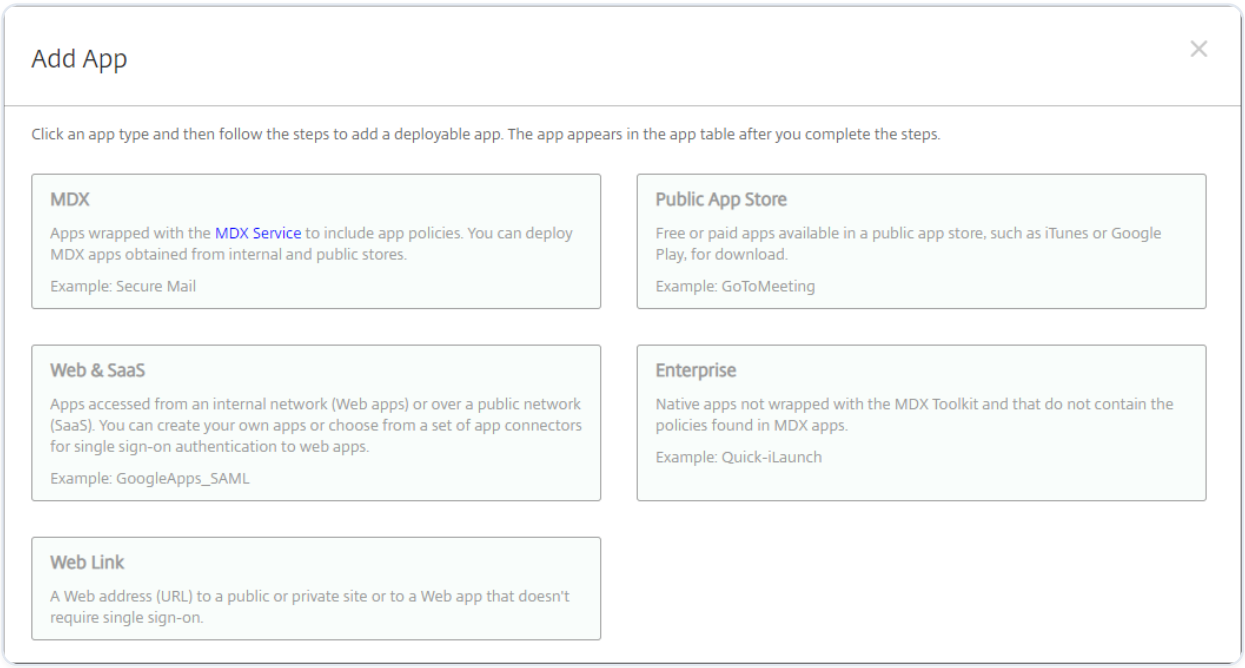


Paso 1: Agregar y configurar aplicaciones

Agregue la aplicación de una de estas dos maneras:

- Publique la aplicación directamente en Google Play Store administrado y agréguela a la consola de Citrix Endpoint Management como una aplicación de tienda de Google Play administrada. Siga la documentación de Google sobre cómo Publicar aplicaciones privadas y, a continuación, siga los pasos de la sección Aplicaciones de tienda de aplicaciones administradas.
- Agregue la aplicación a la consola de Citrix Endpoint Management como una aplicación empresarial. Siga estos pasos:

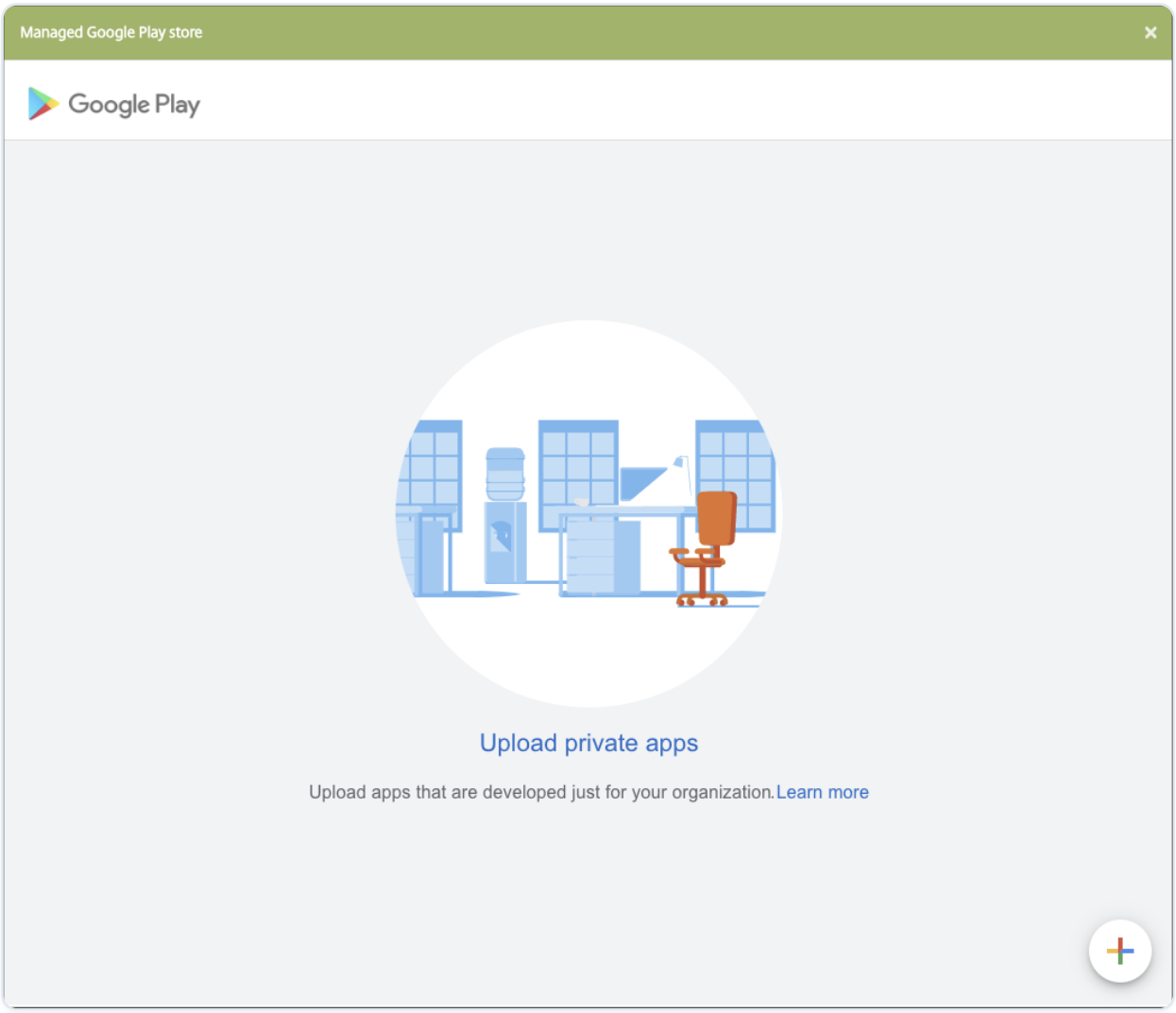
1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones**. Haga clic en **Agregar**. Aparece el cuadro de diálogo **Agregar aplicación**.



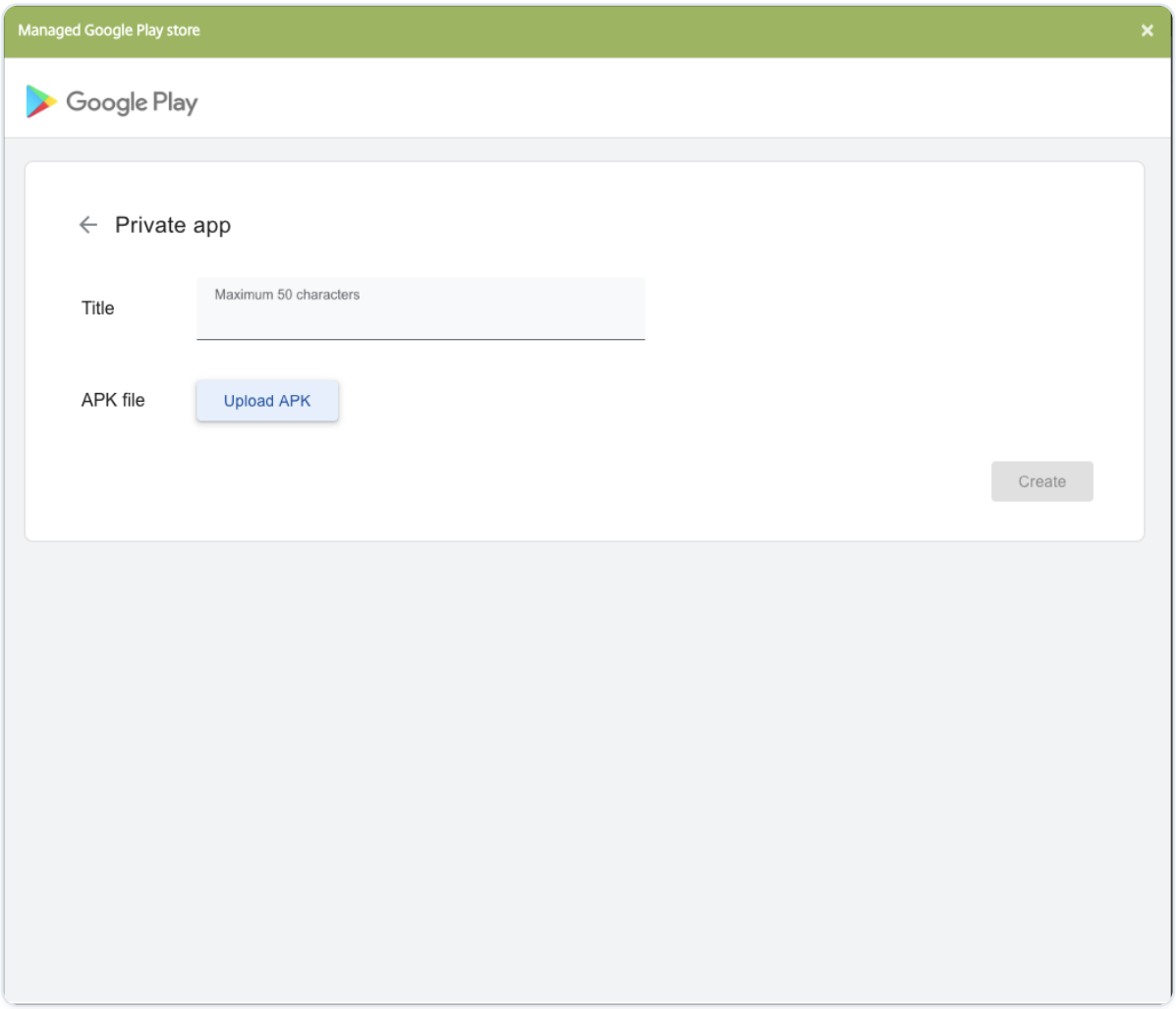
2. Haga clic en **Empresarial**. En el panel **Información de la aplicación**, escriba la siguiente información:

   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre aparece en la tabla Aplicaciones, en Nombre de la aplicación.
   - **Descripción:** Escriba una descripción opcional de la aplicación.

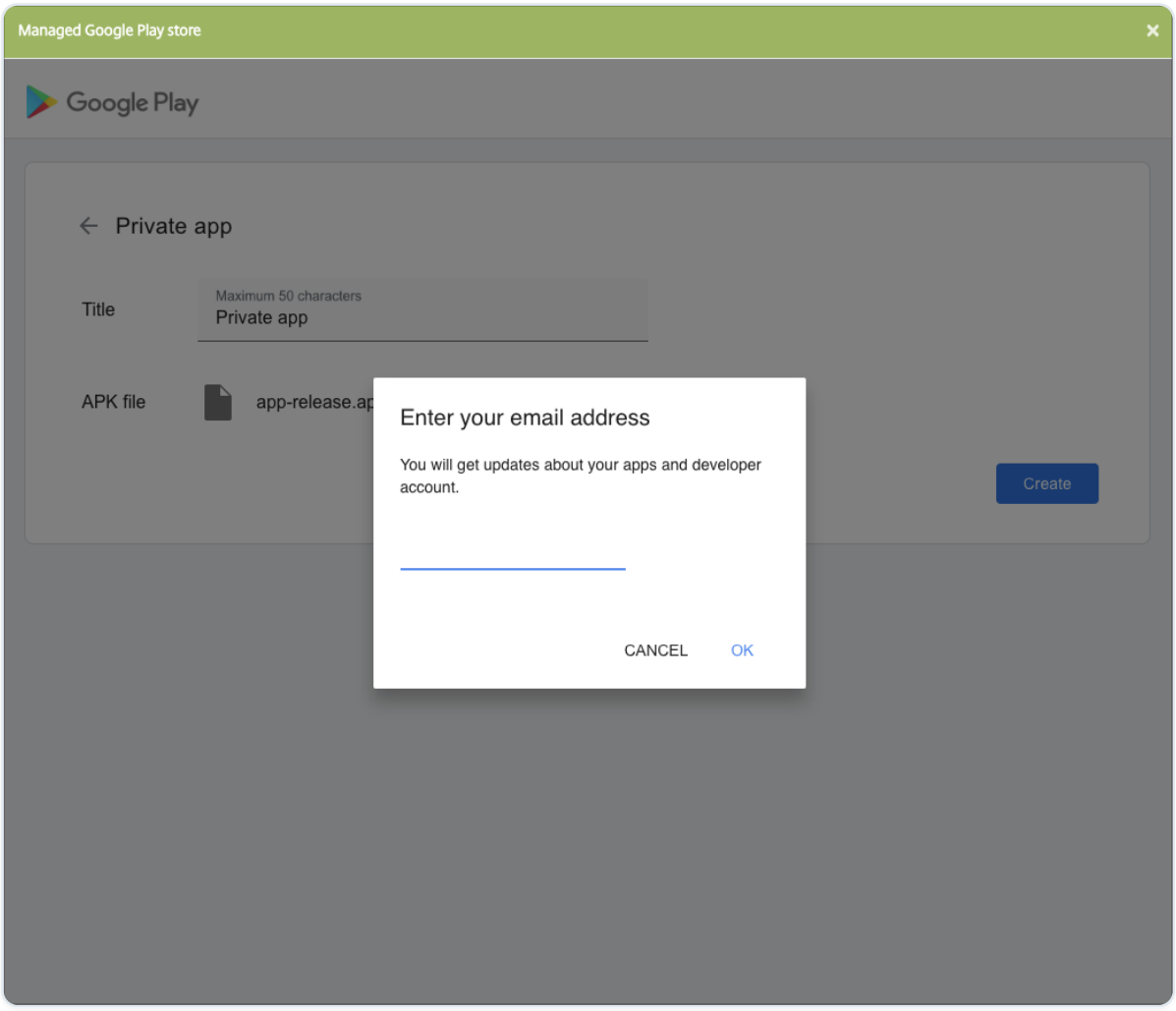
3. Seleccione **Android Enterprise** como plataforma.
4. El botón **Cargar** abre Google Play Store administrado. No es necesario registrarse para obtener una cuenta de desarrollador para publicar una aplicación privada. Haga clic en el icono **Más** en la esquina inferior derecha para continuar.



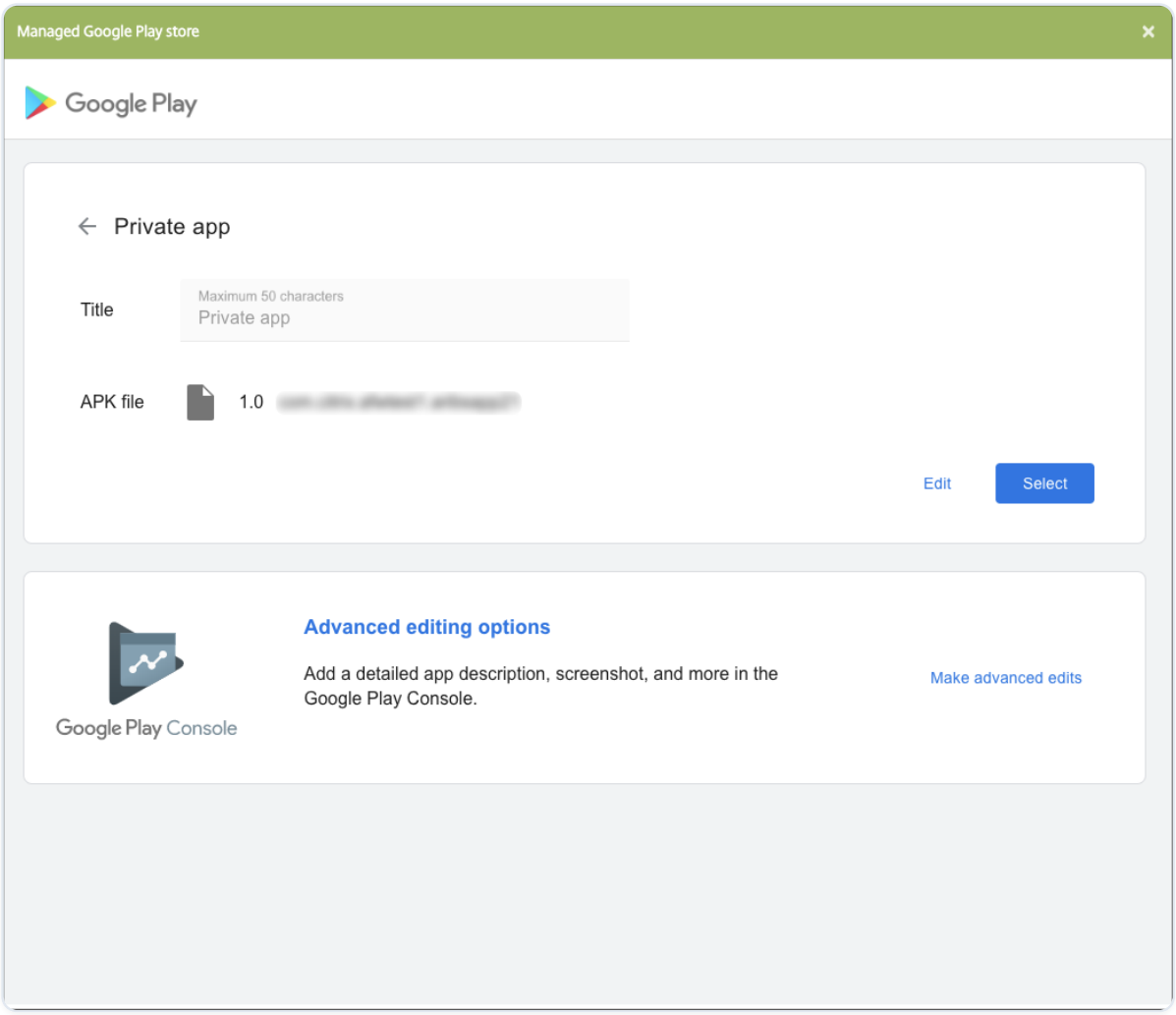
a. Escriba el nombre de su aplicación y cargue el archivo .apk. Cuando termine, haga clic en **Crear**. La publicación de su aplicación privada puede tardar hasta 10 minutos.



b. Introduzca una dirección de correo electrónico para recibir actualizaciones sobre sus aplicaciones.



c. Una vez publicada la aplicación, haga clic en el icono de la aplicación privada. Si desea agregar una descripción de la aplicación, cambiar el icono de la aplicación y realizar otras acciones, haga clic en **Realizar ediciones avanzadas**. De lo contrario, haga clic en **Seleccionar** para abrir la página de información de la aplicación.

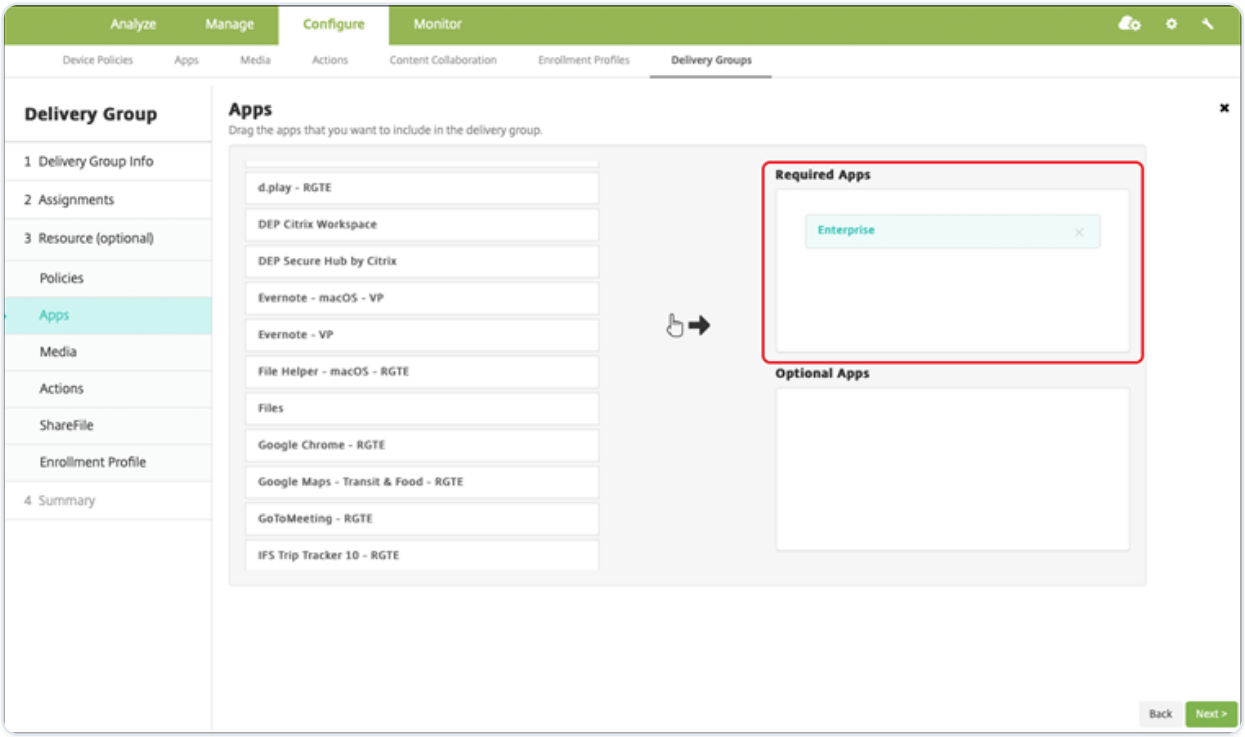


5. Haga clic en **Siguiente**. Aparece la página de información de la aplicación para la plataforma.
6. Configure los ajustes para el tipo de plataforma, como:
    - **Nombre de archivo:** Opcionalmente, escriba un nuevo nombre para la aplicación.
    - **Descripción de la aplicación:** Opcionalmente, escriba una nueva descripción para la aplicación.
    - **Versión de la aplicación:** No puede cambiar este campo.
    - **ID de paquete:** Identificador único de su aplicación.
    - **Versión mínima del SO:** Opcionalmente, escriba la versión más antigua del sistema operativo que el dispositivo puede ejecutar para usar la aplicación.
    - **Versión máxima del SO:** Opcionalmente, escriba la versión más reciente del sistema operativo que el dispositivo debe ejecutar para usar la aplicación.
    - **Dispositivos excluidos:** Opcionalmente, escriba el fabricante o los modelos de dispositivos que no pueden ejecutar la aplicación.
7. Configure las reglas de implementación y la configuración de la tienda.

8. Asigne los grupos de entrega a la aplicación y haga clic en **Guardar**. Para obtener más información, consulte Implementar recursos.

Paso 2: Configurar la implementación de la aplicación

1. Vaya a **Configurar > Grupos de entrega** y seleccione el grupo de entrega que configuró. Haga clic en **Modificar**.
2. En la sección **Aplicaciones**, arrastre las aplicaciones deseadas al cuadro **Aplicaciones requeridas**.



3. En la página **Resumen**, haga clic en **Guardar**.
4. En la página **Grupos de entrega**, seleccione el grupo de entrega y haga clic en **Implementar**.

Aplicaciones privadas habilitadas para MDX

Para agregar aplicaciones de Android Enterprise como aplicaciones empresariales habilitadas para MDX:

1. Cree una aplicación privada de Android Enterprise y habilite MDX en la aplicación.
2. Agregue la aplicación a la consola de Citrix Endpoint Management.
   - Aloje y publique la aplicación en Google Play Store administrado.
   - Agregue la aplicación a la consola de Citrix Endpoint Management como una aplicación Enterprise.
3. Agregue el archivo MDX a Citrix Endpoint Management.

Si decide alojar y publicar aplicaciones a través de Google Play Store, no opte por la firma de certificados de Google. Firme la aplicación con el mismo certificado utilizado para habilitar MDX en la aplicación. Para obtener más información sobre la publicación de aplicaciones, consulte la documentación de Google sobre Publicar su aplicación y Firmar su aplicación. El SDK de MAM no encapsula aplicaciones, por lo que no requiere un certificado diferente al utilizado para desarrollar la aplicación.

Para obtener más información sobre la publicación de aplicaciones privadas a través de Google Play Console, consulte la documentación de Google sobre cómo Publicar aplicaciones privadas desde Play Console.

Para publicar una aplicación a través de Citrix Endpoint Management, consulte las siguientes secciones.

Prepare una aplicación Android Enterprise

Al crear una aplicación Android Enterprise, asegúrese de seguir las Prácticas recomendadas para aplicaciones privadas de Google.

Después de crear una aplicación Android Enterprise, integre el SDK de MAM con la aplicación o encapsule la aplicación mediante MDX Toolkit. Luego, agregue los archivos resultantes a XenMobile.

Puede actualizar la aplicación cargando un archivo .apk actualizado. Los siguientes pasos cubren la encapsulación de aplicaciones con MDX Toolkit.

1. Cree su aplicación Android Enterprise y genere un archivo .apk firmado.
2. El siguiente archivo de ejemplo tiene todas las directivas conocidas, algunas de las cuales podrían no ser aplicables a su entorno. Cualquier configuración inutilizable se ignora. Cree un archivo XML con los siguientes parámetros:

```
<?xml version="1.0" encoding="UTF-8"?>

<MobileAppPolicies>

    <PolicySchemaVersion>

        1.0

    </PolicySchemaVersion>

    <Policies>
```

```
        <DevicePasscode>false</DevicePasscode>

        <AppPasscode>false</AppPasscode>

        <MaxOfflinePeriod>72</MaxOfflinePeriod>

        <StepupAuthAddress/>

        <RequireUserEntropy>false</RequireUserEntropy>

        <BlockRootedDevices>true</BlockRootedDevices>

        <BlockDebuggerAccess>false</BlockDebuggerAccess>

        <RequireDeviceLock>false</RequireDeviceLock>

        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
NonCompliantDeviceBehavior>

        <WifiOnly>false</WifiOnly>

        <RequireInternalNetwork>false</RequireInternalNetwork>

        <InternalWifiNetworks/>

        <AllowedWifiNetworks/>

        <UpgradeGracePeriod>168</UpgradeGracePeriod>

        <WipeDataOnAppLock>false</WipeDataOnAppLock>

        <ActivePollPeriod>60</ActivePollPeriod>

        <PublicFileAccessLimitsList/>

        <CutAndCopy>Unrestricted</CutAndCopy>

        <Paste>Unrestricted</Paste>

        <DocumentExchange>Unrestricted</DocumentExchange>

        <OpenInExclusionList/>
```

```
        <InboundDocumentExchange>Unrestricted</InboundDocumentExchange>

        <InboundDocumentExchangeWhitelist/>

        <connectionSecurityLevel>TLS</connectionSecurityLevel>

        <DisableCamera>false</DisableCamera>

        <DisableGallery>false</DisableGallery>

        <DisableMicrophone>false</DisableMicrophone>

        <DisableLocation>false</DisableLocation>

        <DisableSms>false</DisableSms>

        <DisableScreenCapture>false</DisableScreenCapture>

        <DisableSensor>false</DisableSensor>

        <DisableNFC>false</DisableNFC>

        <BlockLogs>false</BlockLogs>

        <DisablePrinting>false</DisablePrinting>

        <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
MvpnNetworkAccess>

        <MvpnSessionRequired>False</MvpnSessionRequired>

        <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>

        <DisableLocalhostConnections>false</
DisableLocalhostConnections>

        <CertificateLabel/>

        <DefaultLoggerOutput>file,console</DefaultLoggerOutput>

        <DefaultLoggerLevel>15</DefaultLoggerLevel>

        <MaxLogFiles>2</MaxLogFiles>
```

```
        <MaxLogFileSize>2</MaxLogFileSize>

        <RedirectSystemLogs>false</RedirectSystemLogs>

        <EncryptLogs>false</EncryptLogs>

        <GeofenceLongitude>0</GeofenceLongitude>

        <GeofenceLatitude>0</GeofenceLatitude>

        <GeofenceRadius>0</GeofenceRadius>

        <EnableGoogleAnalytics>false</EnableGoogleAnalytics>

        <Authentication>OfflineAccessOnly</Authentication>

        <ReauthenticationPeriod>480</ReauthenticationPeriod>

        <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>

    </Policies>

</MobileAppPolicies>
```

3. Encapsule la aplicación usando MDX Toolkit. Para obtener información sobre el uso de MDX Toolkit, consulte Encapsular aplicaciones móviles Android.

   Establezca el parámetro **apptype** en **Premium**. Utilice el archivo XML del paso anterior en el comando que se describe a continuación.

   Si conoce la URL de la tienda de la aplicación, establezca el parámetro **storeURL** en la URL de la tienda. Los usuarios descargan la aplicación desde la URL de la tienda después de que usted la publique.

   Aquí tiene un ejemplo de un comando de MDX Toolkit utilizado para encapsular una aplicación llamada SampleAEapp:

   ```
   ```

   ```
    java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en
   -Duser.variant
   ```

```
 -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap

 -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk

 -out ~/Desktop/AEAppFiles/SampleAEApp.mdx

 -MinPlatform 5.0

 -keystore /MyKeystore

 -storepass mystorepwd123

 -keyalias key0

 -keypass mykeypwd123

 -storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"

 -appType Premium

 -premiumMdxPolicies <Path to Premium policy XML>

```

Al encapsular la aplicación, se genera un archivo .apk encapsulado y un archivo .mdx.

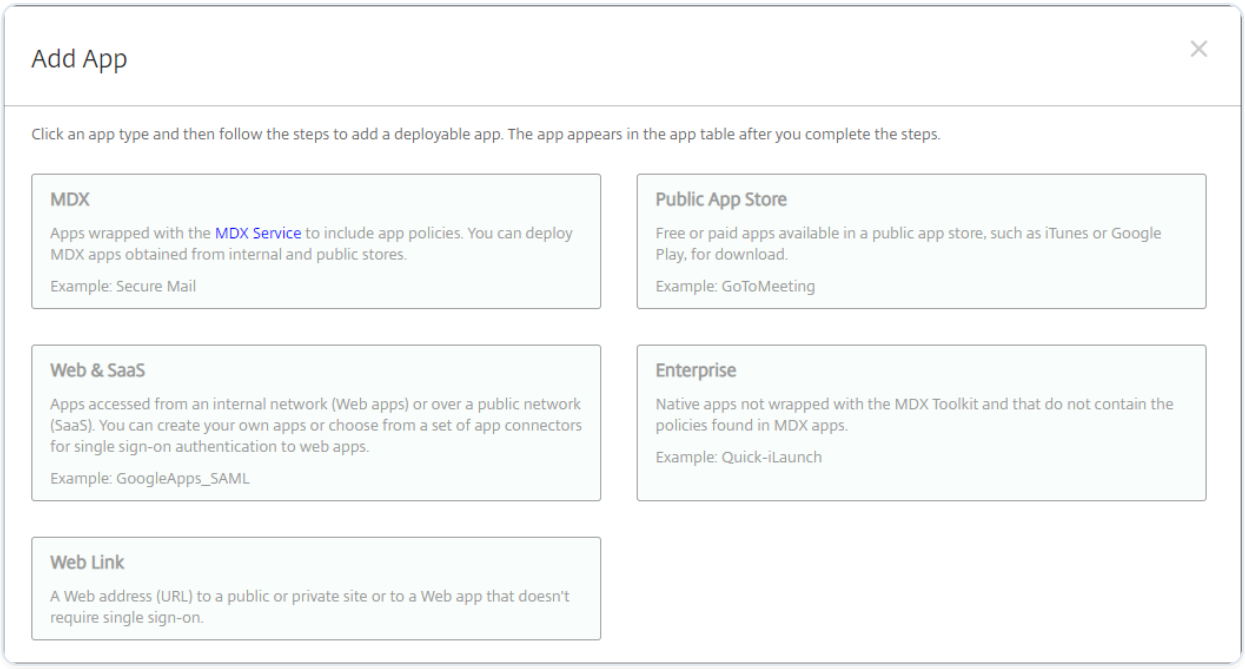
Agregar el archivo .apk encapsulado

Agregue la aplicación de una de estas dos maneras:

- Publique la aplicación directamente en Google Play Store administrado y agréguela a la consola de Citrix Endpoint Management como una aplicación de tienda de Google Play administrada. Siga la documentación de Google sobre cómo Publicar aplicaciones privadas y, a continuación, siga los pasos de la sección Aplicaciones de tienda de aplicaciones administradas.
- Agregue la aplicación a la consola de Citrix Endpoint Management como una aplicación empresarial. Siga estos pasos:

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones**. Se abrirá la página **Aplicaciones**.

2. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.

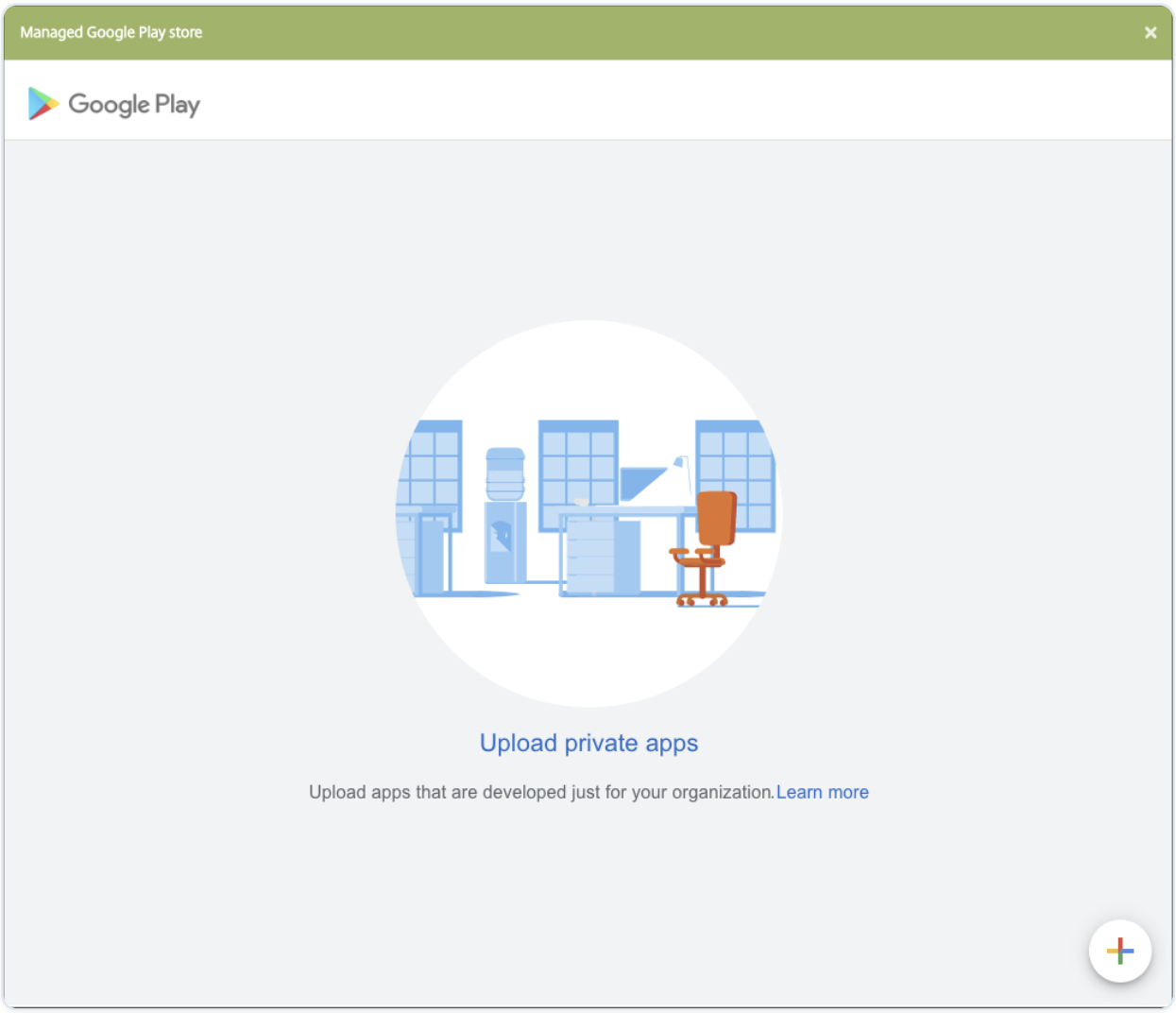


3. Haga clic en **Empresa**. En el panel **Información de la aplicación**, escriba la siguiente información:

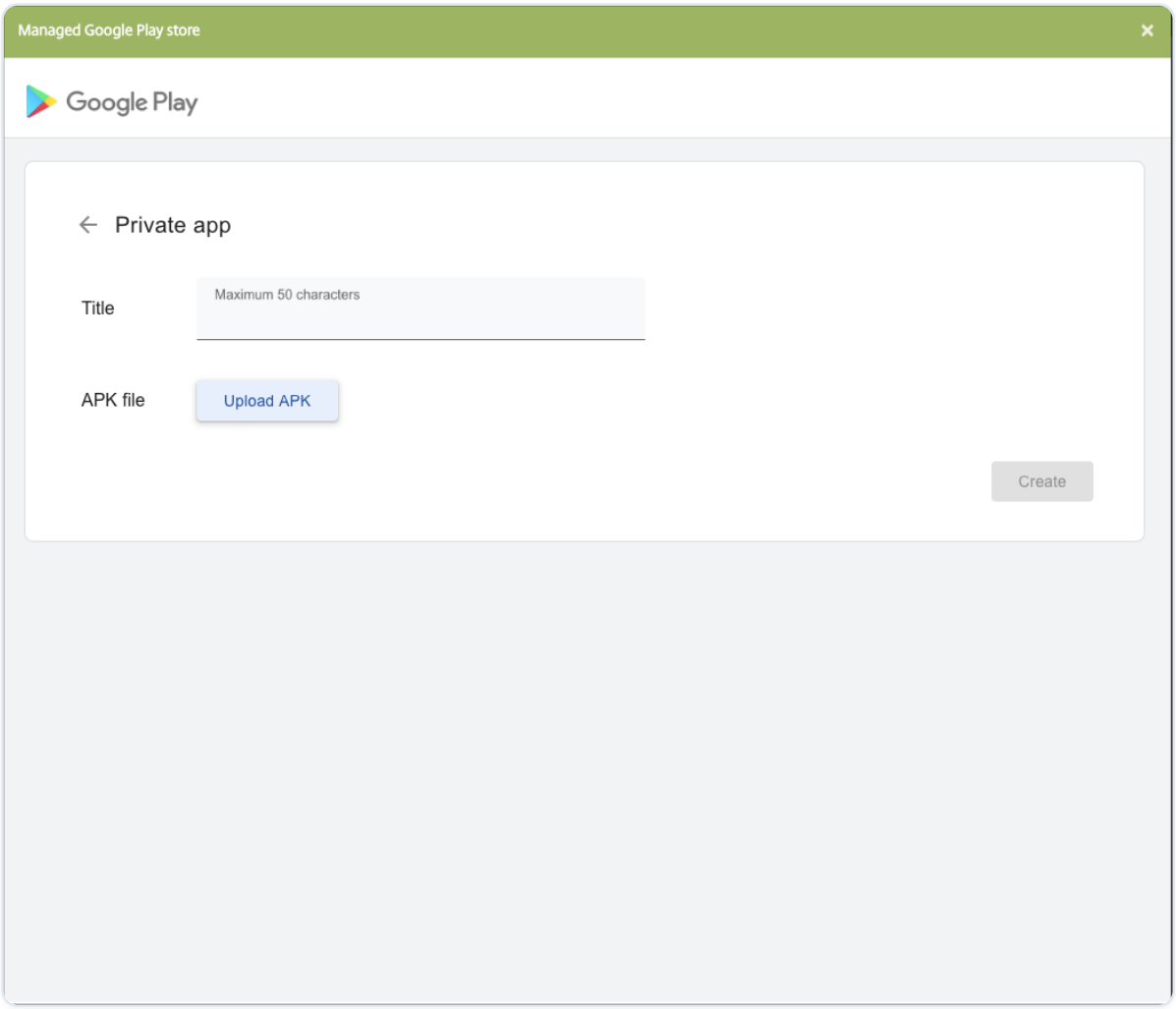
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre aparece en la tabla Aplicaciones, en Nombre de la aplicación.
   - **Descripción:** Escriba una descripción opcional de la aplicación.

4. Seleccione **Android Enterprise** como plataforma.

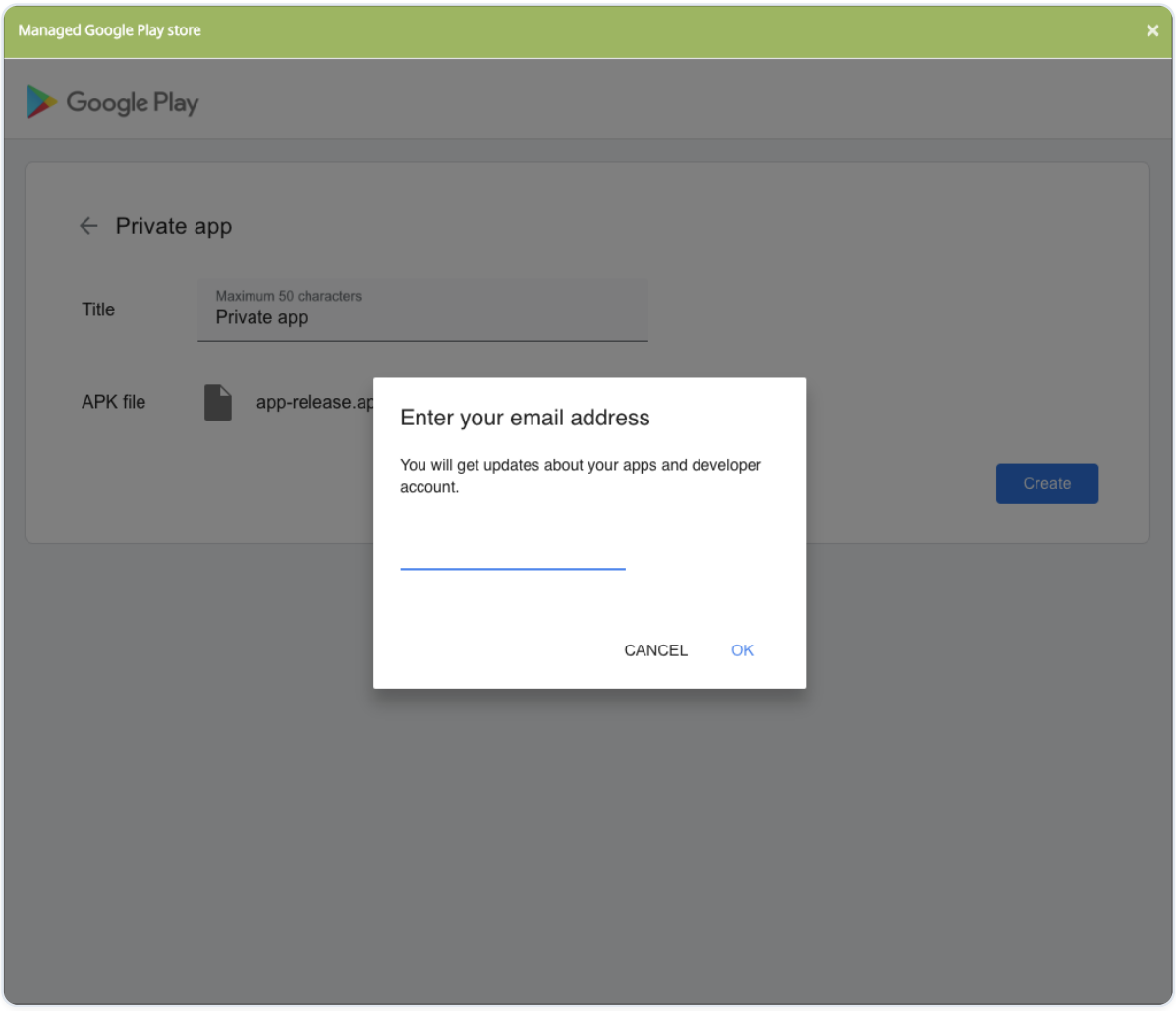
5. El botón **Cargar** abre Google Play Store administrado. No es necesario registrarse para obtener una cuenta de desarrollador para publicar una aplicación privada. Haga clic en el icono **Más** en la esquina inferior derecha para continuar.



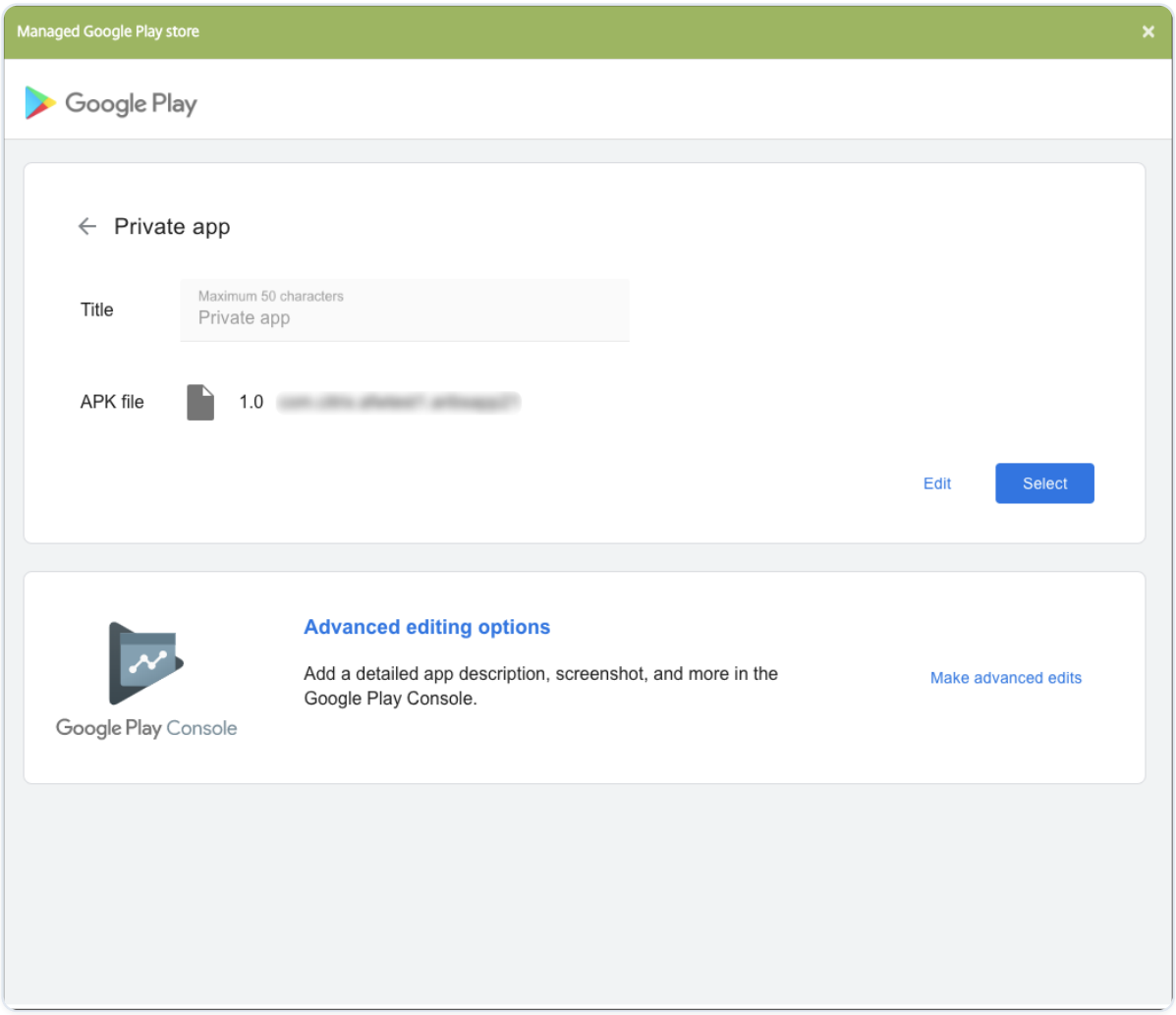
a. Escriba el nombre de su aplicación y cargue el archivo .apk. Cuando termine, haga clic en **Crear**. La publicación de su aplicación privada puede tardar hasta 10 minutos.



b. Introduzca una dirección de correo electrónico para recibir actualizaciones sobre sus aplicaciones.



c. Una vez publicada la aplicación, haga clic en el icono de la aplicación privada y, a continuación, en **Seleccionar** para abrir la página de información de la aplicación.



6. Haga clic en **Siguiente**. Aparecerá la página de información de la aplicación para la plataforma.
7. Configure los ajustes para el tipo de plataforma, como:

    - **Nombre de archivo:** Opcionalmente, escriba un nuevo nombre para la aplicación.
    - **Descripción de la aplicación:** Opcionalmente, escriba una nueva descripción para la aplicación.
    - **Versión de la aplicación:** No puede cambiar este campo.
    - **ID de paquete:** Identificador único de su aplicación.
    - **Versión mínima del SO:** Opcionalmente, escriba la versión más antigua del sistema operativo que el dispositivo puede ejecutar para usar la aplicación.
    - **Versión máxima del SO:** Opcionalmente, escriba la versión más reciente del sistema operativo que el dispositivo debe ejecutar para usar la aplicación.
    - **Dispositivos excluidos:** Opcionalmente, escriba el fabricante o los modelos de dispositivos que no pueden ejecutar la aplicación.

8. Configure las reglas de implementación y la configuración de la tienda.
9. En la página **Aplicación empresarial**, haga clic en **Siguiente**. Aparece la página **Aprobaciones**.

   Para usar flujos de trabajo que requieran aprobación antes de permitir a los usuarios acceder a la aplicación, consulte Aplicar flujos de trabajo. Si no necesita un flujo de trabajo de aprobación, puede ir al paso 13.
10. Haga clic en **Siguiente**.
11. Aparece la página **Asignación de grupos de entrega**. No es necesario realizar ninguna acción en esta página. Los grupos de entrega y el programa de implementación de esta aplicación se configuran al agregar el archivo .mdx. Haga clic en **Guardar**.

Opcional: Agregar o cambiar la URL de la tienda

Si no conocía la URL de la tienda al empaquetar la aplicación, agréguela ahora.

1. Vea la aplicación en Google Play Store administrado. Al seleccionar la aplicación, la URL de la tienda aparece en la barra de direcciones de su navegador. Copie el nombre del paquete de la aplicación del formulario de URL. Por ejemplo: `https://play.google.com/store/apps/details?id=SampleAEappPackage`. La URL que copie podría comenzar con `https://play.google.com/work/`. Asegúrese de cambiar `work` a `store`.
2. Utilice MDX Toolkit para agregar la URL de la tienda al archivo .mdx:

```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \

setinfo \

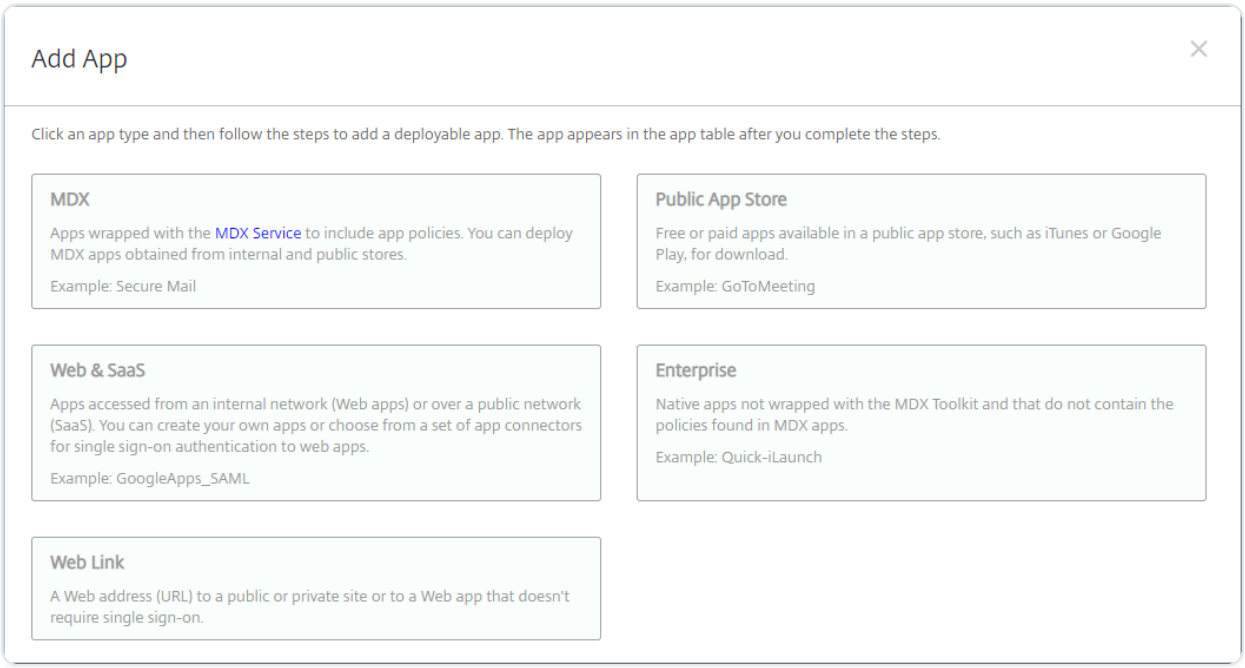
-in ~/Desktop/SampleApps/Sample.mdx \

-out ~/Desktop/SampleApps/wrapped/Sample.mdx \

-storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"
```

Agregar el archivo .mdx

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones**. Haga clic en **Agregar**. Aparece el cuadro de diálogo **Agregar aplicación**.

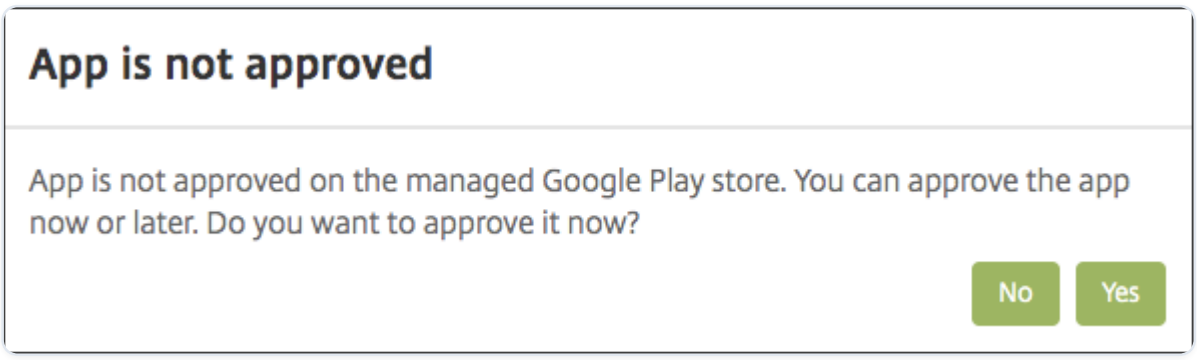


2. Haga clic en **MDX**. Aparece la página **Información de la aplicación MDX**. En el panel **Información de la aplicación**, escriba la siguiente información:

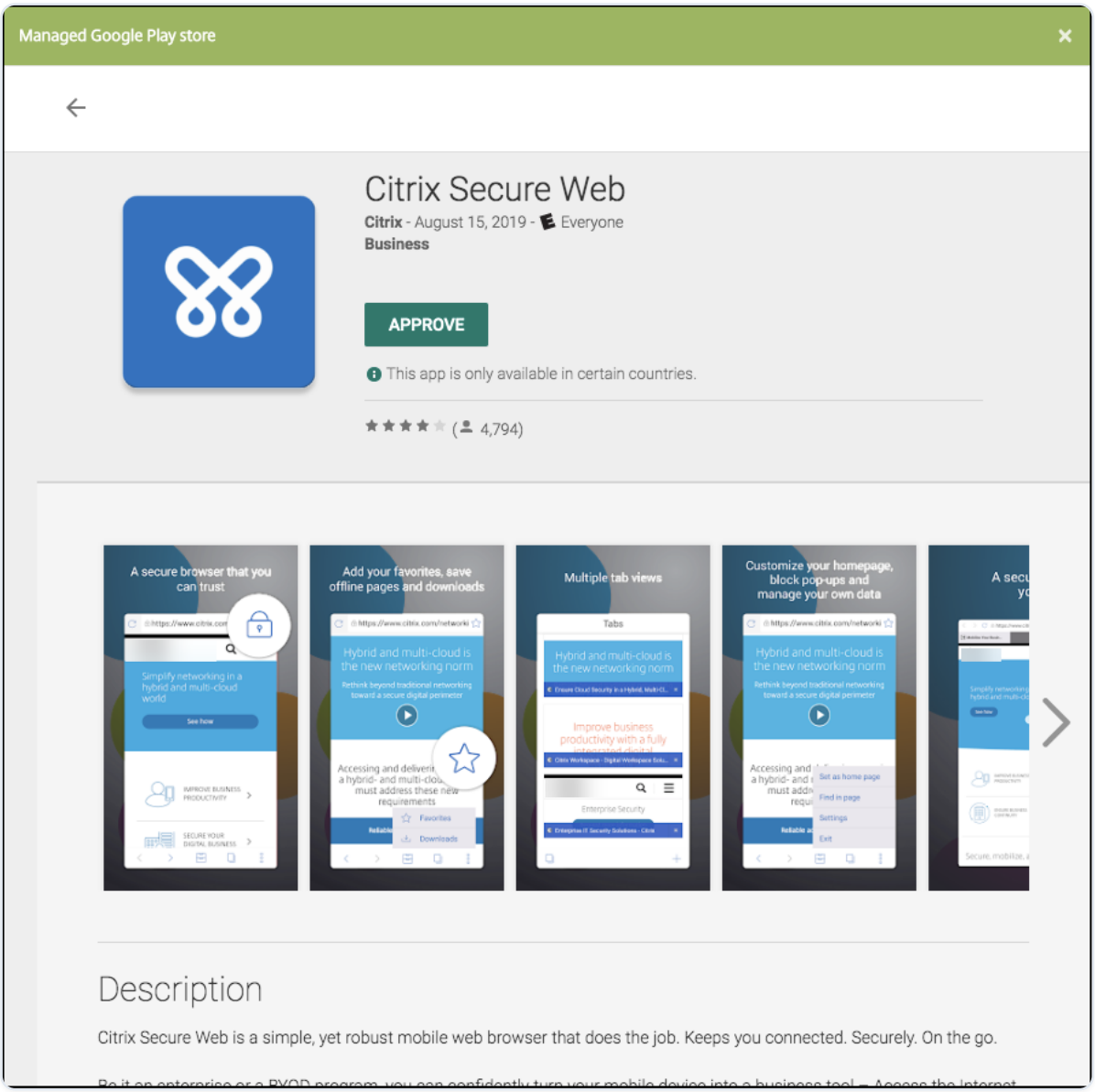
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. El nombre aparece en **Nombre de la aplicación** en la tabla **Aplicaciones**.
   - **Descripción:** Escriba una descripción opcional de la aplicación.

3. Seleccione **Android Enterprise** como plataforma.
4. Haga clic en **Cargar** y vaya al archivo MDX. Android Enterprise solo admite aplicaciones empaquetadas con el MDX Toolkit.

   - La interfaz de usuario le notifica si la aplicación adjunta requiere aprobación de Google Play Store administrado. Para aprobar la aplicación sin salir de la consola de Citrix Endpoint Management, haga clic en **Sí**.

     Una vez que se abra Google Play Store administrado, siga las instrucciones para aprobar y guardar la aplicación.



Cuando agregue la aplicación correctamente, aparecerá la página **Detalles de la aplicación**.

5. Configure estos ajustes:

   - **Nombre de archivo:** Escriba el nombre de archivo asociado a la aplicación.
   - **Descripción de la aplicación:** Escriba una descripción para la aplicación.
   - **Versión de la aplicación:** Opcionalmente, escriba el número de versión de la aplicación.
   - **ID del paquete:** Escriba el ID del paquete de la aplicación obtenido de Google Play Store administrado.
   - **Versión mínima del SO:** Opcionalmente, escriba la versión más antigua del sistema operativo que el dispositivo puede ejecutar para usar la aplicación.
   - **Versión máxima del SO:** Opcionalmente, escriba la versión más reciente del sistema operativo que el dispositivo debe ejecutar para usar la aplicación.

- **Dispositivos excluidos:** Opcionalmente, escriba el fabricante o los modelos de dispositivos que no pueden ejecutar la aplicación.

6. Configure las **directivas MDX**. Las directivas MDX varían según la plataforma e incluyen opciones para áreas de directivas, como Autenticación, Seguridad del dispositivo y Restricciones de aplicaciones. En la consola, cada una de las directivas tiene una información sobre herramientas que la describe. Para obtener información sobre las directivas de aplicaciones disponibles para cada tipo de plataforma de dispositivo, consulte:

   - Información general sobre el SDK de MAM
   - Directivas de aplicaciones de terceros de MDX de un vistazo

7. Configure las reglas de implementación y la configuración del almacén.

   La opción **Implementar para conexión siempre activa** se aplica cuando ha configurado la clave de implementación en segundo plano de programación en **Parámetros > Propiedades del servidor**.

   La opción siempre activa:

   - No está disponible para dispositivos iOS
   - No está disponible para clientes de Android y Android Enterprise que comenzaron a usar Citrix Endpoint Management con la versión 10.18.19 o posterior
   - No se recomienda para clientes de Android y Android Enterprise que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19

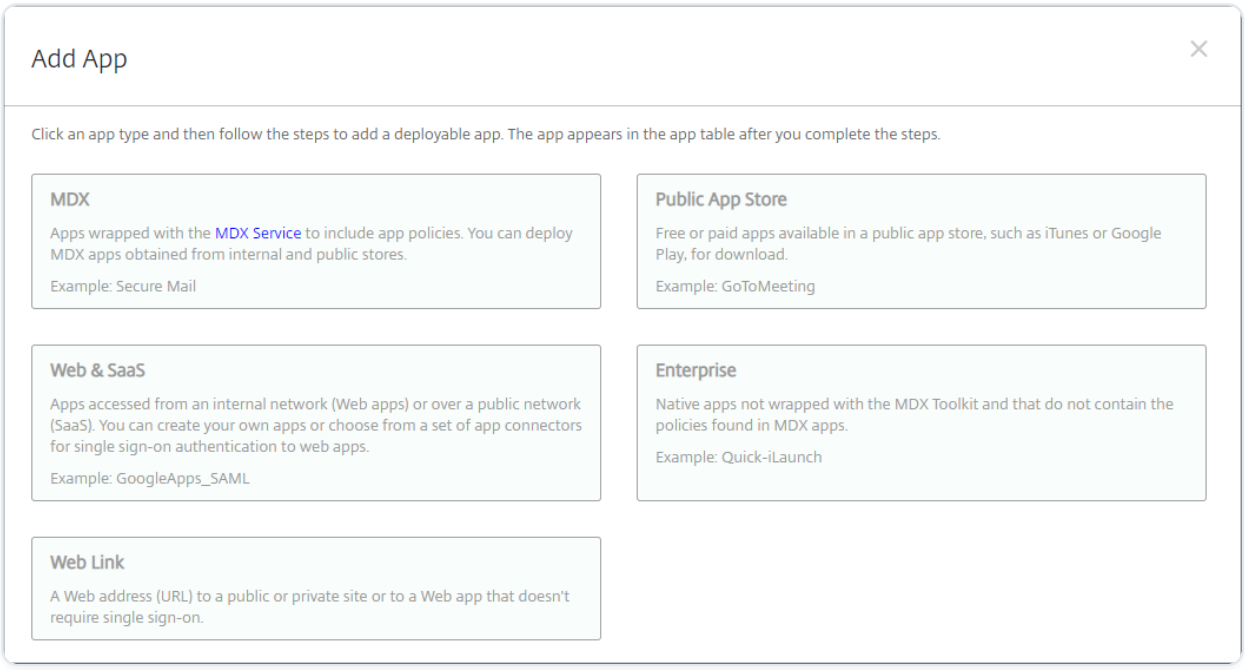
   El programa de implementación que configure es el mismo para todas las plataformas. Cualquier cambio que realice se aplica a todas las plataformas, excepto a **Implementar para conexión siempre activa**.

8. Asigne los grupos de entrega a la aplicación y haga clic en **Guardar**. Para obtener información, consulte Implementar recursos.

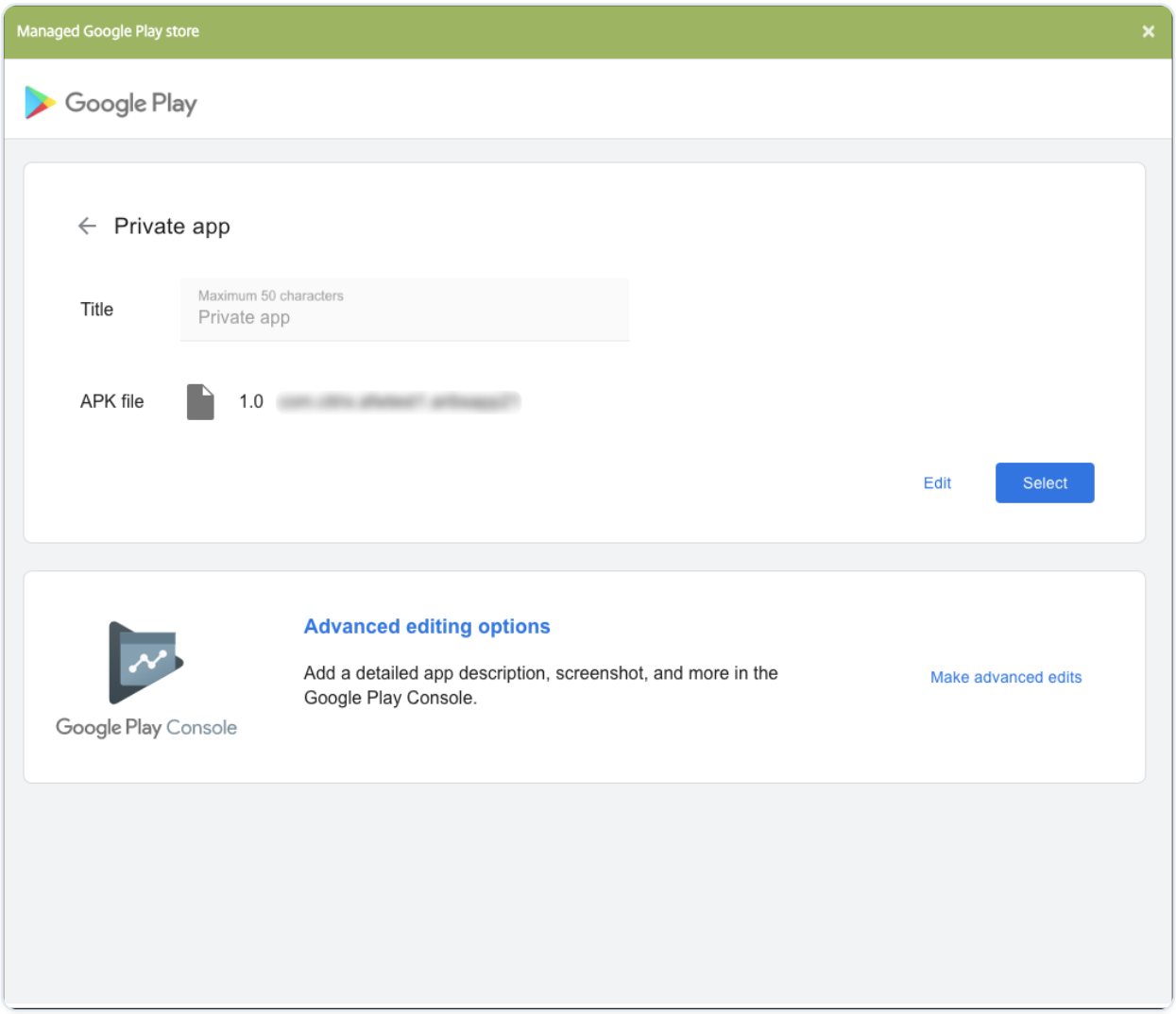
Actualizar la aplicación

Para actualizar la aplicación de Android Enterprise, empaquete y cargue un archivo .apk actualizado:

1. Empaquete el archivo .apk de la aplicación actualizada mediante el SDK de MAM o MDX Toolkit.
2. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones**. Se abre la página **Aplicaciones**.



3. Haga clic en **Agregar**. Aparece el cuadro de diálogo **Agregar aplicación**.
4. Haga clic en **Empresa**. En el panel **Información de la aplicación**, escriba la siguiente información:
    - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre aparece en la tabla Aplicaciones, en Nombre de la aplicación.
    - **Descripción:** Escriba una descripción opcional de la aplicación.
5. Seleccione **Android Enterprise** como plataforma.
6. Haga clic en **Siguiente**. Aparece la página **Aplicación empresarial**.
7. Haga clic en **Cargar**.
8. En la página de Google Play Store administrada, seleccione la aplicación que quiere actualizar.
9. En la página de información de la aplicación, haga clic en **editar** junto al nombre del archivo .apk.



10. Vaya al nuevo archivo .apk y cárguelo.
11. En la página de Google Play Store administrada, haga clic en **Guardar**.

Android Enterprise heredado para clientes de Google Workspace (anteriormente G Suite)

Los clientes de Google Workspace deben usar la configuración de Android Enterprise heredado para configurar Android Enterprise heredado. Google ha cambiado recientemente el nombre de G Suite a Google Workspace.

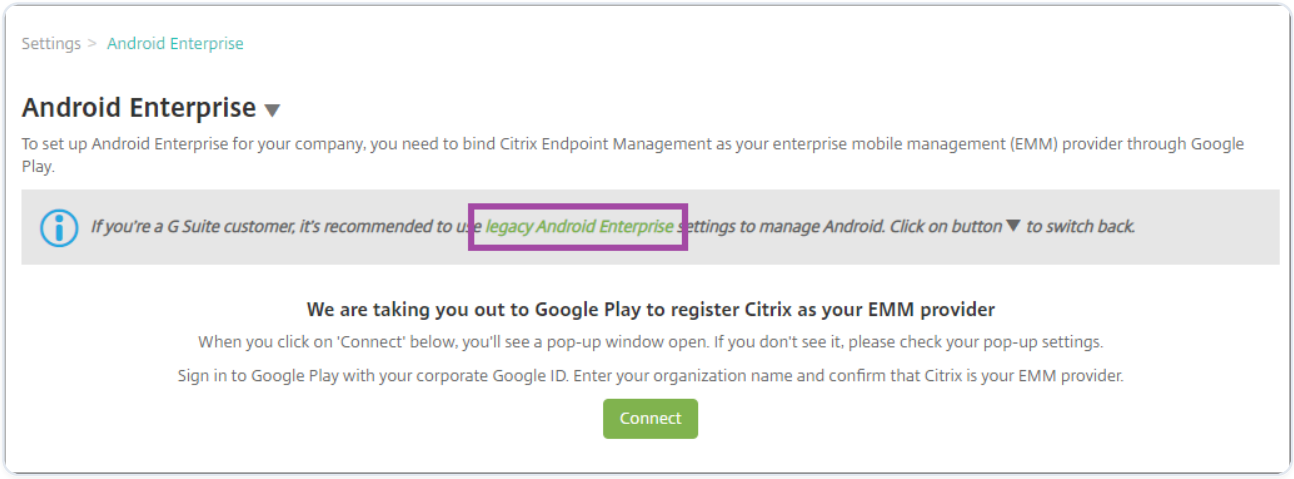
Si su organización ya usa Google Workspace para proporcionar a los usuarios acceso a las aplicaciones de Google, puede usar Google Workspace para registrar Citrix como su EMM. Si su organización usa Google Workspace, tiene un ID de empresa existente y cuentas de Google existentes para los usuarios. Para usar Citrix Endpoint Management con Google Workspace, debe sincronizarse con su directorio LDAP y recuperar la información de la cuenta de Google de Google mediante la API de Google Directory. Debido a que este tipo de empresa está vinculada a un dominio existente, cada dominio solo puede crear una empresa. Para inscribir un dispositivo en

Citrix Endpoint Management, cada usuario debe iniciar sesión manualmente con su cuenta de Google existente. La cuenta les da acceso a Google Play administrado, además de cualquier otro servicio de Google proporcionado por su plan de Google Workspace.

Requisitos para Android Enterprise heredado:

- Un dominio de acceso público
- Una cuenta de administrador de Google
- Dispositivos Android compatibles con perfiles administrados
- Una cuenta de Google con Google Play instalado
- Un perfil de trabajo configurado en el dispositivo

Para empezar a configurar Android Enterprise heredado, haga clic en **Android Enterprise heredado** en la página **Android Enterprise** en la configuración de Citrix Endpoint Management.



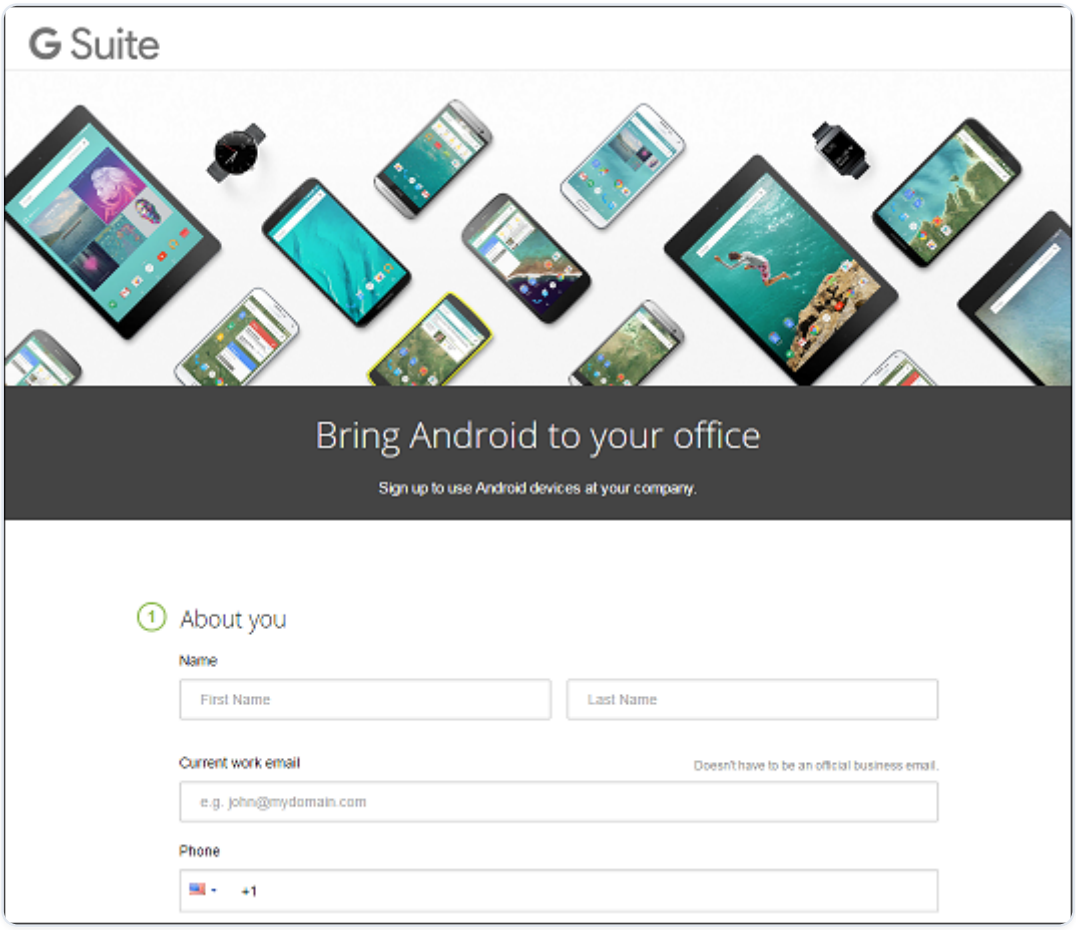
Crear una cuenta de Android Enterprise

Antes de poder configurar una cuenta de Android Enterprise, debe verificar su nombre de dominio con Google.

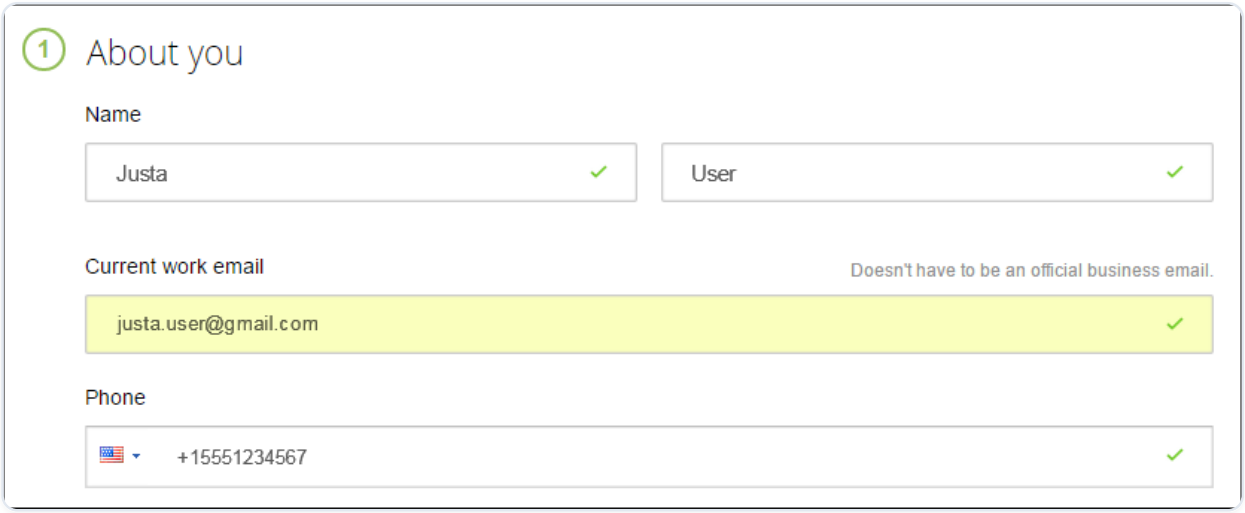
Si ya ha verificado su nombre de dominio con Google, puede saltar a este paso: Configurar una cuenta de servicio de Android Enterprise y descargar un certificado de Android Enterprise.

1. Vaya a `<https://gsuite.google.com/signup/basic/welcome>`.

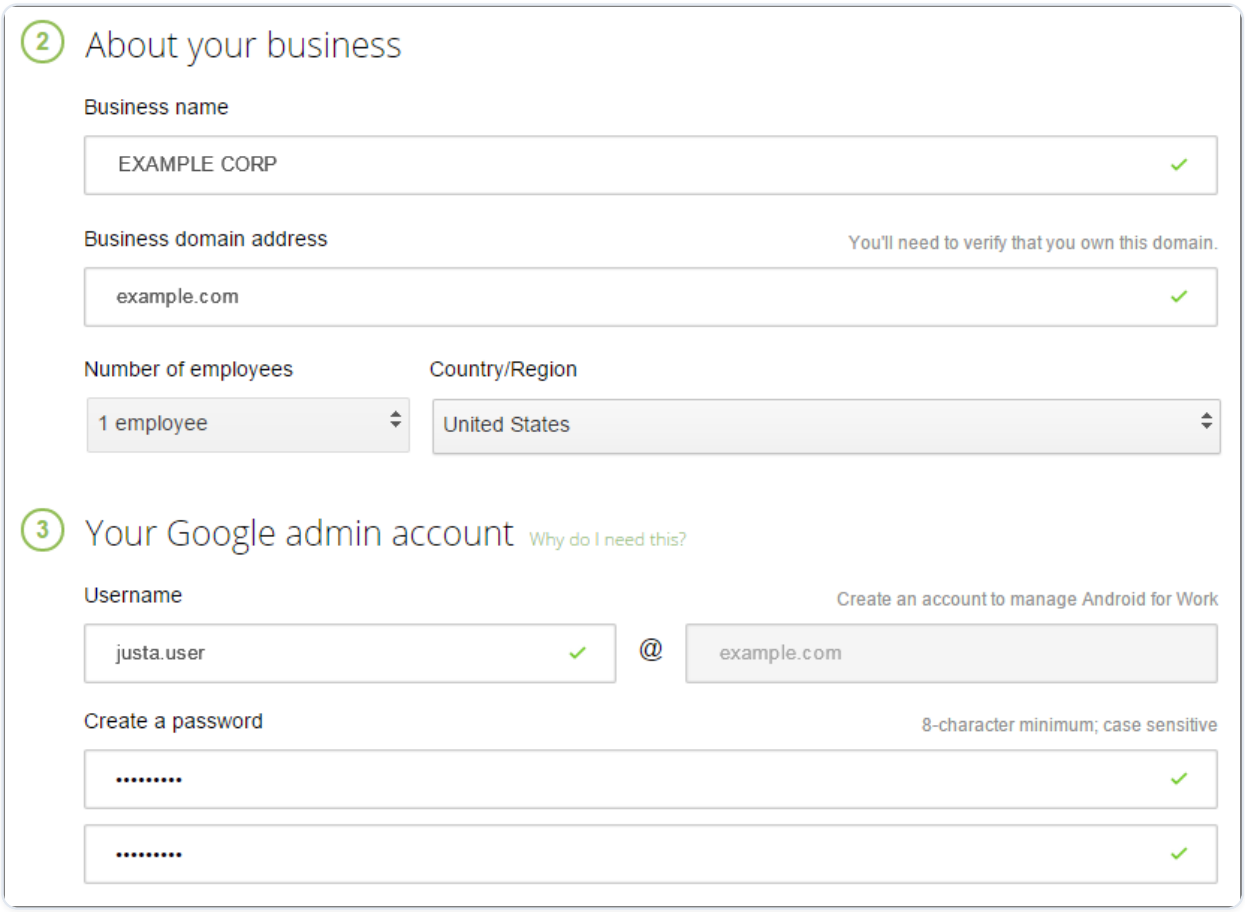
   La siguiente página muestra dónde escribe la información de su administrador y de la empresa.



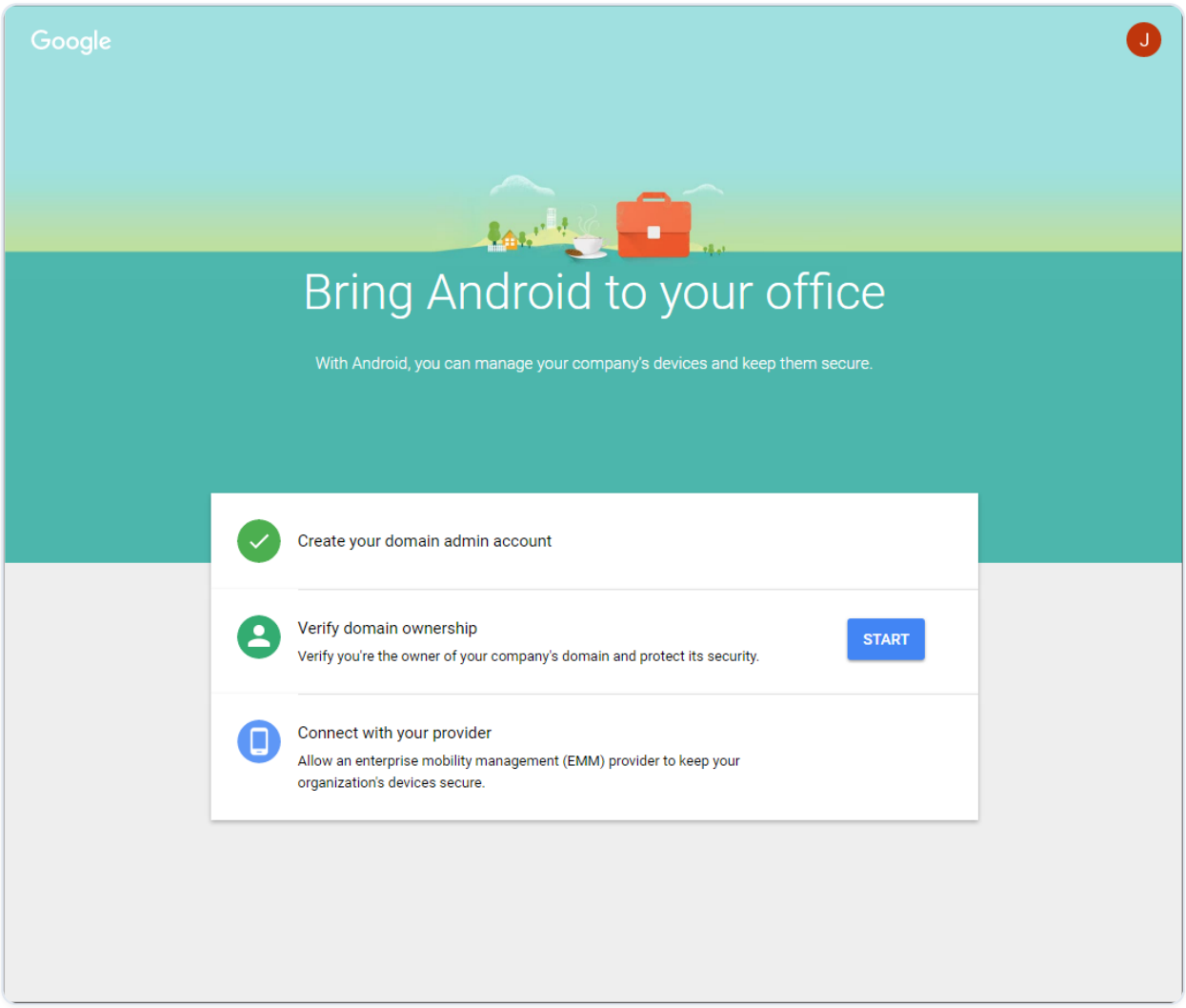
2. Escriba la información de usuario de su administrador.



3. Escriba la información de su empresa, además de la información de su cuenta de administrador.



El primer paso del proceso se ha completado y verá la siguiente página.



verificar la propiedad del dominio

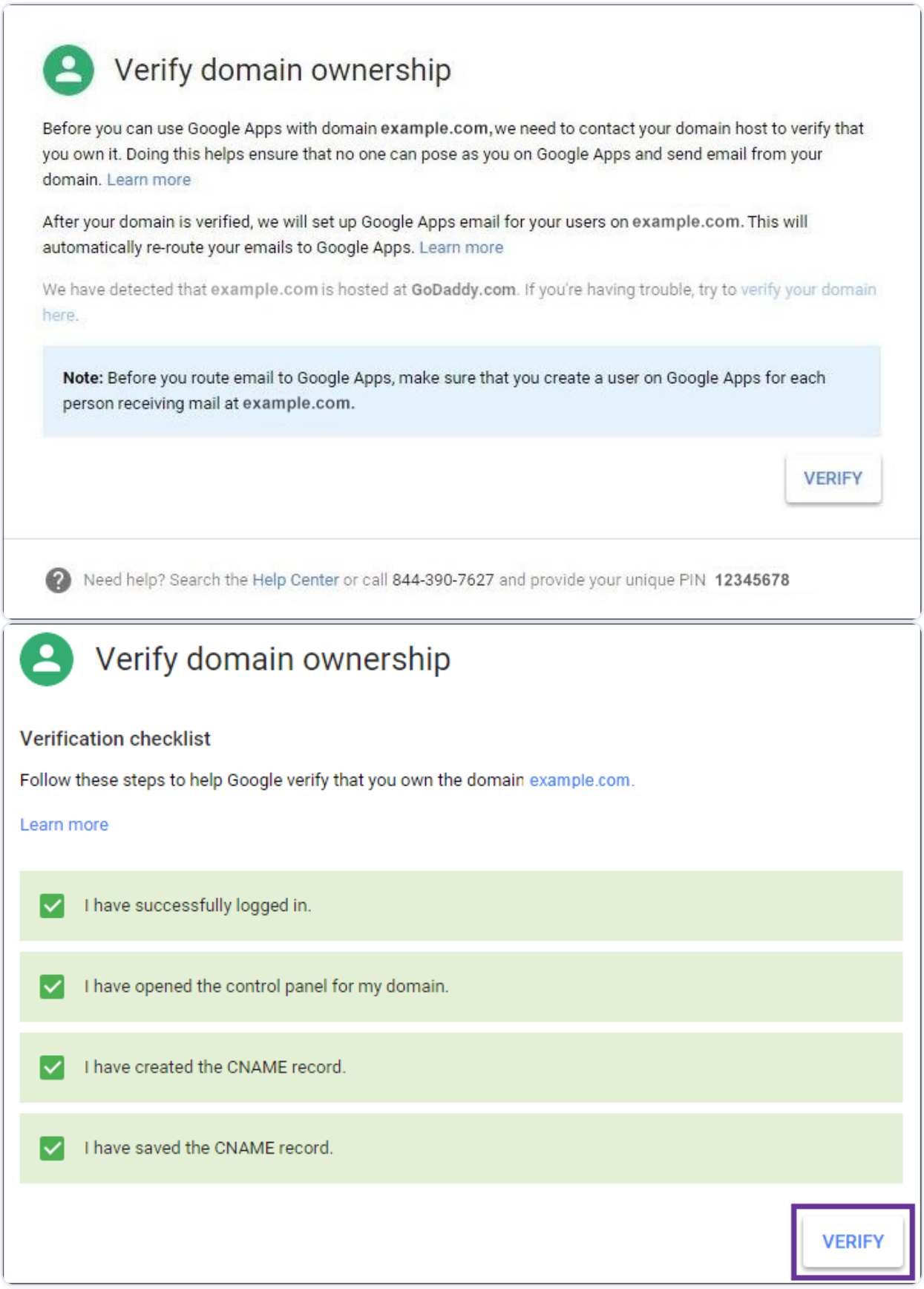
Permita que Google verificar su dominio de una de las siguientes maneras:

- Agregue un registro TXT o CNAME al sitio web de su proveedor de dominio.
- Cargue un archivo HTML al servidor web de su dominio.
- Agregue una etiqueta `<meta>` a su página de inicio. Google recomienda el primer método. Este artículo no cubre los pasos para verificar la propiedad de su dominio, pero puede encontrar la información que necesita aquí: https://support.google.com/a/answer/6248925.

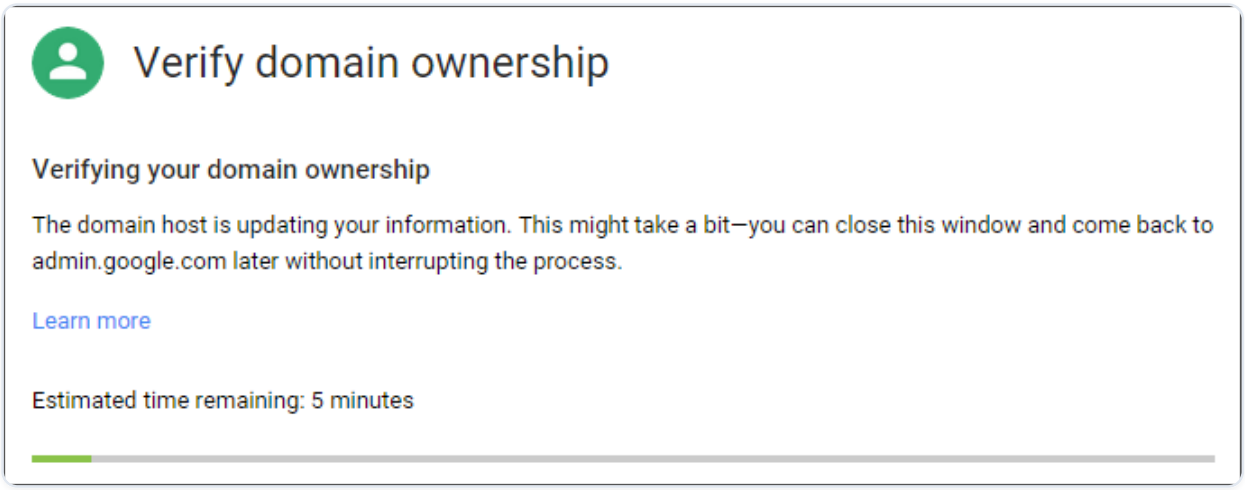
1. Haga clic en **Iniciar** para comenzar la verificación de su dominio.

   Aparece la página **verificar la propiedad del dominio**. Siga las instrucciones de la página para verificar su dominio.

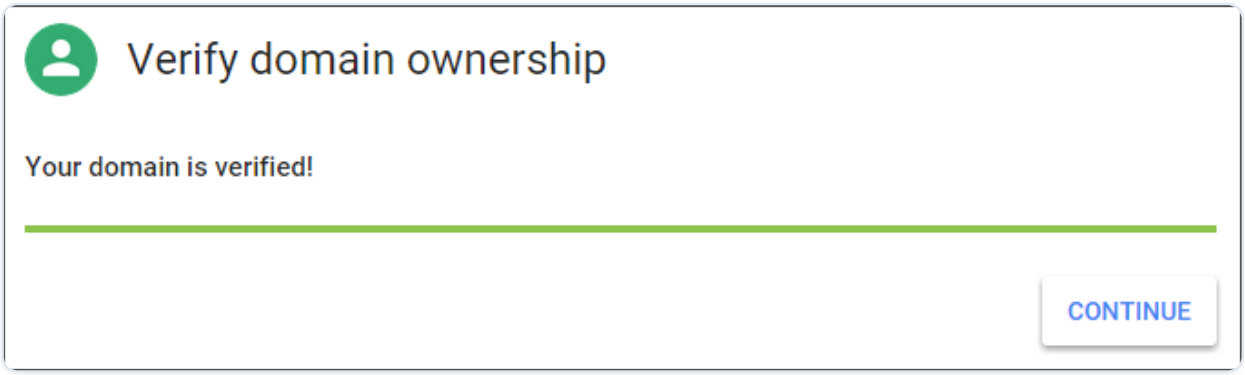
2. Haga clic en **verificar**.



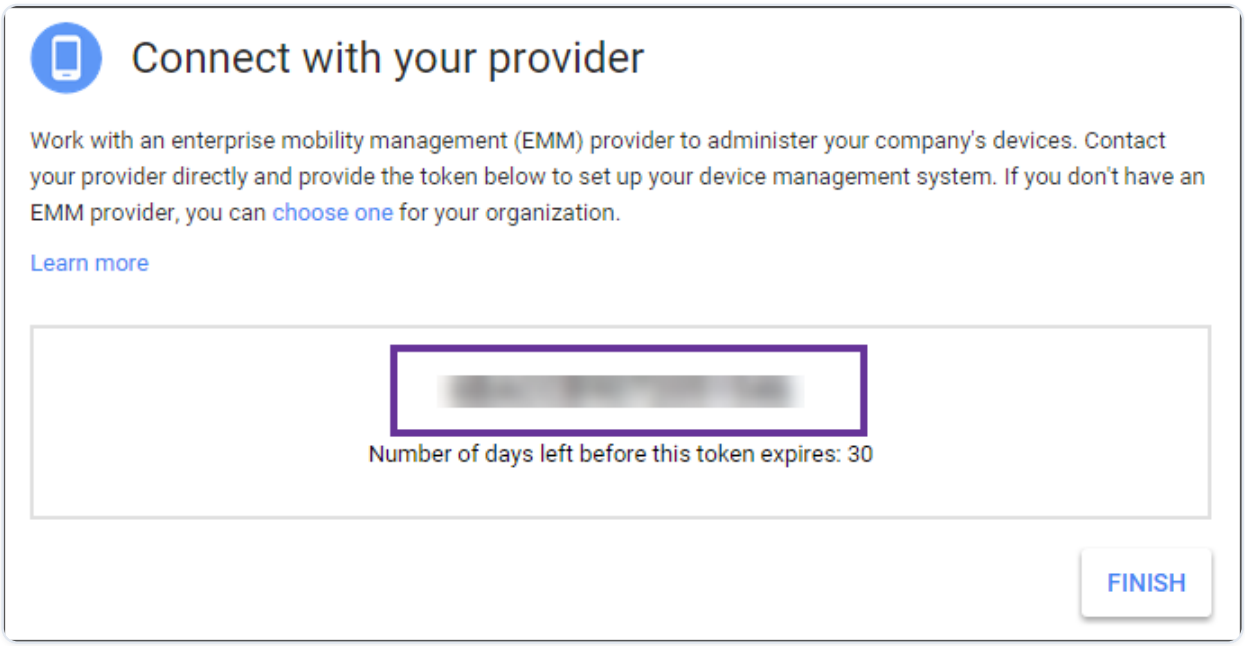
3. Google verifica la propiedad de su dominio.



4. Después de una verificación correcta, aparece la siguiente página. Haga clic en **Continuar**.



5. Google crea un token de enlace EMM que usted proporciona a Citrix® y utiliza al configurar los ajustes de Android Enterprise. Copie y guarde el token; lo necesitará más adelante en el procedimiento de configuración.



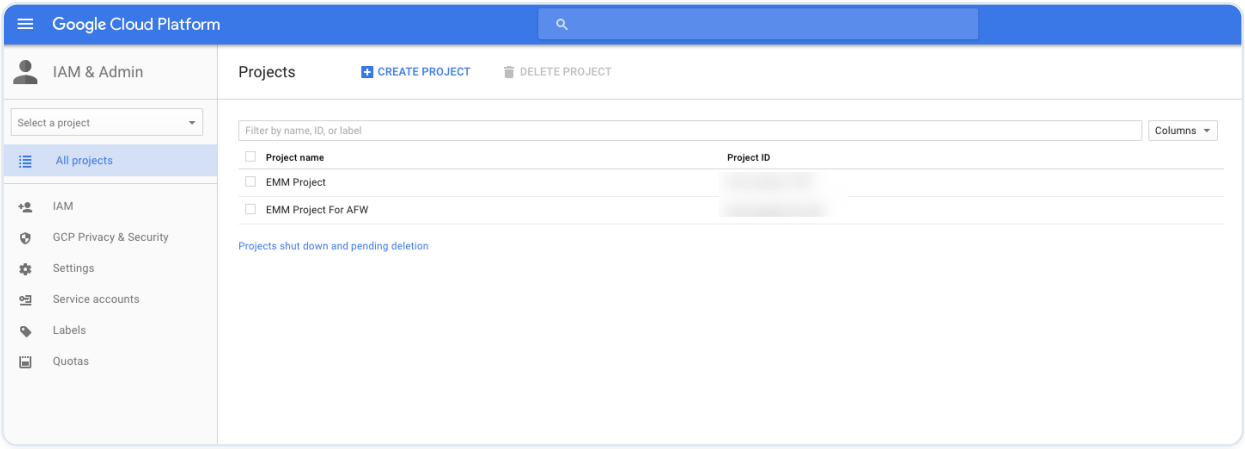
6. Haga clic en **Finalizar** para completar la configuración de Android Enterprise. Aparece una página que indica que ha verificado correctamente su dominio.

Después de crear una cuenta de servicio de Android Enterprise, puede iniciar sesión en la consola de administración de Google para gestionar la configuración de administración de movilidad.

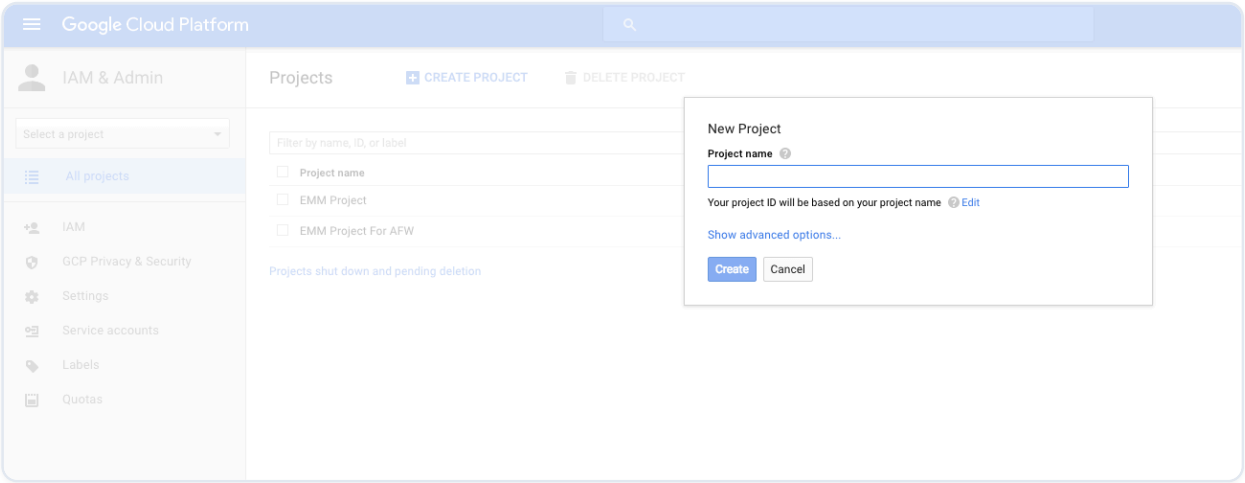
Configurar una cuenta de servicio de Android Enterprise y descargar un certificado de Android Enterprise

Para permitir que Citrix Endpoint Management se ponga en contacto con los servicios de Google Play y Directorio, debe crear una cuenta de servicio utilizando el portal de proyectos de Google para desarrolladores. Esta cuenta de servicio se utiliza para la comunicación de servidor a servidor entre Citrix Endpoint Management y los servicios de Google para Android. Para obtener más información sobre el protocolo de autenticación que se utiliza, vaya a `<https://developers.google.com/identity/protocols/OAuth2ServiceAccount>`.

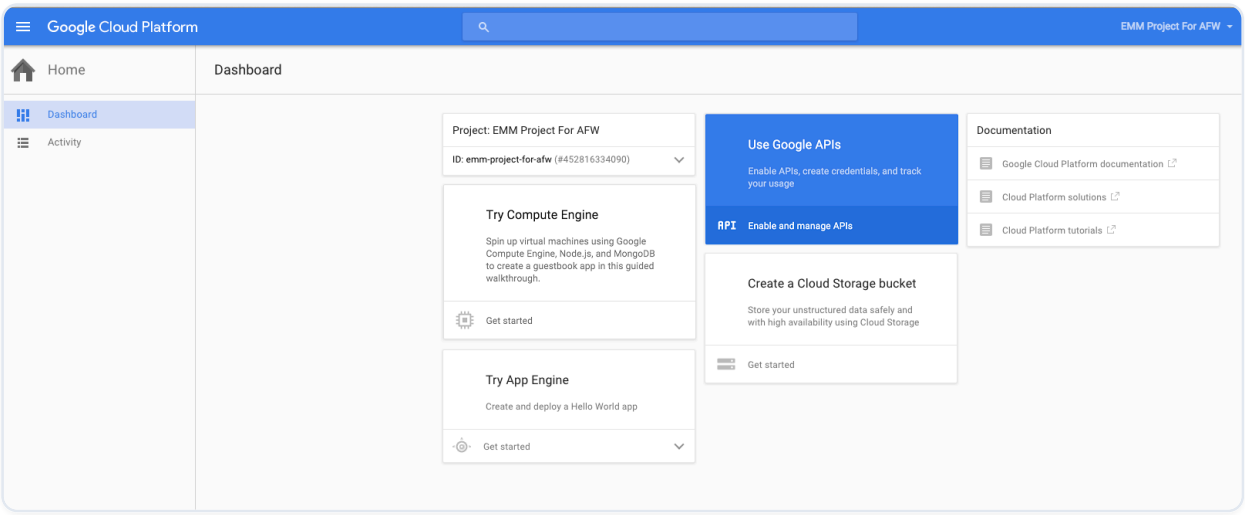
1. En un navegador web, vaya a `<https://console.cloud.google.com/project>` e inicie sesión con sus credenciales de administrador de Google
2. En la lista **Proyectos**, haga clic en **Crear proyecto**.



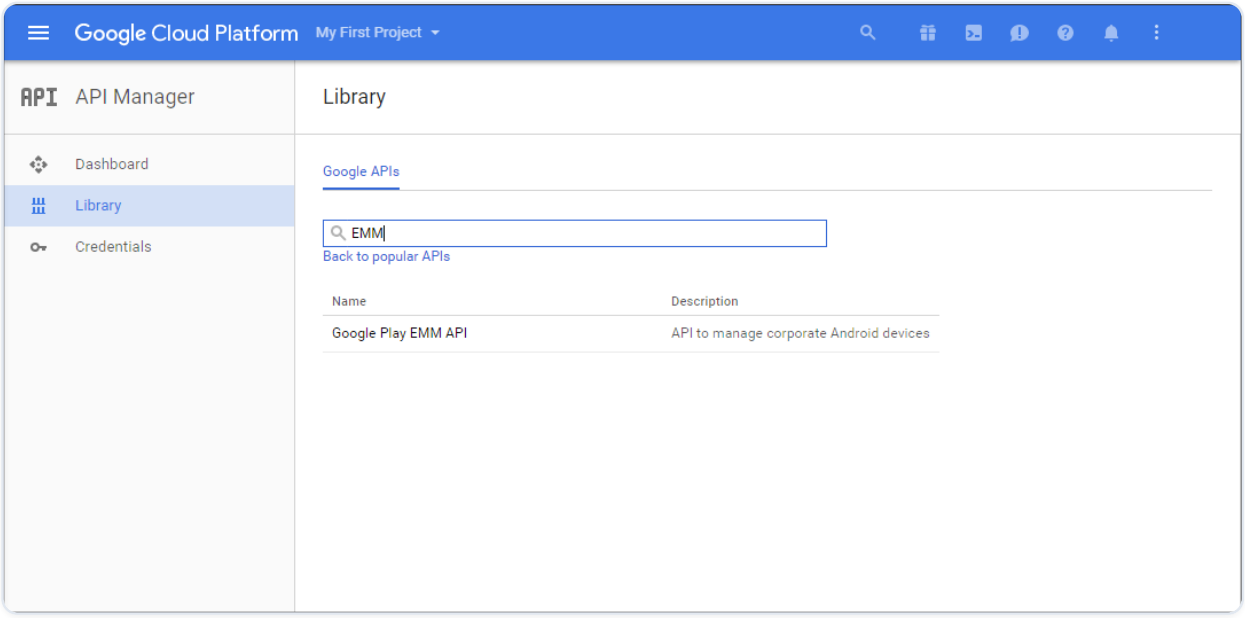
3. En **Nombre del proyecto**, escriba un nombre para el proyecto.



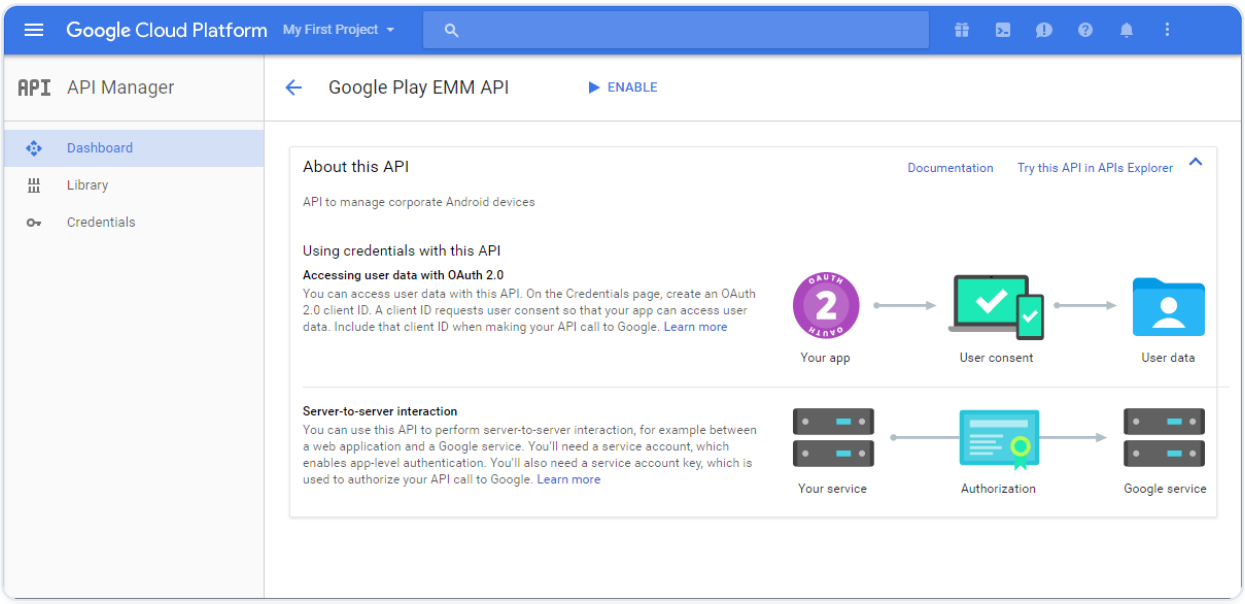
4. En el Panel de control, haga clic en **Usar API de Google**.



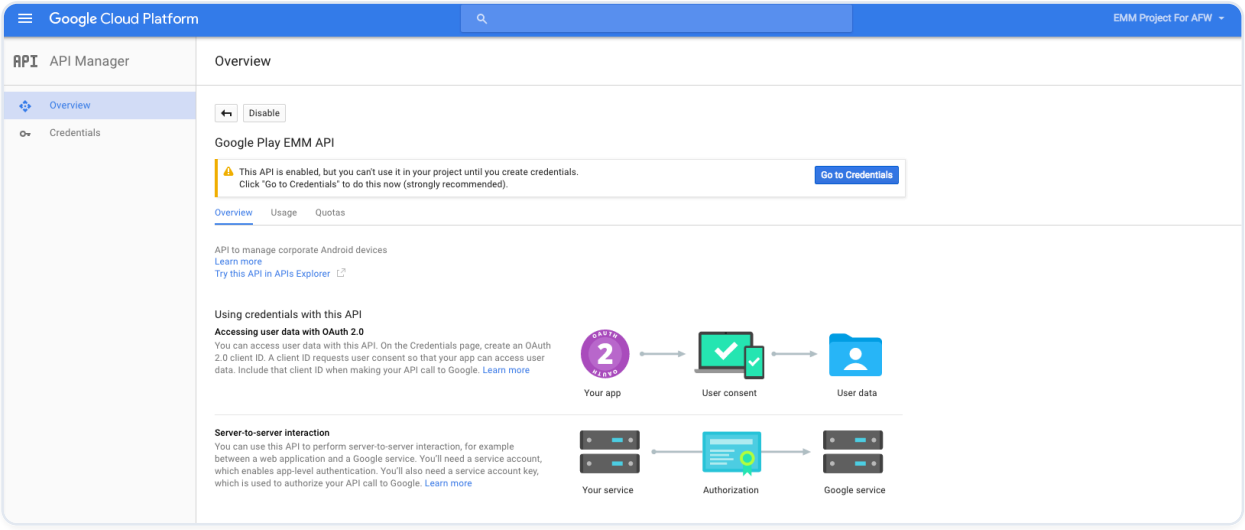
5. Haga clic en **Biblioteca**, en **Buscar**, escriba **EMM** y, a continuación, haga clic en el resultado de la búsqueda.



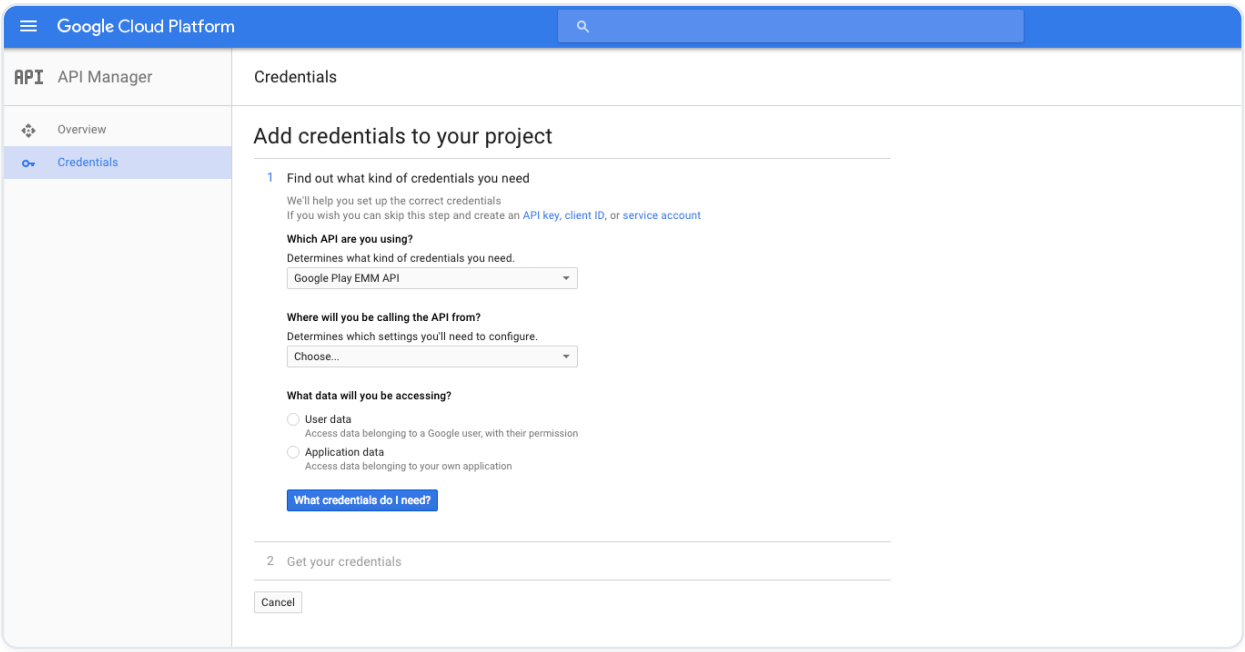
6. En la página **Información general**, haga clic en **Habilitar**.



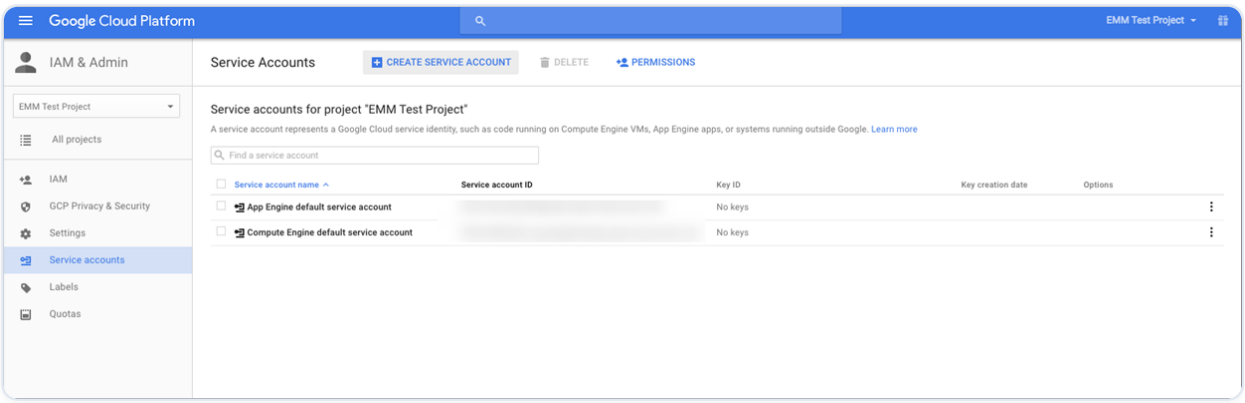
7. Junto a **API de EMM de Google Play**, haga clic en **Ir a Credenciales**.



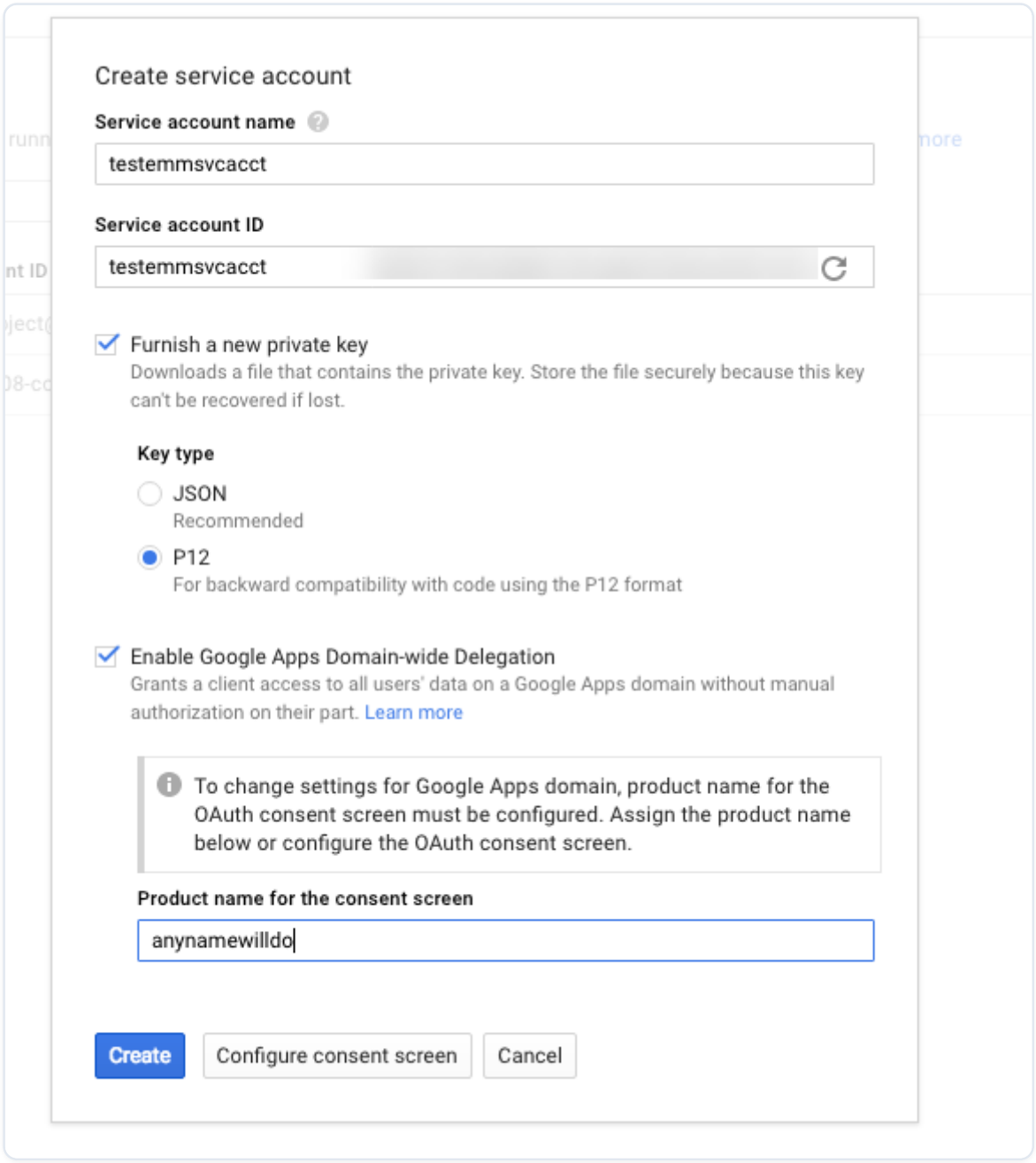
8. En la lista **Agregar credenciales a nuestro proyecto**, en el paso 1, haga clic en **cuenta de servicio**.



9. En la página **Cuentas de servicio**, haga clic en **Crear cuenta de servicio**.

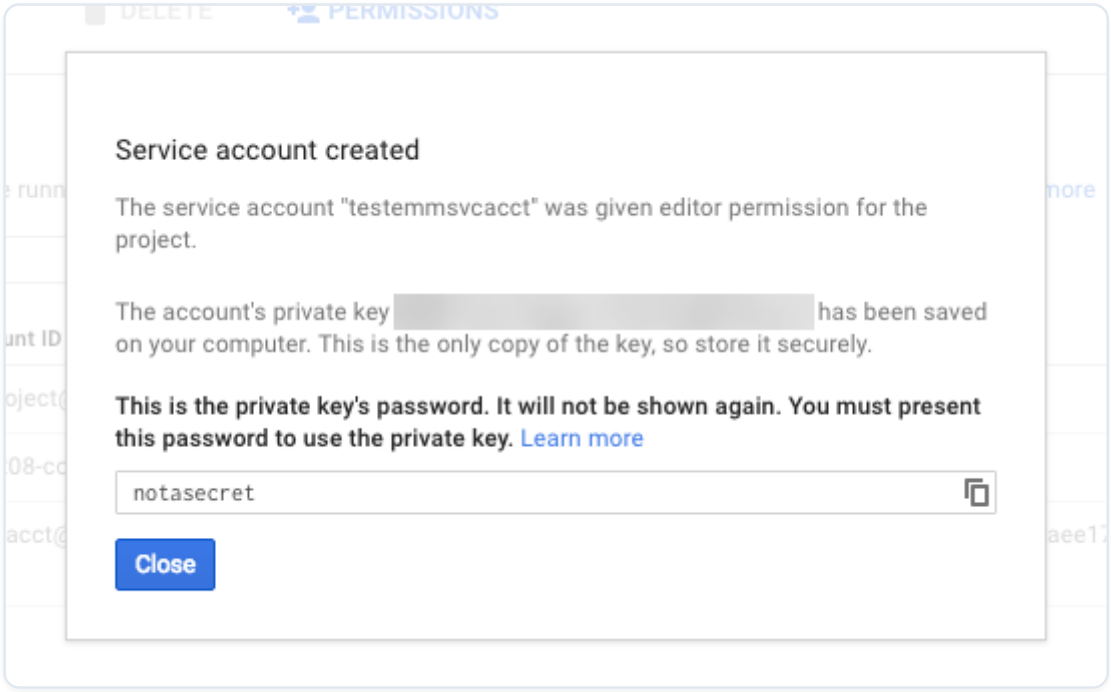


10. En **Crear cuenta de servicio**, asigne un nombre a la cuenta y seleccione la casilla de verificación **Proporcionar una nueva clave privada**. Haga clic en **P12**, seleccione la casilla de verificación **Habilitar delegación de todo el dominio de Google Apps** y, a continuación, haga clic en **Crear**.

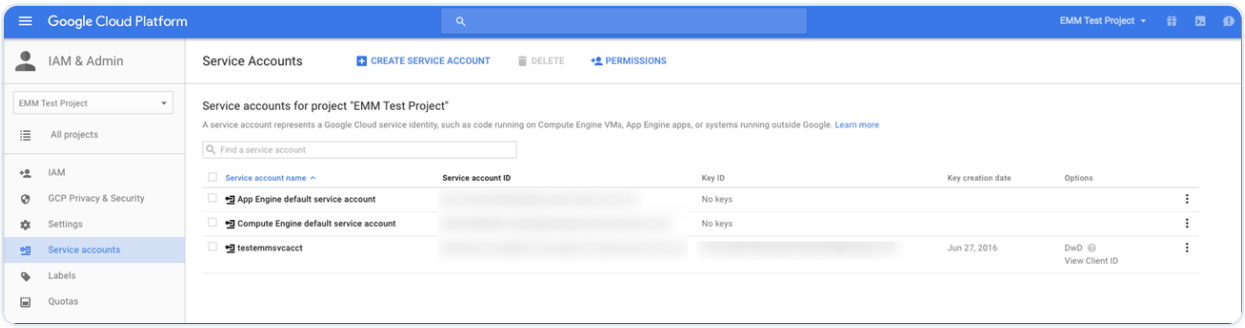


El certificado (archivo P12) se descarga en su equipo. Asegúrese de guardar el certificado en una ubicación segura.

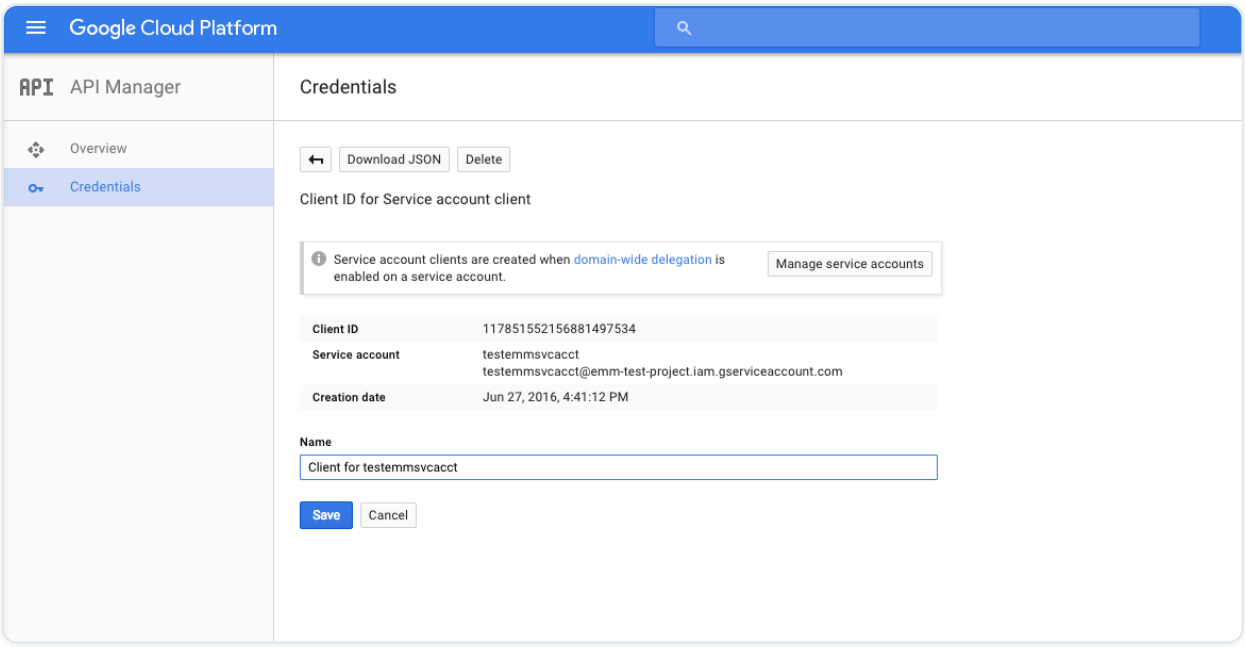
11. En la página de confirmación **Cuenta de servicio creada**, haga clic en **Cerrar**.



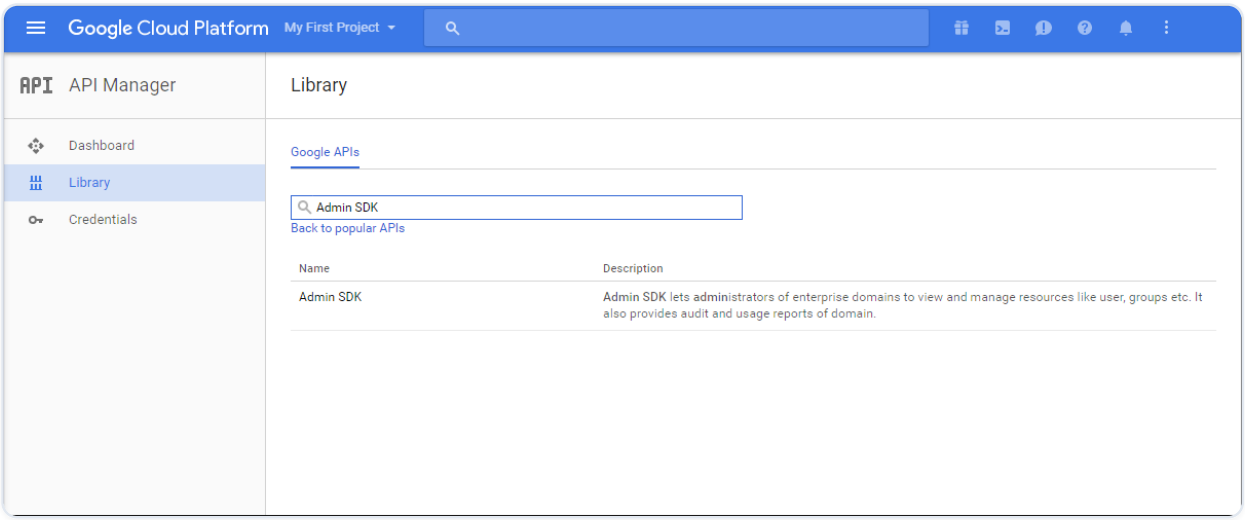
12. En **Permisos**, haga clic en **Cuentas de servicio** y, a continuación, en **Opciones** de su cuenta de servicio, haga clic en **Ver ID de cliente**.



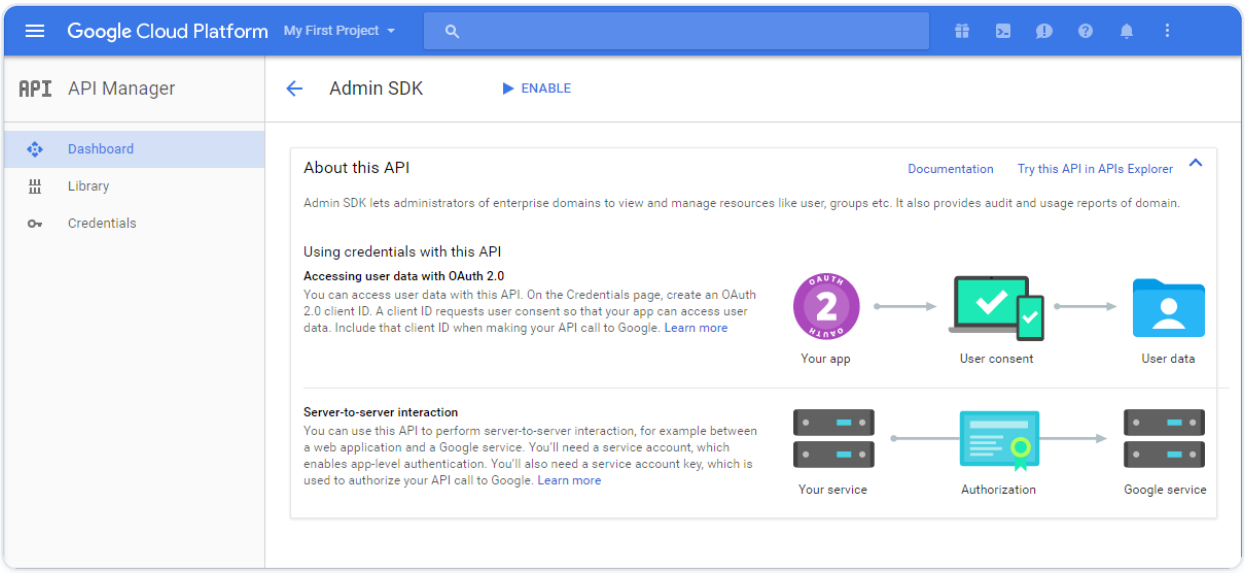
13. Se muestran los detalles necesarios para la autorización de la cuenta en la consola de administración de Google. Copie el **ID de cliente** y el **ID de cuenta de servicio** en una ubicación donde pueda recuperar la información más tarde. Necesita esta información, junto con el nombre de dominio, para enviarla al soporte de Citrix y que la añadan a una lista de permitidos.



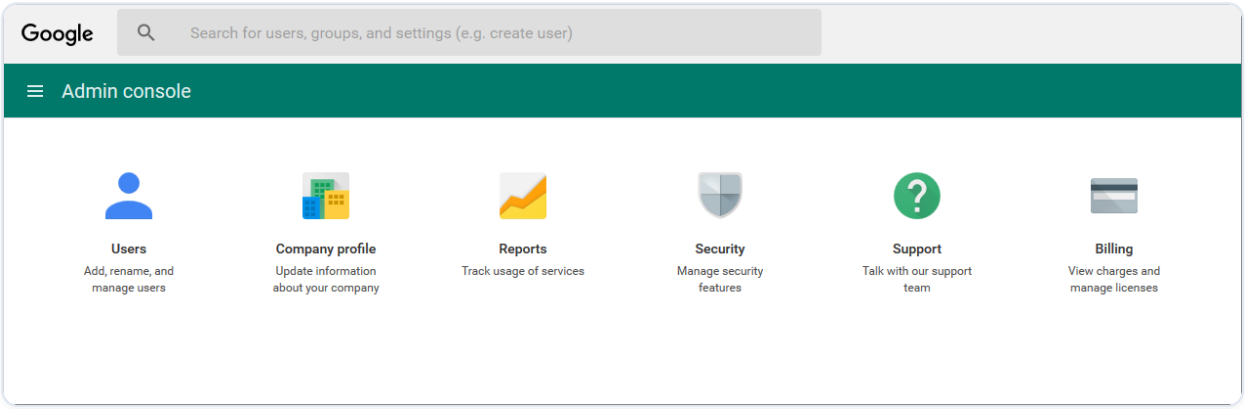
14. En la página **Biblioteca**, busque **Admin SDK** y, a continuación, haga clic en el resultado de la búsqueda.



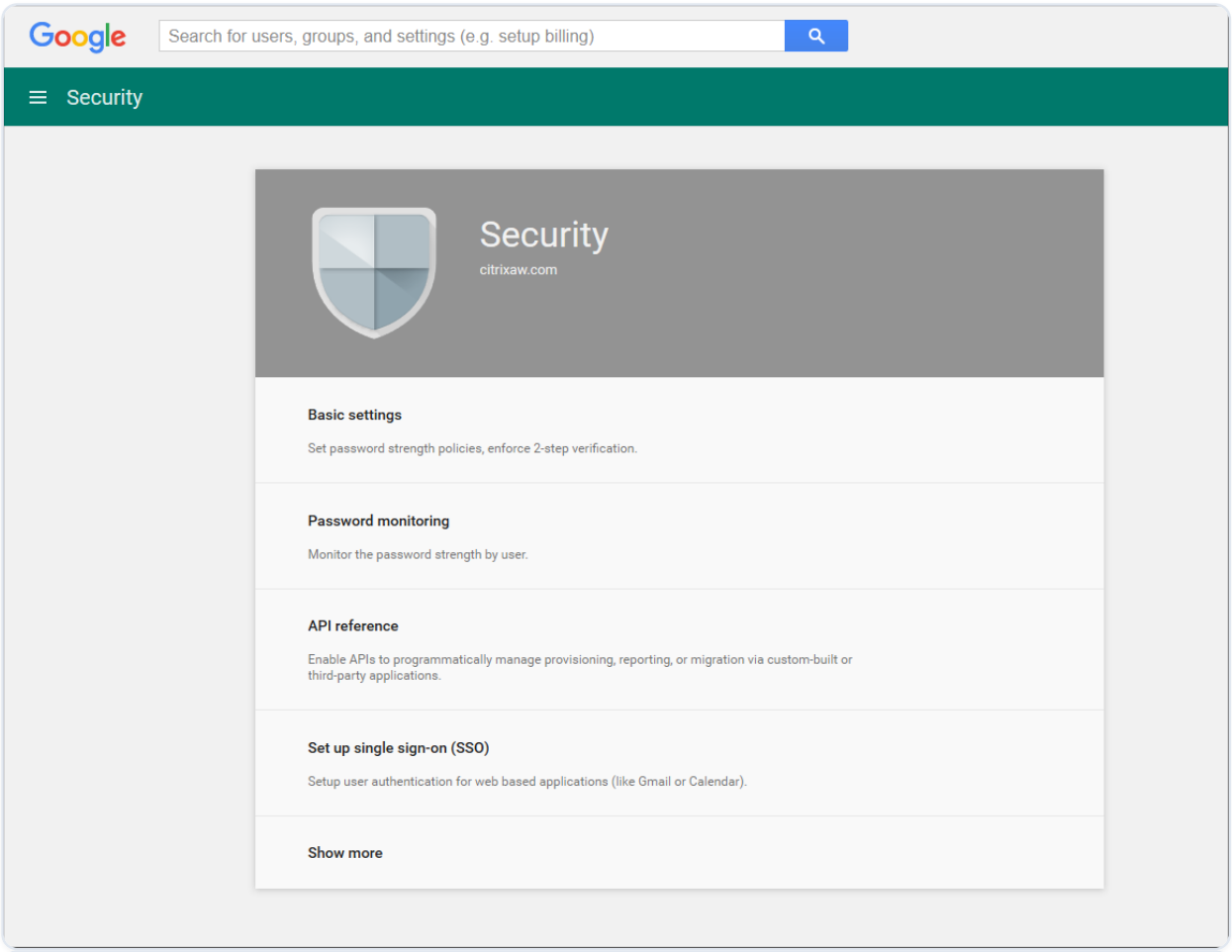
15. En la página **Información general**, haga clic en **Habilitar**.

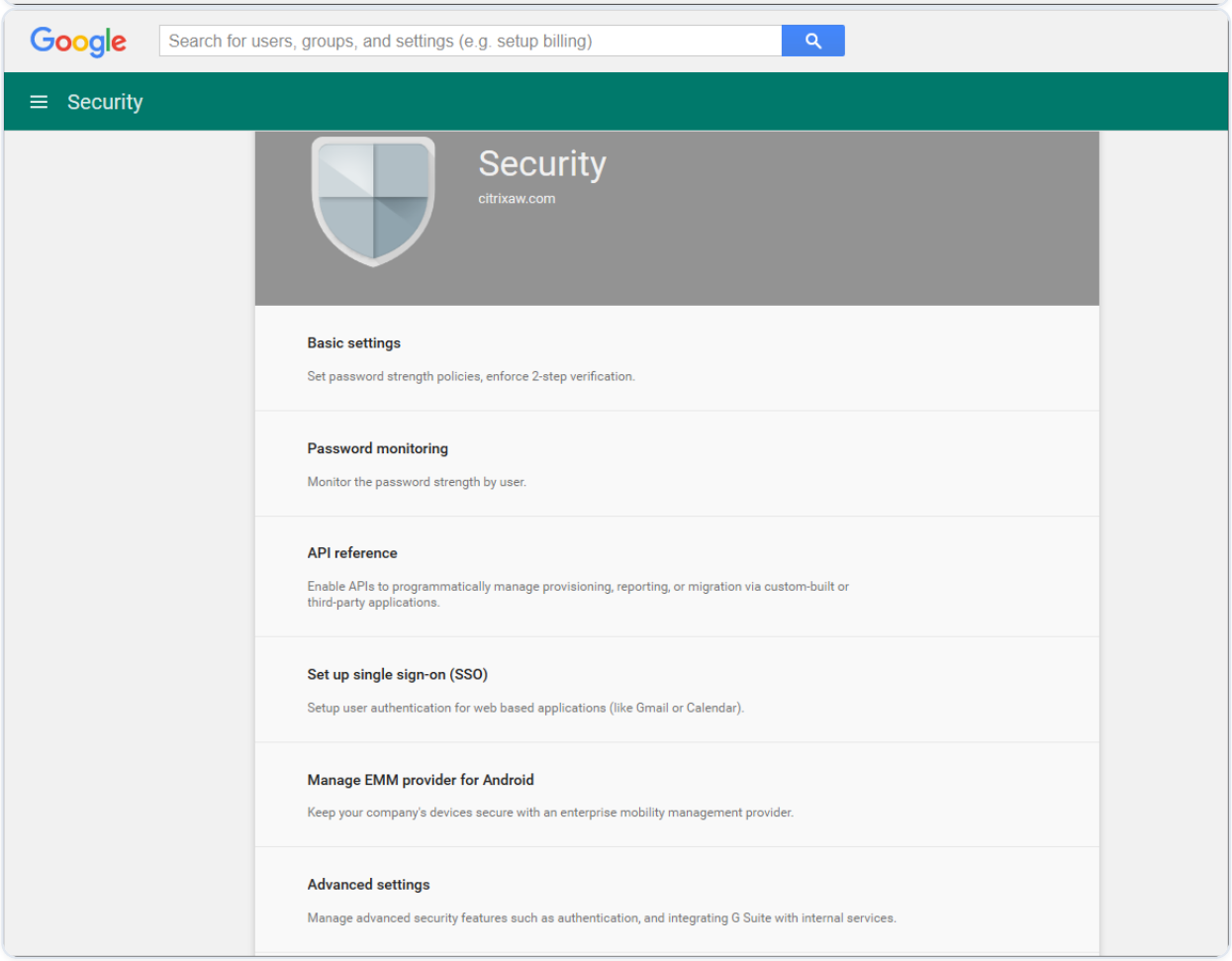


16. Abra la consola de administración de Google de su dominio y, a continuación, haga clic en **Seguridad**.

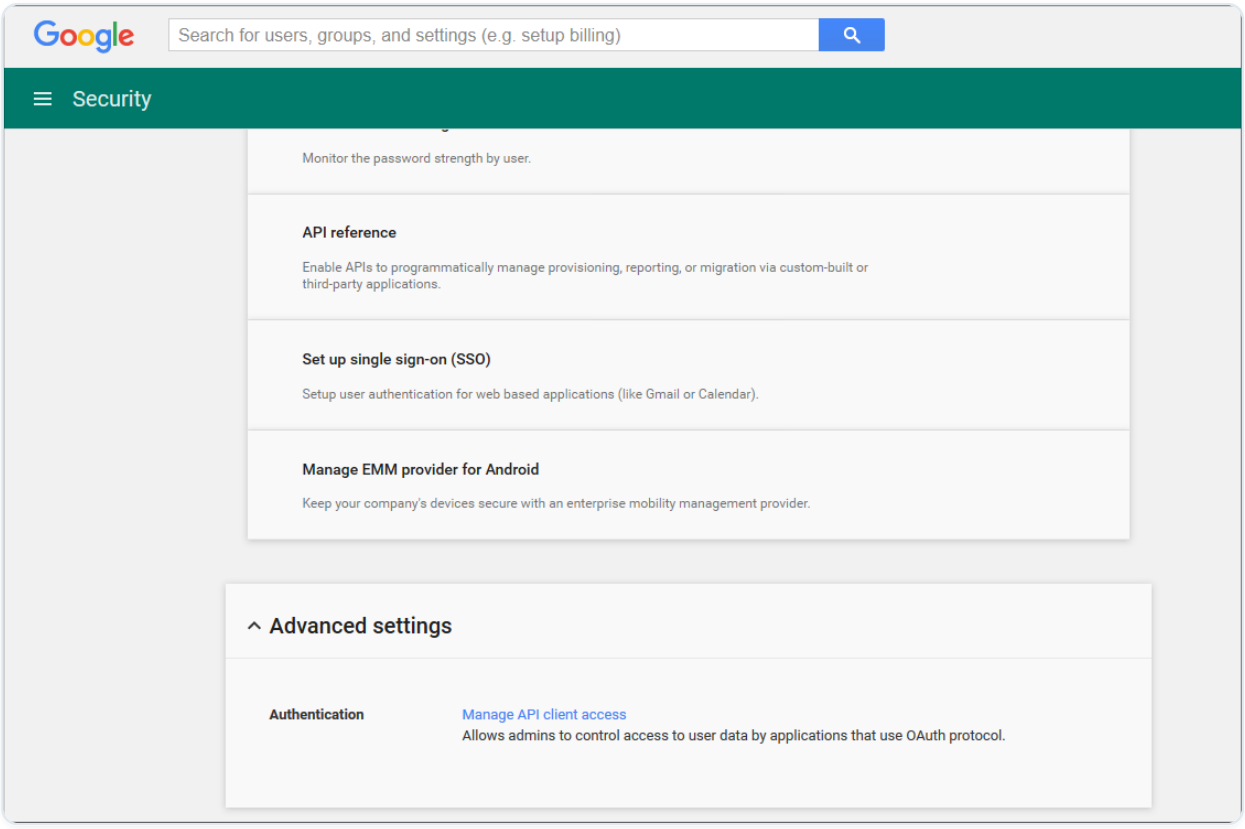


17. En la página **Settings**, haga clic en **Show more** y, a continuación, en **Advanced settings**.

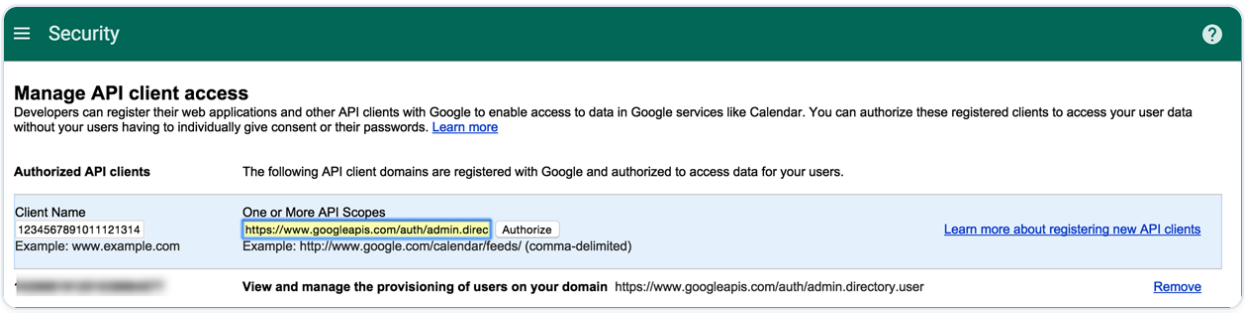

Google
Search for users, groups, and settings (e.g. setup billing)
Security
Security
citrixaw.com
Basic settings
Set password strength policies, enforce 2-step verification.
Password monitoring
Monitor the password strength by user.
API reference
Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.
Set up single sign-on (SSO)
Setup user authentication for web based applications (like Gmail or Calendar).
Show more


Google
Search for users, groups, and settings (e.g. setup billing)
Security
Security
citrixaw.com
Basic settings
Set password strength policies, enforce 2-step verification.
Password monitoring
Monitor the password strength by user.
API reference
Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.
Set up single sign-on (SSO)
Setup user authentication for web based applications (like Gmail or Calendar).
Manage EMM provider for Android
Keep your company's devices secure with an enterprise mobility management provider.
Advanced settings
Manage advanced security features such as authentication, and integrating G Suite with internal services.

18. Haga clic en **Manage API client access**.



19. En **Client Name**, escriba el ID de cliente que guardó anteriormente; en **One or More API Scopes**, escriba `https://www.googleapis.com/auth/admin.directory.user` y, a continuación, haga clic en **Authorize**.



Vinculación a EMM

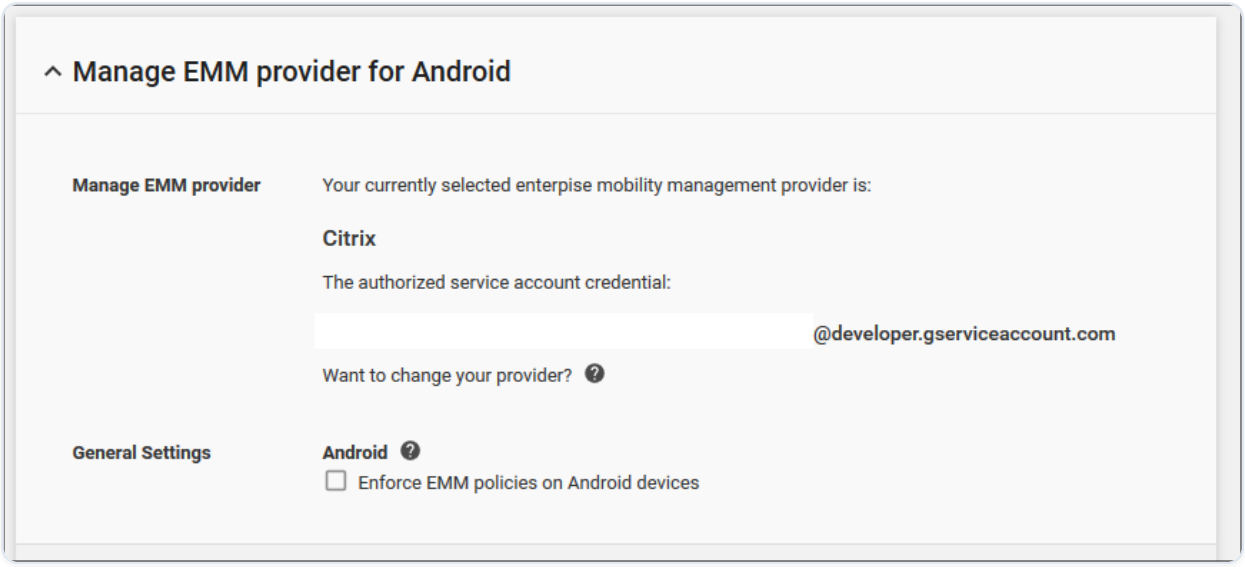
Antes de poder usar Citrix Endpoint Management para administrar sus dispositivos Android, debe ponerse en contacto con el Soporte técnico de Citrix y proporcionar su nombre de dominio, cuenta de servicio y token de vinculación. Citrix vincula el token a Citrix Endpoint Management como su proveedor de administración de movilidad empresarial (EMM). Para obtener información de contacto del Soporte técnico de Citrix, consulte Soporte técnico de Citrix.

1. Para confirmar la vinculación, inicie sesión en el portal de administración de Google y, a continuación, haga clic en **Security**.

2. Haga clic en **Manage EMM provider for Android**.

   Verá que su cuenta de Google Android Enterprise está vinculada a Citrix como su proveedor de EMM.

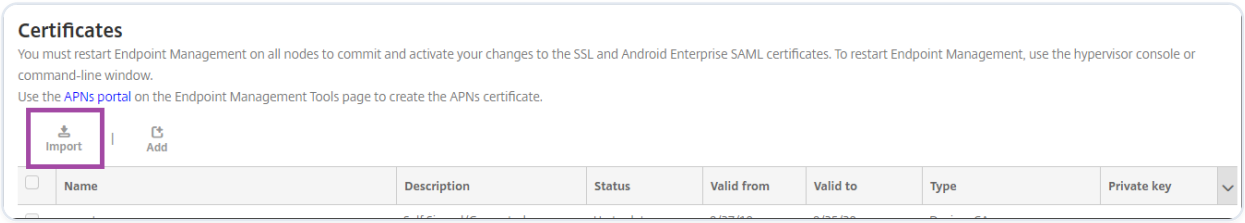
   Después de confirmar la vinculación del token, puede empezar a usar la consola de Citrix Endpoint Management para administrar sus dispositivos Android. Importe el certificado P12 que generó en el paso 14. Configure los ajustes del servidor de Android Enterprise, habilite el inicio de sesión único (SSO) basado en SAML y defina al menos una directiva de dispositivo de Android Enterprise.



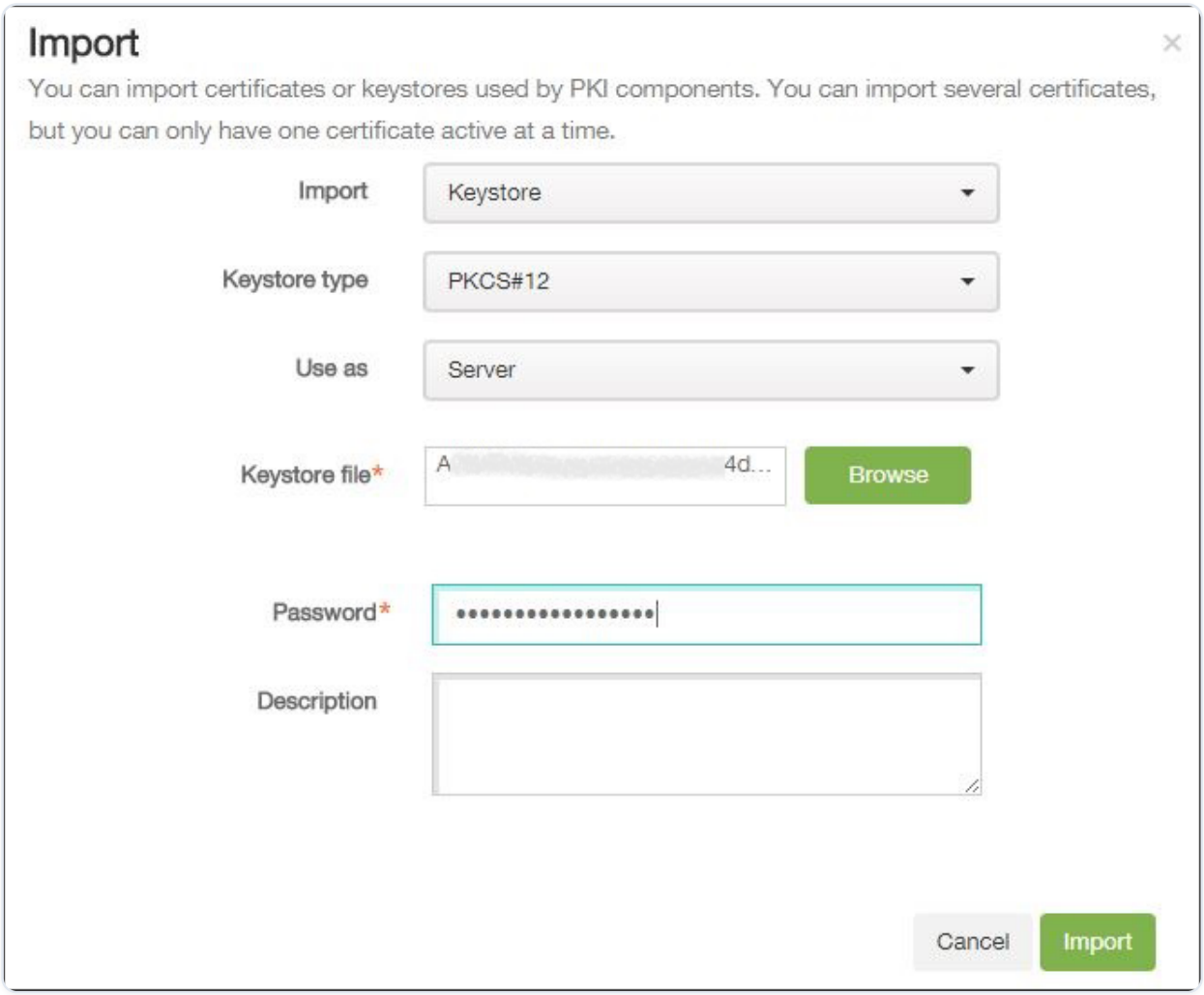
Importar el certificado P12

Siga estos pasos para importar su certificado P12 de Android Enterprise:

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha de la consola para abrir la página **Configuración** y, a continuación, haga clic en **Certificados**. Aparecerá la página **Certificados**.



2. Haga clic en **Importar**. Aparecerá el cuadro de diálogo **Importar**.



Configure los siguientes ajustes:

- **Importar:** Haga clic en **Almacén de claves** en la lista desplegable.
- **Tipo de almacén de claves:** Haga clic en **PKCS#12** en la lista desplegable.
- **Usar como:** Haga clic en **Servidor** en la lista desplegable.
- **Archivo de almacén de claves:** Haga clic en **Examinar** y vaya al certificado P12.
- **Contraseña:** Escriba la contraseña del certificado. Esta contraseña es la contraseña de la clave privada que creó al configurar su cuenta de Android Enterprise.
- **Descripción:** Opcionalmente, escriba una descripción del certificado.

3. Haga clic en **Importar**.

Configurar los ajustes del servidor de Android Enterprise

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha de la consola. Aparecerá la página **Configuración**.
2. En **Plataformas**, haga clic en **Android Enterprise**. Aparece la página **Android Enterprise**.

La página de Android Enterprise(/en-us/citrix-endpoint-management/media/android-enterprise-legacy-settings.png)

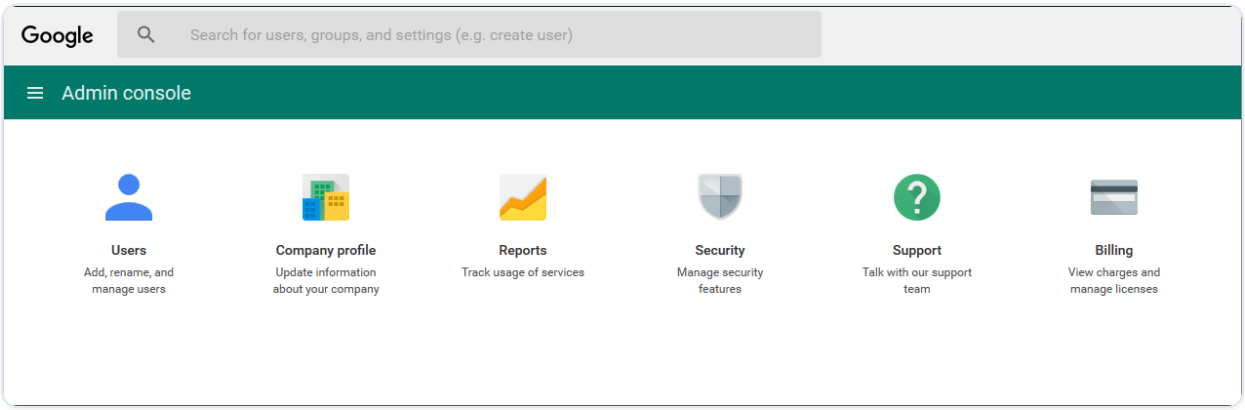
Configure los siguientes ajustes y, a continuación, haga clic en **Guardar**.

- **Nombre de dominio:** Escriba el nombre de dominio de Android Enterprise; por ejemplo, domain.com.
- **Cuenta de administrador de dominio:** Escriba el nombre de usuario del administrador de dominio; por ejemplo, la cuenta de correo electrónico utilizada para Google Developer Portal.
- **ID de cuenta de servicio:** Escriba el ID de su cuenta de servicio; por ejemplo, el correo electrónico asociado en la cuenta de servicio de Google (`serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com`).
- **ID de cliente:** Escriba el ID de cliente numérico de su cuenta de servicio de Google.
- **Habilitar Android Enterprise:** Seleccione para habilitar o inhabilitar Android Enterprise.

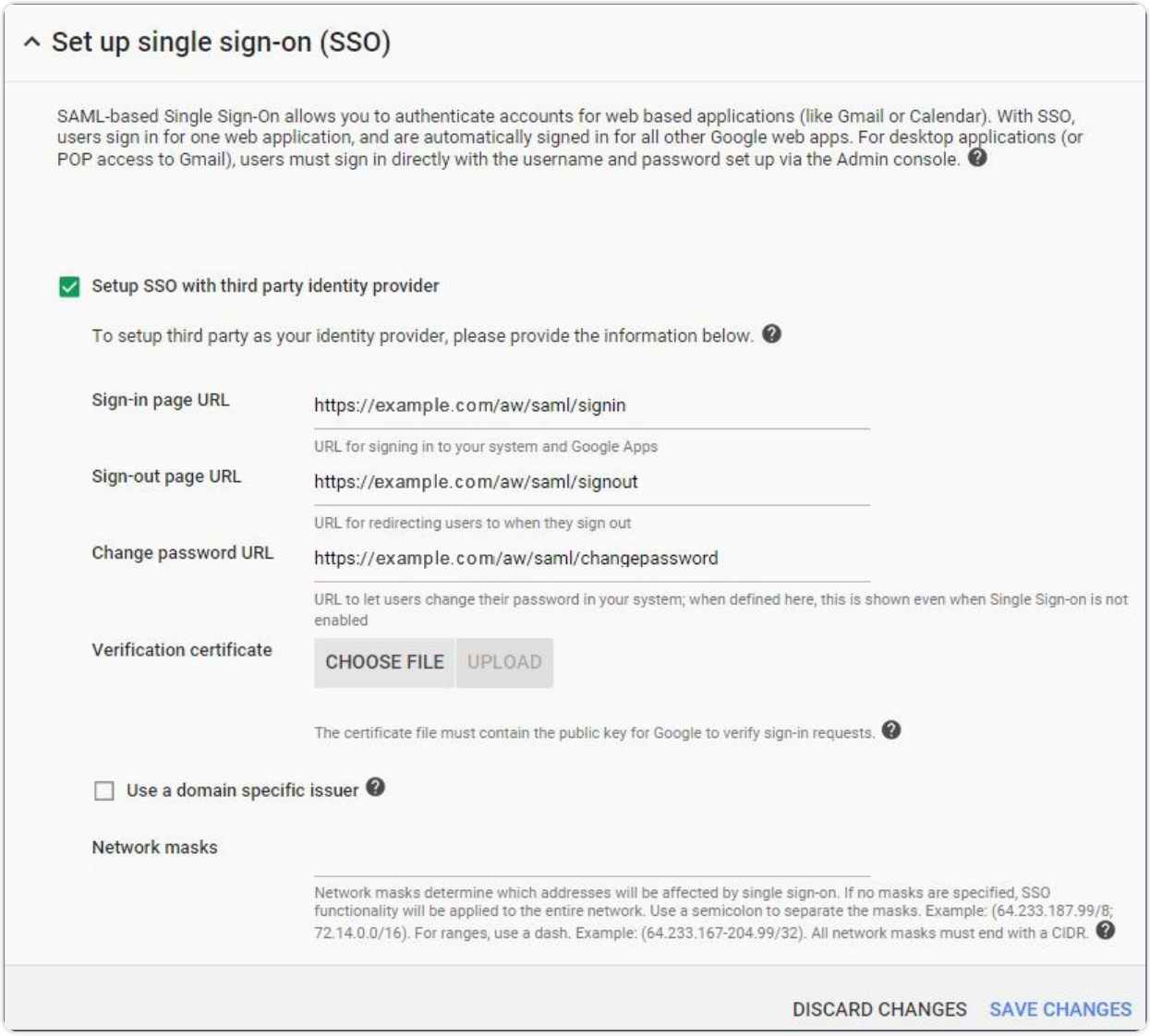
Habilitar el inicio de sesión único basado en SAML

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje de la esquina superior derecha. Aparece la página **Configuración**.
2. Haga clic en **Certificados**. Aparece la página **Certificados**.

   La página de Certificados(/en-us/citrix-endpoint-management/media/android-enterprise-certs-export.png)
3. En la lista de certificados, haga clic en el certificado SAML.
4. Haga clic en **Exportar** y guarde el certificado en su equipo.
5. Inicie sesión en el portal de administración de Google con sus credenciales de administrador de Android Enterprise. Para acceder al portal, consulte el portal de administración de Google.
6. Haga clic en **Seguridad**.



7. En **Seguridad**, haga clic en **Configurar inicio de sesión único (SSO)** y, a continuación, configure los siguientes ajustes.

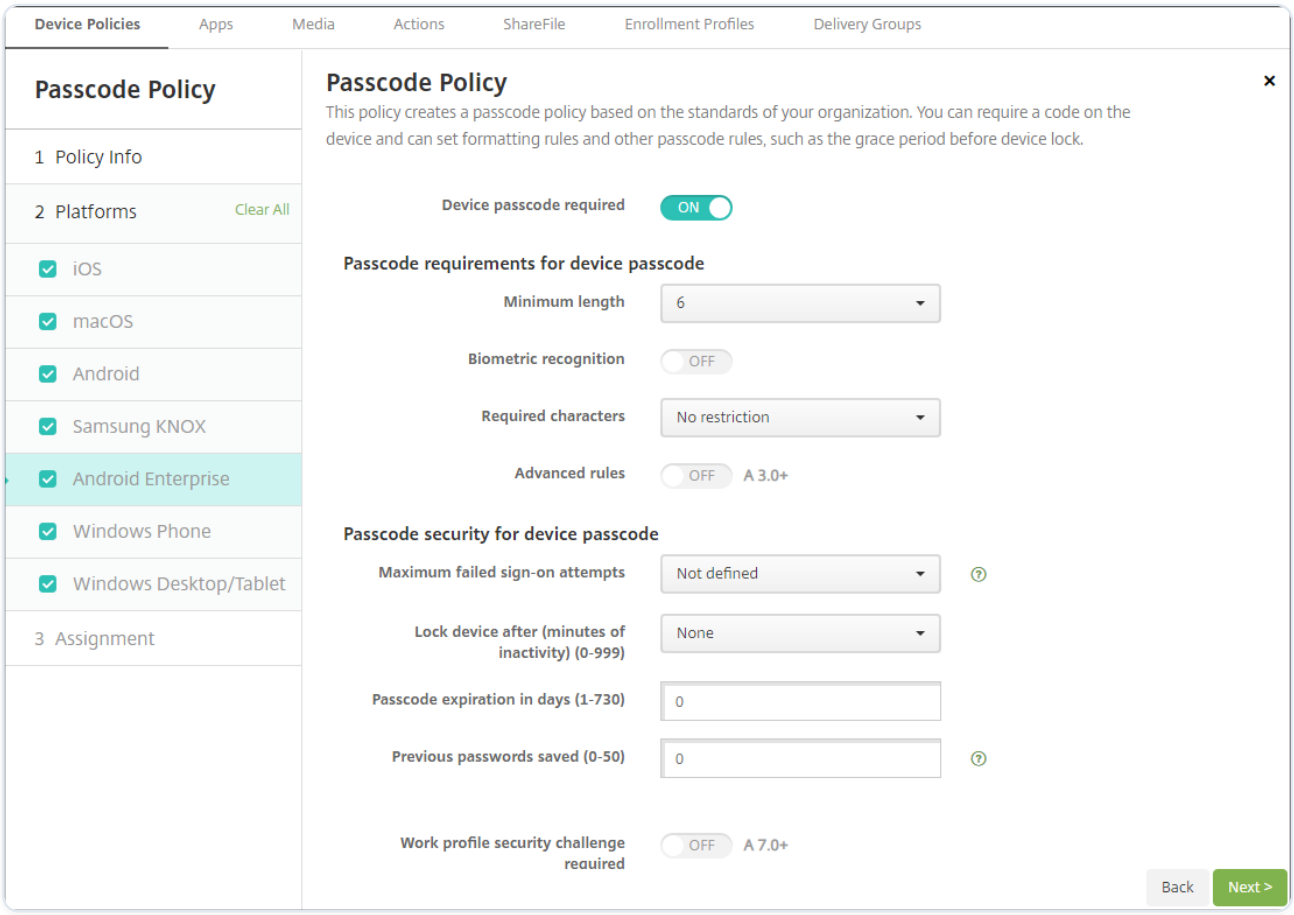


- **URL de la página de inicio de sesión:** Escriba la URL para los usuarios que inician sesión en su sistema y en Google Apps. Por ejemplo: `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **URL de la página de cierre de sesión:** Escriba la URL a la que se redirige a los usuarios cuando cierran sesión. Por ejemplo: `https://<Xenmobile-FQDN>/aw/saml/signout`.
- **URL para cambiar la contraseña:** Escriba la URL para permitir que los usuarios cambien su contraseña en su sistema. Por ejemplo: `https://<Xenmobile-FQDN>/aw/saml/changepassword`. Si este campo está definido, los usuarios verán esta solicitud incluso cuando el SSO no esté disponible.
- **Certificado de verificación:** Haga clic en **ELEGIR ARCHIVO** y, a continuación, vaya al certificado SAML exportado desde Citrix Endpoint Management.

8. Haga clic en **GUARDAR CAMBIOS**.

Configurar una directiva de dispositivo de Android Enterprise

Configure una directiva de código de acceso para que los usuarios deban establecer un código de acceso en sus dispositivos la primera vez que se inscriban.



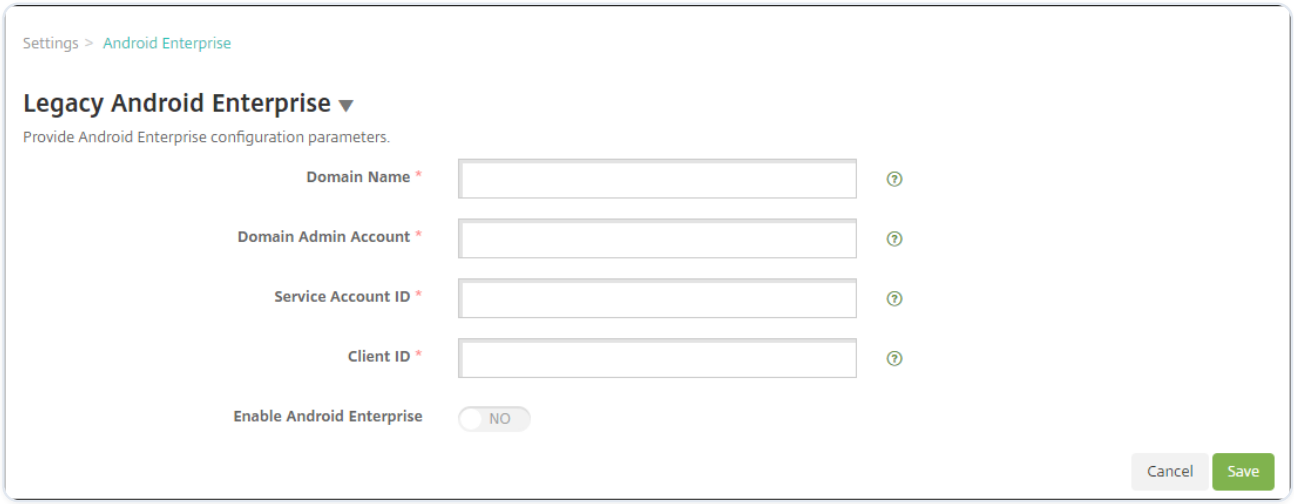
Los pasos básicos para configurar cualquier directiva de dispositivo son los siguientes.

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar** y, a continuación, haga clic en **Directivas de dispositivo**.
2. Haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar nueva directiva**, seleccione la directiva que desea agregar. En este ejemplo, haga clic en **Contraseña**.
4. Complete la página **Información de la directiva**.
5. Haga clic en **Android Enterprise** y, a continuación, configure los ajustes de la directiva.
6. Asigne la directiva a un grupo de entrega.

Configurar los ajustes de la cuenta de Android Enterprise

Antes de poder empezar a administrar aplicaciones y directivas de Android en los dispositivos, debe configurar un dominio de Android Enterprise y la información de la cuenta en Citrix Endpoint Management. Primero, complete las tareas de configuración de Android Enterprise en Google para configurar un administrador de dominio y obtener un ID de cuenta de servicio y un token de enlace.

1. En la consola web de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha. Se muestra la página **Configuración**.
2. En **Plataformas**, haga clic en **Android Enterprise**. Aparece la página de configuración de **Android Enterprise**.



1. En la página de **Android Enterprise**, configure los siguientes ajustes:
   - **Nombre de dominio:** Escriba su nombre de dominio.
   - **Cuenta de administrador de dominio:** Escriba su nombre de usuario de administrador de dominio.
   - **ID de cuenta de servicio:** Escriba su ID de cuenta de servicio de Google.
   - **ID de cliente:** Escriba el ID de cliente de su cuenta de servicio de Google.
   - **Habilitar Android Enterprise:** Seleccione si desea habilitar Android Enterprise o no.
2. Haga clic en **Guardar**.

Configurar el acceso de socio de Google Workspace para Citrix Endpoint Management

Algunas características de Citrix Endpoint Management para Chrome usan las API de socio de Google para comunicarse entre Citrix Endpoint Management y su dominio de Google Workspace.

Por ejemplo, Citrix Endpoint Management requiere las API para las directivas de dispositivo que administran características de Chrome, como el modo Incógnito y el modo Invitado.

Para habilitar las API de socio, configure su dominio de Google Workspace en la consola de Citrix Endpoint Management y, a continuación, configure su cuenta de Google Workspace.

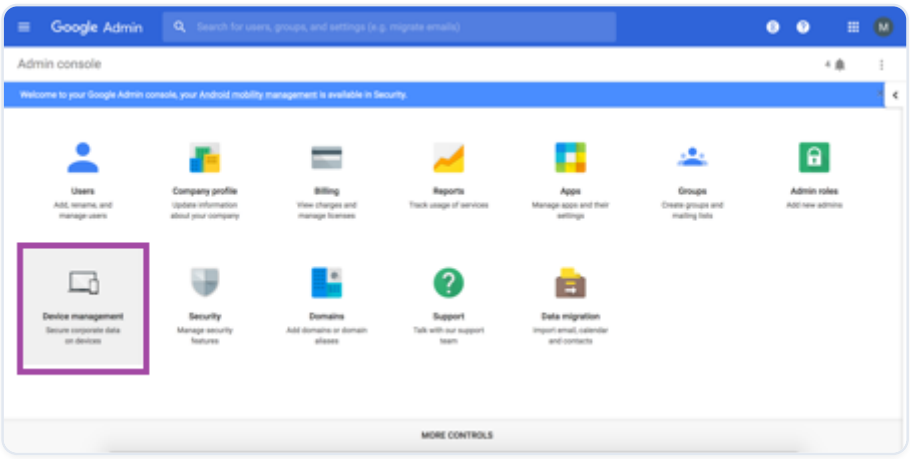
Configurar su dominio de Google Workspace en Citrix Endpoint Management

Para permitir que Citrix Endpoint Management se comunique con las API de su dominio de Google Workspace, vaya a **Parámetros > Configuración de Google Chrome** y configure los ajustes.

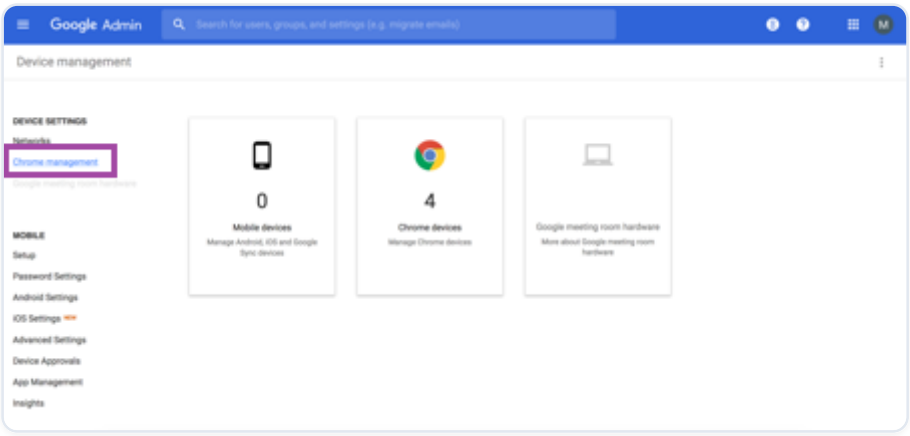
- **Dominio de Google Workspace:** El dominio de Google Workspace que aloja las API necesarias para Citrix Endpoint Management.
- **Cuenta de administrador de Google Workspace:** La cuenta de administrador de su dominio de Google Workspace.
- **ID de cliente de Google Workspace:** El ID de cliente de Citrix. Utilice este valor para configurar el acceso de socio para su dominio de Google Workspace.
- **ID de empresa de Google Workspace:** El ID de empresa de su cuenta, rellenado desde su cuenta de empresa de Google.

Habilitar el acceso de socio para dispositivos y usuarios en su dominio de Google Workspace

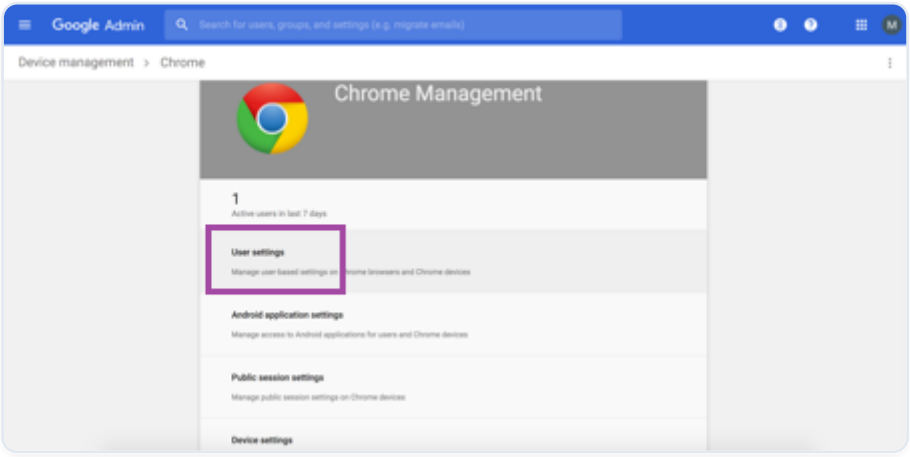
1. Inicie sesión en la consola de administración de Google: `<https://admin.google.com>`
2. Haga clic en **Administración de dispositivos**.



3. Haga clic en **Administración de Chrome**.



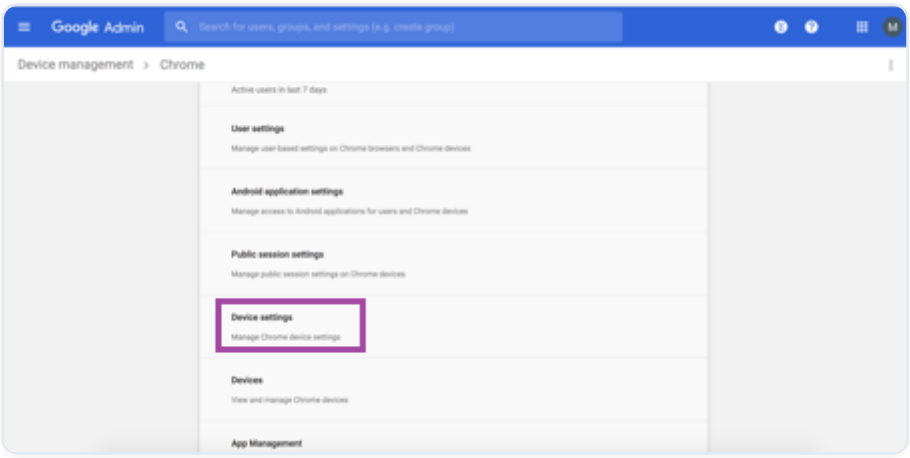
4. Haga clic en **Configuración de usuario**.



5. Busque **Administración de Chrome - Acceso de socios**.



6. Seleccione la casilla de verificación **Habilitar Administración de Chrome - Acceso de socios**.
7. Confirme que comprende y desea habilitar el acceso de socios. Haga clic en **Guardar**.
8. En la página de administración de Chrome, haga clic en **Configuración de dispositivos**.



9. Busque **Administración de Chrome - Acceso de socios**.



10. Seleccione la casilla de verificación **Habilitar Administración de Chrome - Acceso de socios**.
11. Confirme que comprende y desea habilitar el acceso de socios. Haga clic en **Guardar**.
12. Vaya a la página de **Seguridad** y, a continuación, haga clic en **Configuración avanzada**.



13. Haga clic en **Administrar acceso de cliente de API**.
14. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Configuración de Google Chrome** y copie el valor de ID de cliente de G Suite. A continuación, vuelva a la

página **Administrar acceso de cliente de API** y pegue el valor copiado en el campo **Nombre de cliente**.

15. En **Uno o más ámbitos de API**, agregue la URL: `https://www.googleapis.com/auth/chromedevicemanagementapi`



16. Haga clic en **Autorizar**.

    Aparece el mensaje "Se han guardado sus parámetros".

Inscribir dispositivos Android Enterprise

Si el proceso de inscripción de dispositivos requiere que los usuarios introduzcan un nombre de usuario o un ID de usuario, el formato aceptado dependerá de cómo esté configurado el servidor de Citrix Endpoint Management para buscar usuarios por nombre principal de usuario (UPN) o nombre de cuenta SAM.

Si el servidor de Citrix Endpoint Management está configurado para buscar usuarios por UPN, los usuarios deben introducir un UPN con el formato:

- *nombredeusuario@dominio*

Si el servidor de Citrix Endpoint Management está configurado para buscar usuarios por SAM, los usuarios deben introducir un SAM en uno de estos formatos:

- *nombredeusuario@dominio*
- *dominio\nombredeusuario*

Para determinar el tipo de nombre de usuario para el que está configurado el servidor de Citrix Endpoint Management:

1. En la consola del servidor de Citrix Endpoint Management, haga clic en el icono de engranaje de la esquina superior derecha. Aparecerá la página **Parámetros**.
2. Haga clic en **LDAP** para ver la configuración de la conexión LDAP.
3. Cerca de la parte inferior de la página, consulte el campo **Búsqueda de usuario por**:

- Si está establecido en **userPrincipalName**, el servidor de Citrix Endpoint Management está configurado para UPN.
- Si está establecido en **sAMAccountName**, el servidor de Citrix Endpoint Management está configurado para SAM.

Anular la inscripción de una empresa de Android Enterprise

Puede anular la inscripción de una empresa de Android Enterprise mediante la consola del servidor de Citrix Endpoint Management y las herramientas de Citrix Endpoint Management.

Al realizar esta tarea, el servidor de Citrix Endpoint Management abre una ventana emergente para las herramientas de Citrix Endpoint Management. Antes de empezar, asegúrese de que el servidor de Citrix Endpoint Management tenga permiso para abrir ventanas emergentes en el explorador que está utilizando. Algunos exploradores, como Google Chrome, requieren que inhabilite el bloqueo de elementos emergentes y que agregue la dirección del sitio de Citrix Endpoint Management a la lista de permitidos de elementos emergentes.

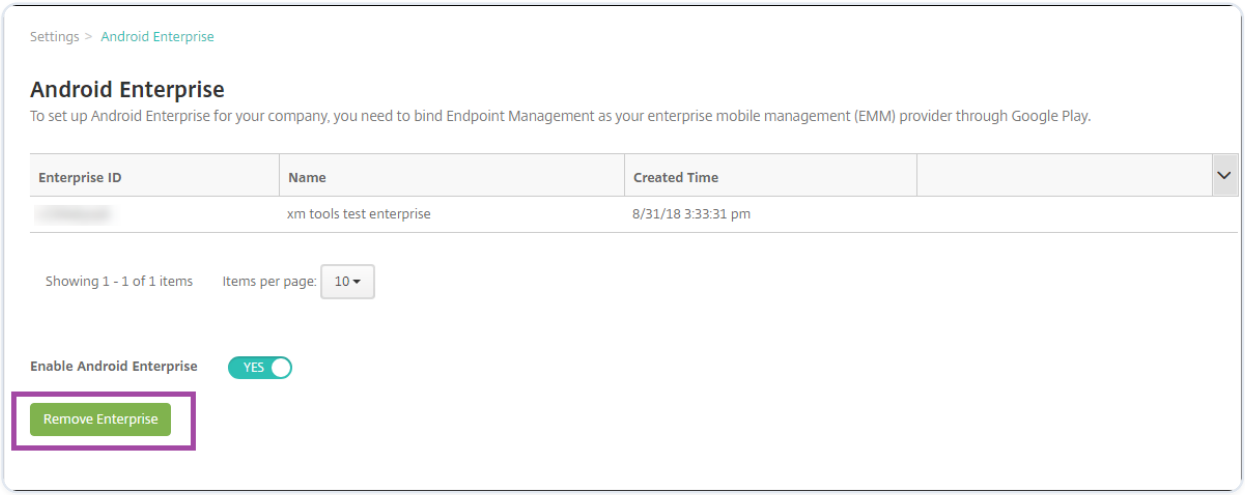
> **Advertencia:**
>
> Una vez que se anula la inscripción de una empresa, las aplicaciones de Android Enterprise en los dispositivos ya inscritos a través de ella se restablecen a sus estados predeterminados. Google ya no administra los dispositivos. Volver a inscribirlos en una empresa de Android Enterprise podría no restaurar la funcionalidad anterior sin una configuración adicional.

> Una vez que se anula la inscripción de la empresa de Android Enterprise:

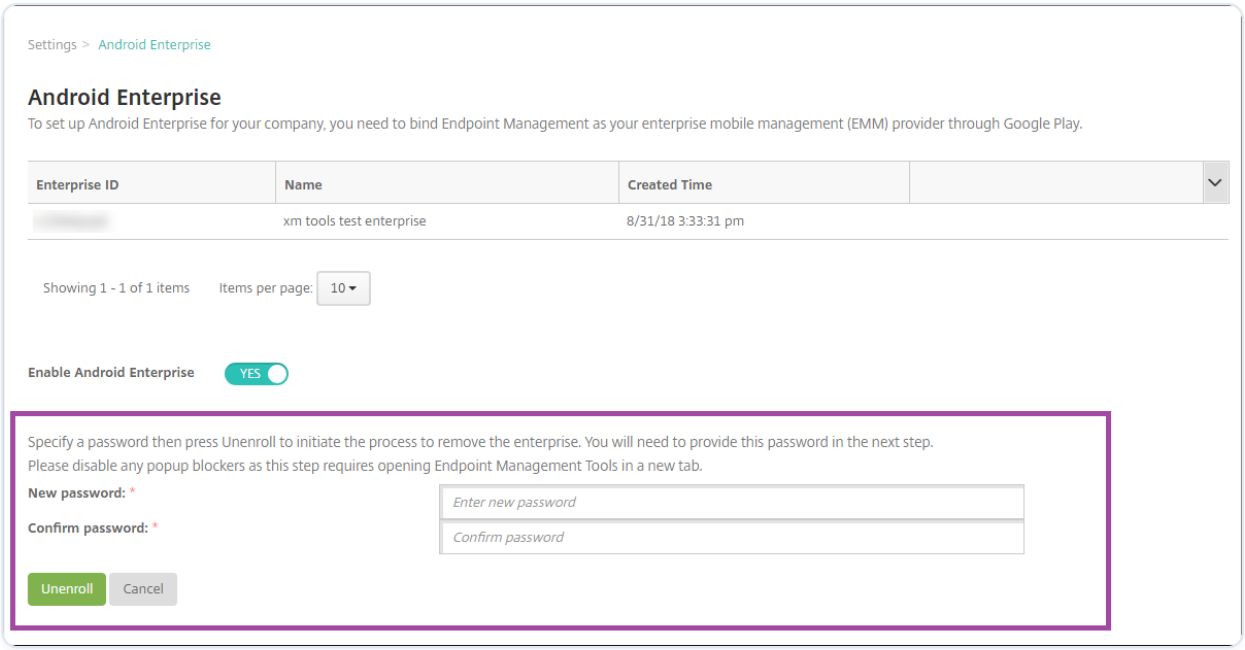
- Los dispositivos y usuarios inscritos a través de la empresa tienen las aplicaciones de Android Enterprise restablecidas a su estado predeterminado. Los permisos de aplicaciones y las directivas de configuraciones administradas aplicadas anteriormente ya no tienen efecto.
- Los dispositivos inscritos a través de la empresa son administrados por Citrix Endpoint Management, pero no son administrados desde la perspectiva de Google. No se pueden agregar nuevas aplicaciones de Android Enterprise. No se pueden aplicar permisos de aplicaciones ni directivas de configuraciones administradas. Otras directivas, como Programación, Contraseña y Restricciones, aún se pueden aplicar a estos dispositivos.
- Si intenta inscribir dispositivos en Android Enterprise, se inscribirán como dispositivos Android, no como dispositivos Android Enterprise.

Para anular la inscripción de una empresa de Android Enterprise:

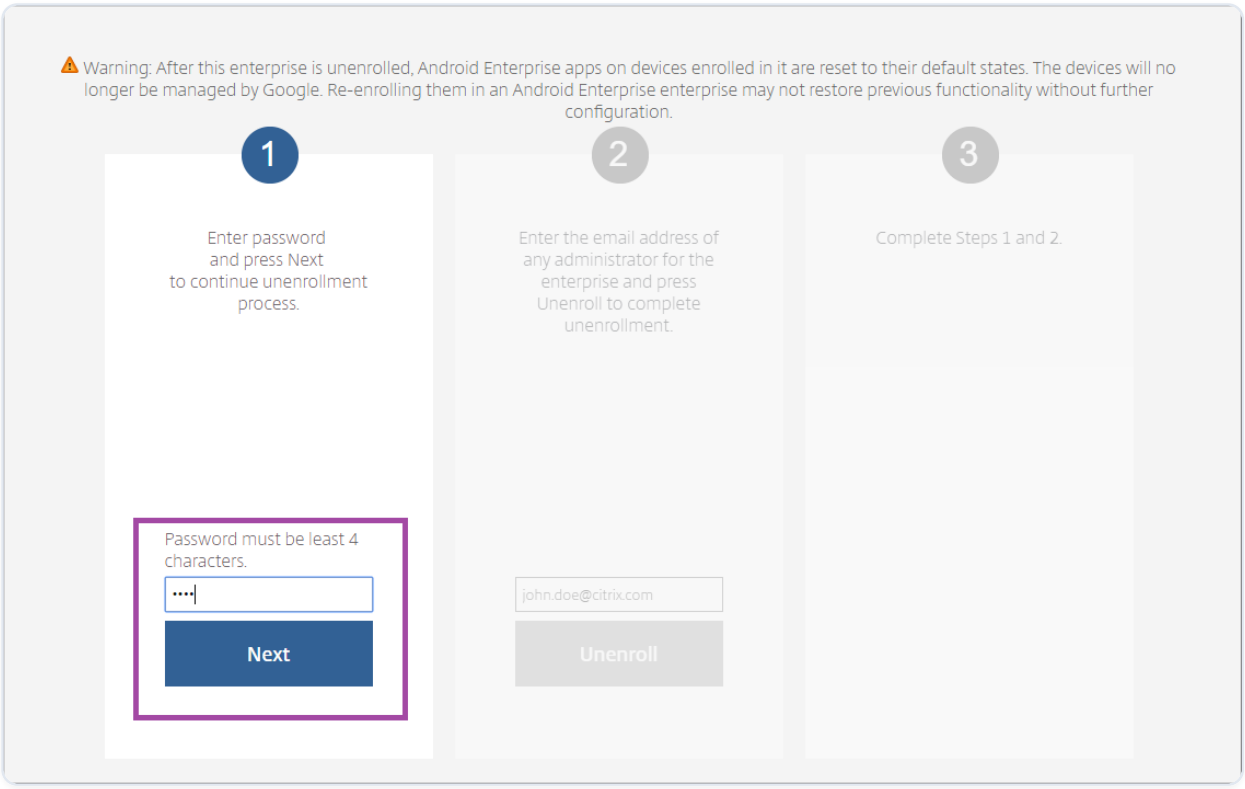
1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje de la esquina superior derecha. Aparecerá la página Configuración.
2. En la página Configuración, haga clic en **Android Enterprise**.
3. Haga clic en **Quitar empresa**.



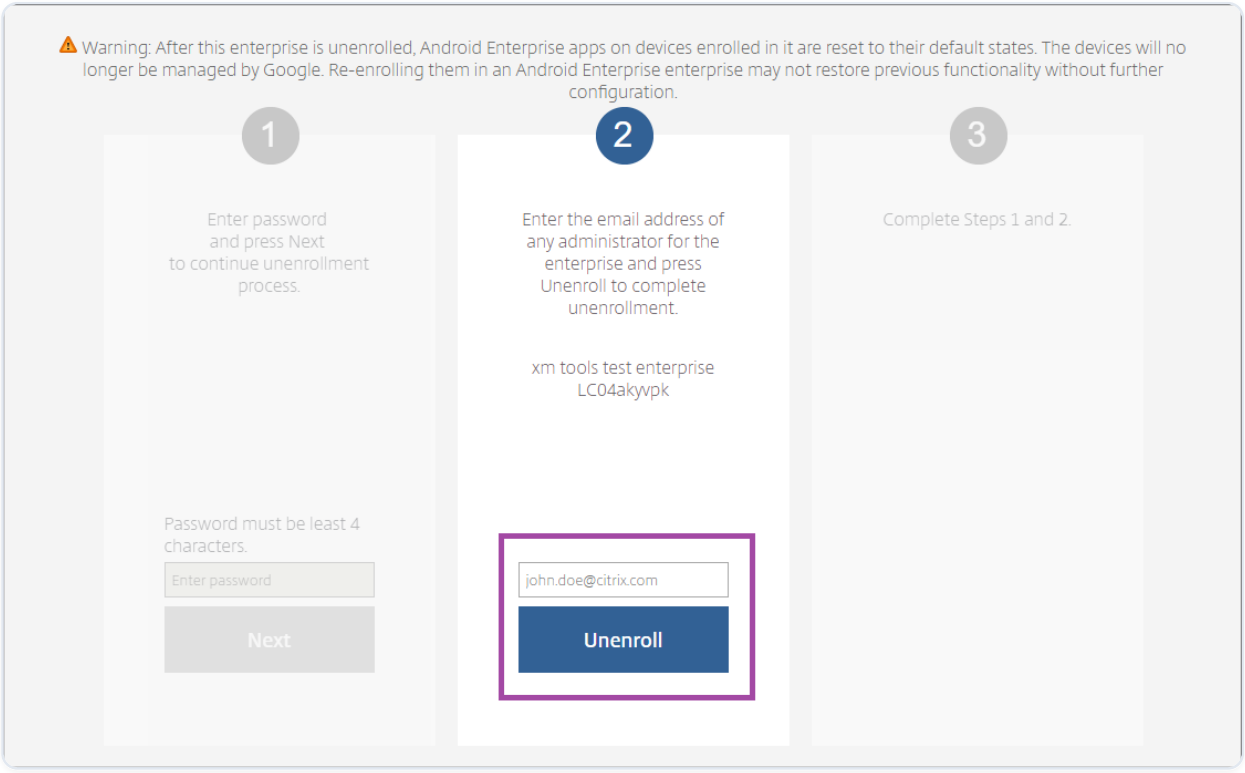
4. Especifique una contraseña. La necesitará para el siguiente paso para completar la anulación de la inscripción. A continuación, haga clic en **Anular inscripción**.



5. Cuando se abra la página Citrix Endpoint Management Tools, introduzca la contraseña que creó en el paso anterior.



6. Haga clic en **Anular inscripción**.



Aprovisionamiento de dispositivos totalmente administrados en Android Enterprise

Solo los dispositivos propiedad de la empresa pueden ser dispositivos totalmente administrados en Android Enterprise. En los dispositivos totalmente administrados, la empresa u organización

controla todo el dispositivo, no solo el perfil de trabajo. Los dispositivos totalmente administrados también se conocen como dispositivos administrados por el trabajo.

Citrix Endpoint Management admite estos métodos de inscripción para dispositivos totalmente administrados:

- **afw#xenmobile:** Con este método de inscripción, el usuario introduce los caracteres `afw#xenmobile` al configurar el dispositivo. Este token identifica el dispositivo como administrado por Citrix Endpoint Management y descarga Citrix Secure Hub.
- **Código QR:** El aprovisionamiento con código QR es una forma sencilla de aprovisionar una flota distribuida de dispositivos que no admiten NFC, como las tabletas. El método de inscripción con código QR se puede utilizar en dispositivos de flota que se hayan restablecido a su configuración de fábrica. El método de inscripción con código QR configura y establece dispositivos totalmente administrados escaneando un código QR desde el asistente de configuración.
- **Toque NFC (comunicación de campo cercano):** El método de inscripción con toque NFC se puede utilizar en dispositivos de flota que se hayan restablecido a su configuración de fábrica. Un toque NFC transfiere datos entre dos dispositivos mediante comunicación de campo cercano. Bluetooth, Wi-Fi y otros modos de comunicación están deshabilitados en un dispositivo restablecido de fábrica. NFC es el único protocolo de comunicación que el dispositivo puede utilizar en este estado.

`afw#xenmobile`

El método de inscripción se utiliza después de encender un dispositivo nuevo o restablecido de fábrica para la configuración inicial. Los usuarios introducen `afw#xenmobile` cuando se les pide que introduzcan una cuenta de Google. Esta acción descarga e instala Citrix Secure Hub. A continuación, los usuarios siguen las indicaciones de configuración de Citrix Secure Hub para completar la inscripción.

Este método de inscripción se recomienda para la mayoría de los clientes porque la última versión de Citrix Secure Hub se descarga de Google Play Store. A diferencia de otros métodos de inscripción, no es necesario proporcionar Citrix Secure Hub para su descarga desde el servidor de Citrix Endpoint Management.

Requisitos previos:

- Compatible con todos los dispositivos Android que ejecuten el sistema operativo Android.

Código QR

Para inscribir un dispositivo en modo dispositivo mediante un código QR, debe generar un código QR creando un JSON y convirtiéndolo en un código QR. Las cámaras de los dispositivos escanean el código QR para inscribir el dispositivo.

Requisitos previos:

- Compatible con todos los dispositivos Android que ejecuten Android 7.0 y versiones posteriores.

CREAR UN CÓDIGO QR A PARTIR DE UN JSON

Cree un JSON con los siguientes campos.

Estos campos son obligatorios:

Clave: android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME

Valor: com.zenprise/com.zenprise.configuration.AdminFunction

Clave: android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM

Valor: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

Clave: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

Valor: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`

Estos campos son opcionales:

- **android.app.extra.PROVISIONING_LOCALE:** Introduzca los códigos de idioma y país.

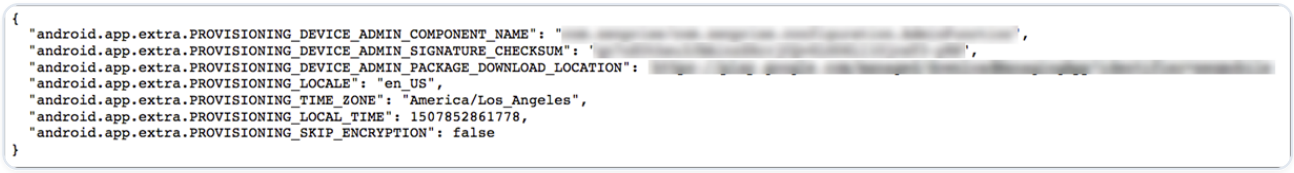
  Los códigos de idioma son códigos de idioma ISO de dos letras en minúscula (como en) tal como los define ISO 639-1. Los códigos de país son códigos de país ISO de dos letras en mayúscula (como US) tal como los define ISO 3166-1. Por ejemplo, introduzca en_US para el inglés hablado en Estados Unidos.
- **android.app.extra.PROVISIONING_TIME_ZONE:** La zona horaria en la que se ejecuta el dispositivo.

  Escriba el nombre de la base de datos del área/ubicación. Por ejemplo, escriba **America/Los_Angeles** para la hora del Pacífico. Si no escribe un nombre, la zona horaria se rellena automáticamente.
- **android.app.extra.PROVISIONING_LOCAL_TIME:** Hora en milisegundos desde la Época.

La época Unix (o tiempo Unix, tiempo POSIX o marca de tiempo Unix) es el número de segundos que han transcurrido desde January 1, 1970 (medianoche UTC/GMT). La hora no incluye segundos intercalares (en ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** Establezca en **true** para omitir el cifrado durante la creación del perfil. Establezca en **false** para forzar el cifrado durante la creación del perfil.

Un JSON típico tiene el siguiente aspecto:



Valide el JSON creado utilizando cualquier herramienta de validación de JSON, como https://jsonlint.com. Convierta esa cadena JSON en un código QR utilizando cualquier generador de códigos QR en línea.

Este código QR es escaneado por un dispositivo restablecido de fábrica para inscribir el dispositivo como un dispositivo totalmente administrado.

Para inscribir el dispositivo

Para inscribir un dispositivo como dispositivo totalmente administrado, el dispositivo debe estar en estado de restablecimiento de fábrica.

1. Toque la pantalla seis veces en la pantalla de bienvenida para iniciar el flujo de inscripción con código QR.
2. Cuando se le solicite, conéctese a la red Wi-Fi. La ubicación de descarga de Citrix Secure Hub en el código QR (codificada en el JSON) es accesible a través de esta red Wi-Fi.

   Una vez que el dispositivo se conecta correctamente a la red Wi-Fi, descarga un lector de códigos QR de Google e inicia la cámara.
3. Apunte la cámara al código QR para escanearlo.

   Android descarga Citrix Secure Hub desde la ubicación de descarga en el código QR, valida la firma del certificado de firma, instala Citrix Secure Hub y lo establece como propietario del dispositivo.

Para obtener más información sobre el aprovisionamiento de dispositivos mediante el método de código QR, consulte la documentación de la API de Google para desarrolladores de EMM de Android.

Toque NFC

Para inscribir un dispositivo como dispositivo totalmente administrado mediante toques NFC se necesitan dos dispositivos: uno restablecido a la configuración de fábrica y otro que ejecute la herramienta de aprovisionamiento de Citrix Endpoint Management.

Requisitos previos:

- Dispositivos Android compatibles
- Citrix Endpoint Management habilitado para Android Enterprise
- Un dispositivo nuevo o restablecido de fábrica, aprovisionado para Android Enterprise como dispositivo totalmente administrado. Los pasos para completar este requisito previo se encuentran más adelante en este artículo.
- Otro dispositivo con capacidad NFC, que ejecute la herramienta de aprovisionamiento configurada. La herramienta de aprovisionamiento está disponible en Citrix Secure Hub o en la página de descargas de Citrix.

Cada dispositivo puede tener un solo perfil de Android Enterprise, administrado por una aplicación de gestión de movilidad empresarial (EMM). En Citrix Endpoint Management, Citrix Secure Hub es la aplicación EMM. Solo se permite un perfil en cada dispositivo. Intentar añadir una segunda aplicación EMM elimina la primera aplicación EMM.

DATOS TRANSFERIDOS MEDIANTE EL TOQUE NFC

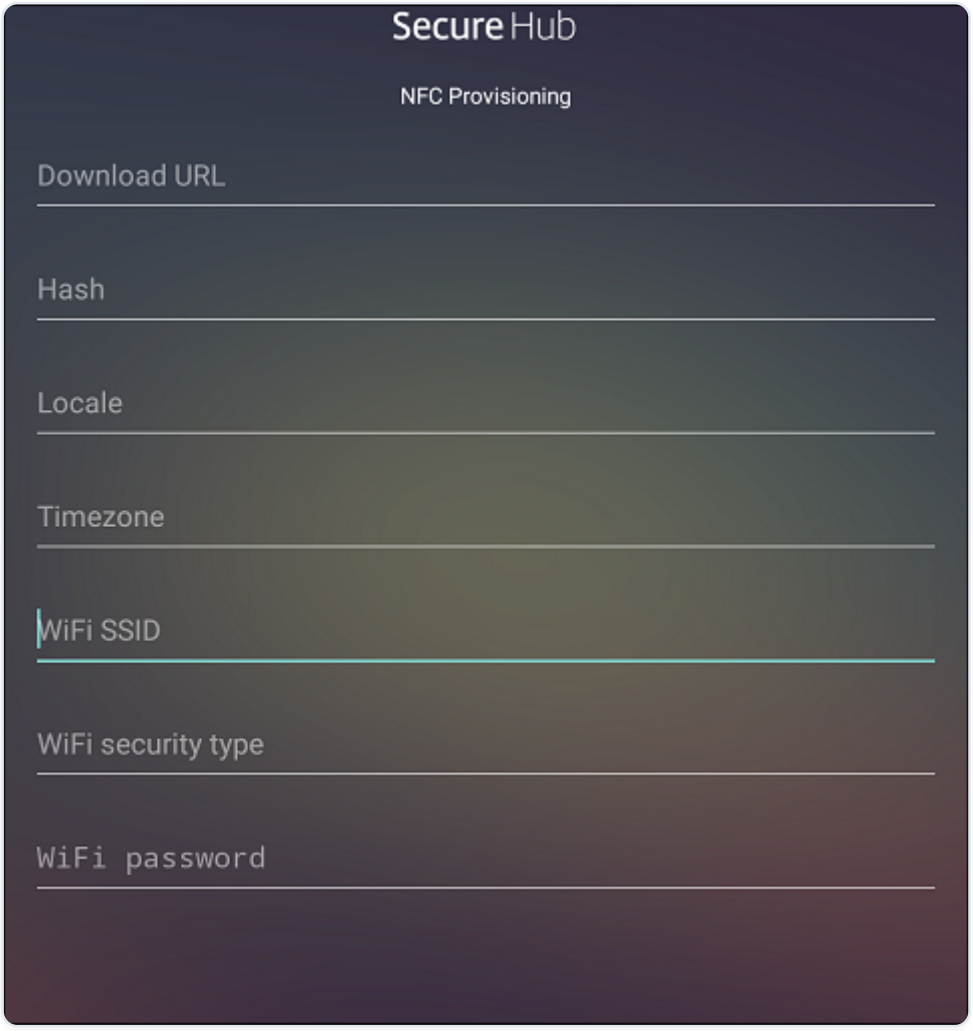
Para aprovisionar un dispositivo restablecido de fábrica, debe enviar los siguientes datos mediante un toque NFC para inicializar Android Enterprise:

- Nombre del paquete de la aplicación del proveedor EMM que actúa como propietario del dispositivo (en este caso, Citrix Secure Hub).
- Ubicación de intranet/Internet desde la que el dispositivo puede descargar la aplicación del proveedor EMM.
- Hash SHA-256 de la aplicación del proveedor EMM para verificar si la descarga se ha realizado correctamente.
- Detalles de conexión Wi-Fi para que un dispositivo restablecido de fábrica pueda conectarse y descargar la aplicación del proveedor EMM. Nota: Android ya no es compatible con Wi-Fi 802.1x para este paso.
- Zona horaria del dispositivo (opcional).
- Ubicación geográfica del dispositivo (opcional).

Cuando se tocan los dos dispositivos, los datos de la Herramienta de aprovisionamiento se envían al dispositivo restablecido de fábrica. Esos datos se utilizan luego para descargar Citrix Secure Hub con la configuración de administrador. Si no introduce los valores de zona horaria y ubicación, Android configura automáticamente los valores en el nuevo dispositivo.

CONFIGURACIÓN DE LA HERRAMIENTA DE APROVISIONAMIENTO DE CITRIX ENDPOINT MANAGEMENT

Antes de realizar un toque NFC, debe configurar la Herramienta de aprovisionamiento. Esta configuración se transfiere luego al dispositivo restablecido de fábrica durante el toque NFC.



Puede introducir datos en los campos obligatorios o rellenarlos mediante un archivo de texto. Los pasos del siguiente procedimiento describen cómo configurar el archivo de texto y tienen descripciones para cada campo. La aplicación no guarda la información después de introducirla, por lo que es posible que desee crear un archivo de texto para guardar la información para uso futuro.

Para configurar la Herramienta de aprovisionamiento mediante un archivo de texto

Asigne el nombre nfcprovisioning.txt al archivo y colóquelo en la carpeta **/sdcard/** de la tarjeta SD del dispositivo. La aplicación podrá leer el archivo de texto y rellenar los valores.

El archivo de texto debe contener los siguientes datos:

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<download_location>`

Esta línea es la ubicación de intranet/internet de la aplicación del proveedor de EMM. Después de que el dispositivo restablecido de fábrica se conecte a la red Wi-Fi tras el toque NFC, el dispositivo debe tener acceso a esta ubicación para la descarga. La URL es una URL normal, sin necesidad de formato especial.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>`

Esta línea es la suma de comprobación (checksum) de la aplicación del proveedor de EMM. Esta suma de comprobación se utiliza para verificar que la descarga se ha realizado correctamente. Los pasos para obtener la suma de comprobación se describen más adelante en este artículo.

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

Esta línea es el SSID de la red Wi-Fi conectada del dispositivo en el que se ejecuta la herramienta de aprovisionamiento.

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

Los valores admitidos son WEP y WPA2. Si la red Wi-Fi no está protegida, este campo debe estar vacío.

`android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>`

Si la red Wi-Fi no está protegida, este campo debe estar vacío.

`android.app.extra.PROVISIONING_LOCALE=<locale>`

Introduzca los códigos de idioma y país. Los códigos de idioma son códigos de idioma ISO de dos letras en minúsculas (como en) definidos por ISO 639-1. Los códigos de país son códigos de país ISO de dos letras en mayúsculas (como US) definidos por ISO 3166-1. Por ejemplo, escriba en_US para el inglés hablado en Estados Unidos. Si no introduce ningún código, el país y el idioma se rellenan automáticamente.

`android.app.extra.PROVISIONING_TIME_ZONE=<timezone>`

La zona horaria en la que se ejecuta el dispositivo. Escriba el nombre de la base de datos del área/ubicación. Por ejemplo, escriba **America/Los_Angeles** para la hora del Pacífico. Si no escribe un nombre, la zona horaria se rellena automáticamente.

`android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>`

Estos datos no son obligatorios, ya que el valor está codificado en la aplicación como Citrix Secure Hub. Se mencionan aquí solo por motivos de exhaustividad.

Si hay una red Wi-Fi protegida con WPA2, un archivo nfcprovisioning.txt completado podría tener el siguiente aspecto:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
```

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
```

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Si hay una red Wi-Fi desprotegida, un archivo nfcprovisioning.txt completado podría tener el siguiente aspecto:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

PARA OBTENER LA SUMA DE COMPROBACIÓN DE CITRIX SECURE HUB

La suma de comprobación de Citrix Secure Hub es un valor constante: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`. Para descargar un archivo APK de Citrix Secure Hub, utilice el siguiente enlace de Google Play Store: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

PARA OBTENER LA SUMA DE COMPROBACIÓN DE UNA APLICACIÓN

Requisitos previos:

- La herramienta **apksigner** de Android SDK Build Tools
- Línea de comandos de OpenSSL

Para obtener la suma de comprobación de cualquier aplicación, siga estos pasos:

1. Descargue el archivo APK de la aplicación desde Google Play Store.
2. En la línea de comandos de OpenSSL, navegue hasta la herramienta **apksigner**: `android-sdk/build-tools/<version>/apksigner` y escriba lo siguiente:

   ```
   apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{(?<=SHA-256 digest:) .*}'  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
   ```

   El comando devuelve una suma de comprobación válida.
3. Para generar el código QR, introduzca la suma de comprobación en el campo `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM`. Por ejemplo:

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",


"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUth
eu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?
identifier=xenmobile",

  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"

   }

}
```

BIBLIOTECAS UTILIZADAS

La herramienta de aprovisionamiento utiliza las siguientes bibliotecas en su código fuente:

- biblioteca v7 `appcompat`, biblioteca de soporte de diseño y biblioteca de soporte de paleta v7

  Para obtener información, busque la Guía de características de la biblioteca de soporte en la documentación para desarrolladores de Android.

- Butter Knife de Jake Wharton bajo licencia Apache 2.0

Aprovisionar dispositivos con perfil de trabajo en Android Enterprise

En los dispositivos con perfil de trabajo de Android Enterprise, se separan de forma segura las áreas corporativa y personal en un dispositivo. Por ejemplo, los dispositivos BYOD pueden ser dispositivos con perfil de trabajo. La experiencia de inscripción para dispositivos con perfil de trabajo es similar a la inscripción de Android en Citrix Endpoint Management. Los usuarios descargan Citrix Secure Hub de Google Play e inscriben sus dispositivos.

De forma predeterminada, la depuración USB y la configuración de orígenes desconocidos están deshabilitadas en un dispositivo cuando se inscribe en Android Enterprise como dispositivo con perfil de trabajo.

> **Consejo:**
>
> Al inscribir dispositivos en Android Enterprise como dispositivos con perfil de trabajo, vaya siempre a Google Play. Desde allí, habilite Citrix Secure Hub para que aparezca en el perfil personal del usuario.

Android OS

> **Nota:**
>
> Este artículo no se aplica a los dispositivos administrados con Android Enterprise. Para obtener información sobre esos dispositivos, consulte otros artículos de esta sección.

> Citrix Endpoint Management también es compatible con dispositivos con sistema operativo Android que no se administran a través de un programa empresarial de Android o Samsung. Para controlar cómo y cuándo los dispositivos Android se conectan al servicio de Citrix Endpoint Management, utilice Firebase Cloud Messaging (FCM). Para obtener información, consulte Firebase Cloud Messaging.

Los perfiles de inscripción determinan si los dispositivos Android se inscriben en MAM, MDM o MDM+MAM, con la opción de que los usuarios puedan excluirse de MDM. Citrix Endpoint Management admite los siguientes tipos de autenticación para dispositivos Android en MDM+MAM. Para obtener información, consulte los siguientes artículos:

- Autenticación de dominio o de dominio más token de seguridad
- Certificado de cliente o certificado más autenticación de dominio
- Proveedores de identidades:
  - Autenticación con Azure Active Directory a través de Citrix Cloud
  - Autenticación con Okta a través de Citrix Cloud

Otro método de autenticación poco utilizado es un certificado de cliente más un token de seguridad. Para obtener información, consulte `<https://support.citrix.com/article/CTX215200>`.

Un flujo de trabajo general para iniciar la administración de dispositivos Android es el siguiente:

1. Complete el proceso de incorporación. Consulte Incorporación y configuración de recursos y Preparar la inscripción de dispositivos y la entrega de recursos.
2. Elija y configure un método de inscripción. Consulte Métodos de inscripción admitidos.
3. Configurar directivas de dispositivos Android.
4. Inscribir dispositivos Android.
5. Configure las acciones de seguridad de dispositivos y aplicaciones. Consulte Acciones de seguridad.

Para ver los sistemas operativos compatibles, consulte Sistemas operativos de dispositivos compatibles.

Métodos de inscripción admitidos

La siguiente tabla enumera los métodos de inscripción que Citrix Endpoint Management admite para dispositivos Android:

MÉTODO	COMPATIBLE
Inscripción masiva	No
Inscripción manual	Sí

MÉTODO	COMPATIBLE
Invitaciones de inscripción	Sí

Agregar un dispositivo Android manualmente

Si quiere agregar un dispositivo Android o iOS manualmente, por ejemplo, para realizar pruebas, siga estos pasos.

1. En la consola de Citrix Endpoint Management, haga clic en **Administrar > Dispositivos**. Aparece la página **Dispositivos**.

   Página Dispositivos(/en-us/citrix-endpoint-management/media/manage-devices-columns.png)

2. Haga clic en **Agregar**. Aparece la página **Agregar dispositivo**.

   Página Agregar dispositivo(/en-us/citrix-endpoint-management/media/manage-devices-add-device.png)

3. Configure estos parámetros:

   - **Seleccionar plataforma:** Haga clic en **Android**.
   - **Número de serie:** Escriba el número de serie del dispositivo.
   - **IMEI/MEID:** Opcionalmente, escriba la información IMEI/MEID del dispositivo.

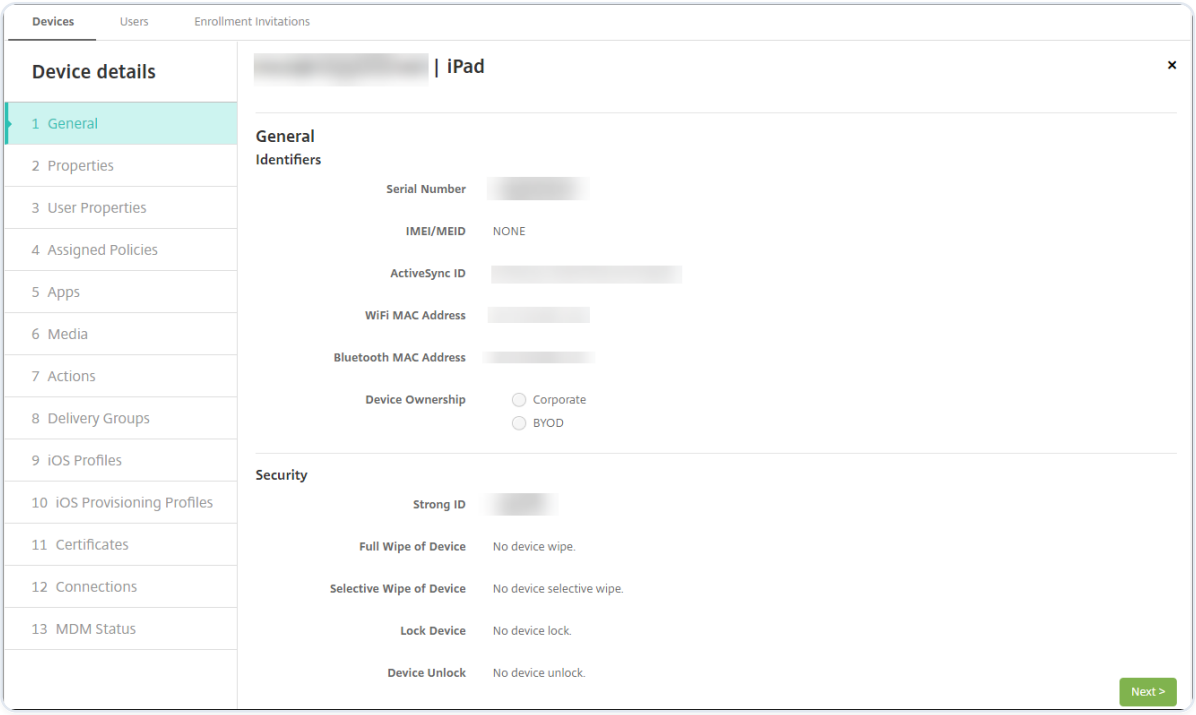
4. Haga clic en **Agregar**. Aparece la tabla **Dispositivos** con el dispositivo agregado al final de la lista. Para ver y confirmar los detalles del dispositivo: Elija el dispositivo que agregó y, a continuación, en el menú que aparece, haga clic en **Modificar**.

   > **Nota:**
   >
   > Cuando selecciona la casilla de verificación junto a un dispositivo, el menú de opciones aparece encima de la lista de dispositivos. Cuando hace clic en cualquier otro lugar de la lista, el menú de opciones aparece en el lado derecho de la lista.

   - LDAP configurado
   - Si utiliza grupos locales y usuarios locales:
     - Uno o varios grupos locales.
     - Usuarios locales asignados a grupos locales.

- Los grupos de entrega están asociados con grupos locales.

- Si utiliza Active Directory:
  - Los grupos de entrega están asociados con grupos de Active Directory.



5. La página **General** enumera los **Identificadores** del dispositivo, como el número de serie y otra información para el tipo de plataforma. En **Propiedad del dispositivo**, seleccione **Corporativo** o **BYOD**.

   La página **General** también enumera las propiedades de **Seguridad** del dispositivo, como ID seguro, Bloquear dispositivo, Omisión de bloqueo de activación y otra información para el tipo de plataforma. El campo **Borrado completo del dispositivo** incluye el código PIN del usuario. El usuario debe introducir ese código después de borrar el dispositivo. Si el usuario olvida el código, puede consultarlo aquí.

6. La página **Propiedades** enumera las propiedades del dispositivo que Citrix Endpoint Management debe aprovisionar. Esta lista muestra las propiedades del dispositivo incluidas en el archivo de aprovisionamiento utilizado para agregar el dispositivo. Para agregar una propiedad, haga clic en **Agregar** y, a continuación, seleccione una propiedad de la lista. Para ver los valores válidos de cada propiedad, consulte el PDF Nombres y valores de las propiedades del dispositivo.

   Cuando agrega una propiedad, aparece inicialmente en la categoría donde la agregó. Después de hacer clic en **Siguiente** y volver a la página **Propiedades**, la propiedad aparece en la lista correspondiente.

Para eliminar una propiedad, pase el ratón por encima de la entrada y, a continuación, haga clic en la **X** del lado derecho. Citrix Endpoint Management elimina el elemento inmediatamente.

7. Las secciones restantes de **Detalles del dispositivo** contienen información resumida del dispositivo.

   - **Propiedades de usuario:** Muestra los roles RBAC, las pertenencias a grupos, las cuentas de Google Play administradas y las propiedades del usuario. Puede retirar una cuenta de Google Play administrada desde esta página.
   - **Directivas asignadas:** Muestra el número de directivas implementadas, pendientes y fallidas. Proporciona el nombre, el tipo y la información de la última implementación de cada directiva. Permite restablecer el estado de implementación a pendiente y volver a implementar las directivas que el usuario eliminó.
   - **Aplicaciones:** Muestra, para el último inventario, el número de implementaciones de aplicaciones instaladas, pendientes y fallidas. Proporciona el nombre, el identificador, el tipo y otra información de la aplicación. Para obtener una descripción de las claves de inventario de iOS y macOS, como **HasUpdateAvailable**, consulte Protocolo de administración de dispositivos móviles (MDM).
   - **Contenido multimedia:** Muestra, para el último inventario, el número de implementaciones de contenido multimedia implementadas, pendientes y fallidas.
   - **Acciones:** Muestra el número de acciones implementadas, pendientes y fallidas. Proporciona el nombre de la acción y la hora de la última implementación.
   - **Grupos de entrega:** Muestra el número de grupos de entrega correctos, pendientes y fallidos. Para cada implementación, proporciona el nombre del grupo de entrega y la hora de implementación. Seleccione un grupo de entrega para ver información más detallada, incluido el estado, la acción y el canal o usuario.
   - **Perfiles de iOS:** Muestra el último inventario de perfiles de iOS, incluidos el nombre, el tipo, la organización y la descripción.
   - **Perfiles de aprovisionamiento de iOS:** Muestra información del perfil de aprovisionamiento de distribución empresarial, como el UUID, la fecha de caducidad y el estado administrado.
   - **Certificados:** Muestra, para los certificados válidos, caducados o revocados, información como el tipo, el proveedor, el emisor, el número de serie y el número de días restantes antes de la caducidad.

- **Conexiones:** Muestra el estado de la primera conexión y el estado de la última conexión. Proporciona para cada conexión el nombre de usuario, la hora de la penúltima (anterior a la última) autenticación y la hora de la última autenticación.
- **Estado de MDM:** Muestra información como el estado de MDM, la hora del último envío y la hora de la última respuesta del dispositivo.

Configurar directivas de dispositivos Android

Utilice estas directivas para configurar cómo Citrix Endpoint Management interactúa con los dispositivos que ejecutan Android. Esta tabla enumera todas las directivas de dispositivo disponibles para dispositivos Android.

APN	Acceso a aplicaciones	Inventario de aplicaciones
Bloqueo de aplicaciones	Desinstalación de aplicaciones	Credenciales
Opciones de Citrix Endpoint Management	Desinstalación de Citrix Endpoint Management	Archivos
Configuración del iniciador	Ubicación	Red
Código de acceso	Restricciones	Programación
Tienda	Términos y condiciones	Túnel
VPN	Clip web	

Inscribir dispositivos Android

1. Vaya a Google Play Store en su dispositivo Android, descargue la aplicación Citrix Secure Hub y, a continuación, toque la aplicación.
2. Cuando se le pida que instale la aplicación, haga clic en **Siguiente** y luego en **Instalar**.
3. Una vez instalado Citrix Secure Hub, toque **Abrir**.
4. Para dispositivos con Android 6.0 o posterior, acepte los permisos necesarios:
    - ¿Permitir que Citrix Secure Hub realice y administre llamadas telefónicas? (obligatorio)
    - ¿Permitir que Citrix Secure Hub acceda a fotos, contenido multimedia y archivos en su dispositivo? (obligatorio)

- ¿Permitir que Citrix Secure Hub acceda a la ubicación de este dispositivo? (opcional)

5. Introduzca sus credenciales corporativas, como el nombre del servidor de Citrix Endpoint Management, el nombre principal de usuario (UPN) o la dirección de correo electrónico. A continuación, haga clic en **Siguiente**.
6. Elija cómo inscribir su dispositivo:

   - Para inscribirse en MDM+MAM, toque **Sí, inscribir**.
   - Para inscribirse en MAM, toque **No**.

7. En la pantalla **Activar administrador de dispositivos**, toque **Activar**.
8. Introduzca su contraseña corporativa y, a continuación, toque **Iniciar sesión**.
9. Según cómo esté configurado Citrix Endpoint Management, es posible que se le pida que cree un PIN de Citrix. Puede usar el PIN para iniciar sesión en Citrix Secure Hub y en otras aplicaciones habilitadas para Citrix Endpoint Management, como Citrix Secure Mail y Citrix Files. Introduzca su PIN de Citrix dos veces. En la pantalla **Crear PIN de Citrix**, introduzca un PIN.
10. Vuelva a introducir el PIN. Se abrirá Citrix Secure Hub. A continuación, puede acceder a la tienda de aplicaciones para ver las aplicaciones que puede instalar en su dispositivo Android.
11. Si configuró Citrix Endpoint Management para enviar aplicaciones a los dispositivos automáticamente después de la inscripción, se pedirá a los usuarios que instalen las aplicaciones. Además, las directivas que configure en Citrix Endpoint Management se implementarán en el dispositivo. Toque **Instalar** para instalar la aplicación.

Para anular la inscripción y volver a inscribir un dispositivo Android

Los usuarios pueden anular la inscripción desde Citrix Secure Hub. Cuando los usuarios anulan la inscripción siguiendo el procedimiento siguiente, el dispositivo sigue apareciendo en el inventario de dispositivos de la consola de Citrix Endpoint Management. Sin embargo, no se pueden realizar acciones en el dispositivo. Por ejemplo, no se puede rastrear el dispositivo ni supervisar su cumplimiento.

1. Toque para abrir la aplicación Citrix Secure Hub.
2. Según tenga un teléfono o una tableta, haga lo siguiente:

   En un teléfono:

   - Deslice el dedo desde la izquierda de la pantalla para abrir un panel de configuración.
   - Toque **Preferencias**, toque **Cuentas** y, a continuación, toque **Eliminar cuenta**.

En una tableta:

- Toque la flecha junto a su dirección de correo electrónico en la esquina superior derecha.
- Toque **Preferencias**, toque **Cuentas** y, a continuación, toque **Eliminar cuenta**.

3. En la ventana **¿Eliminar cuenta?**, toque **Sí, eliminar**. Citrix Secure Hub anula la inscripción de su dispositivo. Siga las instrucciones en pantalla para volver a inscribir su dispositivo.

Acciones de seguridad

Android admite las siguientes acciones de seguridad. Para obtener una descripción de cada acción de seguridad, consulte Acciones de seguridad.

Bloqueo de apps	Borrado de apps	Renovación de certificados
Borrado completo	Localizar	Bloquear
Bloquear y restablecer contraseña	Notificar	Revocar
Borrado selectivo		

Nota:

Para dispositivos con Android 6.0 o superior, la acción de seguridad Localizar requiere que el usuario conceda el permiso de Ubicación durante la inscripción. El usuario puede optar por no conceder el permiso de Ubicación. Si el usuario no concede el permiso durante la inscripción, Citrix Endpoint Management vuelve a solicitar el permiso de ubicación al enviar el comando Localizar.

Firebase Cloud Messaging

Nota:

Firebase Cloud Messaging (FCM) se conocía anteriormente como Google Cloud Messaging (GCM). Algunas etiquetas y mensajes de la consola de Citrix Endpoint Management utilizan la terminología de GCM.

> Citrix recomienda utilizar Firebase Cloud Messaging (FCM) para controlar cómo y cuándo los dispositivos Android se conectan a Citrix Endpoint Management. Citrix Endpoint Management, cuando está configurado para FCM, envía notificaciones de conexión a los dispositivos Android que tienen FCM habilitado. Cualquier acción de seguridad o comando de implementación activa una notificación push para solicitar al usuario que se vuelva a conectar al servidor de Citrix Endpoint Management.

Una vez que complete los pasos de configuración de este artículo y un dispositivo se registre, el dispositivo se registrará en el servicio FCM de Citrix Endpoint Management. Esa conexión permite la comunicación casi en tiempo real desde su servicio Citrix Endpoint Management a su dispositivo mediante FCM. El registro de FCM funciona para nuevas inscripciones de dispositivos y para dispositivos inscritos anteriormente.

Cuando Citrix Endpoint Management necesita iniciar una conexión con el dispositivo, se conecta al servicio FCM. Luego, el servicio FCM notifica al dispositivo que se conecte. Este tipo de conexión es similar a la que utiliza Apple para su servicio de notificaciones push.

Requisitos previos

- Cliente de Citrix Secure Hub más reciente
- Credenciales de la cuenta de desarrollador de Google
- Servicios de Google Play instalados en dispositivos Android habilitados para FCM

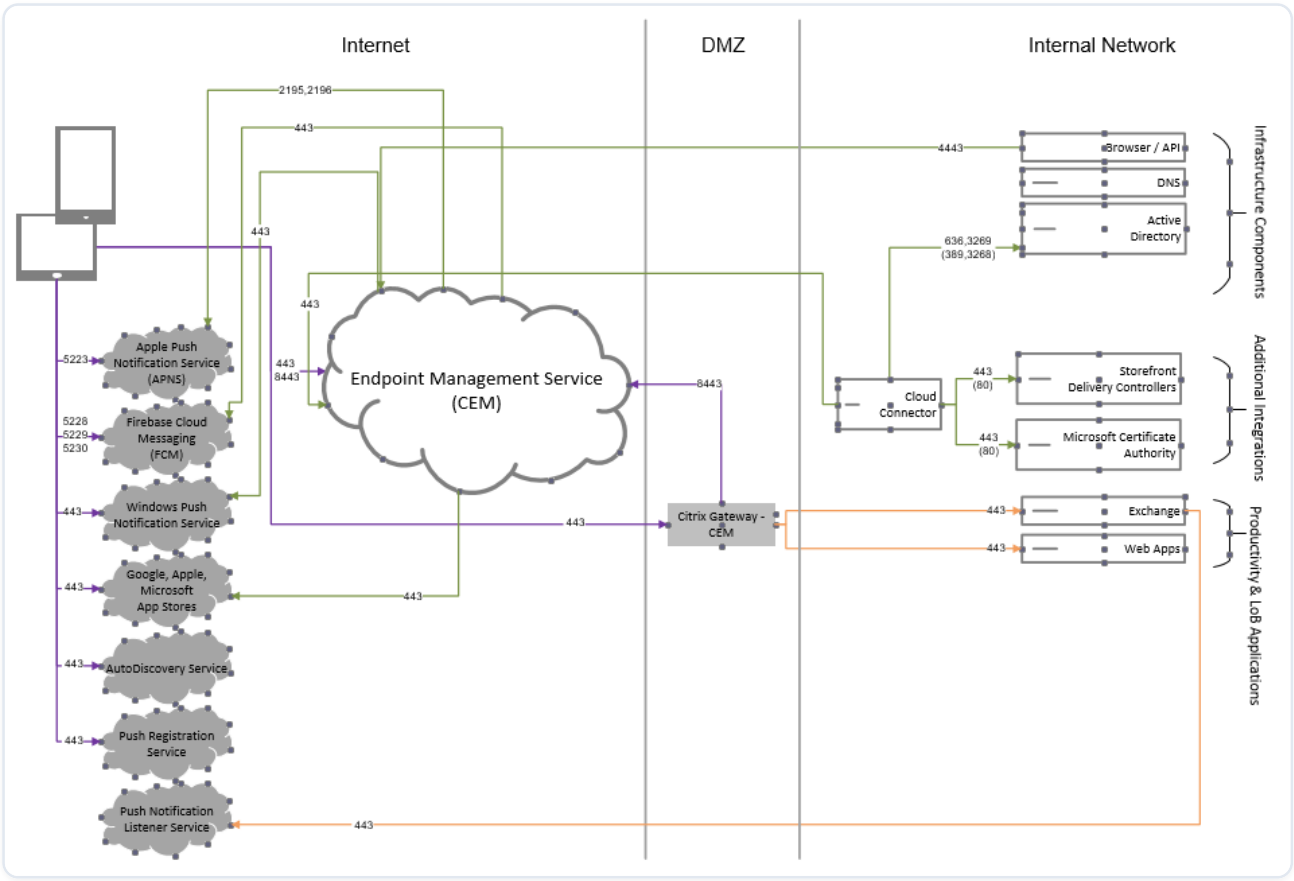
Puertos de firewall

- Abra el puerto 443 en Citrix Endpoint Management para `fcm.googleapis.com` y `Google.com`.
- Abra la comunicación saliente de Internet para la Wi-Fi del dispositivo en los puertos 5228, 5229 y 5230.
- Para permitir las conexiones salientes, FCM recomienda agregar los puertos 5228 a 5230 a una lista de permitidos, sin restricciones de IP. Sin embargo, si necesita restricciones de IP, FCM recomienda agregar todas las direcciones IP de los bloques IPv4 e IPv6 a una lista de permitidos. Esos bloques se enumeran en el ASN de 15169 de Google. Actualice esa lista mensualmente.

Para obtener más información, consulte Requisitos de puertos.

Arquitectura

Este diagrama muestra el flujo de comunicación para FCM en la red externa e interna.

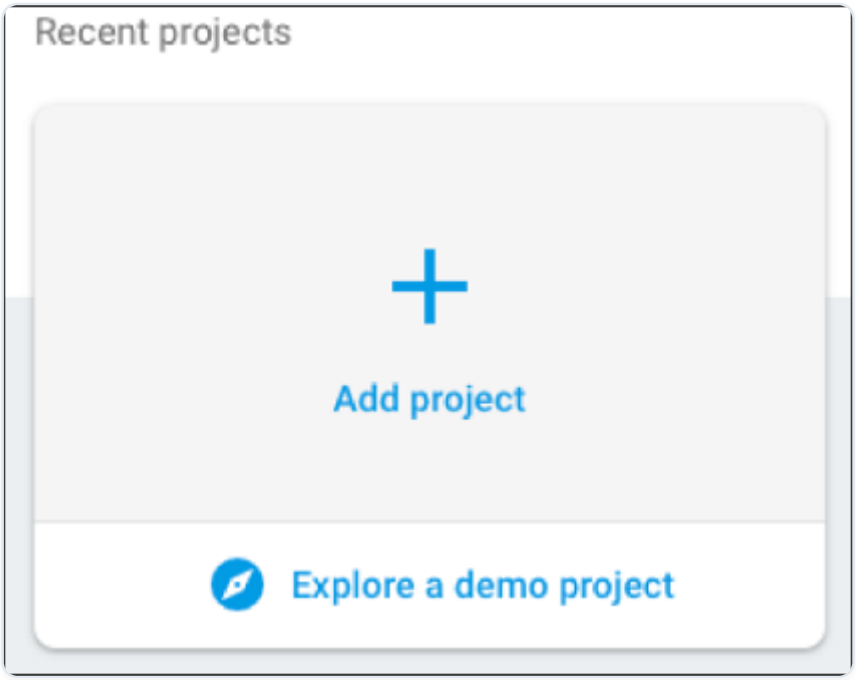


Para configurar su cuenta de Google para FCM

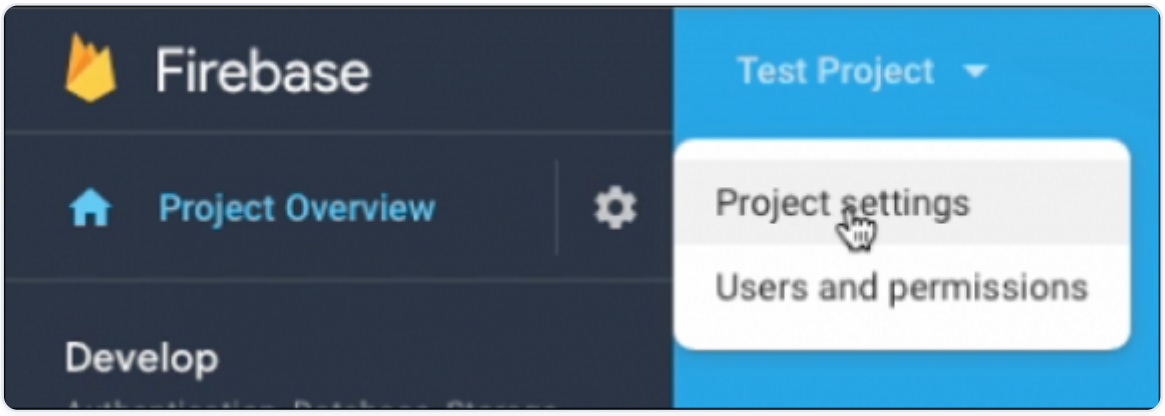
1. Inicie sesión en la siguiente URL utilizando las credenciales de su cuenta de desarrollador de Google:

   `<https://console.firebase.google.com/>`

2. Haga clic en **Añadir proyecto**.



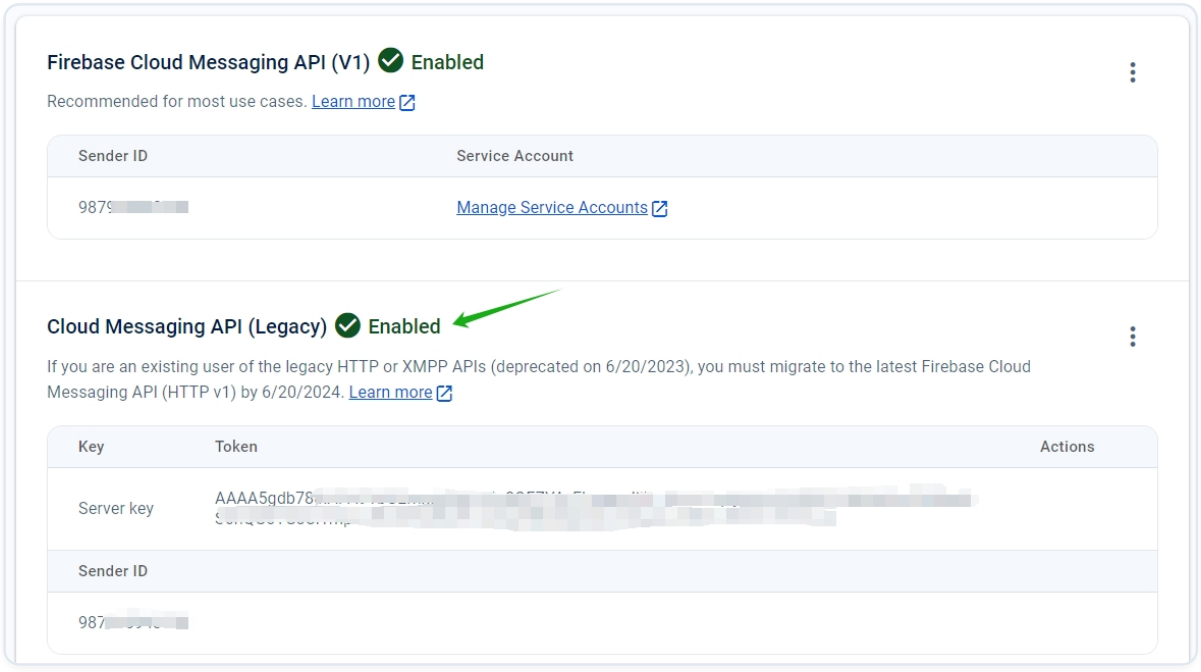
3. Después de crear el proyecto, haga clic en **Configuración del proyecto**.



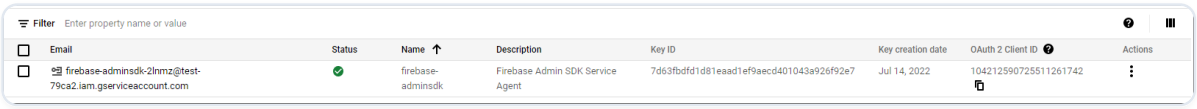
> **Nota:**
>
> Google va a dejar de usar las API heredadas de FCM para HTTP, que se utilizan actualmente en nuestra implementación de FCM. La fecha límite de migración es el June 21, 2024. Necesitamos migrar FCM de la API heredada de FCM a la API HTTP v1. Para obtener más información, consulte Migrar de las API heredadas de FCM a HTTP v1.

4. Haga clic en la pestaña **Cloud Messaging**. verificar que la API de Firebase Cloud Messaging está habilitada y haga clic en **Administrar cuentas de servicio**.

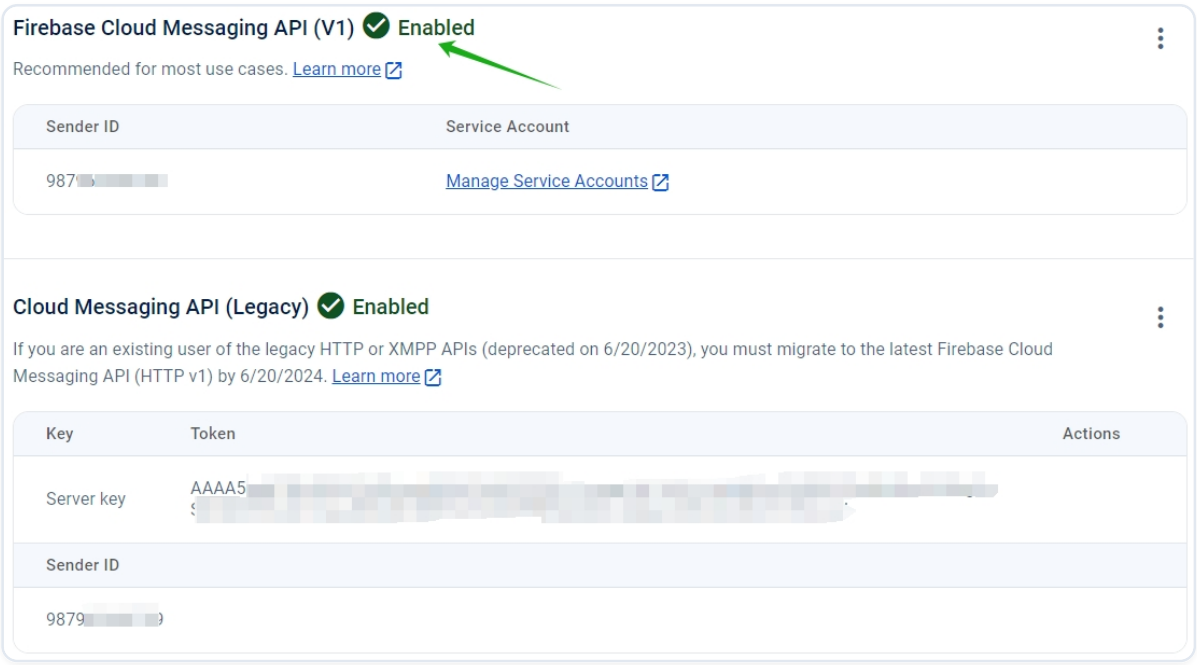
   a. Antes de la migración, podía usar la API heredada; asegúrese de que la API de Cloud Messaging (heredada) esté habilitada. Copie los valores de los campos **Clave** e **ID de remitente**.



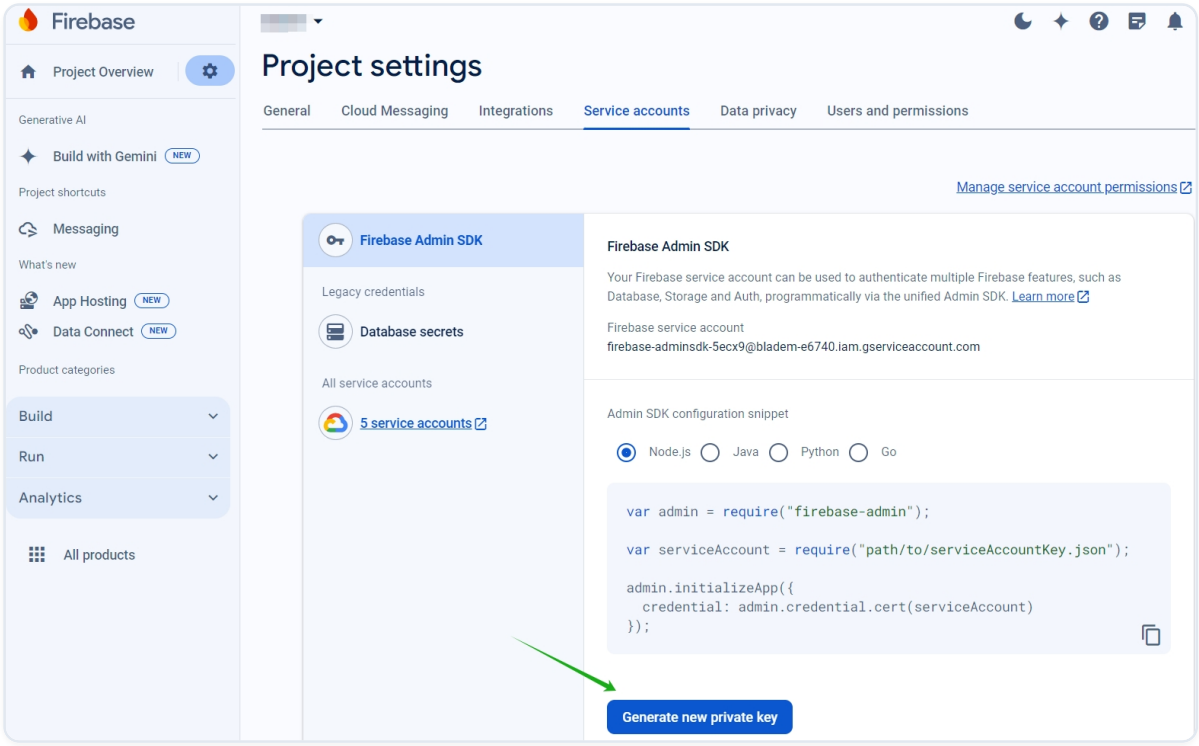
Si no tiene una clave en la lista, haga clic en los puntos suspensivos en **Acciones** para agregar una clave.



b. Después de la migración, la API heredada de Google queda obsoleta. Debe habilitar la Firebase Cloud Messaging API(V1). Para obtener más información, consulte Migrar de las API de FCM heredadas a HTTP v1.



Descargue el archivo JSON de la cuenta de servicio desde **Cuentas de servicio** en **Configuración del proyecto**. Consulte la sección Proporcionar credenciales manualmente para generar un archivo de clave privada para su cuenta de servicio. Haga clic en **Generar nueva clave privada** para descargar el archivo JSON de la clave de la cuenta de servicio.



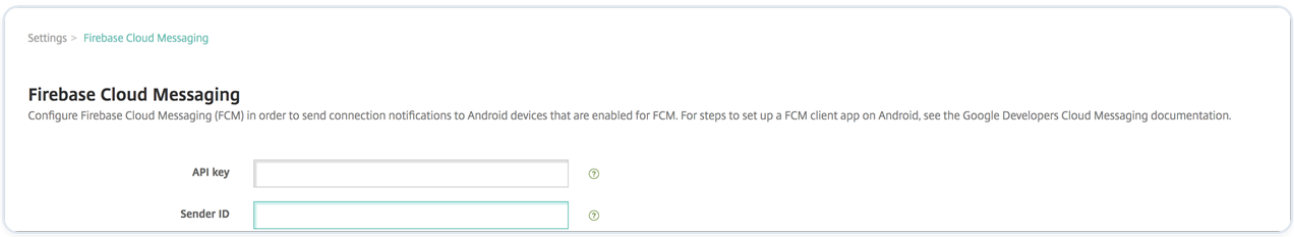
Para conocer los pasos para configurar una aplicación cliente de FCM en Android, consulte este artículo de Google Developers Cloud Messaging: `<https://firebase.google.com/docs/cloud-messaging/android/client>`.

Para configurar Citrix Endpoint Management para FCM

En la consola de Citrix Endpoint Management, vaya a **Configuración > Firebase Cloud Messaging**.

Para la API de Cloud Messaging (heredada)

1. Introduzca la **clave** de Firebase Cloud Messaging del último paso de la configuración de Firebase Cloud Messaging en el campo **Clave de API**.
2. Introduzca el valor de **ID de remitente** del procedimiento anterior.

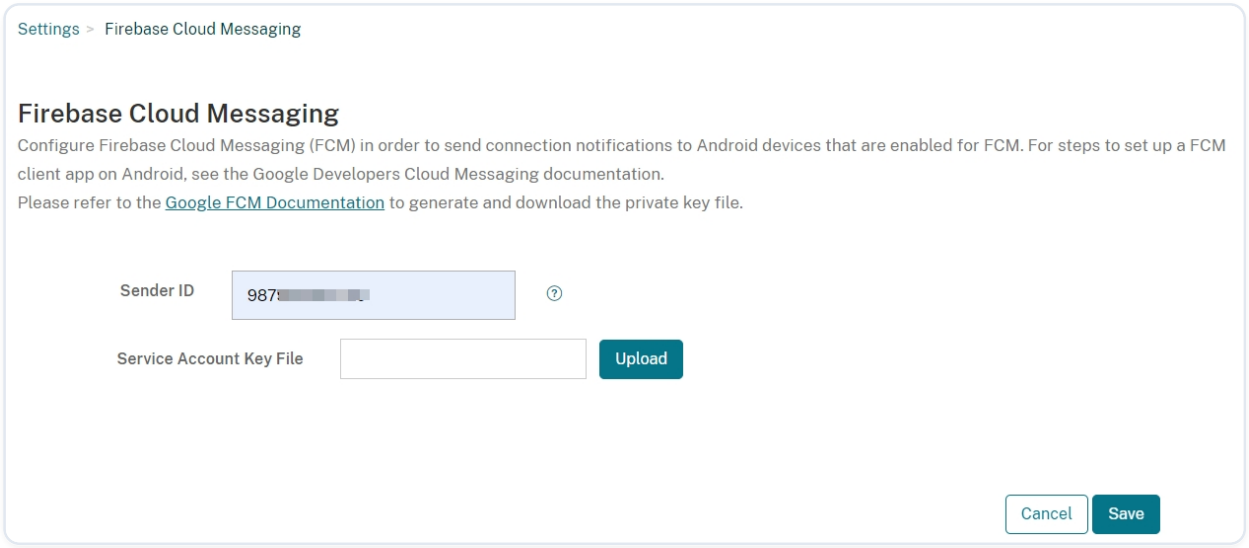


Para la API de Firebase Cloud Messaging (V1)

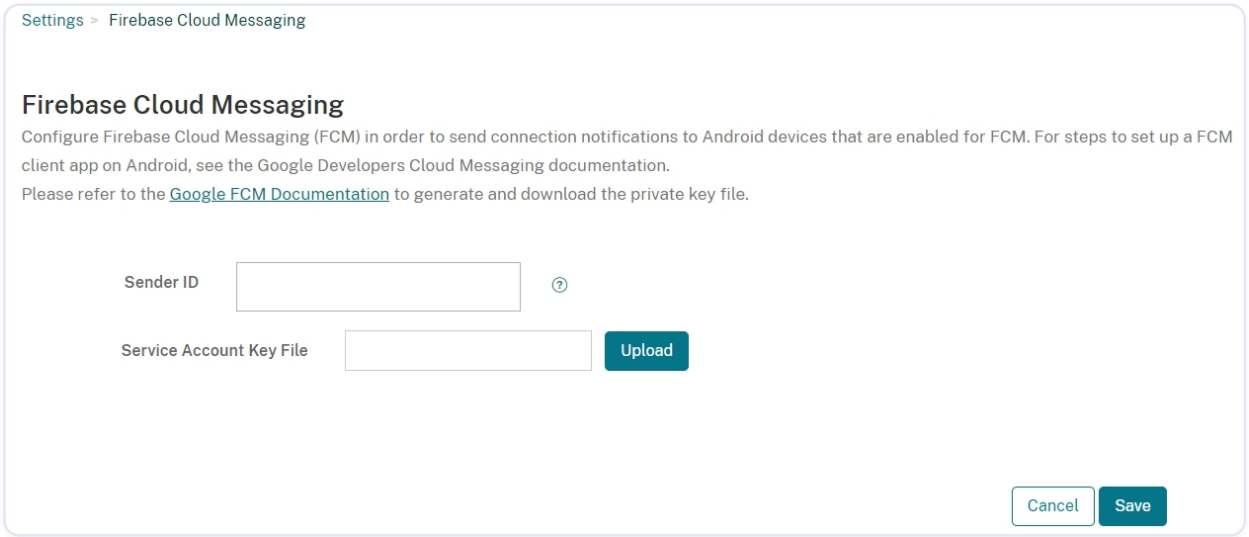
> **Notas:**

- Para habilitar la API V1 de FCM para Citrix Endpoint Management versión 24.6.0 y posteriores, consulte el artículo del Centro de conocimientos CTX677031.
- Si es un nuevo usuario de FCM, omita el paso 1 y continúe a partir del paso 2.

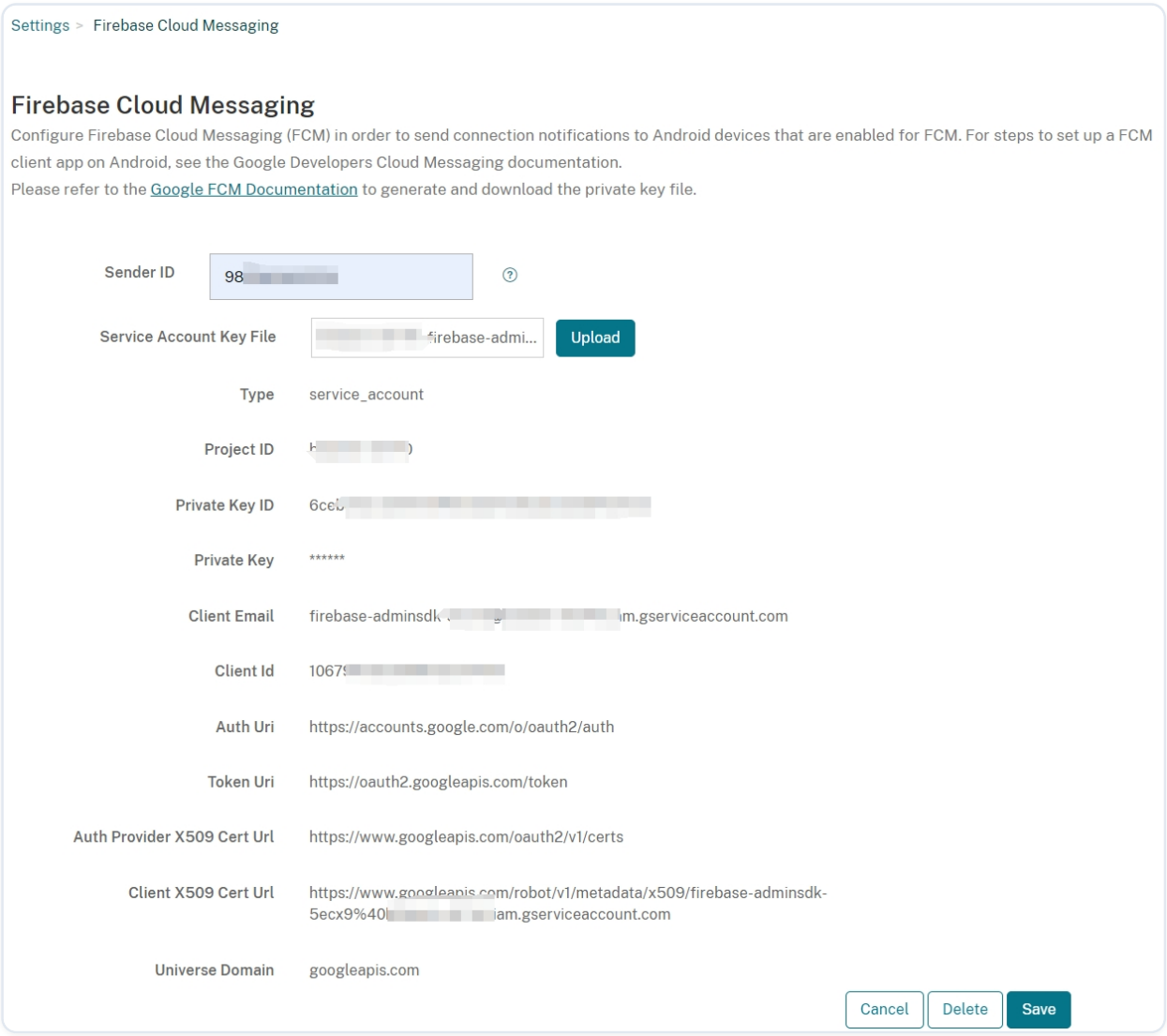
1. Si ya utiliza FCM, observará que el ID de remitente se rellena automáticamente con su proyecto de FCM actual y que aparece una nueva opción para cargar el archivo de clave de cuenta de servicio (**Service Account Key File**).



2. Si es un nuevo usuario de FCM, introduzca el **ID de remitente** y cargue el **archivo de clave de cuenta de servicio** del procedimiento anterior.



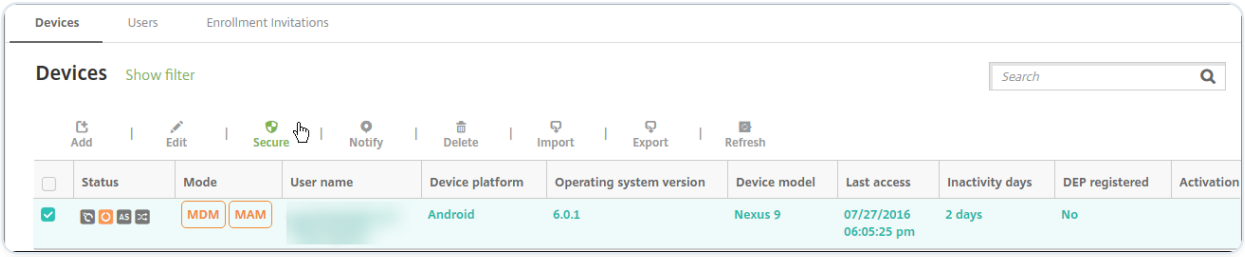
3. El archivo cargado se analizará y los campos correspondientes se generarán automáticamente.



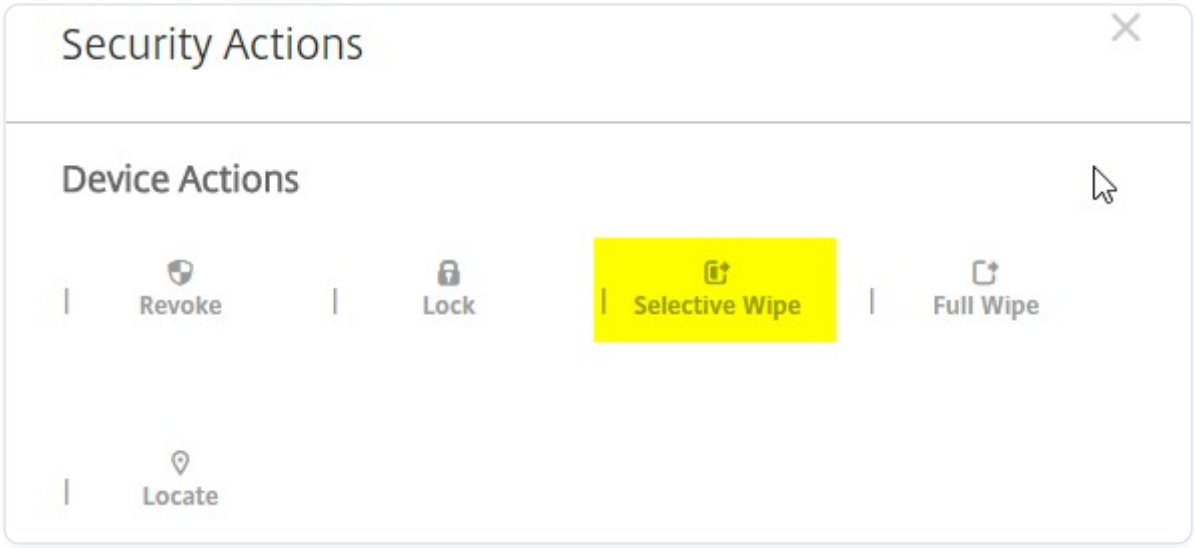
4. verificar la información y haga clic en **Guardar**.

Para probar su configuración

1. Inscriba un dispositivo Android.
2. Deje el dispositivo inactivo durante un tiempo para que se desconecte de Citrix Endpoint Management.
3. Desde la consola de Citrix Endpoint Management, haga clic en **Administrar**, seleccione el dispositivo Android y, a continuación, haga clic en **Proteger**.



4. En **Acciones del dispositivo**, haga clic en **Borrado selectivo**.



En una configuración correcta, el borrado selectivo se produce en el dispositivo.

Compatibilidad con la retroalimentación de configuraciones administradas (versión preliminar técnica)

> **Nota:**
>
> Las funciones en la versión preliminar técnica están disponibles para su uso en entornos que no son de producción o de producción limitada, y para dar a los clientes la oportunidad de compartir sus comentarios. Citrix® no acepta casos de soporte para funciones en versión preliminar técnica, pero agradece los comentarios para mejorarlas. Puede enviar sus comentarios sobre esta función haciendo clic en **Enviar sus comentarios**. Citrix podría actuar sobre los comentarios en función de su gravedad, criticidad e importancia.

La función de retroalimentación de configuraciones administradas permite a los administradores obtener retroalimentación sobre los estados de las aplicaciones desde dispositivos Android configurados con políticas de configuración administradas. Esta retroalimentación se puede utilizar para supervisar la eficacia y el estado de estas políticas.

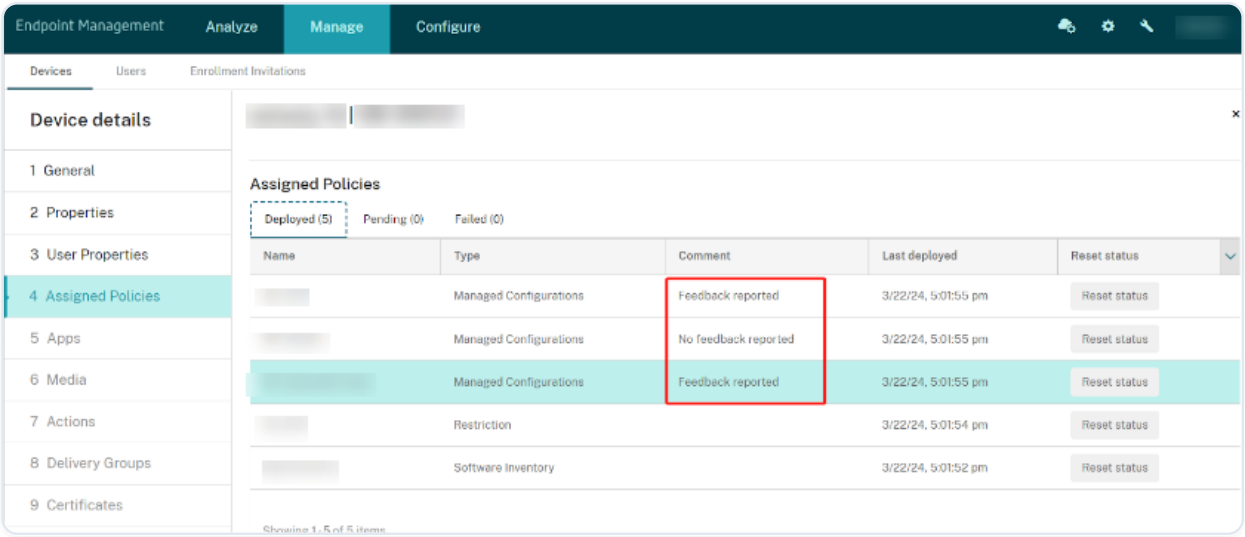
Requisitos previos

1. `App Support`: La aplicación debe ser compatible con las políticas de configuración administradas.
2. `Keyed App States`: La aplicación también debe ser compatible con los estados de aplicación con clave. Para obtener información detallada sobre cómo funciona la

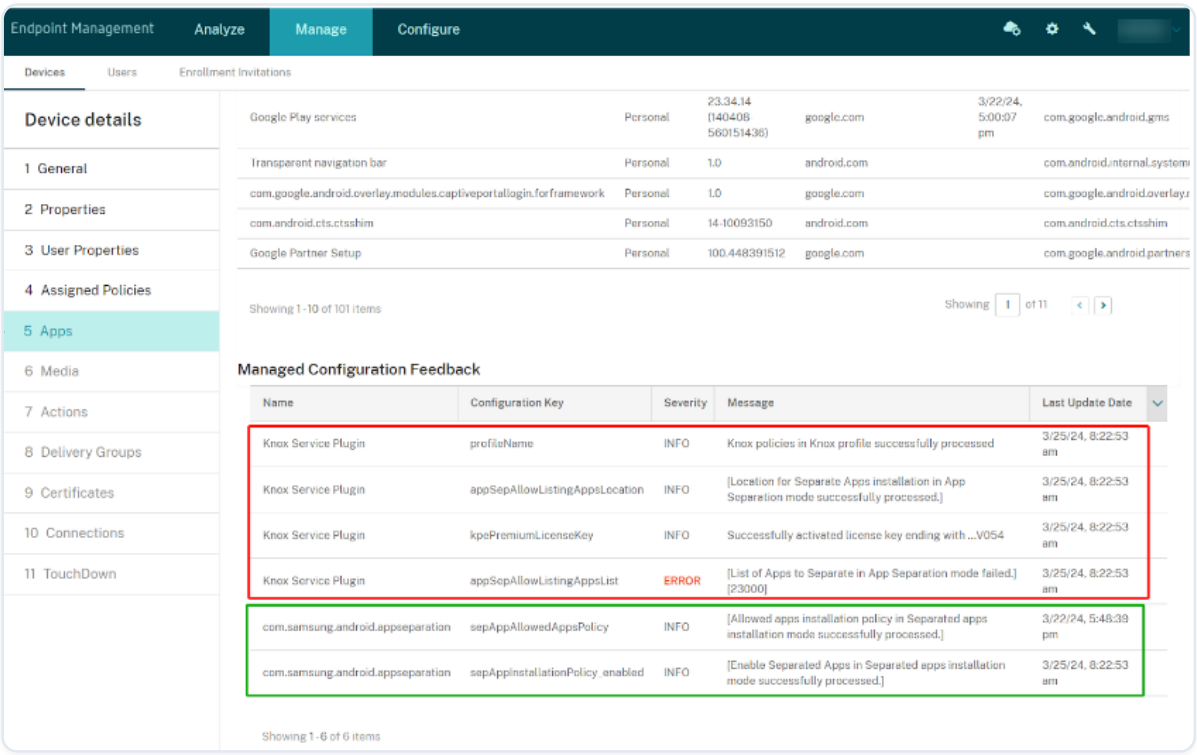
retroalimentación de la aplicación, consulte Enviar retroalimentación de la aplicación a los EMM.

Procedimiento para administrar y utilizar la retroalimentación de configuración

1. Habilite la función `afw.app_managed_configurations.feedback` para el servidor de Citrix Endpoint Management (CEM) especificado.
2. verificar la política de configuración administrada.
   - Confirme que el dispositivo Android está inscrito y que la política de configuración administrada se ha aplicado correctamente.
   - Vaya a **Detalles del dispositivo** y haga clic en **Políticas asignadas**. Se muestran los comentarios relacionados con la política de configuración administrada.
     - **Retroalimentación informada**: Indica que hay retroalimentación disponible para esta aplicación relacionada con la política.
     - **No se ha informado de retroalimentación**: Indica que no se ha informado de retroalimentación para esta aplicación relacionada con la política.



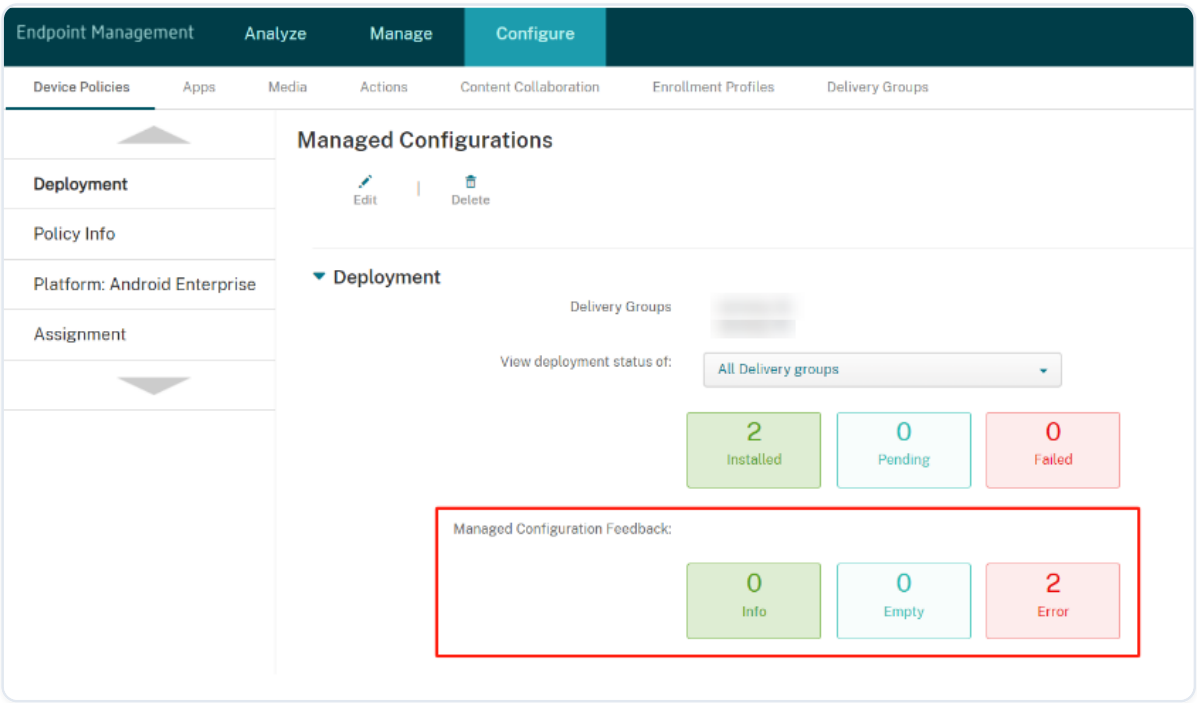
   - Navegue hasta **Detalles del dispositivo** y haga clic en **Aplicaciones**. Los comentarios detallados se muestran en la tabla **Comentarios de configuración administrada** que contiene todos los datos de las aplicaciones.



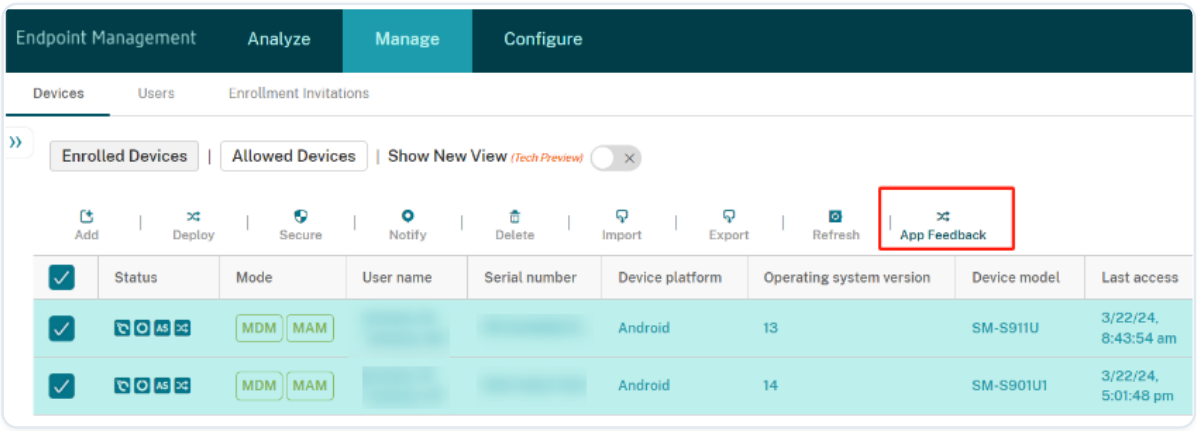
Nota:

En la captura de pantalla anterior, el cuadro rojo resalta el complemento Know Service, mientras que el cuadro verde indica las aplicaciones separadas.

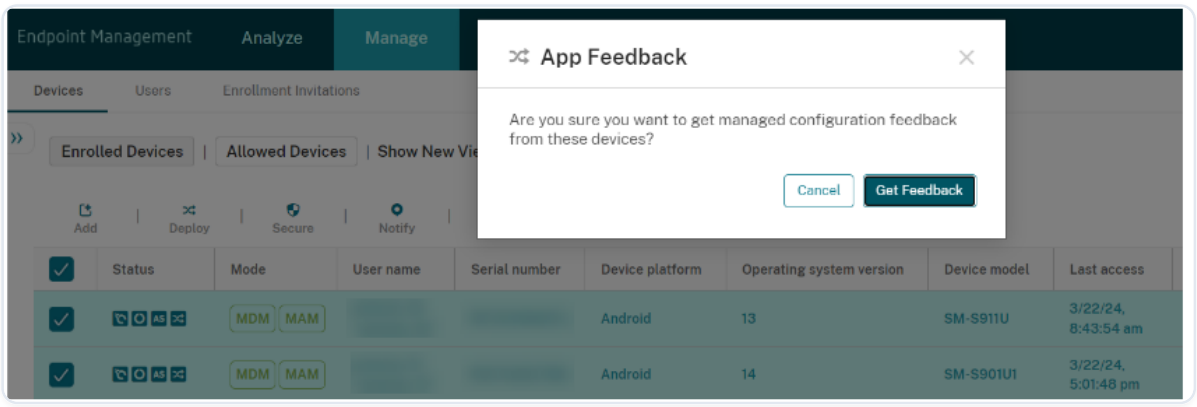
- Para una única política de configuración administrada, puede comprobar los detalles de los comentarios de todos los dispositivos asignados:
  - **Información**: Todos los dispositivos con datos de comentarios notificados que no contienen errores.
  - **Error**: Todos los dispositivos con datos de comentarios notificados que contienen errores.
  - **Vacío**: todos los dispositivos sin datos de comentarios notificados.



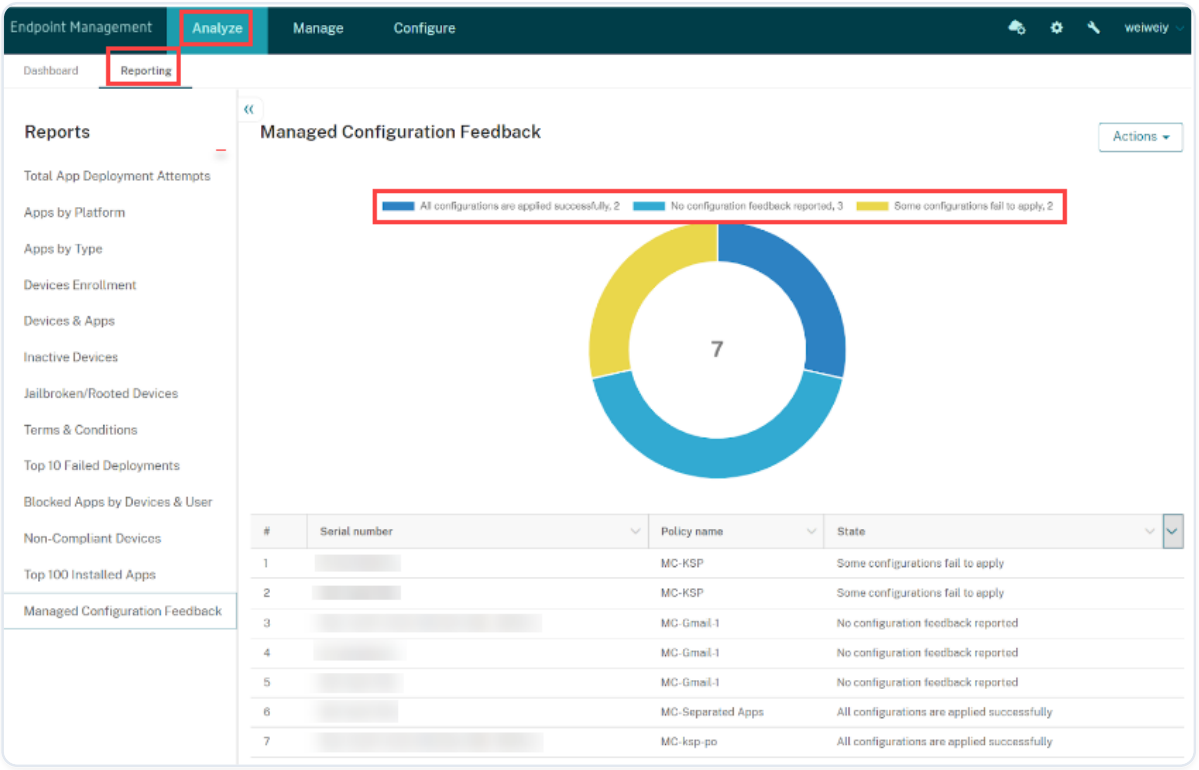
- Para obtener los comentarios manualmente, haga clic en **Administrar** y seleccione la casilla de verificación para localizar los dispositivos correspondientes. Por ejemplo, puede seleccionar las casillas de verificación correspondientes y hacer clic en **Comentarios de la aplicación**.



- Haga clic en **Obtener comentarios** para obtener los comentarios de configuración administrada de los dispositivos seleccionados.



- En el informe de comentarios de configuración administrada, seleccione **Analizar** y haga clic en **Informes** para obtener un comentario general. Puede ver los informes de todos los dispositivos, administrar las políticas de configuración y los errores de configuración relacionados.



3. Se han introducido dos propiedades de servidor para ajustar la programación de comentarios. Utilice las herramientas de administración en la nube para modificar estas propiedades y controlar cuándo se guardan los datos de comentarios en la base de datos.

   a. Tamaño del lote para actualizar la base de datos de comentarios de configuración administrada de Android Enterprise:

      - clave: `android.managed.configuration.feedback.db.update.batch.size`
      - Puede definir el tamaño del lote de informes que se almacenarán en la base de datos; solo los datos almacenados en la base de datos se podrán mostrar en la interfaz de usuario. El valor predeterminado es 100 y el valor máximo es 1000.

   b. Intervalo de tiempo de actualización de la base de datos de comentarios de configuración administrada de Android Enterprise:

      - clave: `android.managed.configuration.feedback.db.update.time.interval`
      - Puede especificar cuánto tiempo se almacenan los informes en la base de datos, incluso si el tamaño no alcanza el límite del lote. El valor predeterminado es de seis horas.

Solución de problemas

De forma predeterminada, los informes de comentarios se recuperan durante cada registro de dispositivo (cuando Secure Hub se conecta al servidor). Sin embargo, puede recuperar manualmente el informe de dispositivos específicos mediante el botón Comentarios de la aplicación.

Android SafetyNet

Puede usar la función Android SafetyNet para evaluar la compatibilidad y la seguridad de los dispositivos Android que tienen instalado Citrix Secure Hub. Android SafetyNet no está disponible para implementaciones de MAM.

Cuando esta función está habilitada, la API de atestación de SafetyNet examina la información de software y hardware de un dispositivo para crear un perfil de ese dispositivo. Luego, la API busca el mismo perfil dentro de una lista de modelos de dispositivos que han pasado las pruebas de compatibilidad de Android. La API también utiliza esta información para determinar si una fuente desconocida ha modificado Citrix Secure Hub.

Cuando la función Android SafetyNet está habilitada, Citrix Secure Hub envía la solicitud de la API de atestación de SafetyNet a los servicios de Google Play y el resultado se notifica a Citrix Endpoint Management. Citrix Endpoint Management actualiza la información del dispositivo con los resultados de la atestación. Puede establecer acciones automatizadas que utilicen los resultados de la atestación para activar acciones en el dispositivo.

Para obtener más información sobre cómo funciona la API de atestación de SafetyNet, consulte la documentación para desarrolladores de Android.

Calcule cuántas solicitudes de la API de atestación de SafetyNet necesita

Las solicitudes de la API de atestación de SafetyNet se envían:

- Cuando un dispositivo se inscribe en Citrix Endpoint Management
- Cuando se produce una autenticación en línea de Citrix Secure Hub

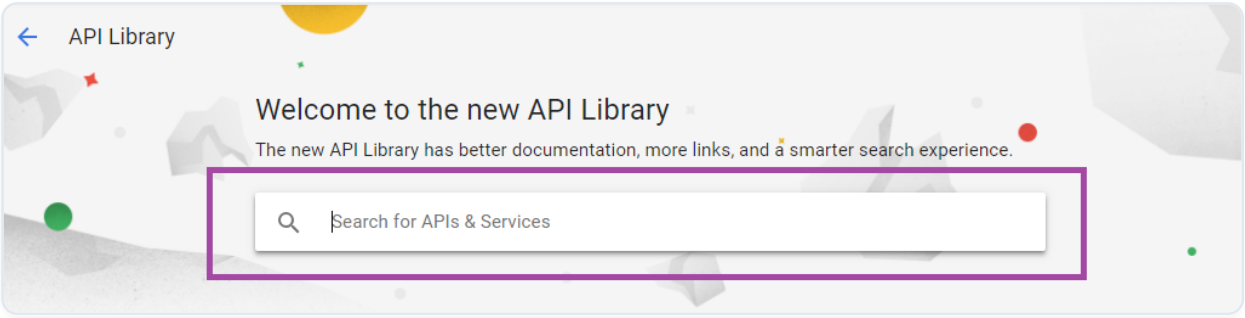
  La autenticación en línea se produce cuando una sesión del servidor caduca o cuando un usuario cierra la sesión del servidor y luego vuelve a iniciarla. Citrix Secure Hub solicita al usuario que proporcione credenciales para autenticarse con el servidor.
- Cuando se reinicia un dispositivo
- En un intervalo de tiempo recurrente que configure, entre 24 y 1000 horas.

Si su implementación de Citrix Endpoint Management realiza más de 10 000 solicitudes al día, rellene este formulario de solicitud de cuota.

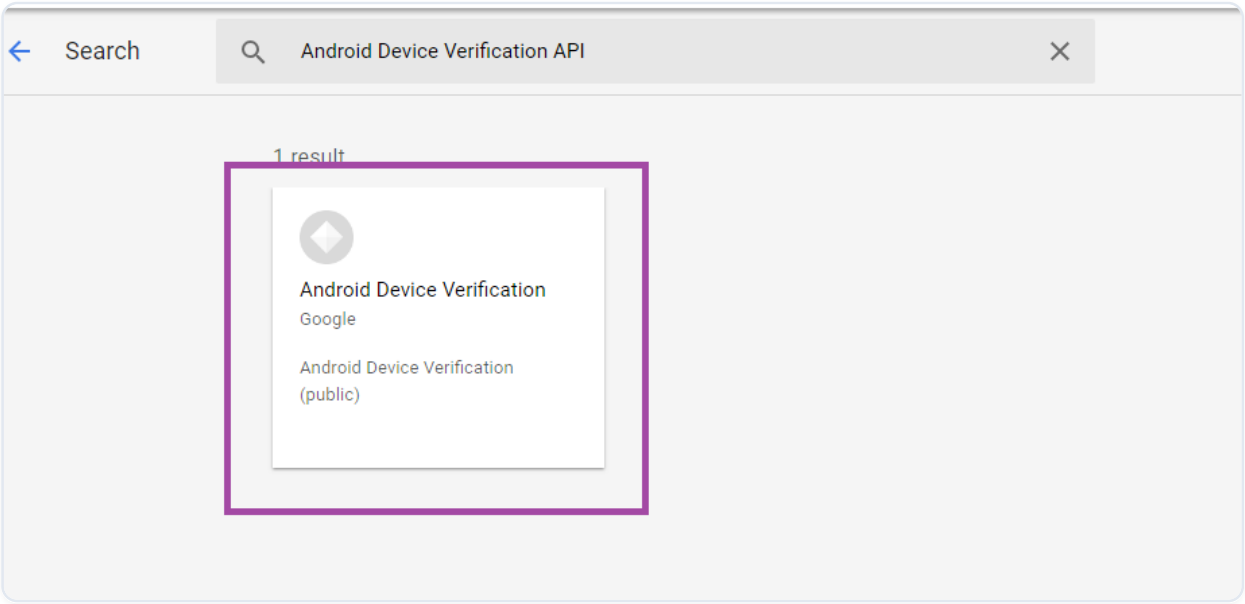
Obtener la clave de la API de SafetyNet

Para habilitar Android SafetyNet en Citrix Endpoint Management, necesita la clave de la **API de SafetyNet**.

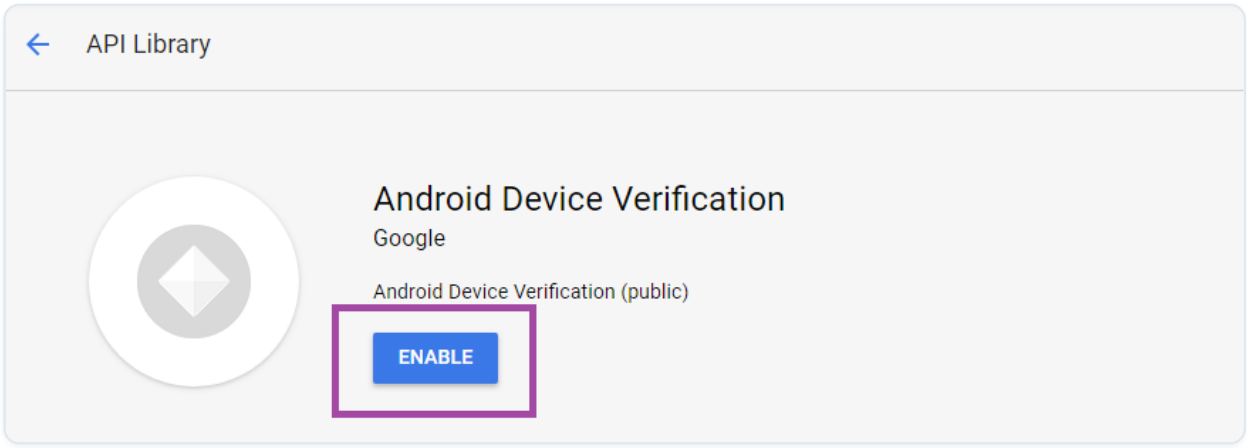
1. Inicie sesión en la consola de la API de Google con las credenciales de su cuenta de administrador de Google.
2. Vaya a la página Biblioteca.
3. Busque "Android Device Verification API".



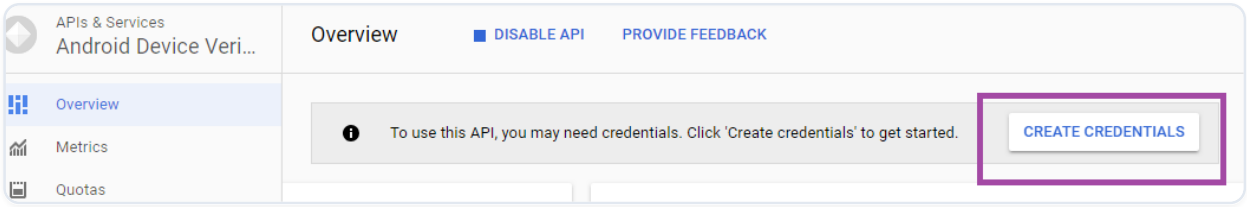
4. Haga clic en **Android Device Verification API**.



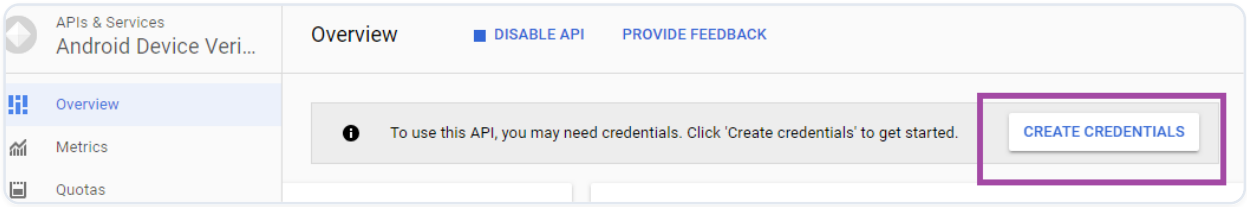
5. Si la API aún no está habilitada, haga clic en **Habilitar**.



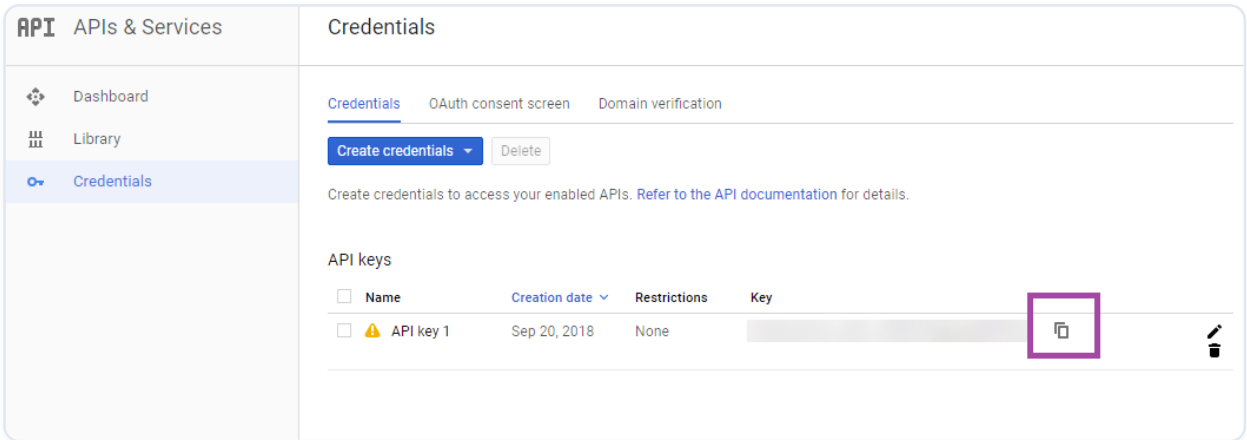
6. Haga clic en **Administrar**.
7. Haga clic en **Crear credenciales** para generar una clave de API.



8. Seleccione **Android Device Verification** y haga clic en **¿Qué credenciales necesito?**. Luego, haga clic en **Listo**.



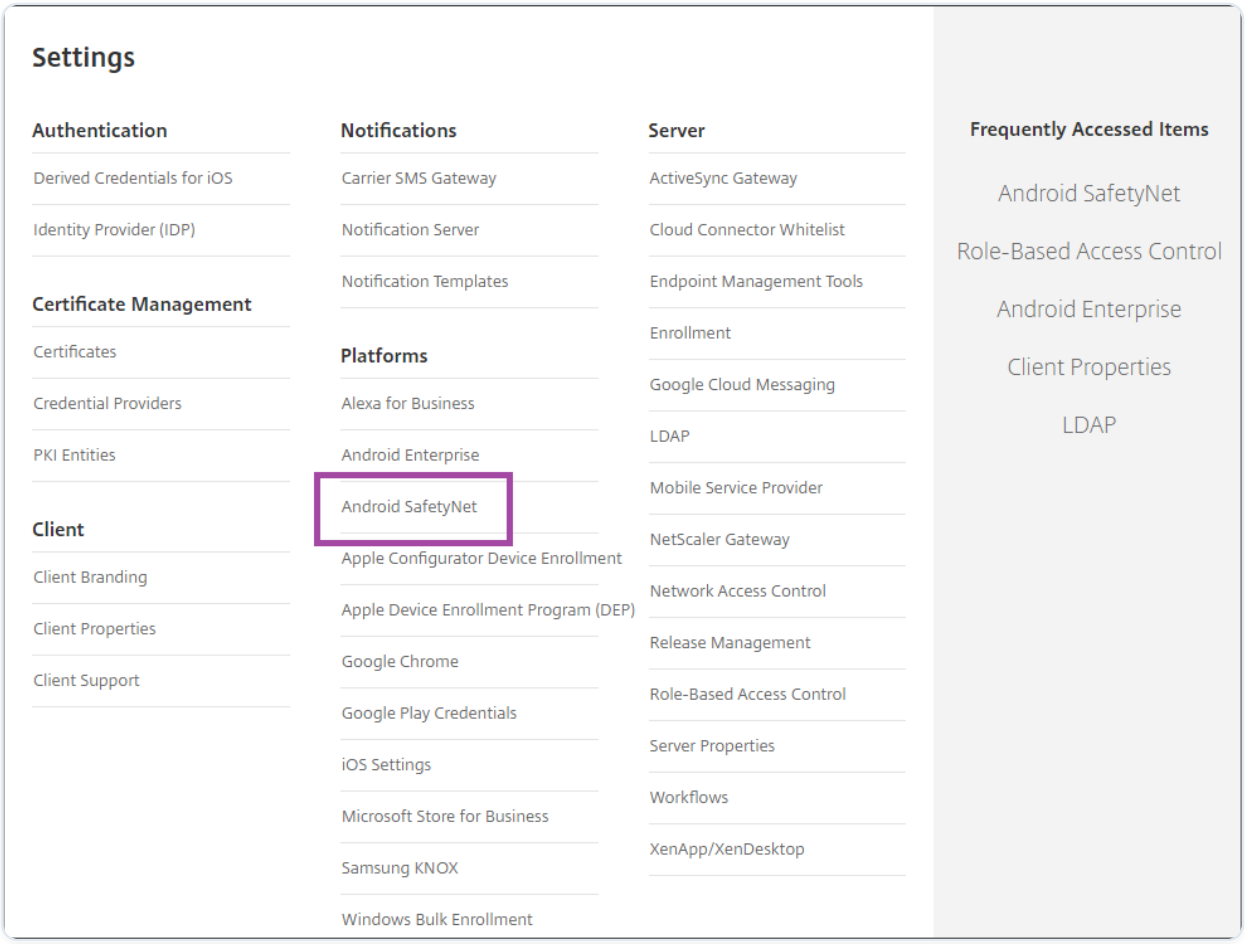
9. En la página **Credenciales**, haga clic en el icono de copiar junto a la clave para copiarla.



10. Guarde la clave para poder pegarla en la consola de Citrix Endpoint Management cuando habilite Android SafetyNet.

Habilitar Android SafetyNet

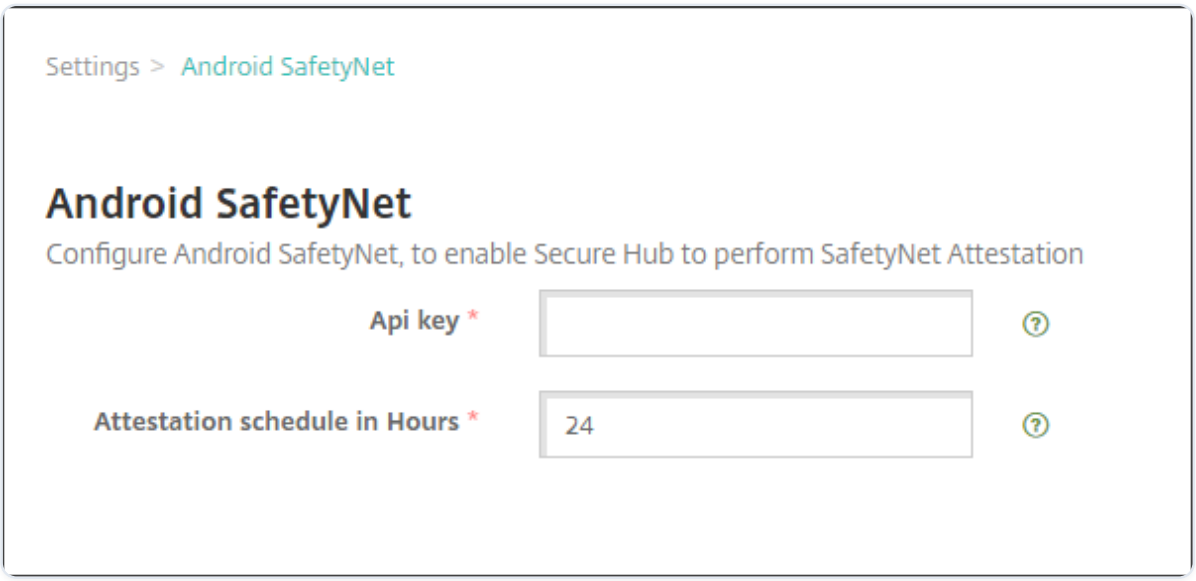
1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha. Aparecerá la página **Configuración**.
2. En la página **Configuración**, haga clic en **Android SafetyNet**.



3. Configure estos ajustes:

   - **Clave de API**. Pegue la clave de API de SafetyNet que obtuvo de la consola de la API de Google.
   - **Programación de atestación en horas**. Escriba el intervalo en el que la API de atestación de SafetyNet evalúa sus dispositivos Android, en horas. El valor mínimo es de 24 horas. El

valor máximo es de 1000 horas. El valor predeterminado es de 24 horas.

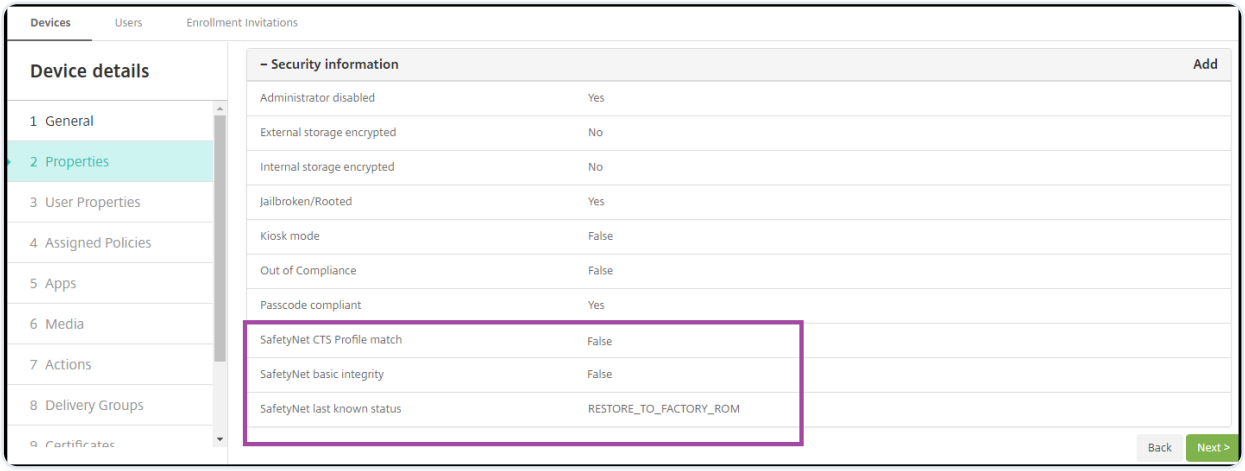


4. Haga clic en **Guardar**.

Ver los resultados de Android SafetyNet

Para ver los resultados de la evaluación de la API de atestación de SafetyNet para un dispositivo:

1. En la consola de Citrix Endpoint Management, haga clic en **Administrar > Dispositivos**.
2. Seleccione los dispositivos Android para ver los resultados de la API de atestación de SafetyNet. A continuación, haga clic en **Mostrar más**.
3. En la página **Detalles del dispositivo**, seleccione **Propiedades**.
4. Los resultados aparecen en la sección **Seguridad**.



La API de atestación de SafetyNet devuelve estos estados para cada dispositivo:

- **Coincidencia de perfil CTS de SafetyNet:** Si este valor es **True**, el dispositivo tiene un perfil que coincide con uno que ha superado la Suite de pruebas de compatibilidad de Android

(CTS). Si este valor se establece como **False**, el dispositivo no tiene un perfil que coincida con uno que haya superado la CTS de Android.

- **Integridad básica de SafetyNet:** Si este valor es **True**, la API de atestación de SafetyNet no encontró pruebas de que una fuente desconocida haya modificado Citrix Secure Hub en el dispositivo. Si este valor se establece como **False**, una fuente desconocida ha modificado Citrix Secure Hub en el dispositivo.
- **Último estado conocido de SafetyNet:** Este valor muestra el último estado conocido de SafetyNet del dispositivo:
  - **Correcto:** La API de atestación de SafetyNet no encontró pruebas de que una fuente desconocida haya modificado Citrix Secure Hub en el dispositivo.
  - **LOCK_BOOTLOADER:** El usuario debe bloquear el cargador de arranque (bootloader) del dispositivo. Una fuente desconocida ha modificado Citrix Secure Hub en el dispositivo.
  - **RESTORE_TO_FACTORY_ROM:** El usuario debe restaurar el dispositivo a una ROM de fábrica limpia. Una fuente desconocida ha modificado Citrix Secure Hub en el dispositivo.

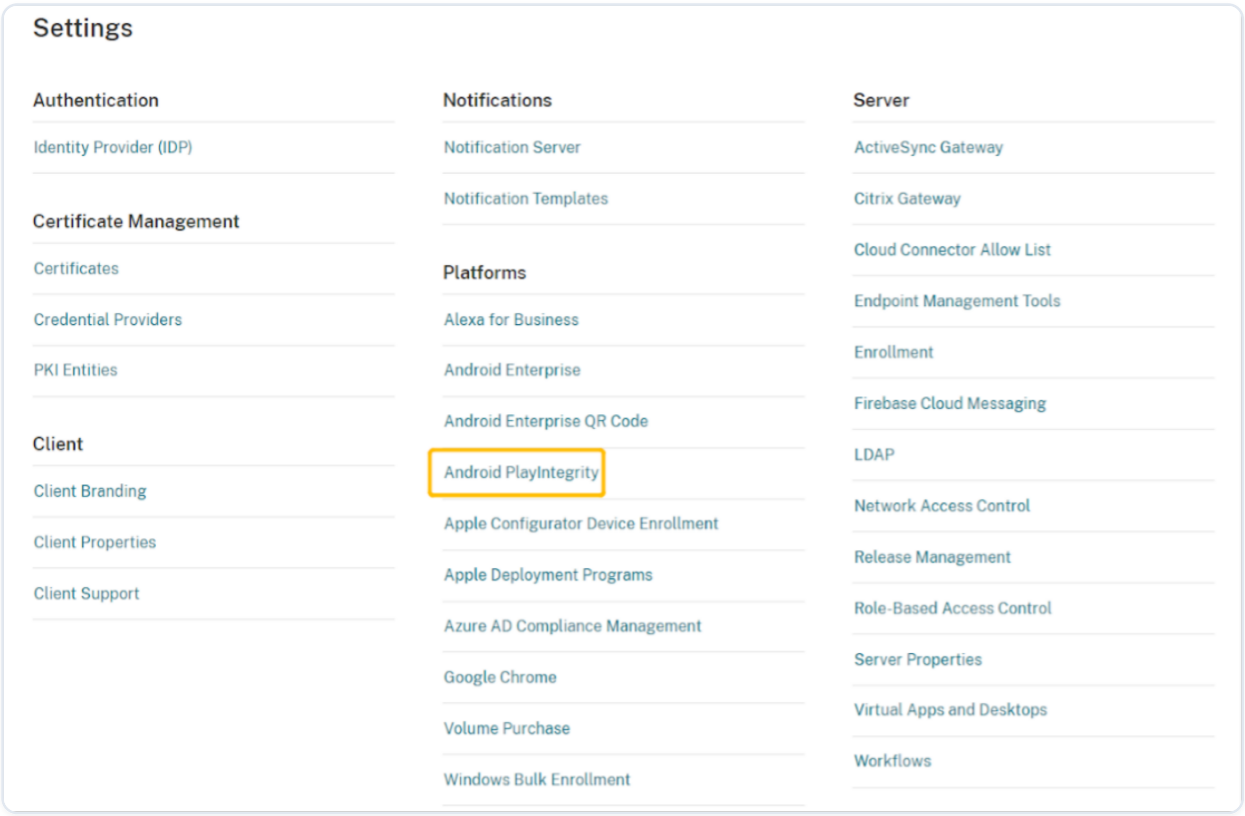
API de Play Integrity

La API de Play Integrity ayuda a proteger sus aplicaciones y juegos de interacciones potencialmente arriesgadas y fraudulentas, como trampas y accesos no autorizados, lo que le permite responder con las acciones adecuadas para prevenir ataques y reducir el abuso. Para obtener más información, consulte API de Play Integrity.

Habilitar la API de Play Integrity

Siga estos pasos para cambiar a la API de Play Integrity.

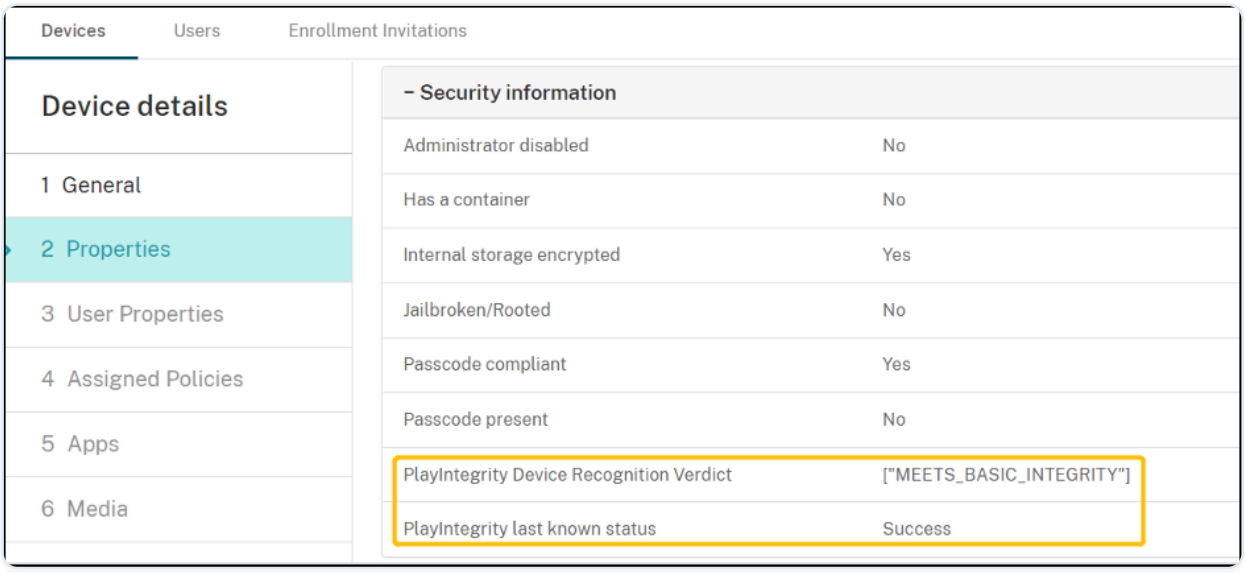
1. Active la función de indicador de obsolescencia *afw.safetynet.attestation.api.* para el servidor de Citrix Endpoint Management especificado.
2. En la consola de Citrix Endpoint Management, seleccione **Android PlayIntegrity** en la página **Configuración**.



3. Introduzca un valor en la programación de atestación en el campo de horas. Es el tiempo de intervalo en el que la API de atestación de PlayIntegrity evalúa su dispositivo. El valor mínimo es de 24 horas y el valor máximo es de 1000 horas. El valor predeterminado es de 24 horas. Haga clic en **Guardar**.
4. Actualice a Citrix Secure Hub para Android versión 23.7.0. Cierre la sesión de su dispositivo e inicie sesión en Citrix Secure Hub para activar la atestación a través de la API de Play Integrity.

Ver y analizar los resultados de la atestación de la API de Play Integrity

1. En la consola de Citrix Endpoint Management, vaya a **Administrar > Dispositivos**.
2. Seleccione el dispositivo para el que desea ver los resultados de la atestación de la API de Play Integrity. Haga clic en **Mostrar más**.
3. En la ficha **Dispositivos**, seleccione **Propiedades**. Los resultados aparecen en la sección **Información de seguridad**.



4. La atestación de la API de Play Integrity devuelve los siguientes estados:

   - Si el campo **Veredicto de reconocimiento de dispositivo de PlayIntegrity** tiene **“MEETS_BASIC_INTEGRITY”**, significa que Citrix Secure Hub que se ejecuta en el dispositivo al menos supera la integridad básica del sistema.
   - Si el campo **Veredicto de reconocimiento de dispositivo de PlayIntegrity** no tiene **“MEETS_BASIC_INTEGRITY”**, significa que Citrix Secure Hub en el dispositivo podría estar ejecutándose en una versión no reconocida de Android, podría tener un gestor de arranque desbloqueado o podría no haber sido certificado por el fabricante.
   - Si el **último estado conocido de PlayIntegrity** es **Correcto**, significa que la atestación de la API de PlayIntegrity se ha ejecutado correctamente.
   - Si el **último estado conocido de PlayIntegrity** es **Error**, significa que la atestación de la API de PlayIntegrity no se ha podido ejecutar.

Nota:

El administrador puede borrar la marca de función que le permite usar SafetyNet, antes del cierre definitivo de la atestación de SafetyNet, a finales de noviembre de 2023.

Limitaciones

1. Los dispositivos COSU y DO recién inscritos se marcan como no conformes, incluso si los dispositivos son conformes.

La API de Play Integrity devuelve un valor vacío para la primera atestación durante la inscripción de DO, lo que hace que el dispositivo parezca no conforme. Esta limitación es un problema conocido de Google. Se ha publicado DPC Support Lib 20230418 para solucionar este problema.

La solución está disponible a partir de la versión 23.9.0. Hasta entonces, utilice estos pasos como solución alternativa:

- Borre la marca de función y siga utilizando la API de SafetyNet para seguir utilizando la API de atestación de SafetyNet.
- Cierre sesión y vuelva a iniciarla para activar una atestación después de la inscripción. También puede esperar a la siguiente atestación periódica, que es la predeterminada de 24 horas.

Este problema solo ocurre durante la inscripción. La API de Play Integrity funciona correctamente después de la inscripción.

2. Los dispositivos WPCOD recién inscritos se marcan como no conformes incluso cuando los dispositivos son conformes. Google está revisando este problema.

Samsung

Samsung ofrece varias soluciones compatibles con Citrix Endpoint Management.

Para controlar cómo y cuándo los dispositivos Android se conectan al servicio de Citrix Endpoint Management, utilice Firebase Cloud Messaging (FCM). Para obtener más información, consulte Firebase Cloud Messaging.

Los perfiles de inscripción determinan si los dispositivos Android se inscriben en MAM, MDM o MDM+MAM, con la opción de que los usuarios puedan excluirse de MDM. Citrix Endpoint Management admite los siguientes tipos de autenticación para dispositivos Android inscritos en MDM+MAM. Para obtener más información, consulte los siguientes artículos:

- Autenticación de dominio o de dominio más token de seguridad
- Autenticación de certificado de cliente o de certificado más dominio
- Proveedores de identidades:
  - Autenticación con Azure Active Directory a través de Citrix Cloud
  - Autenticación con Okta a través de Citrix Cloud

Otro método de autenticación poco utilizado es un certificado de cliente más un token de seguridad. Para obtener más información, consulte `<https://support.citrix.com/article/CTX215200>`.

Un flujo de trabajo general para iniciar la administración de dispositivos Android es el siguiente:

1. Complete el proceso de incorporación. Consulte Incorporación y configuración de recursos y Preparar la inscripción de dispositivos y la entrega de recursos.
2. Elija y configure un método de inscripción. Consulte Métodos de inscripción admitidos.
3. Implementar claves de licencia de Samsung.
4. Configurar directivas de dispositivos Samsung.
5. Configure las acciones de seguridad de dispositivos y aplicaciones. Consulte Acciones de seguridad.

Para ver los sistemas operativos compatibles, consulte Sistemas operativos de dispositivos compatibles.

Métodos de inscripción admitidos

La siguiente tabla enumera los métodos de inscripción que Citrix Endpoint Management admite para dispositivos Android:

MÉTODO	COMPATIBLE
Inscripción manual	Sí
Invitaciones de inscripción	Sí

Para obtener información sobre la inscripción de dispositivos, consulte Inscribir dispositivos Android.

Implementar claves de licencia de Samsung

Samsung tiene la clave de Knox Platform Enterprise. Para obtener más información, consulte Directiva de dispositivo de clave de Knox Platform for Enterprise

Configurar directivas de dispositivo Samsung

Directivas de dispositivo:

Restricciones de aplicaciones	Desinstalación de aplicaciones	Código de acceso
Restricciones	VPN	

Acciones de seguridad

Android admite las siguientes acciones de seguridad. Para obtener una descripción de cada acción de seguridad, consulte Acciones de seguridad.

Bloqueo de app	Borrado de app	Renovación de certificados
Borrado completo	Localizar	Bloquear
Bloquear y restablecer contraseña	Notificar	Revocar
Borrado selectivo		

> **Nota:**
>
> Para los dispositivos que ejecutan Android 6.0 y versiones posteriores, la acción de seguridad **Localizar** requiere que el usuario conceda el permiso de ubicación durante la inscripción. El usuario puede optar por no conceder los permisos de ubicación. Si el usuario no concede el permiso durante la inscripción, Citrix Endpoint Management vuelve a solicitar los permisos de ubicación al enviar el comando Localizar.

Control de acceso a la red

Puede utilizar su solución de control de acceso a la red (NAC) para ampliar la evaluación de seguridad de dispositivos de Citrix Endpoint Management para dispositivos Android y Apple. Su solución NAC utiliza la evaluación de seguridad de Citrix Endpoint Management para facilitar y gestionar las decisiones de autenticación. Una vez que configure su dispositivo NAC, las directivas de dispositivo y los filtros NAC que configure en Citrix Endpoint Management se aplicarán.

El uso de Citrix Endpoint Management con una solución NAC añade QoS y un control más granular sobre los dispositivos internos de su red. Para obtener un resumen de las ventajas de integrar NAC con Citrix Endpoint Management, consulte Control de acceso.

Citrix admite estas soluciones para la integración con Citrix Endpoint Management:

- NetScaler Gateway
- ForeScout

Citrix® no garantiza la integración para otras soluciones NAC.

Con un dispositivo NAC en su red:

- Citrix Endpoint Management admite NAC como una función de seguridad de punto final para dispositivos iOS, Android Enterprise y Android.
- Puede habilitar filtros en Citrix Endpoint Management para establecer dispositivos como conformes o no conformes para NAC, según reglas o propiedades. Por ejemplo:
  - Si un dispositivo administrado en Citrix Endpoint Management no cumple los criterios especificados, Citrix Endpoint Management marca el dispositivo como no conforme. Un dispositivo NAC bloquea los dispositivos no conformes en su red.
  - Si un dispositivo administrado en Citrix Endpoint Management tiene aplicaciones no conformes instaladas, un filtro NAC puede bloquear la conexión VPN. Como resultado, un dispositivo de usuario no conforme no puede acceder a aplicaciones o sitios web a través de la VPN.
  - Si utiliza NetScaler Gateway para NAC, puede habilitar la tunelización dividida para evitar que el plug-in de NetScaler Gateway envíe tráfico de red innecesario a NetScaler Gateway. Para obtener más información sobre la tunelización dividida, consulte Configurar la tunelización dividida.

Filtros de cumplimiento de NAC admitidos

Citrix Endpoint Management admite los siguientes filtros de cumplimiento de NAC:

Dispositivos anónimos: Comprueba si un dispositivo está en modo anónimo. Esta comprobación está disponible si Citrix Endpoint Management no puede volver a autenticar al usuario cuando un dispositivo intenta volver a conectarse.

Aplicaciones prohibidas: Comprueba si un dispositivo tiene aplicaciones prohibidas, tal como se define en una directiva de acceso a aplicaciones. Para obtener más información sobre esa directiva, consulte Directivas de dispositivo de acceso a aplicaciones.

Dispositivos inactivos: Comprueba si un dispositivo está inactivo según lo definido por la configuración **Umbral de días de inactividad del dispositivo** en **Propiedades del servidor**. Para obtener más información, consulte Propiedades del servidor.

Aplicaciones obligatorias que faltan: Comprueba si a un dispositivo le faltan aplicaciones obligatorias, tal como se define en una directiva de acceso a aplicaciones.

Aplicaciones no sugeridas: Comprueba si un dispositivo tiene aplicaciones no sugeridas, tal como se define en una directiva de acceso a aplicaciones.

Contraseña no conforme: Comprueba si la contraseña del usuario es conforme. En dispositivos iOS y Android, Citrix Endpoint Management puede determinar si la contraseña actual del dispositivo cumple con la directiva de código de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para establecer una contraseña si Citrix Endpoint Management envía una directiva de código de acceso al dispositivo. Antes de que el usuario establezca la contraseña, el código de acceso podría no ser conforme.

Dispositivos no conformes: Comprueba si un dispositivo no es conforme, basándose en la propiedad de dispositivo No conforme. Normalmente, las acciones automatizadas o terceros que utilizan las API de Citrix Endpoint Management cambian esa propiedad.

Estado revocado: Comprueba si el certificado del dispositivo está revocado. Un dispositivo revocado no puede volver a inscribirse hasta que se autorice de nuevo.

Dispositivos Android rooteados y iOS con jailbreak: Comprueba si un dispositivo Android o iOS tiene jailbreak.

Dispositivos no administrados: Comprueba si Citrix Endpoint Management está administrando un dispositivo. Por ejemplo, un dispositivo inscrito en MAM o un dispositivo no inscrito no se administra.

> **Nota:**
>
> El filtro Implícitamente conforme/No conforme establece el valor predeterminado solo en los dispositivos que administra Citrix Endpoint Management. Por ejemplo, cualquier dispositivo que tenga una aplicación bloqueada instalada o que no esté inscrito, se marca como No conforme. El dispositivo NAC bloquea esos dispositivos de su red.

Información general de la configuración

Recomendamos configurar los componentes de NAC en el orden indicado.

1. Configurar directivas de dispositivo para admitir NAC:

   Para dispositivos iOS: Consulte Configurar la directiva de dispositivo VPN para admitir NAC.

   Para dispositivos Android Enterprise: Consulte Crear una configuración administrada de Android Enterprise para Citrix SSO.

   Para dispositivos Android: Consulte Configurar el protocolo Citrix SSO para Android.

2. Habilitar filtros NAC en Citrix Endpoint Management.
3. Configure una solución NAC:

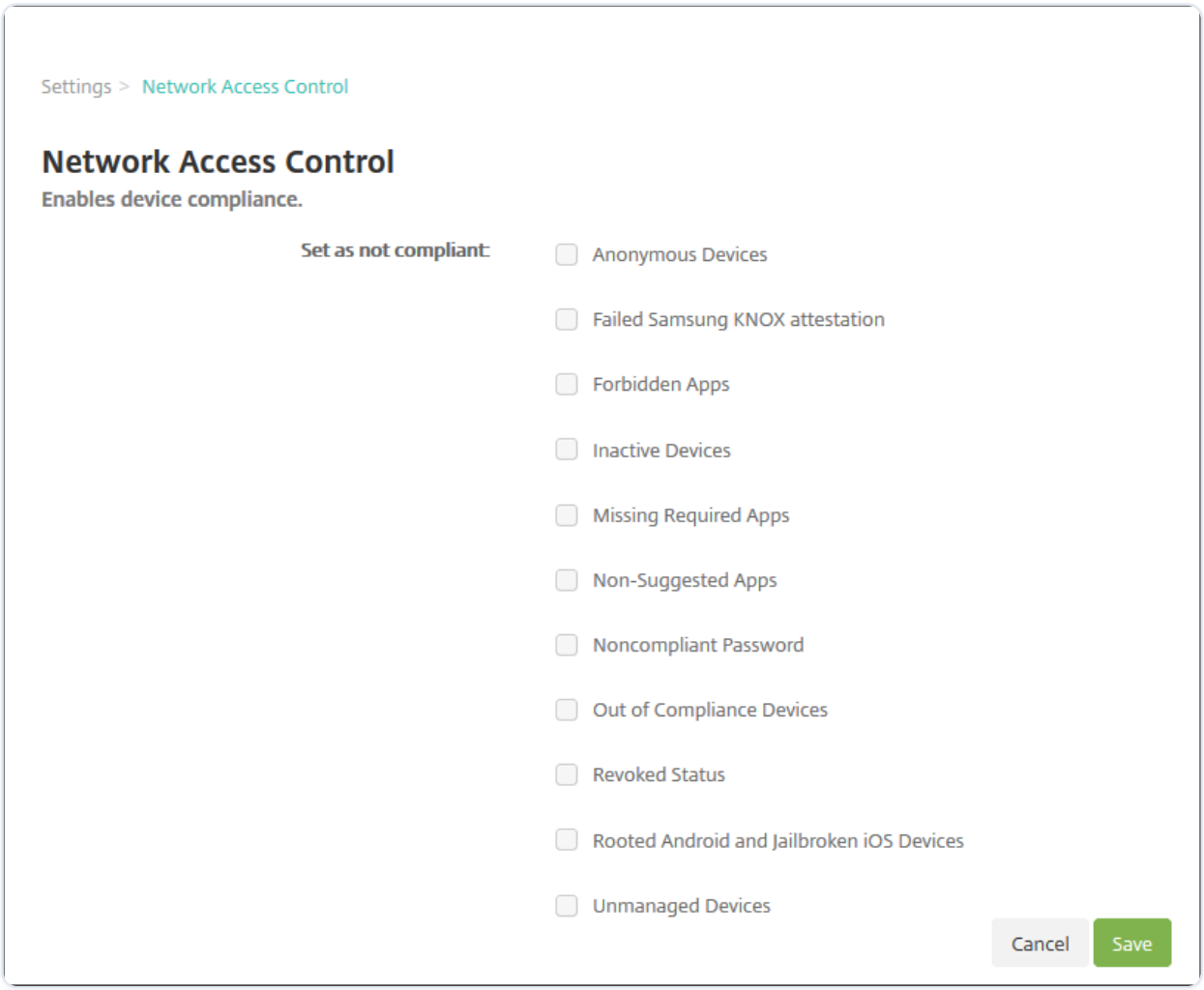
   - NetScaler Gateway, detallado en Actualizar las directivas de NetScaler Gateway para admitir NAC.

     Requiere que instale Citrix SSO en los dispositivos. Consulte Clientes de NetScaler Gateway.

   - ForeScout: Consulte la documentación de ForeScout.

Habilitar filtros NAC en Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Control de acceso a la red**.



2. Seleccione las casillas de verificación de los filtros **Establecer como no compatible** que quiera habilitar.
3. Haga clic en **Guardar**.

Actualizar las directivas de NetScaler Gateway para admitir NAC

Debe configurar directivas avanzadas (no clásicas) de autenticación y sesiones VPN en su servidor virtual VPN.

Estos pasos actualizan un NetScaler Gateway con cualquiera de estas características:

- Está integrado con Citrix Endpoint Management.
- O bien, está configurado para VPN, no forma parte del entorno de Citrix Endpoint Management y puede acceder a Citrix Endpoint Management.

En su servidor VPN virtual, desde una ventana de consola, haga lo siguiente. Los FQDN y las direcciones IP de los comandos y ejemplos son ficticios.

1. Si utiliza directivas clásicas en su servidor virtual VPN, elimine y desvincule todas las directivas clásicas. Para comprobarlo, escriba:

   `show vpn vserver <VPN_VServer>`

   Elimine cualquier resultado que contenga la palabra **Classic**. Por ejemplo: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

   Para eliminar la directiva, escriba:

   `unbind vpn vserver <VPN_VServer> -policy <policy_name>`
2. Cree la directiva de sesión avanzada correspondiente escribiendo lo siguiente.

   `add vpn sessionPolicy <policy_name> <rule> <session action>`

   Por ejemplo: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`
3. Vincule la directiva a su servidor virtual VPN escribiendo lo siguiente.

   `bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100`
4. Cree un servidor virtual de autenticación escribiendo lo siguiente.

   `add authentication vserver <authentication vserver name> <service type> <ip address>`

   Por ejemplo: `add authentication vserver authvs SSL 0.0.0.0` En el ejemplo, `0.0.0.0` significa que el servidor virtual de autenticación no está expuesto al público.
5. Enlace un certificado SSL con el servidor virtual escribiendo lo siguiente.

   `bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>`

   Por ejemplo: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`
6. Asocie un perfil de autenticación al servidor virtual de autenticación desde el servidor virtual VPN. Primero, cree el perfil de autenticación escribiendo lo siguiente.

   `add authentication authnProfile <profile name> -authnVsName <authentication vserver name>`

   Por ejemplo:

   `add authentication authnProfile xm_nac_prof -authnVsName authvs`

7. Asocie el perfil de autenticación con el servidor virtual VPN escribiendo lo siguiente.

   ```
   set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
   ```

   Por ejemplo:

   ```
   set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof
   ```

8. Compruebe la conexión de NetScaler Gateway a un dispositivo escribiendo lo siguiente.

   ```
   curl -v -k https://<Endpoint Management_server>:4443/Citrix/Device/v1/Check
   --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
   ```

   Por ejemplo, esta consulta verifica la conectividad obteniendo el estado de cumplimiento del primer dispositivo (`deviceid_1`) inscrito en el entorno:

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-
   VPN-Device-ID: deviceid_1"
   ```

   Un resultado correcto es similar al siguiente ejemplo.

   ```
   HTTP/1.1 200 OK

   < Server: Apache-Coyote/1.1

   < X-Citrix-Device-State: Non Compliant

   < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   ```

9. Cuando el paso anterior se realice correctamente, cree la acción de autenticación web para Citrix Endpoint Management. Primero, cree una expresión de directiva para extraer el ID del dispositivo del complemento VPN de iOS. Escriba lo siguiente.

   ```
   add policy expression xm_deviceid_expression
   "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\',
   \'&\').VALUE(\"deviceidvalue\")"
   ```

10. Envíe la solicitud a Citrix Endpoint Management escribiendo lo siguiente. En este ejemplo, la IP de Citrix Endpoint Management es `10.207.87.82` y el FQDN es `example.em.cloud.com:4443` .

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort
    4443 -fullReqExpr q{"GET /Citrix/Device/v1/Check HTTP/1.1\r\n" + "Host:
    ```

`example.em.cloud.com:4443\r\n" + "X-Citrix-VPN-Device-ID: " + xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.RES.STATUS.EQ(\"200\") &&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ(\"Compliant\")"`

La salida correcta para el NAC de Citrix Endpoint Management es `HTTP status 200 OK`. El encabezado `X-Citrix-Device-State` debe tener el valor de `Compliant`.

11. Cree una directiva de autenticación con la que asociar la acción escribiendo lo siguiente.

    `add authentication Policy <policy name> -rule <rule> -action <web authentication action>`

    Por ejemplo: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")" -action xm_nac`

12. Convierta la directiva LDAP existente en una directiva avanzada escribiendo lo siguiente.

    `add authentication Policy <policy_name> -rule <rule> -action <LDAP action name>`

    Por ejemplo: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. Agregue una etiqueta de directiva con la que asociar la directiva LDAP escribiendo lo siguiente.

    `add authentication policylabel <policy_label_name>`

    Por ejemplo: `add authentication policylabel ldap_pol_label`

14. Asocie la directiva LDAP a la etiqueta de directiva escribiendo lo siguiente.

    `bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT`

15. Conecte un dispositivo compatible para realizar una prueba de NAC y confirmar la autenticación LDAP correcta. Escriba lo siguiente.

    `bind authentication vserver <authentication vserver> -policy <web authentication policy> -priority 100 -nextFactor <ldap policy label> -gotoPriorityExpression END`

16. Agregue la interfaz de usuario para asociarla con el servidor virtual de autenticación. Escriba el siguiente comando para recuperar el ID del dispositivo.

`add authentication loginSchemaPolicy <schema policy>-rule <rule> -action lschema_single_factor_deviceid`

17. Enlace el servidor virtual de autenticación escribiendo lo siguiente.

    `bind authentication vserver authvs -policy lschema_xm_nac_pol -priority 100 -gotoPriorityExpression END`

18. Cree una directiva de autenticación avanzada LDAP para habilitar la conexión de Citrix Secure Hub. Escriba lo siguiente.

    `add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\").NOT" -action 10.200.80.60_LDAP`

    `bind authentication vserver authvs -policy ldap_xm_test_pol -priority 110 -gotoPriorityExpression NEXT`

Apple

iOS

Para gestionar dispositivos iOS en Citrix Endpoint Management, debe configurar un certificado del servicio de notificaciones push de Apple (APNs) de Apple. Para obtener información, consulte Certificados APNs.

Los perfiles de inscripción determinan si los dispositivos iOS se inscriben en MDM+MAM, con la opción de que los usuarios puedan inhabilitar la administración de dispositivos móviles (MDM). Citrix Endpoint Management admite los siguientes tipos de autenticación para dispositivos iOS en MDM+MAM. Para obtener información, consulte los siguientes artículos:

- Autenticación de dominio o de dominio más token de seguridad
- Autenticación de certificado de cliente o de certificado más dominio
- Proveedores de identidades:
  - Autenticación con Azure Active Directory a través de Citrix Cloud
  - Autenticación con Okta a través de Citrix Cloud

Requisitos para certificados de confianza en iOS 13:

> Apple tiene nuevos requisitos para los certificados de servidor TLS. verificar que todos los certificados cumplen los nuevos requisitos de Apple. Consulte la publicación de Apple, `<https://support.apple.com/es-es/HT210176>`. Para obtener ayuda con la administración de certificados, consulte Cargar certificados.

> Un flujo de trabajo general para iniciar la administración de dispositivos iOS es el siguiente:

1. Complete el proceso de incorporación. Consulte Incorporación y configuración de recursos y Preparar la inscripción de dispositivos y la entrega de recursos.
2. Elija y configure un método de inscripción. Consulte Métodos de inscripción admitidos.
3. Configurar directivas de dispositivos iOS.
4. Inscribir dispositivos iOS.
5. Configure acciones de seguridad de dispositivos y aplicaciones. Consulte Acciones de seguridad.

Para ver los sistemas operativos compatibles, consulte Sistemas operativos de dispositivos compatibles.

Compatibilidad con iOS 14

Citrix Endpoint Management y las aplicaciones móviles de Citrix son compatibles con iOS 14, pero actualmente no admiten las nuevas funciones de iOS 14.

Para los dispositivos iOS supervisados, puede posponer las actualizaciones de software hasta 90 días. En la directiva de restricciones de dispositivos para iOS, utilice estas configuraciones:

- **Forzar actualizaciones de software retrasadas**
- **Aplicar retraso en la actualización de software**

Consulte Configuración de iOS. Esas configuraciones no están disponibles para dispositivos en modo de inscripción de usuario o en modo no supervisado (MDM completo).

Nombres de host de Apple que deben permanecer abiertos

Algunos nombres de host de Apple deben estar abiertos para garantizar el correcto funcionamiento de iOS, macOS y Apple App Store. Bloquear esos nombres de host puede afectar la instalación, actualización y el correcto funcionamiento de lo siguiente: iOS, aplicaciones de iOS, el funcionamiento de MDM y la inscripción de dispositivos y aplicaciones. Para obtener más información, consulte `<https://support.apple.com/es-es/HT201999>`.

Métodos de inscripción compatibles

Usted especifica cómo administrar los dispositivos iOS en los perfiles de inscripción. Puede elegir entre las siguientes configuraciones de inscripción:

- **Inscripción de usuario de Apple:** Para dispositivos BYOD, ofrece un equilibrio entre la privacidad de los datos personales y la seguridad de los datos corporativos. Este modo de inscripción está disponible como vista previa pública. Para habilitar esta función, póngase en contacto con su equipo de soporte.
- **Inscripción de dispositivos de Apple:** Para dispositivos iOS supervisados, con perfiles personales y corporativos separados en el dispositivo.
- **No administrar dispositivos:** Excluya estos dispositivos de MDM si solo desea administrar aplicaciones.

Para obtener más información sobre la creación de perfiles de inscripción, consulte Perfiles de inscripción.

Citrix Endpoint Management admite los siguientes métodos de inscripción para dispositivos iOS:

MÉTODO	COMPATIBLE
Apple Business Manager	Sí
Apple School Manager	Sí
Apple Configurator	Sí
Inscripción manual	Sí
Invitaciones de inscripción	Sí

Los programas de implementación de Apple incluyen Apple Business Manager (ABM) para organizaciones empresariales y Apple School Manager (ASM) para organizaciones educativas. Para obtener más información, consulte Implementar dispositivos a través de los programas de implementación de Apple.

Apple School Manager es un tipo de Programa de implementación de Apple para educación. Consulte Integrar con las funciones de Apple Education.

Utilice los programas de implementación de Apple para inscribir dispositivos iOS, iPadOS y macOS de forma masiva. Puede comprar esos dispositivos directamente a Apple, a un distribuidor autorizado de Apple participante o a un operador. Tanto si compra dispositivos iOS directamente a

Apple como si no, puede utilizar Apple Configurator para inscribir esos dispositivos. Consulte Inscribir dispositivos Apple de forma masiva.

ID de Apple gestionados

La inscripción de usuarios se integra estrechamente con los ID de Apple gestionados. Puede crear un ID de Apple gestionado manualmente mediante ABM/ASM o dinámicamente con Azure Active Directory (AAD).

Para la autenticación no federada, cree ID de Apple gestionados mediante ABM/ASM para añadir una cuenta. Para obtener información sobre cómo añadir una cuenta en ABM/ASM, consulte la documentación de Apple en `https://support.apple.com/guide/apple-business-manager/welcome/web` y ASM en `https://support.apple.com/guide/apple-school-manager/welcome/web`. Recomendamos lo siguiente para evitar pasos adicionales cuando los usuarios se inscriban:

- Utilice un correo electrónico que coincida con la dirección de correo electrónico corporativa al crear un ID de Apple gestionado.
- Establezca el rol de usuario en **Personal**.
- Pida a los usuarios que cambien manualmente su contraseña antes de inscribirse. Informe a los usuarios de que recomendamos que utilicen la misma contraseña que la de la cuenta corporativa.

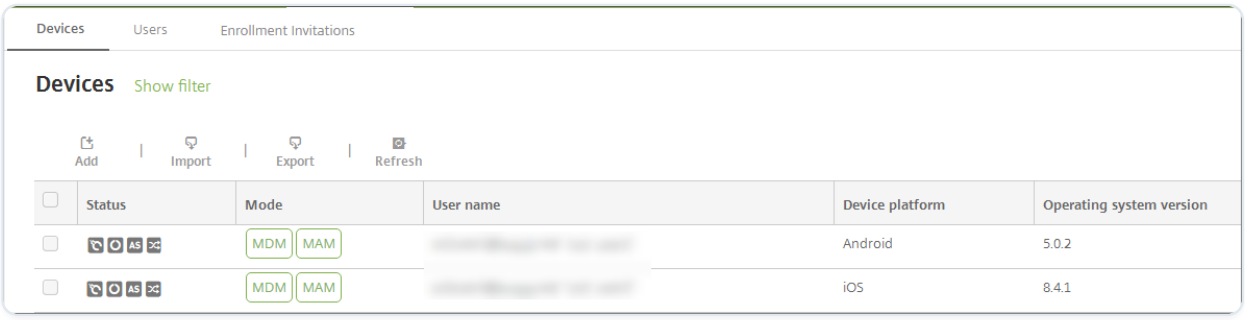
Para crear ID de Apple gestionados dinámicamente, configure Citrix Cloud para que utilice AAD como su proveedor de identidades. Para obtener más información sobre cómo configurar Citrix Cloud para que utilice AAD, consulte Autenticación con Azure Active Directory a través de Citrix Cloud. Además, configure la autenticación federada en ABM/ASM. Para obtener más información sobre cómo configurar la autenticación federada en ABM o ASM, consulte la Guía del usuario de Apple Business Manager y la Guía del usuario de Apple School Manager.

Cuando crea ID de Apple gestionados manualmente, puede configurar un dominio personalizado para usarlo en lugar del dominio predeterminado. El dominio personalizado que configure reemplaza al dominio existente. Por ejemplo, sus direcciones de correo electrónico corporativas siguen el formato `first.last@company.com`, pero en su lugar desea usar `mycompany.website.com` como dominio para el ID de Apple gestionado. Al crear el ID de Apple gestionado en ABM/ASM, la dirección de correo electrónico se convierte en `first.last@mycompany.website.com`.

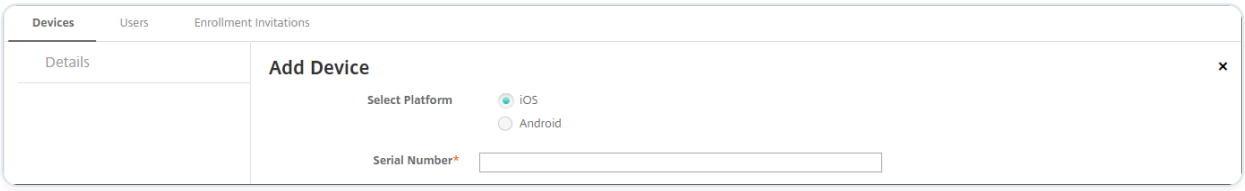
Añadir un dispositivo iOS manualmente

Si desea añadir un dispositivo iOS manualmente, por ejemplo, para fines de prueba, siga estos pasos.

1. En la consola de Citrix Endpoint Management, haga clic en **Administrar > Dispositivos**. Aparecerá la página **Dispositivos**.



2. Haga clic en **Agregar**. Aparecerá la página **Agregar dispositivo**.



3. Configure estos ajustes:

   - **Seleccionar plataforma:** Haga clic en **iOS**.
   - **Número de serie:** Escriba el número de serie del dispositivo.

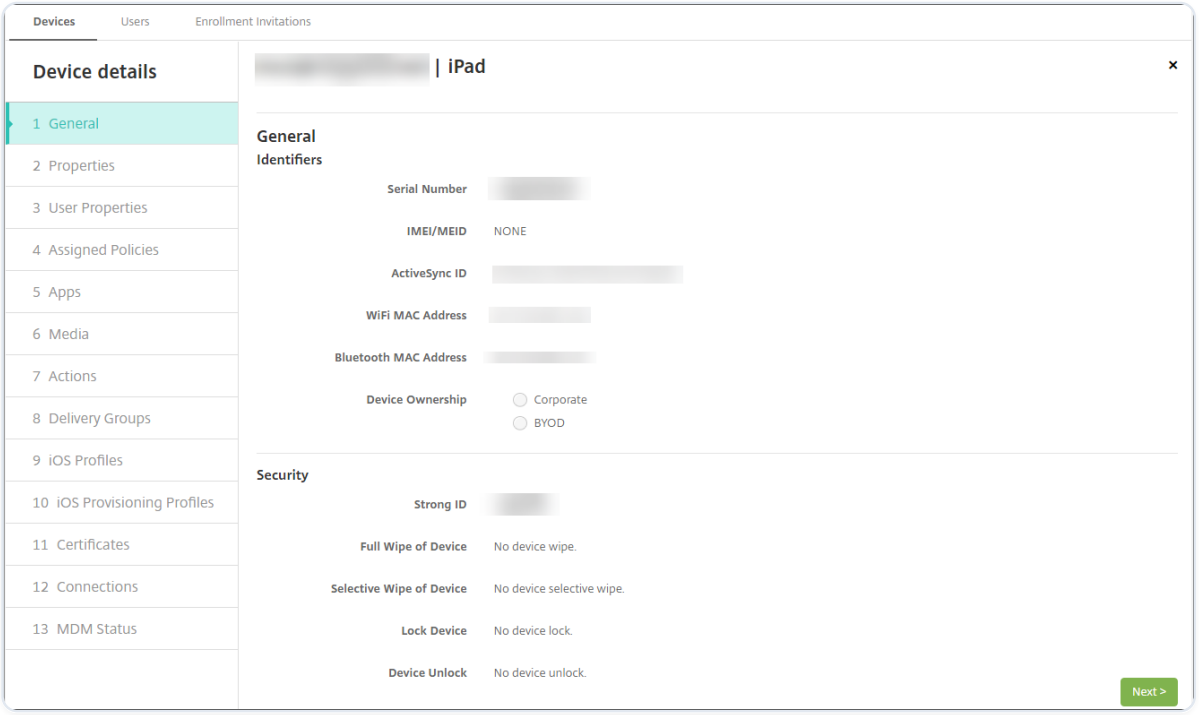
4. Haga clic en **Añadir**. La tabla **Dispositivos** aparece con el dispositivo añadido al final de la lista. Para ver y confirmar los detalles del dispositivo: Elija el dispositivo que ha añadido y, a continuación, en el menú que aparece, haga clic en **Modificar**.

> **Nota:**
>
> Al seleccionar la casilla de verificación junto a un dispositivo, el menú de opciones aparece encima de la lista de dispositivos. Si hace clic en cualquier otra parte de la lista, el menú de opciones aparece en el lado derecho de la lista.

   - LDAP configurado
   - Si utiliza grupos locales y usuarios locales:
     - Uno o varios grupos locales.

- Usuarios locales asignados a grupos locales.
- Los grupos de entrega están asociados a grupos locales.

- Si utiliza Active Directory:
  - Los grupos de entrega están asociados a grupos de Active Directory.



5. La página **General** enumera los **Identificadores** del dispositivo, como el número de serie y otra información para el tipo de plataforma. Para **Propiedad del dispositivo**, seleccione **Corporativo** o **BYOD**.

   La página **General** también enumera las propiedades de **Seguridad** del dispositivo, como ID seguro, Bloquear dispositivo, Omisión de bloqueo de activación y otra información para el tipo de plataforma. El campo **Borrado completo del dispositivo** incluye el código PIN del usuario. El usuario debe introducir ese código después de borrar el dispositivo. Si el usuario olvida el código, puede consultarlo aquí.

6. La página **Propiedades** enumera las propiedades del dispositivo que Citrix Endpoint Management aprovisiona. Esta lista muestra las propiedades del dispositivo incluidas en el archivo de aprovisionamiento utilizado para añadir el dispositivo. Para añadir una propiedad, haga clic en **Agregar** y, a continuación, seleccione una propiedad de la lista. Para ver los valores válidos de cada propiedad, consulte el PDF Nombres y valores de las propiedades del dispositivo.

Cuando añade una propiedad, aparece inicialmente en la categoría donde la añadió. Después de hacer clic en **Siguiente** y volver a la página **Propiedades**, la propiedad aparece en la lista correspondiente.

Para eliminar una propiedad, pase el ratón por encima de la entrada y, a continuación, haga clic en la **X** del lado derecho. Citrix Endpoint Management elimina el elemento inmediatamente.

7. Las secciones restantes de **Detalles del dispositivo** contienen resúmenes del dispositivo.

   - **Propiedades de usuario:** Muestra los roles RBAC, las pertenencias a grupos, las cuentas de compra por volumen y las propiedades del usuario. Puede retirar una cuenta de compra por volumen desde esta página.
   - **Directivas asignadas:** Muestra el número de directivas implementadas, pendientes y fallidas. Proporciona el nombre, el tipo y la información de la última implementación de cada directiva. Permite restablecer el estado de implementación a pendiente y volver a implementar las directivas que el usuario eliminó.
   - **Aplicaciones:** Muestra, para el último inventario, el número de implementaciones de aplicaciones instaladas, pendientes y fallidas. Proporciona el nombre, el identificador, el tipo y otra información de la aplicación. Para obtener una descripción de las claves de inventario de iOS y macOS, como **HasUpdateAvailable**, consulte Protocolo de administración de dispositivos móviles (MDM).
   - **Contenido multimedia:** Muestra, para el último inventario, el número de implementaciones de contenido multimedia implementadas, pendientes y fallidas.
   - **Acciones:** Muestra el número de acciones implementadas, pendientes y fallidas. Proporciona el nombre de la acción y la hora de la última implementación.
   - **Grupos de entrega:** Muestra el número de grupos de entrega correctos, pendientes y fallidos. Para cada implementación, proporciona el nombre del grupo de entrega y la hora de implementación. Seleccione un grupo de entrega para ver información más detallada, incluido el estado, la acción y el canal o usuario.
   - **Perfiles de iOS:** Muestra el último inventario de perfiles de iOS, incluidos el nombre, el tipo, la organización y la descripción.
   - **Perfiles de aprovisionamiento de iOS:** Muestra información del perfil de aprovisionamiento de distribución empresarial, como el UUID, la fecha de caducidad y el estado administrado.

- **Certificados:** Muestra, para los certificados válidos, caducados o revocados, información como el tipo, el proveedor, el emisor, el número de serie y el número de días restantes antes de la caducidad.
- **Conexiones:** Muestra el estado de la primera conexión y el estado de la última conexión. Proporciona para cada conexión, el nombre de usuario, la penúltima (anterior a la última) hora de autenticación y la última hora de autenticación.
- **Estado de MDM:** Muestra información como el estado de MDM, la hora del último envío y la hora de la última respuesta del dispositivo.

Configurar directivas de dispositivos iOS

Utilice estas directivas para configurar cómo Citrix Endpoint Management interactúa con los dispositivos que ejecutan iOS o iPadOS. Esta tabla enumera todas las directivas de dispositivos disponibles para dispositivos iOS y iPadOS.

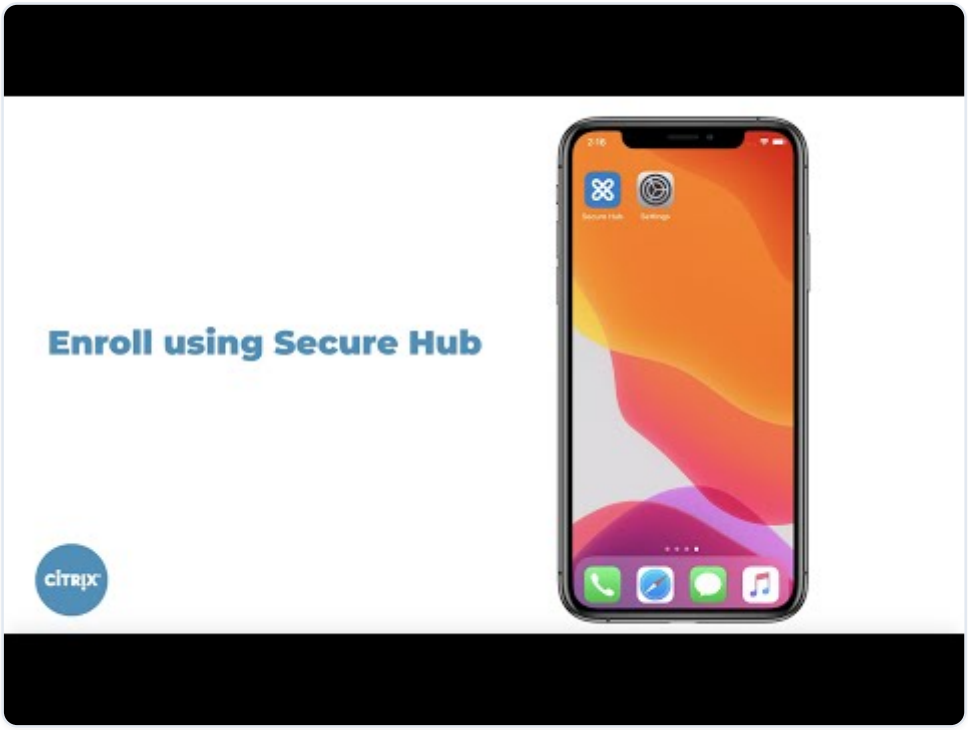
Duplicación de AirPlay	AirPrint	APN	
Acceso a aplicaciones	Atributos de aplicaciones	Configuración de aplicaciones	
Inventario de aplicaciones	Bloqueo de aplicaciones	Desinstalación de aplicaciones	
Notificaciones de aplicaciones	Bluetooth	Calendario (CalDAV)	
Móvil	Contactos (CardDAV)	Credenciales	
Nombre del dispositivo	Configuración educativa	Exchange	
Fuente	Diseño de la pantalla de inicio	Importar perfil de iOS y macOS	
LDAP	Ubicación	Mensaje de la pantalla de bloqueo	
Correo	Dominios administrados	Usuarios residentes máximos(/es-es/	

		citrix-endpoint-management/policies/maximum-resident-users-policy.html)	
Opciones de MDM(/es-es/citrix-endpoint-management/policies/mdm-options-policy.html)	Red(/es-es/citrix-endpoint-management/policies/network-policy.html#ios-settings)	Uso de red(/es-es/citrix-endpoint-management/policies/network-usage-policy.html)	
Información de la organización(/es-es/citrix-endpoint-management/policies/organization-info-policy.html)	Actualización del SO(/es-es/citrix-endpoint-management/policies/control-os-updates.html#ios-settings)	Código de acceso(/es-es/citrix-endpoint-management/policies/passcode-policy.html#ios-settings)	
Período de gracia de bloqueo por código de acceso(/es-es/citrix-endpoint-management/policies/passcode-lock-grace-period.html)	Punto de acceso personal(/es-es/citrix-endpoint-management/policies/personal-hotspot-policy.html)	Eliminación de perfil(/es-es/citrix-endpoint-management/policies/profile-removal-policy.html)	
Perfil de aprovisionamiento(/es-es/citrix-endpoint-management/policies/provisioning-profile-policy.html)	Eliminación de perfil de aprovisionamiento(/es-es/citrix-endpoint-management/policies/provisioning-profile-removal-policy.html)	Proxy(/es-es/citrix-endpoint-management/policies/proxy-policy.html)	
Restricciones(/es-es/citrix-endpoint-management/	Itinerancia(/es-es/citrix-endpoint-management/	SCEP	

policies/restrictions-policy.html#ios-settings)	policies/roaming-policy.html)		
Cuenta SSO	Tienda	Calendarios suscritos	
Términos y condiciones	VPN	Fondo de pantalla	
Filtro de contenido web	Clip web		

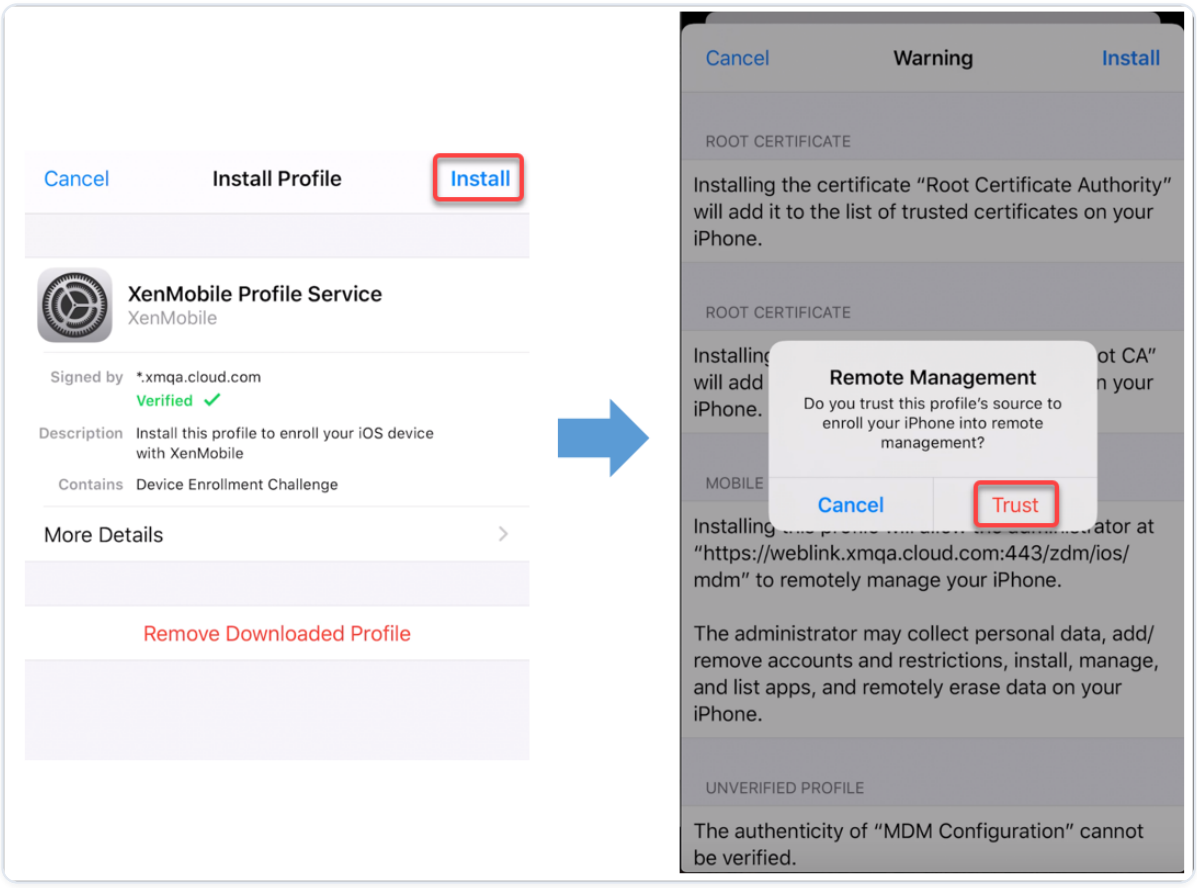
Inscribir dispositivos iOS

Esta sección muestra cómo los usuarios inscriben dispositivos iOS (12.2 o posterior) en Citrix Endpoint Management. Para obtener más información sobre la inscripción de iOS, vea el siguiente vídeo:



1. Vaya a la App Store en su dispositivo iOS, descargue la aplicación Citrix Secure Hub y, a continuación, toque la aplicación.
2. Cuando se le pida que instale la aplicación, toque **Siguiente** y, a continuación, toque **Instalar**.
3. Una vez instalada la aplicación Citrix Secure Hub, toque **Abrir**.

4. Introduzca sus credenciales corporativas, como el nombre de su servidor Citrix Endpoint Management, el nombre principal de usuario (UPN) o la dirección de correo electrónico. A continuación, haga clic en **Siguiente**.
5. Toque **Sí, inscribir** para inscribir su dispositivo iOS.
6. Aparece una lista de los datos que recopila Citrix Endpoint Management. Haga clic en **Siguiente**. Aparece una explicación de cómo una organización utiliza esos datos. Haga clic en **Siguiente**.
7. Después de escribir sus credenciales, toque **Permitir** cuando se le solicite, para descargar el perfil de configuración. Después de descargar el perfil de configuración, toque **Cerrar**.
8. En la configuración de su dispositivo, instale el perfil de XenMobile®.
    - Vaya a **Ajustes > General > Perfil > Servicio de perfiles de XenMobile** y toque **Instalar** para añadir el perfil.
    - En la ventana de notificación, toque **Confiar** para inscribir su dispositivo en la administración remota.



9. Una vez que la inscripción se realice correctamente, abra Citrix Secure Hub. Si se está inscribiendo en MDM+MAM: Después de que sus credenciales se validen, cree y confirme su PIN de Citrix cuando se le solicite.

10. Una vez completado el flujo de trabajo, el dispositivo estará inscrito. A continuación, puede acceder a la tienda de aplicaciones para ver las aplicaciones que puede instalar en su dispositivo iOS.

Acciones de seguridad

La inscripción de dispositivos iOS admite las siguientes acciones de seguridad. Para obtener una descripción de cada acción de seguridad, consulte Acciones de seguridad.

- Omisión de bloqueo de activación
- Bloqueo de apps
- Borrado de apps
- Bloqueo de activación de ASM
- Renovación de certificados
- Borrar restricciones
- Habilitar/Deshabilitar modo perdido
- Habilitar/Deshabilitar seguimiento
- Borrado completo
- Localizar
- Bloquear
- Hacer sonar
- Solicitar/Detener duplicación de AirPlay
- Reiniciar/Apagar
- Revocar/Autorizar
- Borrado selectivo
- Desbloquear

La inscripción de usuarios para iOS admite las siguientes acciones de seguridad:

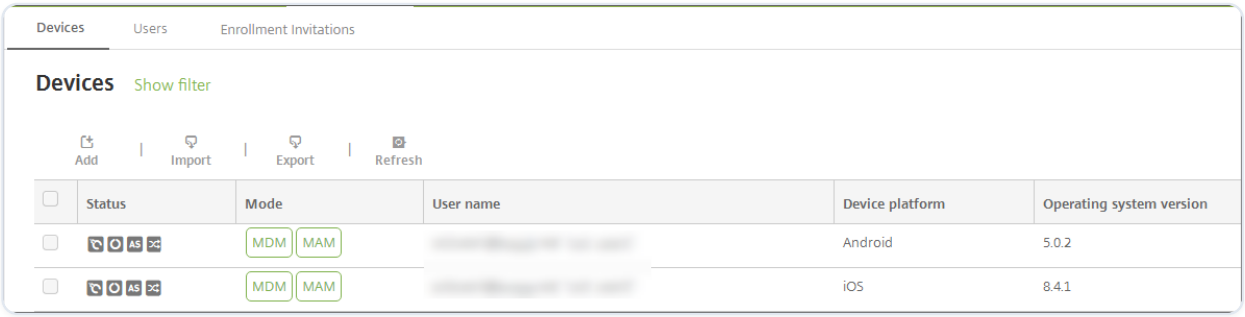
- Revocar
- Bloquear
- Borrado selectivo
- Renovación de certificado

Bloquear dispositivos iOS

Puede bloquear un dispositivo iOS perdido con un mensaje y un número de teléfono que se muestran en la pantalla de bloqueo del dispositivo.

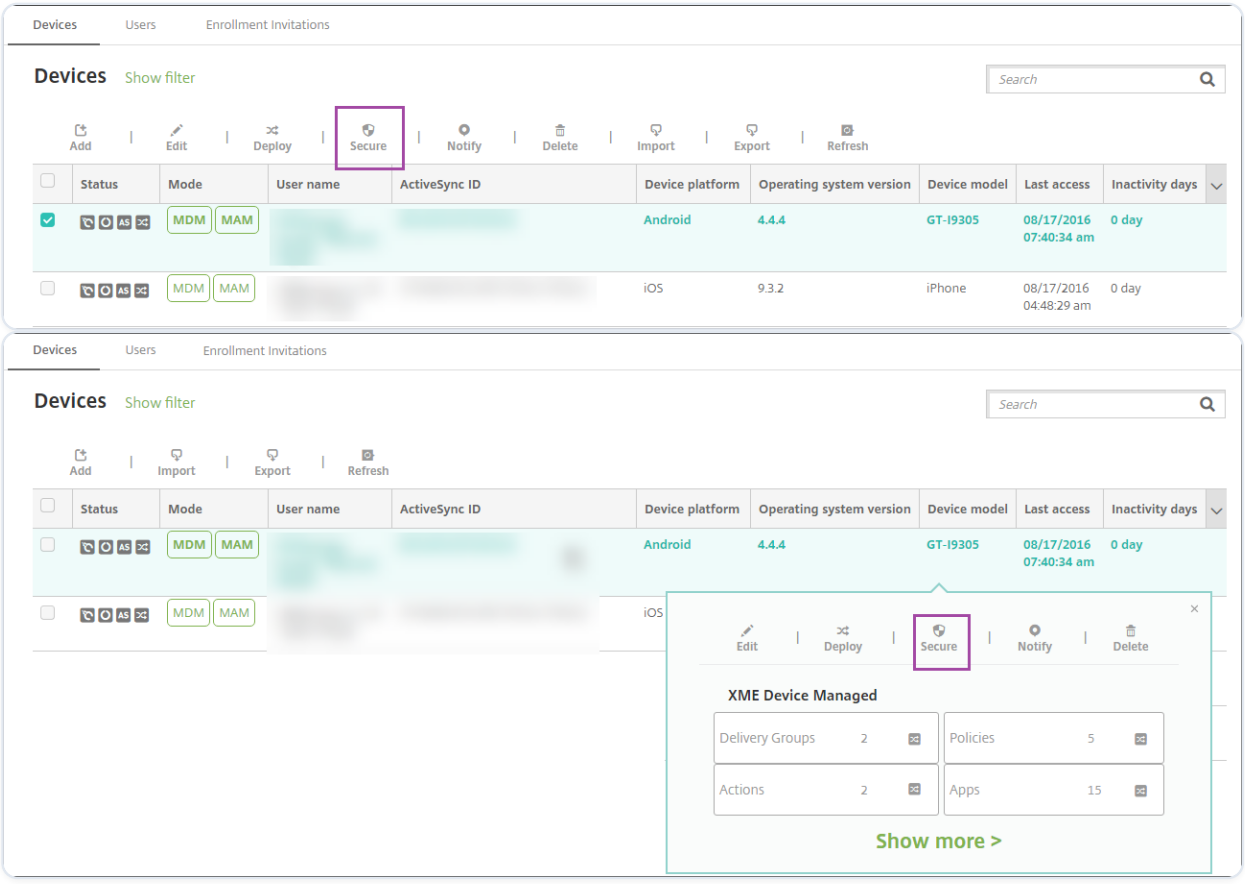
Para mostrar un mensaje y un número de teléfono en un dispositivo bloqueado, establezca la directiva Passcode en **true** en la consola de Citrix Endpoint Management. En su lugar, los usuarios pueden habilitar el código de acceso en el dispositivo manualmente.

1. Haga clic en **Administrar > Dispositivos**. Aparece la página **Dispositivos**.

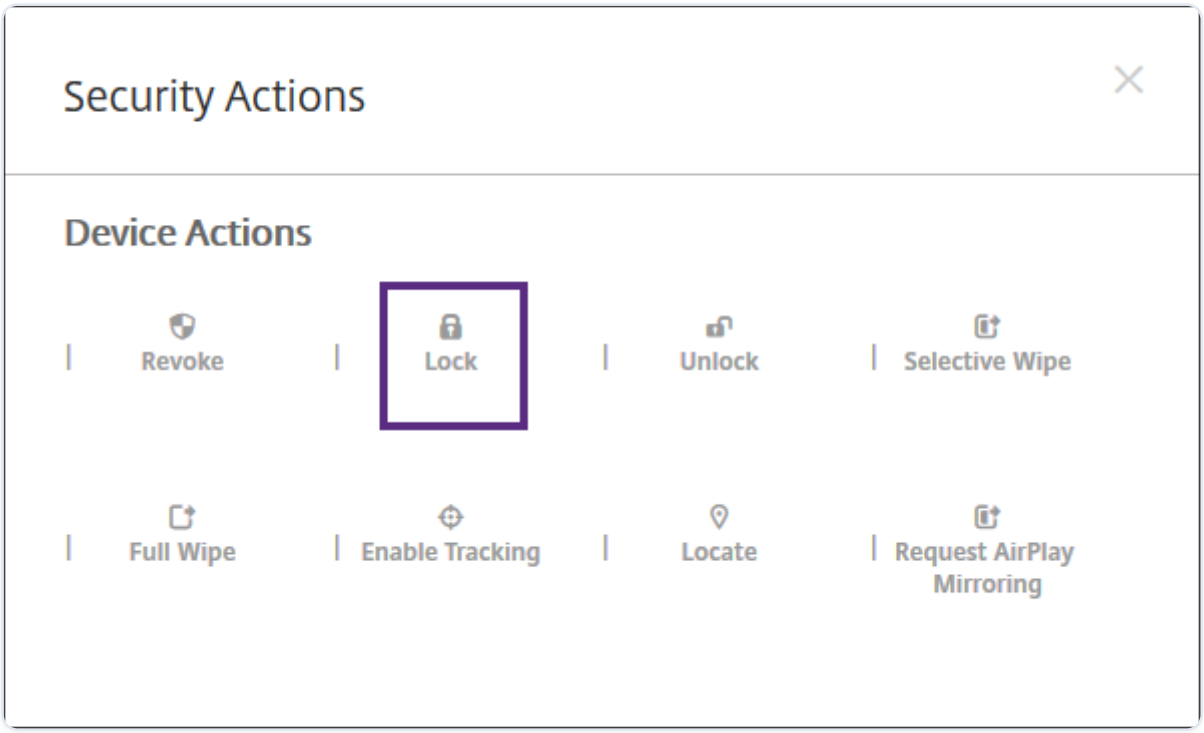


2. Seleccione el dispositivo iOS que quiere bloquear.

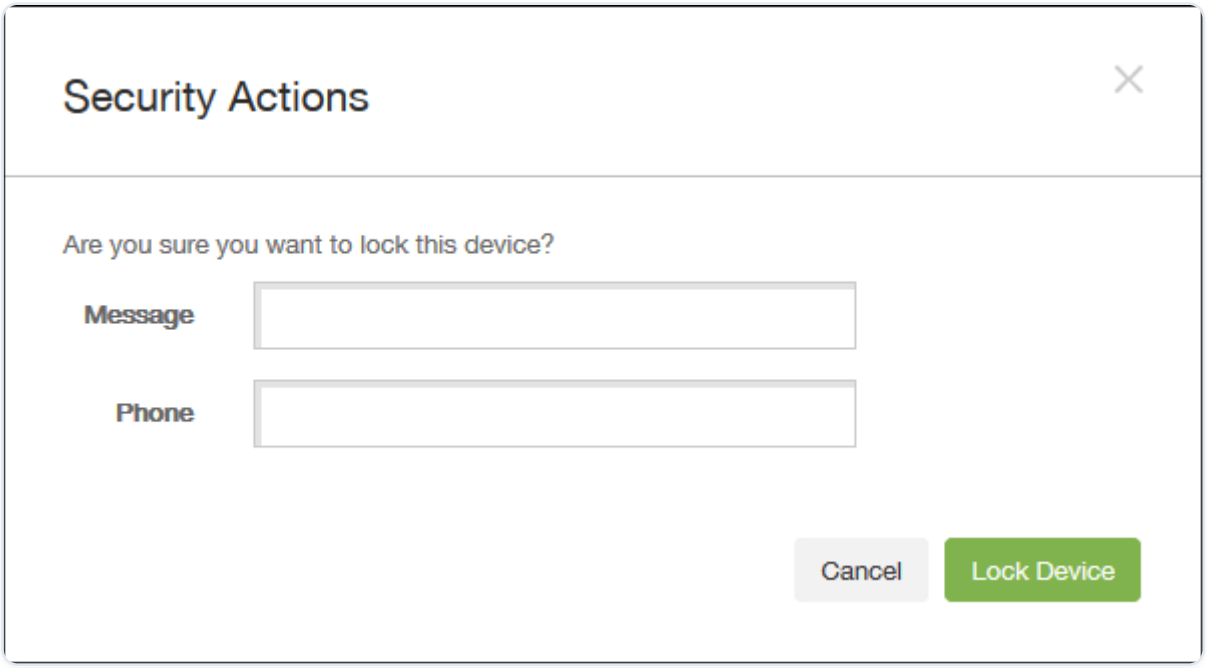
   Active la casilla de verificación junto a un dispositivo para mostrar el menú de opciones encima de la lista de dispositivos. Haga clic en cualquier otro lugar de la lista para mostrar el menú de opciones en el lado derecho de la lista.



3. En el menú de opciones, haga clic en **Proteger**. Aparece el cuadro de diálogo **Acciones de seguridad**.



4. Haga clic en **Bloquear**. Se muestra el cuadro de diálogo de confirmación **Acciones de seguridad**.



5. Opcionalmente, escriba un mensaje y un número de teléfono que aparecerán en la pantalla de bloqueo del dispositivo.

   iOS añade las palabras "iPad perdido" a lo que escriba en el campo **Mensaje**.

Si deja el campo **Mensaje** vacío y proporciona un número de teléfono, Apple muestra el mensaje "Llamar al propietario" en la pantalla de bloqueo del dispositivo.

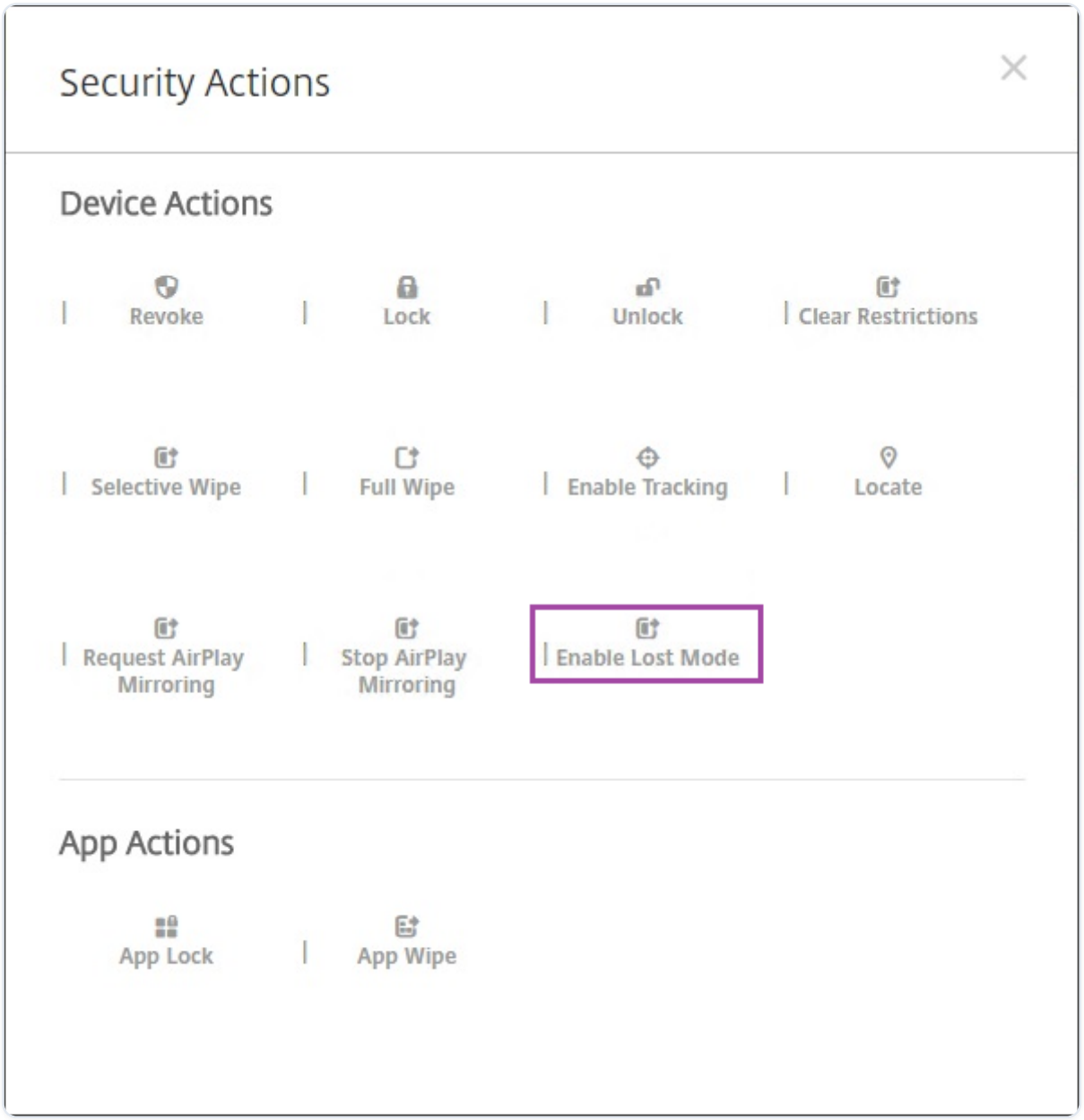
6. Haga clic en **Bloquear dispositivo**.

Poner dispositivos iOS en modo Perdido

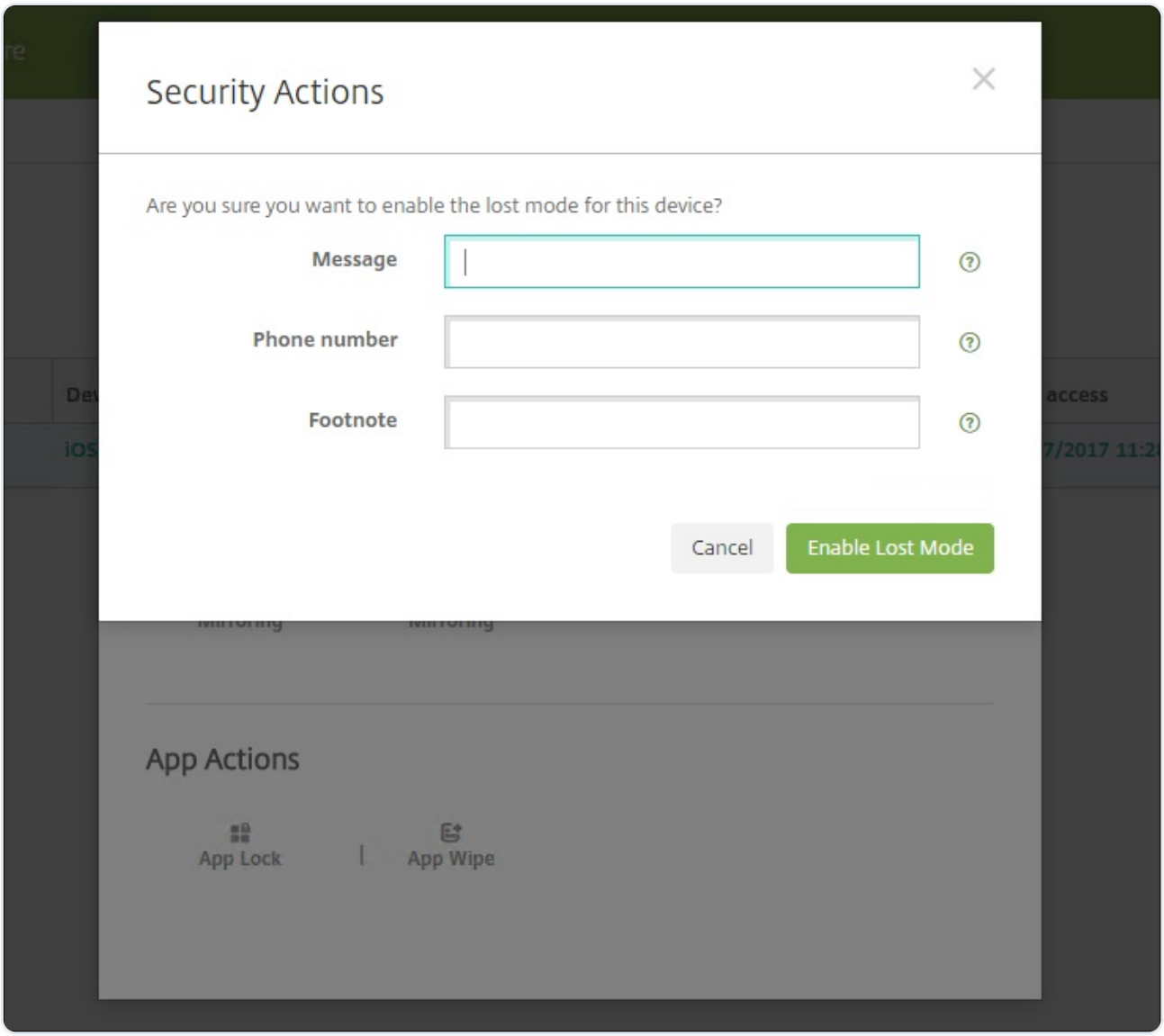
La propiedad de dispositivo Modo Perdido de Citrix Endpoint Management pone un dispositivo iOS en Modo Perdido. A diferencia del Modo Perdido administrado por Apple, el Modo Perdido de Citrix Endpoint Management no requiere que un usuario realice ninguna de las siguientes acciones para permitir la localización de su dispositivo: configurar el ajuste **Buscar mi iPhone/iPad** o habilitar los Servicios de ubicación para Citrix Secure Hub.

En el Modo Perdido de Citrix Endpoint Management, solo Citrix Endpoint Management puede desbloquear el dispositivo. (Por el contrario, si utiliza la función de bloqueo de dispositivos de Citrix Endpoint Management, los usuarios pueden desbloquear el dispositivo directamente mediante un código PIN que usted proporcione.

Para habilitar o inhabilitar el modo perdido: Vaya a **Administrar > Dispositivos**, elija un dispositivo iOS supervisado y, a continuación, haga clic en **Proteger**. A continuación, haga clic en **Habilitar modo perdido** o **Inhabilitar modo perdido**.



Si hace clic en **Habilitar modo perdido**, escriba la información que aparecerá en el dispositivo cuando esté en modo perdido.



Utilice cualquiera de los siguientes métodos para comprobar el estado del Modo Perdido:

- En la ventana **Acciones de seguridad**, verificar si el botón está configurado como **Inhabilitar modo perdido**.
- En **Administrar > Dispositivos**, en la ficha **General**, en **Seguridad**, consulte la última acción de Habilitar modo perdido o Inhabilitar modo perdido.

La pestaña General(/en-us/citrix-endpoint-management/media/manage-devices-ios-lost-mode.png)

- En **Administrar > Dispositivos**, en la pestaña **Propiedades**, verificar que el valor de la configuración **Modo perdido de MDM habilitado** es correcto.

La configuración de modo perdido de MDM habilitado(/en-us/citrix-endpoint-management/media/manage-devices-details-properties.png)

Si habilita el modo perdido de Citrix Endpoint Management en un dispositivo iOS, la consola de Citrix Endpoint Management también cambia de la siguiente manera:

- En **Configurar > Acciones**, la lista de **Acciones** no incluye estas acciones automatizadas: **Revocar el dispositivo**, **Borrar el dispositivo selectivamente** y **Borrar el dispositivo por completo**.
- En **Administrar > Dispositivos**, la lista de **Acciones de seguridad** ya no incluye las acciones de dispositivo **Revocar** y **Borrado selectivo**. Aún puede usar una acción de seguridad para realizar una acción de **Borrado completo**, según sea necesario.

iOS añade las palabras "iPad perdido" a lo que escriba en el **Mensaje** de la pantalla **Acciones de seguridad**.

Si deja el **Mensaje** vacío y proporciona un número de teléfono, Apple muestra el mensaje "Llamar al propietario" en la pantalla de bloqueo del dispositivo.

Omitir un bloqueo de activación de iOS

El Bloqueo de activación es una función de Buscar mi iPhone/iPad que impide la reactivación de un dispositivo supervisado perdido o robado. El Bloqueo de activación requiere el ID de Apple y la contraseña del usuario antes de que alguien pueda realizar estas acciones: Desactivar Buscar mi iPhone/iPad, borrar el dispositivo o reactivar el dispositivo. Para los dispositivos que posee su organización, omitir un Bloqueo de activación es necesario para, por ejemplo, restablecer o reasignar dispositivos.

Para habilitar el Bloqueo de activación, configure e implemente la directiva de dispositivo Opciones de MDM de Citrix Endpoint Management. A continuación, puede administrar un dispositivo desde la consola de Citrix Endpoint Management sin las credenciales de Apple del usuario. Para omitir el requisito de credenciales de Apple de un Bloqueo de activación, emita la acción de seguridad Omitir Bloqueo de activación desde la consola de Citrix Endpoint Management.

Por ejemplo, si el usuario devuelve un teléfono perdido o para configurar el dispositivo antes o después de un Borrado completo: Cuando el teléfono solicite la credencial de la cuenta de Apple App Store, omita ese paso emitiendo la acción de seguridad Omitir Bloqueo de activación.

REQUISITOS DEL DISPOSITIVO PARA OMITIR EL BLOQUEO DE ACTIVACIÓN

- Supervisado a través de Apple Configurator o Apple Deployment Program
- Configurado con una cuenta de iCloud
- Buscar mi iPhone/iPad habilitado
- Inscrito en Citrix Endpoint Management

- La directiva de dispositivo Opciones de MDM, con el bloqueo de activación habilitado, se implementa en los dispositivos

Para omitir un bloqueo de activación antes de emitir un borrado completo de un dispositivo:

1. Vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Proteger** y, a continuación, haga clic en **Omitir bloqueo de activación**.
2. Borre el dispositivo. La pantalla de bloqueo de activación no aparece durante la configuración del dispositivo.

Para omitir un bloqueo de activación después de emitir un borrado completo de un dispositivo:

1. Restablezca o borre el dispositivo. La pantalla de bloqueo de activación aparece durante la configuración del dispositivo.
2. Vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Proteger** y, a continuación, haga clic en **Omitir bloqueo de activación**.
3. Toque el botón Atrás del dispositivo. Aparece la pantalla de inicio.

Tenga en cuenta lo siguiente:

- Aconseje a sus usuarios que no desactiven Buscar mi iPhone/iPad. No realice un borrado completo desde el dispositivo. En cualquiera de esos casos, se le pedirá al usuario que introduzca la contraseña de la cuenta de iCloud. Después de la validación de la cuenta, el usuario no verá una pantalla de Activar iPhone/iPad después de borrar todo el contenido y la configuración.
- Para un dispositivo que tiene un código de omisión de bloqueo de activación generado y tiene el bloqueo de activación habilitado: si no puede omitir la página Activar iPhone/iPad después de un borrado completo, no necesita eliminar el dispositivo de Citrix Endpoint Management. Usted o el usuario pueden ponerse en contacto con el soporte técnico de Apple para desbloquear el dispositivo directamente.
- Durante un inventario de hardware, Citrix Endpoint Management consulta un dispositivo para obtener un código de omisión de bloqueo de activación. Si hay un código de omisión disponible, el dispositivo lo envía a Citrix Endpoint Management. Luego, para eliminar el código de omisión del dispositivo, envíe la acción de seguridad Omitir bloqueo de activación desde la consola de Citrix Endpoint Management. En ese momento, Citrix Endpoint Management y Apple tienen el código de omisión necesario para desbloquear el dispositivo.
- La acción de seguridad Omitir bloqueo de activación depende de la disponibilidad de un servicio de Apple. Si la acción no funciona, puede desbloquear un dispositivo utilizando una de las siguientes formas:

- En el dispositivo, introduzca manualmente las credenciales de la cuenta de iCloud.
- Deje el campo de nombre de usuario vacío y escriba el código de omisión en el campo de contraseña. Para buscar el código de omisión, vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Editar** y haga clic en **Propiedades**. El **código de omisión del bloqueo de activación** se encuentra en **Información de seguridad**.

macOS

Para administrar dispositivos macOS en Citrix Endpoint Management, debe configurar un certificado del servicio de notificaciones push de Apple (APNs) de Apple. Para obtener información, consulte Certificados APNs.

Citrix Endpoint Management inscribe dispositivos macOS en MDM. Citrix Endpoint Management admite los siguientes tipos de autenticación de inscripción para dispositivos macOS en MDM.

- Dominio
- Dominio más contraseña de un solo uso
- URL de invitación más contraseña de un solo uso

> **Requisitos para certificados de confianza en macOS 15:**

> Apple tiene nuevos requisitos para los certificados de servidor TLS. verificar que todos los certificados cumplen los nuevos requisitos de Apple. Consulte la publicación de Apple, `<https://support.apple.com/es-es/HT210176>`. Para obtener ayuda con la administración de certificados, consulte Cargar certificados.

> Un flujo de trabajo general para iniciar la administración de dispositivos macOS es el siguiente:

1. Complete el proceso de incorporación. Consulte Incorporación y configuración de recursos y Preparar la inscripción de dispositivos y la entrega de recursos.
2. Elija y configure un método de inscripción. Consulte Métodos de inscripción admitidos.
3. Configurar directivas de dispositivos macOS.
4. Inscribir dispositivos macOS.
5. Configure acciones de seguridad de dispositivos y aplicaciones. Consulte Acciones de seguridad.

Para ver los sistemas operativos compatibles, consulte Sistemas operativos de dispositivos compatibles.

Nombres de host de Apple que deben permanecer abiertos

Algunos nombres de host de Apple deben estar abiertos para garantizar el correcto funcionamiento de iOS, macOS y Apple App Store. Bloquear esos nombres de host puede afectar la instalación, actualización y el correcto funcionamiento de lo siguiente: iOS, aplicaciones de iOS, el funcionamiento de MDM y la inscripción de dispositivos y aplicaciones. Para obtener más información, consulte `<https://support.apple.com/es-es/HT201999>`.

Métodos de inscripción admitidos

La siguiente tabla enumera los métodos de inscripción que Citrix Endpoint Management admite para dispositivos macOS:

MÉTODO	ADMITIDO
Programa de implementación de Apple	Sí
Gestor de centros educativos de Apple	Sí
Apple Configurator	No
Inscripción manual	Sí
Invitaciones de inscripción	Sí

Apple tiene programas de inscripción de dispositivos para cuentas empresariales y educativas. Para las cuentas empresariales, se inscribe en el Apple Deployment Program para usar el Apple Deployment Program para la inscripción y administración de dispositivos en Citrix Endpoint Management. Ese programa es para dispositivos iOS, macOS y Apple TV. Consulte Implementar dispositivos a través de Apple Deployment Program.

Para las cuentas educativas, debe crear una cuenta de Apple School Manager. Apple School Manager unifica el Deployment Program y Volume Purchase. Apple School Manager es un tipo de Education Apple Deployment Program. Consulte Integrar con las funciones de Apple Education.

Puede usar el Apple Deployment Program para inscribir de forma masiva dispositivos iOS, macOS y Apple TV. Puede comprar esos dispositivos directamente a Apple, a un distribuidor autorizado de Apple participante o a un operador.

Configurar directivas de dispositivos macOS

Utilice estas directivas para configurar cómo Citrix Endpoint Management interactúa con los dispositivos que ejecutan macOS. Esta tabla enumera todas las directivas de dispositivos disponibles para dispositivos macOS.

Duplicación de AirPlay	Inventario de aplicaciones	Desinstalación de aplicaciones
Calendario (CalDAV)	Contactos (CardDAV)	Credenciales
Nombre del dispositivo	Exchange	FileVault
Cortafuegos	Fuente	Importar perfil de iOS y macOS

Actualización del SO	Código de acceso	Eliminación de perfiles
Restricciones	SCEP	VPN
Clip web		

Inscribir dispositivos macOS

Citrix Endpoint Management ofrece dos métodos para inscribir dispositivos que ejecutan macOS. Ambos métodos permiten a los usuarios de macOS inscribirse de forma inalámbrica, directamente desde sus dispositivos.

- **Enviar a los usuarios una invitación de inscripción:** Este método de inscripción le permite establecer cualquiera de los siguientes modos de seguridad de inscripción para dispositivos macOS:
  - Nombre de usuario + contraseña
  - Nombre de usuario + PIN
  - Autenticación de dos factores

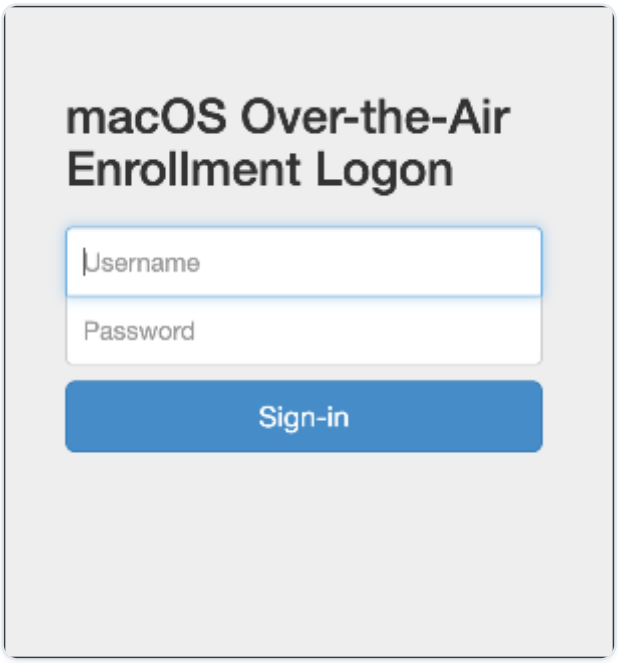
  Cuando el usuario sigue las instrucciones de la invitación de inscripción, aparece una pantalla de inicio de sesión con el nombre de usuario ya rellenado.
- **Enviar a los usuarios un enlace de inscripción:** Este método de inscripción para dispositivos macOS envía a los usuarios un enlace de inscripción, que pueden abrir en los

navegadores Safari o Chrome. A continuación, el usuario se inscribe proporcionando su nombre de usuario y contraseña.

Para evitar el uso de un enlace de inscripción para dispositivos macOS, establezca la propiedad del servidor **Enable macOS OTAE** en **false**. Como resultado, los usuarios de macOS solo pueden inscribirse mediante una invitación de inscripción.

Enviar una invitación de inscripción a usuarios de macOS

1. Agregue una invitación para la inscripción de usuarios de macOS. Consulte Invitaciones de inscripción.
2. Después de que los usuarios reciban la invitación y hagan clic en el enlace, aparecerá la siguiente pantalla en el navegador Safari. Citrix Endpoint Management rellena el nombre de usuario. Si eligió **Two Factor** para el modo de seguridad de inscripción, aparecerá otro campo.



3. Los usuarios instalan los certificados según sea necesario. Que los usuarios vean la solicitud para instalar certificados depende de si ha configurado lo siguiente para macOS: un certificado SSL de confianza pública y un certificado de firma digital de confianza pública. Para obtener información sobre los certificados, consulte Certificados y autenticación.
4. Los usuarios proporcionan las credenciales solicitadas.

Las directivas del dispositivo Mac se instalan. Ahora puede empezar a administrar dispositivos macOS con Citrix Endpoint Management del mismo modo que administra dispositivos móviles.

Enviar un enlace de instalación a usuarios de macOS

1. Envíe el enlace de inscripción `https://serverFQDN:8443/instanceName/macos/otae`, que los usuarios pueden abrir en los navegadores Safari o Chrome.

   - **serverFQDN** es el nombre de dominio completo (FQDN) del servidor que ejecuta Citrix Endpoint Management.
   - El puerto **8443** es el puerto seguro predeterminado. Si configuró un puerto diferente, utilice ese puerto en lugar del 8443.
   - La **instanceName**, a menudo mostrada como `zdm`, es el nombre especificado durante la instalación del servidor.

   Para obtener más información sobre cómo enviar enlaces de instalación, consulte Para enviar un enlace de instalación.
2. Los usuarios instalan los certificados según sea necesario. Si configuró un certificado SSL de confianza pública y un certificado de firma digital para iOS y macOS, los usuarios verán la solicitud para instalar los certificados. Para obtener información sobre los certificados, consulte Certificados y autenticación.
3. Los usuarios inician sesión en sus Mac.

   Las directivas del dispositivo Mac se instalan. Ahora puede empezar a administrar dispositivos macOS con Citrix Endpoint Management del mismo modo que administra dispositivos móviles.

Acciones de seguridad

macOS admite las siguientes acciones de seguridad. Para obtener una descripción de cada acción de seguridad, consulte Acciones de seguridad.

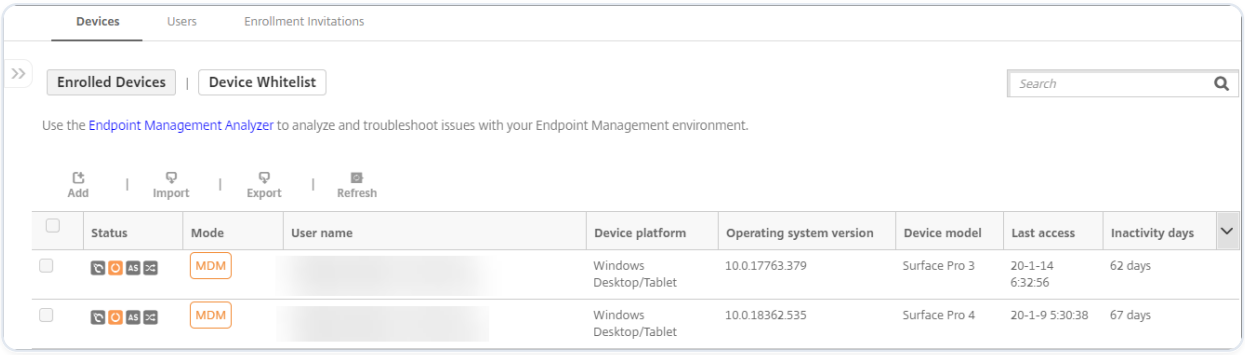
Revocar	Bloquear	Borrado selectivo
Borrado completo	Renovación de certificados	Rotar clave de recuperación personal

Bloquear dispositivos macOS

Puede bloquear de forma remota un dispositivo macOS perdido. Citrix Endpoint Management bloquea el dispositivo. A continuación, genera un código PIN y lo establece en el dispositivo. Para acceder al dispositivo, el usuario escribe el código PIN. Utilice **Cancelar bloqueo** para quitar el bloqueo de la consola de Citrix Endpoint Management.

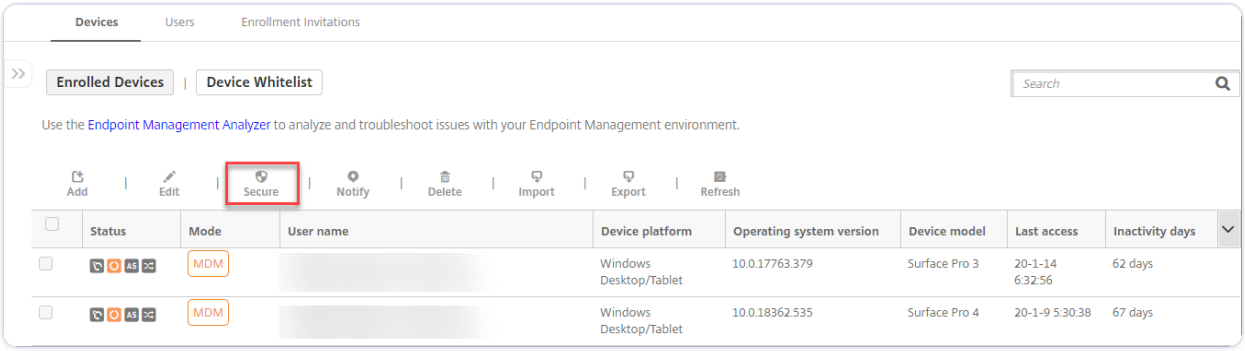
Puede usar la directiva de dispositivo Contraseña para configurar más ajustes asociados al código PIN. Para obtener más información, consulte Configuración de macOS.

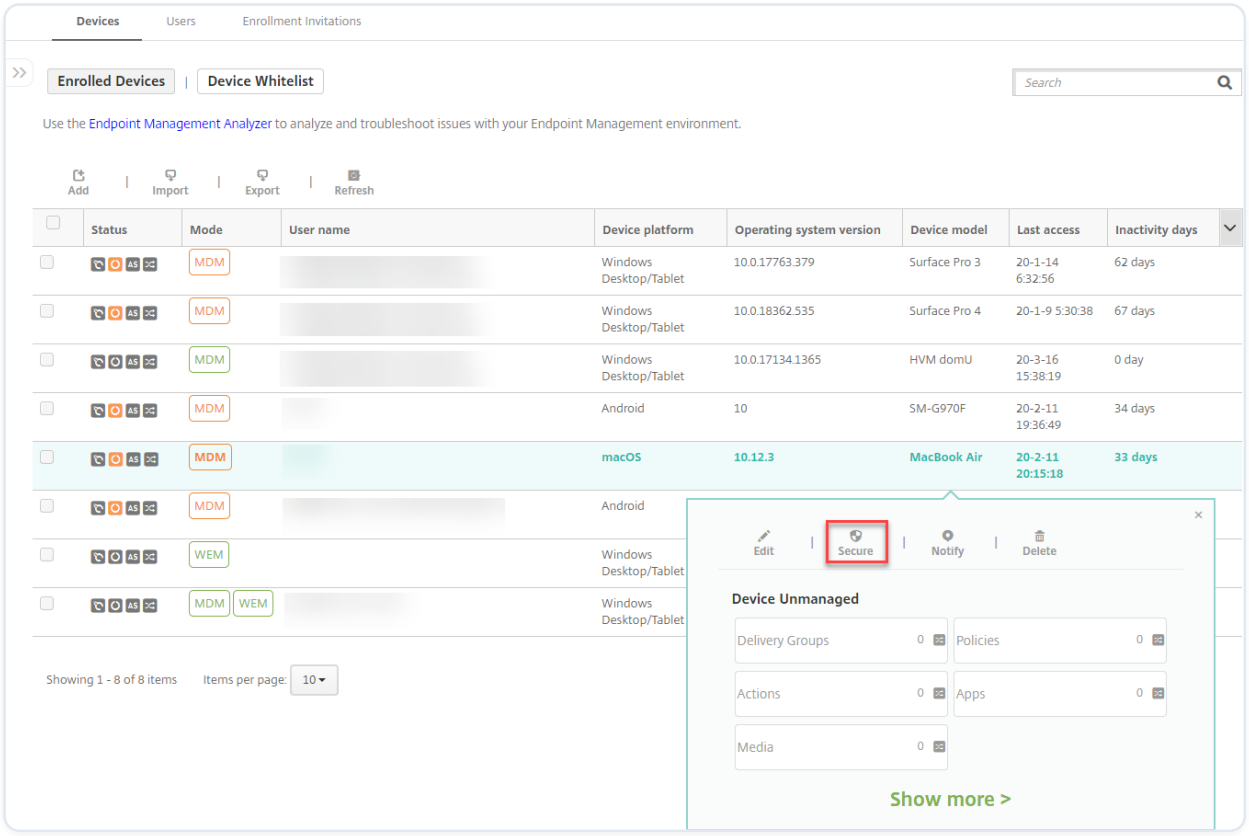
1. Haga clic en **Administrar > Dispositivos**. Aparece la página **Dispositivos**.



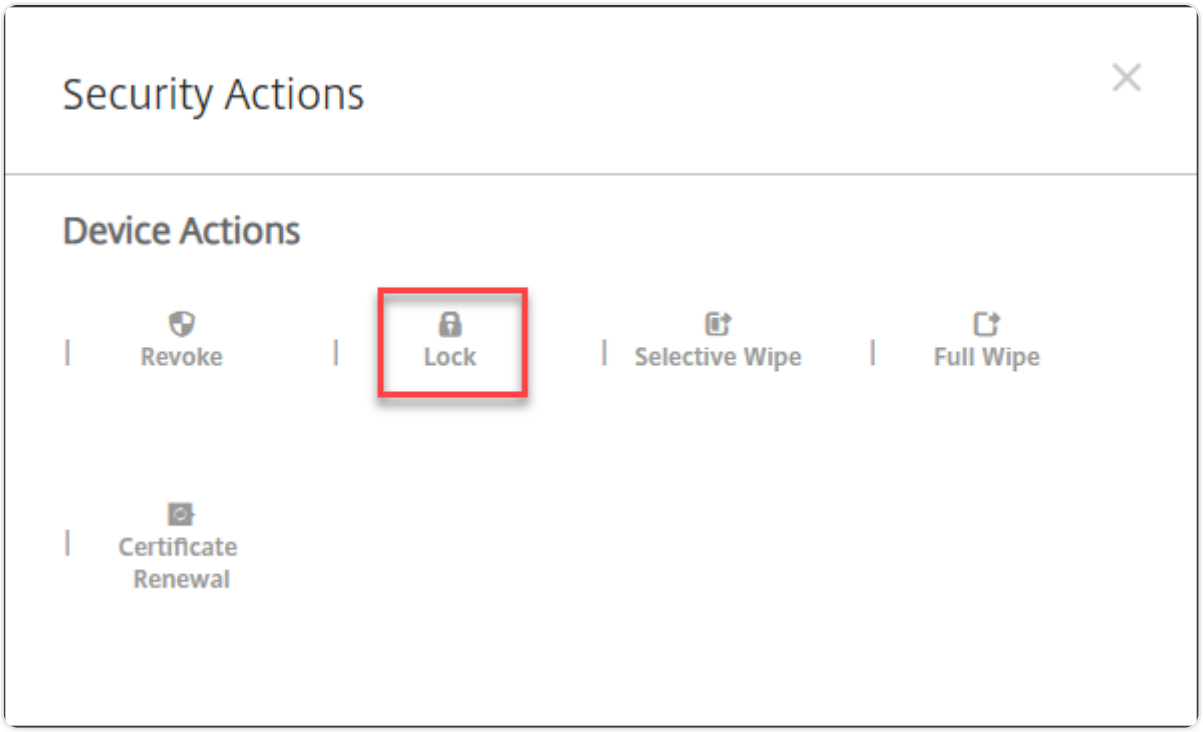
2. Seleccione el dispositivo macOS que quiere bloquear.

   Seleccione la casilla de verificación junto a un dispositivo para mostrar el menú de opciones encima de la lista de dispositivos. También puede hacer clic en cualquier otro lugar de un elemento de la lista para mostrar el menú de opciones en el lado derecho de la lista.

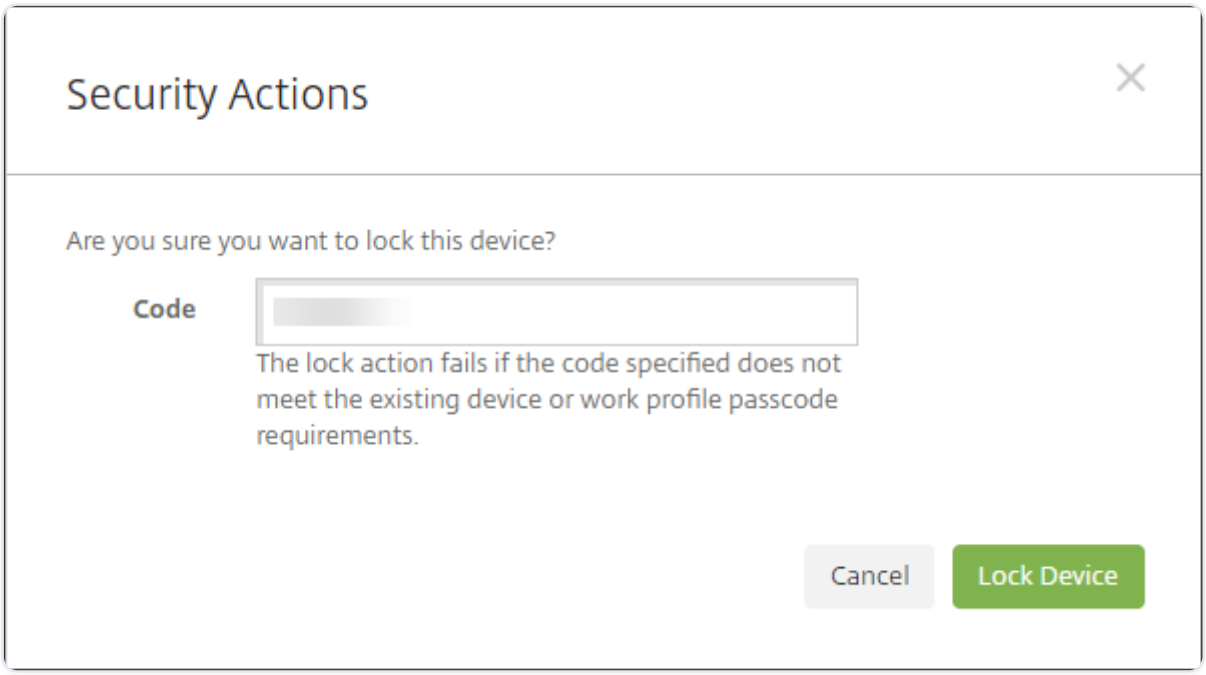




3. En el menú de opciones, haga clic en **Proteger**. Aparece el cuadro de diálogo **Acciones de seguridad**.



4. Haga clic en **Bloquear**. Se muestra el cuadro de diálogo de confirmación **Acciones de seguridad**.



5. Haga clic en **Bloquear dispositivo**.

> **Importante:**
>
> También puede especificar un código de acceso en lugar de usar el código que genera Citrix Endpoint Management. La acción de bloqueo falla si el código especificado no cumple los requisitos de código del dispositivo o del perfil de trabajo existente.

Token de arranque

Un token de arranque ayuda a conceder el atributo SecureToken de macOS a las cuentas cuando inicia sesión en un dispositivo macOS. SecureToken se transmite de una cuenta de confianza a otra. Las cuentas habilitadas para SecureToken pueden realizar operaciones criptográficas en el dispositivo. Sin el token de arranque, debe seguir flujos de trabajo complejos para crear cuentas en ese dispositivo antes de agregar cuentas de usuario individuales.

Citrix Endpoint Management admite el depósito de tokens de arranque para dispositivos macOS inscritos a través del Programa de implementación de Apple. Utiliza el Programa de implementación de Apple para inscribir dispositivos macOS que compra directamente a Apple, a un distribuidor autorizado de Apple participante o a un operador. Para obtener información sobre cómo inscribirse en el Programa de implementación de Apple, consulte Implementar dispositivos a través del Programa de implementación de Apple.

Los tokens de arranque se generan durante el flujo de trabajo del Asistente de configuración. Específicamente, se generan durante la creación de cuentas de usuario locales. El Asistente de configuración se ejecuta la primera vez que los usuarios inician sus dispositivos. Los tokens se guardan en la base de datos de Citrix Endpoint Management y no son visibles para usted ni para los usuarios finales. Al eliminar los dispositivos de su sitio de Citrix Endpoint Management, se eliminan los tokens. Realizar un restablecimiento de fábrica no los elimina.

Requisitos previos:

- macOS 11.0 o posterior
- Dispositivos macOS que tienen el chip de seguridad Apple T2
- Dispositivos macOS inscritos a través del Programa de implementación de Apple

Una ventaja de depositar tokens de arranque con Citrix Endpoint Management es que las cuentas remotas se pueden habilitar para FileVault y pueden desbloquear el volumen de FileVault. Para obtener información sobre FileVault, consulte Directiva de dispositivos de FileVault.

Implementar dispositivos a través de los programas de implementación de Apple

Los programas de implementación de Apple (ADP) le permiten inscribir automáticamente dispositivos Apple en Citrix Endpoint Management sin tener que tocar o preparar los dispositivos antes de que los usuarios los reciban. Después de que un usuario desempaqueta y activa el dispositivo, este se inscribe automáticamente en Citrix Endpoint Management, y todas las configuraciones de administración, aplicaciones y libros están listas para el usuario.

Los ADP incluyen Apple Business Manager (ABM) para organizaciones empresariales y Apple School Manager (ASM) para organizaciones educativas. ABM y ASM están disponibles para dispositivos iOS, iPadOS y macOS. Para obtener más información sobre la elegibilidad de los dispositivos, consulte la Guía del usuario de Apple Business Manager y la Guía del usuario de Apple School Manager.

> **Nota:**
>
> ABM y ASM combinan los anteriores programas Device Enroll Program y Volume Purchase Program de Apple.
>
> Este artículo le guía a través del flujo de trabajo general de implementación con ABM o ASM:

1. Inscribirse en ABM o ASM
2. Conectar su cuenta de ABM o ASM a Citrix Endpoint Management
3. Pedir dispositivos
4. Asignar dispositivos a Citrix Endpoint Management
5. Comprar contenido en volumen y sincronizarlo con Citrix Endpoint Management
6. Configurar reglas de implementación para directivas y aplicaciones de dispositivos
7. Agregar grupos de entrega a los que se les hayan asignado usuarios y recursos

Una vez completado este proceso de implementación, los dispositivos están listos para ser desempaquetados y activados para una inscripción automática de dispositivos.

Requisitos previos

Abra los puertos necesarios para la conectividad entre Citrix Endpoint Management y Apple. Para obtener más información, consulte Requisitos de puertos.

Inscribirse en ABM o ASM

Para empezar a implementar dispositivos en Apple, inscríbase en ABM o ASM.

ABM y ASM están disponibles para organizaciones y no para particulares. Debe proporcionar muchos detalles e información de la organización para crear una cuenta. La solicitud y la aprobación de las cuentas pueden tardar un tiempo.

Inscribirse en ABM

Para inscribirse en ABM, vaya a business.apple.com. Haga clic en **Enroll now** para solicitar una nueva cuenta.

La mejor práctica es usar una dirección de correo electrónico de su organización, como `deployment@company.com`. El proceso de inscripción puede tardar unos días. Después de recibir sus credenciales de inicio de sesión, siga los pasos proporcionados en ABM para crear una cuenta.

Inscribirse en ASM

Para crear su cuenta de ASM, vaya a Apple School Manager y siga las instrucciones para inscribirse. La primera vez que inicie sesión en ASM, se abrirá el Asistente de configuración.

- Para obtener información sobre los requisitos previos de ASM, el Asistente de configuración y las tareas de administración, consulte la Guía del usuario de Apple School Manager.

- Al configurar una cuenta de usuario de ASM, utilice un nombre de dominio que difiera del nombre de dominio de Active Directory. Por ejemplo, anteponga al nombre de dominio de ASM algo como `appleid`.
- Cuando conecta ASM a sus datos de lista, ASM crea ID de Apple gestionados para instructores y estudiantes. Sus datos de lista incluyen instructores, estudiantes y clases. Para obtener información sobre cómo agregar datos de lista a ASM, consulte la Guía del usuario de Apple School Manager, enlazada anteriormente en esta lista.
- Puede personalizar el formato de ID de Apple gestionado para su institución, como se describe en la Guía del usuario de Apple School Manager, enlazada anteriormente en esta lista.

> **Importante:**
>
> No cambie los ID de Apple gestionados después de importar la información de ASM a Citrix Endpoint Management.

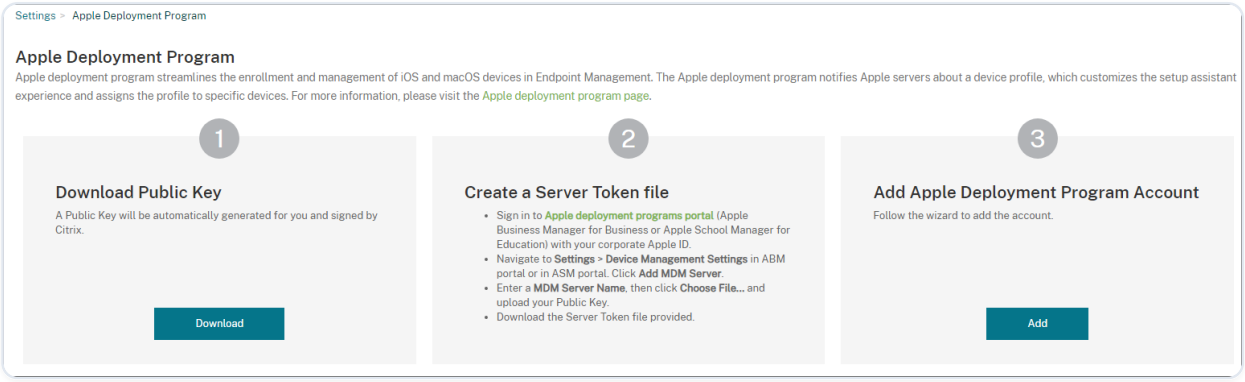
- Si compró dispositivos a través de revendedores o proveedores, vincule esos dispositivos a ASM. Para obtener información, consulte la Guía del usuario de Apple School Manager, enlazada anteriormente en esta lista.

Conecte su cuenta de ABM o ASM a Citrix Endpoint Management

Después de crear su cuenta de ABM o ASM, conéctela con su implementación del servidor de Citrix Endpoint Management.

Paso 1: Descargue una clave pública de su servidor de Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, vaya a **Settings > Apple Deployment Programs**.



2. En **Download Public Key**, haga clic en **Download**.

Paso 2: Cree y descargue un archivo de token de servidor desde su cuenta de Apple

1. Inicie sesión en Apple Business Manager o Apple School Manager con una cuenta de administrador o de gestor de inscripción de dispositivos.
2. En la parte inferior de la barra lateral, haga clic en **Settings** y, a continuación, en **Device Management Settings > Add MDM Server**.
3. En la configuración **MDM Server Name**, escriba un nombre para el servidor de Citrix Endpoint Management. El nombre del servidor que escriba es para su referencia. No es la URL ni el nombre del servidor.
4. En **Upload Public Key**, haga clic en **Choose File**. Cargue la clave pública que descargó de Citrix Endpoint Management y, a continuación, guarde los cambios.
5. Haga clic en **Download Token** para descargar el archivo de token del servidor en su equipo.

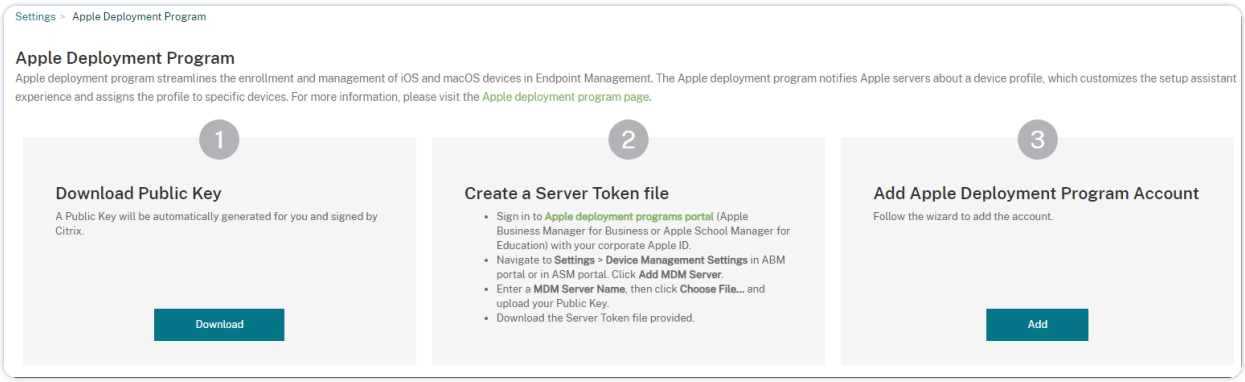
   Cargue el archivo de token del servidor al agregar la cuenta de ABM o ASM a Citrix Endpoint Management. La información de su token aparece en la consola de Citrix Endpoint Management después de importar el archivo de token.
6. En **Default Device Assignment**, haga clic en **Change**. Elija cómo desea asignar los dispositivos y, a continuación, proporcione la información solicitada. Para obtener más información, consulte la ABM User Guide o la Apple School Manager User Guide.

Paso 3: Añadir su cuenta a Citrix Endpoint Management

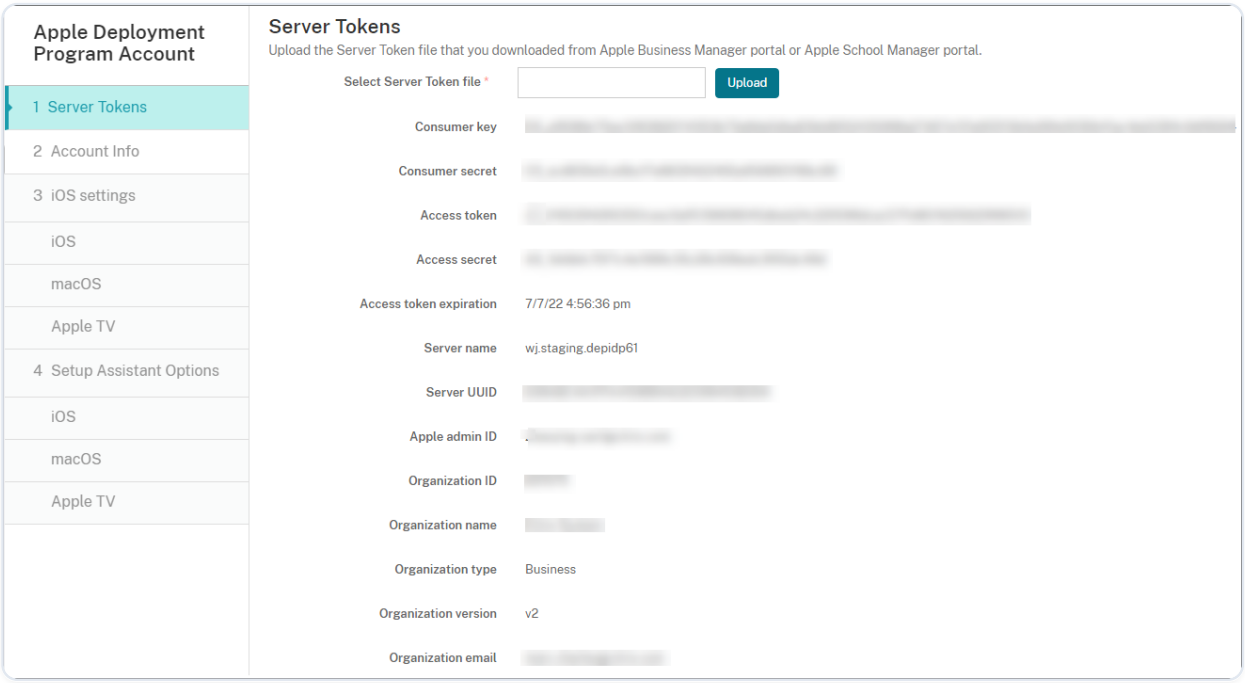
Puede añadir varias cuentas de ABM o ASM a Citrix Endpoint Management. Esta función le permite usar diferentes parámetros de inscripción y opciones del asistente de configuración por país, departamento, etc. A continuación, asocia las cuentas de ABM o ASM con diferentes directivas de dispositivo.

Por ejemplo, puede centralizar todas sus cuentas de ABM o ASM de diferentes países en el mismo servidor de Citrix Endpoint Management para importar y supervisar todos los dispositivos ABM o ASM. Primero, personaliza la configuración de inscripción y las opciones del asistente de configuración por departamento, jerarquía organizativa u otra estructura. Luego, configura las directivas para proporcionar la funcionalidad adecuada en toda su organización y permitir que los usuarios reciban la asistencia adecuada.

1. En la consola de Citrix Endpoint Management, vaya a **Settings > Apple Deployment Program** y, en **Add Apple Deployment Program Account**, haga clic en **Add**.

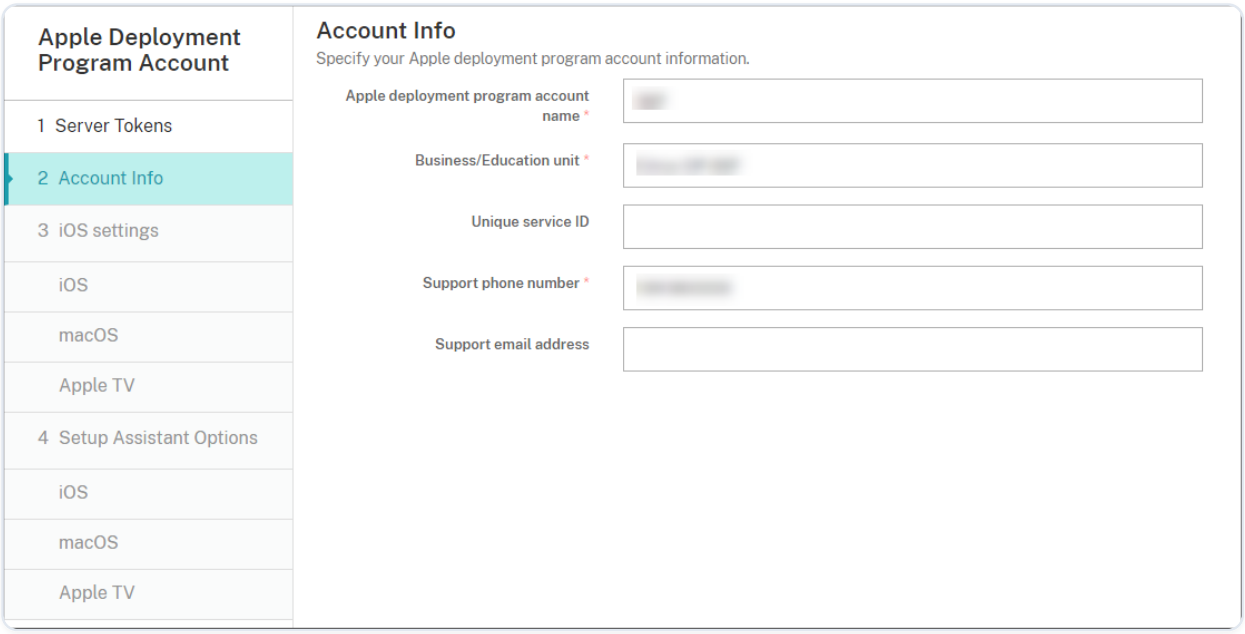


2. En la página **Server Tokens**, especifique el archivo de token del servidor y, a continuación, haga clic en **Upload**.



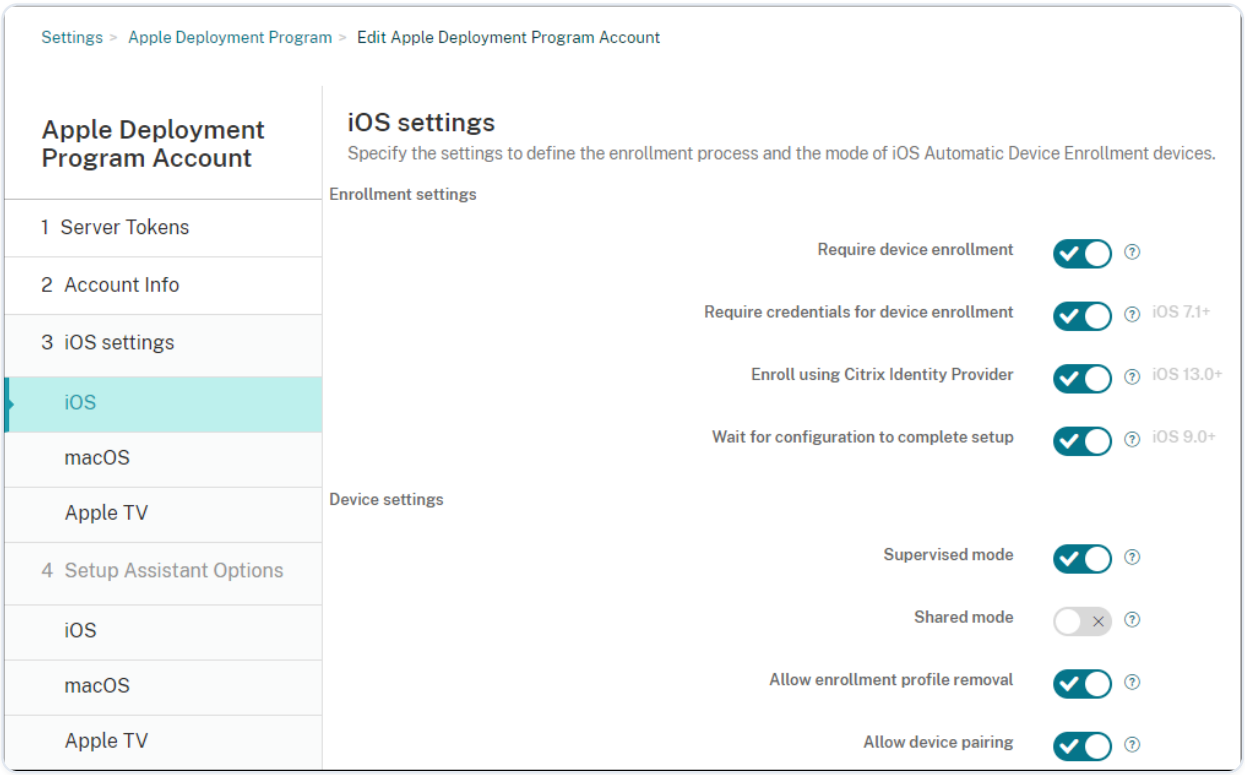
Aparece la información del token del servidor.

3. En la página **Account Info**, especifique estos parámetros:



- **Nombre de la cuenta del programa de implementación de Apple:** Un nombre descriptivo único para esta cuenta de ADP, que identifica cómo organiza las cuentas de ADP, por ejemplo, por país o jerarquía organizativa.
- **Unidad de negocio/educación:** La unidad de negocio o el departamento al que está asignado el dispositivo. Este campo es obligatorio.
- **ID de servicio único:** Un ID único opcional para ayudarle a identificar aún más la cuenta.
- **Número de teléfono de soporte:** Un número de teléfono de soporte al que los usuarios llaman para obtener ayuda durante la configuración. Este campo es obligatorio.
- **Dirección de correo electrónico de soporte:** Una dirección de correo electrónico de soporte opcional disponible para los usuarios finales.
- **Sufijo educativo:** Para cuentas de ASM. Escriba el sufijo asignado a los dispositivos inscritos a través de esta cuenta.

4. En **iOS Settings**, especifique estos parámetros:



Parámetros de inscripción:

- **Requerir inscripción de dispositivos:** Si se debe exigir a los usuarios que inscriban sus dispositivos. El valor predeterminado es **Activado**.
- **Requerir credenciales para la inscripción de dispositivos:** Si se debe exigir a los usuarios que introduzcan sus credenciales durante la configuración de ABM y ASM. Recomendamos que exija a todos los usuarios que introduzcan sus credenciales durante la inscripción de dispositivos, permitiendo que solo los usuarios autorizados inscriban dispositivos. El valor predeterminado es **Activado**.

  Cuando habilita ABM o ASM antes de la primera configuración y no selecciona esta opción, Citrix Endpoint Management crea los componentes de ABM o ASM. Esta creación incluye componentes como el usuario, Citrix Secure Hub, el inventario de software y el grupo de implementación. Si selecciona esta opción, Citrix Endpoint Management no crea los componentes. Como resultado, si más tarde desactiva esta opción, los usuarios que no hayan introducido sus credenciales no podrán inscribirse en ABM o ASM porque estos componentes no existen. Para agregar componentes de ABM o ASM, en ese caso, inhabilite y luego habilite la cuenta de ABM o ASM.
- **Inscribirse con Citrix Identity Provider:** Si se debe inscribir con Citrix Identity Provider. Este parámetro solo está disponible para cuentas de ABM. Si está **Activado**, los dispositivos iOS habilitados para ADP se inscriben solo mediante el proveedor de identidades de Citrix. El valor predeterminado es **Desactivado**.

Para activar el parámetro, primero debe configurar Citrix Identity Provider como su proveedor de identidades. Vaya a **Settings > Identity Provider (IDP)**, haga clic en **Add** y seleccione **Citrix Identity Provider**.

Si este parámetro está establecido en **Activado**, tenga en cuenta las siguientes consideraciones:

- No puede eliminar la configuración correspondiente de Citrix Identity Provider en la página **Settings > Identity Provider (IDP)**.
- Al modificar la configuración correspondiente de Citrix Identity Provider, no puede cambiar a un proveedor de identidades diferente.

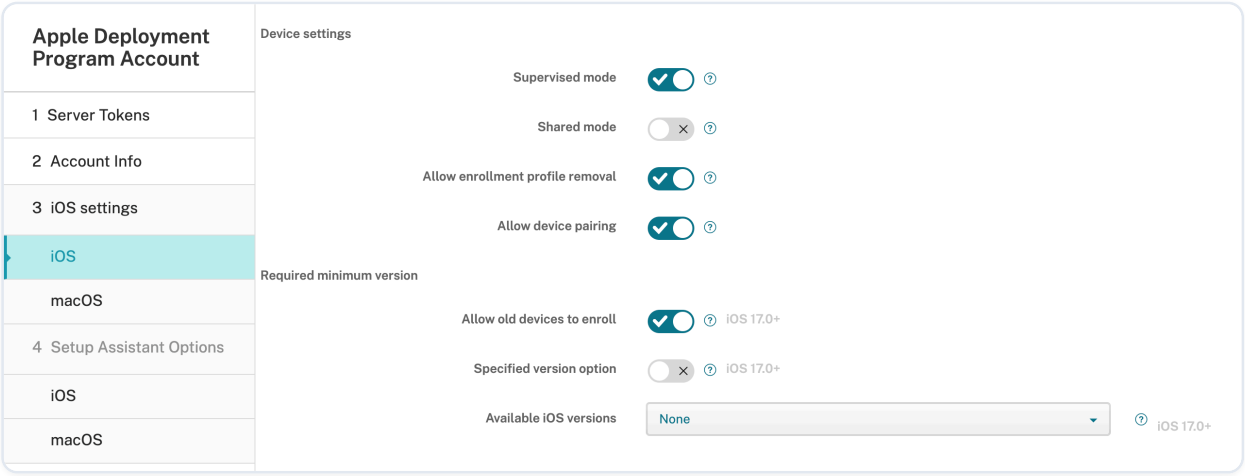
- **Esperar a que la configuración complete la instalación:** Si se debe exigir que los dispositivos de los usuarios estén en modo Asistente de configuración hasta que todos los recursos de MDM se implementen en el dispositivo. Este parámetro está disponible para dispositivos en modo supervisado. El valor predeterminado es **Desactivado**.
- La documentación de Apple indica que los siguientes comandos podrían no funcionar mientras un dispositivo está en modo Asistente de configuración:
  - InviteToProgram
  - InstalarAplicación
  - AplicarCódigoDeCanje
  - InstalarContenidoMultimedia
  - SolicitarDuplicación
  - BloqueoDeDispositivo

Configuración del dispositivo:

- **Modo supervisado:** Establezca en **Activado** si utiliza Apple Configurator para administrar los dispositivos inscritos o cuando la opción **Esperar a que la configuración complete la configuración** esté habilitada. El valor predeterminado es **Activado**. Para obtener más información sobre cómo poner un dispositivo iOS en modo supervisado, consulte Implementar dispositivos con Apple Configurator 2.
- **Permitir la eliminación del perfil de inscripción:** Si se permite que los dispositivos utilicen un perfil que se puede eliminar de forma remota. El valor predeterminado es **Desactivado**.

- **Permitir el emparejamiento de dispositivos:** Si puede administrar los dispositivos inscritos a través de Apple Music y Apple Configurator. El valor predeterminado es **Desactivado**.

Versión mínima requerida



- **Permitir la inscripción de dispositivos antiguos:** Si está habilitada, los dispositivos pueden inscribirse incluso si no pudieron actualizar a la versión mínima requerida actual. El valor predeterminado es Activado. Esta opción solo está disponible en iOS 17.0 y versiones posteriores.
- **Opción de versión especificada:** Si se permite al administrador introducir la versión especificada manualmente. El valor predeterminado es **Desactivado**. Esta opción solo está disponible en iOS 17.0 y versiones posteriores.
- **Versiones de iOS disponibles:** Puede elegir las versiones de iOS disponibles de la lista. Si el dispositivo tiene una versión de iOS inferior a la versión actual, iniciará el proceso de actualización en el dispositivo. Si la versión caduca en el futuro, se utiliza una versión mínima de la lista de versiones disponibles. El valor predeterminado es Ninguno; no tendrá efecto si se establece como Ninguno. Esta opción solo está disponible en iOS 17.0 y versiones posteriores.
- **Versión especificada:** Si el dispositivo tiene una versión de iOS inferior a la versión actual, iniciará el proceso de actualización en el dispositivo. Si la versión caduca en el futuro, se utiliza una versión mínima de la lista de versiones disponibles. Introduzca el número de versión correcto; de lo contrario, pueden producirse errores desconocidos.

Identidades de supervisión

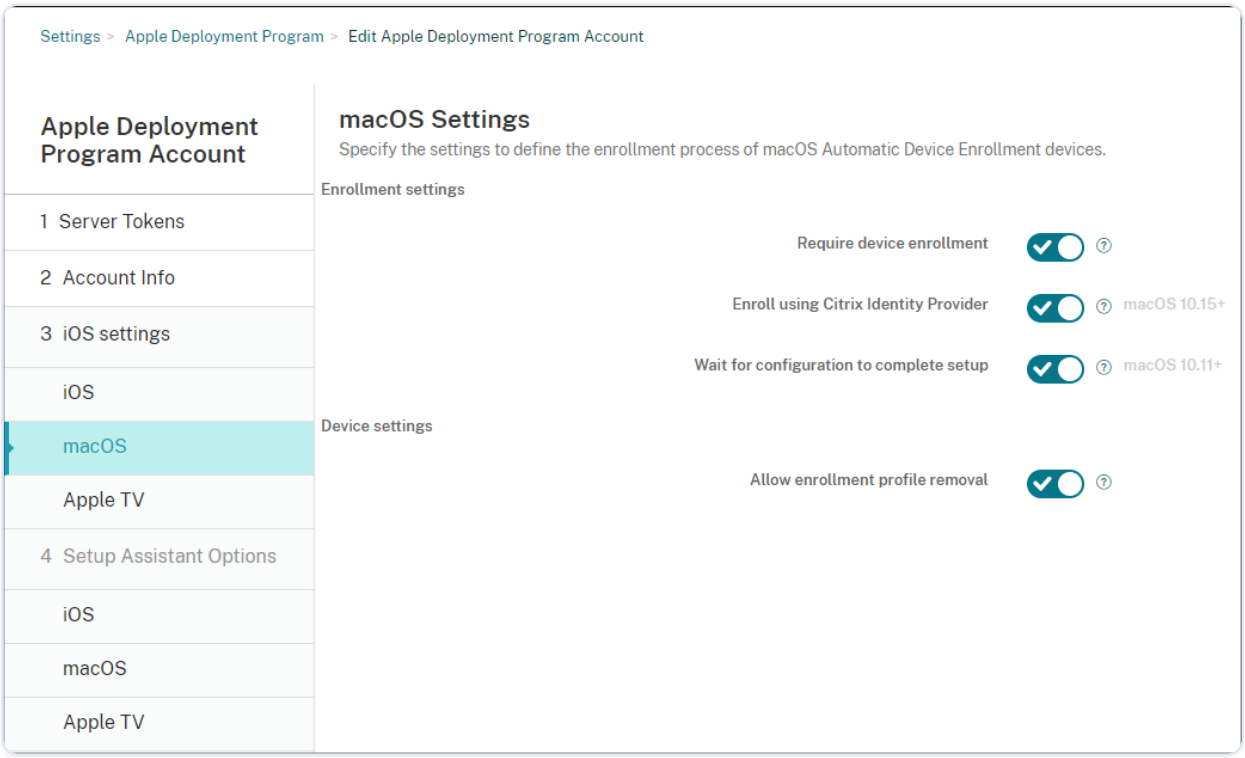
Si utiliza la herramienta GroundControl, puede añadir un certificado para realizar lo siguiente:

- Anular las restricciones de emparejamiento para evitar el mensaje "Confiar en este host".

- Escalar las acciones de los dispositivos administrados a través de USB para realizar actividades como la instalación de perfiles sin interacción del usuario. Esto permite a GroundControl habilitar el modo de aplicación única y el bloqueo del dispositivo para la retirada.
- Restaurar una copia de seguridad en dispositivos ABM o ASM.

Para obtener más información sobre GroundControl, consulte el sitio web de GroundControl.

5. En **Configuración de macOS**, especifique estos ajustes:



Parámetros de inscripción:

- **Requerir inscripción de dispositivos:** Si se debe exigir a los usuarios que inscriban sus dispositivos. El valor predeterminado es **Activado**.
- **Inscribir con Citrix Identity Provider:** Si se debe inscribir con Citrix Identity Provider. Esta configuración solo está disponible para cuentas ABM. Si está **Activado**, los dispositivos macOS habilitados para ADP se inscriben solo mediante el proveedor de identidades de Citrix. El valor predeterminado es **Desactivado**.

  Para activar la configuración, primero debe configurar Citrix Identity Provider como su proveedor de identidades. Vaya a **Configuración > Proveedor de identidades (IDP)**, haga clic en **Agregar** y seleccione **Citrix Identity Provider**.

  Si esta configuración está establecida en **Activado**, tenga en cuenta las siguientes consideraciones:

    - No puede eliminar la configuración correspondiente de Citrix Identity Provider en la página **Configuración > Proveedor de identidades (IDP)**.
    - Al editar la configuración correspondiente de Citrix Identity Provider, no puede cambiar a un proveedor de identidades diferente.

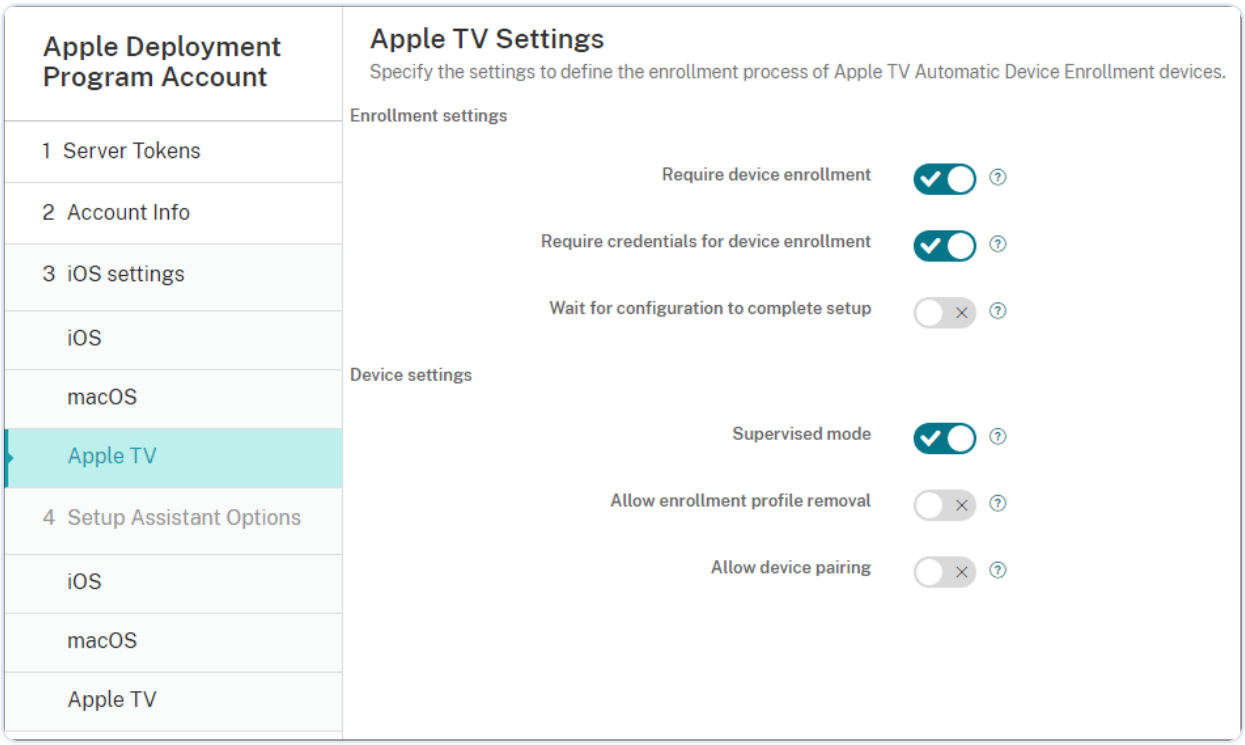
- **Esperar a que la configuración complete la instalación:** Si está **Activado**, el dispositivo macOS no continúa en el asistente de configuración hasta que el código de acceso del recurso MDM se implemente en el dispositivo. Esa implementación ocurre antes de la creación de la cuenta local. Esta configuración está disponible para dispositivos macOS 10.11 y superiores. El valor predeterminado es **Desactivado**.

Configuración del dispositivo:

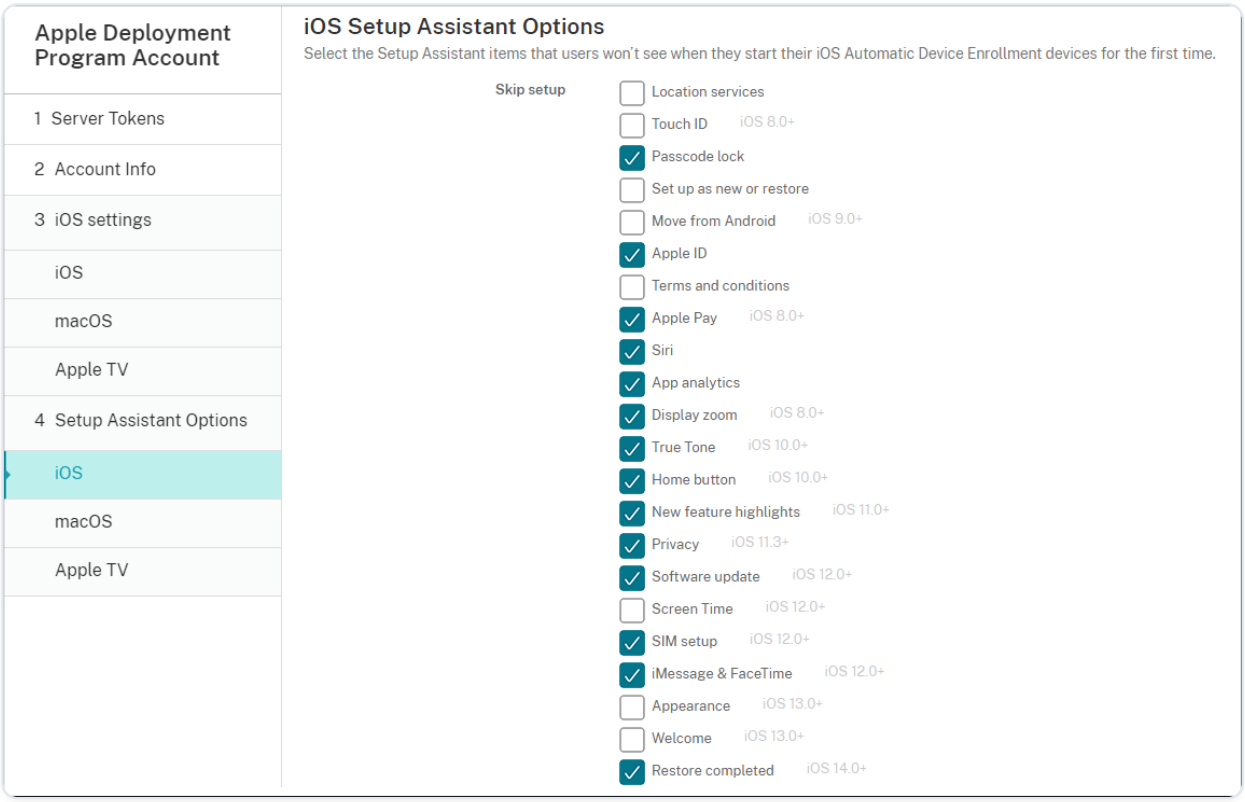
- **Permitir la eliminación del perfil de inscripción:** Si se permite que los dispositivos utilicen un perfil que se puede eliminar de forma remota. El valor predeterminado es **Desactivado**.

6. En **Configuración de Apple TV**, especifique esta configuración:

    - **Requerir inscripción de dispositivo:** Impide que los usuarios omitan la inscripción.
    - **Requerir credenciales para la inscripción de dispositivos:** Solicita credenciales durante la inscripción. Cuando esta configuración está desactivada, Apple TV se inscribe como el "usuario predeterminado del Programa de inscripción de dispositivos".
    - **Esperar a que la configuración complete la instalación:** El dispositivo espera en la pantalla del **Asistente de configuración** hasta que se implementen todos los recursos.
    - **Modo supervisado:** Ofrece más capacidad al administrador al configurar restricciones.
    - **Permitir la eliminación del perfil de inscripción:** Permite a los usuarios eliminar los perfiles de inscripción.
    - **Permitir el emparejamiento de dispositivos:** Permite que los dispositivos inscritos a través del Programa de inscripción de dispositivos se administren mediante herramientas de Apple, como Apple App Store y Apple Configurator.



7. En **Opciones del Asistente de configuración de iOS**, seleccione los pasos que el Asistente de configuración de iOS omite cuando los usuarios inician sus dispositivos por primera vez. Cuando se omite una pantalla, la función relacionada utiliza la configuración predeterminada. Los usuarios pueden configurar las funciones omitidas una vez completada la configuración, a menos que restrinja completamente el acceso a esas funciones. Para obtener más información sobre cómo restringir el acceso a las funciones, consulte Directiva de dispositivo de restricciones. El valor predeterminado para todos los elementos está desmarcado. Las siguientes descripciones explican lo que ocurre cuando se selecciona una configuración.



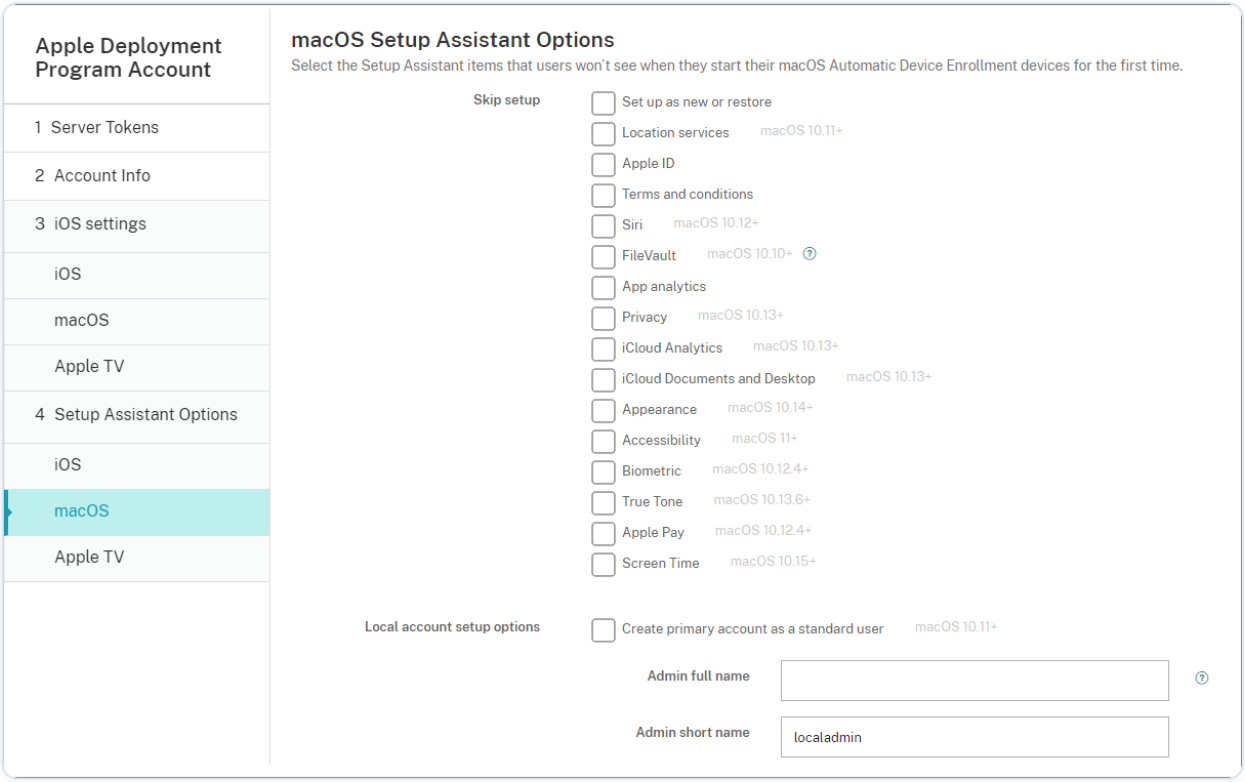
- **Servicios de ubicación:** Impide que los usuarios configuren el servicio de ubicación en el dispositivo.
- **Touch ID:** Impide que los usuarios configuren Touch ID o Face ID en dispositivos iOS. Obsoleto en iOS 15.
- **Bloqueo por código:** Impide a los usuarios configurar un código para el dispositivo. Si no existe un código, los usuarios no pueden usar Touch ID ni Apple Pay.
- **Configurar como nuevo o restaurar:** Impide a los usuarios configurar el dispositivo como nuevo o desde una copia de seguridad de iCloud o Apple App Store.
- **Mover desde Android:** Impide a los usuarios transferir datos de un dispositivo Android a un dispositivo iOS. Esta opción solo está disponible cuando se selecciona **Configurar como nuevo o restaurar** (es decir, se omite el paso).
- **ID de Apple:** Impide a los usuarios configurar una cuenta de ID de Apple gestionado para el dispositivo.
- **Términos y condiciones:** Impide a los usuarios leer y aceptar los términos y condiciones de uso del dispositivo.
- **Apple Pay:** Impide a los usuarios configurar Apple Pay. Si esta opción está desactivada, los usuarios deben configurar Touch ID y el ID de Apple. Asegúrese de que esas opciones estén desactivadas.
- **Siri:** Impide al usuario configurar Siri.

- **Análisis de aplicaciones:** Impide a los usuarios configurar si desean compartir datos de fallos y estadísticas de uso con Apple.
- **Zoom de pantalla:** Impide a los usuarios configurar la resolución de pantalla (estándar o con zoom) en dispositivos iOS. Obsoleto en iOS 17.
- **True Tone:** Impide a los usuarios configurar sensores de cuatro canales para ajustar dinámicamente el balance de blancos de la pantalla.
- **Botón de inicio:** Impide a los usuarios configurar el estilo de respuesta del botón de inicio. Obsoleto en iOS 15.
- **Novedades destacadas:** Impide a los usuarios ver pantallas que muestran información sobre las nuevas funciones del software de Apple.
- **Privacidad:** Impide a los usuarios ver el panel de datos y privacidad. Para iOS 11.3 y versiones posteriores.
- **Actualización de software:** Impide a los usuarios actualizar iOS a la última versión. Para iOS 12.0 y versiones posteriores.
- **Tiempo de uso:** Impide a los usuarios activar Tiempo de uso. Para iOS 12.0 y versiones posteriores.
- **Configuración de SIM:** Impide a los usuarios configurar un plan de datos móviles. Para iOS 12.0 y posterior.
- **iMessage y FaceTime:** Impide a los usuarios habilitar iMessage y FaceTime. Para iOS 12.0 y posterior.
- **Apariencia:** Impide a los usuarios seleccionar el modo de apariencia. Para iOS 13.0 y posterior.
- **Bienvenida:** Impide al usuario ver la pantalla **Empezar**. Para iOS 13.0 y posterior.
- **Restauración completada:** Impide a los usuarios ver si una restauración se completa durante la configuración. Para iOS 14.0 y posterior.
- **Actualización completada:** Impide a los usuarios ver si una actualización de software se completa durante la configuración. Para iOS 14.0 y posterior.
- **App Store:** Impide a los usuarios configurar la App Store. Para iOS 11.1 y posterior.
- **Botón de acción:** Impide a los usuarios ver el panel de configuración del Botón de acción. Para iOS 17.0 y posterior.
- **Modo de aislamiento:** Impide a los usuarios ver el panel del Modo de aislamiento si se ha configurado una cuenta de Apple. Para iOS 17.1 y posterior.
- **Inteligencia:** Impide a los usuarios ver el panel de Inteligencia. Para iOS 18.0 y posterior.

- **Botón de cámara:** Impide a los usuarios ver el panel del Botón de cámara. Para iOS 18.0 y posterior.

La cuenta aparece en **Configuración > Programa de implementación de Apple**.

8. En **Opciones del Asistente de Configuración de macOS**, seleccione los pasos que el Asistente de Configuración de macOS omite cuando los usuarios inician sus dispositivos por primera vez. Cuando se omite una pantalla, la función relacionada utiliza la configuración predeterminada. Los usuarios pueden configurar las funciones omitidas una vez completada la configuración, a menos que restrinja completamente el acceso a esas funciones. Para obtener más información sobre cómo restringir el acceso a las funciones, consulte Directiva de dispositivo de restricciones. La configuración predeterminada para todos los elementos está desactivada. Las siguientes descripciones explican lo que ocurre cuando se selecciona una configuración.



- **Configurar como nuevo o restaurar:** Impide a los usuarios configurar el dispositivo como nuevo, desde una copia de seguridad de Time Machine o realizar una migración del sistema.
- **Servicios de ubicación:** Impide a los usuarios configurar el servicio de ubicación en el dispositivo. Para macOS 10.11 y versiones posteriores.
- **ID de Apple:** Impide a los usuarios configurar una cuenta de ID de Apple gestionado para el dispositivo.

- **Términos y condiciones:** Impide a los usuarios leer y aceptar los términos y condiciones de uso del dispositivo.
- **Siri:** Impide al usuario configurar Siri. Para macOS 10.12 y versiones posteriores.
- **FileVault:** Utilice FileVault para cifrar el disco de arranque. Citrix Endpoint Management solo aplica la configuración de FileVault si el sistema tiene una única cuenta de usuario local y esa cuenta ha iniciado sesión en iCloud.

  Puede utilizar la función de cifrado de disco FileVault de macOS para proteger el volumen del sistema cifrando su contenido (https://support.apple.com/es-es/HT204837). Si ejecuta el asistente de configuración en un Mac portátil de última generación que no tiene FileVault activado, es posible que se le pida que active esta función. La solicitud aparece tanto en sistemas nuevos como en sistemas actualizados a OS X 10.10 o 10.11, pero solo si el sistema tiene una única cuenta de administrador local y esa cuenta ha iniciado sesión en iCloud.
- **Análisis de aplicaciones:** Impide a los usuarios configurar si desean compartir datos de fallos y estadísticas de uso con Apple.
- **Privacidad:** Impide a los usuarios ver el panel Datos y privacidad. Para macOS 10.13 y versiones posteriores.
- **Análisis de iCloud:** Impide a los usuarios elegir si desean enviar datos de diagnóstico de iCloud a Apple. Para macOS 10.13 y versiones posteriores.
- **Documentos y Escritorio de iCloud:** Impide a los usuarios configurar el Escritorio y Documentos de iCloud. Para macOS 10.13 y versiones posteriores.
- **Apariencia:** Impide a los usuarios seleccionar el modo de apariencia. Para macOS 10.14 y versiones posteriores.
- **Accesibilidad:** Impide al usuario escuchar Voice Over automáticamente. Solo disponible si el dispositivo está conectado a Ethernet. Para macOS 11 y versiones posteriores.
- **Biométrico:** Impide al usuario configurar Touch ID y Face ID. Para macOS 10.12.4 y versiones posteriores.
- **True Tone:** Impide a los usuarios configurar sensores de cuatro canales para ajustar dinámicamente el balance de blancos de la pantalla. Para macOS 10.13.6 y versiones posteriores.
- **Apple Pay:** Impide a los usuarios configurar Apple Pay. Si esta opción está desactivada, los usuarios deben configurar Touch ID y el ID de Apple. Asegúrese de que las opciones **ID de Apple** y **Biométrico** estén desactivadas.

- **Tiempo de uso:** Impide a los usuarios activar Tiempo de uso. Para macOS 10.15 y versiones posteriores.
- **App Store:** Impide al usuario configurar la App Store. Para macOS 11.1 y versiones posteriores.
- **Desbloquear con Apple Watch:** Impide a los usuarios desbloquear su Mac con un Apple Watch. Para macOS 12 y versiones posteriores.
- **Opciones de configuración de cuenta local:** Especifique la configuración para crear una cuenta en el dispositivo. Citrix Endpoint Management crea primero la cuenta de administrador local utilizando la información que especifique aquí. Cuando los usuarios activan su dispositivo, se crea una cuenta de usuario como cuenta principal. La opción **Crear cuenta principal como usuario estándar** determina si la cuenta principal tiene privilegios de administrador.

Importante:

Puede seleccionar **Crear cuenta principal como usuario estándar** solo después de establecer **Esperar a que la configuración complete la instalación** en **Activado** en la página **Configuración de macOS**.

- **Crear cuenta principal como usuario estándar:** Cuando se selecciona, Citrix Endpoint Management crea el usuario con permisos estándar en lugar de concederle privilegios de administrador en el dispositivo. Omita esta opción si desea conceder al usuario privilegios de administrador en el dispositivo. De forma predeterminada, esta opción no está seleccionada.
- **Nombre completo del administrador:** Escriba el nombre que el sistema muestra para la cuenta de administrador.
- **Nombre corto del administrador:** Escriba el nombre que el dispositivo muestra para la carpeta de inicio y en el shell.
- **Contraseña de administrador:** Escriba una contraseña segura para la cuenta de administrador.
- **Mostrar cuenta de administrador en Usuarios y grupos:** Si está desmarcada, la cuenta de administrador no aparece en **Usuarios y grupos** en la configuración de macOS. Si crea la cuenta principal como usuario estándar, habilite esta configuración para ocultar la cuenta de administrador que Citrix Endpoint Management crea primero.

Para mejorar la seguridad, Citrix Endpoint Management comprueba si debe rotar la contraseña de la cuenta de administrador diariamente. De forma predeterminada, Citrix Endpoint Management rota la contraseña cada 7 días. Para cambiar el valor predeterminado, actualice la propiedad del servidor `mac.dep.admin.passwd.rotate`. Para obtener más información, consulte Propiedades del servidor.

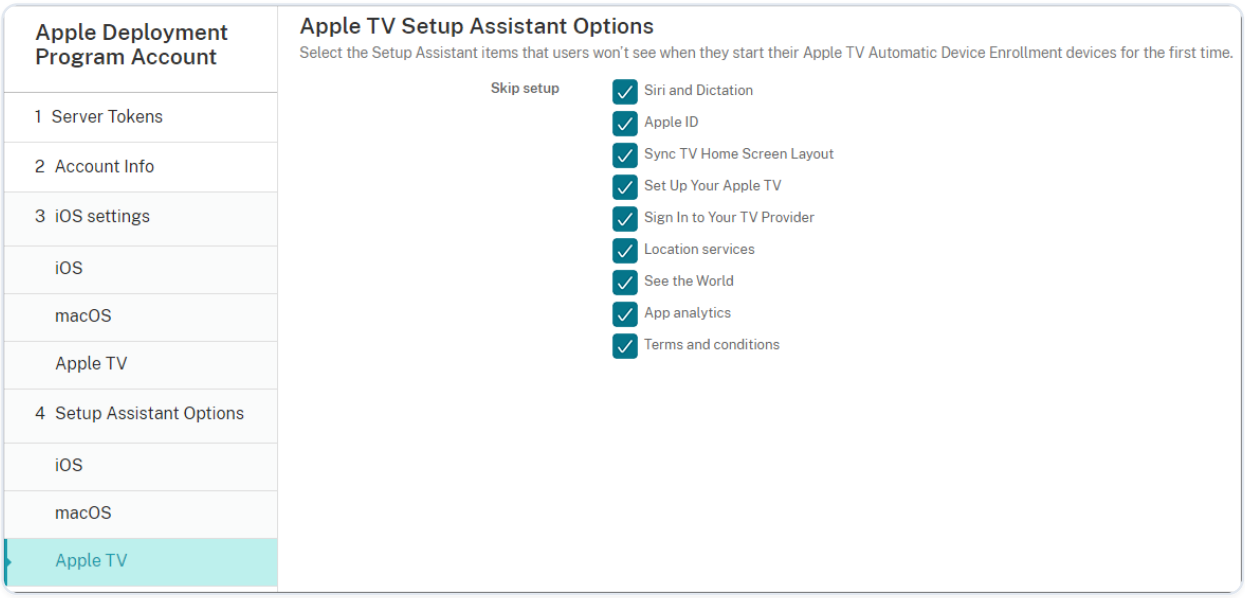
Para aumentar la solidez y la seguridad de las contraseñas, Citrix Endpoint Management genera contraseñas de la siguiente manera:

- 12 caracteres de longitud
- 3 letras mayúsculas
- 3 letras minúsculas
- 3 números
- 3 caracteres especiales: `! \@ # \$ % \^ * ? + = -`

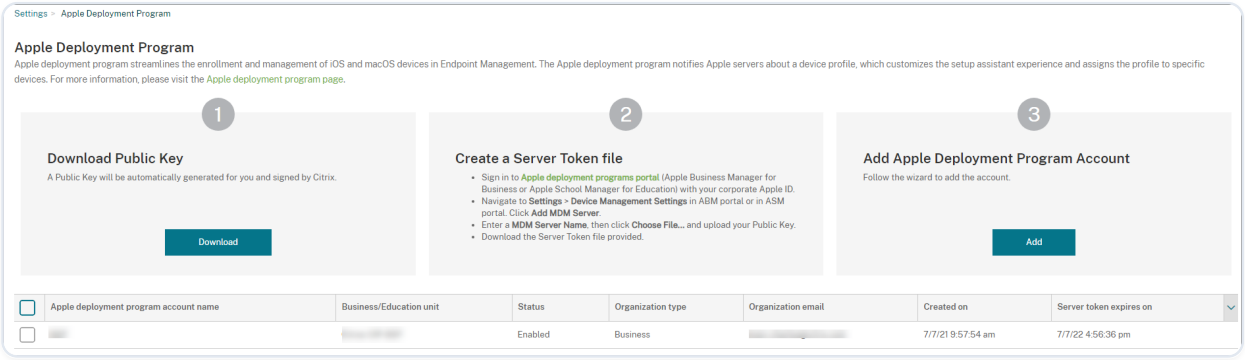
Para ver la contraseña anterior, la contraseña actual y el estado de cambio de contraseña de un dispositivo, vaya a **Administrar > Dispositivos**. Haga clic en ese dispositivo, haga clic en **Mostrar más** y, a continuación, vea la página **Detalles del dispositivo > General**. La sección **Seguridad** muestra lo siguiente:

- **Contraseña de administrador anterior:** Permite ver la contraseña anterior. Citrix Endpoint Management solo muestra la última contraseña. Haga clic en **Mostrar contraseña** para ver la contraseña.
- **Contraseña de administrador actual:** Permite ver la contraseña actual.
- **Cambiar contraseña de administrador:** Permite ver el estado de cambio de contraseña. Puede aparecer la siguiente información, según el estado real:
  - Se solicitó el cambio de contraseña en \<valor de hora específico\>.
  - La contraseña se cambió en \<valor de hora específico\>.
  - Los intentos de cambiar la contraseña fallaron en \<valor de hora específico\>.
  - La contraseña aún no se ha cambiado.

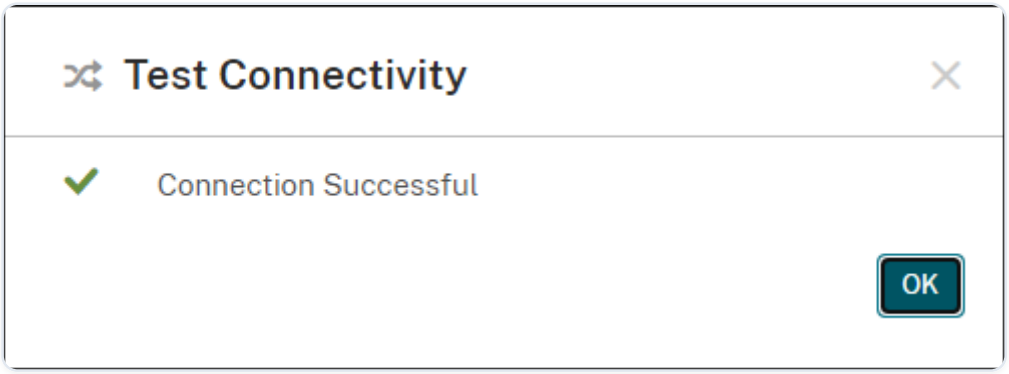
9. En **Opciones del Asistente de configuración de Apple TV**, seleccione los pasos del Asistente de configuración de Apple TV que los usuarios omiten al iniciar sus dispositivos por primera vez. La opción predeterminada para todos los elementos está desactivada. Guarde los cambios.



10. La cuenta aparece en **Parámetros > Programa de implementación de Apple**. Para probar la conectividad entre Citrix Endpoint Management y Apple, seleccione la cuenta y haga clic en **Probar conectividad**.



Aparece un mensaje de estado.



Pedir dispositivos

Puede pedir dispositivos directamente desde los siguientes canales:

- Apple. Proporcione sus números de cliente de Apple al vendedor.

- Distribuidores autorizados de Apple o proveedores participantes. Proporcione su ID de organización al vendedor y obtenga su ID de distribuidor.

Para obtener más información sobre la administración de proveedores de dispositivos, consulte la Guía del usuario de Apple Business Manager o la Guía del usuario de Apple School Manager.

Una vez que se envía el pedido, los dispositivos Apple que compró se agregan a su cuenta de ABM o ASM.

Asignar dispositivos a Citrix Endpoint Management

En el portal de ABM o ASM, busque un número de pedido y utilícelo para asignar los dispositivos de este pedido a su Citrix Endpoint Management. También puede agregar dispositivos iPhone, iPad, iPod touch y Apple TV a ABM o ASM mediante Apple Configurator 2, independientemente de dónde se hayan comprado los dispositivos.

Para obtener más información, consulte la Guía del usuario de Apple Business Manager o la Guía del usuario de Apple School Manager.

Comprar contenido en volumen y sincronizarlo con Citrix Endpoint Management

ABM y ASM le permiten comprar, distribuir y administrar licencias de aplicaciones y libros en volumen desde una única cuenta de organización. Para permitir que su Citrix Endpoint Management se comunique con ABM o ASM para obtener la información de licencia para la distribución, complete los siguientes pasos:

1. En el portal de ABM o ASM, compre aplicaciones y libros públicos en **Apps and Books** y compre aplicaciones personalizadas desarrolladas para su Citrix Endpoint Management en **Custom Apps**.
2. En el portal de ABM o ASM, descargue el token de contenido asignado a su Citrix Endpoint Management.

   Para obtener más información sobre los pasos 1 y 2, consulte la Guía del usuario de Apple Business Manager o la Guía del usuario de Apple School Manager.
3. En la consola de Citrix Endpoint Management, cree una cuenta de Compra por volumen basada en el token de contenido que descargó.

   Para obtener más información, consulte Agregar aplicaciones mediante la Compra por volumen de Apple.

Una vez creada la cuenta de Compra por volumen, las aplicaciones y los libros que compró aparecen en **Administrar** > **Aplicaciones**, y los dispositivos que asignó al servidor de Citrix Endpoint Management aparecen en **Administrar > Dispositivos**.

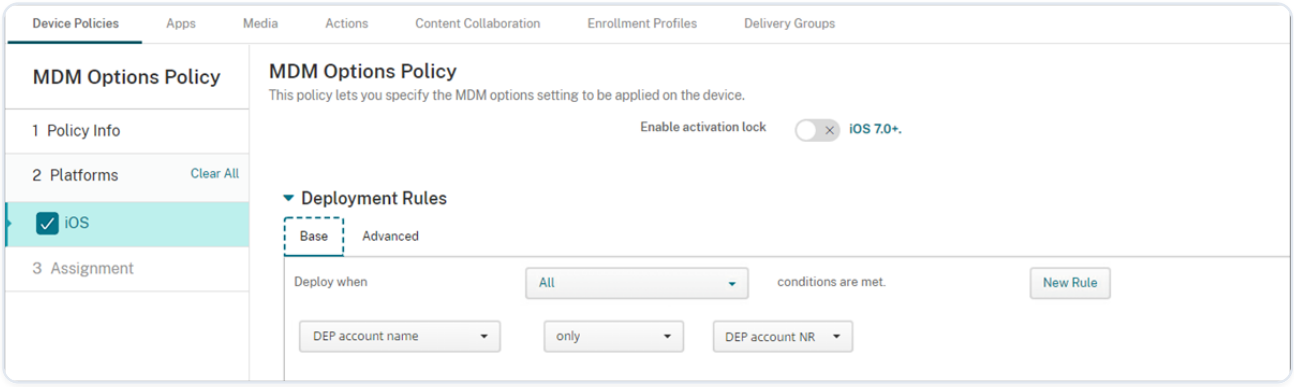
Configurar reglas de implementación para directivas de dispositivos y aplicaciones

Puede asociar cuentas de ABM o ASM con diferentes directivas de dispositivos y aplicaciones al configurar directivas de dispositivos y aplicaciones.

1. En las páginas **Configurar > Directivas de dispositivos** y **Configurar > Aplicaciones**, expanda **Reglas de implementación**.
2. Especifique que una directiva o aplicación se implemente para una cuenta ABM en particular o para todas las cuentas ABM, excepto la seleccionada.

La lista de cuentas ABM incluye solo aquellas cuentas con un estado de habilitado o inhabilitado. Si la cuenta ABM está inhabilitada, el dispositivo ABM no pertenece a esta cuenta. Por lo tanto, Citrix Endpoint Management no implementa la aplicación o directiva en el dispositivo.

En el siguiente ejemplo, una directiva de dispositivo se implementa solo para dispositivos con el nombre de cuenta ABM "ABM Account NR".



Inscribir dispositivos Apple de forma masiva

Puede inscribir un gran número de dispositivos iOS, iPadOS y macOS en Citrix Endpoint Management de dos maneras:

- Utilice los Programas de Implementación de Apple (ADP) para inscribir dispositivos Apple que compre directamente a Apple o a un distribuidor autorizado de Apple participante o a un operador.

  Para obtener más información sobre la implementación de dispositivos habilitados para ADP, consulte Implementar dispositivos a través de los Programas de Implementación de Apple.

Este artículo describe cómo los usuarios inscriben dispositivos habilitados para ADP y cómo volver a inscribir los dispositivos.

- Utilice Apple Configurator 2 para inscribir dispositivos iOS, independientemente de si los compra directamente a Apple.

Este artículo describe cómo implementar dispositivos de forma masiva mediante Apple Configurator 2.

Acerca de la inscripción masiva

Los ADP incluyen Apple Business Manager (ABM) para empresas y Apple School Manager (ASM) para educación. La inscripción masiva a través de los ADP presenta las siguientes características:

- No es necesario tocar ni preparar los dispositivos.
- Una vez que complete la configuración de implementación en Citrix Endpoint Management, puede entregar los dispositivos a los usuarios, quienes podrán empezar a usarlos de inmediato.
- Puede simplificar el proceso de configuración para los usuarios eliminando algunos de los pasos del Asistente de Configuración.
- Para obtener más información sobre la configuración de ABM y ASM, consulte la documentación disponible en Apple Business Manager y Apple School Manager.

La inscripción masiva a través de Apple Configurator 2 presenta las siguientes características:

- Conecte los dispositivos iOS a un Mac con macOS 10.7.2 o posterior y la aplicación Apple Configurator 2. Prepare los dispositivos iOS y configure las directivas a través de Apple Configurator 2.
- Los dispositivos se inscriben automáticamente en Citrix Endpoint Management durante el proceso de configuración. Una vez completada la configuración, Citrix Endpoint Management envía directivas, aplicaciones y otros recursos a los dispositivos. A continuación, puede empezar a administrar los dispositivos.
- Para obtener más información sobre el uso de Apple Configurator 2, consulte la Ayuda de Apple Configurator.

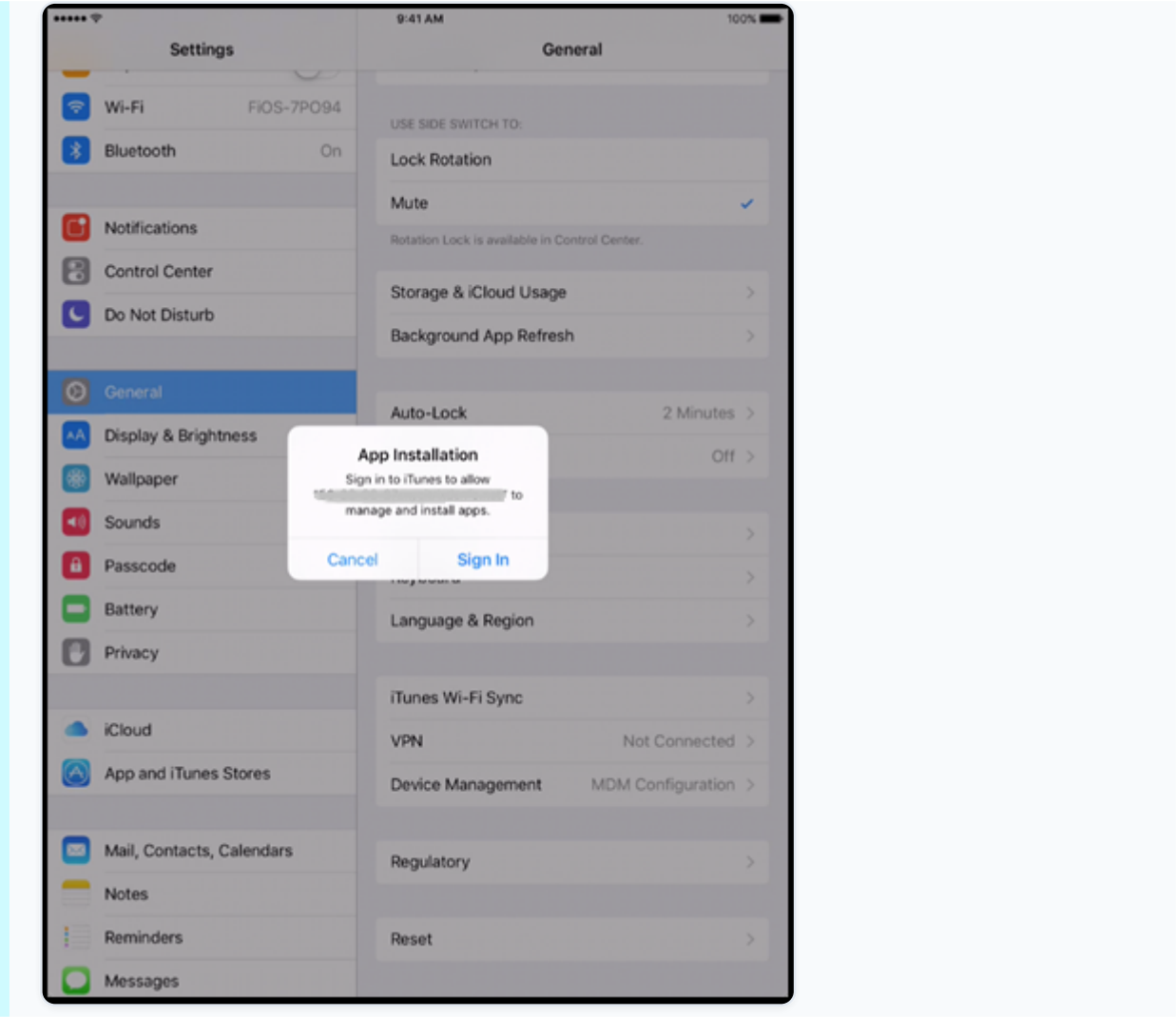
Cómo los usuarios inscriben dispositivos habilitados para ADP

Los usuarios inscriben sus dispositivos en Citrix Endpoint Management de la siguiente manera:

1. Los usuarios inician su dispositivo.

2. Citrix Endpoint Management entrega al dispositivo la configuración de ADP que configuró en la página **Settings > Apple Deployment Programs**.
3. Los usuarios configuran los ajustes iniciales en su dispositivo.
4. El dispositivo inicia automáticamente el proceso de inscripción de dispositivos de Citrix Endpoint Management.
5. Los usuarios continúan configurando los demás ajustes iniciales en su dispositivo.
6. En la pantalla de inicio, es posible que se les pida a los usuarios que inicien sesión en la App Store de Apple para que puedan descargar Citrix Secure Hub.

> **Nota:**
>
> Este paso es opcional si configura Citrix Endpoint Management para implementar la aplicación Citrix Secure Hub mediante la asignación de aplicaciones de compra por volumen basada en dispositivos. En este caso, no necesita crear una cuenta de Apple App Store ni usar una cuenta existente.



7. Los usuarios abren Citrix Secure Hub e introducen sus credenciales. Si la directiva lo requiere, es posible que se les pida a los usuarios que creen y verificar un PIN de Citrix.

   Citrix Endpoint Management implementa las aplicaciones restantes necesarias en el dispositivo.

Volver a inscribir los dispositivos habilitados para ADP

Los dispositivos habilitados para ADP se inscriben desde un estado de restablecimiento de fábrica. Para volver a inscribir un dispositivo habilitado para ADP, primero debe completar un borrado completo para anular la inscripción del dispositivo. Los pasos detallados son los siguientes:

1. En la página **Administrar > Dispositivos**, seleccione el dispositivo.
2. Haga clic en **Seguridad**.
3. Haga clic en **Borrado completo** para anular la inscripción del dispositivo y dejarlo en el estado de restablecimiento de fábrica.

4. Inicie el dispositivo.

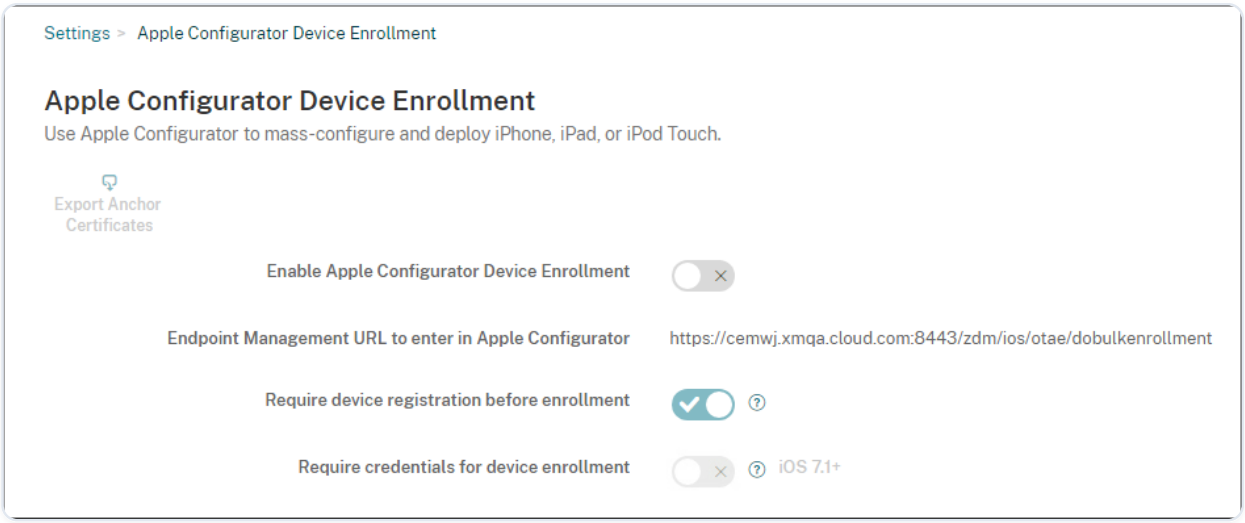
> **Importante:**
>
> No utilice **Borrado selectivo** para anular la inscripción de un dispositivo habilitado para ADP, ya que la inscripción de ADP requiere que el dispositivo esté en el estado de restablecimiento de fábrica.

Implementar dispositivos con Apple Configurator 2

Puede usar Apple Configurator 2 para implementar un gran número de dispositivos con configuraciones, aplicaciones y datos, e inscribir estos dispositivos en Citrix Endpoint Management.

Paso 1: Configurar los ajustes en Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Inscripción de dispositivos con Apple Configurator**.

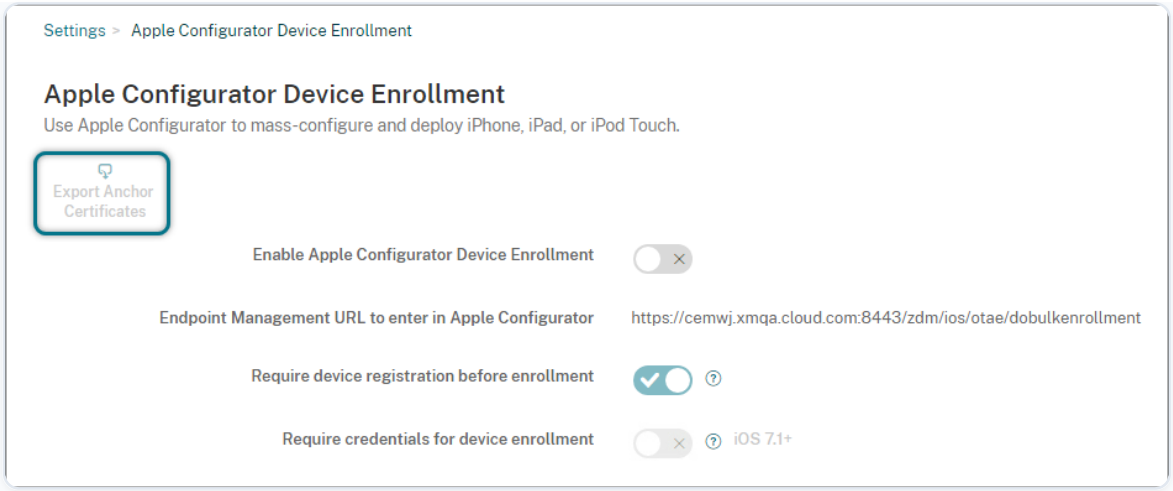


2. Establezca **Habilitar la inscripción de dispositivos con Apple Configurator** en **Sí**.
3. Copie el ajuste **URL de inscripción para introducir en Apple Configurator** y pegue esta URL cuando configure los ajustes en Apple Configurator 2. Este ajuste proporciona la URL del servidor de Citrix Endpoint Management que se comunica con Apple. La URL de inscripción es el nombre de dominio completo (FQDN) del servidor de Citrix Endpoint Management, como `mdm.server.url.com`, o la dirección IP.
4. Para evitar que se inscriban dispositivos desconocidos, establezca **Requerir el registro del dispositivo antes de la inscripción** en **Sí**. Nota: Si este ajuste está establecido en **Sí**, debe

agregar los dispositivos configurados a **Administrar > Dispositivos** en Citrix Endpoint Management manualmente o a través de un archivo CSV antes de la inscripción.

5. Para exigir a los usuarios de dispositivos iOS que introduzcan sus credenciales al inscribirse, establezca **Requerir credenciales para la inscripción de dispositivos** en **Sí**. El valor predeterminado es **No**.

> **Nota:**
>
> Si el servidor de Citrix Endpoint Management utiliza un certificado SSL de confianza, omita este paso. Haga clic en **Exportar certificados de anclaje** y guarde el archivo certchain.pem en el llavero de macOS (inicio de sesión o Sistema).



Paso 2: Configurar los ajustes en Apple Configurator 2

1. Prepare un Mac que ejecute macOS 10.7.2 o posterior y tenga Apple Configurator 2 instalado.
2. Utilice un cable Dock Connector a USB para conectar dispositivos Apple al Mac. Puede configurar hasta 30 dispositivos conectados simultáneamente. Si no tiene un Dock Connector, utilice uno o varios concentradores USB 2.0 de alta velocidad con alimentación para conectar los dispositivos.
3. Inicie Apple Configurator 2. El configurador muestra los dispositivos que puede preparar para la supervisión.
4. Para preparar un dispositivo para la supervisión:

   - Seleccione **Supervisar dispositivos** si tiene la intención de mantener el control del dispositivo volviendo a aplicar una configuración regularmente. Haga clic en **Siguiente**.

> **Importante:**
>
> Poner un dispositivo en modo supervisado instala la versión seleccionada de iOS en el dispositivo, borrando completamente cualquier dato de usuario o aplicación previamente almacenados en el dispositivo.

- En iOS, haga clic en **Más reciente** para la última versión de iOS que desee instalar.

5. En **Inscribir en el servidor MDM**, elija un servidor MDM. Para añadir un servidor, haga clic en **Siguiente**.
6. En **Definir un servidor MDM**, proporcione un nombre para el servidor y pegue la URL del servidor MDM desde la consola de Citrix Endpoint Management.
7. En **Asignar a la organización**, elija una organización para supervisar el dispositivo.

   Para obtener más información sobre cómo preparar dispositivos con Apple Configurator 2, consulte la página de ayuda de Apple Configurator, Preparar dispositivos.
8. A medida que se prepara cada dispositivo, enciéndalo para iniciar el Asistente de configuración de iOS, que prepara el dispositivo para el primer uso.

Agregar dispositivos a ABM o ASM con Apple Configurator 2

Puede agregar dispositivos iPhone, iPad y Apple TV a su cuenta de ABM o ASM con Apple Configurator 2, independientemente de dónde se hayan comprado los dispositivos. Después de agregar dispositivos, estos aparecen en la sección **Dispositivos**. Estos dispositivos ya no incluyen la configuración de inscripción asignada a través de Apple Configurator 2. Para obtener más información, consulte la Guía del usuario de Apple Business Manager o la Guía del usuario de Apple School Manager.

Renovar el token ADP

Citrix Endpoint Management muestra una advertencia de caducidad de la licencia cuando caduca su token ADP. Reemplace el token de ASM o ABM.

Paso 1: Descargar una clave pública del servidor de Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Programa de implementación de Apple** para descargar una nueva clave pública.

Paso 2: Crear y descargar un archivo de token de servidor desde su cuenta de Apple

1. Inicie sesión en ABM para descargar el token.

2. Abra **Parámetros** y seleccione el servidor del que necesita un token. Haga clic en **Modificar**.
3. En **Parámetros del servidor MDM**, cargue la nueva clave pública que descargó de Citrix Endpoint Management y guarde los cambios.
4. Haga clic en **Descargar token** para descargar el nuevo token.

Paso 3: Cargar un archivo de token de servidor en Citrix Endpoint Management

1. En Citrix Endpoint Management, vaya a **Ajustes > Programa de implementación de Apple**.
2. Seleccione la cuenta del Programa de implementación, haga clic en **Modificar** y cargue el archivo de token del servidor.
3. Haga clic en **Siguiente** y guarde los cambios.

Integrar con las funciones de Apple Education

Puede usar Citrix Endpoint Management como su solución de Administración de dispositivos móviles (MDM) en un entorno que utiliza Apple Education. La compatibilidad con Citrix Endpoint Management incluye Apple School Manager (ASM) y la aplicación Classroom para iPad. La directiva de dispositivo de configuración educativa de Citrix Endpoint Management configura los dispositivos de instructores y estudiantes para su uso con Apple Education.

Usted proporciona iPads preconfigurados y supervisados a instructores y estudiantes. Esa configuración incluye la inscripción de ASM en Citrix Endpoint Management, una cuenta de ID de Apple gestionado configurada con una nueva contraseña y las aplicaciones y iBooks de compra por volumen requeridos.

Para obtener más información sobre las funciones de Apple Education, consulte el sitio de Apple Education y la Guía de implementación de Apple Education del mismo sitio.

Apple School Manager

Siga estos pasos generales para integrar Citrix Endpoint Management con ASM.

1. Cree una cuenta para su institución en ASM para inscribir su institución en ASM.
2. Configure una cuenta de compra por volumen educativa para Apple School Manager.
3. Agregue contraseñas para los usuarios de Apple School Manager.
4. Planifique y agregue recursos y grupos de entrega a Citrix Endpoint Management.
5. Pruebe las inscripciones de dispositivos de instructores y estudiantes.
6. Proporcione los dispositivos preconfigurados a instructores y estudiantes.
7. Administre los datos de instructores, estudiantes y clases.

8. Si un dispositivo se pierde o es robado, puede bloquearlo y localizarlo.

Para obtener información sobre cómo inscribirse en ASM y conectar su cuenta a Citrix Endpoint Management, consulte Implementar dispositivos a través del programa de implementación de Apple.

Requisitos previos

- NetScaler Gateway
- Perfil de inscripción configurado para MDM+MAM.
- Apple iPad de tercera generación (versión mínima) o iPad Mini, con iOS 9.3 (versión mínima)

> **Nota:**
>
> Citrix Endpoint Management no valida las cuentas de usuario de ASM con LDAP o Active Directory. Sin embargo, puede conectar Citrix Endpoint Management a LDAP o Active Directory para la administración de usuarios y dispositivos no relacionados con instructores o estudiantes de ASM. Por ejemplo, puede usar Active Directory para proporcionar Citrix Secure Mail y Citrix Secure Web a otros miembros de ASM, como administradores de TI y gerentes.

> Dado que los instructores y estudiantes de ASM son usuarios locales, no es necesario implementar Citrix Secure Hub en sus dispositivos.

> La inscripción de MAM que incluye la autenticación de NetScaler Gateway no admite usuarios locales (solo usuarios de Active Directory). Por lo tanto, Citrix Endpoint Management implementa solo las aplicaciones de compra por volumen y los iBooks necesarios en los dispositivos de instructores y estudiantes.

Aplicación Classroom para iPad

La aplicación Classroom para iPad permite a los instructores conectarse y administrar los dispositivos de los estudiantes. Puede ver las pantallas de los dispositivos, abrir aplicaciones en iPads, compartir y abrir enlaces web, y presentar la pantalla de un estudiante en Apple TV.

Classroom es gratuita en la App Store. Cargue la aplicación en la consola de Citrix Endpoint Management. Luego, use la directiva de dispositivo de Configuración de educación para configurar la aplicación Classroom, que implementa en los dispositivos de los instructores.

Para obtener más información sobre cómo implementar la aplicación Classroom, consulte Distribuir aplicaciones de Apple.

Para obtener más información sobre los requisitos, la configuración y las funciones de la aplicación Classroom, consulte la guía del usuario de Classroom en el sitio de soporte de Apple.

Agregar contraseñas para usuarios de Apple School Manager

Después de agregar una cuenta de ASM, Citrix Endpoint Management importa clases y usuarios de ASM. Citrix Endpoint Management trata las clases como grupos locales y usa el término "grupo" en la consola. Si una clase tiene un nombre de grupo en ASM, Citrix Endpoint Management asigna el nombre de grupo a la clase. De lo contrario, Citrix Endpoint Management usa el ID del sistema de origen para el nombre del grupo. Citrix Endpoint Management no usa el nombre del curso para el nombre de la clase porque los nombres de los cursos en ASM no son únicos.

Citrix Endpoint Management utiliza los ID de Apple gestionados para crear usuarios locales con el tipo de usuario **ASM**. Los usuarios son locales porque ASM crea las credenciales independientemente de todas las fuentes de datos externas. Como resultado, Citrix Endpoint Management no utiliza un servidor de directorio para autenticar a estos nuevos usuarios.

ASM no envía contraseñas temporales de usuario a Citrix Endpoint Management. Puede importarlas desde un archivo CSV o agregarlas manualmente. Para importar contraseñas temporales de usuario:

1. Obtenga el archivo CSV generado por ASM al crear las contraseñas temporales de ID de Apple gestionados.
2. Edite el archivo CSV, sustituyendo las contraseñas temporales por nuevas contraseñas que los usuarios proporcionen para inscribirse en Citrix Endpoint Management. No hay restricciones en el tipo de contraseña para este fin.

   El formato de una entrada en el archivo CSV es el siguiente: `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`!

   Donde:

   Usuario: `user@appleid.citrix.com`

   Nombre: `Firstname`

   Segundo nombre: `Middle`

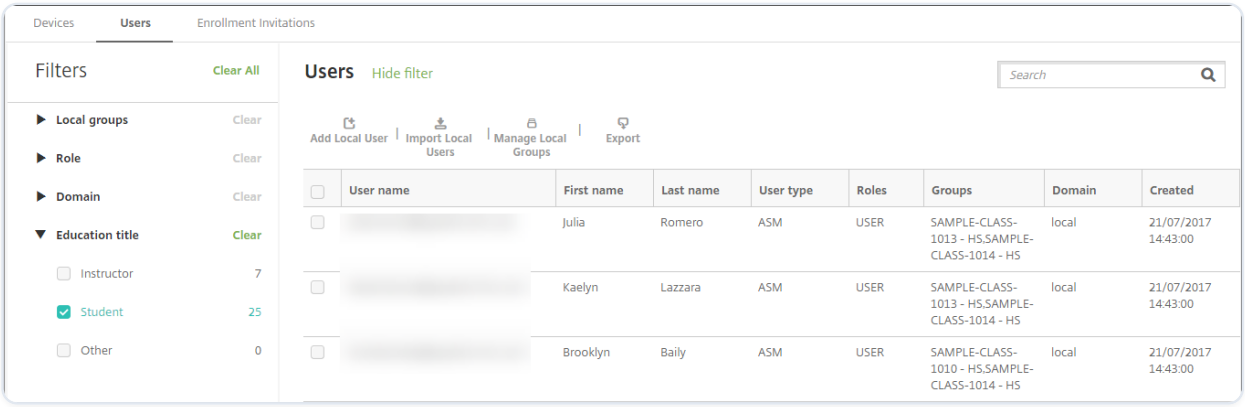
Apellido: `Lastname`

Contraseña: `Password123!`!

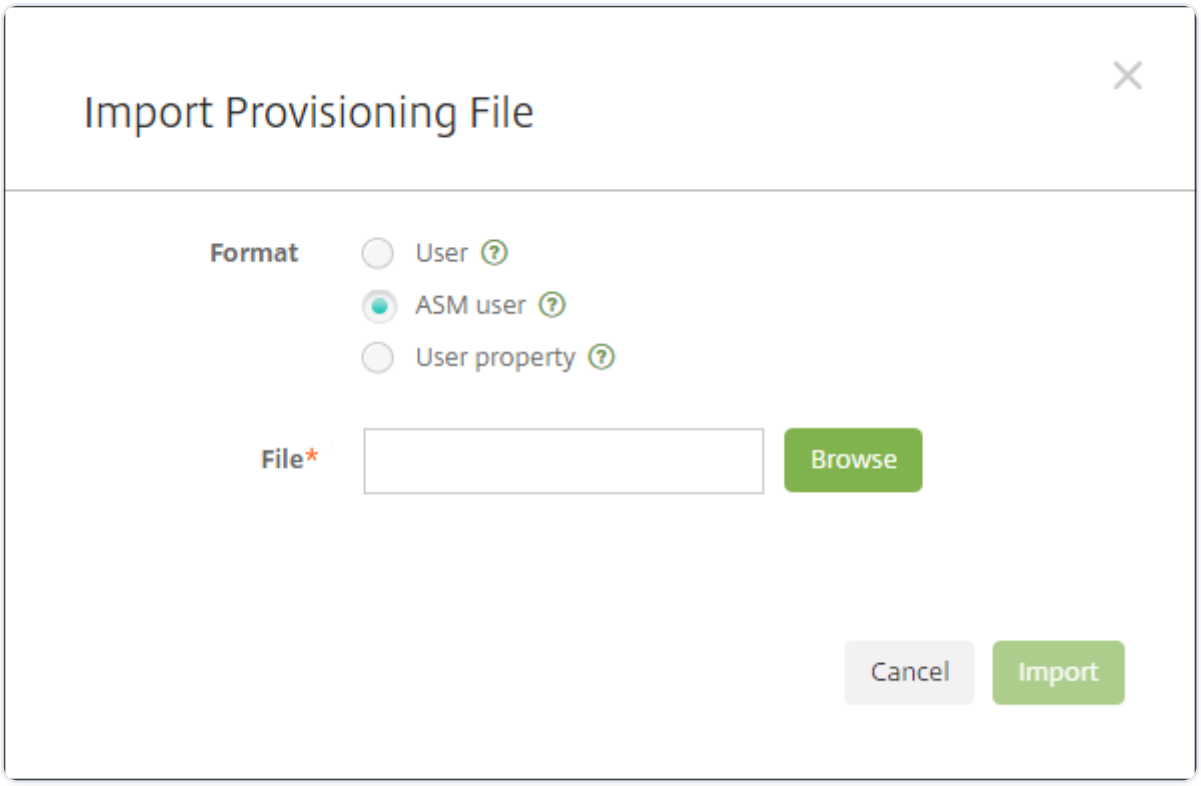
3. En la consola de Citrix Endpoint Management, haga clic en **Administrar > Usuarios**. Aparece la página **Usuarios**.

   La siguiente muestra de pantalla de **Administrar > Usuarios** muestra una lista de usuarios importados de ASM. En la lista de **Usuarios**:

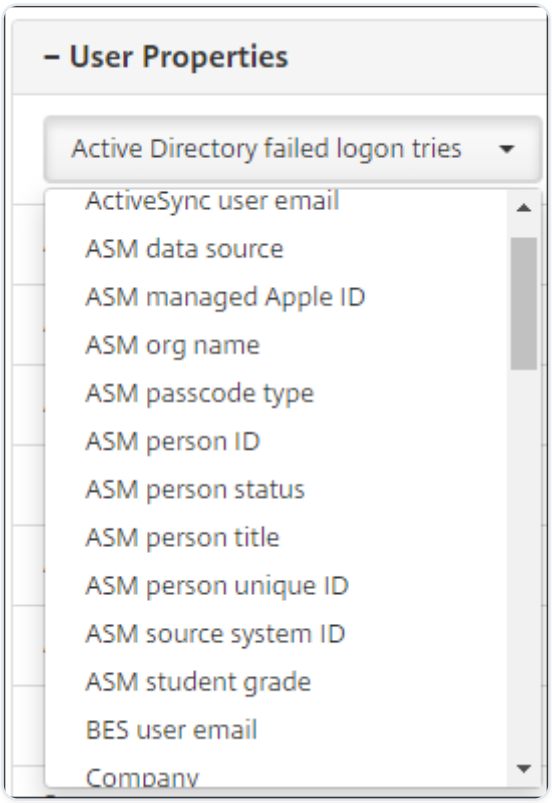
   - **Nombre de usuario** muestra el ID de Apple gestionado.
   - El tipo de usuario es **ASM**, para indicar que la cuenta se originó en ASM.
   - Los **Grupos** muestran las clases.



4. Haga clic en **Importar usuarios locales**. Aparece el cuadro de diálogo **Importar archivo de aprovisionamiento**.
5. En Formato, elija **Usuario de ASM**, vaya al archivo CSV que preparó en el paso 2 y, a continuación, haga clic en **Importar**.



6. Para ver las propiedades de un usuario local, seleccione el usuario y, a continuación, haga clic en **Modificar**.



Además de las propiedades de nombre, están disponibles estas propiedades de ASM:

- **Origen de datos de ASM:** El origen de datos de la clase, como **CSV** o **SFTP**.

- **ID de Apple gestionado de ASM:** Un ID de Apple gestionado puede incluir el nombre de su institución y `appleid`. Por ejemplo, el ID podría ser similar a johnappleseed@appleid.myschool.edu. Citrix Endpoint Management requiere un ID de Apple gestionado para la autenticación.
- **Nombre de la organización de ASM:** El nombre que asignó a la cuenta en Citrix Endpoint Management.
- **Tipo de código de acceso de ASM:** Política de contraseñas de la persona: **compleja** (una contraseña que no es de estudiante de ocho o más números y letras), **cuatro** (dígitos) o **seis** (dígitos).
- **ID único de persona de ASM:** Identificador del usuario.
- **Estado de la persona de ASM:** Especifica si el ID de Apple gestionado está **Activo** o **Inactivo**. Este estado se activa después de que el usuario proporcione su nueva contraseña para la cuenta del ID de Apple gestionado.
- **Título de la persona de ASM:** Instructor, Estudiante u Otro.
- **ASM person unique ID:** Identificador único para el usuario.
- **ASM source system ID:** Identificador para el origen del sistema.
- **ASM student grade:** Información de la calificación del estudiante (no utilizada por los instructores).

Planificar y agregar recursos y grupos de entrega a Citrix Endpoint Management

Un grupo de entrega especifica los recursos que se implementarán en categorías de usuarios. Por ejemplo, puede crear un grupo de entrega para instructores y estudiantes. Alternativamente, puede crear varios grupos de entrega para personalizar las aplicaciones, los medios y las directivas que se envían a varios instructores o estudiantes. Puede crear uno o varios grupos de entrega por clase. También puede crear uno o varios grupos de entrega para administradores (otro personal de su institución educativa).

Los recursos que implementa en los dispositivos de los usuarios incluyen directivas de dispositivo, aplicaciones de compra por volumen (Volume Purchase apps) e iBooks.

- Directivas de dispositivo:

  Si los instructores utilizan la aplicación Classroom, se requiere la directiva de dispositivo de configuración educativa. Asegúrese de revisar otras directivas de dispositivo para determinar cómo desea configurar y restringir los iPads de instructores y estudiantes.

- Aplicaciones de compra por volumen:

Citrix Endpoint Management requiere que implemente aplicaciones de compra por volumen como aplicaciones obligatorias para los usuarios educativos. Citrix Endpoint Management no admite la implementación de dichas aplicaciones de compra por volumen como opcionales.

Si utiliza la aplicación Apple Classroom, impleméntela solo en los dispositivos de los instructores.

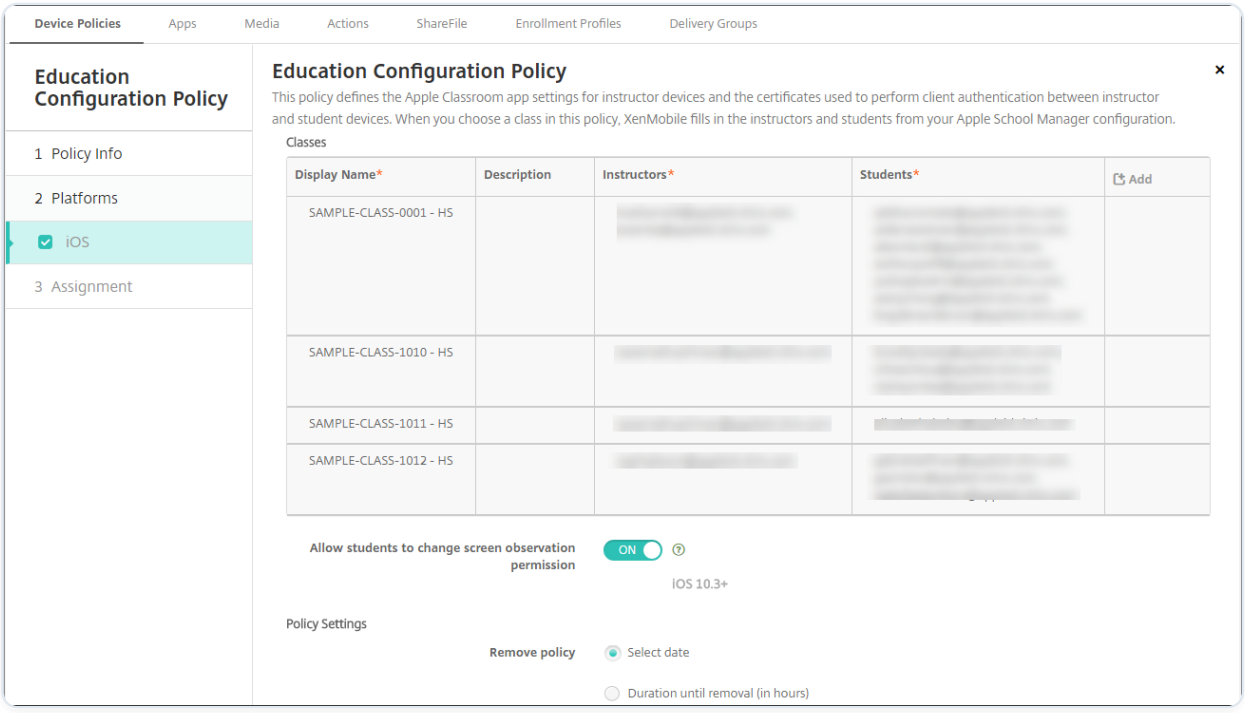
Implemente cualquier otra aplicación que desee proporcionar a instructores o estudiantes. Esta solución no utiliza la aplicación Citrix Secure Hub, por lo que no es necesario implementarla en instructores o estudiantes.

- iBooks de compra por volumen:

  Después de que Citrix Endpoint Management se conecte a su cuenta de ASM, los iBooks que haya comprado aparecerán en la consola de Citrix Endpoint Management, en **Configurar > Medios**. Los iBooks que aparecen en esa página están disponibles para agregarlos a los grupos de entrega. Citrix Endpoint Management solo admite la adición de iBooks como medios obligatorios.

Después de planificar los recursos y los grupos de entrega para instructores y estudiantes, puede crear esos elementos en la consola de Citrix Endpoint Management.

1. Cree las directivas de dispositivo que desee implementar en los dispositivos de instructores o estudiantes. Para obtener información sobre la directiva de dispositivo de configuración educativa, consulte Directiva de dispositivo de configuración educativa.

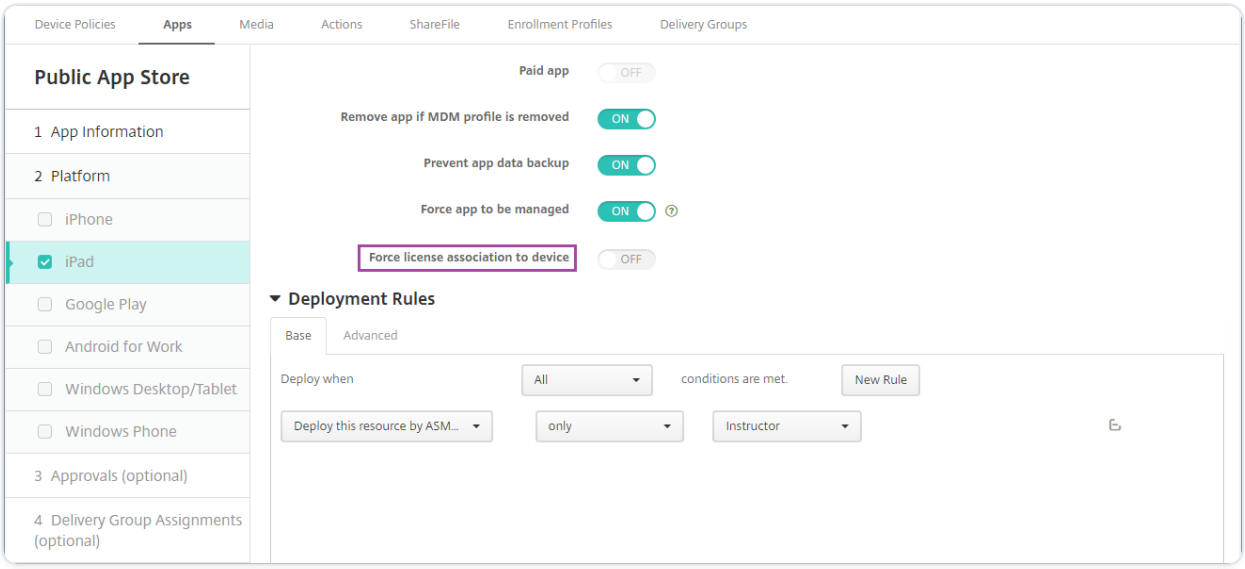


Para obtener información sobre las directivas de dispositivo, consulte Directivas de dispositivo y los artículos de directivas individuales.

2. Configure las aplicaciones (**Configurar > Aplicaciones**) y los iBooks (**Configurar > Contenido multimedia**):

   - De forma predeterminada, Citrix Endpoint Management asigna aplicaciones e iBooks a nivel de usuario. Durante la primera implementación, los instructores y los estudiantes reciben una solicitud para registrarse en ASM. Después de aceptar la invitación, los usuarios reciben sus aplicaciones e iBooks de ASM en la siguiente implementación (en un plazo de seis horas). Citrix recomienda forzar la implementación de aplicaciones e iBooks a los nuevos usuarios de ASM. Para ello, seleccione el grupo de entrega y haga clic en **Implementar**.

     Puede optar por asignar aplicaciones (pero no iBooks) a nivel de dispositivo. Para ello, cambie la configuración **Forzar asociación de licencias al dispositivo** a **Activado**. Cuando asigna aplicaciones a nivel de dispositivo, los usuarios no reciben una invitación para unirse al programa de compra por volumen.

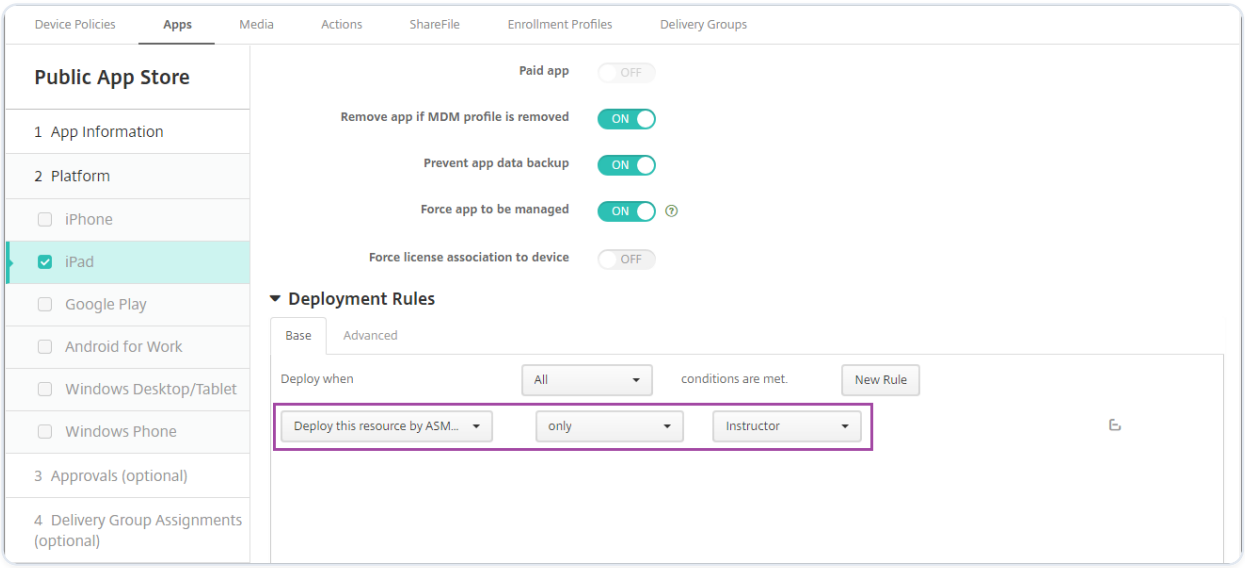


   - Para implementar una aplicación solo para instructores, seleccione un grupo de entrega que incluya solo instructores o utilice la siguiente regla de implementación:

```
Deploy this resource by ASM device type

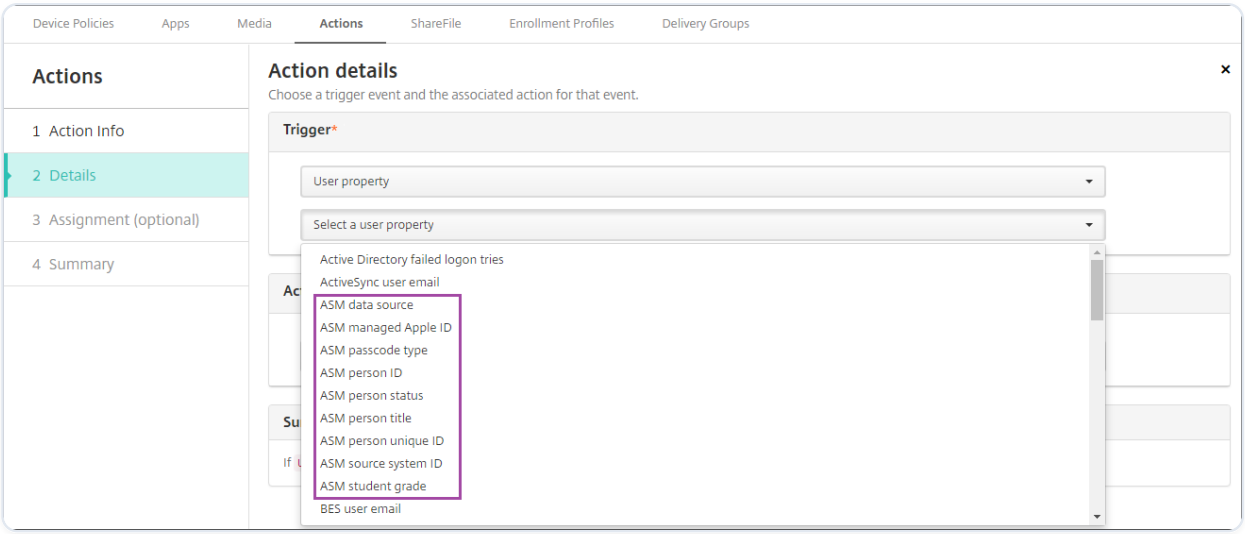
only

Instructor
```



- Para obtener ayuda con la adición de aplicaciones de compra por volumen, consulte Agregar una aplicación de la App Store pública.

3. Opcional. Cree acciones basadas en las propiedades de usuario de ASM. Por ejemplo, puede crear una acción para enviar una notificación a los dispositivos de los estudiantes cuando se instala una nueva aplicación. Alternativamente, puede crear una acción que se active por una propiedad de usuario, como se muestra en el siguiente ejemplo.



Para crear una acción, vaya a **Configurar > Acciones**. Para obtener información sobre la configuración de acciones, consulte Acciones automatizadas.

4. En **Configurar > Grupos de entrega**, cree grupos de entrega para instructores y para estudiantes. Elija las clases que se importaron de ASM. Además, cree una regla de implementación para instructores y estudiantes.

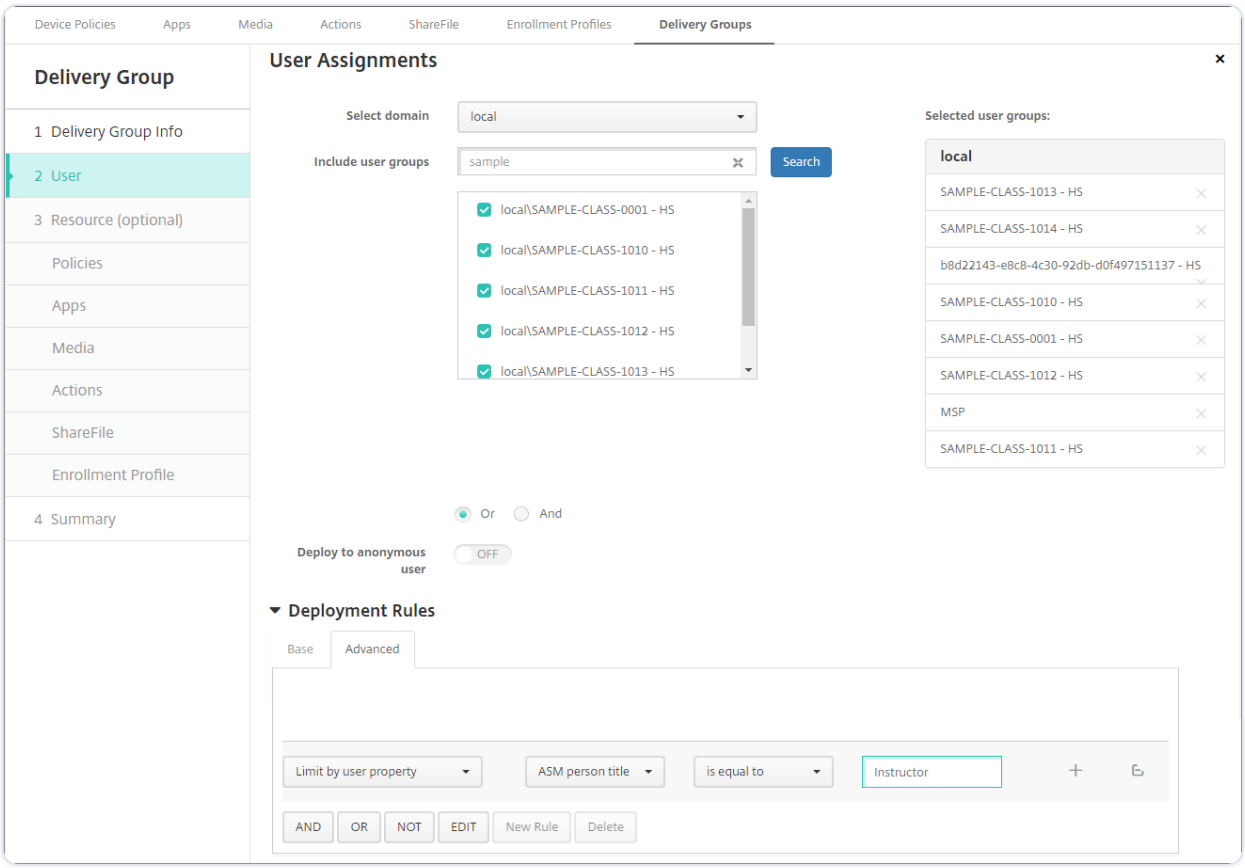
   Por ejemplo, las siguientes asignaciones de usuario son para instructores. La regla de implementación es:

```
Limit by user property

ASM person title

is equal to

Instructor
```



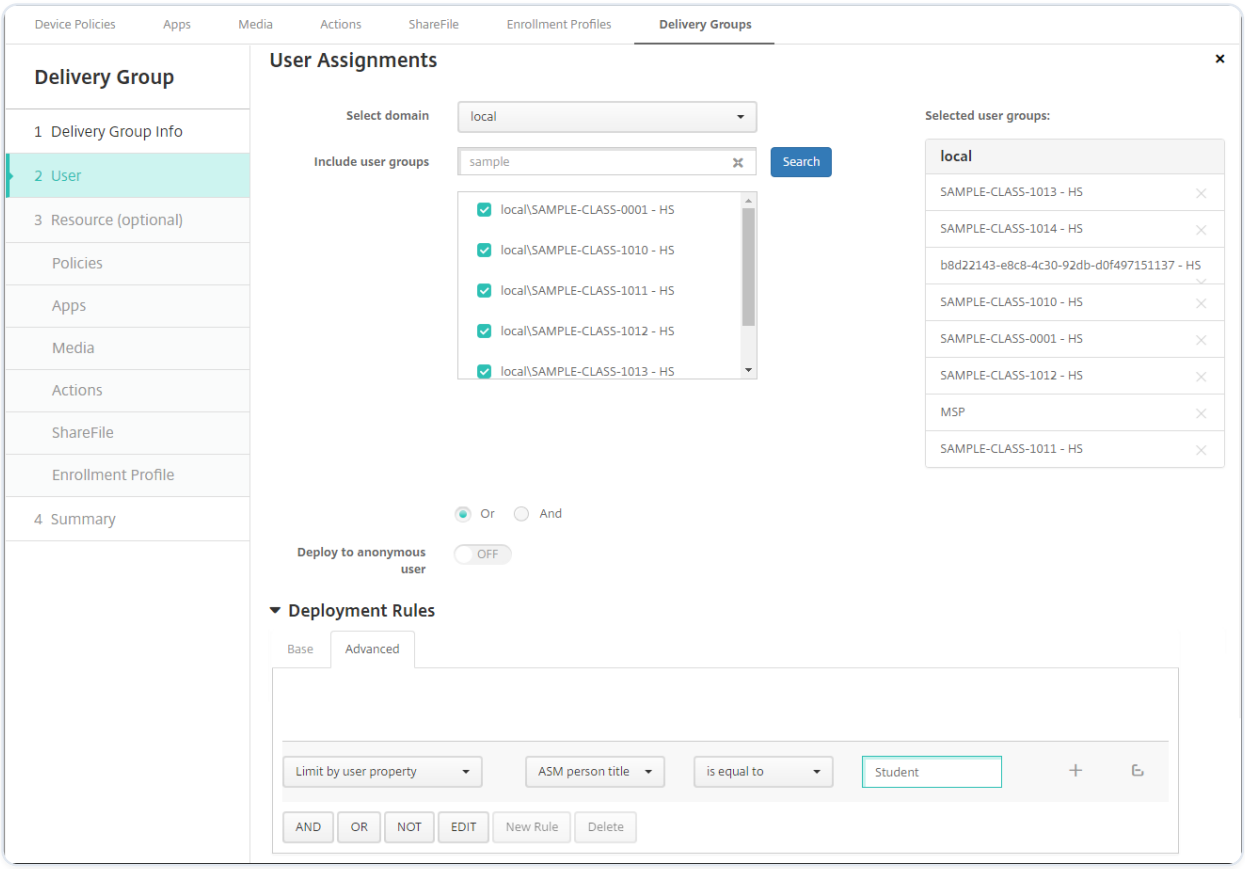
Las siguientes asignaciones de usuario son para estudiantes. La regla de implementación es:

```
Limit by user property

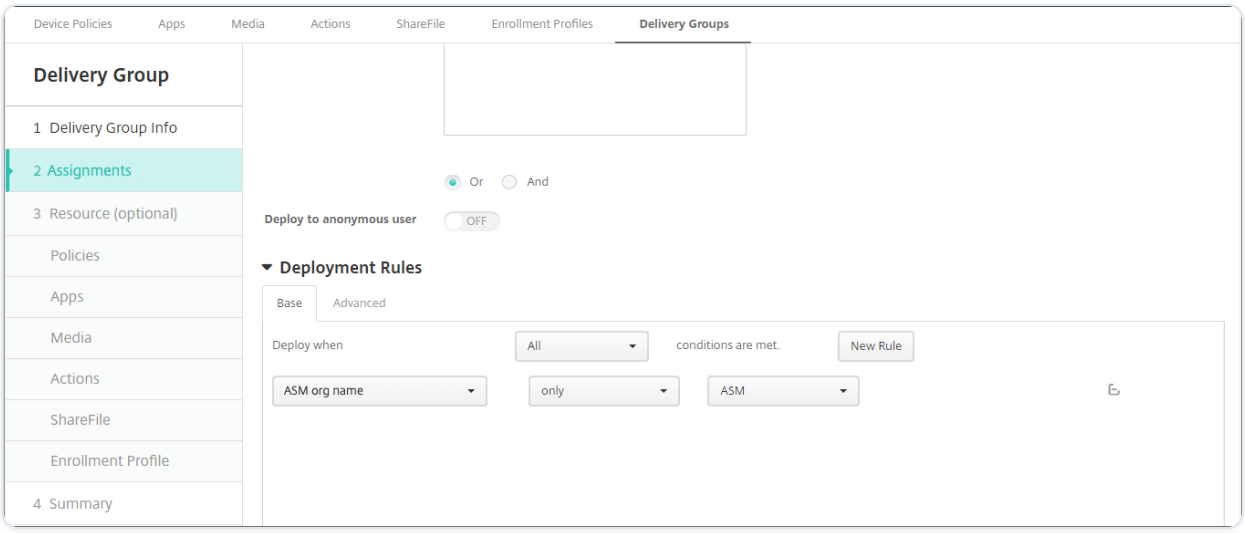
ASM person title

is equal to

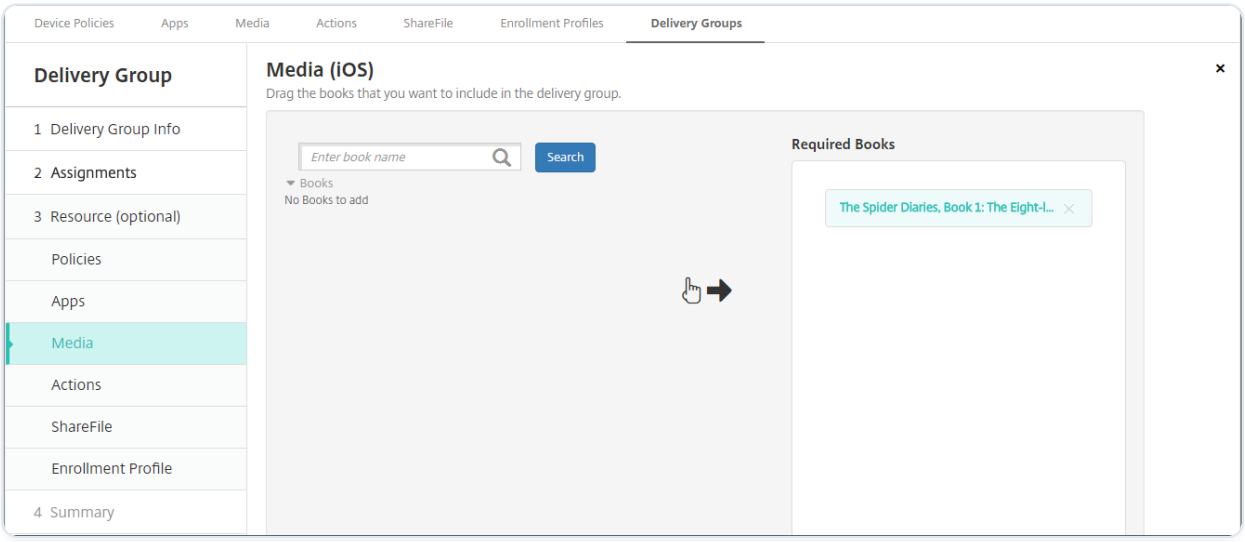
Student
```



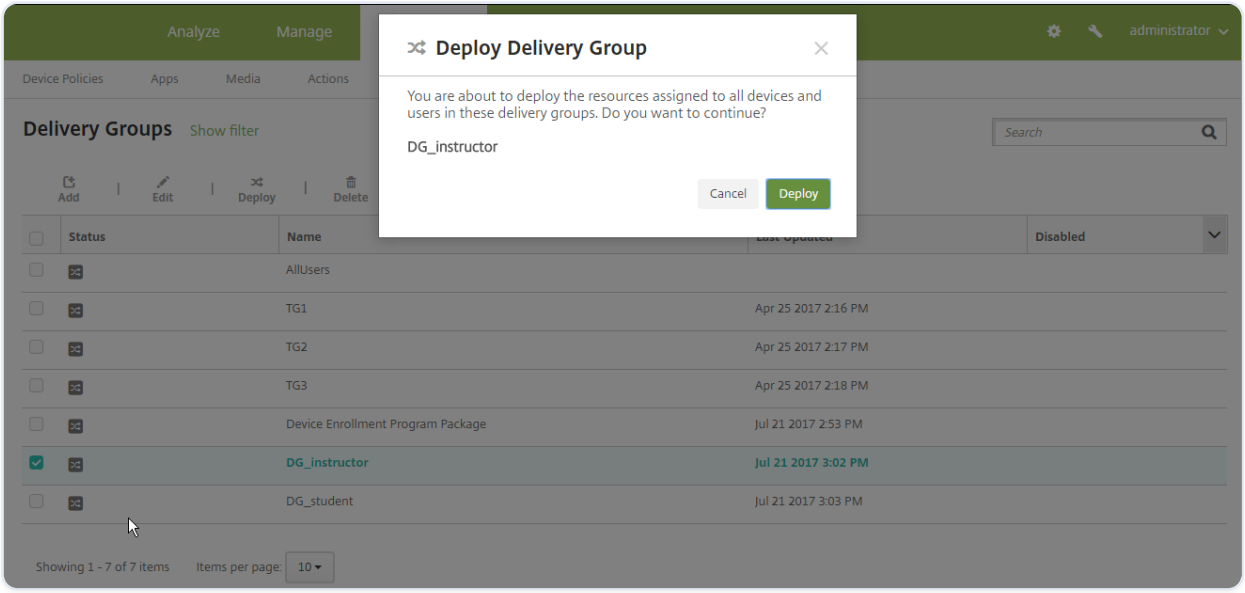
También puede filtrar un grupo de entrega mediante una regla de implementación basada en el nombre de la organización de ASM.



5. Asigne los recursos a los grupos de entrega. El siguiente ejemplo muestra un iBook en un grupo de entrega.



El siguiente ejemplo muestra el cuadro de diálogo de confirmación que aparece al seleccionar un grupo de entrega y hacer clic en **Implementar**.



Para obtener más información, consulte "Para modificar un grupo de entrega" y "Para implementar en grupos de entrega" en Implementar recursos.

Probar las inscripciones de dispositivos de instructores y estudiantes

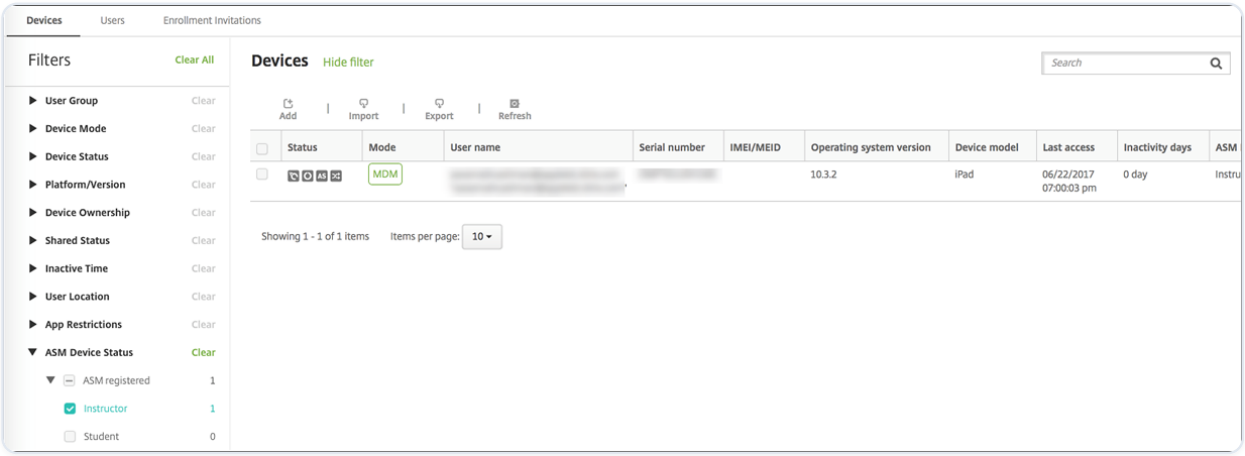
Puede inscribir dispositivos mediante cualquiera de los siguientes métodos:

- Un administrador escolar puede inscribir dispositivos de instructores y estudiantes utilizando la contraseña de usuario que puede establecer en la consola de Citrix Endpoint Management. Como resultado, puede proporcionar a los usuarios dispositivos que ya están configurados con aplicaciones y contenido multimedia.
- Cuando los usuarios reciben los dispositivos, se inscriben utilizando la contraseña de usuario que usted les proporciona. Una vez completada la inscripción, Citrix Endpoint Management envía las directivas de dispositivo, las aplicaciones y el contenido multimedia a los dispositivos.

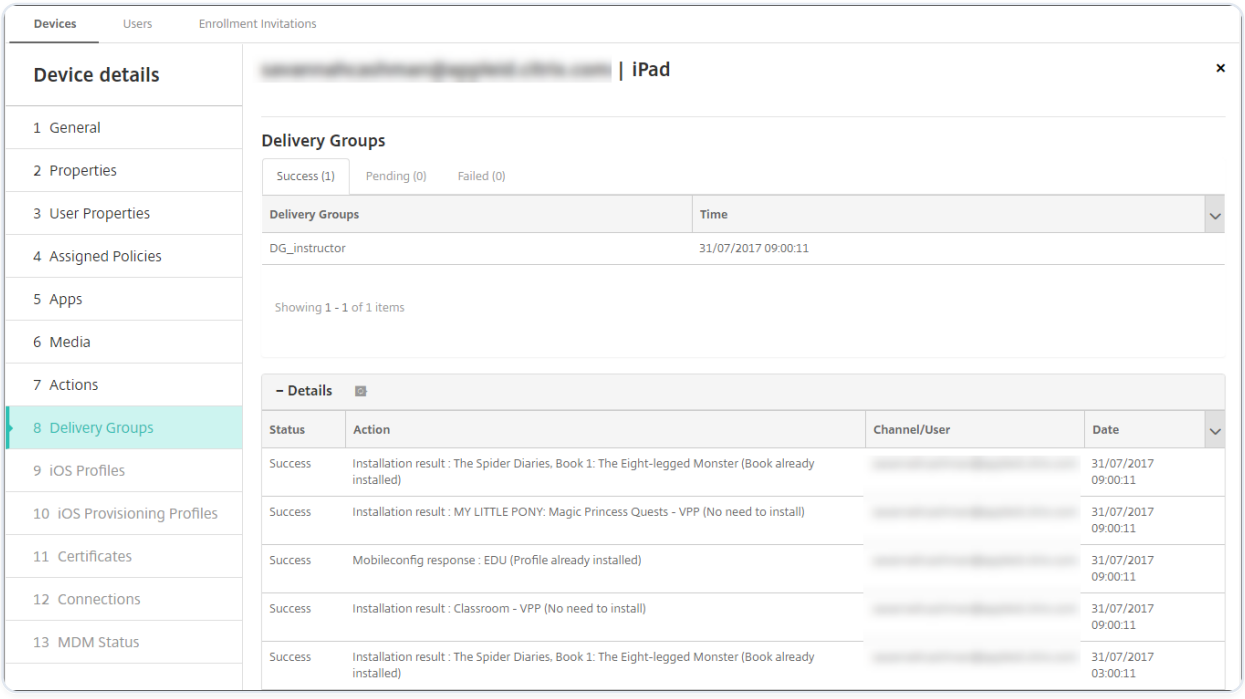
Para probar la inscripción, utilice dispositivos del Programa de implementación de Apple que estén vinculados a ASM.

1. Si los dispositivos no están vinculados a ASM, borre el contenido y la configuración del dispositivo realizando un restablecimiento completo.
2. Inscriba un dispositivo ASM con un instructor. Luego, inscriba un dispositivo ASM con un estudiante.
3. En la página **Administrar > Dispositivos**, compruebe que ambos dispositivos ASM estén inscritos solo en MDM.

   Puede filtrar la página **Dispositivos** por el estado del dispositivo ASM: **ASM registrado**, **ASM compartido**, **Instructor** y **Estudiante**.



4. Para verificar que los recursos de MDM se implementaron correctamente para cada dispositivo: seleccione el dispositivo, haga clic en **Editar** y compruebe las distintas páginas.



Distribuir dispositivos

Apple recomienda que organice un evento para poder distribuir los dispositivos a instructores y estudiantes.

Si no distribuye dispositivos preinscritos, también debe proporcionar lo siguiente a estos usuarios:

- Contraseñas de Citrix Endpoint Management para la inscripción
- Contraseñas temporales de ASM para ID de Apple gestionados.

La experiencia del usuario por primera vez es la siguiente.

1. La primera vez que un usuario inicia su dispositivo después de un restablecimiento completo, Citrix Endpoint Management le solicita en la pantalla de inscripción que inscriba su dispositivo.
2. El usuario proporciona su ID de Apple gestionado y la contraseña de Citrix Endpoint Management utilizada para autenticarse en Citrix Endpoint Management.
3. En el paso de configuración del ID de Apple, el dispositivo solicita al usuario que proporcione su ID de Apple gestionado y la contraseña temporal de ASM. Esos elementos autentican al usuario en los servicios de Apple.
4. El dispositivo solicita al usuario que cree una contraseña para su ID de Apple gestionado, que se utiliza para proteger sus datos en iCloud.
5. Al final del Asistente de configuración, Citrix Endpoint Management comienza a instalar las directivas, aplicaciones y medios en el dispositivo. Para las aplicaciones y los iBooks asignados a nivel de usuario, el asistente solicita a los instructores y estudiantes que se registren en Compras por volumen. Después de aceptar la invitación, los usuarios reciben sus aplicaciones y iBooks de Compras por volumen en la siguiente implementación (en un plazo de seis horas).

Administrar datos de instructores, estudiantes y clases

Al administrar datos de instructores, estudiantes y clases, tenga en cuenta lo siguiente:

- No cambie los ID de Apple gestionados después de importar la información de ASM a Citrix Endpoint Management. Citrix Endpoint Management también utiliza los identificadores de usuario de ASM para identificar a los usuarios.
- Si agrega o cambia datos de clase en ASM después de crear una o varias directivas de dispositivo de Configuración educativa: Edite las directivas y, a continuación, vuelva a implementarlas.

- Si el instructor de una clase cambia después de implementar la directiva de dispositivo de Configuración educativa: Revise la directiva para asegurarse de que se actualiza en la consola de Citrix Endpoint Management y, a continuación, vuelva a implementarla.
- Si actualiza las propiedades de usuario en el portal de ASM, Citrix Endpoint Management también actualiza esas propiedades en la consola. Sin embargo, Citrix Endpoint Management no recibe la propiedad de título de persona de ASM (Instructor, Estudiante u Otro) de la misma manera que recibe otras propiedades. Por lo tanto, si cambia el título de persona de ASM en ASM, complete los siguientes pasos para reflejar ese cambio en Citrix Endpoint Management.

Para administrar los datos:

1. En el portal de ASM, actualice la calificación del estudiante y borre la calificación del instructor.
2. Si cambió una cuenta de estudiante a una cuenta de instructor, elimine al usuario de la lista de estudiantes de la clase. Luego, agregue al usuario a la lista de instructores en la misma clase o en otra.

   Si cambió una cuenta de instructor a una cuenta de estudiante, elimine al usuario de la clase. Luego, agregue al usuario a la lista de estudiantes en la misma clase o en otra. Sus actualizaciones aparecen en la consola de Citrix Endpoint Management durante la siguiente sincronización (cada cinco minutos de forma predeterminada) o recuperación (cada 24 horas de forma predeterminada).
3. Edite la directiva de dispositivo de Configuración educativa para aplicar el cambio y vuelva a implementarla.

   - Si elimina un usuario del portal de ASM, Citrix Endpoint Management también elimina a ese usuario de la consola de Citrix Endpoint Management después de una recuperación.

     Puede reducir el intervalo entre las dos líneas base cambiando este valor de propiedad del servidor: **bulk.enrollment.fetchRosterInfoDelay** (el valor predeterminado es **1440** minutos).
   - Después de implementar los recursos: Si un alumno se une a una clase, cree un grupo de entrega solo con ese alumno e implemente los recursos para él.
   - Si un alumno o instructor pierde su contraseña temporal, pídale que se ponga en contacto con el administrador de ASM. El administrador puede proporcionar la contraseña temporal o generar una nueva.

Administrar un dispositivo perdido o robado

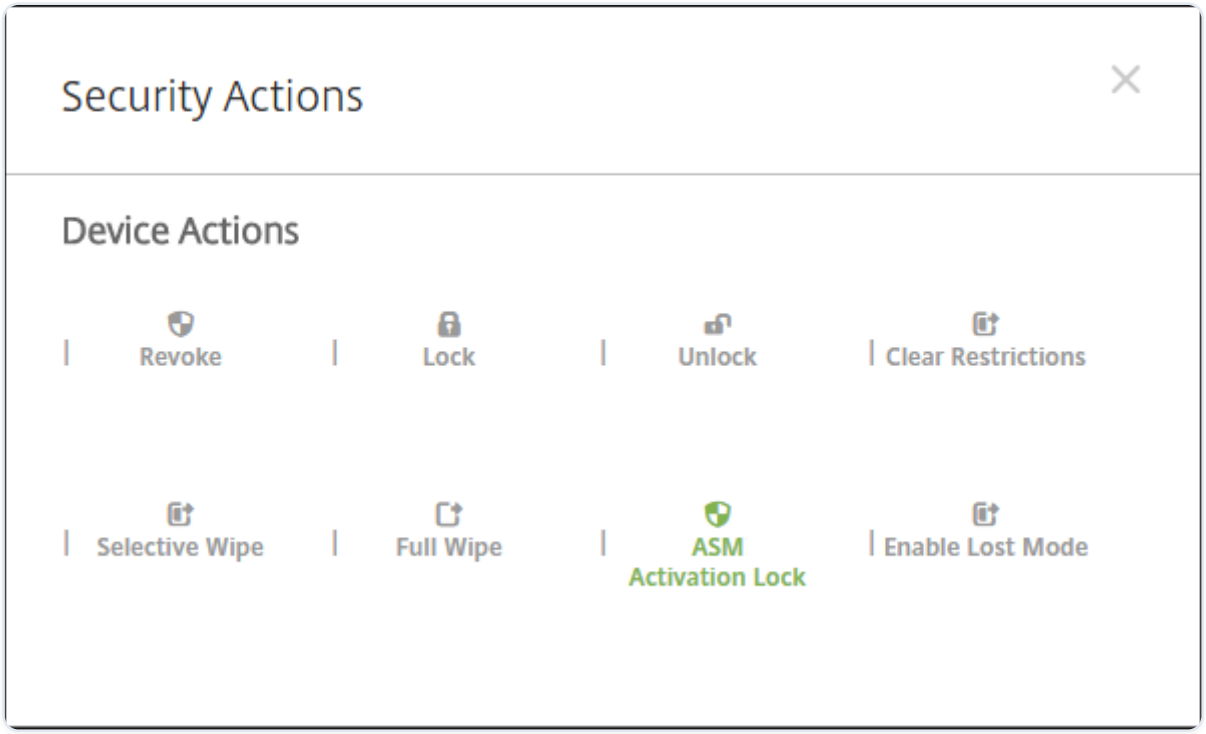
El servicio Buscar mi iPhone/iPad de Apple incluye una función de Bloqueo de activación. El Bloqueo de activación impide que usuarios no autorizados utilicen o revendan un dispositivo perdido o robado que esté inscrito en el Programa de implementación de Apple.

Citrix Endpoint Management incluye una acción de seguridad de **Bloqueo de activación de ASM** que le permite enviar un código de bloqueo a un dispositivo inscrito en el Programa de implementación de Apple de ASM.

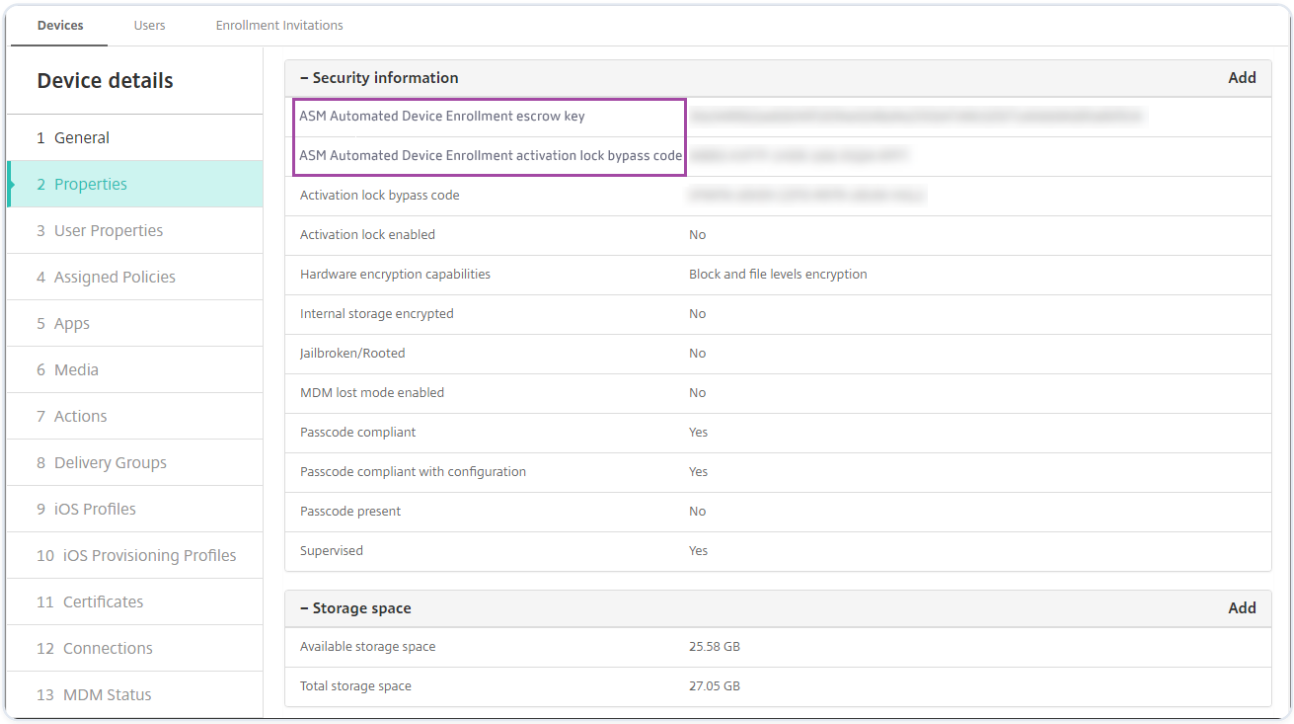
Cuando utiliza la acción de seguridad **Bloqueo de activación de ASM**, Citrix Endpoint Management puede localizar dispositivos sin necesidad de que los usuarios activen el servicio Buscar mi iPhone/iPad. Cuando un dispositivo ASM se restablece por completo o se borra por completo, el usuario proporciona su ID de Apple gestionado y su contraseña para desbloquear el dispositivo.

Para liberar el bloqueo desde la consola, haga clic en la acción de seguridad **Omitir bloqueo de activación**. Para obtener información sobre cómo omitir un bloqueo de activación, consulte Omitir un bloqueo de activación de iOS. El usuario también puede dejar el inicio de sesión en blanco y escribir el **código de omisión de bloqueo de activación de ASM** como contraseña. Esa información está disponible en **Detalles del dispositivo**, en la ficha **Propiedades**.

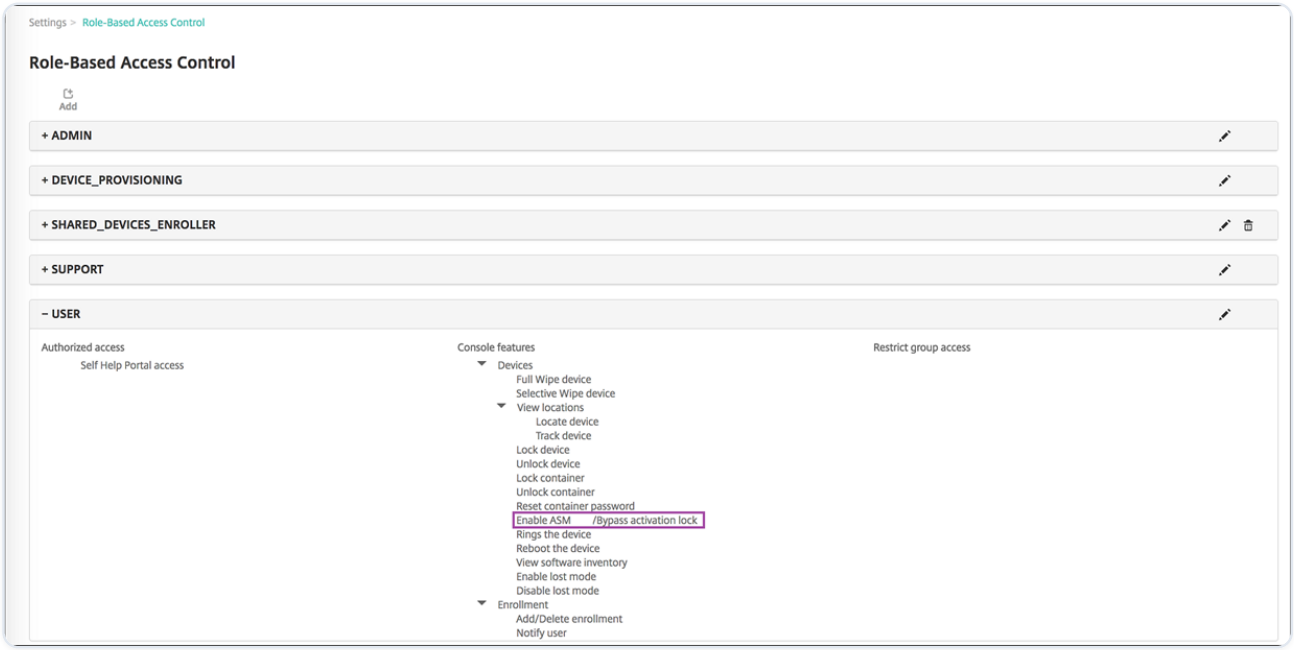
Para establecer el bloqueo de activación, vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Seguridad** y, a continuación, haga clic en **Bloqueo de activación de ASM**.



Las propiedades **Clave de depósito de ASM** y **Código de omisión de bloqueo de activación de ASM** aparecen en **Detalles del dispositivo**.



El permiso RBAC para un Bloqueo de activación de ASM es **Dispositivos > Habilitar bloqueo de activación de omisión de ASM**.



iPad compartidos

La función de iPad compartidos permite que varios usuarios utilicen un iPad. La experiencia del usuario se puede personalizar aunque los dispositivos sean compartidos. Puede utilizar iPad

compartidos para fines educativos o empresariales. Apple School Manager (ASM) admite los roles de instructor y estudiante, además de los roles que admite Apple Business Manager (ABM).

Requisitos previos para iPad compartidos

- Apple School Manager o Apple Business Manager
- Citrix Endpoint Management
- Cualquier iPad Pro, iPad de quinta generación, iPad Air 2 o posterior, y iPad mini 4 o posterior
- Al menos 32 GB de almacenamiento
- Dispositivos supervisados

Configurar iPad compartidos

Varios estudiantes o empleados pueden compartir un iPad para diferentes propósitos.

Usted o los propietarios de los dispositivos inscriben los iPad compartidos y, a continuación, implementan directivas de dispositivo, aplicaciones y contenido multimedia en los dispositivos. Después de eso, los usuarios proporcionan sus credenciales de Apple ID gestionado para iniciar sesión en un iPad compartido. Si anteriormente implementó una directiva de configuración educativa para los estudiantes, ya no inician sesión como "Otro usuario" para compartir dispositivos.

Citrix Endpoint Management utiliza dos canales de comunicación para los iPad compartidos: el canal del sistema para el propietario del dispositivo (instructor o supervisor) y el canal de usuario para el usuario residente actual (estudiante o empleado). Citrix Endpoint Management utiliza esos canales para enviar los comandos MDM adecuados para los recursos compatibles con Apple.

Los recursos que se implementan a través del canal del sistema son:

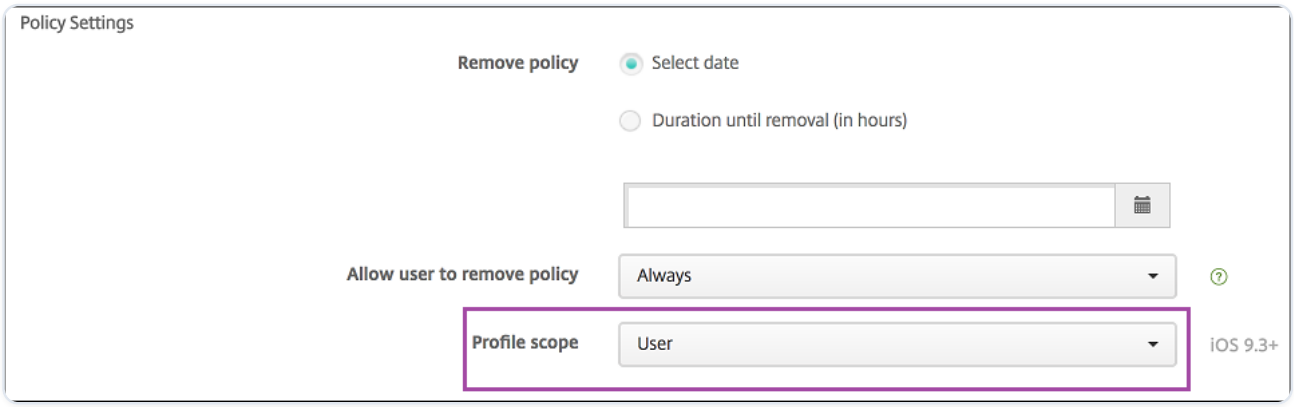
- Directivas de dispositivo, como Configuración educativa, Mensaje de pantalla de bloqueo, Número máximo de usuarios residentes y Período de gracia de bloqueo por código
- Aplicaciones de compra por volumen basadas en dispositivos Apple no admite aplicaciones empresariales ni aplicaciones de compra por volumen basadas en el usuario en iPad compartidos. Las aplicaciones instaladas en un iPad compartido son globales para el dispositivo y no por usuario.
- iBooks de compra por volumen basados en el usuario Apple admite la asignación de iBooks de compra por volumen basados en el usuario en iPads compartidos.

Los recursos que se implementan a través del canal de usuario son:

- Directivas de dispositivo: Notificaciones de aplicaciones, Diseño de pantalla de inicio, Restricciones y Webclip.

  Citrix Endpoint Management solo admite estas directivas de dispositivo a través del canal de usuario.

Al configurar las directivas de dispositivo, se especifica el canal de implementación en la configuración de directiva **Ámbito del perfil**.



Para quitar las directivas de dispositivo que implementó a través del canal de usuario, asegúrese de elegir un **Ámbito de implementación** de **Usuario** para la directiva de eliminación de perfiles.

Flujo de trabajo general

Normalmente, se proporcionan iPads compartidos preconfigurados y supervisados a los propietarios de los dispositivos. Esas personas distribuyen los dispositivos a estudiantes o empleados. Si no distribuye iPads compartidos preinscritos: Asegúrese de proporcionar a los propietarios de los dispositivos sus contraseñas del servidor de Citrix Endpoint Management para que puedan inscribir sus dispositivos.

El flujo de trabajo general para configurar e inscribir iPads compartidos es el siguiente.

1. Utilice la consola del servidor de Citrix Endpoint Management para agregar cuentas de ASM o ABM (**Parámetros > Programa de implementación de Apple**) con el **Modo compartido** habilitado. Para obtener más información, consulte a continuación «Administrar cuentas para iPads compartidos».
2. Como se describe en esta sección, agregue las directivas de dispositivo, las aplicaciones y los medios necesarios a Citrix Endpoint Management. Asigne esos recursos a grupos de entrega.
3. Pida a los propietarios de los dispositivos que realicen un restablecimiento completo en los iPads compartidos. Aparece la pantalla de administración remota para la inscripción.
4. Los propietarios de los dispositivos inscriben los iPads compartidos. Citrix Endpoint Management implementa los recursos configurados en cada iPad compartido inscrito.

Después de un reinicio automático, los propietarios de los dispositivos pueden compartir los dispositivos con los usuarios. Aparece una página de inicio de sesión en el iPad.

5. Un usuario del dispositivo introduce su ID de Apple gestionado y su contraseña temporal de ASM. El iPad compartido se autentica en ASM y solicita al usuario que cree una contraseña de ASM. Para el siguiente inicio de sesión en el iPad compartido, el usuario del dispositivo proporciona la nueva contraseña de ASM.
6. Otro usuario del dispositivo que comparte el iPad puede iniciar sesión repitiendo el paso anterior.

Administrar cuentas para iPads compartidos

Si ya utiliza Citrix Endpoint Management con Apple Education o Apple Business: Tiene una cuenta ASM/ABM existente configurada en Citrix Endpoint Management para dispositivos que no son compartidos, como los dispositivos utilizados por los propietarios de los dispositivos. Puede utilizar la misma cuenta ASM/ABM y el mismo servidor de Citrix Endpoint Management tanto para dispositivos compartidos como no compartidos.

Organizar iPads compartidos en grupos de dispositivos

ASM/ABM le permite organizar dispositivos en grupos creando varios servidores MDM. Cuando asigne los iPads compartidos a un servidor MDM, cree un grupo de dispositivos para cada grupo de iPads compartidos:

- Grupo 1 de iPads compartidos > Servidor MDM del Grupo de dispositivos 1
- Grupo 2 de iPads compartidos > Servidor MDM del Grupo de dispositivos 2
- Grupo N de iPads compartidos > Servidor MDM del Grupo de dispositivos N

Añadir cuentas ASM para cada grupo de dispositivos

Cuando crea varias cuentas ASM/ABM desde la consola del servidor de Citrix Endpoint Management, importa automáticamente grupos de iPads compartidos:

- Servidor MDM del Grupo de dispositivos 1 > Cuenta del Grupo de dispositivos 1
- Servidor MDM del Grupo de dispositivos 2 > Cuenta del Grupo de dispositivos 2
- Servidor MDM del Grupo de dispositivos N > Cuenta del Grupo de dispositivos N

Los requisitos específicos para los iPads compartidos son los siguientes:

- Una cuenta ASM/ABM para cada grupo de dispositivos con estas configuraciones habilitadas:
    - **Requerir inscripción de dispositivos**

- **Modo supervisado**
- **Modo compartido**

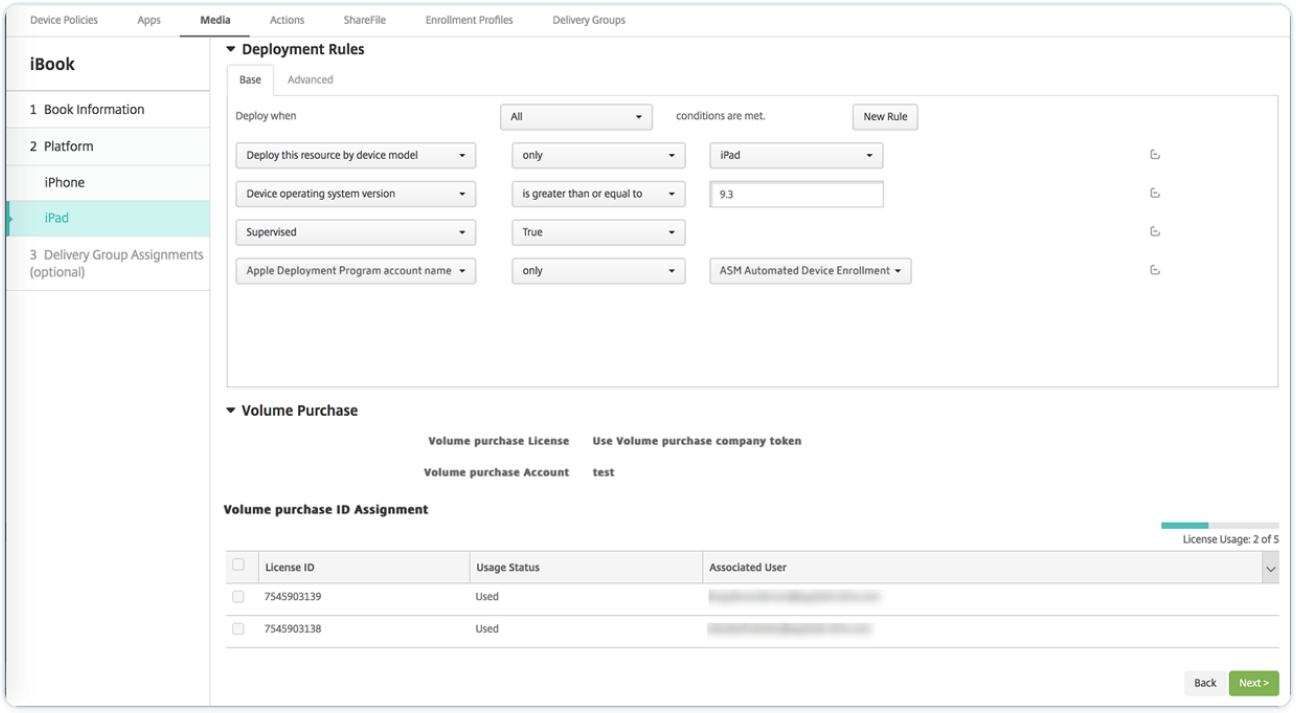
- Para una organización educativa determinada, asegúrese de usar el mismo **Sufijo educativo** para todas las cuentas de ASM.

Aplicaciones para iPads compartidos

Los iPads compartidos admiten la asignación de aplicaciones de compra por volumen basadas en dispositivos. Antes de implementar una aplicación en un iPad compartido, Citrix Endpoint Management envía una solicitud al servidor de Apple Volume Purchase para asignar licencias de compra por volumen a los dispositivos. Para comprobar las asignaciones de compra por volumen, vaya a **Configurar > Aplicaciones > iPad** y expanda **Compra por volumen**.

Contenido multimedia para iPads compartidos

Los iPads compartidos admiten la asignación de iBooks de compra por volumen basados en usuarios. Antes de implementar iBooks en un iPad compartido, Citrix Endpoint Management envía una solicitud al servidor de Apple Volume Purchase para asignar licencias de compra por volumen a los usuarios. Para comprobar las asignaciones de compra por volumen, vaya a **Configurar > Contenido multimedia > iPad** y expanda **Compra por volumen**.



Reglas de implementación para iPads compartidos

Para la implementación de iPads compartidos, las reglas a nivel de grupo de entrega no se aplican porque se relacionan con las propiedades del usuario. Para filtrar las directivas, aplicaciones y

contenido multimedia para cada grupo de dispositivos: Agregue una regla de implementación para los recursos basada en el nombre de la cuenta. Por ejemplo:

- Para la cuenta del Grupo de dispositivos 1, establezca esta regla de implementación:

```
Apple Deployment Program account name

Only

Device Group 1 account
```

- Para la cuenta del Grupo de dispositivos 2, establezca esta regla de implementación:

```
Apple Deployment Program account name

Only

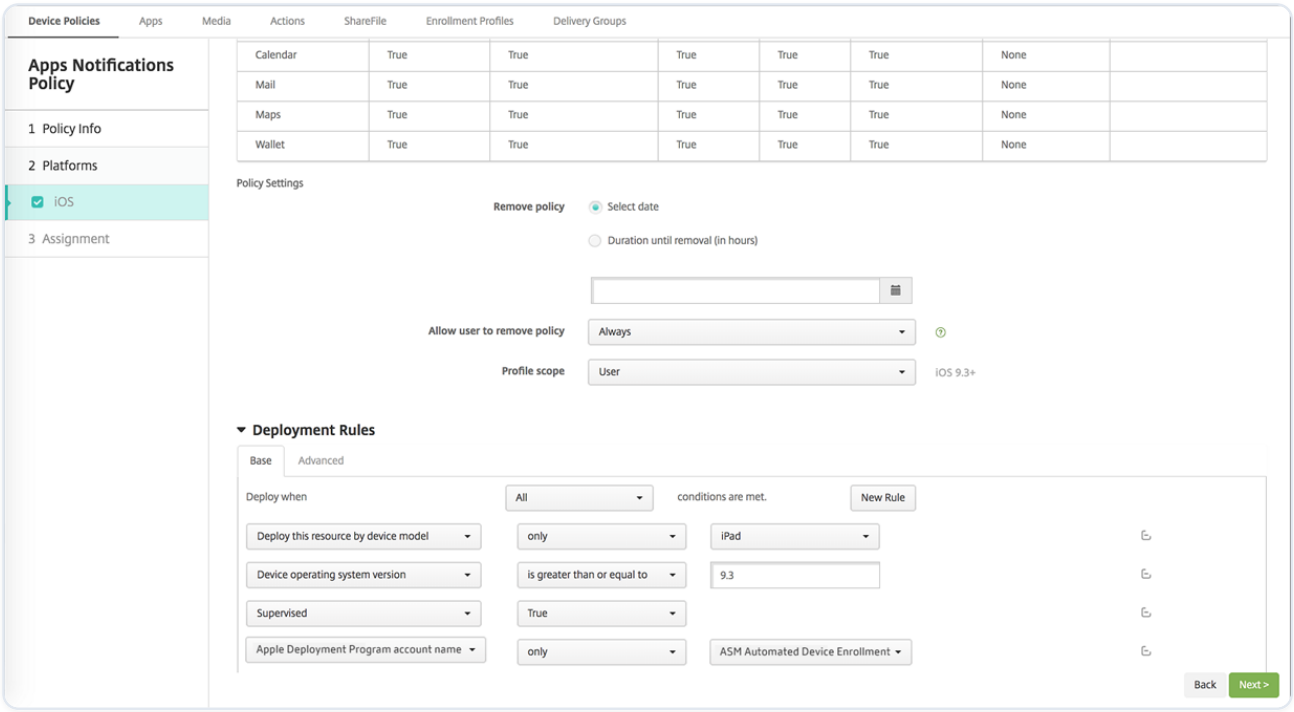
Device Group 2 account
```

- Para la cuenta del Grupo de dispositivos N, establezca esta regla de implementación:

```
Apple Deployment Program account name

Only

Device Group N account
```



Para implementar la aplicación Apple Classroom solo en los propietarios de dispositivos (que utilizan iPads no compartidos), filtre los recursos por el estado compartido de ASM con estas reglas de implementación:

```
Deploy this resource regarding ASM/ABM shared mode

only

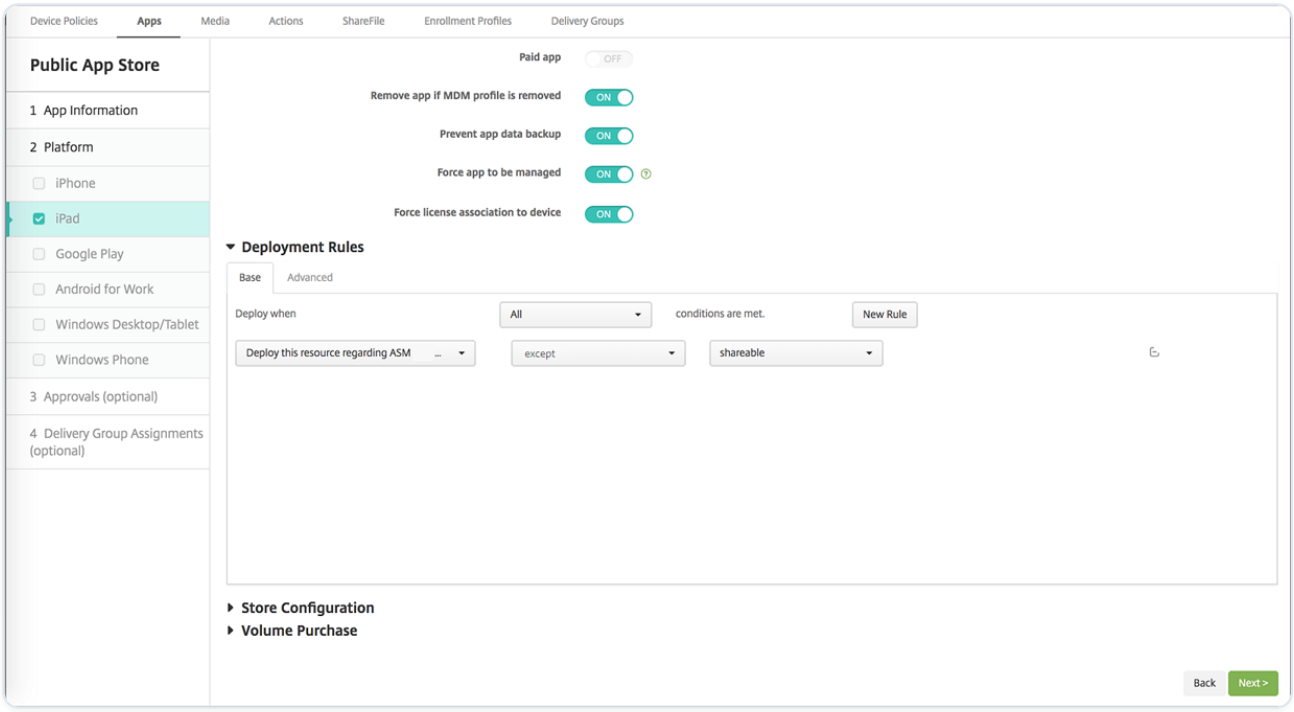
unshared
```

O bien:

```
Deploy this resource regarding ASM/ABM shared mode

except

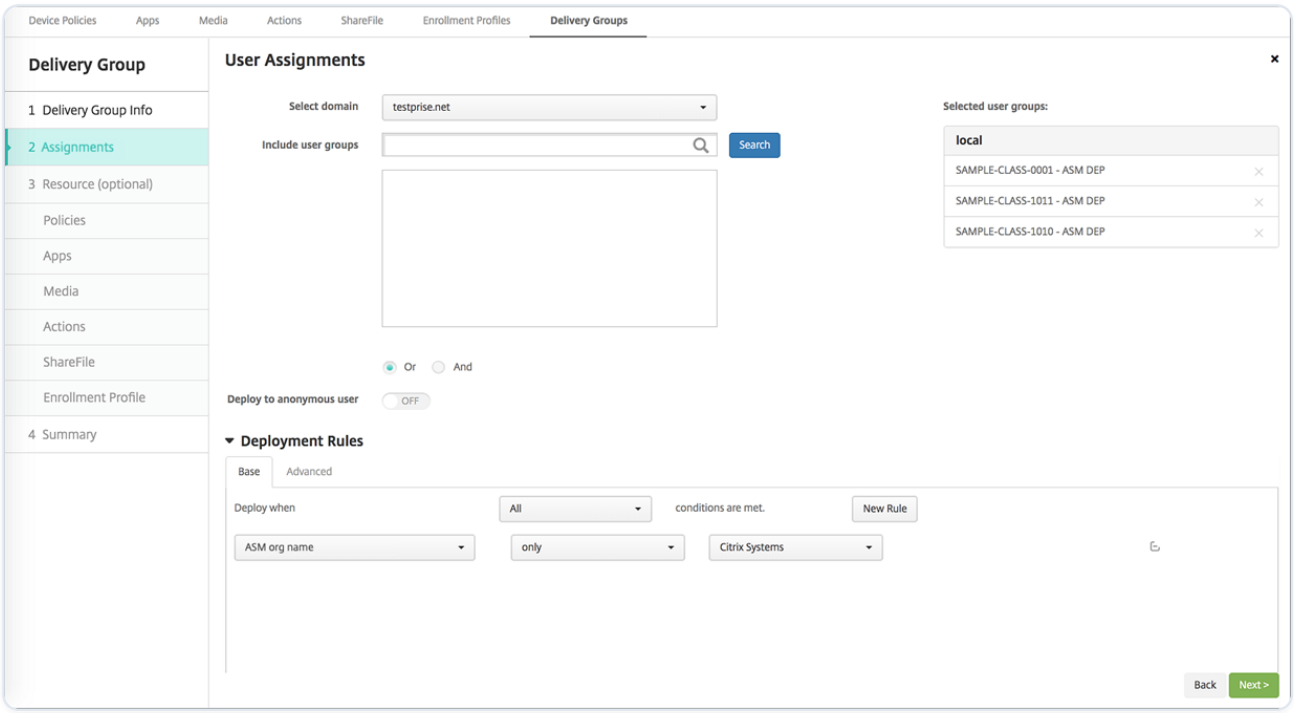
shareable
```



Grupos de entrega para iPads compartidos

Para el grupo de dispositivos:

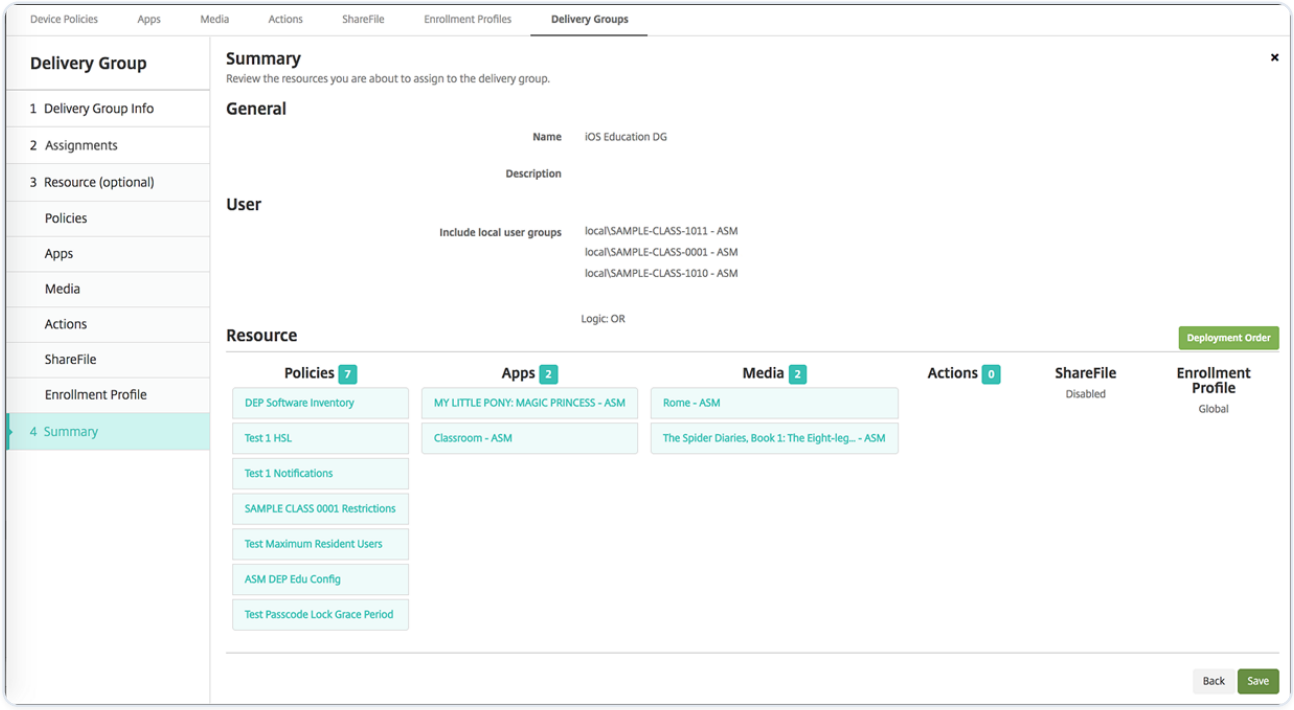
- Configure un grupo de entrega. Para los instructores, asigne todas las clases que define la directiva de Configuración de educación.



- Ese grupo de entrega debe incluir estos recursos de MDM:
  - Directivas de dispositivo:
    - Configuración de educación (para ASM)

- Mensaje de pantalla de bloqueo
- Notificaciones de aplicaciones
- Diseño de pantalla de inicio
- Restricciones
- Número máximo de usuarios residentes
- Período de gracia del bloqueo por código

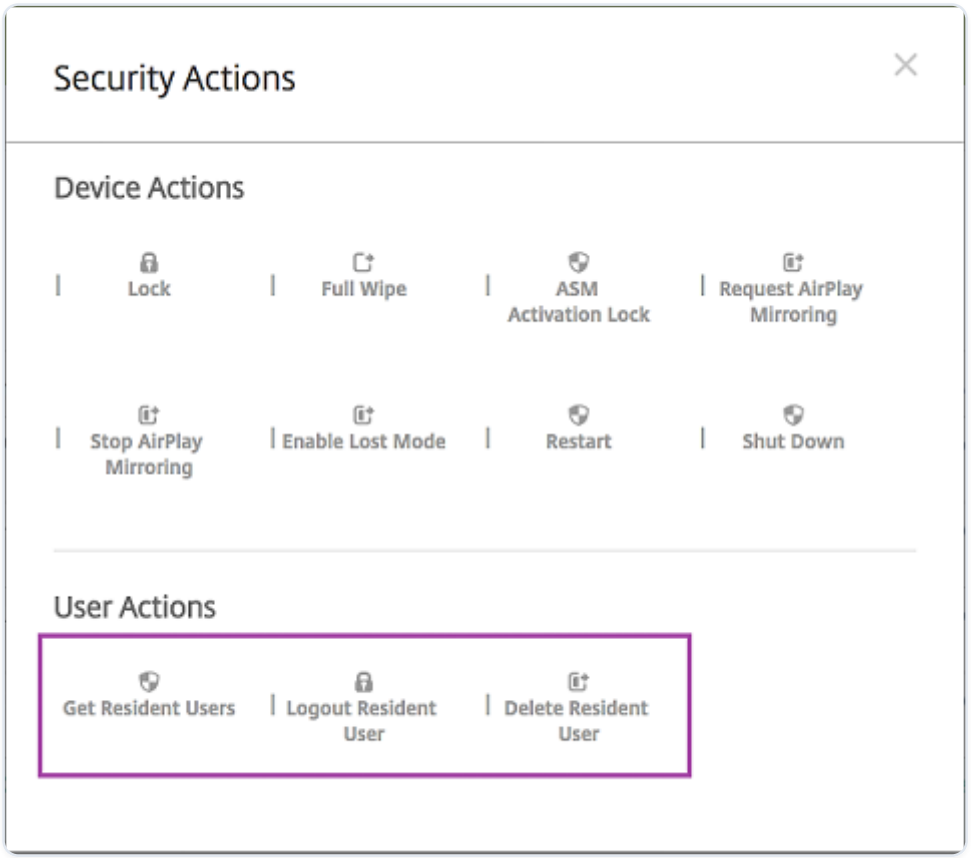
- Aplicaciones de compra por volumen obligatorias
- iBooks de compra por volumen obligatorios



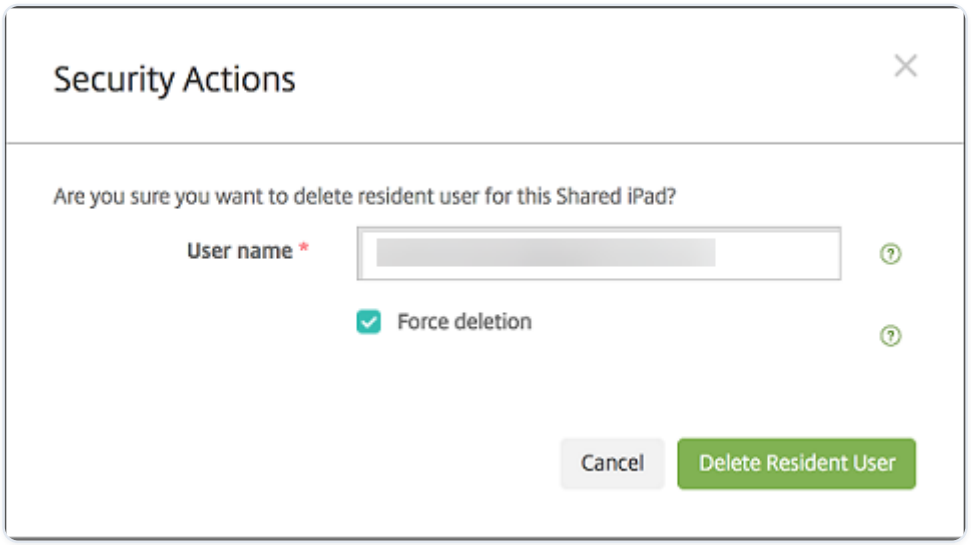
Acciones de seguridad para iPads compartidos

Además de las acciones de seguridad existentes, puede utilizar estas acciones de seguridad para iPads compartidos:

- **Obtener usuarios residentes:** Enumera los usuarios que tienen cuentas activas en el dispositivo actual. Esta acción fuerza una sincronización entre el dispositivo y la consola de Citrix Endpoint Management.
- **Cerrar sesión de usuario residente:** Fuerza el cierre de sesión del usuario actual.
- **Eliminar usuario residente:** Elimina la sesión actual de un usuario específico. El usuario puede iniciar sesión de nuevo.
- **Eliminar todos los usuarios:** Elimina todos los usuarios del dispositivo.



Después de hacer clic en **Eliminar usuario residente**, puede especificar el nombre de usuario.



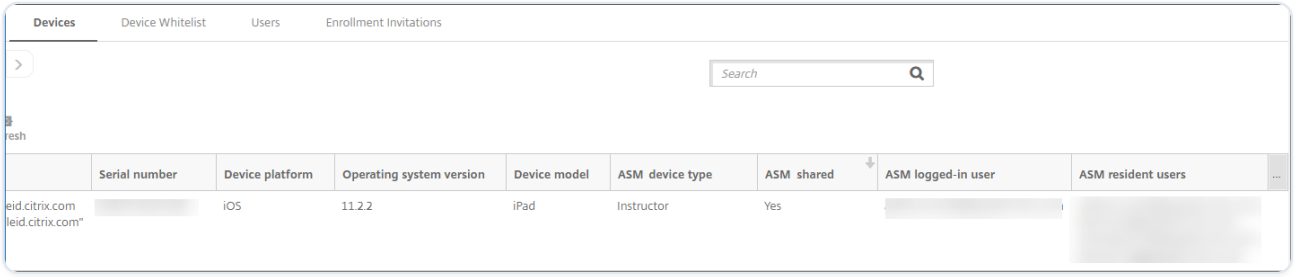
Los resultados de las acciones de seguridad aparecen en las páginas **Administrar > Dispositivos > General** y **Administrar > Dispositivos > Grupos de entrega**.

Obtener información sobre iPads compartidos

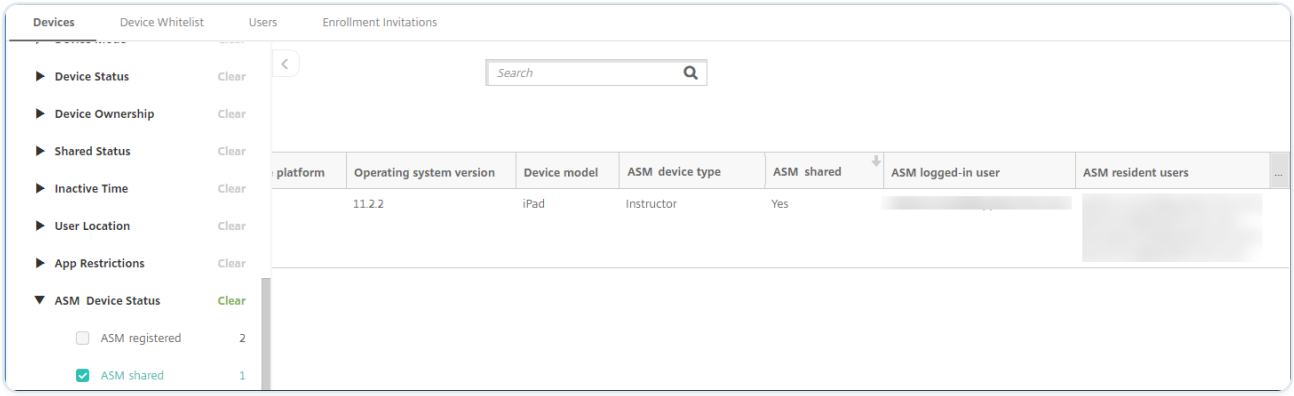
Encuentre información específica de los iPads compartidos en la página **Administrar > Dispositivos**:

- Busque:
  - Si un dispositivo es compartido (**Compartido por ASM/ABM**)

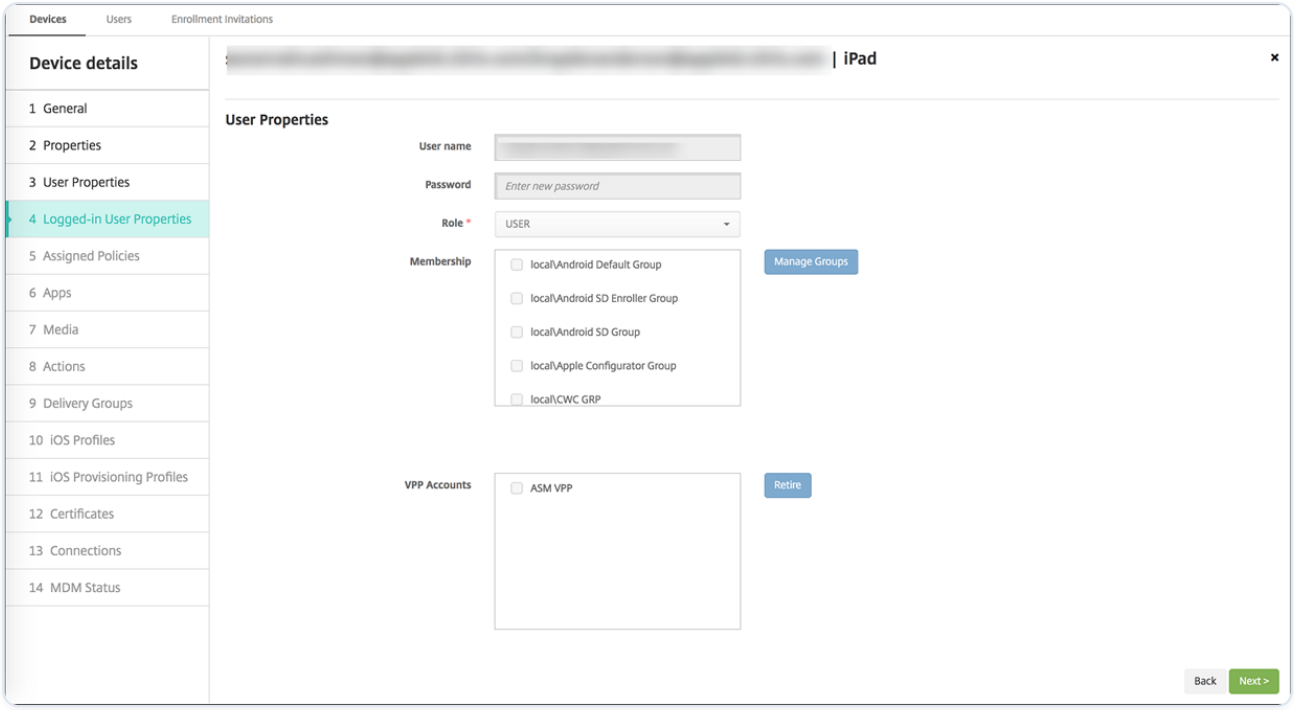
- Quién ha iniciado sesión en el dispositivo compartido (**Usuario con sesión iniciada en ASM/ABM**)
- Todos los usuarios asignados al dispositivo compartido (**Usuarios residentes de ASM/ABM**)

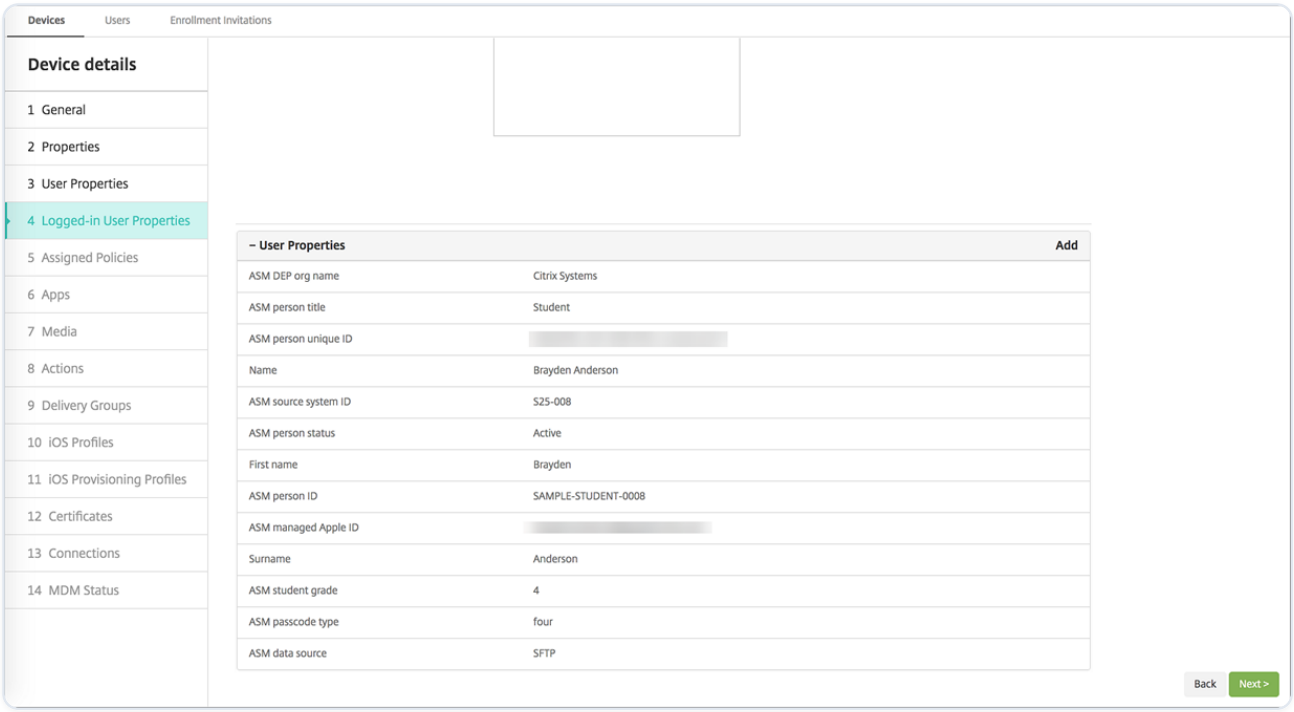


- Filtre la lista de dispositivos por su **Estado del dispositivo ASM/ABM:**

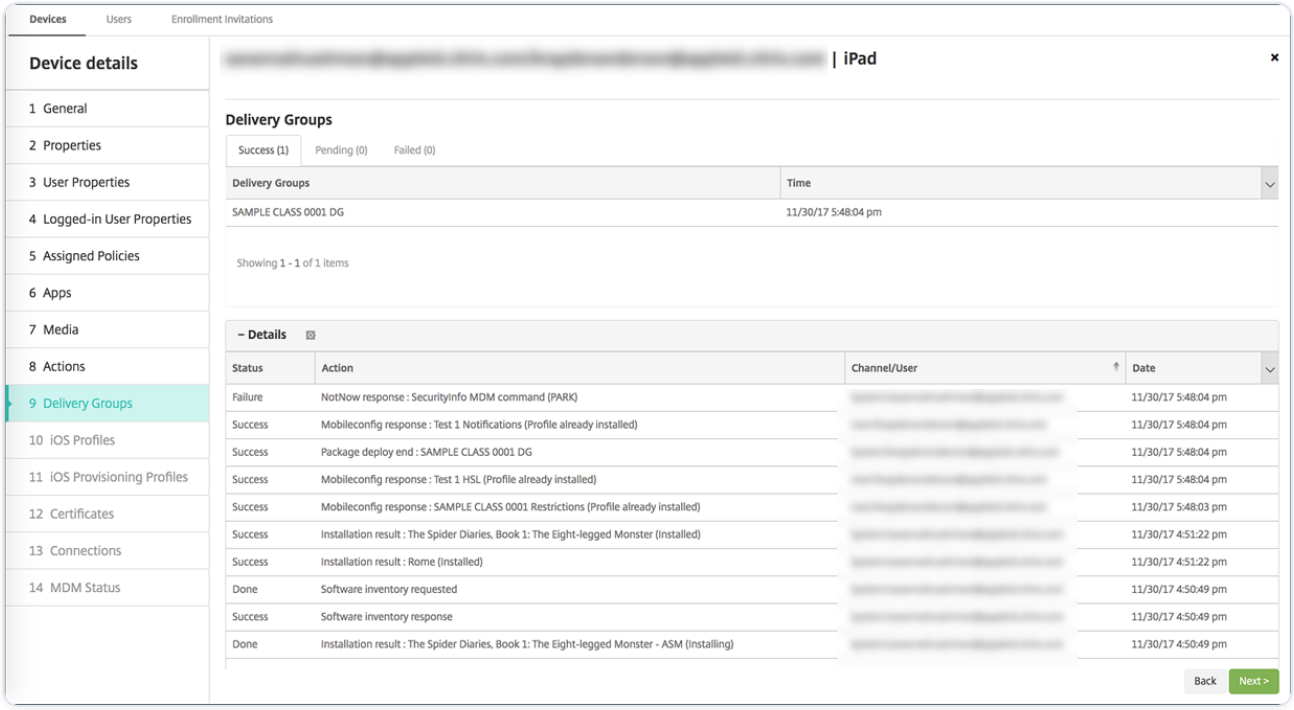


- Vea los detalles del usuario que ha iniciado sesión en un iPad compartido, en la página **Administrar > Dispositivos > Propiedades del usuario con sesión iniciada**.



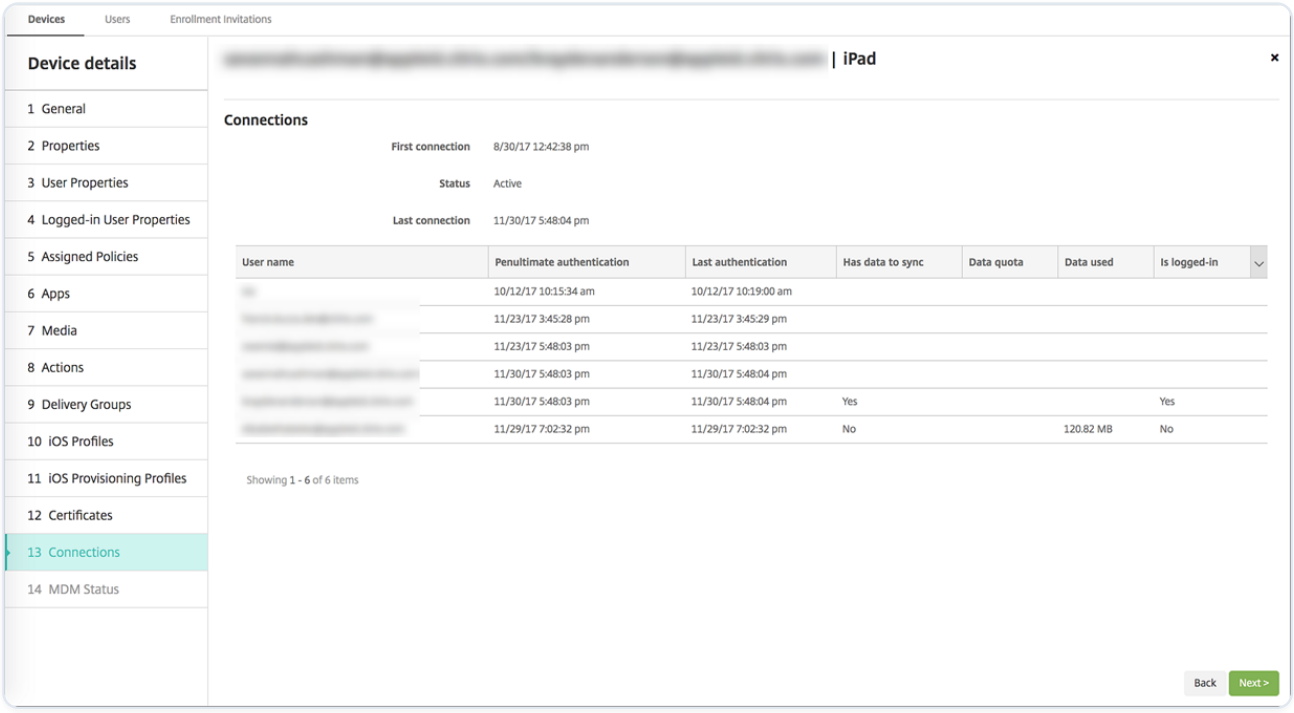


- Consulte el canal utilizado para implementar recursos en los propietarios y usuarios de dispositivos en un grupo de entrega en la página **Administrar > Dispositivos > Grupos de entrega**. La columna **Canal/Usuario** muestra el tipo (**Sistema** o **Usuario**) y el destinatario.

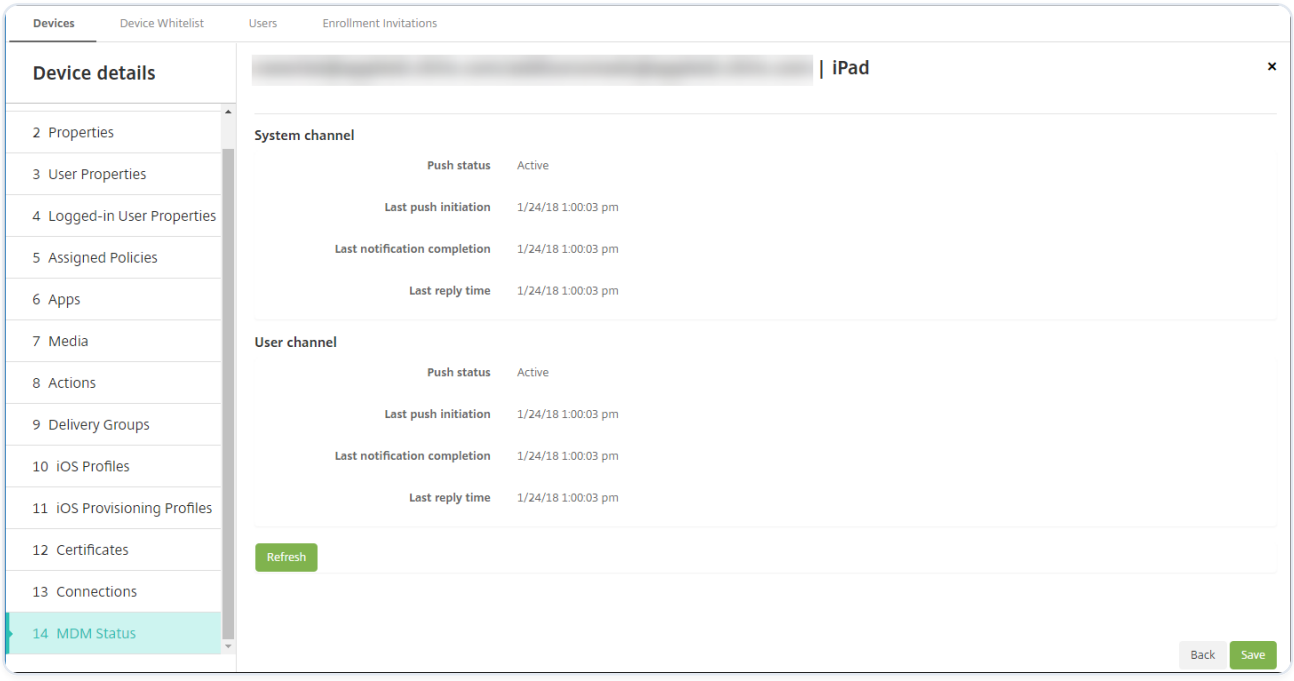


- Obtenga información sobre los usuarios residentes:
  - **Tiene datos para sincronizar:** Si el usuario tiene datos para sincronizar con la nube.
  - **Cuotas de datos:** La cuota de datos establecida para el usuario en bytes. Es posible que no aparezca una cuota si las cuotas de usuario están desactivadas temporalmente o no se aplican al usuario.

- **Datos utilizados:** La cantidad de datos utilizados por el usuario en bytes. Es posible que no aparezca un valor si se produce un error mientras el sistema recopila la información.
- **Sesión iniciada:** Si el usuario ha iniciado sesión en el dispositivo.



- Ver el estado de las notificaciones push para ambos canales.



Distribuir aplicaciones de Apple

Citrix Endpoint Management administra las aplicaciones implementadas en los dispositivos. Puede organizar e implementar los siguientes tipos de aplicaciones iOS/iPadOS y macOS.

- **Tienda de aplicaciones pública (solo iOS/iPadOS):** Estas aplicaciones incluyen aplicaciones gratuitas o de pago disponibles en una tienda de aplicaciones pública, como Apple App Store o Google Play. Por ejemplo, GoToMeeting.
- **Empresarial (iOS/iPadOS/macOS):** Aplicaciones nativas que no tienen MDX habilitado y no tienen las directivas asociadas con las aplicaciones MDX.
- **MDX (solo iOS/iPadOS):** Aplicaciones preparadas con el MAM SDK o empaquetadas con el MDX Toolkit. Estas aplicaciones incluyen directivas MDX. Puede obtener aplicaciones MDX de fuentes internas y tiendas públicas.
- **Compra por volumen (iOS/iPadOS/macOS):** Aplicaciones con licencias administradas a través del programa Apple Volume Purchase.
- **Aplicaciones personalizadas de iOS (solo iOS/iPadOS):** Aplicaciones empresariales (B2B) propietarias desarrolladas internamente o por un tercero.

Para obtener más información sobre los diferentes tipos de aplicaciones, consulte Agregar aplicaciones.

Algunas implementaciones requieren una cuenta de Apple Business Management (ABM) o Apple School Management (ASM). Consulte las siguientes secciones para obtener más información.

Para cada tipo de aplicación y método de distribución, Citrix recomienda un conjunto de prácticas de configuración. Para obtener información sobre la distribución de aplicaciones para otras plataformas, consulte Agregar aplicaciones. Las siguientes secciones proporcionan información más detallada para la configuración de aplicaciones iOS.

Pasos generales para la distribución de aplicaciones

ESCENARIO	PASO 1: VINCULAR CUENTAS	PASO 2: AGREGAR Y CONFIGURAR APLICACIONES	PASO 3: CONFIGURAR GRUPOS DE ENTREGA E IMPLEMENTAR APLICACIONES
Aplicaciones de la tienda de aplicaciones públicas(#public-app-store-apps), incluidas las	No aplicable	**En Citrix Endpoint Management: Configurar > Aplicaciones**, agregue aplicaciones de la **tienda de aplicaciones públicas** para	**En Citrix Endpoint Management:** Configure e implemente aplicaciones mediante grupos de entrega.

ESCENARIO	PASO 1: VINCULAR CUENTAS	PASO 2: AGREGAR Y CONFIGURAR APLICACIONES	PASO 3: CONFIGURAR GRUPOS DE ENTREGA E IMPLEMENTAR APLICACIONES
aplicaciones de movilidad de Citrix		iPhone o iPad. Configure las aplicaciones y asígnelas a los grupos de entrega.	
Aplicaciones de la tienda de aplicaciones públicas entregadas con Apple Volume Purchase(#public-app-store-apps-delivered-with-apple-volume-purchase), incluidas las aplicaciones de movilidad de Citrix	Inscríbase en un programa de implementación de Apple. **En Citrix Endpoint Management:** Vaya a **Parámetros > Compra por volumen** para agregar su cuenta de compra por volumen.	**En ABM o ASM:** Compre y agregue aplicaciones desde Aplicaciones y libros. **En Citrix Endpoint Management:** Vaya a **Configurar > Aplicaciones**, configure las aplicaciones y asígnelas a los grupos de entrega.	**En Citrix Endpoint Management:** Configure e implemente aplicaciones mediante grupos de entrega.
Aplicaciones empresariales(#enterprise-apps)	No aplicable	**En Citrix Endpoint Management:** Vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar** y, a continuación, en **Empresa**. Cargue el archivo IPA. Configure las aplicaciones y asígnelas a los grupos de entrega.	**En Citrix Endpoint Management:** Configure e implemente aplicaciones mediante grupos de entrega.
Aplicaciones MDX(#mdx-apps)	No aplicable	**En Citrix Endpoint Management:** Vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar** y, a	**En Citrix Endpoint Management:** Configure y despliegue

ESCENARIO	PASO 1: VINCULAR CUENTAS	PASO 2: AGREGAR Y CONFIGURAR APLICACIONES	PASO 3: CONFIGURAR GRUPOS DE ENTREGA E IMPLEMENTAR APLICACIONES
		continuación, en **MDX**. Asegúrese de seleccionar **iPad/ iPhone** para la plataforma. Cargue el archivo MDX. Configure las aplicaciones y asígnelas a los grupos de entrega.	aplicaciones usando grupos de entrega.
Aplicaciones MDX distribuidas mediante Apple Volume Purchase	Inscríbase en un programa de implementación de Apple. **En Citrix Endpoint Management:** Vaya a **Settings > Volume Purchase** para añadir su cuenta de Volume Purchase.	**En ABM:** Compre y añada aplicaciones MDX desde Apps and Books. Vincule la aplicación a su cuenta de ABM. **En Citrix Endpoint Management:** Vaya a **Configure > Apps**, configure las aplicaciones y asígnelas a grupos de entrega.	**En Citrix Endpoint Management:** Configure y despliegue aplicaciones usando grupos de entrega.
Aplicaciones personalizadas	Inscríbase en un programa de implementación de Apple. **En Citrix Endpoint Management:** Vaya a **Settings > Volume Purchase** para añadir su cuenta de Volume Purchase.	**En ABM:** Añada su aplicación a la App Store como una aplicación privada. Vincule la aplicación a su cuenta de ABM. **En Citrix Endpoint Management:** Vaya a **Configure > Apps**, configure las aplicaciones y	**En Citrix Endpoint Management:** Configure y despliegue aplicaciones usando grupos de entrega.

ESCENARIO	PASO 1: VINCULAR CUENTAS	PASO 2: AGREGAR Y CONFIGURAR APLICACIONES	PASO 3: CONFIGURAR GRUPOS DE ENTREGA E IMPLEMENTAR APLICACIONES
		asígnelas a grupos de entrega.	
Aplicaciones personalizadas habilitadas para MDX	Inscríbase en un programa de implementación de Apple. **En Citrix Endpoint Management:** Vaya a **Settings > Volume Purchase** para añadir su cuenta de Volume Purchase.	**En ABM:** Añada su aplicación a la tienda de aplicaciones como una aplicación privada. Vincule la aplicación a su cuenta de ABM. **En Citrix Endpoint Management:** Vaya a **Configure > Apps** y cargue el archivo MDX. Configure las aplicaciones y asígnelas a grupos de entrega.	**En Citrix Endpoint Management:** Configure y despliegue aplicaciones usando grupos de entrega.

Aplicaciones de la tienda de aplicaciones públicas

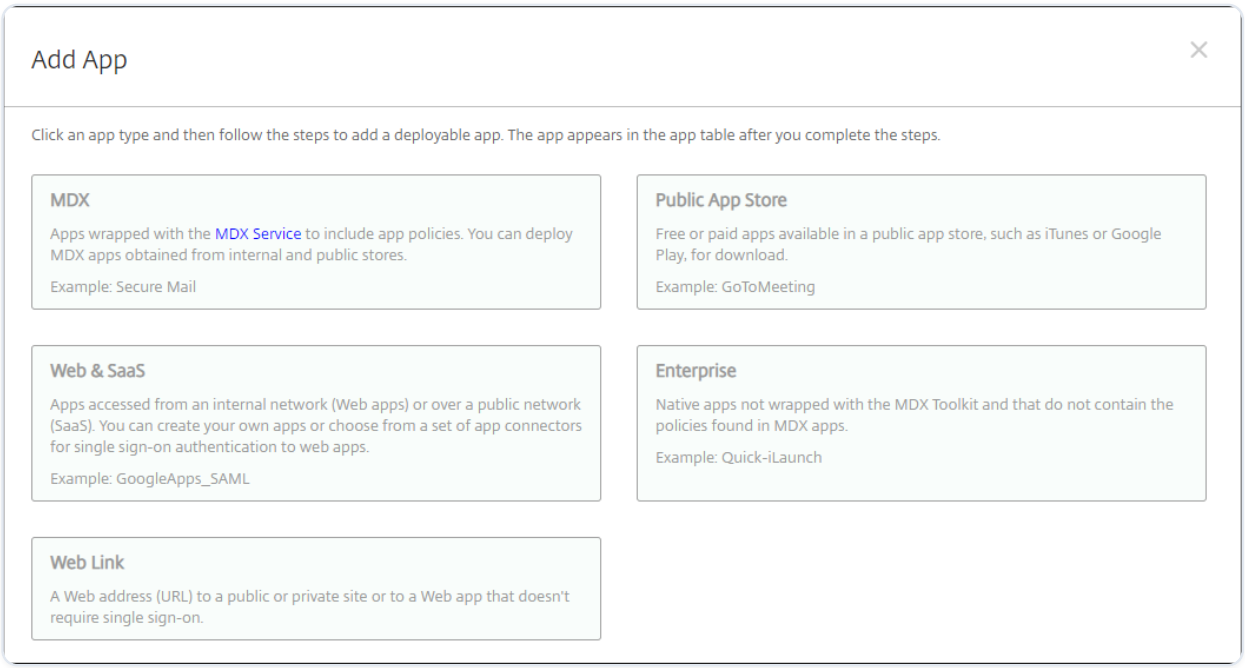
Puede añadir aplicaciones gratuitas y de pago disponibles en la App Store a Citrix Endpoint Management.

DISPONIBILIDAD DE LA FUNCIÓN	
Requiere supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	No
Disponible en	iOS/iPadOS

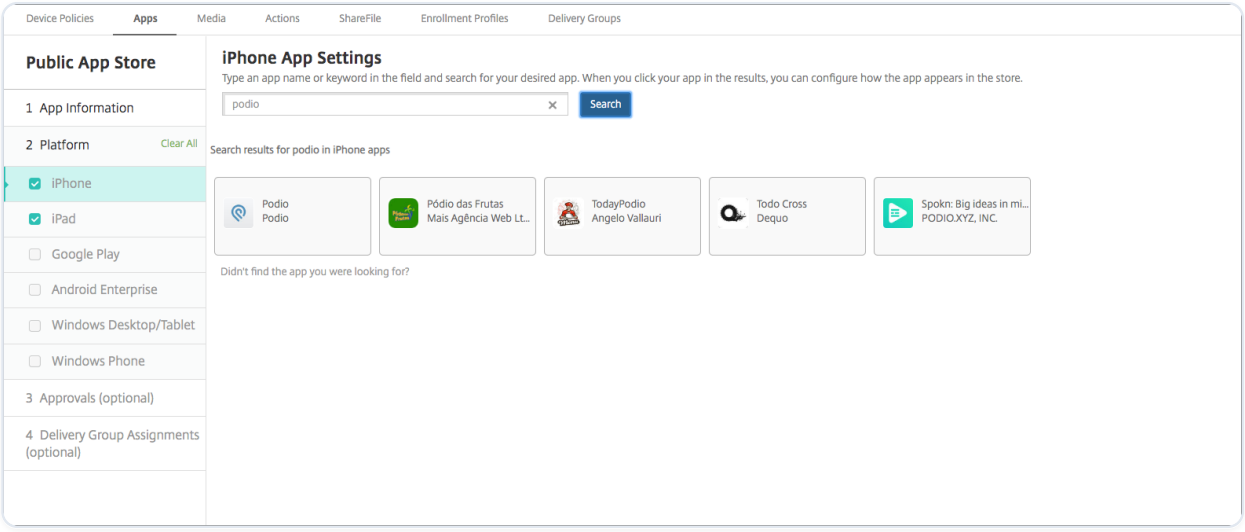
Paso 1: Agregar y configurar aplicaciones

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar**.

2. Haga clic en **Tienda de aplicaciones pública**.



3. Seleccione **iPhone** o **iPad** para las plataformas
4. Escriba el nombre de la aplicación en el cuadro de búsqueda y haga clic en **Buscar**.

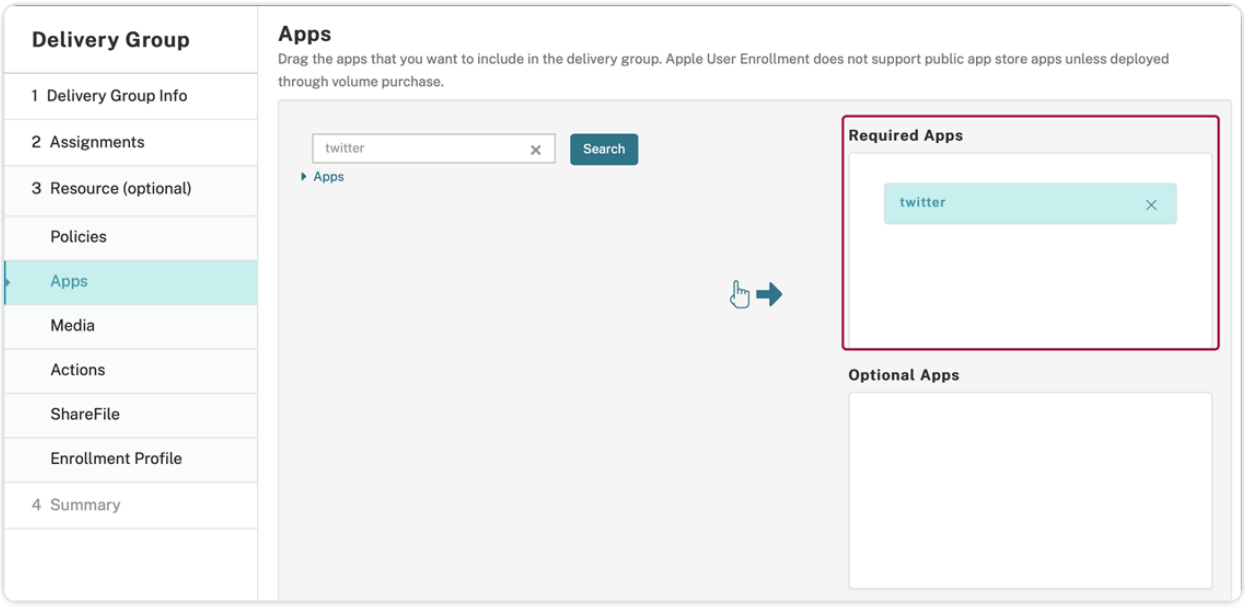


5. Aparecen las aplicaciones que coinciden con los criterios de búsqueda. Haga clic en la aplicación deseada.
6. Asigne un grupo de entrega a la aplicación y haga clic en **Guardar**.

Paso 2: Configurar la implementación de aplicaciones

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones**.
2. Seleccione la aplicación que quiere configurar y haga clic en **Modificar**.
3. Citrix® recomienda habilitar la función **Forzar la administración de la aplicación**.
4. Asigne los grupos de entrega y haga clic en **Guardar**.

5. Vaya a **Configurar > Grupos de entrega** y haga clic en **Agregar**.
6. En la sección **Aplicaciones**, arrastre las aplicaciones deseadas al cuadro **Aplicaciones requeridas**.



7. Vuelva a **Configurar > Grupos de entrega**.
8. Seleccione el grupo de entrega y haga clic en **Implementar**.
9. Los usuarios reciben una solicitud para instalar la aplicación y esta se instala en segundo plano después de que la aceptan.



Aplicaciones de la tienda de aplicaciones pública entregadas con Apple Volume Purchase

Puede administrar las licencias de aplicaciones iOS/iPadOS a través del programa Apple Volume Purchase. Siga estos pasos para agregar aplicaciones de Volume Purchase a Citrix Endpoint Management.

DISPONIBILIDAD DE FUNCIONES	
Requiere supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	Sí
Disponible en	iOS/iPadOS/macOS

Paso 1: Vincular cuentas

1. Configure e inscríbase en Apple Business Manager (ABM) o Apple School Manager (ASM). Para obtener más información sobre estos programas, consulte la documentación de Apple.
2. Vincule su cuenta de ABM/ASM con Citrix Endpoint Management. Para obtener más información sobre cómo vincular cuentas de compra por volumen, consulte Compra por volumen de Apple.
3. Cuando agregue su cuenta de compra por volumen, habilite **Actualización automática de aplicaciones**. Esta configuración garantiza que las aplicaciones en los dispositivos de los usuarios se actualicen automáticamente cuando aparezca una actualización en la tienda de Apple. Si una aplicación tiene habilitada la configuración **Forzar que la aplicación sea administrada**, se actualiza sin pedir confirmación al usuario. La actualización se produce independientemente de si la aplicación es obligatoria u opcional.

   Para usar las configuraciones **Forzar que la aplicación sea administrada** y **Actualización automática de aplicaciones**, habilite la propiedad de servidor `apple.app.force.managed`. Consulte Propiedades del servidor.

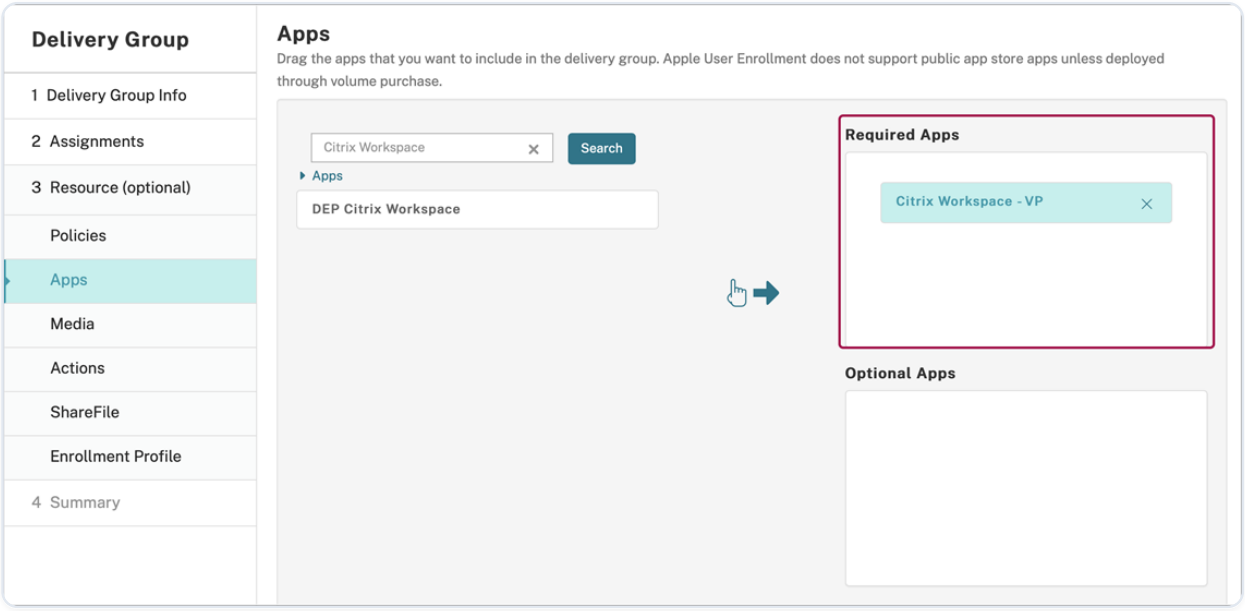
Paso 2: Obtener aplicaciones y licencias de Apple

Compre las aplicaciones en su cuenta de ABM/ASM. Puede realizar compras en Apple Books (solo para iOS/iPadOS) y en la App Store de Apple. Tenga en cuenta que debe comprar todas las aplicaciones, incluso si son gratuitas. Una vez que compre licencias en ABM/ASM, Citrix Endpoint Management mostrará la aplicación automáticamente.

Para obtener información sobre cómo poner las aplicaciones a disposición de su empresa, consulte la documentación de Apple.

Paso 3: Configurar la implementación de aplicaciones

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones**.
2. Seleccione la aplicación de compra por volumen que desea configurar y haga clic en **Modificar**.
3. Seleccione las plataformas: **iPhone**, **iPad** o **macOS**.
4. Citrix recomienda habilitar la función **Forzar la administración de la aplicación** (solo iOS/iPadOS).
5. Asigne los grupos de entrega y haga clic en **Guardar**.
6. Vaya a **Configurar > Grupos de entrega** y haga clic en **Agregar**.
7. En la sección **Aplicaciones**, arrastre las aplicaciones deseadas al cuadro **Aplicaciones requeridas**.



8. Vuelva a **Configurar > Grupos de entrega**.
9. Seleccione el grupo de entrega y haga clic en **Implementar**.

10. Los usuarios reciben una solicitud para instalar la aplicación y esta se instala en segundo plano después de que la aceptan.



Aplicaciones empresariales

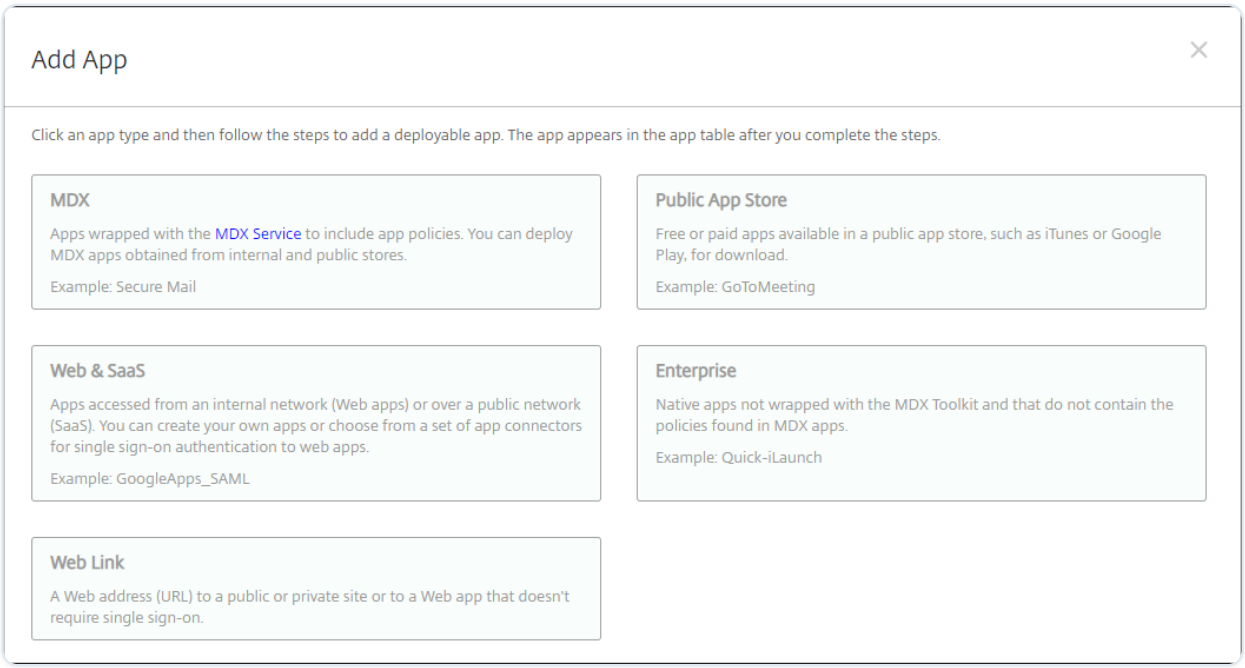
También puede agregar aplicaciones nativas que no tienen ninguna directiva MDX asociada. Siga estos pasos para agregar aplicaciones que no existen en App Store.

DISPONIBILIDAD DE FUNCIONES	
Requiere supervisión del dispositivo	No
Disponible para el modo de inscripción de usuario	Sí
Sistema operativo	iOS/iPadOS/macOS

Paso 1: Añadir y configurar aplicaciones

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar**.

2. Haga clic en **Empresa**.



3. En la página **Información de la aplicación**, configure lo siguiente:

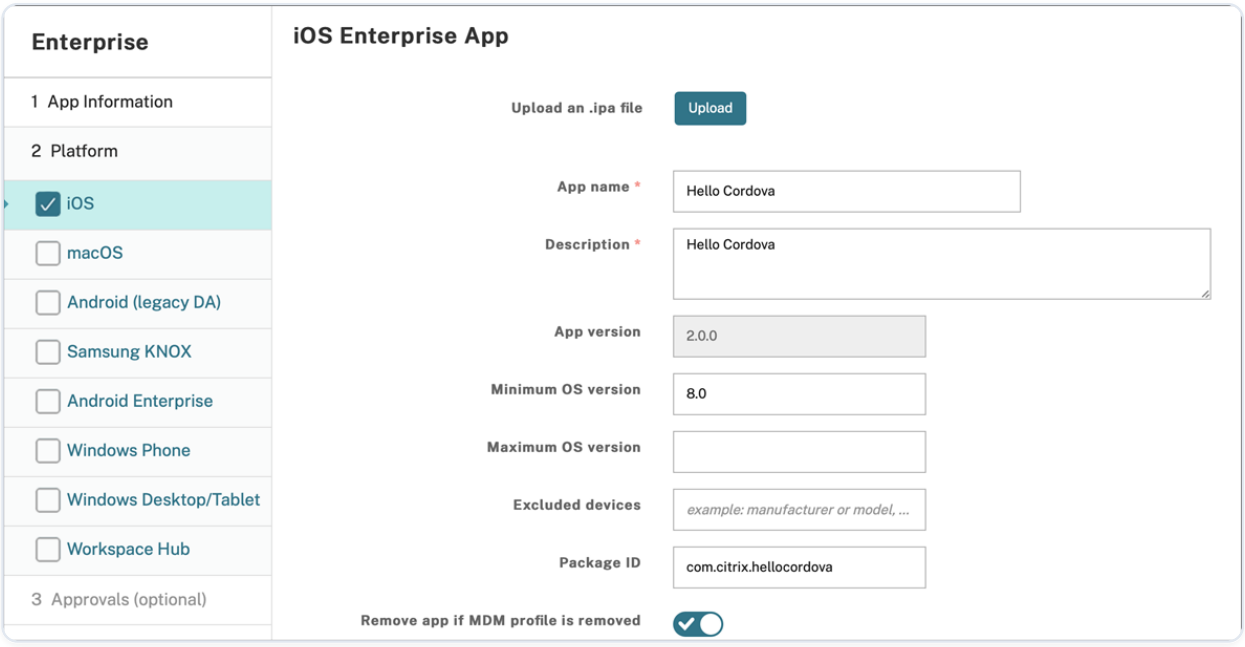
   - **Nombre:** Escriba un nombre descriptivo para la aplicación. El nombre aparece en Nombre de la aplicación en la tabla Aplicaciones.
   - **Descripción:** Escriba una descripción opcional de la aplicación.
   - **Categoría de aplicación:** Opcionalmente, en la lista, haga clic en la categoría a la que quiere añadir la aplicación.

4. Haga clic en **Siguiente**. Aparece la página **Plataformas de aplicaciones**.
5. Seleccione las plataformas: **iPhone**, **iPad** o **macOS**.
6. Cargue el archivo IPA (iOS/iPadOS) o cargue el archivo PKG (macOS)
7. Haga clic en **Siguiente**. Aparece la página **Detalles de la aplicación**.
8. Configure estos ajustes:

   - **Nombre de archivo:** Opcionalmente, escriba un nuevo nombre para la aplicación.
   - **Descripción de la aplicación:** Opcionalmente, escriba una nueva descripción para la aplicación.
   - **Versión de la aplicación:** No puede cambiar este campo.
   - **Versión mínima del SO:** Opcionalmente, escriba la versión más antigua del sistema operativo que el dispositivo puede ejecutar para usar la aplicación.
   - **Versión máxima del SO:** Opcionalmente, escriba el sistema operativo más reciente que el dispositivo debe ejecutar para usar la aplicación.

- **Dispositivos excluidos:** Opcionalmente, escriba el fabricante o los modelos de dispositivos que no pueden ejecutar la aplicación.
- **Eliminar aplicación si se elimina el perfil MDM:** Seleccione si desea eliminar la aplicación de un dispositivo cuando se elimina el perfil MDM. El valor predeterminado es Activado. (Solo iOS/iPadOS)
- **Evitar la copia de seguridad de los datos de la aplicación:** Seleccione si desea evitar que la aplicación haga una copia de seguridad de los datos. El valor predeterminado es Activado. (Solo iOS/iPadOS)
- **Forzar la administración de la aplicación:** Si instala una aplicación no administrada, seleccione **Activado** si desea que los usuarios de dispositivos no supervisados vean un mensaje para permitir la administración de la aplicación. Si aceptan el mensaje, la aplicación se administra. Si una aplicación tiene la configuración **Forzar la administración de la aplicación** habilitada, se actualiza sin pedir confirmación al usuario. La actualización se produce independientemente de si la aplicación es obligatoria u opcional. (Solo iOS/iPadOS)

Para usar las configuraciones **Forzar la administración de la aplicación** y **Actualización automática de la aplicación**, habilite la propiedad de servidor `apple.app.force.managed`. Consulte Propiedades del servidor.

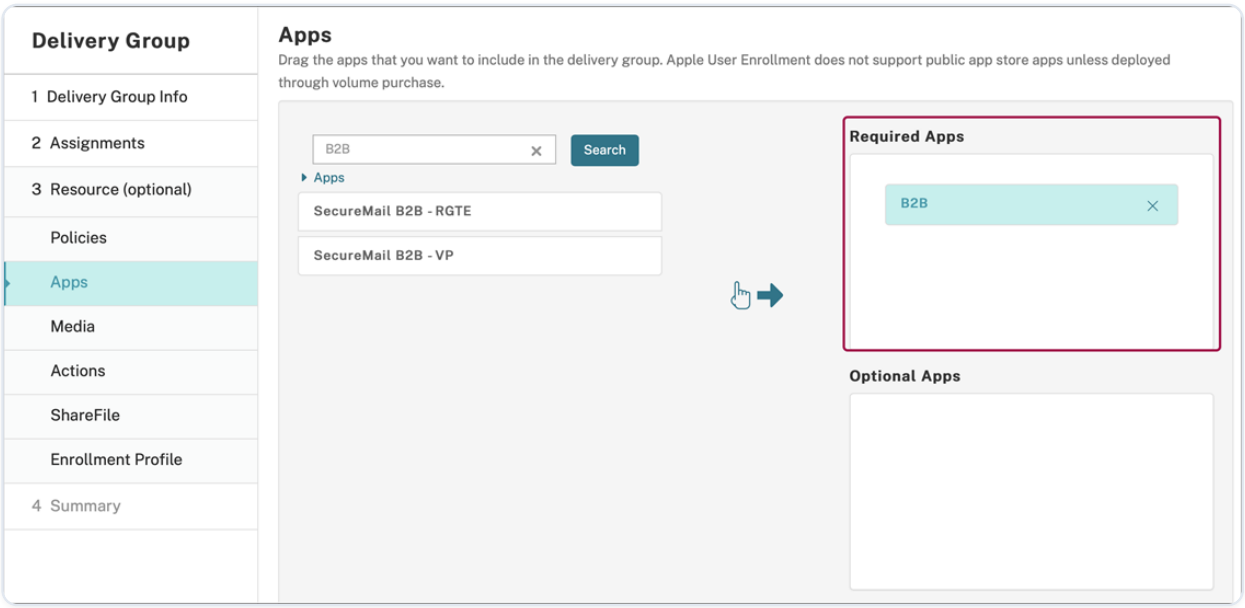


9. Asigne un grupo de entrega a la aplicación y haga clic en **Guardar**.

Paso 2: Configurar la implementación de la aplicación

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Grupos de entrega**. Seleccione el grupo de entrega que desea configurar y haga clic en la página **Aplicaciones**.

2. Arrastre las aplicaciones deseadas al cuadro **Aplicaciones obligatorias**.



3. Vaya a **Configurar > Grupos de entrega**.
4. Seleccione el grupo de entrega y haga clic en **Implementar**.
5. Los usuarios reciben una solicitud para instalar la aplicación y esta se instala en segundo plano después de que la aceptan.



Aplicaciones MDX

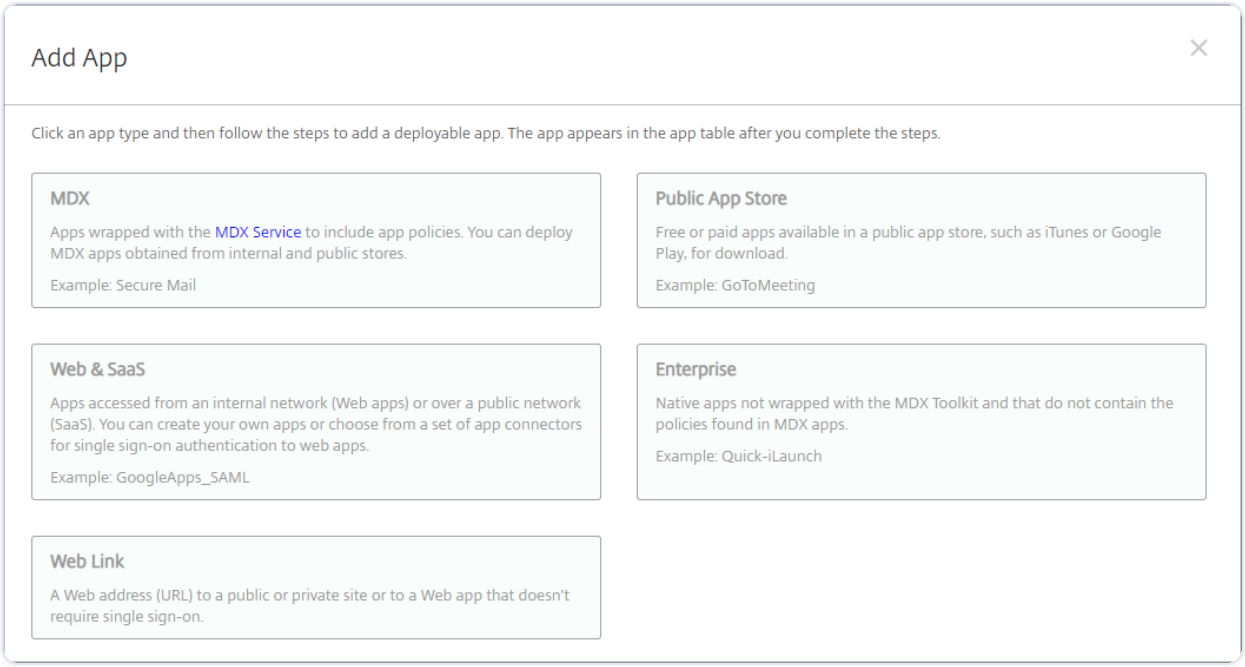
Para usar las directivas MDX y las funciones de seguridad, agregue aplicaciones habilitadas para MAM SDK o empaquetadas con MDX. Puede implementar aplicaciones MDX mediante Compra por volumen o sin ella.

DISPONIBILIDAD DE FUNCIONES	
Requiere supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	Sí
Disponible en	iOS/iPadOS

Para agregar la versión MDX de una aplicación de la tienda de aplicaciones pública, siga los pasos de Aplicaciones de la tienda de aplicaciones pública y, a continuación, siga los pasos de esta sección.

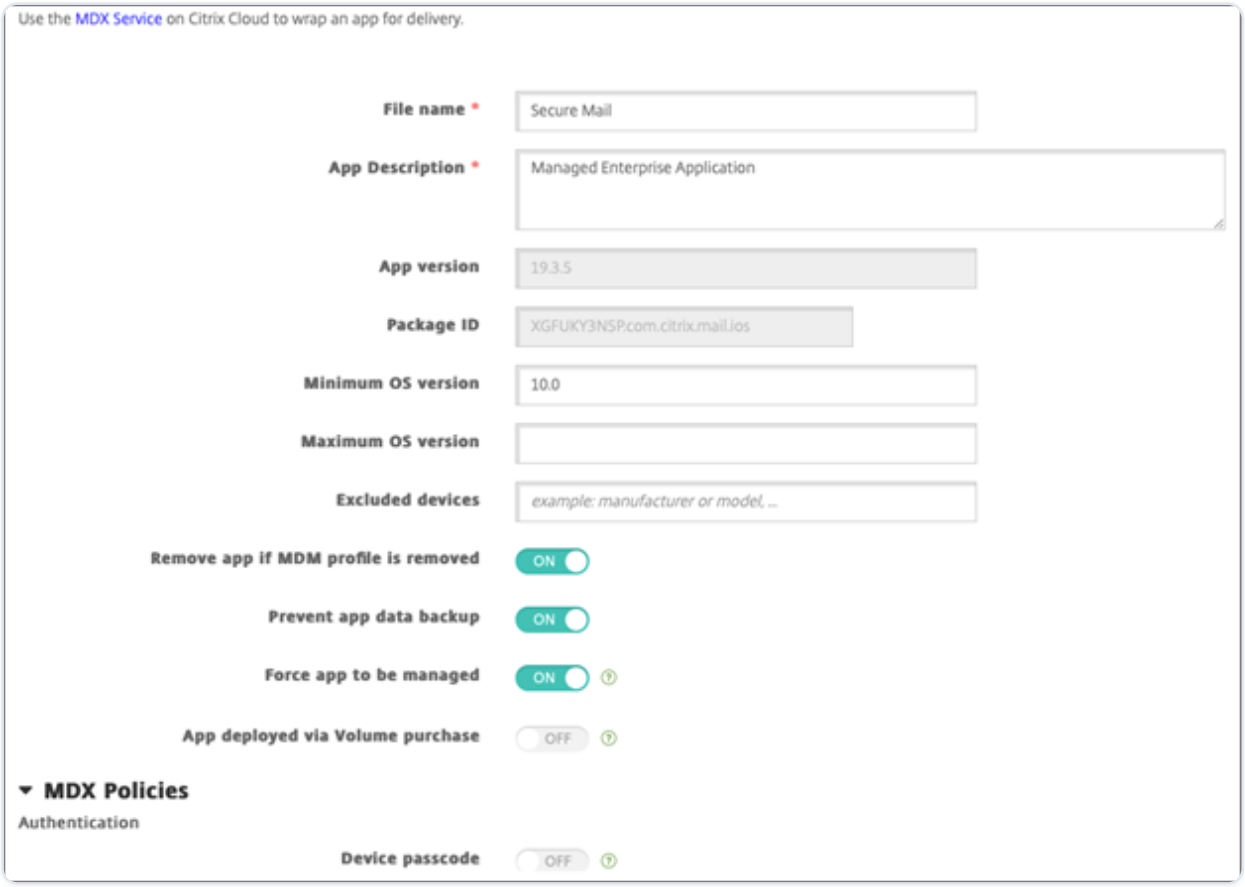
Paso 1: Agregar y configurar aplicaciones

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar**.
2. Haga clic en **MDX**.

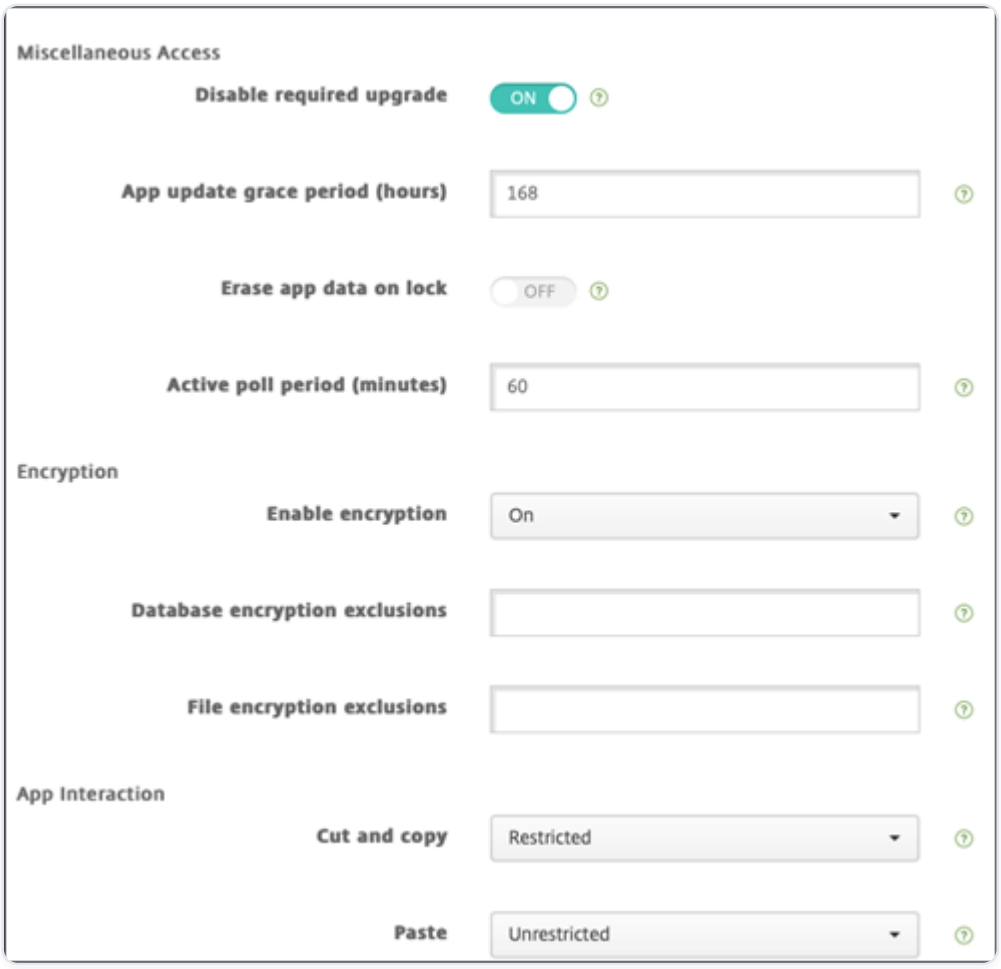


3. Seleccione **iPhone** o **iPad** para las plataformas.
4. Cargue el archivo MDX.

5. Configure los detalles de la aplicación. Establezca **Aplicación implementada a través de Volume Purchase** en **Desactivado**. Citrix también recomienda habilitar la función **Forzar la administración de la aplicación**.



6. Configure las directivas MDX. Establezca **Deshabilitar actualización obligatoria** en **Activado**.

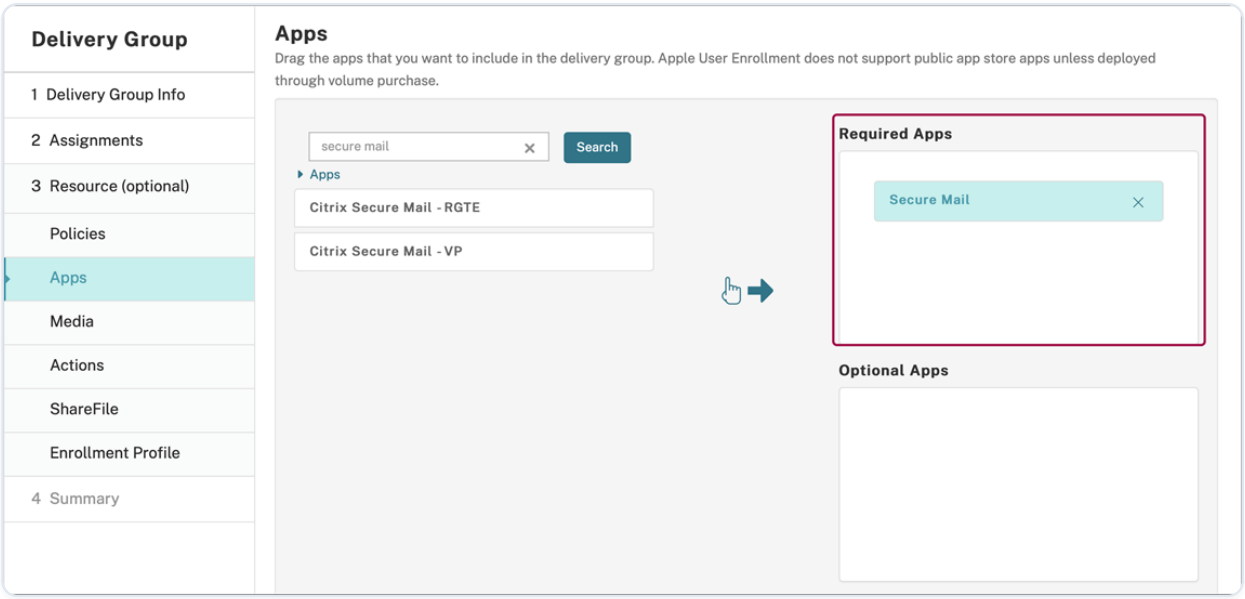


7. Asigne un grupo de entrega a la aplicación y haga clic en **Guardar**.

Paso 2: Configurar la implementación de la aplicación

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Grupos de entrega** y haga clic en **Agregar**.

2. En la sección **Aplicaciones**, arrastre las aplicaciones deseadas al cuadro **Aplicaciones requeridas**.



3. Vaya a **Configurar > Grupos de entrega**.
4. Seleccione el grupo de entrega y haga clic en **Implementar**.
5. Los usuarios reciben una solicitud para instalar la aplicación y esta se instala en segundo plano después de que la aceptan.



Aplicaciones MDX distribuidas mediante Apple Volume Purchase

Para usar las directivas MDX y las funciones de seguridad, agregue aplicaciones que tengan el SDK de MAM habilitado o que estén encapsuladas en MDX. Para implementar aplicaciones mediante Volume Purchase, las aplicaciones deben existir en la tienda de aplicaciones.

DISPONIBILIDAD DE FUNCIONES	
Requiere supervisión del dispositivo	No
Disponible para el modo de inscripción de usuario	Sí
Disponible en	iOS/iPadOS

Paso 1: Vincular cuentas

1. Configure e inscríbase en Apple Business Manager (ABM) o Apple School Manager (ASM). Para obtener más información sobre estos programas, consulte la documentación de Apple.
2. Vincule su cuenta de ABM/ASM con Citrix Endpoint Management. Para obtener más información sobre cómo vincular cuentas de compra por volumen, consulte Compra por volumen de Apple.
3. Cuando agregue su cuenta de compra por volumen, habilite **Actualización automática de aplicaciones**. Esta configuración garantiza que las aplicaciones en los dispositivos de los usuarios se actualicen automáticamente cuando aparezca una actualización en la tienda de Apple. Si una aplicación tiene habilitada la configuración **Forzar que la aplicación sea administrada**, se actualiza sin pedir confirmación al usuario. La actualización se produce independientemente de si la aplicación es obligatoria u opcional.

   Para usar las configuraciones **Forzar que la aplicación sea administrada** y **Actualización automática de aplicaciones**, habilite la propiedad de servidor `apple.app.force.managed`. Consulte Propiedades del servidor.

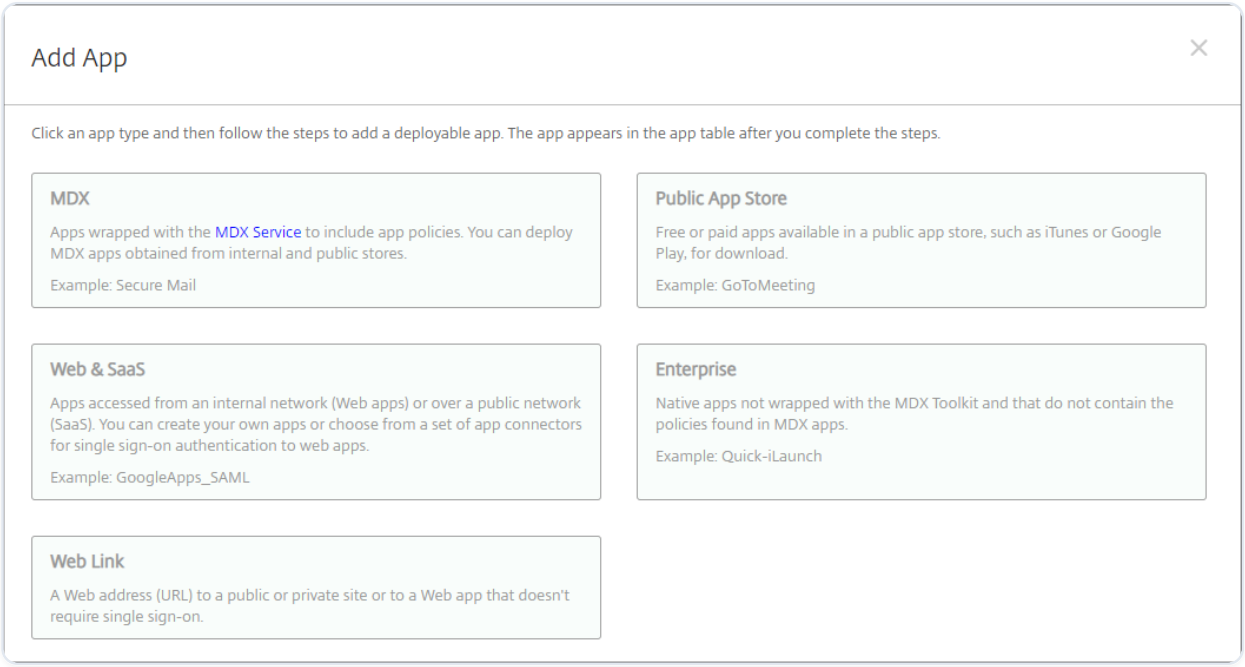
Paso 2: Obtener aplicaciones y licencias de Apple

Compre las aplicaciones en su cuenta de ABM/ASM. Puede realizar compras en Apple Books (solo para iOS/iPadOS) y en la App Store de Apple. Tenga en cuenta que debe comprar todas las aplicaciones, incluso si son gratuitas. Una vez que compre licencias en ABM/ASM, Citrix Endpoint Management mostrará la aplicación automáticamente.

Para obtener información sobre cómo poner las aplicaciones a disposición de su empresa, consulte la documentación de Apple.

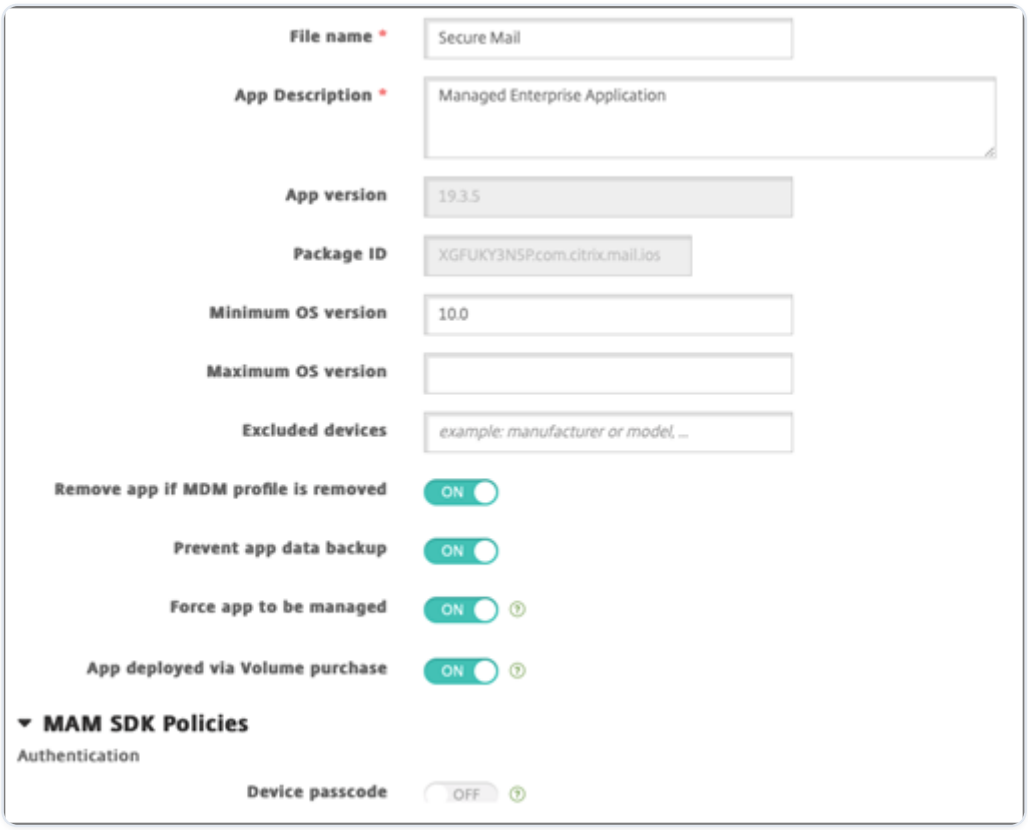
Paso 3: Agregar y configurar aplicaciones

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar**.
2. Haga clic en **MDX**.

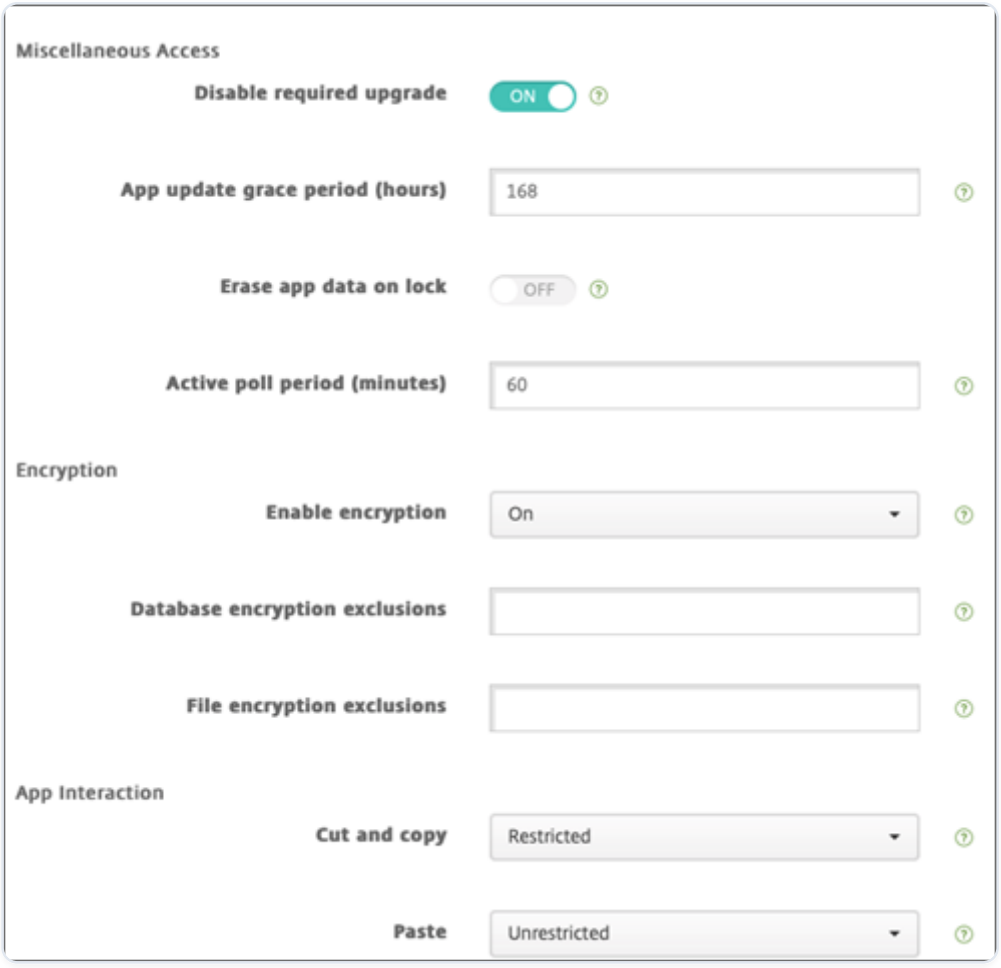


3. Seleccione **iPhone** o **iPad** para las plataformas.
4. Cargue el archivo MDX.
5. Configure los detalles de la aplicación. Establezca **Aplicación implementada a través de Volume Purchase** en **Activado**. Citrix también recomienda habilitar la función **Forzar la**

administración de la aplicación.



6. Configure las directivas MDX. Establezca **Inhabilitar actualización obligatoria** en **Activado**.

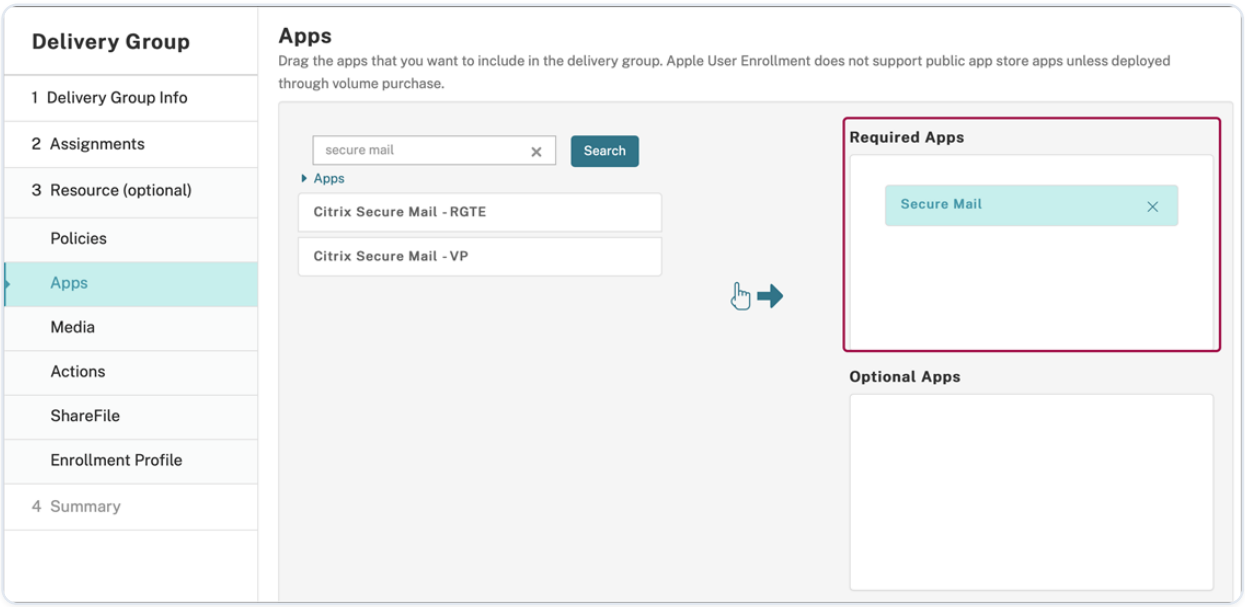


7. Asigne un grupo de entrega a la aplicación para cada plataforma y haga clic en **Guardar**.

Esta configuración da como resultado dos entradas para esta aplicación en la lista de aplicaciones. Cuando seleccione una aplicación para configurar, seleccione la aplicación con **Tipo MDX**.

Paso 4: Configurar la implementación de la aplicación

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Grupos de entrega** y haga clic en **Agregar**.
2. En la sección **Aplicaciones**, arrastre las aplicaciones MDX deseadas al cuadro **Aplicaciones requeridas**.



3. Vaya a **Configurar > Grupos de entrega**.
4. Seleccione el grupo de entrega y haga clic en **Implementar**.

5. Los usuarios reciben una solicitud para instalar la aplicación y esta se instala en segundo plano después de que la aceptan.



Aplicaciones personalizadas

Las aplicaciones personalizadas son aplicaciones empresariales (B2B) propietarias. Puede usar Citrix Endpoint Management y Apple Volume Purchase para distribuir aplicaciones propietarias de forma privada y segura. Puede distribuir las aplicaciones a socios, clientes, franquiciados y empleados internos específicos.

DISPONIBILIDAD DE FUNCIONES	
Requiere supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	Sí
Disponible en	iOS/iPadOS

Requisitos para aplicaciones personalizadas

- Cuenta de Apple Business Manager o Apple School Manager
- Cuenta de Apple Volume Purchase (requiere dispositivos con iOS 7 o posterior)

- Inscriba los dispositivos en Citrix Endpoint Management, utilizando uno de los siguientes modos de inscripción de Apple:
  - Inscripción automatizada de dispositivos
  - Inscripción de dispositivos
  - Inscripción de usuarios

Paso 1: Vincular cuentas

Para implementar aplicaciones personalizadas mediante Volume Purchase, vincule su cuenta de Volume Purchase a Citrix Endpoint Management.

1. Configure y regístrese en Apple Business Manager (ABM). Para obtener más información sobre estos programas, consulte la documentación de Apple.
2. Vincule su cuenta de ABM con Citrix Endpoint Management. Para obtener más información sobre cómo vincular cuentas de compra por volumen, consulte Compra por volumen de Apple.
3. Cuando agregue su cuenta de compra por volumen, habilite **Actualización automática de aplicaciones**. Esta configuración garantiza que las aplicaciones en los dispositivos de los usuarios se actualicen automáticamente cuando aparezca una actualización en la tienda de Apple. Si una aplicación tiene habilitada la configuración **Forzar que la aplicación sea administrada**, se actualizará sin solicitar la intervención del usuario. La actualización se produce independientemente de si la aplicación es obligatoria u opcional.

   Para usar las configuraciones **Forzar que la aplicación sea administrada** y **Actualización automática de aplicaciones**, habilite la propiedad de servidor `apple.app.force.managed`. Consulte Propiedades del servidor.

Paso 2: Configurar aplicaciones en ABM

Agregue aplicaciones en su cuenta de ABM. Puede cargar y distribuir sus propias aplicaciones personalizadas o comprar licencias para aplicaciones personalizadas de otras organizaciones. Para obtener más información sobre cómo agregar y habilitar aplicaciones personalizadas en ABM, consulte la documentación de Apple.

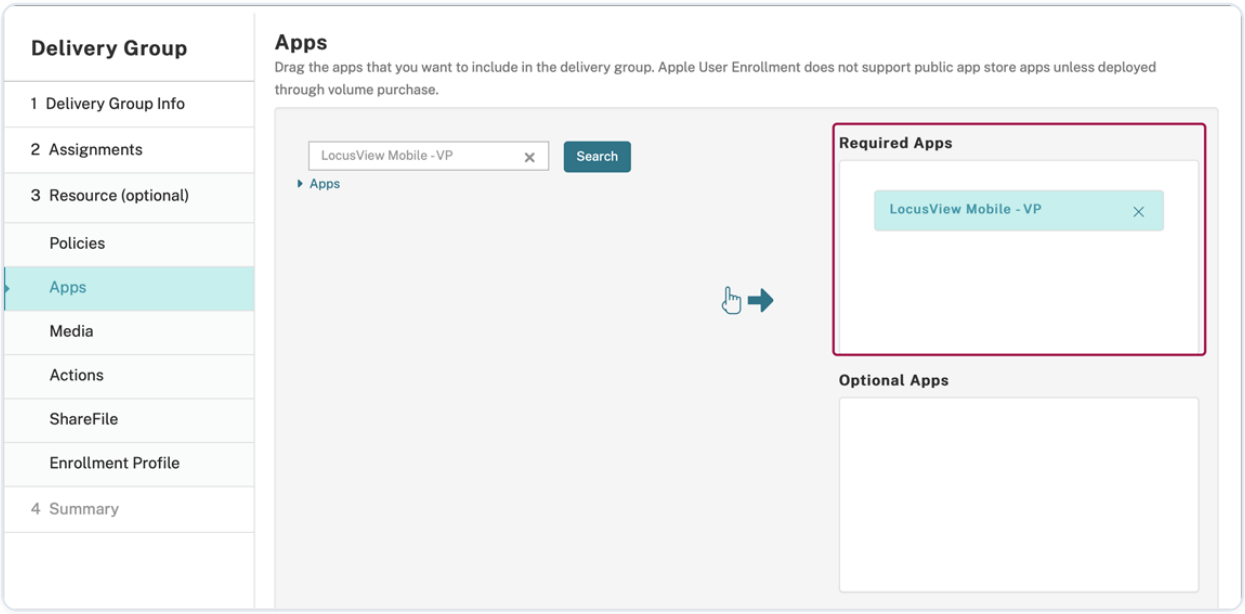
Paso 3: Agregar y configurar aplicaciones en Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones**. Las aplicaciones de compra por volumen aparecen en la lista de aplicaciones.
2. Seleccione la aplicación que desea configurar. Haga clic en **Editar**.
3. Seleccione las plataformas: **iPhone**, **iPad** o **macOS**.

4. Elija los grupos de entrega a los que desea distribuir la aplicación. Haga clic en **Guardar**.

Paso 4: Configurar la implementación de aplicaciones

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Grupos de entrega** y haga clic en **Agregar**.
2. En la sección **Aplicaciones**, arrastre las aplicaciones deseadas al cuadro **Aplicaciones requeridas**.



3. Vuelva a **Configurar > Grupos de entrega**.
4. Seleccione el grupo de entrega que quiere implementar y haga clic en **Implementar**.

5. Los usuarios reciben una solicitud para implementar aplicaciones. Las aplicaciones se instalan en segundo plano después de que los usuarios las aceptan.



Aplicaciones personalizadas habilitadas para MDX

Para usar las directivas MDX y las funciones de seguridad, agregue aplicaciones personalizadas que tengan el SDK de MAM habilitado o que estén encapsuladas en MDX.

DISPONIBILIDAD DE FUNCIONES	
Requiere supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	Sí
Disponible en	iOS/iPadOS

Paso 1: Vincular cuentas

Para implementar aplicaciones personalizadas mediante la compra por volumen, vincule su cuenta de compra por volumen a Citrix Endpoint Management.

1. Configure e inscríbase en Apple Business Manager (ABM). Para obtener más información sobre estos programas, consulte la documentación de Apple.

2. Vincule su cuenta de ABM con Citrix Endpoint Management. Para obtener más información sobre cómo vincular cuentas de compra por volumen, consulte Compra por volumen de Apple.
3. Cuando añada su cuenta de Compra por volumen, habilite **Actualización automática de aplicaciones**. Esta configuración garantiza que las aplicaciones en los dispositivos de los usuarios se actualicen automáticamente cuando aparezca una actualización en la tienda de Apple. Si una aplicación tiene habilitada la configuración **Forzar la administración de la aplicación**, se actualiza sin pedir confirmación al usuario. La actualización se produce independientemente de si la aplicación es obligatoria u opcional.

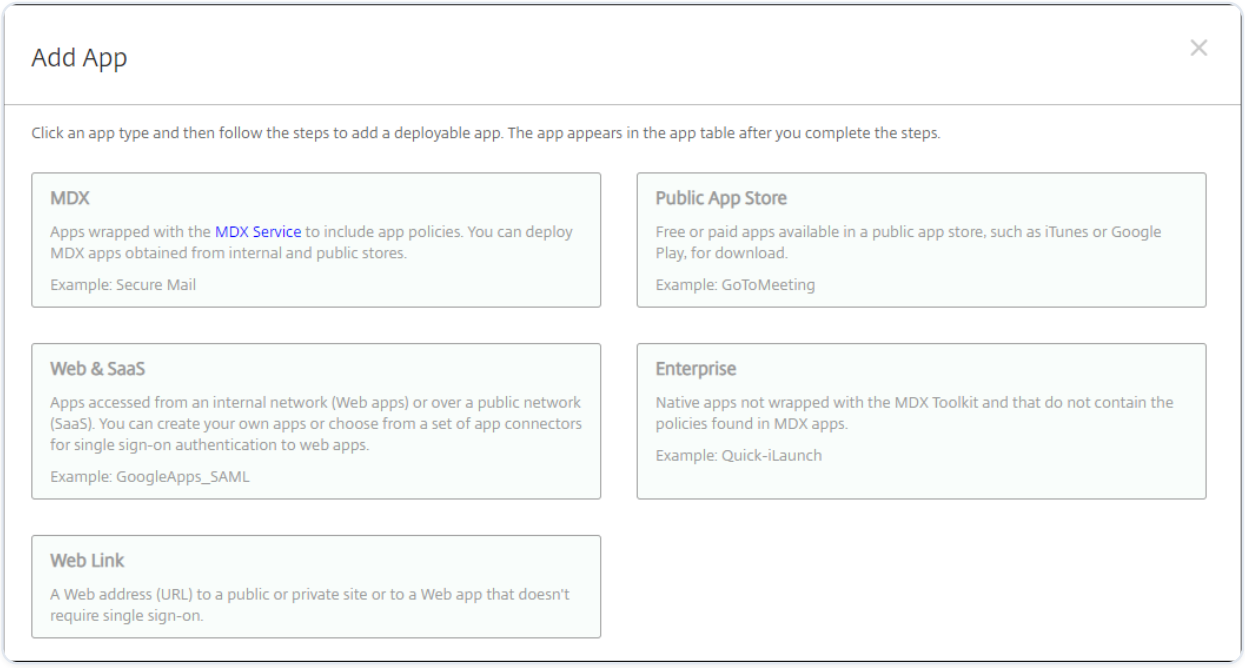
   Para usar las configuraciones **Forzar la administración de la aplicación** y **Actualización automática de aplicaciones**, habilite la propiedad de servidor `apple.app.force.managed`. Consulte Propiedades del servidor.

Paso 2: Configurar aplicaciones en ABM

Agregue aplicaciones en su cuenta de ABM. Puede cargar y distribuir sus propias aplicaciones personalizadas o comprar licencias para aplicaciones personalizadas de otras organizaciones. Para obtener más información sobre cómo agregar y habilitar aplicaciones personalizadas en ABM, consulte la documentación de Apple.

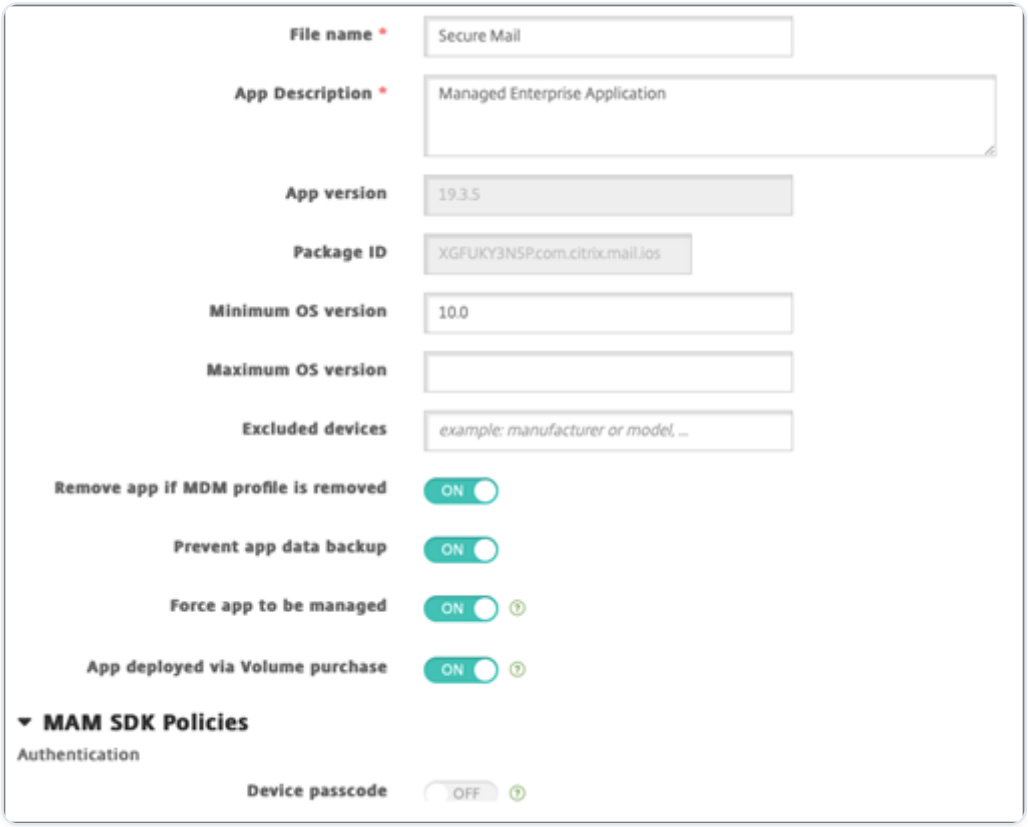
Paso 3: Agregar y configurar aplicaciones en Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones**. Haga clic en **Agregar**.
2. Haga clic en **MDX**.

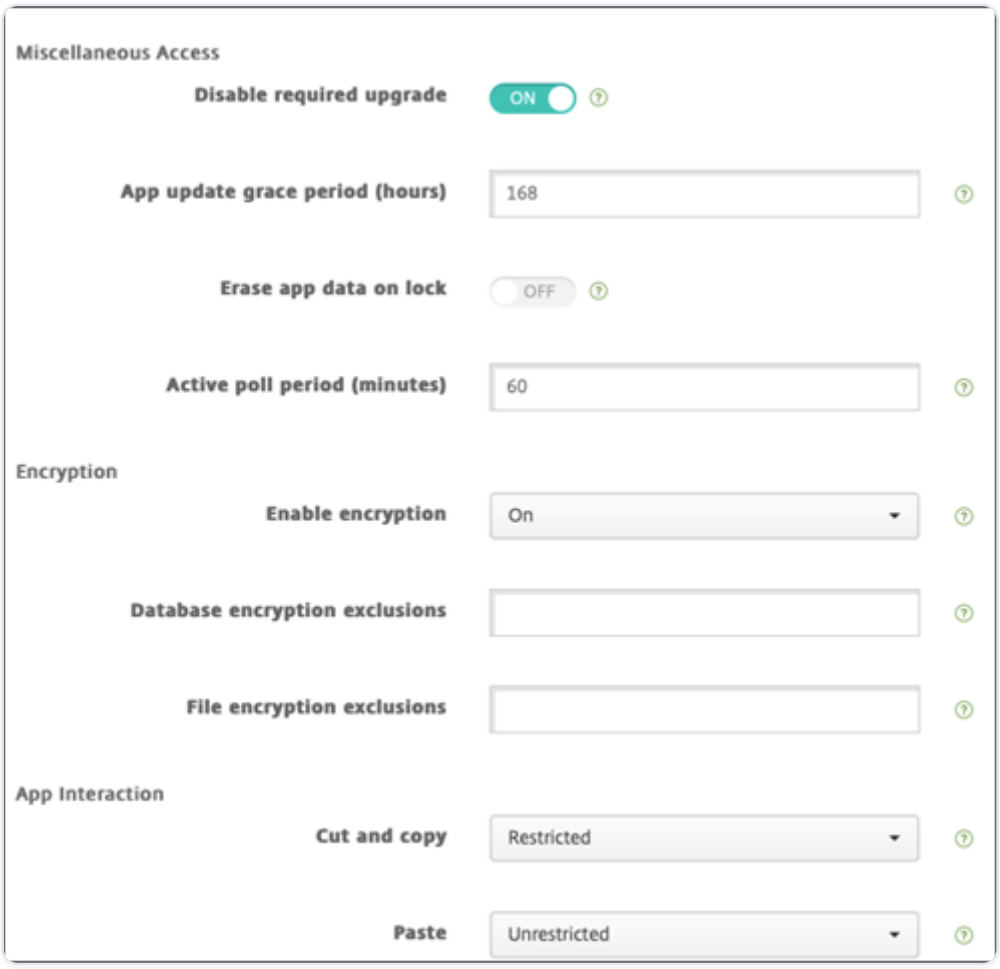


3. Seleccione las plataformas **iPhone** o **iPad**.

4. Cargue el archivo MDX de la aplicación que desea agregar.
5. Configure los detalles de la aplicación. Establezca **Aplicación implementada mediante compra por volumen** en **Activado**. Citrix también recomienda habilitar la función **Forzar la administración de la aplicación**.



6. Configure las directivas MDX. Establezca **Inhabilitar actualización obligatoria** en **Activado**.



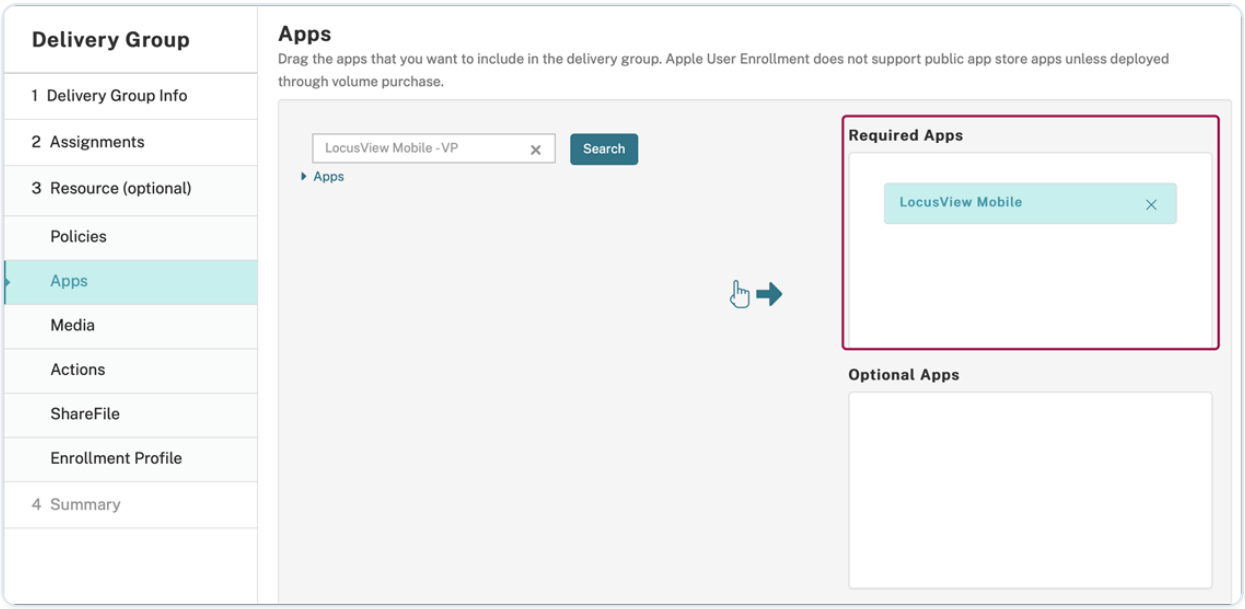
7. Asigne un grupo de entrega a la aplicación y haga clic en **Guardar**.

Esta configuración da como resultado dos entradas para esta aplicación en la lista de aplicaciones. Cuando seleccione una aplicación para configurar, seleccione la aplicación con **Tipo MDX**.

Paso 4: Configurar la implementación de la aplicación

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones**. Las aplicaciones de compra por volumen aparecen en la lista de aplicaciones.
2. Seleccione la aplicación que desea configurar. Haga clic en **Editar**.
3. Elija los grupos de entrega a los que desea que se distribuya la aplicación en cada plataforma. Haga clic en **Guardar**.
4. Vaya a **Configurar > Grupos de entrega** y haga clic en **Agregar**.

5. En la sección **Aplicaciones**, arrastre las aplicaciones MDX deseadas al cuadro **Aplicaciones obligatorias**.



6. Vuelva a **Configurar > Grupos de entrega**.
7. Seleccione el grupo de entrega que desea implementar y haga clic en **Implementar**.
8. Los usuarios reciben una solicitud para implementar aplicaciones. Las aplicaciones se instalan en segundo plano después de que los usuarios aceptan.

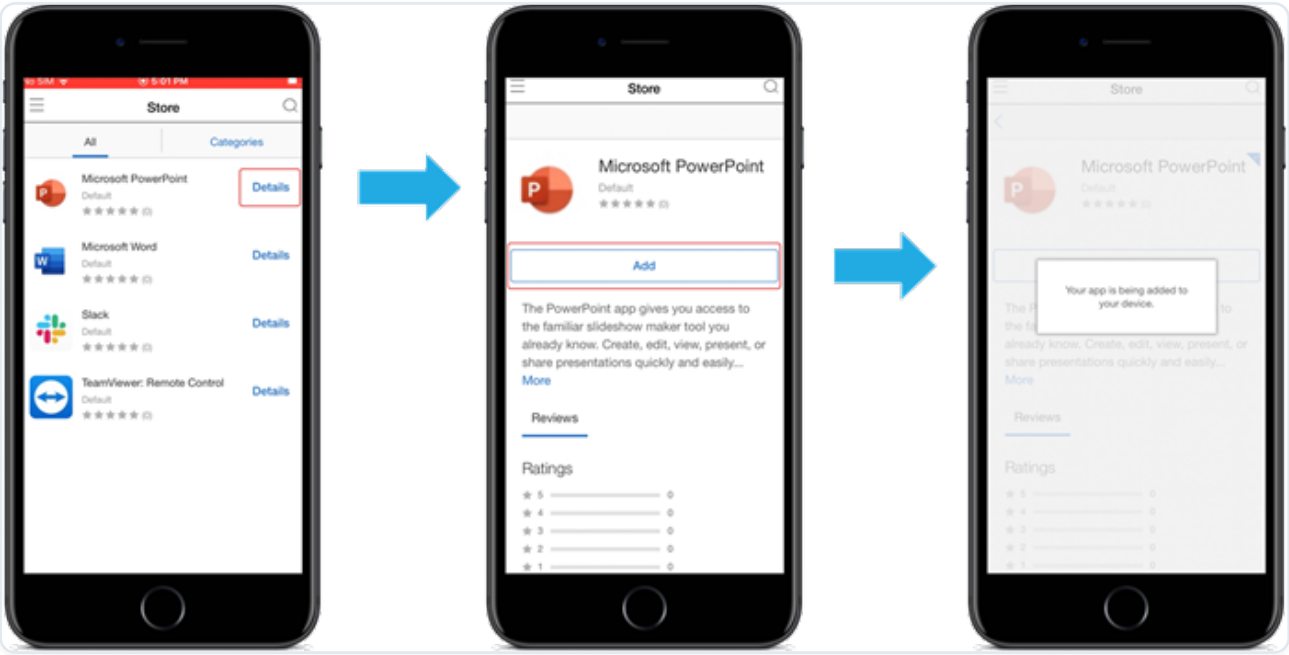


Aplicaciones opcionales (solo iOS/iPadOS)

Citrix recomienda implementar las aplicaciones como **Obligatorias**. Las aplicaciones obligatorias se instalan de forma silenciosa en los dispositivos de los usuarios, lo que minimiza la interacción. Tener esta función habilitada también permite que las aplicaciones se actualicen automáticamente.

Las aplicaciones opcionales permiten a los usuarios elegir qué aplicaciones instalar, pero los usuarios deben iniciar la instalación manualmente a través de Citrix Secure Hub.

Para instalar aplicaciones opcionales, los usuarios deben iniciar Citrix Secure Hub, ir a **Tienda**, seleccionar **Detalles** para la aplicación deseada y hacer clic en **Agregar**.



Control de acceso a la red

Puede utilizar su solución de control de acceso a la red (NAC) para ampliar la evaluación de seguridad de dispositivos de Citrix Endpoint Management para dispositivos Android y Apple. Su solución NAC utiliza la evaluación de seguridad de Citrix Endpoint Management para facilitar y gestionar las decisiones de autenticación. Una vez que configure su dispositivo NAC, las directivas de dispositivo y los filtros NAC que configure en Citrix Endpoint Management se aplicarán.

El uso de Citrix Endpoint Management con una solución NAC añade QoS y un control más granular sobre los dispositivos internos de su red. Para obtener un resumen de las ventajas de integrar NAC con Citrix Endpoint Management, consulte Control de acceso.

Citrix admite estas soluciones para la integración con Citrix Endpoint Management:

- NetScaler Gateway
- ForeScout

Citrix® no garantiza la integración para otras soluciones NAC.

Con un dispositivo NAC en su red:

- Citrix Endpoint Management admite NAC como una función de seguridad de punto final para dispositivos iOS, Android Enterprise y Android.
- Puede habilitar filtros en Citrix Endpoint Management para establecer dispositivos como conformes o no conformes para NAC, según reglas o propiedades. Por ejemplo:
  - Si un dispositivo administrado en Citrix Endpoint Management no cumple los criterios especificados, Citrix Endpoint Management marca el dispositivo como no conforme. Un dispositivo NAC bloquea los dispositivos no conformes en su red.
  - Si un dispositivo administrado en Citrix Endpoint Management tiene aplicaciones no conformes instaladas, un filtro NAC puede bloquear la conexión VPN. Como resultado, un dispositivo de usuario no conforme no puede acceder a aplicaciones o sitios web a través de la VPN.
  - Si utiliza NetScaler Gateway para NAC, puede habilitar la tunelización dividida para evitar que el plug-in de NetScaler Gateway envíe tráfico de red innecesario a NetScaler Gateway. Para obtener más información sobre la tunelización dividida, consulte Configurar la tunelización dividida.

Filtros de cumplimiento de NAC admitidos

Citrix Endpoint Management admite los siguientes filtros de cumplimiento de NAC:

Dispositivos anónimos: Comprueba si un dispositivo está en modo anónimo. Esta comprobación está disponible si Citrix Endpoint Management no puede volver a autenticar al usuario cuando un dispositivo intenta volver a conectarse.

Aplicaciones prohibidas: Comprueba si un dispositivo tiene aplicaciones prohibidas, tal como se define en una directiva de acceso a aplicaciones. Para obtener más información sobre esa directiva, consulte Directivas de dispositivo de acceso a aplicaciones.

Dispositivos inactivos: Comprueba si un dispositivo está inactivo según lo definido por la configuración **Umbral de días de inactividad del dispositivo** en **Propiedades del servidor**. Para obtener más información, consulte Propiedades del servidor.

Aplicaciones obligatorias que faltan: Comprueba si a un dispositivo le faltan aplicaciones obligatorias, tal como se define en una directiva de acceso a aplicaciones.

Aplicaciones no sugeridas: Comprueba si un dispositivo tiene aplicaciones no sugeridas, tal como se define en una directiva de acceso a aplicaciones.

Contraseña no conforme: Comprueba si la contraseña del usuario es conforme. En dispositivos iOS y Android, Citrix Endpoint Management puede determinar si la contraseña actual del dispositivo cumple con la directiva de código de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para establecer una contraseña si Citrix Endpoint Management envía una directiva de código de acceso al dispositivo. Antes de que el usuario establezca la contraseña, el código de acceso podría no ser conforme.

Dispositivos no conformes: Comprueba si un dispositivo no es conforme, basándose en la propiedad de dispositivo No conforme. Normalmente, las acciones automatizadas o terceros que utilizan las API de Citrix Endpoint Management cambian esa propiedad.

Estado revocado: Comprueba si el certificado del dispositivo está revocado. Un dispositivo revocado no puede volver a inscribirse hasta que se autorice de nuevo.

Dispositivos Android rooteados y iOS con jailbreak: Comprueba si un dispositivo Android o iOS tiene jailbreak.

Dispositivos no administrados: Comprueba si Citrix Endpoint Management está administrando un dispositivo. Por ejemplo, un dispositivo inscrito en MAM o un dispositivo no inscrito no se administra.

> **Nota:**
>
> El filtro Implícitamente conforme/No conforme establece el valor predeterminado solo en los dispositivos que administra Citrix Endpoint Management. Por ejemplo, cualquier dispositivo que tenga una aplicación bloqueada instalada o que no esté inscrito, se marca como No conforme. El dispositivo NAC bloquea esos dispositivos de su red.

Información general de la configuración

Recomendamos configurar los componentes de NAC en el orden indicado.

1. Configurar directivas de dispositivo para admitir NAC:

   Para dispositivos iOS: Consulte Configurar la directiva de dispositivo VPN para admitir NAC.

   Para dispositivos Android Enterprise: Consulte Crear una configuración administrada de Android Enterprise para Citrix SSO.

Para dispositivos Android: Consulte Configurar el protocolo Citrix SSO para Android.

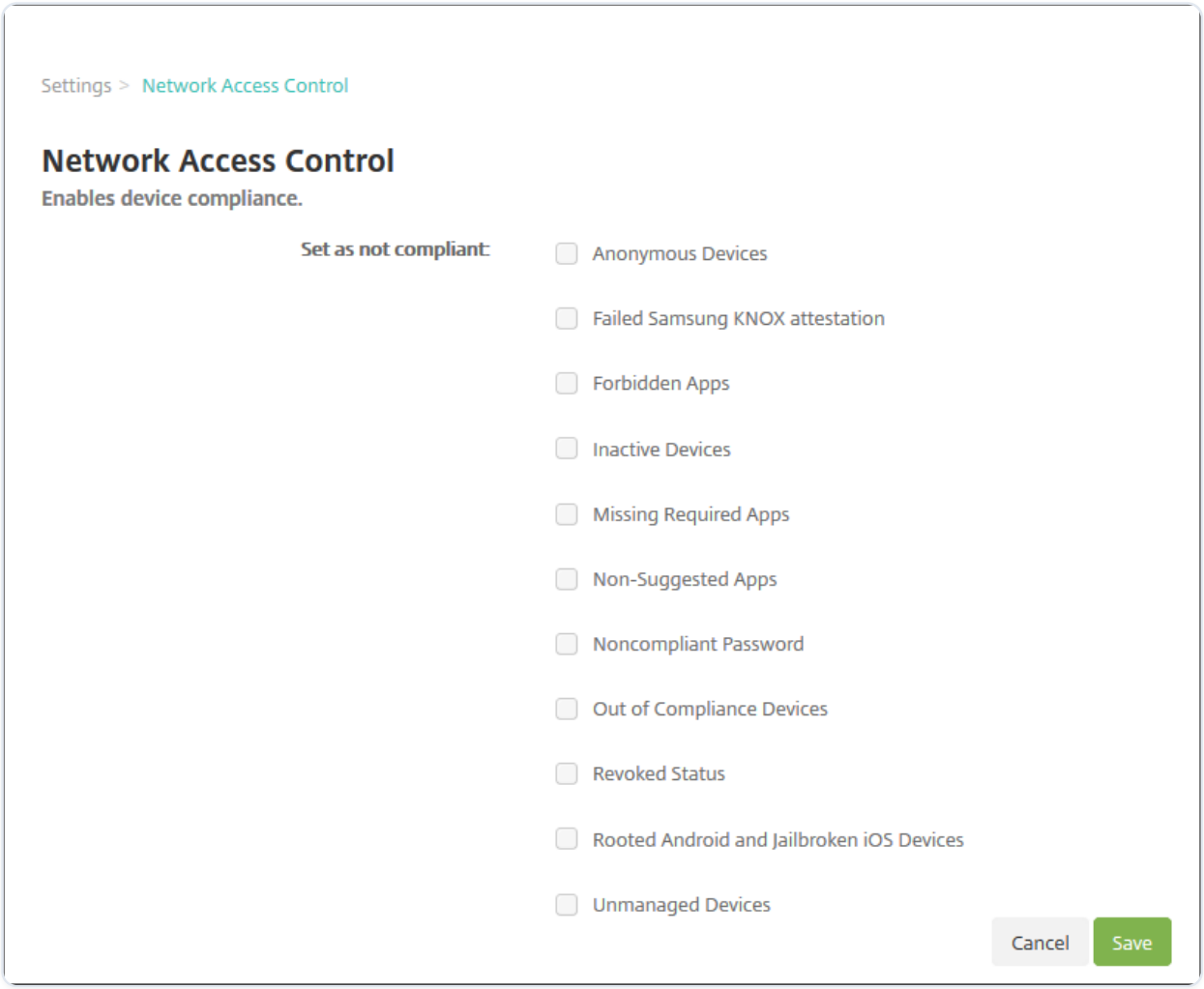
2. Habilitar filtros NAC en Citrix Endpoint Management.
3. Configure una solución NAC:

   - NetScaler Gateway, detallado en Actualizar las directivas de NetScaler Gateway para admitir NAC.

     Requiere que instale Citrix SSO en los dispositivos. Consulte Clientes de NetScaler Gateway.
   - ForeScout: Consulte la documentación de ForeScout.

Habilitar filtros NAC en Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Control de acceso a la red**.



2. Seleccione las casillas de verificación de los filtros **Establecer como no compatible** que quiera habilitar.

3. Haga clic en **Guardar**.

Actualizar las directivas de NetScaler Gateway para admitir NAC

Debe configurar directivas avanzadas (no clásicas) de autenticación y sesiones VPN en su servidor virtual VPN.

Estos pasos actualizan un NetScaler Gateway con cualquiera de estas características:

- Está integrado con Citrix Endpoint Management.
- O bien, está configurado para VPN, no forma parte del entorno de Citrix Endpoint Management y puede acceder a Citrix Endpoint Management.

En su servidor VPN virtual, desde una ventana de consola, haga lo siguiente. Los FQDN y las direcciones IP de los comandos y ejemplos son ficticios.

1. Si utiliza directivas clásicas en su servidor virtual VPN, elimine y desvincule todas las directivas clásicas. Para comprobarlo, escriba:

   `show vpn vserver <VPN_VServer>`

   Elimine cualquier resultado que contenga la palabra **Classic**. Por ejemplo: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

   Para eliminar la directiva, escriba:

   `unbind vpn vserver <VPN_VServer> -policy <policy_name>`
2. Cree la directiva de sesión avanzada correspondiente escribiendo lo siguiente.

   `add vpn sessionPolicy <policy_name> <rule> <session action>`

   Por ejemplo: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`
3. Vincule la directiva a su servidor virtual VPN escribiendo lo siguiente.

   `bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100`
4. Cree un servidor virtual de autenticación escribiendo lo siguiente.

   `add authentication vserver <authentication vserver name> <service type> <ip address>`

   Por ejemplo: `add authentication vserver authvs SSL 0.0.0.0` En el ejemplo, `0.0.0.0` significa que el servidor virtual de autenticación no está expuesto al público.

5. Enlace un certificado SSL con el servidor virtual escribiendo lo siguiente.

   `bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>`

   Por ejemplo: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. Asocie un perfil de autenticación al servidor virtual de autenticación desde el servidor virtual VPN. Primero, cree el perfil de autenticación escribiendo lo siguiente.

   `add authentication authnProfile <profile name> -authnVsName <authentication vserver name>`

   Por ejemplo:

   `add authentication authnProfile xm_nac_prof -authnVsName authvs`

7. Asocie el perfil de autenticación con el servidor virtual VPN escribiendo lo siguiente.

   `set vpn vserver <vpn vserver name> -authnProfile <authn profile name>`

   Por ejemplo:

   `set vpn vserver _XM_EndpointManagement -authnProfile xm_nac_prof`

8. Compruebe la conexión de NetScaler Gateway a un dispositivo escribiendo lo siguiente.

   `curl -v -k https://<Endpoint Management_server>:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"`

   Por ejemplo, esta consulta verifica la conectividad obteniendo el estado de cumplimiento del primer dispositivo (`deviceid_1`) inscrito en el entorno:

   `curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"`

   Un resultado correcto es similar al siguiente ejemplo.

   ```
   HTTP/1.1 200 OK

   < Server: Apache-Coyote/1.1

   < X-Citrix-Device-State: Non Compliant
   ```

```
< Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
```

9. Cuando el paso anterior se realice correctamente, cree la acción de autenticación web para Citrix Endpoint Management. Primero, cree una expresión de directiva para extraer el ID del dispositivo del complemento VPN de iOS. Escriba lo siguiente.

   ```
   add policy expression xm_deviceid_expression
   "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\',
   \'&\').VALUE(\"deviceidvalue\")"
   ```

10. Envíe la solicitud a Citrix Endpoint Management escribiendo lo siguiente. En este ejemplo, la IP de Citrix Endpoint Management es `10.207.87.82` y el FQDN es `example.em.cloud.com:4443`.

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort
    4443 -fullReqExpr q{"GET /Citrix/Device/v1/Check HTTP/1.1\r\n" + "Host:
    example.em.cloud.com:4443\r\n" + "X-Citrix-VPN-Device-ID: " +
    xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule
    "HTTP.RES.STATUS.EQ(\"200\") &&HTTP.RES.HEADER(\"X-Citrix-Device-
    State\").EQ(\"Compliant\")"
    ```

    La salida correcta para el NAC de Citrix Endpoint Management es `HTTP status 200 OK`. El encabezado `X-Citrix-Device-State` debe tener el valor de `Compliant`.

11. Cree una directiva de autenticación con la que asociar la acción escribiendo lo siguiente.

    ```
    add authentication Policy <policy name> -rule <rule> -action <web
    authentication action>
    ```

    Por ejemplo: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")" -action xm_nac`

12. Convierta la directiva LDAP existente en una directiva avanzada escribiendo lo siguiente.

    ```
    add authentication Policy <policy_name> -rule <rule> -action <LDAP action
    name>
    ```

    Por ejemplo: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. Agregue una etiqueta de directiva con la que asociar la directiva LDAP escribiendo lo siguiente.

`add authentication policylabel <policy_label_name>`

Por ejemplo: `add authentication policylabel ldap_pol_label`

14. Asocie la directiva LDAP a la etiqueta de directiva escribiendo lo siguiente.

    `bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT`

15. Conecte un dispositivo compatible para realizar una prueba de NAC y confirmar la autenticación LDAP correcta. Escriba lo siguiente.

    `bind authentication vserver <authentication vserver> -policy <web authentication policy> -priority 100 -nextFactor <ldap policy label> -gotoPriorityExpression END`

16. Agregue la interfaz de usuario para asociarla con el servidor virtual de autenticación. Escriba el siguiente comando para recuperar el ID del dispositivo.

    `add authentication loginSchemaPolicy <schema policy>-rule <rule> -action lschema_single_factor_deviceid`

17. Enlace el servidor virtual de autenticación escribiendo lo siguiente.

    `bind authentication vserver authvs -policy lschema_xm_nac_pol -priority 100 -gotoPriorityExpression END`

18. Cree una directiva de autenticación avanzada LDAP para habilitar la conexión de Citrix Secure Hub. Escriba lo siguiente.

    `add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\").NOT" -action 10.200.80.60_LDAP`

    `bind authentication vserver authvs -policy ldap_xm_test_pol -priority 110 -gotoPriorityExpression NEXT`

Windows

Escritorio y tableta Windows

Citrix Endpoint Management inscribe dispositivos Windows 10 y Windows 11 en MDM. Citrix Endpoint Management admite los siguientes tipos de autenticación para dispositivos Windows 10 y Windows 11 inscritos en MDM:

- Autenticación basada en dominio

  - Active Directory
  - Azure Active Directory

- Proveedores de identidades:
  - Azure Active Directory
  - Proveedor de identidades de Citrix®

Para obtener más información sobre los tipos de autenticación admitidos, consulte Certificados y autenticación.

Un flujo de trabajo general para iniciar la administración de dispositivos Windows 10 o Windows 11 es el siguiente:

1. Complete el proceso de incorporación. Consulte Incorporación y configuración de recursos y Preparar la inscripción de dispositivos y la entrega de recursos.

   Si tiene previsto inscribir dispositivos Windows mediante el servicio AutoDiscovery, debe configurar el servicio Citrix AutoDiscovery. Solicite asistencia al Soporte técnico de Citrix. Para obtener más información, consulte Solicitar AutoDiscovery para dispositivos Windows.
2. Elija y configure un método de inscripción. Consulte Métodos de inscripción admitidos.
3. Configurar directivas de dispositivos de escritorio y tableta Windows.
4. Los usuarios inscriben dispositivos Windows 10 y Windows 11.
5. Configure acciones de seguridad de dispositivos y aplicaciones. Consulte Acciones de seguridad.

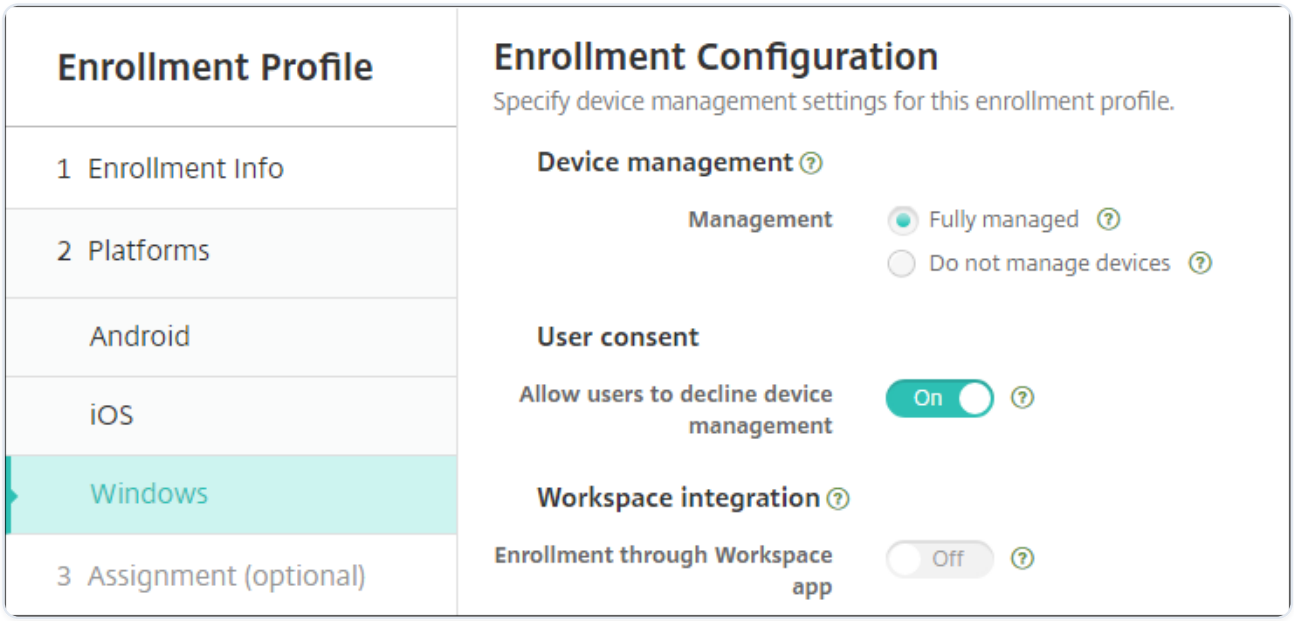
Para ver los sistemas operativos compatibles, consulte Sistemas operativos de dispositivos compatibles.

Métodos de inscripción compatibles

Puede especificar cómo administrar dispositivos Windows 10 y Windows 11 en los perfiles de inscripción. Hay dos opciones disponibles:

- Totalmente administrado (inscripción MDM)
- No administrar dispositivos (sin inscripción MDM)

Para configurar los ajustes de inscripción para dispositivos Windows 10 y Windows 11, vaya a **Configurar > Perfiles de inscripción > Windows**. Para obtener más información sobre los perfiles de inscripción, consulte Perfiles de inscripción.



La siguiente tabla enumera los métodos de inscripción que Citrix Endpoint Management admite para dispositivos Windows 10 y Windows 11:

MÉTODO	COMPATIBLE
Inscripción en Azure Active Directory	Sí
Inscripción en el servicio AutoDiscovery	Sí
Inscripción masiva de Windows	Sí
Inscripción manual	Sí
Invitaciones de inscripción	No

Nota:

- La inscripción manual requiere que los usuarios introduzcan un nombre de dominio completo (FQDN) del servidor de Citrix Endpoint Management. No recomendamos utilizar la inscripción manual. En su lugar, utilice otros métodos para simplificar el proceso de inscripción para los usuarios.
- No puede enviar invitaciones de inscripción a dispositivos Windows. Los usuarios de Windows se inscriben directamente a través de sus dispositivos.

Configurar las directivas de dispositivos de escritorio y tabletas Windows

Utilice estas directivas para configurar cómo Citrix Endpoint Management interactúa con los dispositivos de escritorio y tabletas que ejecutan Windows 10 o Windows 11. Esta tabla enumera todas las directivas de dispositivos disponibles para dispositivos de escritorio y tabletas Windows.

Configuración de aplicaciones	Inventario de aplicaciones	Bloqueo de aplicaciones
Desinstalación de aplicaciones	Protección de aplicaciones	BitLocker
Credenciales	XML personalizado	Defender
Protección de dispositivos	Atestación de estado del dispositivo	Exchange
Firewall	Kiosco	Red
Office	Actualización del SO	Código de acceso
Restricciones	Tienda	Términos y condiciones
VPN	Clip web	Agente de Windows
Configuración de GPO de Windows	Windows Hello para empresas	

Inscribir dispositivos Windows 10 y Windows 11 a través de Azure Active Directory

Importante:

Antes de que los usuarios puedan inscribirse, debe configurar los ajustes de Azure Active Directory (AD) en Azure y, a continuación, configurar Citrix Endpoint Management. Para obtener más información, consulte Conectar Citrix Endpoint Management a Azure AD.

Los dispositivos Windows 10 y Windows 11 pueden inscribirse en Azure como un medio federado de autenticación de AD. Esta inscripción requiere una suscripción a Azure AD Premium.

Puede unir dispositivos Windows 10 y Windows 11 a Microsoft Azure AD mediante cualquiera de los siguientes métodos:

- Para dispositivos propiedad de la empresa:
  - Inscribirse en MDM al unir el dispositivo a Azure AD la primera vez que se enciende. En este escenario, los usuarios completan la inscripción como se describe en este artículo: `<https://docs.microsoft.com/es-es/azure/active-directory/devices/azuread-joined-devices-frx>`.

    Para los dispositivos Windows que inscriba con este método, puede usar Windows AutoPilot para configurar y preconfigurar los dispositivos. Para obtener más información, consulte Usar Windows AutoPilot para configurar dispositivos.
  - Inscribir en MDM al unir el dispositivo a Azure AD desde la página de **Configuración** de Windows después de configurar el dispositivo. En este escenario, los usuarios completan la inscripción como se describe en Inscribir en MDM al unir Azure AD después de configurar dispositivos.
- Para dispositivos personales (BYOD o dispositivos móviles):
  - Inscribir en MDM al registrarse en Azure AD mientras se agrega la cuenta profesional de Microsoft a Windows. En este escenario, los usuarios completan la inscripción como se describe en Inscribir en MDM al registrarse en Azure AD.

Inscribir en MDM al unir Azure AD después de configurar dispositivos

1. En un dispositivo, desde el menú Inicio, vaya a **Configuración > Cuentas > Acceder a trabajo o escuela** y haga clic en **Conectar**.
2. En el cuadro de diálogo **Configurar una cuenta profesional o educativa**, en **Acciones alternativas**, haga clic en **Unir este dispositivo a Azure Active Directory**.
3. Introduzca las credenciales de Azure AD y haga clic en **Iniciar sesión**.
4. Acepte los términos y condiciones que requiere la organización.
   - Si los usuarios hacen clic en **Rechazar**, el dispositivo no se une a Azure AD ni se inscribe en Citrix Endpoint Management.
5. Haga clic en **Unirse** para continuar con el proceso de inscripción.
6. Haga clic en **Listo** para completar el proceso de inscripción.

Inscribir en MDM al registrarse en Azure AD

1. En un dispositivo, desde el menú Inicio, vaya a **Configuración > Cuentas > Acceder a trabajo o escuela** y haga clic en **Conectar**.
2. En el cuadro de diálogo **Configurar una cuenta profesional o educativa**, introduzca las credenciales de Azure AD y haga clic en **Iniciar sesión**.
3. Acepte los términos y condiciones que requiere la organización. El dispositivo se registra en Azure AD y se inscribe en Citrix Endpoint Management.

    - Si los usuarios hacen clic en **Rechazar**, el dispositivo se registra en Azure AD, pero no se inscribe en Citrix Endpoint Management. No hay ningún botón de **Información** en la cuenta.

4. Haga clic en **Unirse** para continuar con el proceso de inscripción.
5. Haga clic en **Listo** para completar el proceso de inscripción.

Inscribir dispositivos Windows mediante el servicio AutoDiscovery

Para configurar el servicio AutoDiscovery para dispositivos Windows, solicite asistencia al Soporte técnico de Citrix. Para obtener más información, consulte Solicitar AutoDiscovery para dispositivos Windows.

> **Nota:**
>
> Para que los dispositivos Windows se inscriban, el certificado de escucha SSL debe ser un certificado público. La inscripción falla para los certificados SSL autofirmados.

Los usuarios realizan los siguientes pasos para completar la inscripción:

1. En un dispositivo, desde el menú Inicio, vaya a **Configuración > Cuentas > Acceder a trabajo o escuela** y haga clic en **Inscribir solo en la administración de dispositivos**.
2. En el cuadro de diálogo **Configurar una cuenta profesional o educativa**, introduzca una dirección de correo electrónico corporativa y haga clic en **Siguiente**.

    Para inscribirse como usuario local, introduzca una dirección de correo electrónico inexistente con el nombre de dominio correcto (por ejemplo, `foo@mydomain.com`). Ese paso permite al usuario omitir una limitación conocida de Microsoft en la que la administración de dispositivos integrada en Windows realiza la inscripción. En el cuadro de diálogo **Conectando a un servicio**, introduzca el nombre de usuario y la contraseña asociados al usuario local. El

dispositivo encuentra un servidor de Citrix Endpoint Management e inicia el proceso de inscripción.

3. Introduzca las credenciales y haga clic en **Continuar**.
4. En el cuadro de diálogo **Términos de uso**, acepte que el dispositivo sea administrado y, a continuación, haga clic en **Aceptar**.

La inscripción de dispositivos Windows unidos a un dominio a través del servicio AutoDiscovery falla si la directiva de dominio inhabilita la inscripción de MDM. Los usuarios pueden usar cualquiera de los siguientes métodos en su lugar:

- Quite los dispositivos del dominio, inscríbalos y, a continuación, vuelva a unirlos.
- Introduzca el FQDN del servidor de Citrix Endpoint Management para continuar.

Inscripción masiva de Windows

Con la inscripción masiva de Windows, puede configurar muchos dispositivos para que un servidor MDM los administre sin necesidad de volver a crear imágenes de los dispositivos. Se utiliza un paquete de aprovisionamiento para la inscripción masiva de dispositivos de escritorio y portátiles con Windows 10 y Windows 11. Para obtener más información, consulte Inscribir dispositivos Windows de forma masiva.

Acciones de seguridad

Los dispositivos Windows 10 y Windows 11 admiten las siguientes acciones de seguridad. Para obtener una descripción de cada acción de seguridad, consulte Acciones de seguridad.

Localizar	Bloquear	Reiniciar
Revocar	Borrado selectivo	Borrar

Conectar Citrix Endpoint Management a Azure AD

Los dispositivos Windows 10 y Windows 11 se pueden inscribir en Azure. Los usuarios creados en Azure AD pueden tener acceso a los dispositivos. Citrix Endpoint Management se implementa en Microsoft Azure como un servicio MDM. La conexión de Citrix Endpoint Management a Azure AD permite a los usuarios inscribir automáticamente sus dispositivos en Citrix Endpoint Management cuando los inscriben en Azure AD.

Para conectar Citrix Endpoint Management a Azure AD, siga estos pasos:

1. En el portal de Azure, vaya a **Azure Active Directory > Movilidad (MDM y MAM) > Agregar aplicación** y haga clic en **Aplicación MDM local**.
2. Proporcione un nombre para la aplicación y haga clic en **Agregar**.
3. (Opcional) Azure no permite que se utilicen dominios no verificados, como cloud.com, para la configuración de IdP. Si su FQDN de inscripción de Citrix Endpoint Management incluye cloud.com, póngase en contacto con el Soporte de Citrix y proporcióneles el registro TXT de Azure. El Soporte de Citrix verifica el subdominio, lo que le permite continuar con la configuración. Si su FQDN está bajo su propio dominio, puede verificarlo normalmente dentro de Azure.
4. Seleccione la aplicación que creó, configure lo siguiente y, a continuación, haga clic en **Guardar**.
    - **Ámbito de usuario de MDM**. Seleccione **Todos**.
    - **URL de los términos de uso de MDM**. Introduzca el formato, `https://<Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe/tou`.
    - **URL de detección de MDM**. Introduzca el formato, `https:// <Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe`.
5. Haga clic en **Configuración de la aplicación MDM local**.
    - En el panel **Propiedades**, establezca el **URI de ID de aplicación** en el formato `https:// < Citrix Endpoint Management Enrollment FQDN>:8443`. Este URI de ID de aplicación es un ID único que no se puede volver a utilizar en ninguna otra aplicación.
    - En el panel **Permisos requeridos**, seleccione **Microsoft Graph** y **Windows Azure Active Directory**.
    - En el panel **Claves**, cree la clave de autenticación. Haga clic en **Guardar** para ver el valor de la clave. El valor de la clave aparece solo una vez. Guarde la clave para usarla más tarde. Necesitará la clave en el paso 7.
6. En la consola de Citrix Endpoint Management, vaya a **Configuración > Proveedor de identidades (IDP)** y, a continuación, haga clic en **Agregar**.
7. En la página **URL de detección**, configure lo siguiente y haga clic en **Siguiente**.
    - **Nombre de IDP**. Introduzca un nombre único para identificar la conexión IdP que está creando.
    - **Tipo de IDP**. Seleccione **Azure Active Directory**.

- **ID de inquilino**. El **ID de directorio** en Azure. Lo verá cuando navegue a **Azure Active Directory > Propiedades** en Azure.

8. En la página **Información de MDM de Windows**, configure lo siguiente y haga clic en **Siguiente**.
   - **URI de ID de aplicación**. El valor de URI de ID de aplicación que escribió en Azure.
   - **ID de cliente**. El ID de aplicación que ve en el panel **Propiedades** de Azure.
   - **Clave**. El valor de clave que creó y guardó en el paso 4 anterior.
9. En la página **Uso de notificaciones de IDP**, configure lo siguiente y haga clic en Siguiente.
   - **Tipo de identificador de usuario**. Seleccione **userPrincipalName**.
   - **Cadena de identificador de usuario**. Introduzca `${id_token}.upn`.
10. Haga clic en **Guardar**.
11. Agregue un usuario de Azure AD como usuario local y asígnelo a un grupo de usuarios local.
12. Cree una directiva de dispositivo de términos y condiciones y un grupo de entrega que incluya ese grupo de usuarios local.

Administración de dispositivos cuando se integra con Workspace Environment Management™

Solo con Workspace Environment Management (WEM), las implementaciones de MDM no son posibles. Solo con Citrix Endpoint Management, está limitado a administrar dispositivos Windows 10 y Windows 11. Al integrar ambos, WEM puede acceder a las funciones de MDM y usted puede administrar un espectro más amplio de sistemas operativos Windows a través de Citrix Endpoint Management. Esa administración toma la forma de configurar GPO de Windows. Actualmente, los administradores importan un archivo ADMX a Citrix Endpoint Management y lo envían a equipos de escritorio y tabletas con Windows 10 y Windows 11 para configurar aplicaciones específicas. Mediante la directiva de dispositivo de configuración de GPO de Windows, puede configurar GPO y enviar cambios al servicio WEM. El agente WEM aplica entonces los GPO a los dispositivos y sus aplicaciones.

La administración de MDM no es un requisito para la integración de WEM. Cualquier dispositivo compatible con WEM puede recibir configuraciones de GPO, incluso si Citrix Endpoint Management no es compatible con ese dispositivo de forma nativa.

Para obtener una lista de los dispositivos compatibles, consulte Requisitos del sistema operativo.

Los dispositivos que reciben la directiva de dispositivo de configuración de GPO de Windows se ejecutan en un nuevo modo de Citrix Endpoint Management llamado WEM. En la lista **Administrar > Dispositivos** de dispositivos inscritos, la columna **Modo** para los dispositivos administrados por WEM muestra **WEM**.

Para obtener más información, consulte política de dispositivos de configuración de GPO de Windows.

Clave de recuperación de BitLocker

Cifrar discos con BitLocker es una función de seguridad útil. Sin embargo, desbloquear dispositivos puede ser un desafío si el usuario pierde su clave de recuperación de BitLocker. Citrix Endpoint Management ahora puede guardar automáticamente y de forma segura las claves de recuperación de BitLocker para los usuarios. Los usuarios pueden encontrar su clave de recuperación de BitLocker en el portal de autoayuda. Para habilitar y encontrar la clave de recuperación de BitLocker:

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Propiedades del servidor**.
2. Busque `shp` y habilite la función `shp.console.enable`. Asegúrese de que `enable.new.shp` permanezca inhabilitado. Para obtener más información sobre cómo habilitar el portal de autoayuda, consulte Configurar los modos de seguridad de inscripción.
3. Vaya a **Configurar > Directivas de dispositivo**. Busque su directiva de BitLocker o cree una y habilite la opción **Copia de seguridad de recuperación de BitLocker en Citrix Endpoint Management**.

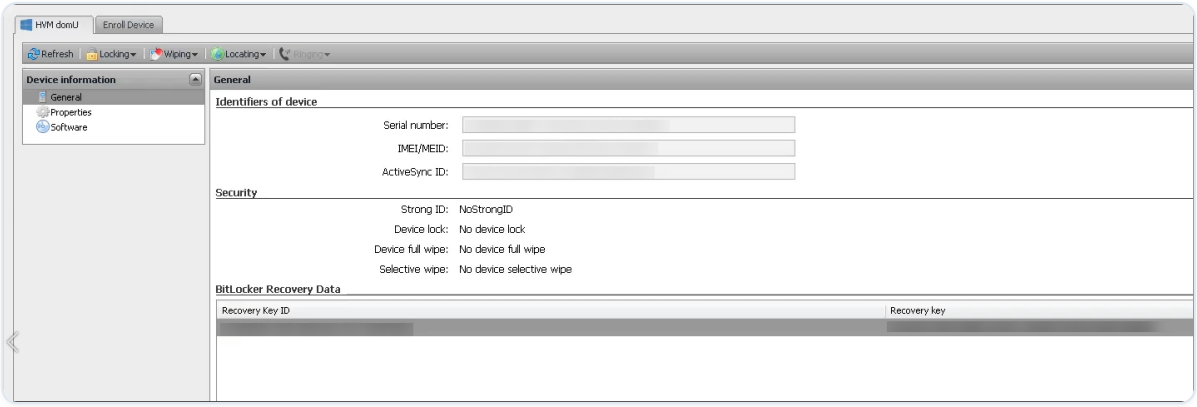
Al desbloquear su dispositivo, los usuarios finales ven un mensaje que les pide que introduzcan su clave. El mensaje también muestra el ID de la clave de recuperación.



Para encontrar su clave de recuperación de BitLocker, los usuarios deben ir al portal de autoayuda.

1. En los detalles **Generales**, consulte los **Datos de recuperación de BitLocker**.

    - **ID de clave de recuperación:** El identificador de la clave de recuperación de BitLocker utilizada para cifrar el disco. Este ID debe coincidir con el ID de clave proporcionado en el mensaje anterior.
    - **Clave de recuperación:** La clave que el usuario debe introducir para desbloquear su disco. Introduzca esta clave en la solicitud de desbloqueo.



Para obtener más información sobre la directiva de dispositivos de BitLocker, consulte Directiva de dispositivos de BitLocker.

Inscribir dispositivos Windows de forma masiva

Citrix Endpoint Management admite la inscripción masiva de dispositivos de escritorio y tabletas con Windows 10 y Windows 11. Con la inscripción masiva, puede configurar muchos dispositivos para que Citrix Endpoint Management los administre sin necesidad de volver a crear imágenes de los dispositivos. Utiliza el paquete de aprovisionamiento para la inscripción masiva.

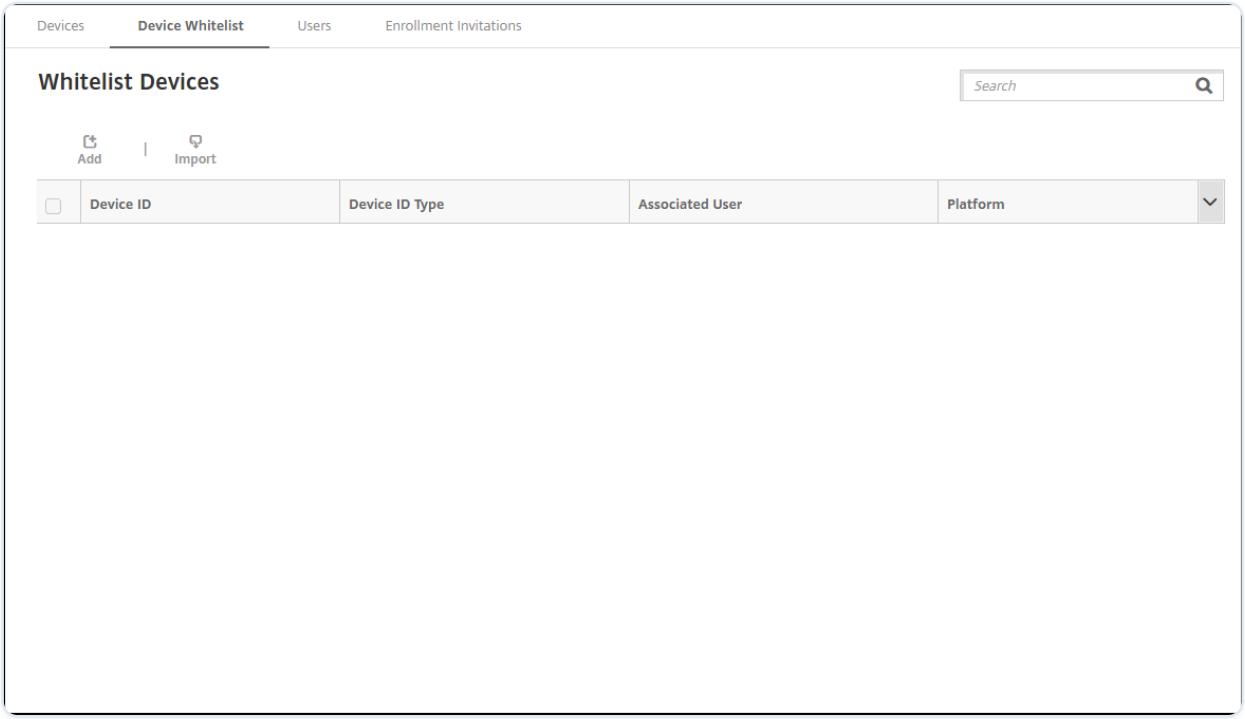
Un flujo de trabajo general para la inscripción masiva de dispositivos Windows 10 y Windows 11 es el siguiente:

1. Asignar dispositivos. Puede asignar dispositivos individualmente o de forma masiva.
2. Configurar la inscripción masiva.
3. Crear un paquete de aprovisionamiento y aplicarlo a cada dispositivo.

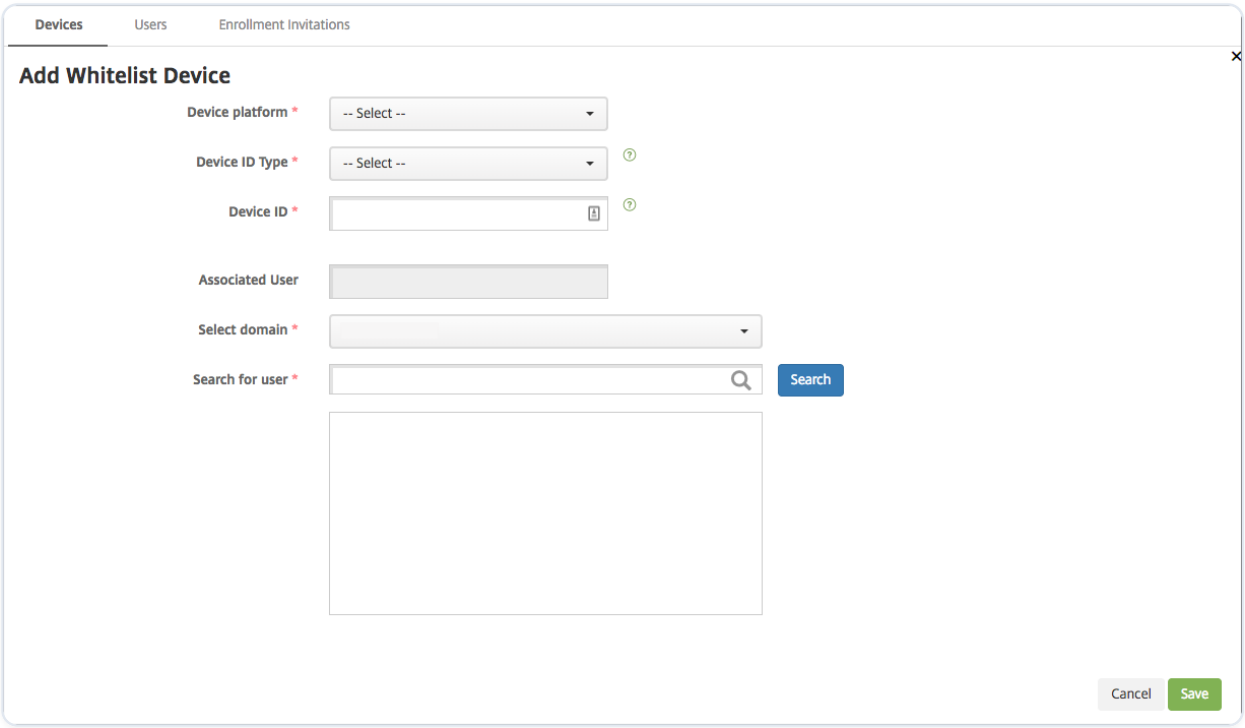
Antes de ejecutar la inscripción masiva, asegúrese de asignar todos los dispositivos a los usuarios correctos. Realice esta asignación agregando los dispositivos individualmente o de forma masiva.

Asignar dispositivos individualmente

1. En la consola de Citrix Endpoint Management, vaya a **Administrar** > **Dispositivos** > **Lista de permitidos de dispositivos**.



2. Para agregar cada dispositivo, haga clic en **Agregar**.



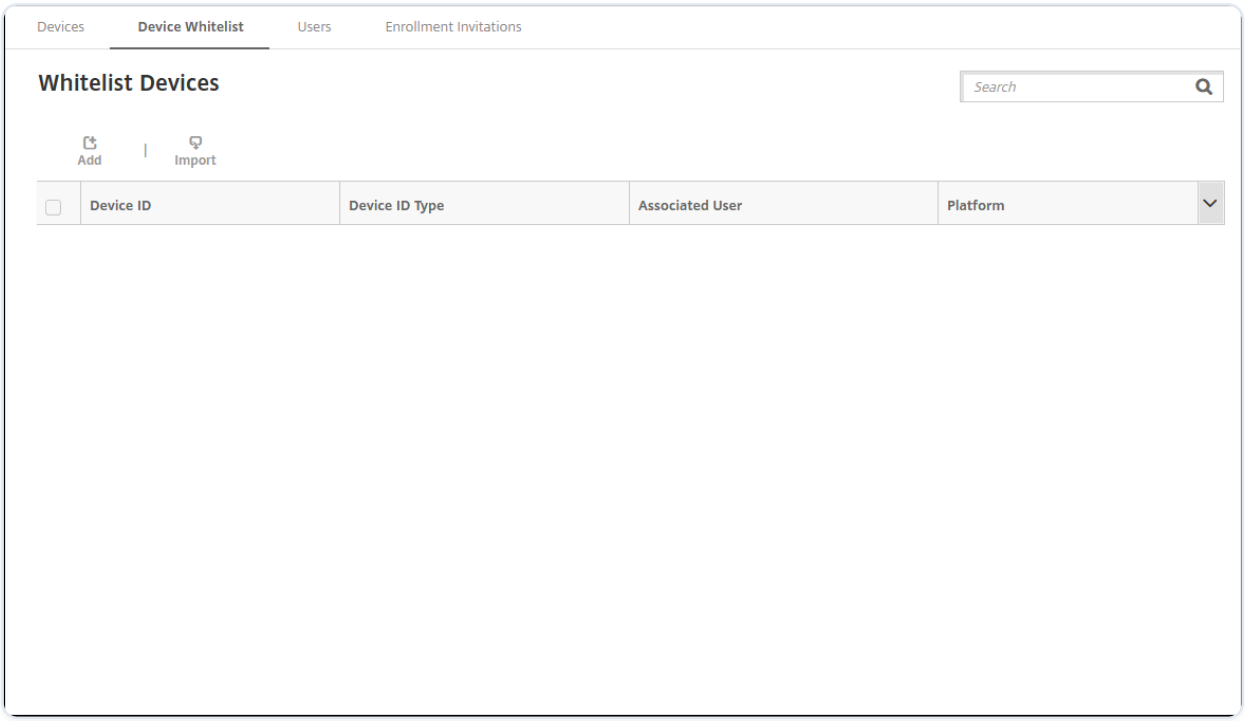
3. Escriba la siguiente información:

   - **Plataforma del dispositivo:** Seleccione **Windows**.
   - **Tipo de ID de dispositivo:** Seleccione un ID que identifique el dispositivo. Citrix Endpoint Management admite **ID de hardware** y **Nombre de dispositivo** para dispositivos Windows.
   - **ID de dispositivo:** Escriba el ID correspondiente al tipo que seleccionó previamente para el dispositivo.
   - **Usuario asociado:** Muestra el usuario asociado a este dispositivo. Este campo se rellena automáticamente con el usuario que seleccione.
   - **Seleccionar dominio:** Seleccione el dominio en el que desea buscar un usuario asociado.
   - **Buscar usuario** Escriba un nombre de usuario completo o parcial en este campo y haga clic en **Buscar** para encontrar un usuario que asociar a este dispositivo.

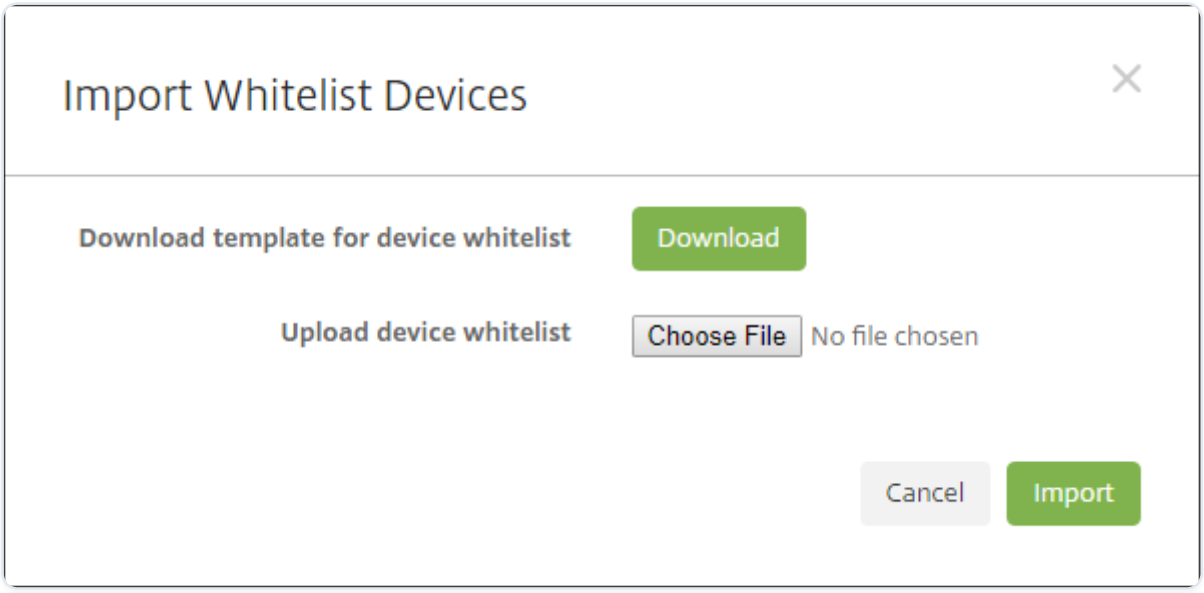
4. Haga clic en **Guardar**.

Agregar dispositivos de forma masiva

1. En la consola de Citrix Endpoint Management, vaya a **Administrar > Dispositivos > Lista de permitidos de dispositivos**.



2. Haga clic en **Importar**.

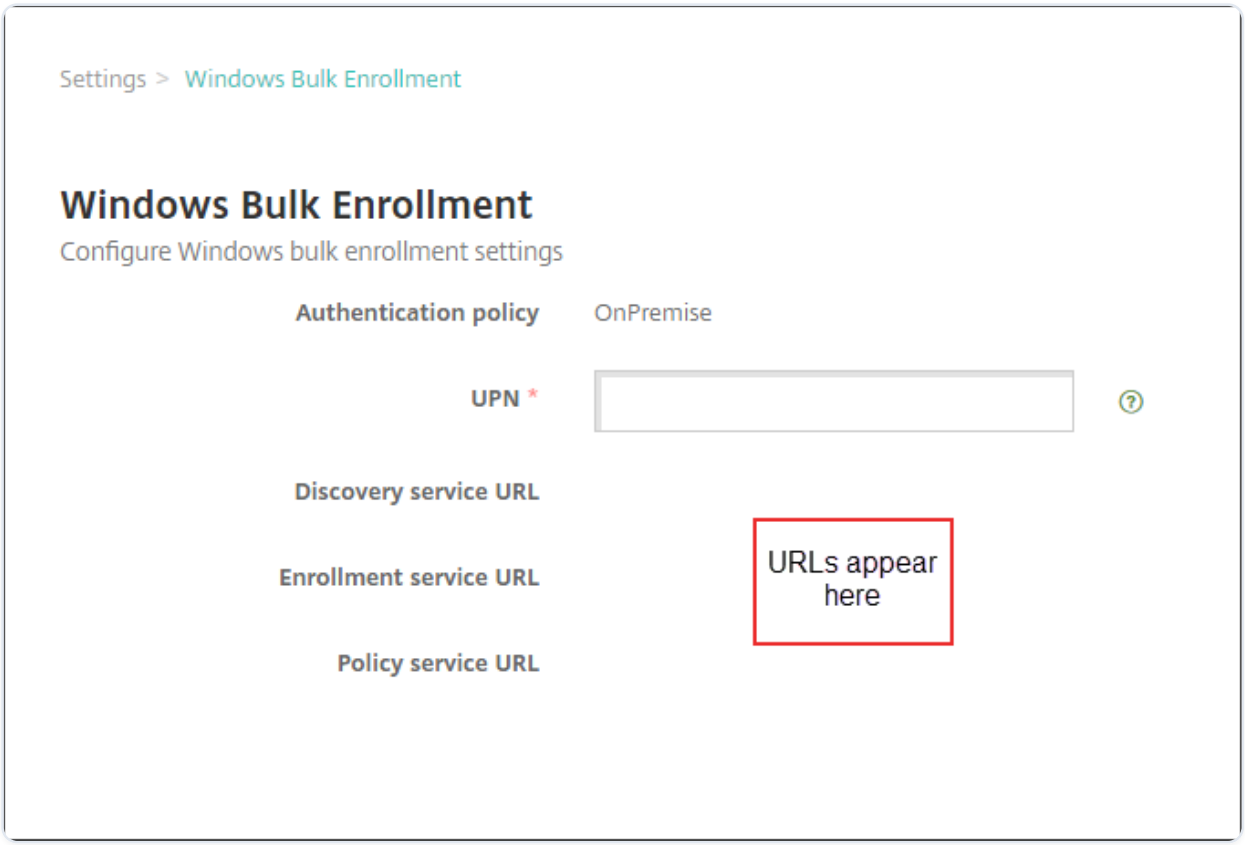


3. Haga clic en **Descargar** para descargar una plantilla (hoja de cálculo) para la lista de permitidos de dispositivos. Rellene esa hoja de cálculo y, a continuación, cárguela utilizando **Elegir archivo** e **Importar**.

Configurar la inscripción masiva

1. En la consola de Citrix Endpoint Management, vaya a **Configuración > Inscripción masiva de Windows**.
2. En el campo **UPN**, escriba un nombre de usuario a través del cual implementar todos los dispositivos. El UPN debe ser un usuario válido en Citrix Endpoint Management que tenga los

permisos de inscripción. Puede proporcionar un UPN diferente al usuario asociado que seleccionó previamente.



Necesita las URL al crear un paquete de aprovisionamiento en el Diseñador de configuración de Windows.

3. Haga clic en **Guardar**.

Crear y aplicar un paquete de aprovisionamiento

Para aprovisionar dispositivos de forma masiva, descargue el Diseñador de configuración de Windows desde Microsoft Store. El Diseñador de configuración de Windows crea paquetes de aprovisionamiento que se utilizan para crear imágenes de dispositivos. Como parte de estos paquetes, puede incluir la configuración de inscripción masiva de Citrix Endpoint Management para que los dispositivos aprovisionados se inscriban automáticamente en Citrix Endpoint Management.

Para obtener información sobre cómo usar un paquete de aprovisionamiento, consulte `<https://docs.microsoft.com/es-es/windows/client-management/mdm/bulk-enrollment-using-windows-provisioning-tool>`. Siga los pasos descritos en la sección *Crear y aplicar un paquete de aprovisionamiento para la autenticación local* de ese documento. Siga esos pasos para incluir la siguiente configuración de inscripción masiva de Citrix Endpoint Management y aplicar el paquete a cada dispositivo.

- **URL del servicio de detección**.
- **URL del servicio de inscripción**.
- **URL del servicio de directivas**.
- **Secreto**. Contraseña del UPN. Anteriormente, escribió el nombre de usuario en el campo UPN.

Inscripción masiva de dispositivos lista para usar

Citrix Endpoint Management admite la inscripción masiva de dispositivos Windows lista para usar. Siga estos pasos para configurar y realizar la inscripción masiva:

1. Utilice la consola de Citrix Endpoint Management para agregar dispositivos (individualmente o de forma masiva) y para configurar la inscripción masiva. Para obtener más información, consulte Agregar dispositivos de forma masiva y Configurar la inscripción masiva.
2. Cree un paquete de aprovisionamiento, como se describe en Crear y aplicar un paquete de aprovisionamiento.

   > **Nota:**
   >
   > Debe configurar el nombre del dispositivo para cada dispositivo al crear un paquete de aprovisionamiento. Para ello, en el Diseñador de configuración de Windows, vaya a **Runtime settings > Accounts > ComputerAccount > ComputerName** y especifique el nombre del dispositivo. El nombre de dispositivo que especifique para cada dispositivo debe coincidir con el nombre que utilizó al importar dispositivos de la lista de permitidos.

3. Coloque ese paquete de aprovisionamiento en una memoria USB.
4. Inserte la memoria USB en el dispositivo de destino la primera vez que el usuario encienda el dispositivo.

   El dispositivo Windows encuentra automáticamente el paquete de aprovisionamiento (.ppkg) en la memoria USB. Para obtener instrucciones detalladas, consulte la documentación de Microsoft sobre cómo aplicar un paquete de aprovisionamiento durante la configuración inicial.

El dispositivo se inscribe automáticamente en Citrix Endpoint Management.

Para los dispositivos que ejecutan Windows 10 (versión 2004 o posterior) o Windows 11, puede simplificar el proceso de inscripción creando un solo paquete de aprovisionamiento. El paquete se

puede aplicar a todos los dispositivos. Como resultado, ya no es necesario crear un paquete de aprovisionamiento para cada dispositivo.

Para simplificar el proceso de inscripción, siga estos pasos al crear un paquete de aprovisionamiento:

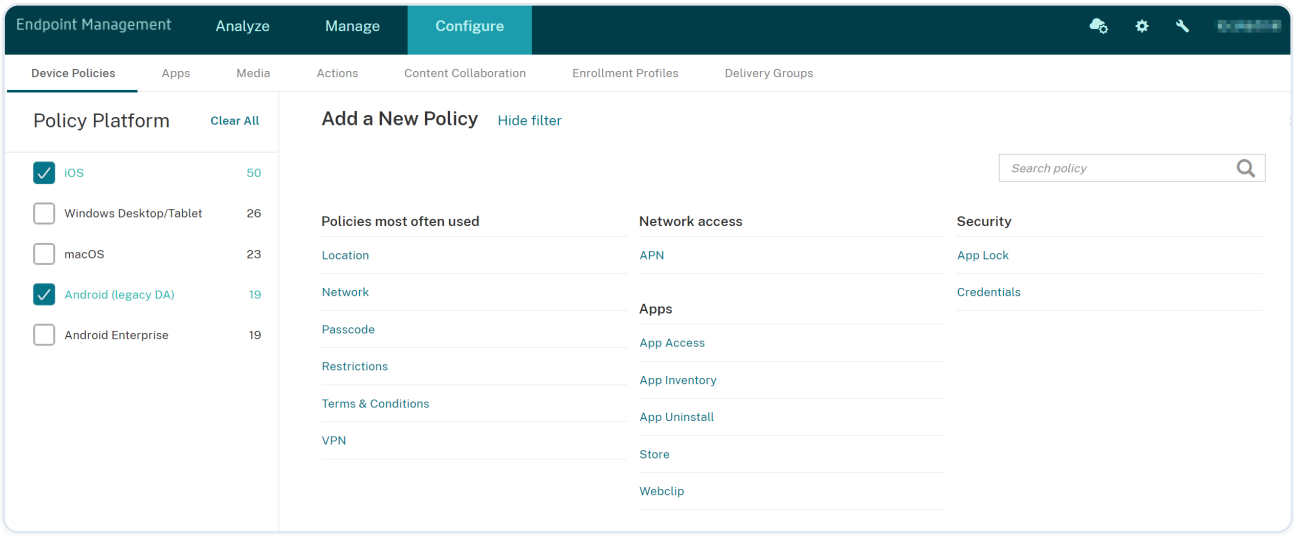
1. En Windows Configuration Designer, vaya a **Runtime settings > Accounts > ComputerAccount > ComputerName**.
2. En el campo **ComputerName**, incluya la siguiente cadena como parte del nombre del dispositivo: `%SERIAL%`. Por ejemplo: `Surface-%SERIAL%`. La cadena se expande al número de serie del BIOS de cada dispositivo.

Directivas de dispositivo

Puede configurar cómo Citrix Endpoint Management interactúa con sus dispositivos creando directivas. Aunque muchas directivas son comunes a todos los dispositivos, cada dispositivo tiene un conjunto de directivas específicas para su sistema operativo. Como resultado, puede encontrar diferencias entre plataformas, e incluso entre distintos fabricantes de dispositivos Android.

Para ver las directivas disponibles por plataforma:

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Directivas de dispositivo**.
2. Haga clic en **Agregar**.
3. Cada plataforma de dispositivo aparece en una lista en el panel **Plataforma de directivas**. Si ese panel no está abierto, haga clic en **Mostrar filtro**.
4. Para ver una lista de todas las directivas disponibles para una plataforma, seleccione esa plataforma. Para ver una lista de las directivas disponibles para varias plataformas, seleccione cada una de esas plataformas. Una directiva aparece en la lista solo si se aplica a cada plataforma seleccionada.



Para obtener una descripción resumida de cada directiva de dispositivo, consulte Resúmenes de directivas de dispositivo en este artículo.

Nota:

> Si su entorno está configurado con objetos de directiva de grupo (GPO):

> Al configurar las directivas de dispositivo de Citrix Endpoint Management para Windows 10 y Windows 11, tenga en cuenta las siguientes reglas. Si una directiva en uno o más dispositivos inscritos entra en conflicto, la directiva alineada con el GPO tiene prioridad.

> Para ver qué directivas admite el contenedor de Android Enterprise, consulte Android Enterprise.

Requisitos previos

- Cree los grupos de entrega que planea usar.
- Instale los certificados de CA necesarios.

Agregar una directiva de dispositivo

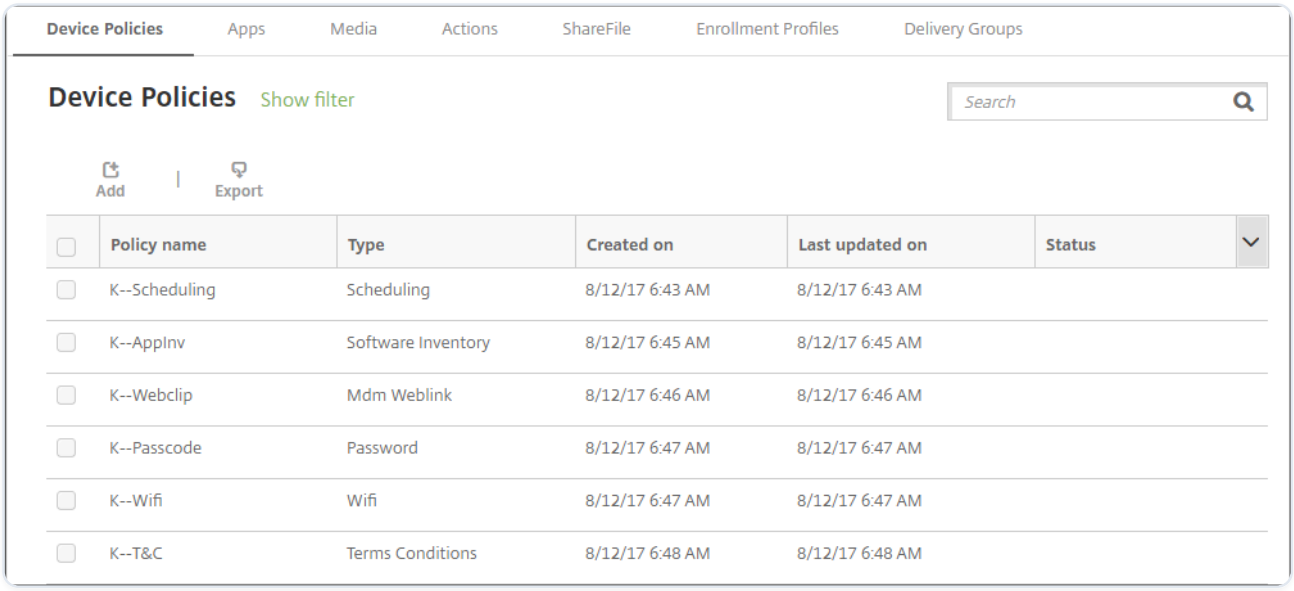
Los pasos básicos para crear una directiva de dispositivo son los siguientes:

1. Asigne un nombre y describa la directiva.

   > **Importante:**
   >
   > No utilice una barra inclinada (/) en el nombre de una directiva. Si lo hace, podría producirse un error al editar la directiva más adelante.

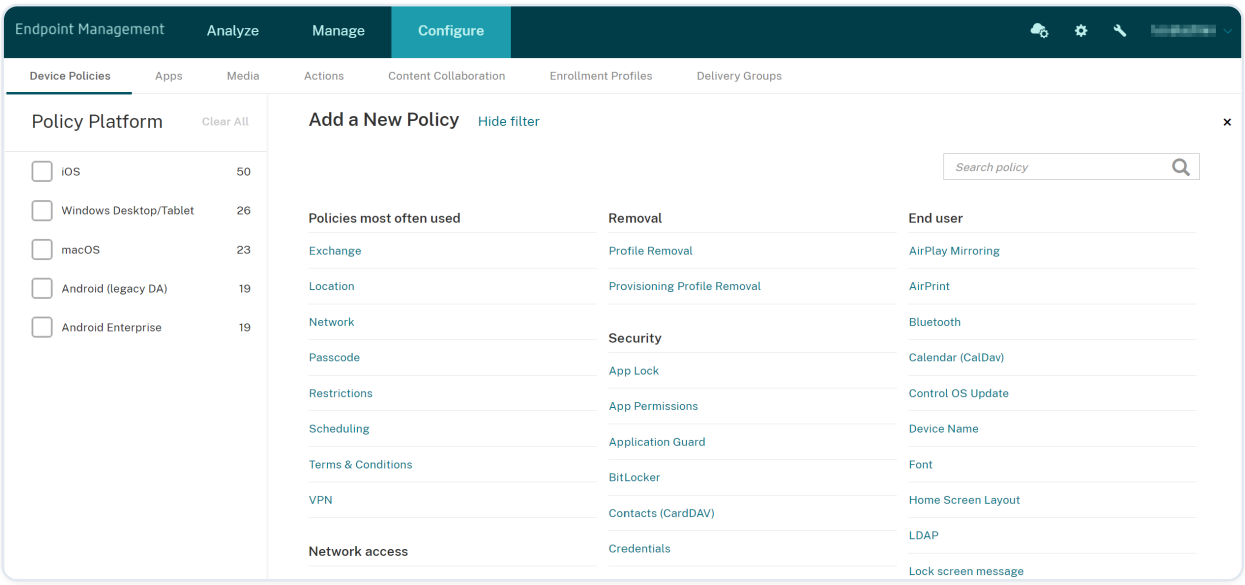
2. Configure la directiva para una o varias plataformas.
3. Cree reglas de implementación (opcional).
4. Asigne la directiva a grupos de entrega.
5. Configure la programación de la implementación (opcional).

Para crear y administrar directivas de dispositivo, vaya a **Configurar > Directivas de dispositivo**.

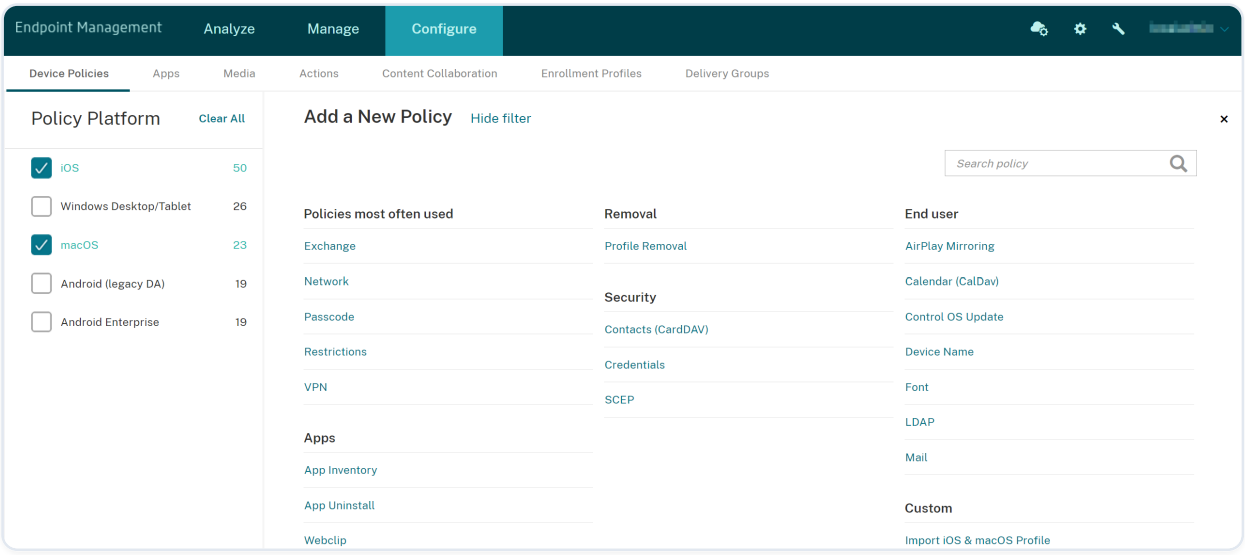


Para agregar una directiva:

1. En la página **Directivas de dispositivo**, haga clic en **Agregar**. Aparece la página **Agregar una nueva directiva**.



2. Haga clic en una o varias plataformas para ver una lista de las directivas de dispositivo para las plataformas seleccionadas. Haga clic en el nombre de una directiva para continuar con la adición de la directiva.



También puede escribir el nombre de la directiva en el cuadro de búsqueda. A medida que escribe, aparecen posibles coincidencias. Si su directiva está en la lista, haga clic en ella. Solo su directiva seleccionada permanece en los resultados. Haga clic en ella para abrir la página **Información de la directiva** de esa directiva.

3. Seleccione las plataformas que desea incluir en la directiva. Las páginas de configuración de las plataformas seleccionadas aparecen en el paso 5.
4. Complete la página **Información de la directiva** y, a continuación, haga clic en **Siguiente**. La página **Información de la directiva** recopila información, como el nombre de la directiva, para ayudarle a identificar y realizar un seguimiento de sus directivas. Esta página es similar para todas las directivas.
5. Complete las páginas de la plataforma. Las páginas de la plataforma aparecen para cada plataforma que seleccionó en el paso 3. Estas páginas son diferentes para cada directiva. Una directiva puede diferir entre plataformas. No todas las directivas se aplican a todas las plataformas.

   Algunas páginas incluyen tablas de elementos. Para eliminar un elemento existente, coloque el cursor sobre la línea que contiene el listado y haga clic en el icono de la papelera en el lado derecho. En el cuadro de diálogo de confirmación, haga clic en **Eliminar**.

   Para modificar un elemento existente, coloque el cursor sobre la línea que contiene el listado y haga clic en el icono del lápiz en el lado derecho.

Para configurar reglas de implementación, asignaciones y programación

Para obtener más información sobre la configuración de reglas de implementación, consulte Implementar recursos.

1. En una página de plataforma, expanda **Reglas de implementación** y, a continuación, configure los siguientes parámetros. La ficha **Base** aparece de forma predeterminada.

    - En las listas, haga clic en las opciones para especificar las condiciones de implementación. Puede elegir implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla alguna condición. La opción predeterminada se establece como **Todas**.
    - Haga clic en **Nueva regla** para definir las condiciones.
    - En las listas, haga clic en las condiciones, como **Propiedad del dispositivo** y **BYOD**.
    - Haga clic en **Nueva regla** de nuevo si desea agregar más condiciones. Puede agregar tantas condiciones como desee.

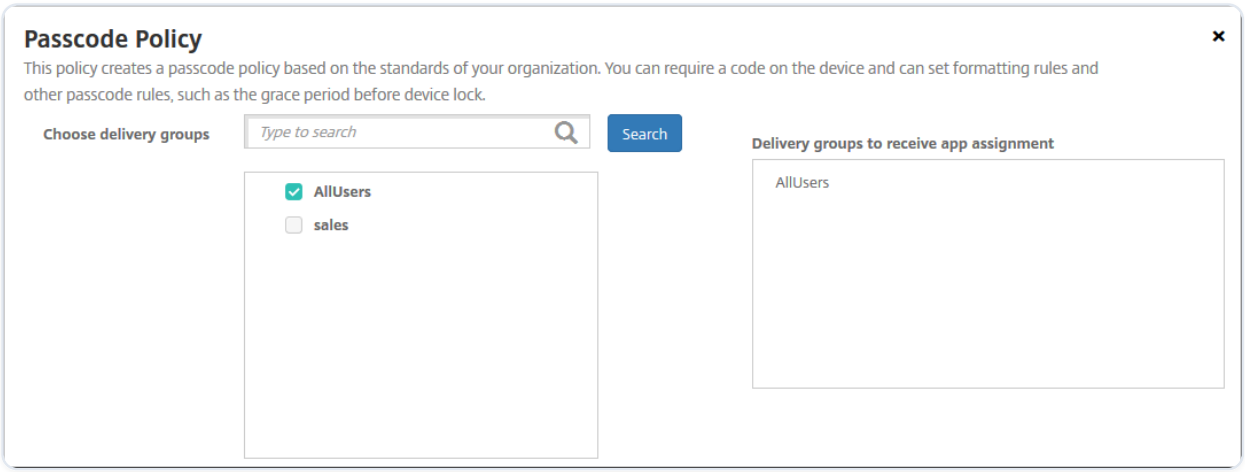
2. Haga clic en la ficha **Avanzado** para combinar las reglas con opciones booleanas. Aparecen las condiciones que eligió en la ficha **Básico**.
3. Puede usar una lógica booleana más avanzada para combinar, modificar o agregar reglas.

    - Haga clic en **AND**, **OR** o **NOT**.
    - En las listas, elija las condiciones que quiere agregar a la regla. A continuación, haga clic en el signo Más (**+**) del lado derecho para agregar la condición a la regla.

      En cualquier momento, puede hacer clic para seleccionar una condición y, a continuación, hacer clic en **EDITAR** o **Eliminar**.
    - Haga clic en **Nueva regla** para agregar otra condición.

4. Haga clic en **Siguiente** para ir a la siguiente página de la plataforma o, cuando todas las páginas de la plataforma estén completas, a la página **Asignaciones**.
5. En la página **Asignaciones**, seleccione los grupos de entrega a los que quiere aplicar la directiva. Si hace clic en un grupo de entrega, el grupo aparece en el cuadro **Grupos de entrega para recibir la asignación de aplicaciones**.

    El cuadro **Grupos de entrega para recibir la asignación de aplicaciones** no aparece hasta que seleccione un grupo de entrega.

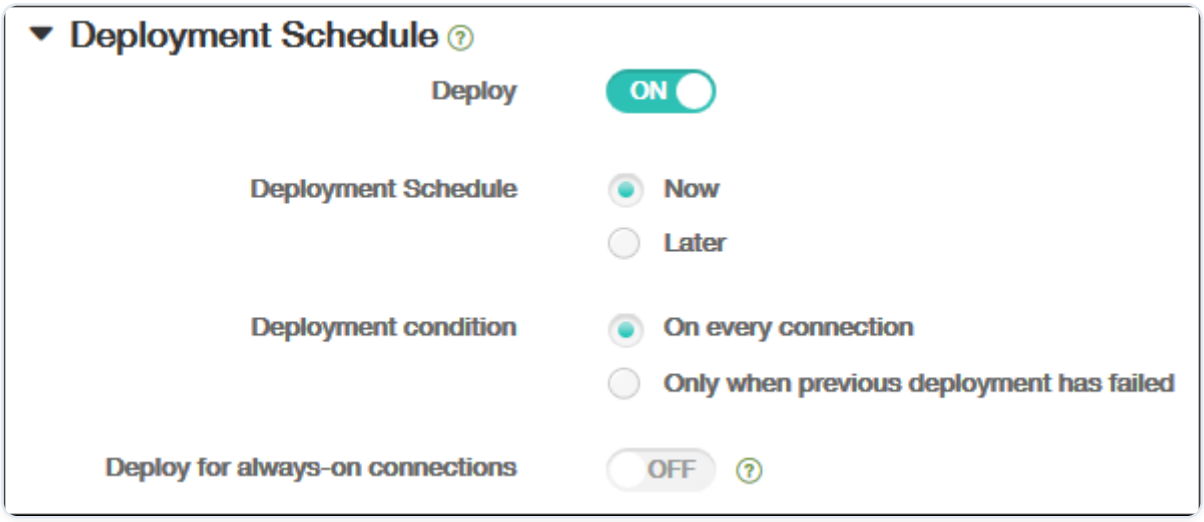


6. En la página **Asignaciones**, expanda **Programación de implementación** y, a continuación, configure los siguientes parámetros:

   - Junto a **Implementar**, haga clic en **Activado** para programar la implementación o en **Desactivado** para evitar la implementación. La opción predeterminada está establecida en **Activado**.
   - Junto a **Programación de implementación**, haga clic en **Ahora** o en **Más tarde**. La opción predeterminada está establecida en **Ahora**.
   - Si hace clic en **Más tarde**, haga clic en el icono del calendario y, a continuación, seleccione la fecha y la hora de la implementación.
   - Junto a **Condición de implementación**, haga clic en **En cada conexión** o en **Solo cuando la implementación anterior haya fallado**. La opción predeterminada está establecida en **En cada conexión**.
   - Junto a **Implementar para conexión siempre activa**, haga clic en **Activado** o **Desactivado**. La opción predeterminada está establecida en **Desactivado**.

     > **Nota:**
     >
     > Esta opción se aplica cuando ha configurado la clave de implementación en segundo plano de programación en **Parámetros > Propiedades del servidor**.
     >
     > La opción de conexión siempre activa:
     >
     > - No está disponible para dispositivos iOS

- No está disponible para clientes de Android y Android Enterprise que empezaron a usar Citrix Endpoint Management con la versión 10.18.19 o posterior
- No se recomienda para clientes de Android y Android Enterprise que empezaron a usar Citrix Endpoint Management antes de la versión 10.18.19 El programa de implementación que configure es el mismo para todas las plataformas. Cualquier cambio que realice se aplica a todas las plataformas, excepto a **Implementar para conexión siempre activa**.



7. Haga clic en **Guardar**.

   La directiva aparece en la tabla **Directivas de dispositivo**.

Eliminar una directiva de dispositivo de un dispositivo

Los pasos para eliminar una directiva de dispositivo de un dispositivo dependen de la plataforma.

- Android

  Para eliminar una directiva de dispositivo de un dispositivo Android, utilice la directiva de dispositivo de desinstalación de Citrix Endpoint Management. Para obtener más información, consulte Directiva de dispositivo de desinstalación de Citrix Endpoint Management.

- iOS y macOS

  Para quitar una directiva de dispositivo de un dispositivo iOS o macOS, utilice la directiva de dispositivo de eliminación de perfiles. En los dispositivos iOS y macOS, todas las directivas forman parte del perfil MDM. Por lo tanto, puede crear una directiva de dispositivo de eliminación de perfiles solo para la directiva que desea quitar. El resto de las directivas y el

perfil permanecen en el dispositivo. Para obtener más información, consulte Directiva de dispositivo de eliminación de perfiles.

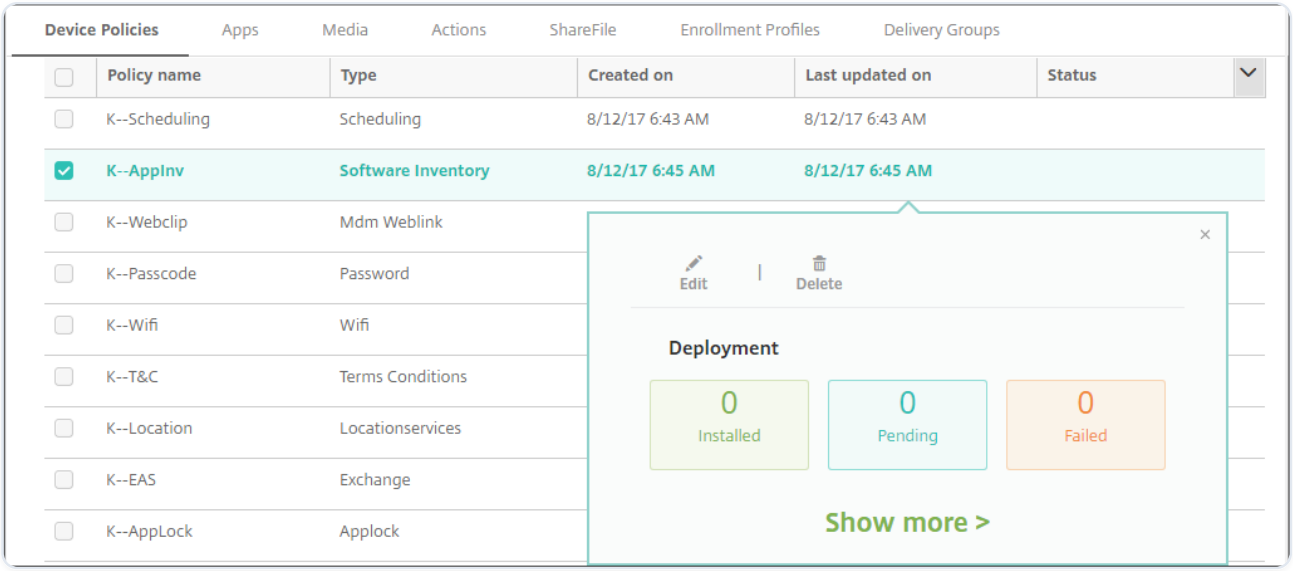
- Windows 10 y Windows 11

  No puede quitar directamente una directiva de dispositivo de un dispositivo Windows de escritorio o tableta. Sin embargo, puede utilizar cualquiera de los siguientes métodos:

  - Anule la inscripción del dispositivo y, a continuación, envíe un nuevo conjunto de directivas al dispositivo. Los usuarios se vuelven a inscribir para continuar.
  - Envíe una acción de seguridad para borrar selectivamente el dispositivo específico. Esa acción elimina todas las aplicaciones y datos corporativos del dispositivo. A continuación, quite la directiva de dispositivo de un grupo de entrega que solo tenga ese dispositivo y envíe el grupo de entrega al dispositivo. Los usuarios se vuelven a inscribir para continuar.

Modificar una directiva de dispositivo

Para modificar una directiva, marque la casilla situada junto a ella. El menú de opciones aparece encima de la lista de directivas. O bien, haga clic en una directiva de la lista para mostrar más controles.



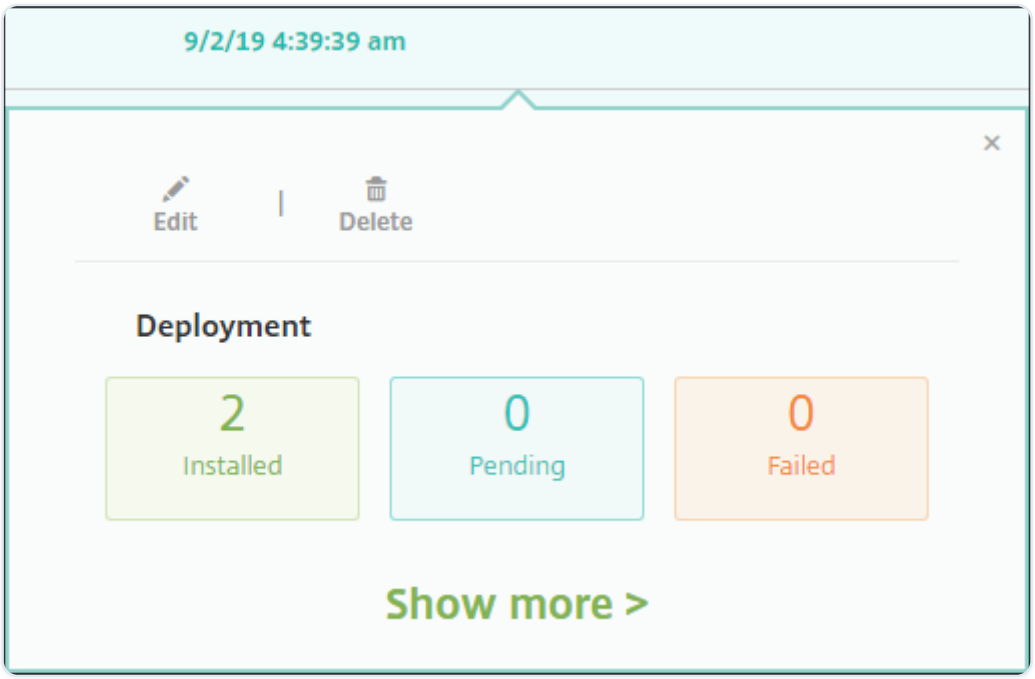
Para ver los detalles de la directiva, haga clic en **Mostrar más**.

Para modificar todos los parámetros de una directiva de dispositivo, haga clic en **Modificar**.

Si hace clic en **Eliminar**, aparece un cuadro de diálogo de confirmación. Haga clic en **Eliminar** de nuevo para eliminar la directiva.

Comprobar el estado de implementación de la directiva

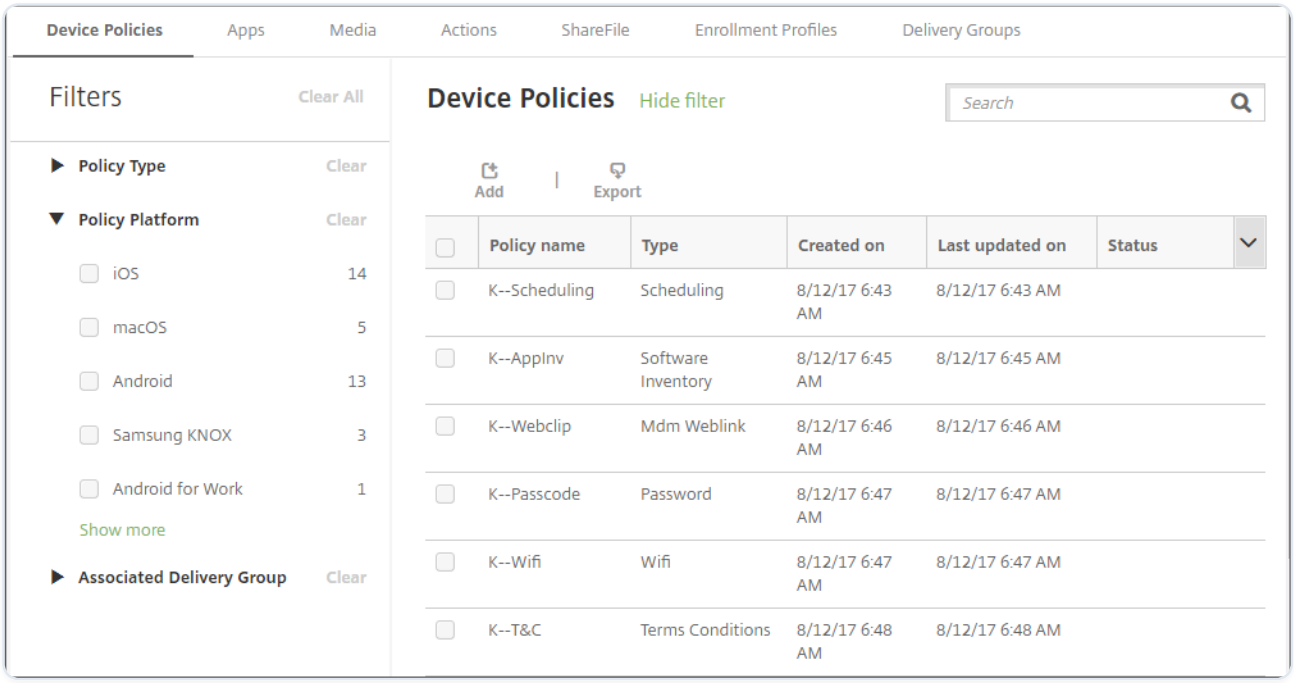
Haga clic en una fila de directivas en la página **Configurar > Directivas de dispositivo** para comprobar su estado de implementación.



Cuando una implementación de política está pendiente, los usuarios pueden actualizar la política desde Citrix Secure Hub tocando **Preferencias > Información del dispositivo > Actualizar política**.

Filtrar la lista de directivas de dispositivo añadidas

Puede filtrar la lista de directivas añadidas por tipos de directiva, plataformas y grupos de entrega asociados. En la página **Configurar > Directivas de dispositivo**, haga clic en **Mostrar filtro**. En la lista, seleccione las casillas de verificación de los elementos que desea ver.



Haga clic en **GUARDAR ESTA VISTA** para guardar un filtro. El nombre del filtro aparece entonces en un botón debajo del botón **GUARDAR ESTA VISTA**.

Resúmenes de directivas de dispositivo

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
AirPlay Mirroring	Añade dispositivos AirPlay específicos (como Apple TV u otro equipo Mac) a los dispositivos iOS. También puede añadir dispositivos a una lista de permitidos para dispositivos supervisados. Esa opción limita a los usuarios únicamente a los dispositivos AirPlay de la lista de permitidos.
AirPrint	Añade impresoras AirPrint a la lista de impresoras AirPrint en dispositivos iOS. Esta directiva facilita la compatibilidad con entornos donde las impresoras y los dispositivos están en subredes diferentes.
APN	Determina la configuración utilizada para conectar sus dispositivos al Servicio General de Radio por Paquetes (GPRS) de un operador de telefonía específico. Esta configuración ya está definida en la mayoría

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
	de los teléfonos nuevos. Utilice esta directiva si su organización no utiliza un APN de consumidor para conectarse a Internet desde un dispositivo móvil.
Acceso a aplicaciones	Define una lista de las aplicaciones que son obligatorias, opcionales o que están prohibidas en el dispositivo. A continuación, puede crear una acción automatizada para reaccionar ante el cumplimiento del dispositivo con esa lista de aplicaciones.
Atributos de la aplicación	Especifica atributos, como un ID de paquete de aplicación administrada o un identificador VPN por aplicación, para dispositivos iOS.
Configuración de la aplicación	Configura de forma remota varias opciones y comportamientos de las aplicaciones que admiten la configuración administrada. Para ello, implementa un archivo de configuración XML (denominado lista de propiedades o `plist`) en dispositivos iOS. O bien, implementa pares clave/valor en dispositivos de escritorio o tabletas con Windows 10.
Inventario de aplicaciones	Recopila un inventario de las aplicaciones en los dispositivos administrados. Citrix Endpoint Management compara el inventario con las directivas de acceso a aplicaciones implementadas en esos dispositivos. De este modo, puede detectar las aplicaciones que están en una lista de permitidas o bloqueadas para el acceso a aplicaciones y, a continuación, actuar correctamente.
Bloqueo de apps	Define una lista de aplicaciones que los usuarios pueden o no pueden ejecutar en dispositivos iOS o en determinados dispositivos Android. Puede convertir un iPad en un quiosco.

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
Permisos de la aplicación	Configura cómo las solicitudes a las aplicaciones de Android Enterprise dentro de los perfiles de trabajo gestionan lo que Google denomina permisos “peligrosos”.
Desinstalación de aplicaciones	Elimina aplicaciones de los dispositivos de los usuarios.
Restricciones de desinstalación de aplicaciones	Especifica las aplicaciones que los usuarios pueden o no pueden desinstalar.
Application Guard	Solo para el navegador Microsoft Edge, esta directiva especifica la configuración de Windows Defender Application Guard. La configuración incluye si se debe bloquear el contenido externo en los sitios empresariales.
Notificaciones de aplicaciones	Controla cómo los usuarios de iOS reciben notificaciones de aplicaciones específicas.
Actualizar automáticamente las aplicaciones administradas	Controla cómo se actualizan las aplicaciones administradas instaladas en dispositivos Android Enterprise.
BitLocker	Configura los ajustes disponibles en la interfaz de BitLocker en dispositivos Windows 10 y Windows 11.
Bluetooth	Habilita o deshabilita Bluetooth en dispositivos iOS.
Navegador	Define si los dispositivos de los usuarios pueden usar el navegador o qué funciones del navegador pueden usar los dispositivos.
Calendario (CalDAV)	Agrega una cuenta de calendario (CalDAV) a dispositivos iOS o macOS. La cuenta CalDAV permite a los usuarios sincronizar datos de programación con cualquier servidor que admita CalDAV.

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
Datos móviles	Configura los ajustes de la red móvil.
Programación de la conexión	Necesario para que los dispositivos Android se conecten a Citrix Endpoint Management para la administración de MDM, el envío de aplicaciones y la implementación de directivas. Si no envía esta directiva a los dispositivos y no habilita Google FCM, un dispositivo no podrá volver a conectarse al servidor.
Contactos (CardDAV)	Agrega una cuenta de contactos (CardDAV) de iOS a dispositivos iOS o macOS. La cuenta de CardDAV permite a los usuarios sincronizar datos de contactos con cualquier servidor compatible con CardDAV.
Credenciales	Permite la autenticación integrada con su configuración de PKI en Citrix Endpoint Management. Por ejemplo, con una entidad PKI, un almacén de claves, un proveedor de credenciales o un certificado de servidor.
XML personalizado	Personaliza funciones como el aprovisionamiento de dispositivos, la habilitación de funciones de dispositivos, la configuración de dispositivos y la gestión de fallos.
Defender	Configura los ajustes de Windows Defender para Windows 10 y Windows 11 para equipos de escritorio y tabletas.
Device Guard	Habilita funciones de seguridad como el arranque seguro, el bloqueo UEFI y la virtualización.
Atestación de estado del dispositivo	Requiere que los dispositivos Windows 10 y Windows 11 informen sobre su estado de salud. Para ello, envían datos específicos e información de tiempo de ejecución al Servicio

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
	de atestación de estado (HAS) para su análisis. El HAS crea y devuelve un Certificado de atestación de estado que el dispositivo envía a Citrix Endpoint Management. Cuando Citrix Endpoint Management recibe el Certificado de atestación de estado, basándose en el contenido de dicho certificado, puede implementar las acciones automáticas que haya configurado.
Nombre del dispositivo	Establece los nombres en los dispositivos iOS y macOS para que pueda identificar los dispositivos. Puede usar macros, texto o una combinación de ambos para definir un nombre de dispositivo.
Configuración de educación	Configura los dispositivos de profesores y alumnos para su uso con Apple Education. Si los profesores utilizan la aplicación Classroom, se requiere la directiva de dispositivo Configuración de educación. Compatible con dispositivos iOS (iPadOS).
Opciones de Citrix Endpoint Management	Configura el comportamiento de Citrix Secure Hub al conectarse a Citrix Endpoint Management desde dispositivos Android.
Desinstalación de Citrix Endpoint Management	Desinstala Citrix Endpoint Management de los dispositivos Android. Cuando se implementa, esta directiva elimina Citrix Endpoint Management de todos los dispositivos del grupo de implementación.
Exchange	Habilita el correo electrónico de ActiveSync para el cliente de correo electrónico nativo del dispositivo.
Archivos	Agrega archivos de script a Citrix Endpoint Management que realizan ciertas funciones para los usuarios. O bien, puede agregar archivos de documentos a los que los usuarios

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
	de dispositivos Android quieran acceder en sus dispositivos. Al agregar el archivo, también puede especificar el directorio en el que desea que se almacene el archivo en el dispositivo.
FileVault	Esta directiva le permite habilitar el cifrado de dispositivos FileVault en dispositivos macOS inscritos. También puede controlar cuántas veces un usuario puede omitir la configuración de FileVault durante el inicio de sesión. Disponible para macOS 10.7 o posterior.
Firewall	Configura los ajustes del firewall. Proporciona las direcciones IP, los puertos y los nombres de host que desea permitir o bloquear en los dispositivos. También puede configurar los ajustes de proxy y de redireccionamiento de proxy.
Fuente	Agrega fuentes a dispositivos iOS y macOS. Las fuentes deben ser TrueType (.TTF) u OpenType (.OFT). Citrix Endpoint Management no admite colecciones de fuentes (.TTC, .OTC).
Diseño de la pantalla de inicio	Especifica el diseño de las aplicaciones y carpetas para la pantalla de inicio de iOS en dispositivos iOS supervisados.
Importar perfil de iOS y macOS	Importa archivos XML de configuración de dispositivos para iOS y macOS en Citrix Endpoint Management. El archivo contiene directivas de seguridad y restricciones de dispositivos que se preparan con Apple Configurator.
Administración de Keyguard	Controla las funciones disponibles para los usuarios antes de que desbloqueen el keyguard del dispositivo y el keyguard de desafío de trabajo. También puede controlar las funciones del keyguard del dispositivo para

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
	dispositivos totalmente administrados y dedicados. Por ejemplo, puede deshabilitar las funciones de la pantalla de bloqueo, como el desbloqueo por huella dactilar, los agentes de confianza y las notificaciones.
Clave de Knox Platform for Enterprise	Le permite proporcionar la información de licencia necesaria de Samsung Knox Platform for Enterprise (KPE).
Configuración del iniciador	Especifica la configuración de Citrix Launcher en dispositivos Android, como las aplicaciones permitidas y una imagen de logotipo personalizada para el icono de Launcher.
LDAP	Proporciona información sobre un servidor LDAP para usar con dispositivos iOS, incluida cualquier información de cuenta necesaria, como el nombre de host del servidor LDAP. La directiva también proporciona un conjunto de directivas de búsqueda LDAP para usar al consultar el servidor LDAP.
Ubicación	Permite geolocalizar dispositivos en un mapa, asumiendo que el dispositivo tiene el GPS habilitado para Citrix Secure Hub. Después de implementar esta directiva en el dispositivo, puede enviar un comando de localización desde Citrix Endpoint Management. El dispositivo responde entonces con sus coordenadas de ubicación. Citrix Endpoint Management también admite directivas de geocercado y seguimiento.
Mensaje de la pantalla de bloqueo	Establece mensajes para que aparezcan en los siguientes dispositivos cuando se pierdan: La ventana de inicio de sesión de los iPad compartidos y la pantalla de bloqueo de los dispositivos iOS supervisados.

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
Correo	Configura una cuenta de correo electrónico en dispositivos iOS o macOS.
Configuraciones administradas	Controla varias opciones de configuración de aplicaciones y restricciones de aplicaciones para dispositivos Android Enterprise.
Dominios administrados	Define dominios administrados que se aplican al correo electrónico y al navegador Safari. Los dominios administrados le ayudan a proteger los datos corporativos controlando qué aplicaciones pueden abrir documentos descargados de dominios mediante Safari. Para los dispositivos iOS supervisados, puede especificar URL o subdominios para controlar cómo los usuarios pueden abrir documentos, archivos adjuntos y descargas desde el navegador.
Número máximo de usuarios residentes	Especifica el número máximo de usuarios para un iPad compartido. Compatible con dispositivos iOS y iPadOS.
Opciones de MDM	Administra Buscar mi iPhone y el Bloqueo de activación de iPad en dispositivos iOS supervisados.
Red	Permite a los administradores implementar los detalles del router Wi-Fi en los dispositivos administrados. Los detalles del router incluyen SSID, datos de autenticación y datos de configuración.
Uso de la red	Establece reglas de uso de la red para especificar cómo las aplicaciones administradas utilizan las redes, como las redes de datos móviles, en dispositivos iOS. Las reglas solo se aplican a las aplicaciones administradas. Las aplicaciones administradas son aplicaciones que se implementan en los

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
	dispositivos de los usuarios a través de Citrix Endpoint Management.
Office	Implementa aplicaciones de Microsoft Office en cualquier dispositivo que ejecute Windows 10 (versión 1709 o posterior) o Windows 11.
Información de la organización	Especifica la información de la organización para los mensajes de alerta que Citrix Endpoint Management implementa en los dispositivos iOS.
Actualización del SO	Implementa las últimas actualizaciones del SO en los dispositivos compatibles y supervisados.
Código de acceso	Aplica un código PIN o una contraseña en un dispositivo administrado. Puede establecer la complejidad y los tiempos de espera para el código de acceso en el dispositivo.
Período de gracia del bloqueo por código de acceso	Especifica el número de minutos que la pantalla de un iPad compartido permanece bloqueada antes de que el usuario deba introducir un código de acceso para desbloquearla. Compatible con dispositivos iOS y iPadOS.
Punto de acceso personal	Permite a los usuarios conectarse a Internet cuando no están dentro del alcance de una red Wi-Fi. Los usuarios se conectan a través de la conexión de datos móviles de su dispositivo iOS, utilizando la funcionalidad de punto de acceso personal.
Eliminación de perfil	Elimina el perfil de la aplicación de los dispositivos macOS.
Perfil de aprovisionamiento	Especifica un perfil de aprovisionamiento de distribución empresarial para enviar a los dispositivos. Al desarrollar y firmar con código

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
	una aplicación empresarial de iOS, normalmente se incluye un perfil de aprovisionamiento. Apple requiere el perfil para que la aplicación se ejecute en un dispositivo iOS. Si falta un perfil de aprovisionamiento o ha caducado, la aplicación se bloquea cuando un usuario toca para abrirla.
Eliminación de perfil de aprovisionamiento	Elimina los perfiles de aprovisionamiento de iOS.
Proxy	Especifica la configuración global del proxy HTTP para los dispositivos que ejecutan iOS. Solo puede implementar una directiva de proxy HTTP global por dispositivo.
Restricciones	Ofrece cientos de opciones para bloquear y controlar las funciones y características de los dispositivos administrados. Ejemplos de opciones de restricción: Deshabilitar la cámara o el micrófono, aplicar reglas de itinerancia y aplicar el acceso a servicios de terceros, como las tiendas de aplicaciones.
Itinerancia	Configura si se permite la itinerancia de voz y datos en dispositivos iOS. Si la itinerancia de voz está deshabilitada, la itinerancia de datos se deshabilita automáticamente.
Clave de licencia MDM de Samsung	Especifica la clave integrada de Samsung Enterprise License Management (ELM) que debe implementar en un dispositivo. Citrix Endpoint Management también es compatible con el servicio Samsung Enterprise Firmware-Over-The-Air (E-FOTA).
SCEP	Configura dispositivos iOS y macOS para recuperar un certificado de un servidor SCEP externo. También puede entregar un certificado al dispositivo mediante SCEP desde una PKI conectada a Citrix Endpoint

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
	Management. Para ello, cree una entidad PKI y un proveedor PKI en modo distribuido.
Cuenta de inicio de sesión único (SSO)	Crea cuentas de SSO para que los usuarios inicien sesión una sola vez para acceder a Citrix Endpoint Management y a los recursos internos de su empresa. Los usuarios no necesitan almacenar ninguna credencial en el dispositivo. Citrix Endpoint Management utiliza las credenciales de usuario empresarial para una cuenta SSO en todas las aplicaciones, incluidas las de App Store. Esta directiva es compatible con la autenticación Kerberos. Disponible para iOS.
Cifrado de almacenamiento	Cifra el almacenamiento interno y externo. Para algunos dispositivos, esta directiva impide que los usuarios utilicen una tarjeta de almacenamiento en sus dispositivos.
Tienda	Especifica si un clip web de la tienda de aplicaciones aparece en la pantalla de inicio de los dispositivos de los usuarios.
Calendarios suscritos	Agrega un calendario suscrito a la lista de calendarios en dispositivos iOS. Asegúrese de suscribirse a un calendario antes de agregarlo a la lista de calendarios suscritos en los dispositivos de los usuarios.
Términos y condiciones	Requiere que los usuarios acepten las directivas específicas de su empresa que rigen las conexiones a la red corporativa. Cuando los usuarios inscriben sus dispositivos en Citrix Endpoint Management, deben aceptar los términos y condiciones para inscribir sus dispositivos. Rechazar los términos y condiciones cancela el proceso de inscripción.

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
Túnel	Define los parámetros de proxy entre el componente cliente de cualquier aplicación de dispositivo móvil y el componente de servidor de la aplicación.
VPN	Proporciona acceso a sistemas back-end que utilizan tecnología de puerta de enlace VPN heredada. Esta directiva proporciona detalles de conexión de puerta de enlace VPN que puede implementar en los dispositivos. Citrix Endpoint Management admite varios proveedores de VPN, incluidos Cisco AnyConnect, Juniper y Citrix VPN. Si su puerta de enlace VPN admite esta opción, puede vincular esta directiva a una CA y habilitar la VPN a petición.
Fondo de pantalla	Agrega un archivo .png o .jpg para establecer el fondo de pantalla en la pantalla de bloqueo, la pantalla de inicio o ambas de un dispositivo iOS. Para usar un fondo de pantalla diferente en iPads y iPhones, cree diferentes directivas de fondo de pantalla e impleméntelas en los usuarios adecuados.
Clip web	Coloca accesos directos, o clips web, a sitios web para que aparezcan junto a las aplicaciones en los dispositivos de los usuarios. Puede especificar sus propios iconos para representar los clips web en dispositivos iOS, macOS y Android. Las tabletas Windows solo requieren una etiqueta y una URL.
Filtro de contenido web	Filtra el contenido web en dispositivos iOS. Citrix Endpoint Management utiliza la función de filtro automático de Apple y los sitios que usted agrega a las listas de permitidos y bloqueados. Disponible solo para dispositivos iOS supervisados.

NOMBRE DE LA DIRECTIVA DE DISPOSITIVO	DESCRIPCIÓN DE LA DIRECTIVA DE DISPOSITIVO
Agente de Windows	Habilite esta directiva para ejecutar scripts de PowerShell cargados en equipos de escritorio y tabletas Windows.
Configuración de GPO de Windows	Configure objetos de directiva de grupo (GPO) para cualquier dispositivo Windows compatible con Citrix Workspace Environment Management.
Windows Hello para empresas	Habilite la función de Windows para que los usuarios puedan aprovisionar Windows Hello para empresas en su dispositivo. La directiva también le permite configurar limitaciones de código de acceso y otras funciones de seguridad.

Directivas de dispositivo por plataforma

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
Directiva de dispositivo de duplicación de AirPlay	X	X				
Directiva de dispositivo de AirPrint	X					

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
Directiva de dispositivo de APN	X			X		
Directiva de dispositivo de acceso a aplicaciones	X			X		
Directiva de dispositivo de atributos de aplicación	X					
Directiva de dispositivo de configuración de aplicación	X				X	
Directiva de dispositivo de inventario de aplicaciones	X	X	X	X	X	

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
Directiva de dispositivo de bloqueo de aplicaciones	X			X	X	
Directiva de dispositivo de permisos de aplicaciones			X			
Directiva de dispositivo de desinstalación de aplicaciones	X	X	X	X		
Directiva de dispositivo de restricciones de desinstalación de aplicaciones						X

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
Directiva de dispositivo de Application Guard					X	
Directiva de dispositivo de notificaciones de aplicaciones	X					
Actualizar automáticamente las aplicaciones administradas			X			
Directiva de dispositivo BitLocker					X	
Directiva de dispositivo Bluetooth	X					

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
Directiva de dispositivo de explorador						X
Directiva de dispositivo de calendario (CalDav)	X	X				
Directiva de dispositivo móvil	X					
Directiva de dispositivo de programación de conexiones			X	X		
Directiva de dispositivo Contactos (CardDAV)	X	X				

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
Directiva de dispositivo Copiar aplicaciones en el contenedor de Samsung						X
Directiva de dispositivo Credenciales	X	X	X	X	X	
Directiva de dispositivo XML personalizado			X		X	
Directiva de dispositivo Defender					X	
Directiva de dispositivo Device Guard					X	

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
Directiva de dispositivo de atestación de estado del dispositivo					X	
Directiva de dispositivo de nombre de dispositivo	X	X				
Directiva de dispositivo de configuración educativa	X					
Directiva de dispositivo de opciones de Citrix Endpoint Management			X	X		

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
Directiva de dispositivo de desinstalación de Citrix Endpoint Management				X		
Directiva de dispositivo de Exchange	X	X	X	X	X	
Directiva de dispositivo de Archivos			X	X		
Directiva de dispositivo de FileVault		X				
Directiva de dispositivo de Firewall		X			X	
Directiva de dispositiv	X	X				

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
o de Fuente						
Directiva de dispositivo de diseño de pantalla de inicio	X					
Directiva de dispositivo de importación de configuración de dispositivo						X
Directiva de dispositivo de importación de perfiles de iOS y macOS	X	X				
Directiva de dispositivo de administración de			X			

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
bloqueo de pantalla						
Directiva de dispositivo de quiosco			X		X	
Directiva de dispositivo de configuración del iniciador			X	X		
Directiva de dispositivo LDAP	X	X				
Directiva de dispositivo de ubicación	X		X	X		
Directiva de dispositivo de mensaje de pantalla	X					

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
de bloqueo						
Directiva de dispositivo de correo	X	X				
Directiva de dispositivo de configuraciones administradas			X			
Directiva de dispositivo de dominios administrados	X					
Directiva de dispositivo de usuarios residentes máximos	X					
Directiva de dispositiv	X					

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
o de opciones de MDM						
Directiva de dispositivo de red	X		X	X		
Directiva de dispositivo de uso de red	X					
Directiva de dispositivo de Office					X	
Política de dispositivo de información de la organización	X					
Política de dispositivo de actualización del SO	X	X	X		X	

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
Política de dispositivo de código de acceso	X	X	X	X	X	
Política de dispositivo de período de gracia de bloqueo de código de acceso	X					
Política de dispositivo de punto de acceso personal	X					
Política de dispositivo de eliminación de perfil	X	X				
Política de dispositiv	X					

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
o de perfil de aprovisionamiento						
Política de dispositivo de eliminación de perfil de aprovisionamiento	X					
Política de dispositivo de proxy	X					
Política de dispositivo de restricciones	X	X		X	X	
Directiva de dispositivo de itinerancia	X					
Directiva de dispositiv			X			

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
o de clave de licencia MDM de Samsung						
Directiva de dispositivo SCEP	X	X				
Directivas de Siri y dictado	X					
Directiva de dispositivo de cuenta SSO	X					
Directiva de dispositivo de cifrado de almacenamiento						
Directiva de dispositivo de tienda	X			X	X	
Directiva de	X					

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
dispositivo de calendarios suscritos						
Directiva de dispositivo de términos y condiciones	X			X	X	
Directiva de dispositivo de túnel				X		
Directiva de dispositivo VPN	X	X		X	X	
Directiva de dispositivo de fondo de pantalla	X					
Directiva de dispositivo de clip web	X	X		X	X	

DIRECTIVA	IOS	MACOS	ANDROID ENTERPRISE	ANDROID (DA HEREDADO)	WINDOWS DE ESCRITORIO/ TABLETA	OTROS
Directiva de dispositivo de filtro de contenido web	X					
Directiva de dispositivo de agente de Windows					X	
Directiva de dispositivo de configuración de GPO de Windows					X	
Directiva de dispositivo de Windows Hello para empresas					X	

Directiva de dispositivo de duplicación de AirPlay

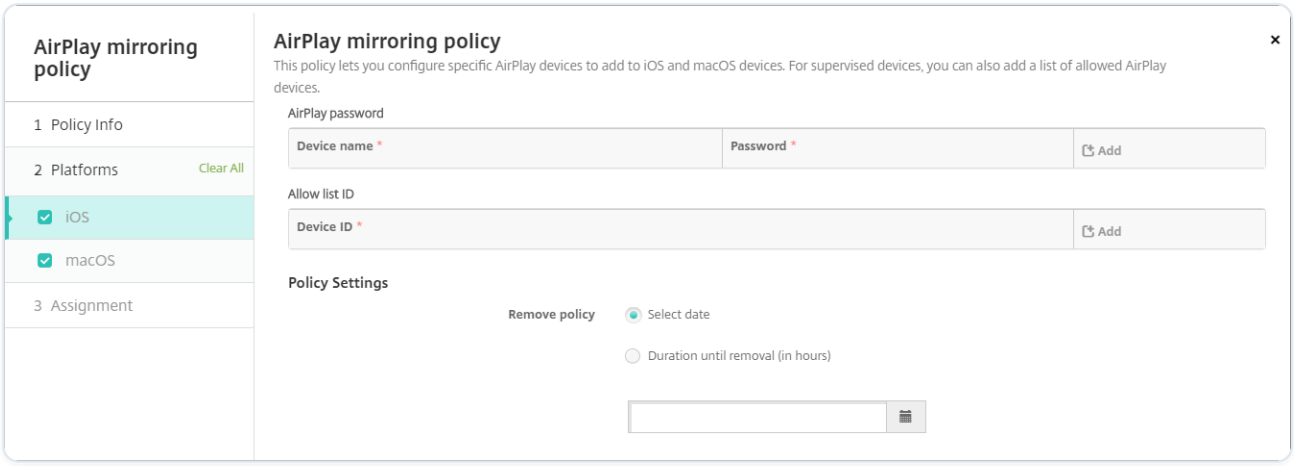
La función Apple AirPlay permite a los usuarios transmitir contenido de forma inalámbrica desde un dispositivo iOS a una pantalla de TV a través de Apple TV, o duplicar exactamente lo que hay en la pantalla de un dispositivo en una pantalla de TV u otro ordenador Mac.

Puede agregar una directiva de dispositivo en Citrix Endpoint Management para agregar dispositivos AirPlay específicos (como Apple TV u otro ordenador Mac) a dispositivos iOS. También tiene la opción de agregar dispositivos a una lista de permitidos para dispositivos supervisados, lo que limita a los usuarios únicamente a esos dispositivos AirPlay. Para obtener información sobre cómo poner un dispositivo en modo supervisado, consulte Implementar dispositivos con Apple Configurator 2.

> **Nota:**
>
> Antes de continuar, asegúrese de tener los ID de dispositivo y las contraseñas de todos los dispositivos que desea agregar.

> Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS



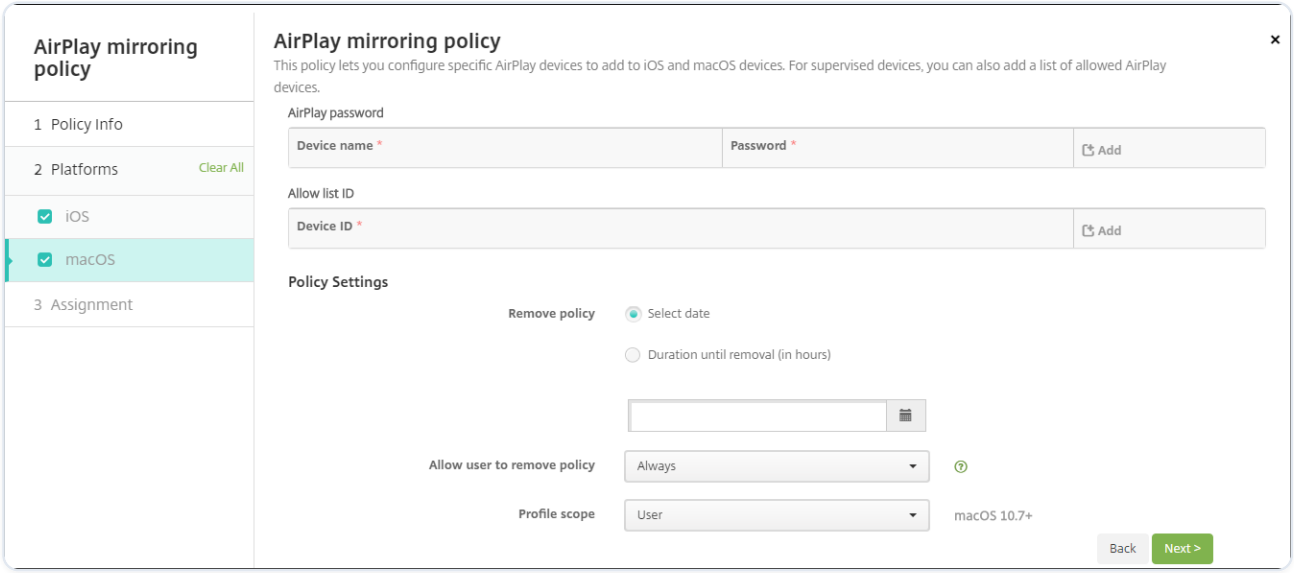
- **Contraseña de AirPlay:** Para cada dispositivo que desee agregar, haga clic en **Agregar** y, a continuación, haga lo siguiente:
  - **Nombre del dispositivo:** Introduzca la dirección de hardware (dirección MAC) en formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - **Contraseña:** Introduzca una contraseña opcional para el dispositivo.

- Haga clic en **Agregar** para agregar el dispositivo o haga clic en **Cancelar** para cancelar la adición del dispositivo.

- **ID de lista de permitidos:** Esta lista se ignora para los dispositivos no supervisados. Los ID de dispositivo de esta lista son los únicos dispositivos AirPlay disponibles para los dispositivos de los usuarios. Para cada dispositivo AirPlay que desee agregar a la lista, haga clic en **Agregar** y, a continuación, haga lo siguiente:
  - **ID de dispositivo:** Escriba el ID de dispositivo en formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - Haga clic en **Agregar** para agregar el dispositivo o haga clic en **Cancelar** para cancelar la adición del dispositivo.

- **Configuración de la directiva**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.

Configuración de macOS



- **Contraseña de AirPlay:** Para cada dispositivo que quiera agregar, haga clic en **Agregar** y, a continuación, haga lo siguiente:

  - **Nombre del dispositivo:** Introduzca la dirección de hardware (dirección MAC) en formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - **Contraseña:** Introduzca una contraseña opcional para el dispositivo.
  - Haga clic en **Agregar** para agregar el dispositivo o haga clic en **Cancelar** para cancelar la adición del dispositivo.

- **ID de lista de permitidos:** Esta lista se ignora para los dispositivos no supervisados. Los ID de dispositivo de esta lista son los únicos dispositivos AirPlay disponibles para los dispositivos de los usuarios. Para cada dispositivo AirPlay que quiera agregar a la lista, haga clic en **Agregar** y, a continuación, haga lo siguiente:
  - **ID de dispositivo:** Escriba el ID de dispositivo en formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
  - Haga clic en **Agregar** para agregar el dispositivo o haga clic en **Cancelar** para cancelar la adición del dispositivo.
- **Configuración de la directiva**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.
  - **Permitir al usuario eliminar la directiva:** Puede seleccionar cuándo los usuarios pueden eliminar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en macOS 10.7 y versiones posteriores.

Directiva de dispositivo AirPrint

La directiva de dispositivo AirPrint agrega impresoras AirPrint a la lista de impresoras AirPrint en los dispositivos iOS. Esta directiva facilita la compatibilidad con entornos donde las impresoras y los dispositivos se encuentran en subredes diferentes.

Nota:

Para configurar la directiva de dispositivo AirPrint, necesita la dirección IP y la ruta de recursos de cada impresora.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Parámetros de iOS

- **Destino de AirPrint:** Para cada destino de AirPrint que quiera agregar, haga clic en **Agregar** y, a continuación, haga lo siguiente:
  - **Dirección IP:** Introduzca la dirección IP de la impresora AirPrint.
  - **Ruta de recursos:** Introduzca la ruta de recursos asociada a la impresora. Este valor corresponde al parámetro del registro Bonjour `_ipps.tcp`. Por ejemplo, `printers/Canon_MG5300_series` o `printers/Xerox_Phaser_7600`.
- **Parámetros de directiva**
  - **Quitar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva. Solo disponible para iOS 6.0 o posterior.

Directiva de dispositivo de permisos de aplicaciones

Para las aplicaciones de Android Enterprise que se encuentran dentro de los perfiles de trabajo: puede configurar cómo las solicitudes a esas aplicaciones gestionan lo que Google denomina permisos «peligrosos». Usted controla si se le pide al usuario que conceda o deniegue la solicitud de permiso de la aplicación. Esta función se aplica a los dispositivos que ejecutan Android 7.0 y versiones posteriores.

Google define los permisos peligrosos como permisos que:

- Dan a la aplicación acceso a datos o recursos que implican información privada del usuario.

- O bien, pueden afectar potencialmente a los datos almacenados del usuario o al funcionamiento de otras aplicaciones. Por ejemplo, la capacidad de leer los contactos del usuario es un permiso peligroso.

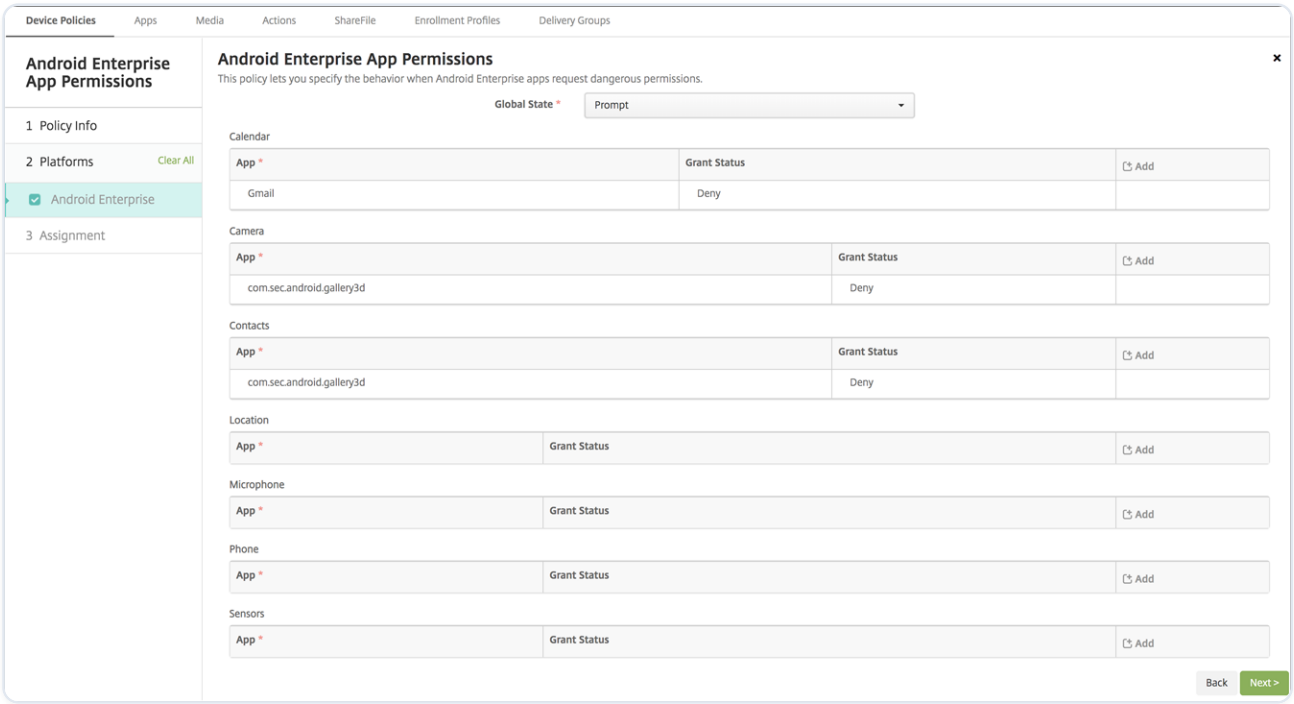
Puede configurar un estado global para controlar el comportamiento de todas las solicitudes de permisos peligrosos. El ámbito de esta configuración son las aplicaciones de Android Enterprise que se encuentran dentro de los perfiles de trabajo. También puede controlar el comportamiento de una solicitud de permiso peligroso para grupos de permisos individuales, según lo definido por Google, para cada aplicación. Esta configuración individual anula el estado global.

Para obtener información sobre cómo Google define los grupos de permisos, consulte la guía para desarrolladores de Android.

De forma predeterminada, se pide a los usuarios que concedan o denieguen las solicitudes de permisos peligrosos.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte (/es-es/citrix-endpoint-management/policies.html)Directivas de dispositivo.

Configuración de Android Enterprise



- **Estado global:** Controla el comportamiento de todas las solicitudes de permisos peligrosos. En la lista, haga clic en **Solicitar**, **Conceder** o **Denegar**.

  - **Solicitar:** Se pide a los usuarios que concedan o denieguen las solicitudes de permisos peligrosos.
  - **Conceder:** Se conceden todas las solicitudes de permisos peligrosos. No se le pide al usuario.
  - **Denegar:** Se deniegan todas las solicitudes de permisos peligrosos. No se le pide al usuario.

  El valor predeterminado es **Preguntar**.

- Establezca un comportamiento individual para cada grupo de permisos, para cada aplicación. Para configurar el comportamiento de un grupo de permisos: Haga clic en **Agregar**. Luego, en **Aplicación**, elija una aplicación de la lista. Si configura aplicaciones del sistema de Android Enterprise, haga clic en **Agregar nuevo** e introduzca el nombre del paquete de la aplicación que habilitó en la directiva de dispositivo Restricciones. En Estado de concesión, elija **Preguntar**, **Conceder** o **Denegar**. Este estado de concesión anula el estado global.

  - **Preguntar:** Se solicita a los usuarios que concedan o denieguen las solicitudes de permisos peligrosos de este grupo de permisos para esta aplicación.
  - **Conceder:** Se conceden las solicitudes de permisos peligrosos de este grupo de permisos para esta aplicación. No se le pregunta al usuario.

    > **Nota:**
    >
    > Para los dispositivos inscritos en el modo **Propietario del perfil**, el permiso **Conceder** no es aplicable para Cámara, Ubicación, Micrófono y Sensor si el dispositivo ejecuta Android 12 o posterior.

  - **Denegar:** Se deniegan las solicitudes de permisos peligrosos de este grupo de permisos para esta aplicación. No se le pregunta al usuario.

  El valor predeterminado es **Preguntar**.

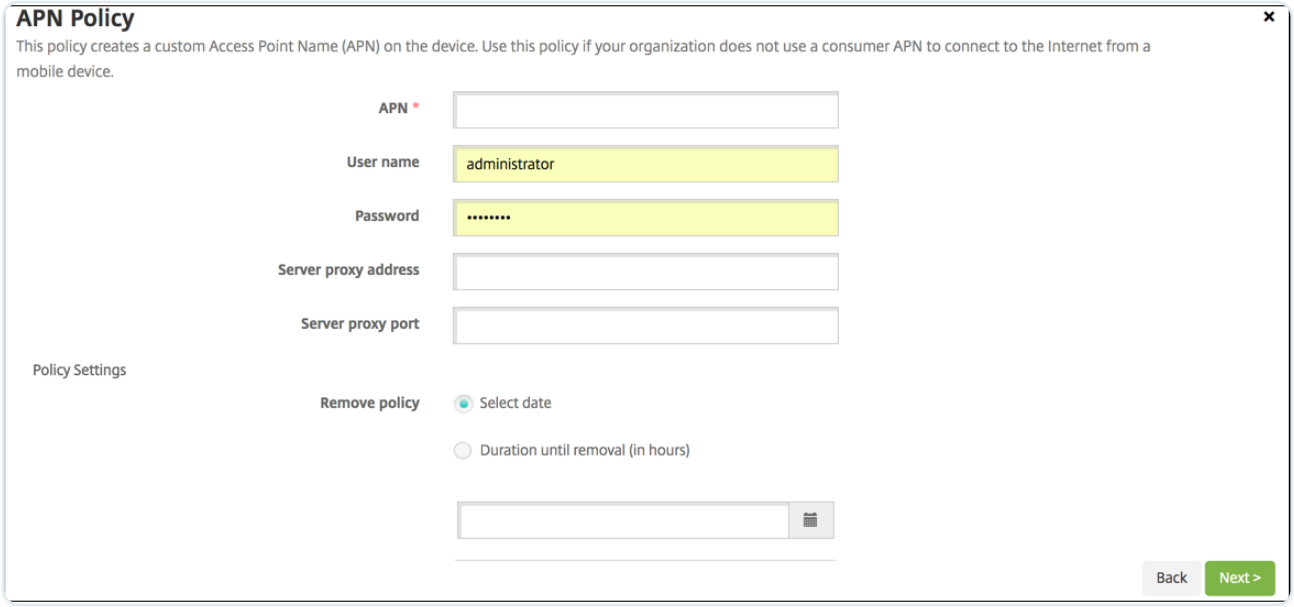
- Haga clic en **Guardar** junto a la aplicación y el estado de concesión.
- Para agregar más aplicaciones al grupo de permisos, haga clic en **Agregar** de nuevo y repita estos pasos.
- Cuando haya terminado de configurar el **Estado de concesión** para los grupos de permisos, haga clic en **Siguiente**.

Directiva de dispositivo APN

Puede agregar una directiva de dispositivo de nombre de punto de acceso (APN) personalizada para dispositivos iOS y Android. Utilice esta directiva si su organización no usa un APN de consumidor para conectarse a Internet desde un dispositivo móvil. Una directiva APN determina la configuración utilizada para conectar sus dispositivos al servicio general de radio por paquetes (GPRS) de un operador de telefonía específico. Esta configuración ya está definida en la mayoría de los teléfonos más recientes.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

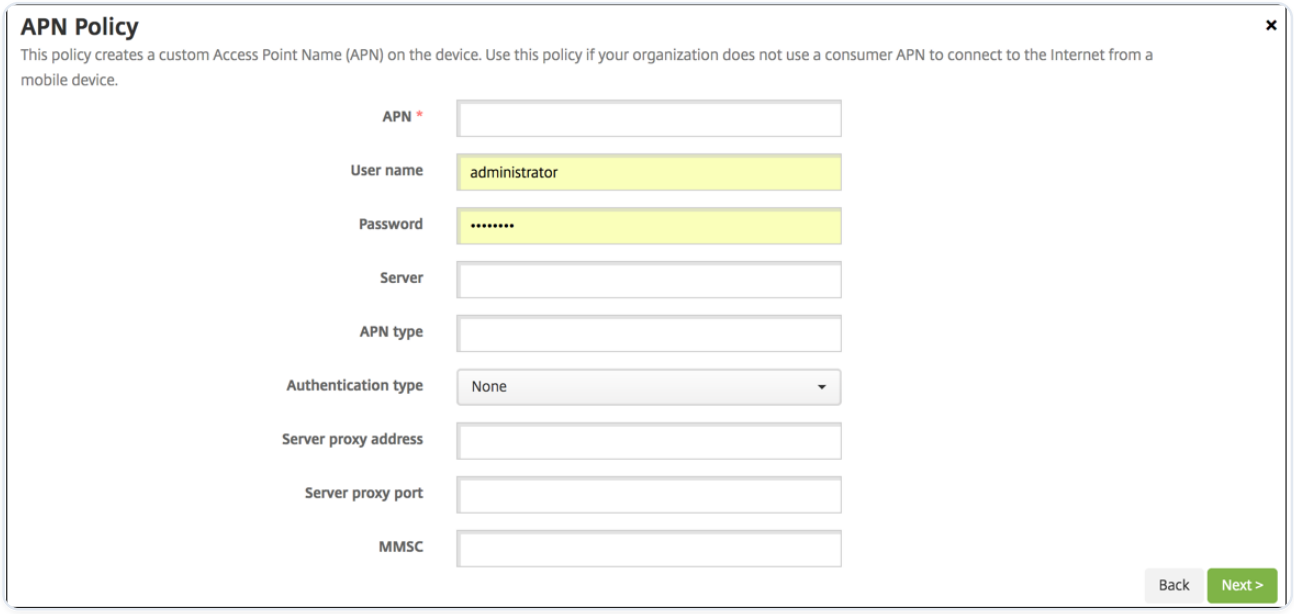


- **APN:** Escriba el nombre del punto de acceso. El nombre debe coincidir con un APN de iOS aceptado o la directiva no funcionará.
- **Nombre de usuario:** Esta cadena especifica el nombre de usuario para este APN. Si falta el nombre de usuario, el dispositivo solicitará la cadena durante la instalación del perfil.
- **Contraseña:** La contraseña del usuario para este APN. Para fines de ofuscación, la contraseña está codificada. Si falta en la carga útil, el dispositivo solicitará la contraseña durante la instalación del perfil.
- **Dirección de proxy del servidor:** La dirección IP o URL del proxy APN.
- **Puerto de proxy del servidor:** El número de puerto para el proxy APN. El número de puerto es obligatorio si ha introducido una dirección de proxy de servidor.
- En **Configuración de directivas**, junto a **Eliminar directiva**, haga clic en **Seleccionar fecha** o en **Duración hasta la eliminación (en horas)**.

- Para la opción **Seleccionar fecha**, haga clic en el calendario para seleccionar la fecha específica de eliminación.
- Para la opción **Contraseña requerida**, escriba la contraseña.

- **Configuración de directivas**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la política. Solo disponible para iOS 6.0 o posterior.

Configuración de Android



- **APN:** Escriba el nombre del punto de acceso. El nombre debe coincidir con un APN de Android aceptado o la política no funcionará.
- **Nombre de usuario:** Esta cadena especifica el nombre de usuario para este APN. Si falta el nombre de usuario, el dispositivo solicitará la cadena durante la instalación del perfil.
- **Contraseña:** La contraseña del usuario para este APN. Para fines de ofuscación, la contraseña está codificada. Si falta en la carga útil, el dispositivo solicitará la contraseña durante la instalación del perfil.
- **Servidor:** Esta configuración, que es anterior a los teléfonos inteligentes, suele estar vacía. Hace referencia a un servidor de puerta de enlace de Protocolo de aplicación inalámbrica (WAP) para teléfonos que no pueden acceder o renderizar sitios web estándar.

- **Tipo de APN:** Esta configuración debe coincidir con el uso previsto por el operador para el punto de acceso. Es una cadena de especificadores de servicio APN separados por comas y debe coincidir con las definiciones publicadas por el operador inalámbrico. Los ejemplos incluyen:
  - `*`: Todo el tráfico pasa por este punto de acceso.
  - `mms`: El tráfico multimedia pasa por este punto de acceso.
  - `default`: Todo el tráfico, incluido el multimedia, pasa por este punto de acceso.
  - `supl`: La ubicación segura del plano de usuario está asociada con el GPS asistido.
  - `dun`: La conexión de acceso telefónico a redes está obsoleta y rara vez se utiliza.
  - `hipri.`: Redes de alta prioridad.
  - `fota`: El firmware por aire se utiliza para recibir actualizaciones de firmware.
- **Tipo de autenticación:** Haga clic en el tipo de autenticación que se utilizará en la lista desplegable. El valor predeterminado es Ninguno.
- **Dirección del proxy del servidor:** La dirección IP o URL del proxy HTTP APN del operador.
- **Puerto del proxy del servidor:** El número de puerto para el proxy APN. El puerto es necesario si ha introducido una dirección de proxy del servidor.
- **MMSC:** La dirección del servidor de puerta de enlace MMS proporcionada por el operador.
- **Dirección del proxy del servidor de mensajería multimedia (MMS):** La dirección del servidor de servicio de mensajería multimedia para el tráfico MMS. MMS sucedió a SMS para el envío de mensajes más grandes con contenido multimedia, como imágenes o vídeos. Estos servidores requieren protocolos específicos (como MM1, ... MM11).
- **Puerto MMS:** El puerto utilizado para el proxy MMS.

Directiva de dispositivo de acceso a aplicaciones

La directiva de dispositivo de acceso a aplicaciones le permite definir una lista de aplicaciones que deben instalarse, pueden instalarse o no deben instalarse. Si las aplicaciones de un dispositivo contradicen esta directiva, Citrix Endpoint Management marca el dispositivo como no conforme. A continuación, puede crear una acción automatizada para reaccionar ante la conformidad de ese dispositivo.

> **Importante:**

> La directiva de dispositivo de acceso a aplicaciones no impide que un usuario instale una aplicación prohibida o desinstale una aplicación requerida.

> Solo puede configurar un tipo de directiva de acceso a la vez. Cada directiva tiene una lista de aplicaciones requeridas, aplicaciones sugeridas o aplicaciones prohibidas, pero no una mezcla dentro de la misma directiva de acceso a aplicaciones. Si crea una directiva para cada tipo de lista, asigne un nombre cuidadosamente a cada directiva para saber qué directiva se aplica a qué lista de aplicaciones.

Para agregar o configurar esta directiva, vaya a **Configurar** > **Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS y Android (DA heredado)

- **Directiva de acceso:** Seleccione el tipo de lista que desea configurar para esta directiva.
  - **Requerida:** La aplicación debe existir en el dispositivo. Si la aplicación no existe, el dispositivo se marca como no conforme. **Requerida** es la opción predeterminada.
  - **Prohibida:** La aplicación no debe existir en el dispositivo. Si la aplicación existe, el dispositivo se marca como no conforme.
- Para agregar una o varias aplicaciones a la lista:
  a. Haga clic en **Agregar** y, a continuación, configure lo siguiente:
    - **Nombre de la aplicación:** Introduzca un nombre de aplicación.
    - **Identificador de la aplicación:** Introduzca un identificador de aplicación opcional.
  b. Haga clic en **Guardar**.
  c. Repita estos pasos para cada aplicación que desee añadir.

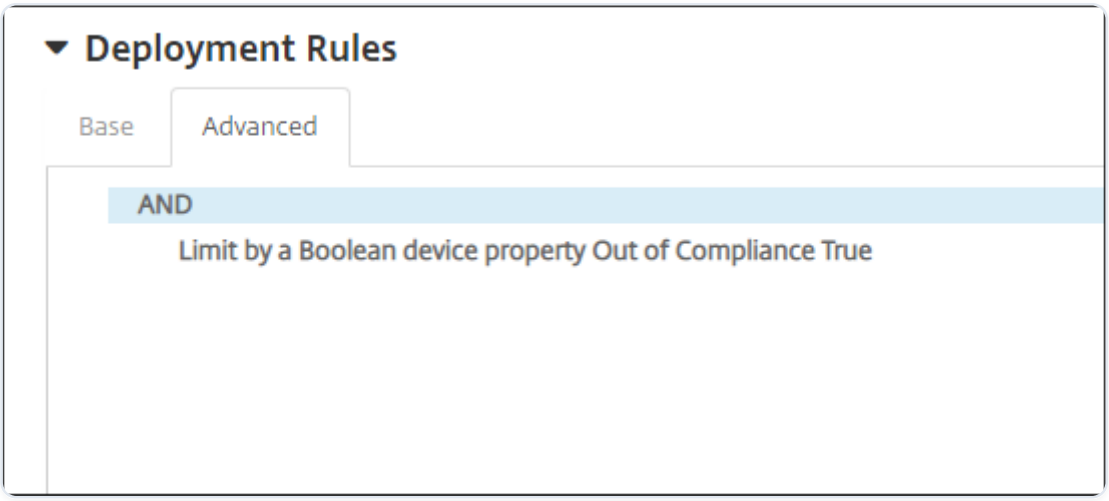
Configurar acciones automatizadas basadas en el cumplimiento del acceso a las aplicaciones

1. Añada una directiva de acceso a aplicaciones para requerir o prohibir aplicaciones.
2. Configure dos acciones automatizadas según si las aplicaciones en cuestión son obligatorias o prohibidas:
   - Obligatorias

- Marque un dispositivo como no conforme si una aplicación obligatoria no existe en el dispositivo.
- Marque un dispositivo como conforme una vez que se instale esa aplicación obligatoria.

- Prohibidas
  - Marque un dispositivo como no conforme si una aplicación prohibida existe en el dispositivo.
  - Marque un dispositivo como conforme una vez que esa aplicación prohibida ya no esté instalada. Para obtener información sobre cómo configurar acciones automatizadas, consulte Acciones automatizadas.

3. Cree una directiva de restricción con la configuración que desea implementar en los dispositivos no conformes.
   a. Como parte de la directiva de restricción, añada una regla de implementación avanzada con las opciones **Limitar por una propiedad booleana del dispositivo**, **No conforme** y **Verdadero**. Consulte Directiva de dispositivo de restricciones.



4. Cree una directiva de eliminación de perfiles para eliminar la directiva de restricción una vez que el dispositivo vuelva a estar conforme.
5. Añada una regla de implementación avanzada con las opciones **Limitar por una propiedad booleana del dispositivo**, **No conforme** y **Falso**. Consulte Directiva de dispositivo de eliminación de perfiles.

Directiva de dispositivo de atributos de aplicación

La directiva de dispositivo **Atributos de aplicación** le permite especificar atributos para las aplicaciones en dispositivos iOS. Al configurar este tipo de directiva, puede lograr lo siguiente:

- Asignar VPN por aplicación a las aplicaciones.
- Evitar que los usuarios desinstalen aplicaciones de misión crítica. Se aplica a iOS 14 y versiones posteriores.
- Si la función Dominios asociados está habilitada, especifique los dominios asociados que se agregarán a las aplicaciones. Se aplica a iOS 13 y versiones posteriores.

  Para obtener más información, consulte Acerca de los dominios asociados.

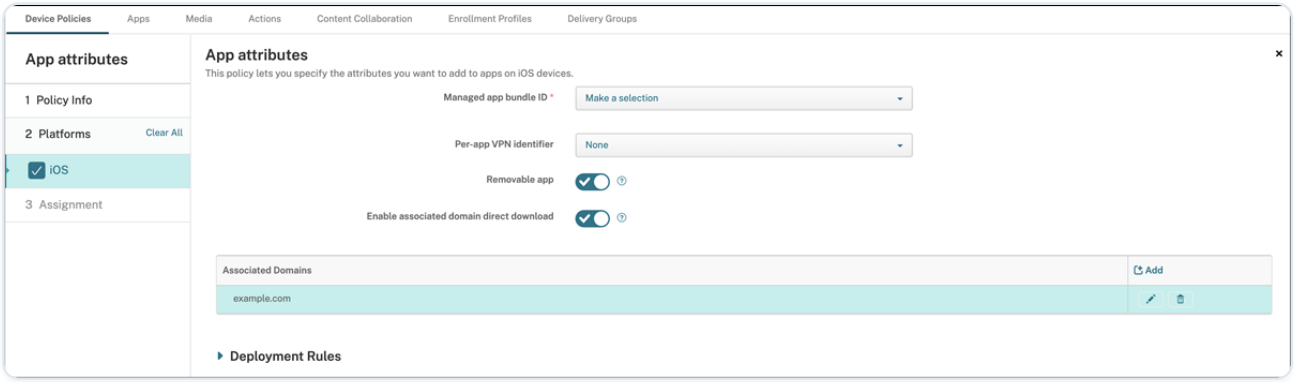
Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Acerca de los dominios asociados

Los dominios asociados le permiten establecer una asociación segura entre los dominios y su aplicación para que pueda compartir credenciales o proporcionar funciones en su aplicación desde sus sitios web. Por ejemplo, con esta función habilitada, puede compartir datos y credenciales de inicio de sesión entre aplicaciones y sitios web de su organización.

Para obtener más información sobre cómo habilitar esta función, consulte Compatibilidad con dominios asociados en el sitio web de Apple.

Configuración de iOS



- **ID de paquete de aplicación administrada:** Especifique una aplicación de las siguientes maneras:
  - Seleccione el ID de paquete de la aplicación. Las opciones solo están disponibles después de habilitar la directiva de dispositivo **Inventario de aplicaciones**, que recopila un inventario de las aplicaciones en los dispositivos administrados.
  - Seleccione **Agregar nuevo** y, a continuación, escriba el ID de paquete de la aplicación. Para encontrar un ID de paquete de aplicación, consulte Buscar el ID de paquete de una aplicación en App Store.

- **Identificador de VPN por aplicación:** (Opcional) Seleccione una VPN por aplicación para esta aplicación. Las opciones incluyen las conexiones VPN por aplicación que configuró en la página **Directivas de dispositivo > Directiva VPN**. Para obtener más información, consulte Configurar una VPN por aplicación.
- **Aplicación extraíble:** (Opcional) Especifique si los usuarios pueden quitar esta aplicación cuando es una aplicación administrada. Para evitar que los usuarios desinstalen esta aplicación, establezca esta opción en **Desactivado**. El valor predeterminado es **Activado**.
- **Habilitar descarga directa de dominio asociado:** (Opcional) El valor predeterminado es **Activado**, lo que indica que esta aplicación realiza la verificación de asociación de sitio reclamada directamente en el dominio en lugar de en los servidores de Apple. Establezca esta opción en **Activado** solo para dominios que no pueden acceder a Internet.
- **Dominios asociados:** (Opcional) Para agregar un dominio asociado a esta aplicación, haga clic en **Agregar** y, a continuación, escriba su nombre de dominio completo (FQDN).

Buscar el ID de paquete de una aplicación en la App Store

1. Busque la aplicación en la App Store y copie el número al final de la URL. Por ejemplo, 363501921 es el ID de aplicación de la aplicación Citrix Workspace.
2. Vaya a `https://itunes.apple.com/lookup?id=` y pegue el número después de esa URL. Se descargará automáticamente un archivo TXT en su equipo.
3. En el archivo TXT, busque `bundleId` y obtenga el ID de paquete de la aplicación. Ejemplo: el ID de paquete de la aplicación Citrix Workspace es `com.citrix.ReceiveriPad`.

Directiva de dispositivo de configuración de aplicaciones

Puede configurar de forma remota las aplicaciones que admiten la configuración administrada implementando:

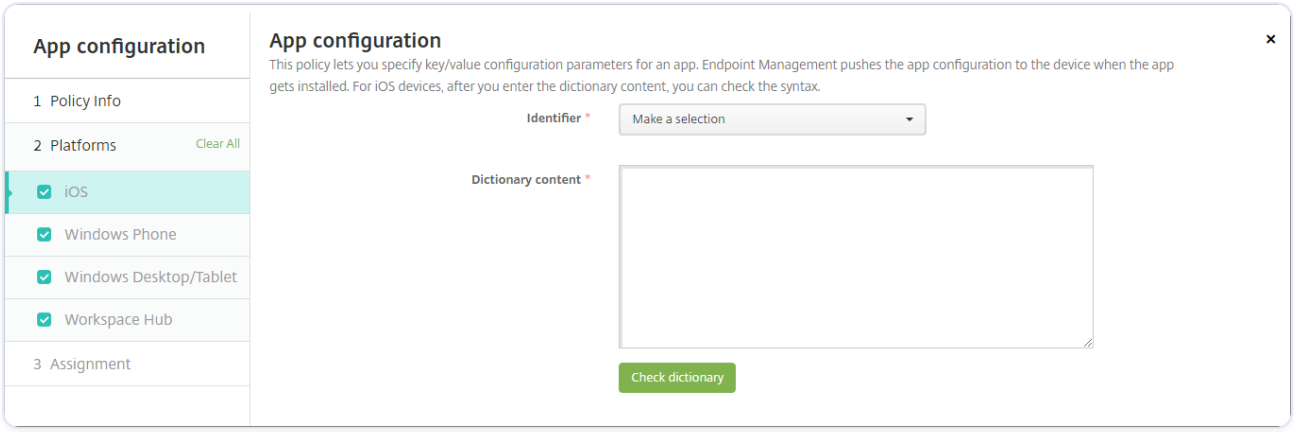
- Un archivo de configuración XML (`.plist`, también llamado lista de propiedades) en dispositivos iOS
- Pares clave-valor para dispositivos de teléfono, escritorio o tableta que ejecuten Windows 10 o Windows 11

La configuración especifica varios ajustes y comportamientos en la aplicación. Citrix Endpoint Management envía la configuración a los dispositivos cuando el usuario instala la aplicación. Los ajustes y comportamientos reales que puede configurar dependen de la aplicación y quedan fuera del alcance de este artículo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

> **Nota:**
>
> Los propietarios de las aplicaciones respectivas definen las variables de configuración de la aplicación. Por ejemplo, Chrome gestiona y mantiene las variables de configuración de la aplicación para Chrome. Para obtener más información, consulte Variables de configuración de la aplicación Chrome.

Configuración de iOS



- **Identificador:** Haga clic en la aplicación que desea configurar en la lista desplegable o haga clic en **Agregar nuevo** para agregar una aplicación a la lista.
  - Si hace clic en **Agregar nuevo**, escriba el identificador de la aplicación en el campo que aparece.
- **Contenido del diccionario:** Escriba, o copie y pegue, la información de configuración de la lista de propiedades XML (`.plist`).
- Haga clic en **Comprobar diccionario**. Citrix Endpoint Management verifica el XML. Si no hay errores, verá **XML válido** debajo del cuadro de contenido. Si aparecen errores de sintaxis debajo del cuadro de contenido, debe corregirlos antes de poder continuar.

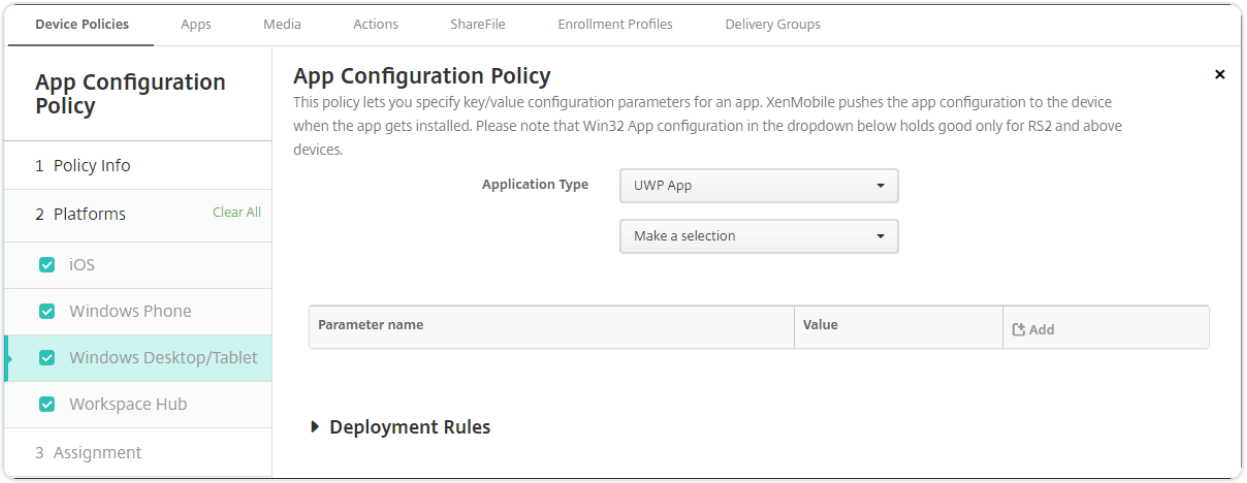
Configuración de Windows para escritorio/tableta

Puede configurar aplicaciones de Plataforma universal de Windows (UWP) o aplicaciones Win 32. Para importar la configuración de directivas de plantillas administrativas de Microsoft (ADMX), configure las aplicaciones Win 32.

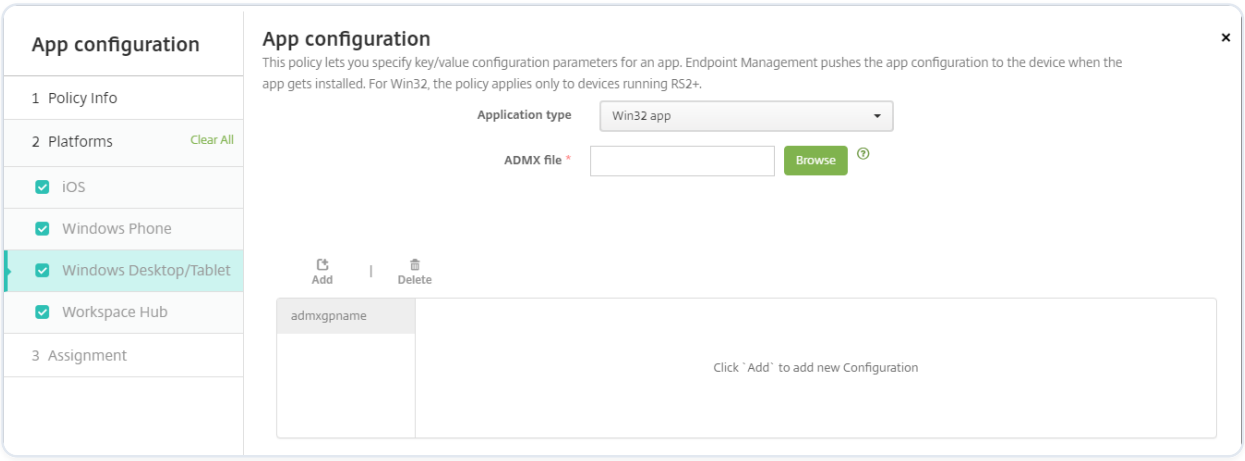
Nota:

La directiva de dispositivo de Configuración de aplicaciones admite archivos ADMX de terceros para aplicaciones de terceros como Office. No se admiten las plantillas ADMX de Microsoft para Windows que se proporcionan como directivas de grupo del sistema operativo disponibles en `%SystemRoot%\PolicyDefinitions`.

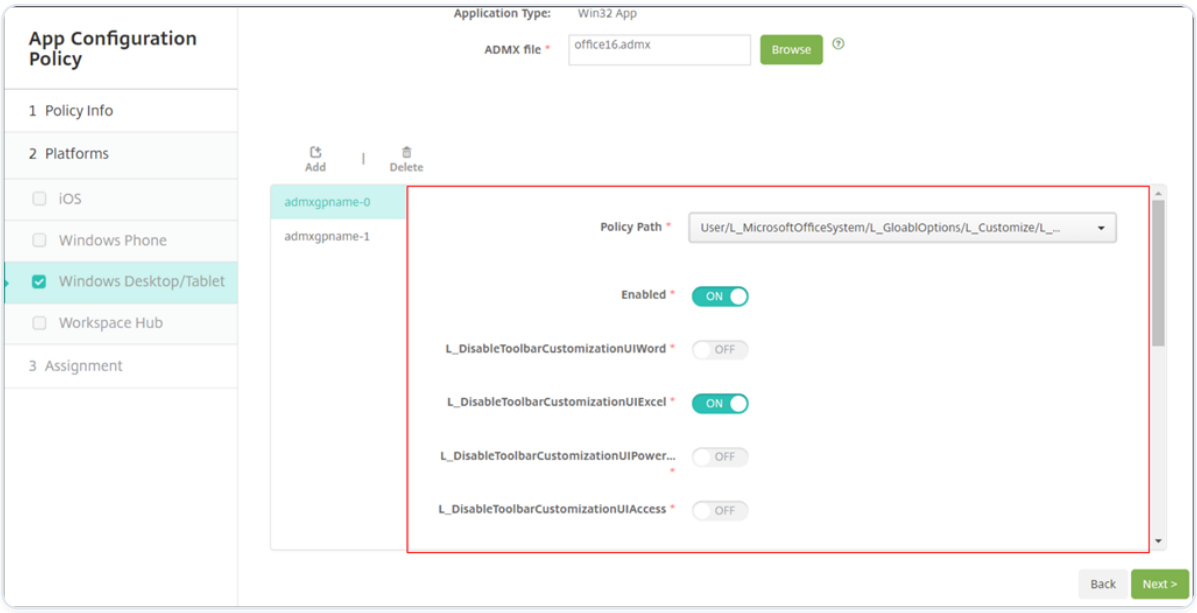
- Si elige **Aplicación UWP:** En la lista **Realizar una selección**, haga clic en la aplicación que quiere configurar o haga clic en **Agregar nuevo** para agregar una aplicación a la lista.



  - Si hace clic en **Agregar nuevo**, escriba el nombre de la familia de paquetes en el campo que aparece.
  - Para cada parámetro de configuración que quiera agregar, haga clic en **Agregar** y, a continuación, haga lo siguiente:
    - **Nombre del parámetro:** Introduzca el nombre de clave de una configuración de aplicación para el dispositivo Windows. Para obtener información sobre la configuración de aplicaciones de Windows, consulte la documentación de Microsoft.
    - **Valor:** Introduzca el valor del parámetro especificado.
    - Haga clic en **Agregar** para añadir el parámetro o haga clic en **Cancelar** para cancelar la adición del parámetro.
- Si elige **Aplicación Win32:** Haga clic en **Examinar** y vaya al archivo ADMX que quiere usar para configurar la directiva.



- Haga clic en **Agregar**. Las opciones de configuración del archivo ADMX aparecen en el lado derecho de la página.



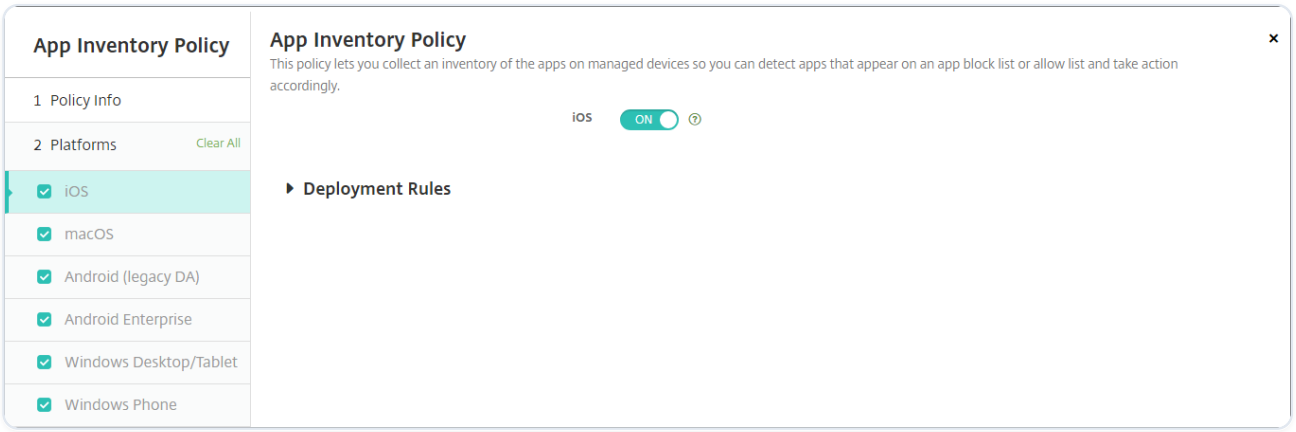
- Elija una ruta de directiva. Si elige la misma ruta más de una vez, se aplica la configuración asociada a la versión más reciente.
- Configure **Habilitar** en **Activado**.
- Introduzca los valores de elementos de lista necesarios como pares clave-valor. Utilice la cadena de texto **&#xF000** para separar cada par clave-valor y el valor y la clave dentro del par.
- Los valores de los elementos que incluyen un decimal podrían requerir valores dentro de un rango específico.

Directiva de dispositivo de inventario de aplicaciones

La directiva de inventario de aplicaciones le permite recopilar un inventario de las aplicaciones en los dispositivos administrados. Citrix Endpoint Management puede entonces comparar el inventario con cualquier directiva de acceso a aplicaciones implementada en esos dispositivos. De esta manera, puede detectar aplicaciones que aparecen en una lista de permitidas o bloqueadas y actuar correctamente. Utilice una directiva de acceso a aplicaciones para definir la lista de permitidas o bloqueadas.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

iOS, macOS, Android (DA heredado), Android Enterprise y Windows Desktop/Tablet



- Para cada plataforma que seleccione, deje la configuración predeterminada o cámbiela a **Desactivado**. El valor predeterminado es **Activado**.

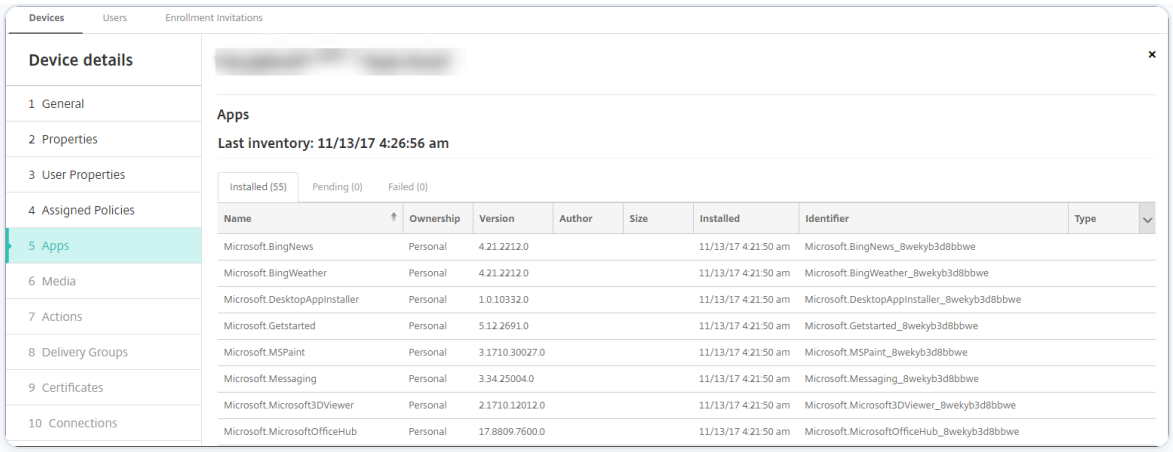
Inventariar y eliminar aplicaciones `Win32`

Puede determinar si las aplicaciones `Win32` en los dispositivos de los usuarios siguen su directiva de dispositivo de acceso a aplicaciones. Para ver un inventario de aplicaciones `Win32` en dispositivos de escritorio y tabletas administrados con Windows 10 y Windows 11:

1. Vaya a **Configurar > Directivas de dispositivo** y agregue una directiva de inventario de aplicaciones para la plataforma **Windows Desktop/Tablet**. Implemente la directiva.
2. Vaya a **Administrar > Dispositivos**, seleccione el dispositivo Windows 10 y Windows 11 que desea ver, haga clic en **Modificar** y, a continuación, haga clic en la ficha **Aplicaciones**.

   Aparecen los resultados del inventario.

> **Nota:**
>
> Si está configurando un dispositivo Windows 11, debe esperar hasta 24 horas para obtener resultados de inventario correctos, según lo diseñado por Microsoft.



3. Compare el inventario de aplicaciones con su directiva de dispositivo de acceso a aplicaciones. Si el dispositivo tiene aplicaciones instaladas que están en la lista de bloqueadas, puede eliminarlas del dispositivo.

Problemas de instalación y desinstalación de aplicaciones causados por un código de producto incorrecto

Si una aplicación `Win32` se configura con el código de producto incorrecto, la aplicación se instala inicialmente; sin embargo, Microsoft no devuelve el estado de la aplicación a Citrix Endpoint Management. Como resultado:

- La directiva de dispositivo de desinstalación de aplicaciones no desinstala la aplicación.
- Citrix Endpoint Management sigue implementando la aplicación porque no tiene confirmación de que la aplicación se haya instalado. Con cada implementación, el dispositivo genera un código de error porque la aplicación ya está instalada. El error que se muestra en **Administrar > Dispositivo > Detalles del grupo de entrega** es: `Msi Application received: Reporting:AppPush id:7z1701-x64.msi: Command execution failed -2147023293`

Para corregir el código de producto:

1. Elimine manualmente la aplicación del dispositivo.
2. En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones** y corrija el código de producto de la aplicación `Win32`.
3. Implemente la aplicación `Win32`.

Directiva de dispositivo de Application Guard

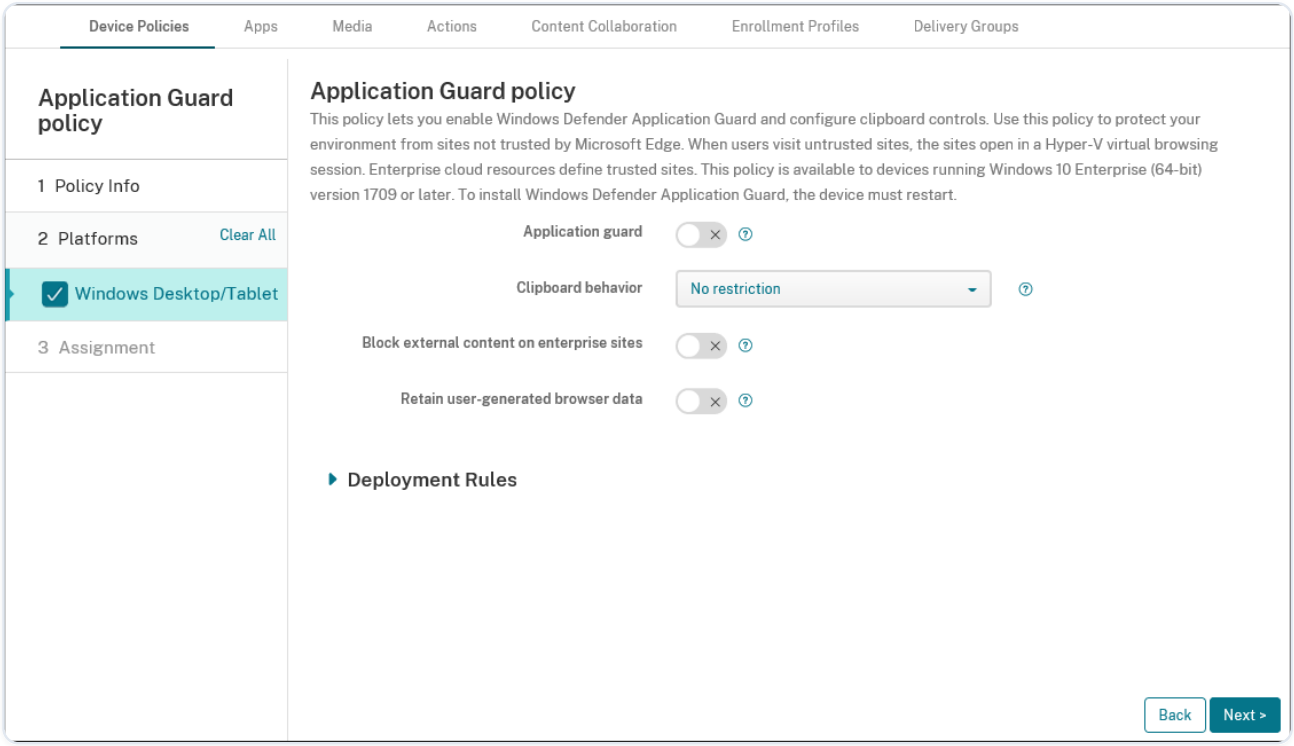
La directiva de Application Guard especifica la configuración de Windows Defender Application Guard. La configuración incluye si se debe habilitar Application Guard y los controles para el comportamiento del portapapeles.

Windows Defender Application Guard protege su entorno de los sitios que su organización no ha definido como de confianza. Cuando los usuarios visitan sitios que no están en la lista de su límite de red aislado: Los sitios se abren en una sesión de navegación virtual en Hyper-V. Los recursos de la nube empresarial definen los sitios de confianza.

Requisitos

- Dispositivos con Windows 10 Enterprise (64 bits) o Windows 11 Enterprise (64 bits). Se requiere reiniciar el dispositivo para instalar Windows Defender Application Guard.
- Navegador Microsoft Edge

Configuración de Windows Desktop y Tablet



- **Application Guard:** Habilita Application Guard. El valor predeterminado es **Desactivado**.
    - **Recursos de la nube empresarial:** Una lista de dominios de la nube empresarial separados por comas.
- **Comportamiento del portapapeles:** Controla las direcciones en las que se puede copiar y pegar contenido. Las opciones son las siguientes:

    - **No configurado**
    - **Permitir copiar y pegar solo del navegador al PC:** Permite a los usuarios copiar y pegar contenido solo de su navegador a su PC.
    - **Permitir copiar y pegar solo del PC al navegador:** Permite a los usuarios copiar y pegar contenido solo de su PC a su navegador.
    - **Permitir copiar y pegar entre el PC y el navegador:** Permite a los usuarios copiar y pegar contenido libremente entre su PC y el navegador.
    - **Bloquear copiar y pegar entre el PC y el navegador:** No permite a los usuarios copiar y pegar contenido entre su PC y el navegador.

- **Contenido del portapapeles:** Controla qué contenido pueden copiar y pegar los usuarios. Las opciones son las siguientes:
    - **Sin restricciones**
    - **Permitir copiar texto:** Permite a los usuarios copiar solo texto.
    - **Permitir copiar imágenes:** Permite a los usuarios copiar solo imágenes.
    - **Permitir copiar texto e imágenes:** Permite a los usuarios copiar tanto texto como imágenes.
- **Bloquear contenido externo en sitios empresariales:** Si está en **Activado**, Windows Defender Application Guard impide que el contenido de sitios no aprobados se cargue en sitios empresariales. El valor predeterminado es **Desactivado**.
- **Conservar los datos del navegador generados por el usuario:** Si está en **Activado**, permite guardar los datos de usuario creados durante una sesión de navegación virtual de Application Guard. Estos datos incluyen elementos como contraseñas, favoritos y cookies. El valor predeterminado es **Desactivado**.

Directiva de bloqueo de aplicaciones en dispositivos

La directiva de bloqueo de aplicaciones en dispositivos define una lista de aplicaciones que están:

- Permitidas para ejecutarse en un dispositivo.
- Bloqueadas para ejecutarse en un dispositivo.

La forma exacta en que funciona la directiva difiere para cada plataforma compatible. Por ejemplo, no se pueden bloquear varias aplicaciones en un dispositivo iOS.

Del mismo modo, para los dispositivos iOS, solo se puede seleccionar una aplicación iOS por directiva. Los usuarios solo pueden usar su dispositivo para ejecutar una única aplicación. No pueden realizar ninguna otra actividad en el dispositivo, excepto las opciones que usted permita específicamente cuando se aplica la directiva de bloqueo de aplicaciones en dispositivos.

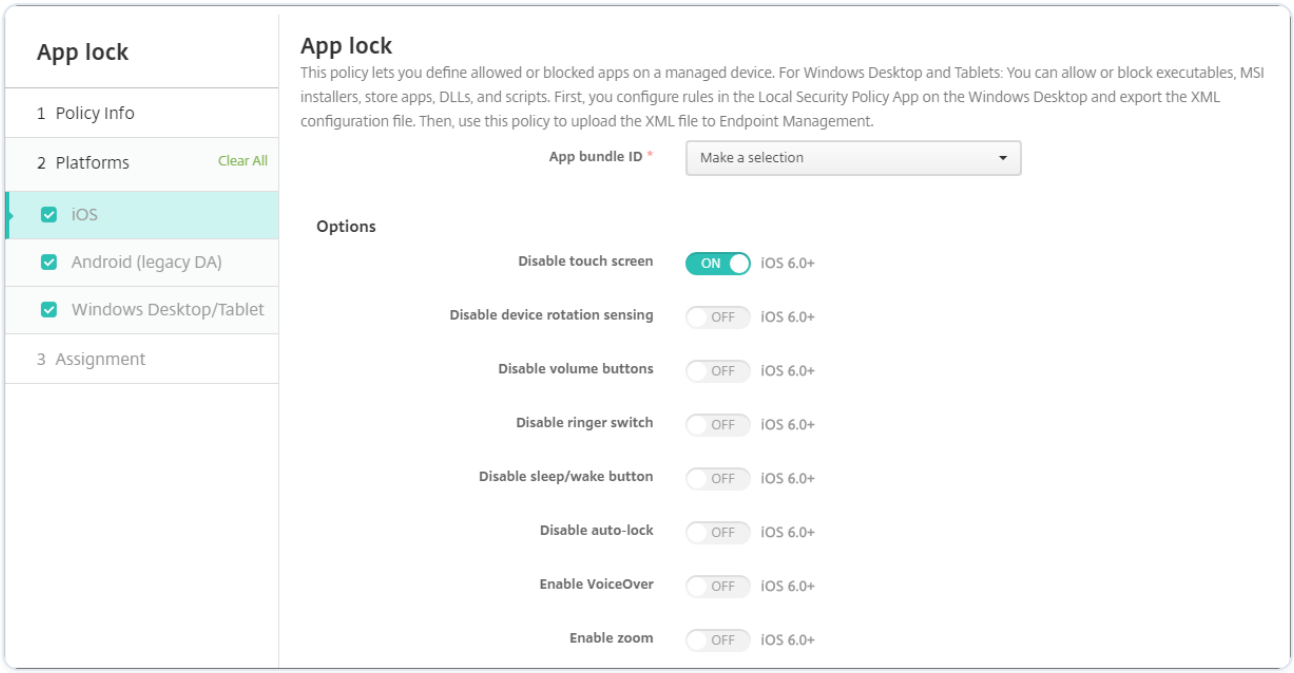
Además, los dispositivos iOS deben estar supervisados para aplicar directivas de bloqueo de aplicaciones.

Aunque la directiva de dispositivos funciona en la mayoría de los dispositivos Android L y M, el bloqueo de aplicaciones no funciona en dispositivos Android N o posteriores. No funciona porque Google dejó de usar la API necesaria.

Para escritorios y tabletas Windows administrados, puede crear una directiva de bloqueo de aplicaciones en dispositivos que defina la lista de aplicaciones en las listas de permitidas y bloqueadas. Puede permitir o bloquear ejecutables, instaladores MSI, aplicaciones de la tienda, DLL y scripts.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivos**. Para obtener más información, consulte Directivas de dispositivos.

Configuración de iOS



- **ID de paquete de aplicación:** Haga clic en la aplicación de la lista desplegable a la que se aplica esta directiva, o haga clic en **Agregar nuevo** para agregar una aplicación a la lista. Si selecciona **Agregar nuevo**, escriba el nombre de la aplicación en el campo que aparece.

- **Opciones:** Para cada opción, el valor predeterminado es **Desactivado**, excepto para **Deshabilitar pantalla táctil**, cuyo valor predeterminado es **Activado**.
  - Deshabilitar pantalla táctil
  - Deshabilitar la detección de rotación del dispositivo
  - Deshabilitar los botones de volumen
  - Deshabilitar el interruptor de timbre

    Cuando **Deshabilitar el interruptor de timbre** está en **Activado**, el comportamiento del timbre depende de la posición en la que se encontraba el interruptor cuando se deshabilitó por primera vez.
  - Deshabilitar el botón de reposo/activación
  - Deshabilitar el bloqueo automático
  - Deshabilitar VoiceOver
  - Habilitar zoom
  - Habilitar inversión de colores
  - Habilitar AssistiveTouch
  - Habilitar lectura de selección
  - Habilitar audio mono
  - Habilitar control por voz
- **Opciones habilitadas por el usuario:** Para cada opción, el valor predeterminado es **Desactivado**.
  - Permitir ajuste de VoiceOver
  - Permitir ajuste de zoom
  - Permitir ajuste de inversión de colores
  - Permitir ajuste de AssistiveTouch
  - Permitir ajuste de control por voz
- **Configuración de directiva**
  - **Quitar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**

- **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
- **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva. Solo disponible para iOS 6.0 o posterior.

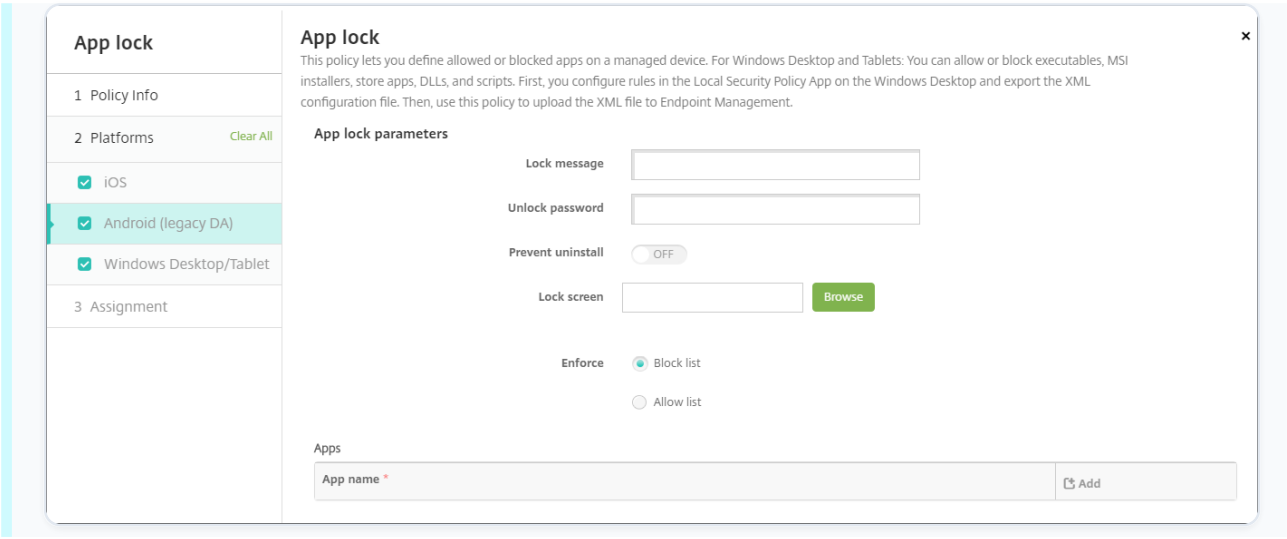
Configurar un iPad como quiosco

Puede usar la directiva de dispositivo de bloqueo de aplicaciones para ejecutar un iPad supervisado como quiosco. Apple se refiere a esta función como Modo de aplicación única. Para obtener más información sobre esta función, consulte la documentación de Apple. Asegúrese de implementar la aplicación que desea ejecutar antes de implementar esta directiva.

1. Vaya a **Configurar > Directivas de dispositivo** y haga clic en **Agregar**.
2. Seleccione la directiva **Bloqueo de aplicaciones**.
3. Escriba un **Nombre de directiva** y una **Descripción** opcional.
4. Seleccione solo la plataforma **iOS**.
5. En **ID de paquete de aplicación**, seleccione la aplicación que desea ejecutar en el iPad.
6. Configure las opciones que desee, como se describió anteriormente, y guarde la directiva.
7. Agregue la directiva al mismo grupo de entrega que su iPad y despliegue la directiva.

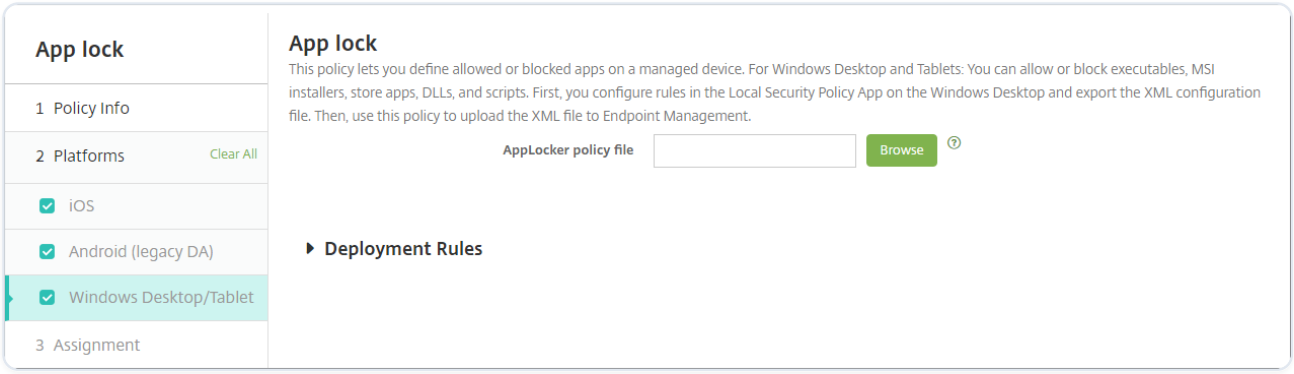
Configuración de Android (DA heredado)

> **Nota:**
>
> No puede bloquear la aplicación de Configuración de Android mediante la directiva de dispositivo Bloqueo de aplicaciones.



- **Parámetros de Bloqueo de aplicaciones**
  - **Mensaje de bloqueo:** Escriba un mensaje que los usuarios verán cuando intenten abrir una aplicación bloqueada.
  - **Contraseña de desbloqueo:** Escriba la contraseña para desbloquear la aplicación.
  - **Impedir desinstalación:** Seleccione si los usuarios pueden desinstalar aplicaciones. El valor predeterminado es **Desactivado**.
  - **Pantalla de bloqueo:** Seleccione la imagen que aparece en la pantalla de bloqueo del dispositivo haciendo clic en **Examinar** y navegando hasta la ubicación del archivo.
  - **Aplicar:** Haga clic en **Lista de bloqueo** para crear una lista de aplicaciones que no pueden ejecutarse en los dispositivos. Haga clic en **Lista de permitidos** para crear una lista de aplicaciones que sí pueden ejecutarse en los dispositivos.
- **Aplicaciones:** Haga clic en **Agregar** y, a continuación, haga lo siguiente:
  - **Nombre de la aplicación:** Haga clic en el nombre de la aplicación en la lista desplegable que desea agregar a la lista de permitidos o de bloqueo. Alternativamente, haga clic en **Agregar nueva** para agregar una aplicación a la lista de aplicaciones disponibles.
  - Si selecciona **Agregar nueva**, escriba el nombre de la aplicación en el campo que aparece.
  - Haga clic en **Guardar** o **Cancelar**.
  - Repita estos pasos para cada aplicación que desee añadir a la lista de permitidas o bloqueadas.

Configuración de escritorio y tableta de Windows



Requisitos previos para el bloqueo de aplicaciones

- En Windows, configure las reglas en el editor de directivas de seguridad local en un escritorio de Windows 10 o Windows 11.
- Exporte el archivo XML de la directiva. Citrix® recomienda crear reglas predeterminadas en Windows para evitar bloquear la configuración predeterminada o causar problemas en los dispositivos.
- A continuación, cargue el archivo XML en Citrix Endpoint Management mediante la directiva de dispositivo de bloqueo de aplicaciones. Para obtener más información sobre cómo crear reglas, consulte este artículo de Microsoft: `<https://docs.microsoft.com/es-es/windows/security/threat-protection/applocker/applocker-overview>`

Para configurar y exportar el archivo XML de la directiva desde Windows

> **Importante:**
>
> Al configurar el archivo XML de la directiva a través del editor de directivas de Windows, utilice el modo Solo auditoría.

1. En el equipo Windows, inicie el editor de **Directiva de seguridad local**. Haga clic en **Inicio**, escriba **directiva de seguridad local** y, a continuación, haga clic en **Directiva de seguridad local**.
2. En el árbol de la consola, expanda **Directivas de control de aplicaciones**.
3. Haga clic en **AppLocker** y, a continuación, en el panel central, haga clic en **Configurar la aplicación de reglas**.
4. Seleccione **Configurado** y, a continuación, **Aplicar reglas**. Cuando habilita una regla, **Aplicar reglas** es la opción predeterminada.

5. Haga clic con el botón derecho en **AppLocker**, haga clic en **Exportar directiva** y, a continuación, guarde el archivo XML.

> **Nota:**
>
> Puede crear **Reglas de ejecutables**, **Reglas de instalador de Windows**, **Reglas de scripts** y **Reglas de aplicaciones empaquetadas**. Para ello, haga clic con el botón derecho en la carpeta y, a continuación, haga clic en **Crear nueva regla**.

Para importar el archivo XML de directiva en Citrix Endpoint Management

Cree una directiva de bloqueo de aplicaciones. Junto a la configuración **Archivo de directiva de bloqueo de aplicaciones**, haga clic en **Examinar** y vaya al archivo XML.

Para dejar de aplicar una directiva de bloqueo de aplicaciones

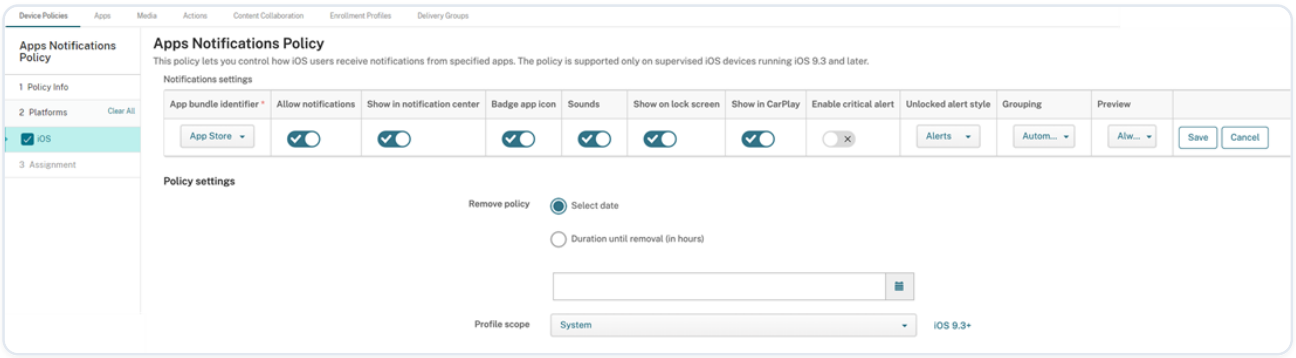
Después de implementar una directiva de bloqueo de aplicaciones en Citrix Endpoint Management: Para dejar de aplicar esa directiva de bloqueo de aplicaciones, cree un archivo XML vacío. A continuación, cree otra directiva de bloqueo de aplicaciones, cargue el archivo e implemente la directiva. Los dispositivos que tienen el bloqueo de aplicaciones habilitado no se ven afectados. Los dispositivos que reciben la directiva por primera vez no tienen la directiva de bloqueo de aplicaciones implementada.

Directiva de dispositivo de notificaciones de aplicaciones

La directiva de notificaciones de aplicaciones le permite controlar cómo los usuarios de iOS reciben notificaciones de aplicaciones específicas. La directiva solo es compatible con dispositivos iOS supervisados que ejecuten iOS 9.3 o posterior.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS



- **Identificador de paquete de aplicación:** Especifique la aplicación donde quiere administrar la configuración de notificaciones:
  - Seleccione el ID de paquete de la aplicación. Las opciones solo están disponibles después de habilitar la directiva de dispositivo **Inventario de aplicaciones**, que recopila un inventario de aplicaciones en los dispositivos administrados.
  - Seleccione **Agregar nuevo** y, a continuación, escriba el ID de paquete de la aplicación. Para buscar un ID de paquete de aplicación, consulte Buscar el ID de paquete de una aplicación en App Store.
- **Permitir notificaciones:** Seleccione **Activado** para permitir las notificaciones.
- **Mostrar en el centro de notificaciones:** Seleccione **Activado** para mostrar las notificaciones en el centro de notificaciones del dispositivo del usuario.
- **Icono de aplicación con distintivo:** Seleccione **Activado** para mostrar un icono de aplicación con distintivo con las notificaciones.
- **Sonidos:** Seleccione **Activado** para incluir sonidos con las notificaciones.
- **Mostrar en la pantalla de bloqueo:** Seleccione **Activado** para mostrar las notificaciones en la pantalla de bloqueo de los dispositivos de los usuarios.
- **Mostrar en CarPlay:** Seleccione **Activado** para mostrar las notificaciones en Apple CarPlay. Se aplica a iOS 12 y versiones posteriores. El valor predeterminado es **Activado**.
- **Habilitar alerta crítica:** Seleccione **Activado** para permitir que la aplicación marque una notificación como crítica, lo que ignora la configuración de No molestar y el timbre. Se aplica a iOS 12 y versiones posteriores. El valor predeterminado es **Desactivado**.
- **Estilo de alerta desbloqueada:** Seleccione **Ninguno**, **Banner** o **Alertas** para configurar la apariencia de las alertas desbloqueadas.
- **Vista previa:** Seleccione cómo los dispositivos muestran las vistas previas de las notificaciones para la aplicación. Se aplica a iOS 14 y versiones posteriores.

  - **Siempre:** Para mostrar las vistas previas de las notificaciones cuando el dispositivo está bloqueado o desbloqueado.
  - **Cuando está desbloqueado:** Para mostrar las vistas previas de las notificaciones solo cuando el dispositivo está desbloqueado.
  - **Nunca:** Para borrar las vistas previas de las notificaciones en el dispositivo.

- **Agrupación:** Seleccione cómo los dispositivos agrupan las notificaciones de la aplicación. Se aplica a dispositivos iOS 12 y versiones posteriores.
  - **Automático:** Para agrupar las notificaciones en grupos especificados por la aplicación.
  - **Por aplicación:** Para agrupar las notificaciones de la aplicación en un solo grupo.
  - **Desactivado:** Para borrar las agrupaciones de notificaciones de la aplicación. Los dispositivos muestran todas las notificaciones en secuencia.

- **Configuración de la directiva**
  - **Eliminar directiva:** Seleccione un método para programar la eliminación de la directiva. Las opciones incluyen las siguientes:
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva. Se aplica a iOS 6.0 o versiones posteriores.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Se aplica a iOS 9.3 y versiones posteriores.

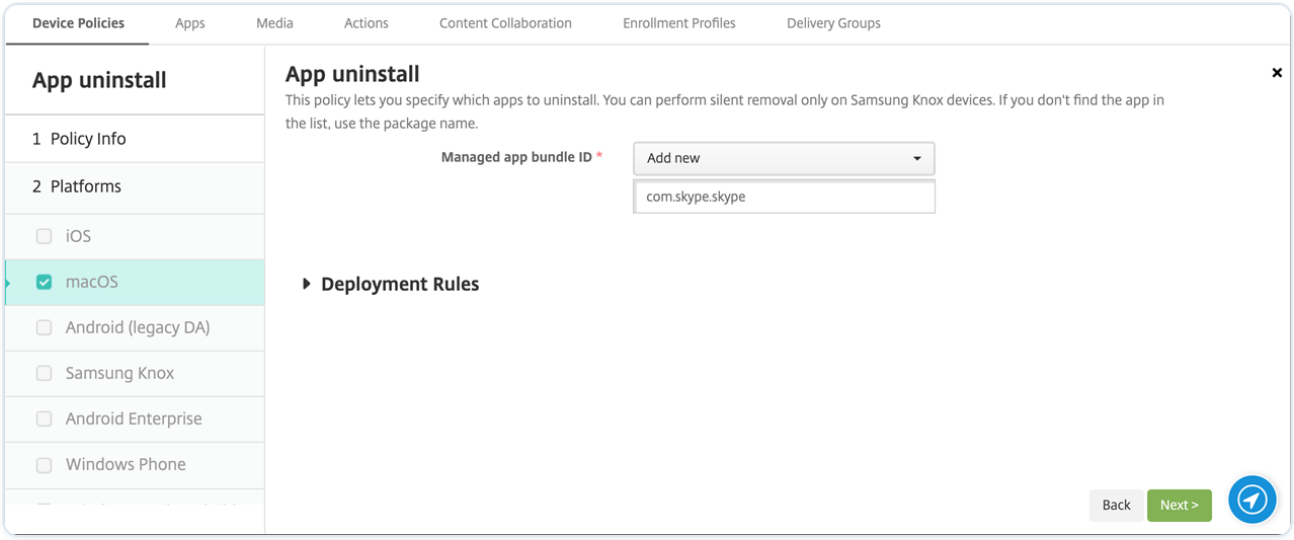
Política de dispositivo de desinstalación de aplicaciones

La política de desinstalación de aplicaciones le permite eliminar aplicaciones de los dispositivos de los usuarios. Puede eliminar una aplicación si ya no desea admitirla o si desea reemplazarla por una aplicación similar de un proveedor diferente.

Cuando esta política se implementa en los dispositivos de los usuarios, estos reciben un mensaje para desinstalar la aplicación y, a continuación, la aplicación se elimina.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS y macOS



- **ID de paquete de aplicación administrada:** En la lista, seleccione una aplicación administrada existente o **Agregar nueva**. Si no hay aplicaciones configuradas para esta plataforma, la lista estará vacía y deberá agregar una nueva aplicación administrada. Al seleccionar **Agregar nueva**, aparece un campo donde puede escribir un nombre de aplicación administrada. Disponible para iOS 5.0 y versiones posteriores y macOS 11.0 y versiones posteriores.

Configuración de Android (DA heredado), Android Enterprise y Windows Desktop/Tablet

- **Aplicaciones para desinstalar:** Para cada aplicación que desee agregar, haga clic en **Agregar** y, a continuación, haga lo siguiente:
  - **Nombre de la aplicación:** Haga clic en una aplicación existente en la lista desplegable o haga clic en **Agregar nueva** para introducir un nuevo nombre de aplicación. Si no hay aplicaciones configuradas para esta plataforma, la lista estará vacía y deberá agregar nuevas aplicaciones.
  - Haga clic en **Agregar** para agregar la aplicación o haga clic en **Cancelar** para cancelar la adición de la aplicación.

Para las aplicaciones de Android Enterprise, habilite también la política de dispositivo de inventario de aplicaciones. Consulte Política de dispositivo de inventario de aplicaciones.

Desinstalar automáticamente una aplicación Enterprise después de la instalación de la aplicación correspondiente de la tienda de aplicaciones pública

Puede configurar Citrix Endpoint Management para eliminar la versión Enterprise de las aplicaciones de Citrix tras la instalación de la versión de la tienda de aplicaciones pública. Esta función evita que los dispositivos de los usuarios tengan dos iconos de aplicación similares después de la instalación de la versión de la tienda de aplicaciones pública.

Una condición de implementación para la política de dispositivo de desinstalación de aplicaciones activa Citrix Endpoint Management para eliminar aplicaciones antiguas de los dispositivos de los usuarios tras la instalación de la nueva versión. Esta función solo está disponible para dispositivos iOS administrados conectados a un servidor de Citrix Endpoint Management en modo empresarial (XME).

Para configurar una regla de implementación con la condición Nombre de la aplicación instalada:

- Especifique el **ID de paquete de aplicación administrada** para la aplicación Enterprise.
- Agregue una regla: haga clic en **Nueva regla** y, como se muestra en el ejemplo, elija **Nombre de la aplicación instalada** e **es igual a**. Escriba el ID de paquete de la aplicación de la tienda de aplicaciones pública.

En el ejemplo, cuando la aplicación de la tienda de aplicaciones pública (com.citrix.mail.ios) se instala en un dispositivo de los grupos de entrega especificados, Citrix Endpoint Management elimina la versión Enterprise (com.citrix.mail).

Política de dispositivo de restricciones de desinstalación de aplicaciones

Puede especificar las aplicaciones que los usuarios pueden o no pueden desinstalar en un dispositivo Amazon.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de Amazon

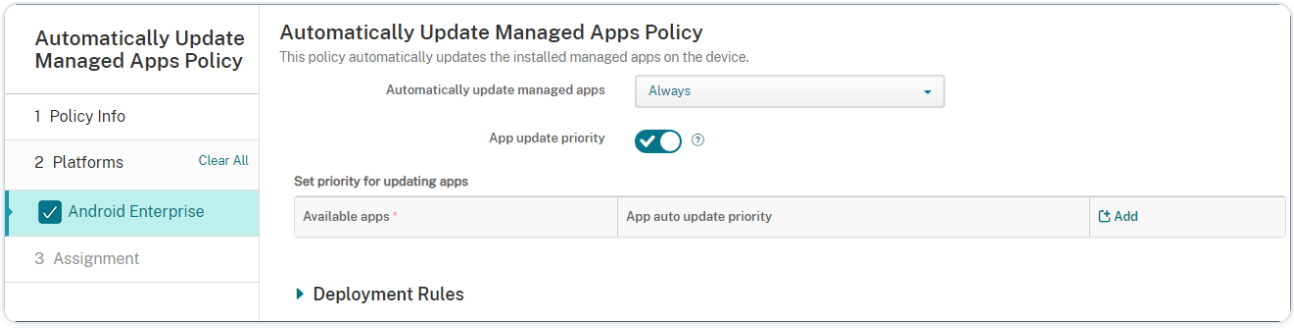
- **Configuración de restricciones de desinstalación de aplicaciones:** Para cada regla de aplicación que quiera agregar, haga clic en **Agregar** y, a continuación, haga lo siguiente:

- **Nombre de la aplicación:** Haga clic en una aplicación de la lista desplegable o en **Agregar nueva** para agregar una aplicación.
- **Regla:** Seleccione si los usuarios pueden desinstalar la aplicación. De forma predeterminada, se permite la desinstalación.
- Haga clic en **Guardar** o en **Cancelar**.

Política de dispositivo para actualizar automáticamente las aplicaciones administradas

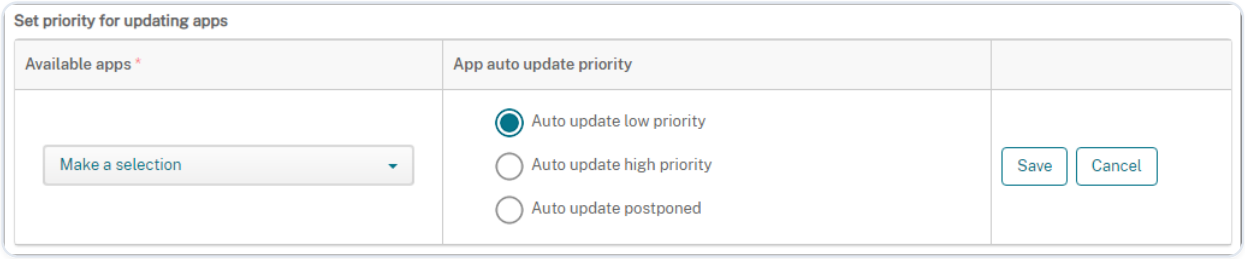
Esta política controla cómo se actualizan las aplicaciones administradas instaladas en los dispositivos Android Enterprise. Puede restringir la capacidad de los usuarios para permitir actualizaciones automáticas de aplicaciones en sus dispositivos. Si permite a los usuarios controlar las actualizaciones automáticas de aplicaciones en sus dispositivos, estos establecen las políticas de actualización automática de aplicaciones en la tienda administrada de Google Play.

Para agregar o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.



- **Actualizar automáticamente las aplicaciones administradas**
  - **Siempre:** Habilita las actualizaciones automáticas de aplicaciones. **Siempre** es la opción predeterminada.
  - **Permitir al usuario configurar la política:** Permite al usuario configurar la política de actualización automática de aplicaciones para el dispositivo en la tienda administrada de Google Play.
  - **Nunca:** Deshabilita las actualizaciones automáticas de aplicaciones.
  - **Solo cuando el dispositivo está conectado a Wi-Fi:** Permite las actualizaciones automáticas de aplicaciones solo cuando el dispositivo está conectado a Wi-Fi.
- **Prioridad de actualización de aplicaciones:** Si está **Activado**, puede configurar un nivel de prioridad de actualización para cada aplicación administrada.

- **Establecer prioridad para actualizar aplicaciones:** Haga clic en **Agregar** para configurar la prioridad de actualización de una aplicación.



  - **Aplicaciones disponibles:** Seleccione una aplicación del menú para configurar la prioridad de actualización.
  - **Prioridad de actualización automática de aplicaciones:** Seleccione una prioridad de actualización de las siguientes:
    - **Prioridad baja de actualización automática:** La aplicación se actualiza cuando el dispositivo se está cargando, no está en uso activo y está conectado a una red no medida.
    - **Actualización automática de alta prioridad:** La aplicación se actualiza lo antes posible, sin restricciones.
    - **Actualización automática pospuesta:** La aplicación no se actualiza automáticamente durante un máximo de 90 días después de que haya una nueva versión disponible. Después de 90 días, la aplicación se actualiza automáticamente con baja prioridad. Una vez que la aplicación se actualiza, no vuelve a actualizarse automáticamente durante otros 90 días. El usuario puede actualizar la aplicación manualmente en cualquier momento.
  - Haga clic en **Guardar** cuando haya terminado. Puede editar una configuración haciendo clic en el icono del lápiz. Elimine la configuración haciendo clic en el icono de la papelera.

Directiva de dispositivo BitLocker

Windows 10 y Windows 11 incluyen una función de cifrado de disco llamada BitLocker, que proporciona protecciones adicionales de archivos y del sistema contra el acceso no autorizado a un dispositivo Windows perdido o robado. Para mayor protección, puede usar BitLocker con chips de Módulo de plataforma segura (TPM), versión 1.2 o posterior. Un chip TPM gestiona las operaciones criptográficas y genera, almacena y limita el uso de claves criptográficas.

A partir de Windows 10, compilación 1703, las directivas MDM pueden controlar BitLocker. Utilice la directiva de dispositivo BitLocker en Citrix Endpoint Management para configurar los ajustes

disponibles en el asistente de BitLocker en dispositivos Windows 10 y Windows 11. Por ejemplo, en un dispositivo con BitLocker habilitado, BitLocker pide a los usuarios varias opciones:

- Cómo quieren desbloquear su unidad al iniciar
- Cómo hacer una copia de seguridad de su clave de recuperación
- Cómo desbloquear una unidad fija.

La configuración de la directiva de dispositivo BitLocker también configura si:

- Habilitar BitLocker en dispositivos sin un chip TPM.
- Mostrar opciones de recuperación en la interfaz de BitLocker.
- Denegar el acceso de escritura a una unidad fija o extraíble cuando BitLocker no está habilitado.
- Guardar de forma segura una clave de recuperación de BitLocker cifrada para que los usuarios puedan acceder a ella en caso de que olviden o extravíen la clave. Esta clave se puede encontrar en el Portal de autoayuda.

> Nota

> Una vez que el cifrado de BitLocker se inicia en un dispositivo, no se pueden cambiar los ajustes de BitLocker en el dispositivo implementando una directiva de dispositivo BitLocker actualizada.

> Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos

- La política de dispositivo BitLocker requiere la edición Windows 10 Enterprise o Windows 11 Enterprise.
- Antes de implementar la política de dispositivo BitLocker, prepare su entorno para el uso de BitLocker. Para obtener información detallada de Microsoft, incluidos los requisitos del sistema de BitLocker y la configuración, consulte los artículos en BitLocker.

Configuración de Windows Desktop y Tablet

BitLocker policy

This policy lets you enable BitLocker on an enrolled machine and specify the encryption mechanism to use.

BitLocker settings

Require device to be encrypted — ON

Encryption settings

Configure encryption methods — ON

Operating system drive — XTS AES 128-bit

Fixed drive — XTS AES 128-bit

Removable drive — XTS AES 128-bit

OS drive settings

Require additional authentication at startup — ON

Block BitLocker on devices without TPM chip — ON

TPM startup — Allow TPM

TPM startup PIN — Allow startup PIN with TPM

TPM startup key — Allow TPM key at startup

TPM startup key and PIN — Allow startup key and PIN with TPM

PIN length

Minimum PIN length — 6

BitLocker password recovery settings

BitLocker Recovery backup to Endpoint Management — ON

The Self-Help Portal displays the recovery key on the Devices page. Enable the server property shp.console.enable to provide access to the portal. **Learn more**

OS drive recovery settings

Enable OS drive recovery — ON

Allow certificate based data recovery agent — ON

48-bit recovery password — Allow 48-bit password

256-bit recovery key — Allow 256-bit recovery key

Hide OS drive recovery options — ON

Save recovery info to Active Directory Domain Services — ON

Recovery info stored in Active Directory Domain Services — Backup recovery password

Enable BitLocker after storing recovery info in Active Directory Domain Services — ON

- **Configuración de BitLocker**
  - **Requerir que el dispositivo esté cifrado:** Determina si se debe solicitar a los usuarios que habiliten el cifrado BitLocker en Windows Desktop o Tablet. Si está en **Activado**, los dispositivos muestran un mensaje después de que finaliza la inscripción, indicando que la empresa requiere el cifrado del dispositivo. Si está en **Desactivado**, no se le solicita al usuario y BitLocker utiliza la configuración de la política. El valor predeterminado es **Desactivado**.
- **Configuración de cifrado**
  - **Configurar métodos de cifrado:** Determina los métodos de cifrado que se utilizarán para tipos de unidades específicos. Si está en **Desactivado**, el asistente de BitLocker solicita al usuario del dispositivo el método de cifrado que se utilizará para un tipo de unidad. El método de cifrado para todas las unidades predetermina a XTS-AES de 128 bits. El método de cifrado para unidades extraíbles predetermina a AES-CBC de 128 bits. Si está en **Activado**, BitLocker utiliza el método de cifrado especificado en la política. Si está en **Activado**, aparecen estas configuraciones adicionales: **Unidad del sistema operativo**, **Unidad fija** y **Unidad extraíble**. Elija el método de cifrado predeterminado para cada tipo de unidad. El valor predeterminado es **Desactivado**.
- **Configuración de la unidad del SO**
  - **Requerir autenticación adicional al inicio:** Especifica la autenticación adicional requerida durante el inicio del dispositivo. También especifica si se permite BitLocker en dispositivos que no tienen un chip TPM. Si está en **Desactivado**, los dispositivos sin TPM no pueden usar el cifrado BitLocker. Para obtener información sobre TPM, consulte el artículo de Microsoft, Trusted Platform Module Technology Overview. Si está en **Activado**, aparecen las siguientes configuraciones adicionales. El valor predeterminado es **Desactivado**.
  - **Bloquear BitLocker en dispositivos sin un chip TPM:** En un dispositivo sin chip TPM, BitLocker requiere que los usuarios creen una contraseña de desbloqueo o una clave de inicio. La clave de inicio se almacena en una unidad USB, que el usuario debe conectar al dispositivo antes del inicio. La contraseña de desbloqueo tiene un mínimo de ocho caracteres. El valor predeterminado es **Desactivado**.
  - **Inicio de TPM:** En un dispositivo con TPM, hay cuatro modos de desbloqueo: solo TPM, TPM + PIN, TPM + clave y TPM + PIN + clave. El inicio de TPM es para el modo solo TPM, en el que las claves de cifrado se almacenan en el chip TPM. Este modo no requiere que el usuario proporcione datos de desbloqueo adicionales. El dispositivo del usuario se

desbloquea automáticamente durante el reinicio, utilizando la clave de cifrado del chip TPM. El valor predeterminado es **Permitir TPM**.

- **PIN de inicio de TPM:** Esta configuración es el modo de desbloqueo TPM + PIN. Un PIN puede tener hasta 20 dígitos. Utilice la configuración **Longitud mínima del PIN** para especificar la longitud mínima del PIN. Un usuario configura un PIN durante la configuración de BitLocker y lo proporciona durante el inicio del dispositivo.
- **Clave de inicio de TPM:** Esta configuración es el modo de desbloqueo TPM + clave. La clave de inicio se almacena en una unidad USB u otra unidad extraíble, que el usuario debe conectar al dispositivo antes del inicio.
- **Clave y PIN de inicio de TPM:** Esta configuración es el modo de desbloqueo TPM + PIN + clave.

  Si el desbloqueo se realiza correctamente, el sistema operativo comienza a cargarse. De lo contrario, el dispositivo entra en modo de recuperación.

- **Longitud del PIN**
  - **Longitud mínima del PIN:** La longitud mínima del PIN de inicio de TPM. El valor predeterminado es **6**.
- **Configuración de recuperación de contraseña de BitLocker**
  - **Copia de seguridad de recuperación de BitLocker en Citrix Endpoint Management:** Si esta opción está habilitada, los usuarios que deban desbloquear sus dispositivos pueden encontrar su clave de recuperación de BitLocker en el portal de autoservicio. El administrador de Citrix Endpoint Management no puede ver la clave de recuperación de BitLocker de un usuario. Para obtener más información sobre cómo ver su clave de recuperación de BitLocker, consulte Clave de recuperación de BitLocker.
- **Configuración de recuperación de la unidad del SO:** Configura las opciones de recuperación para los usuarios de una unidad del SO cifrada con BitLocker.
  - **Habilitar la recuperación de la unidad del SO:** Si el paso de desbloqueo falla, BitLocker solicita al usuario la clave de recuperación configurada. Esta configuración configura las opciones de recuperación de la unidad del sistema operativo disponibles para los usuarios si no tienen la contraseña de desbloqueo o la clave de inicio USB. El valor predeterminado es **Desactivado**.
  - **Permitir agente de recuperación de datos basado en certificado:** Especifica si se permite un agente de recuperación de datos basado en certificado. Agregue un agente de

recuperación de datos desde Directivas de clave pública, que se encuentra en la Consola de administración de directivas de grupo (GPMC) o en el Editor de directivas de grupo local. Para obtener más información sobre los agentes de recuperación de datos, consulte el artículo de Microsoft, Configuración de directiva de grupo de BitLocker. El valor predeterminado es **Desactivado**.

- **Contraseña de recuperación de 48 bits:** Especifica si se permite o se exige a los usuarios que utilicen una contraseña de recuperación. BitLocker genera la contraseña y la almacena en un archivo o en una cuenta de Microsoft Cloud. El valor predeterminado es **Permitir contraseña de 48 bits**.
- **Clave de recuperación de 256 bits:** Especifica si se permite o se exige a los usuarios que utilicen una clave de recuperación. Una clave de recuperación es un archivo BEK que se almacena en una unidad USB. El valor predeterminado es **Permitir clave de recuperación de 256 bits**.
- **Ocultar opciones de recuperación de la unidad del SO:** Especifica si se muestran u ocultan las opciones de recuperación en la interfaz de BitLocker. Si está en **Activado**, no aparecerán opciones de recuperación en la interfaz de BitLocker. En ese caso, registre el dispositivo en Active Directory, guarde las opciones de recuperación en Active Directory y establezca **Guardar información de recuperación en AD DS** en **Activado**. El valor predeterminado es **Desactivado**.
- **Guardar información de recuperación en Active Directory Domain Services:** Especifica si se guardan las opciones de recuperación en Active Directory Domain Services. El valor predeterminado es **Desactivado**.
- **Información de recuperación almacenada en Active Directory Domain Services:** Especifica si se almacena la contraseña de recuperación de BitLocker o la contraseña de recuperación y el paquete de claves en Active Directory Domain Services. Almacenar el paquete de claves permite recuperar datos de una unidad físicamente dañada. El valor predeterminado es **Copia de seguridad de la contraseña de recuperación**.
- **Habilitar BitLocker después de almacenar la información de recuperación en Active Directory Domain Services:** Especifica si se impide a los usuarios habilitar BitLocker a menos que el dispositivo esté conectado al dominio y la copia de seguridad de la información de recuperación de BitLocker en Active Directory se realice correctamente. Si está en **Activado**, un dispositivo debe estar unido al dominio antes de iniciar BitLocker. El valor predeterminado es **Desactivado**.
- **Mensaje y URL de recuperación de prearranque:** Especifica si BitLocker muestra un mensaje y una URL personalizados en la pantalla de recuperación. Si está en **Activado**, aparecerán las siguientes configuraciones adicionales: **Usar mensaje y URL de**

recuperación predeterminados, **Usar mensaje y URL de recuperación vacíos**, **Usar mensaje de recuperación personalizado**, **Usar URL de recuperación personalizada** y **Usar mensaje y URL de recuperación de Citrix Endpoint Management**. Si está en **Desactivado**, se mostrarán el mensaje y la URL de recuperación predeterminados. El valor predeterminado es **Desactivado**.

- **Configuración de recuperación de unidades fijas:** Configura las opciones de recuperación para los usuarios de una unidad fija cifrada con BitLocker. BitLocker no muestra un mensaje a los usuarios sobre el cifrado de unidades fijas. Para desbloquear una unidad durante el inicio, un usuario proporciona una contraseña o una tarjeta inteligente. La configuración de desbloqueo de inicio, que no está en esta directiva, aparece en la interfaz de BitLocker cuando un usuario habilita el cifrado de BitLocker en una unidad fija. Para obtener información sobre la configuración relacionada, consulte **Configurar la recuperación de la unidad del SO**, anteriormente en esta lista. El valor predeterminado es **Desactivado**.
- **Configuración de unidades fijas**
    - **Bloquear el acceso de escritura a unidades fijas que no usan BitLocker:** Si está **Activado**, los usuarios solo pueden escribir en unidades fijas cuando estas están cifradas con BitLocker. El valor predeterminado es **Desactivado**.
- **Configuración de unidades extraíbles**
- **Bloquear el acceso de escritura a unidades extraíbles que no usan BitLocker:** Si está **Activado**, los usuarios solo pueden escribir en unidades extraíbles cuando estas están cifradas con BitLocker. Configure esta opción según si su organización permite el acceso de escritura en otras unidades extraíbles de la organización. El valor predeterminado es **Desactivado**.
- **Bloquear el acceso de escritura a otros dispositivos de la organización:** Si está **Activado**, los usuarios no pueden escribir en otros dispositivos de su organización, como una unidad de red.
- **Otra configuración de unidades**
- **Solicitar otro cifrado de disco:** Permite deshabilitar el mensaje de advertencia para otros cifrados de disco en los dispositivos. El valor predeterminado es **Desactivado**.

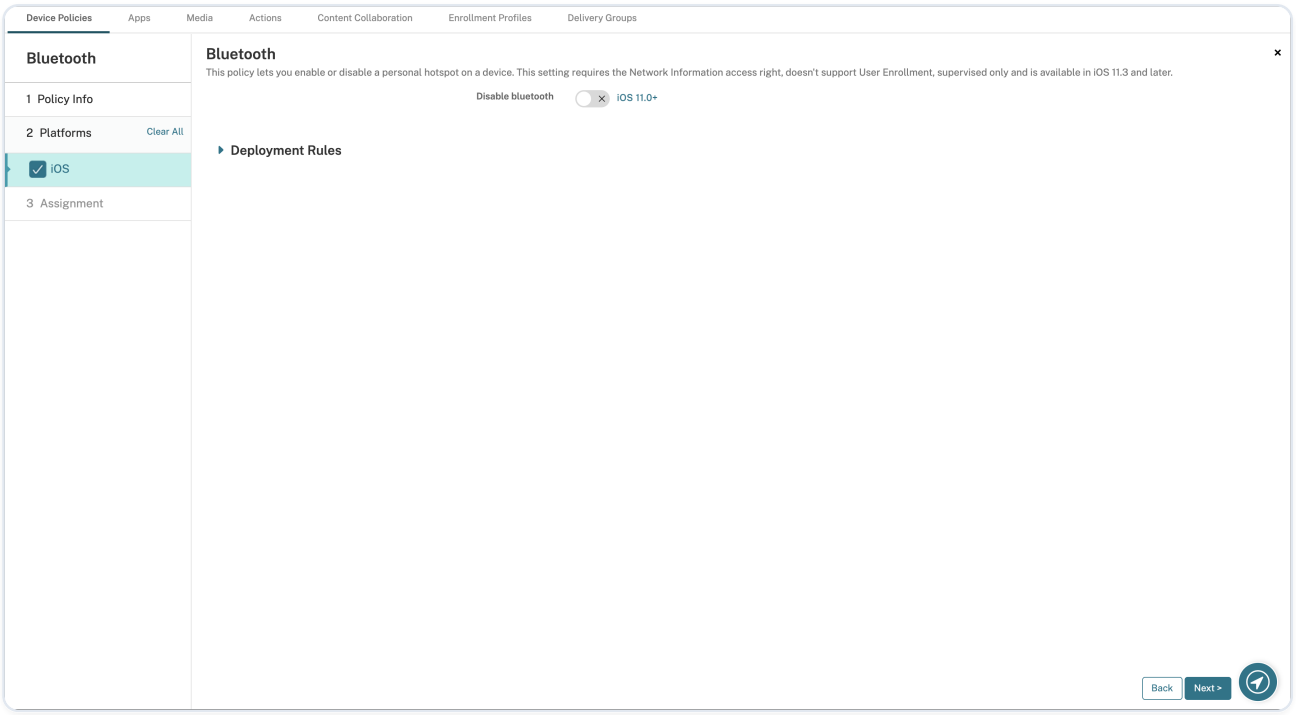
Directiva de dispositivo Bluetooth

Puede configurar una directiva de Bluetooth en dispositivos iOS supervisados para habilitar o deshabilitar Bluetooth.

Esta configuración requiere el derecho de acceso a la información de red, no admite la inscripción de usuarios y está disponible en iOS 11.3 y versiones posteriores.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivos**. Para obtener más información, consulte Directivas de dispositivos.

Configuración de iOS



- **Deshabilitar Bluetooth:** Permite deshabilitar o habilitar Bluetooth en el dispositivo supervisado.

Política de dispositivo de calendario (CalDav)

Puede agregar una política de dispositivo en Citrix Endpoint Management para añadir una cuenta de calendario (CalDAV) a los dispositivos iOS o macOS de los usuarios y permitirles sincronizar datos de programación con cualquier servidor compatible con CalDAV.

Para agregar o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

- **Descripción de la cuenta:** Escriba una descripción de la cuenta. Este campo es obligatorio.
- **Nombre de host:** Escriba la dirección del servidor CalDAV. Este campo es obligatorio.

- **Puerto:** Escriba el puerto al que conectarse al servidor CalDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **URL principal:** Escriba la URL base del calendario del usuario.
- **Nombre de usuario:** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Escriba una contraseña de usuario opcional.
- **Usar SSL:** Seleccione si desea usar una conexión Secure Socket Layer al servidor CalDAV. El valor predeterminado es **Activado**.
- **Configuración de la política**
  - **Eliminar política:** Elija un método para programar la eliminación de la política. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la política. Solo disponible para iOS 6.0 o posterior.

Configuración de macOS

- **Descripción de la cuenta:** Escriba una descripción de la cuenta. Este campo es obligatorio.
- **Nombre de host:** Escriba la dirección del servidor CalDAV. Este campo es obligatorio.
- **Puerto:** Escriba el puerto en el que conectarse al servidor CalDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **URL principal:** Escriba la URL base del calendario del usuario.
- **Nombre de usuario:** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Escriba una contraseña de usuario opcional.
- **Usar SSL:** Seleccione si desea usar una conexión Secure Socket Layer al servidor CalDAV. El valor predeterminado es **Activado**.
- **Configuración de directivas**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**

    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.

- **Permitir al usuario eliminar la directiva:** Puede seleccionar cuándo los usuarios pueden eliminar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**.
- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en macOS 10.7 y versiones posteriores.

Política de dispositivo celular

Esta política le permite configurar los ajustes de red celular en un dispositivo iOS.

Para añadir o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Ajustes de iOS

Puede usar macros en campos que no sean de cadena, como **Puerto del servidor proxy**.

Por ejemplo, puede usar una macro como `${device.xyz}` o `${setting.xyz}`, que se expande en un número entero. También puede usar las macros en un archivo XML de configuración de dispositivo que importe en Citrix Endpoint Management mediante la directiva de dispositivo **Importar perfil de iOS y macOS**.

- **Adjuntar APN**
    - **Nombre:** Un nombre para esta configuración.
    - **Tipo de autenticación:** Haga clic en Challenge Handshake Authentication Protocol (**CHAP**) o Password Authentication Protocol (**PAP**) en la lista desplegable. El valor predeterminado es **PAP**.
    - **Nombre de usuario** y **Contraseña:** El nombre de usuario y la contraseña que se utilizarán para la autenticación.
- **APN**

- **Nombre:** Un nombre para la configuración del Nombre de punto de acceso (APN).
- **Tipo de autenticación:** Haga clic en **CHAP** o **PAP** en la lista desplegable. El valor predeterminado es **PAP**.
- **Nombre de usuario** y **Contraseña:** El nombre de usuario y la contraseña que se utilizarán para la autenticación.
- **Servidor proxy:** La dirección de red del servidor proxy.
- **Puerto del servidor proxy:** El puerto del servidor proxy.

- **Configuración de la directiva**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.

Política de dispositivo de programación de conexiones

> **Importante:**
>
> Citrix recomienda utilizar Firebase Cloud Messaging (FCM) para controlar las conexiones de dispositivos Android y Android Enterprise a Citrix Endpoint Management. Para obtener información sobre el uso de FCM, consulte Firebase Cloud Messaging.
>
> Si decide no utilizar FCM, puede crear directivas de programación de conexiones para controlar cómo y cuándo se conectan los dispositivos de los usuarios a Citrix Endpoint Management. Si decide utilizar FCM, también debe crear una directiva de programación de conexiones.

Puede especificar que los usuarios conecten sus dispositivos manualmente o que los dispositivos se conecten dentro de un período de tiempo definido.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de Android y Android Enterprise

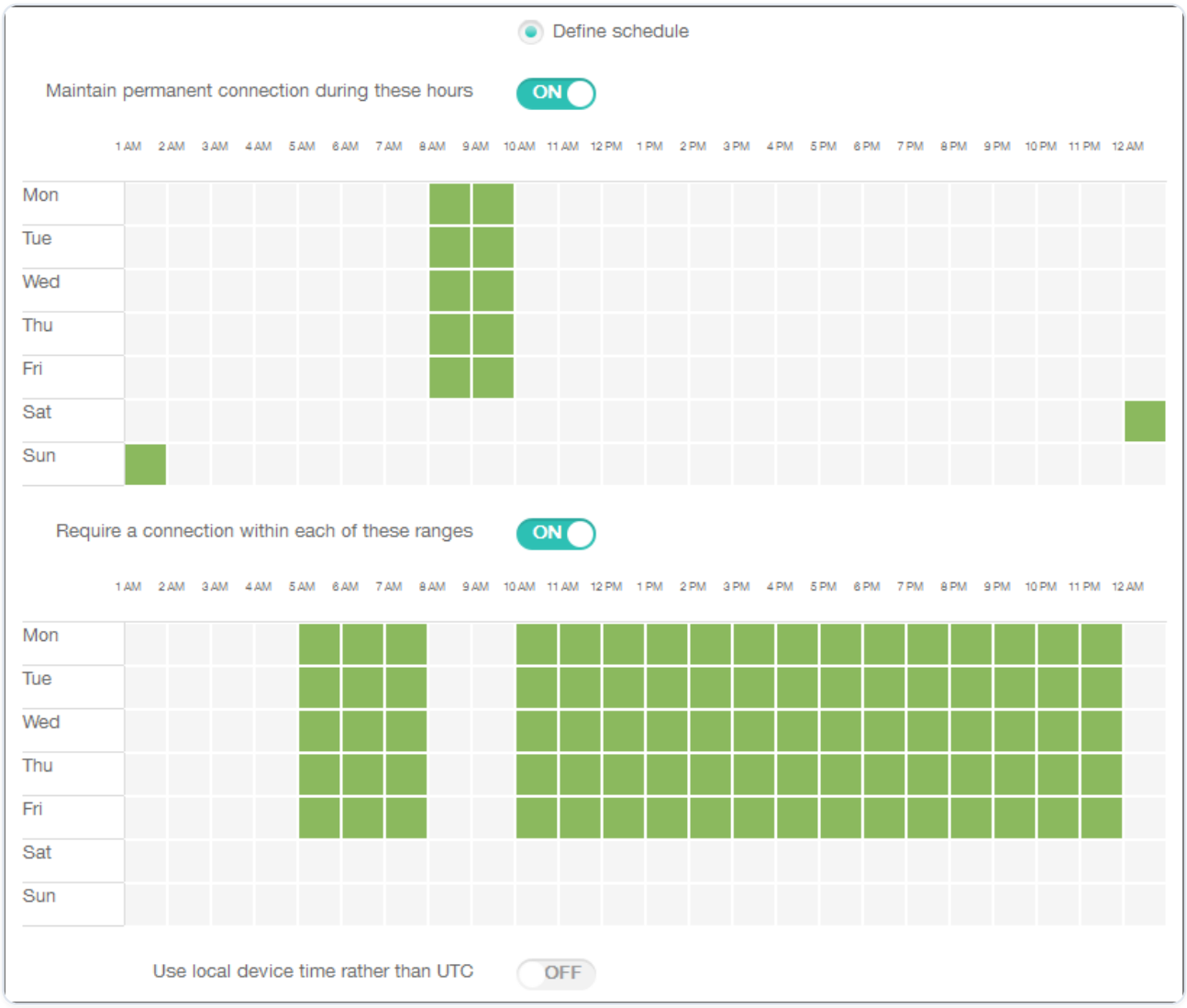
- **Requerir que los dispositivos se conecten:** Haga clic en la opción que desee establecer para esta programación.
    - **Nunca:** Conectarse manualmente. Los usuarios deben iniciar la conexión desde Citrix Endpoint Management en sus dispositivos. Citrix no recomienda esta opción para implementaciones de producción porque impide implementar directivas de seguridad en los dispositivos, lo que significa que los usuarios nunca recibirán nuevas aplicaciones ni directivas. La opción **Nunca** está habilitada de forma predeterminada.
    - **Cada:** Conectarse en el intervalo designado. Cuando esta opción está activa y se envía una directiva de seguridad, como un bloqueo o un borrado, Citrix Endpoint Management procesa la acción en el dispositivo la próxima vez que este se conecta. Al seleccionar esta opción, aparece el campo **Conectar cada N minutos**, donde debe introducir el número de minutos después de los cuales el dispositivo debe volver a conectarse. El valor predeterminado y mínimo es **120**.
    - **Definir programación:** Citrix Endpoint Management en el dispositivo del usuario intenta volver a conectarse al servidor de Citrix Endpoint Management después de una pérdida de conexión de red. Citrix Endpoint Management supervisa la conexión transmitiendo paquetes de control a intervalos regulares dentro del período de tiempo que defina. Consulte a continuación "Definir un período de tiempo de conexión" para saber cómo definir un período de tiempo de conexión.
        - **Requerir una conexión dentro de cada uno de estos rangos:** Los dispositivos de los usuarios deben estar conectados al menos una vez en cualquiera de los períodos de tiempo definidos.
        - **Usar la hora local del dispositivo en lugar de UTC:** Sincronizar los períodos de tiempo definidos con la hora local del dispositivo en lugar de la hora universal coordinada (UTC).

Definir un período de tiempo de conexión

Al habilitar las siguientes opciones, aparece una línea de tiempo donde puede definir los períodos de tiempo que desee. Puede habilitar una o ambas opciones para requerir una conexión permanente durante horas específicas o para requerir una conexión dentro de ciertos períodos de tiempo. Cada cuadrado de la línea de tiempo representa 1 hora. Para especificar una conexión entre las 8:00 AM y las 9:00 AM todos los días de la semana, haga clic en el cuadrado de la línea de tiempo entre las 8 AM y las 9 AM todos los días de la semana.

Por ejemplo, las dos líneas de tiempo de la siguiente figura requieren:

- Una conexión permanente entre las 8:00 AM y las 10:00 AM todos los días laborables
- Una conexión permanente entre la 1:00 AM del sábado y las 2:00 AM del domingo
- Al menos una conexión todos los días laborables entre las 5:00 AM y las 8:00 AM o entre las 10:00 AM y las 12:00 AM



Directiva de dispositivo de contactos (CardDAV)

Puede añadir una directiva de dispositivo en Citrix Endpoint Management para añadir una cuenta de contactos (CardDAV) de iOS a los dispositivos iOS o macOS de los usuarios, lo que les permite sincronizar los datos de contacto con cualquier servidor compatible con CardDAV.

Para añadir o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

- **Descripción de la cuenta:** Escriba una descripción de la cuenta. Este campo es obligatorio.
- **Nombre de host:** Escriba la dirección del servidor CardDAV. Este campo es obligatorio.
- **Puerto:** Escriba el puerto en el que conectarse al servidor CardDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **URL principal:** Escriba la URL base del calendario del usuario.
- **Nombre de usuario:** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Escriba una contraseña de usuario opcional.
- **Usar SSL:** Seleccione si desea utilizar una conexión Secure Socket Layer al servidor CardDAV. El valor predeterminado es **Activado**.
- **Configuración de la directiva**
    - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
        - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
        - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.

Configuración de macOS

- **Descripción de la cuenta:** Escriba una descripción de la cuenta. Este campo es obligatorio.
- **Nombre de host:** Escriba la dirección del servidor CardDAV. Este campo es obligatorio.
- **Puerto:** Escriba el puerto al que conectarse en el servidor CardDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **URL principal:** Escriba la URL base del calendario del usuario.
- **Nombre de usuario:** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Escriba una contraseña de usuario opcional.
- **Usar SSL:** Seleccione si desea utilizar una conexión Secure Socket Layer con el servidor CardDAV. El valor predeterminado es **Activado**.
- **Configuración de la directiva**

- **Quitar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
  - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
  - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.
- **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo pueden los usuarios quitar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso para la eliminación**.
- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en macOS 10.7 y versiones posteriores.

Directiva de dispositivo de credenciales

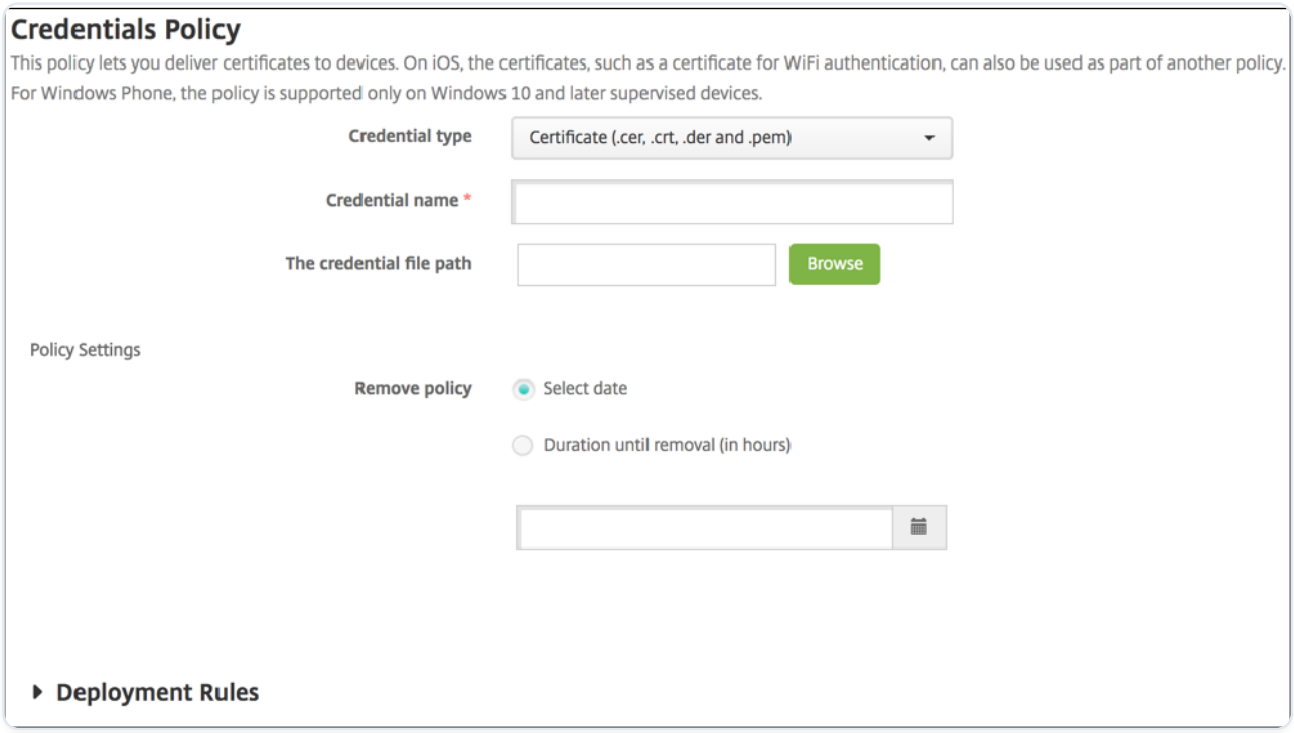
Las directivas de dispositivo de credenciales apuntan a una PKI configurada en Citrix Endpoint Management. Por ejemplo, la configuración de su PKI podría incluir una entidad PKI, un almacén de claves, un proveedor de credenciales o un certificado de servidor. Para obtener más información sobre las credenciales, consulte (/es-es/citrix-endpoint-management/authentication.html).

Cada plataforma compatible requiere un conjunto diferente de valores, que se describen en este artículo.

> **Nota:**
>
> Antes de crear esta directiva, necesita la información de credenciales que piensa usar para cada plataforma, además de los certificados y contraseñas.

> Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte (/es-es/citrix-endpoint-management/policies.html).

Configuración de iOS



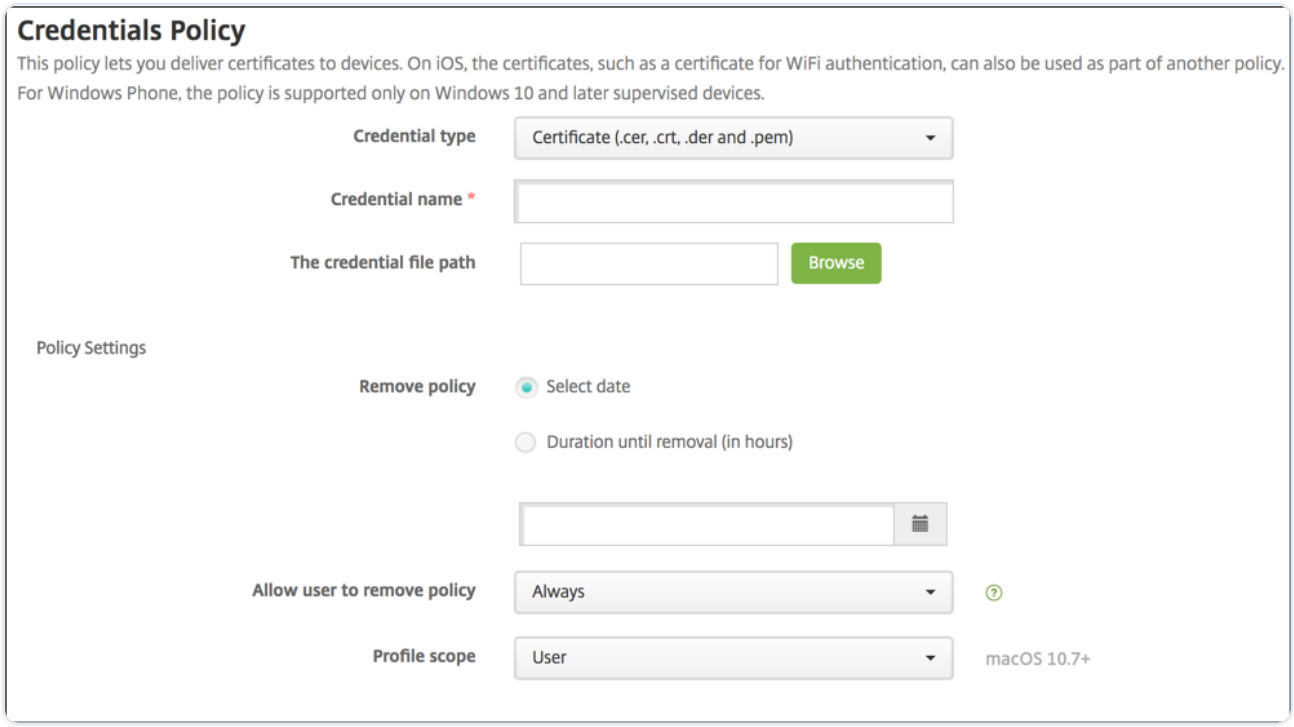
Configure los siguientes parámetros:

- **Tipo de credencial:** Haga clic en el tipo de credencial de la lista desplegable que desea usar con esta directiva y, a continuación, introduzca la siguiente información para la credencial seleccionada:
  - **Certificado**
    - **Nombre de credencial:** Introduzca un nombre único para la credencial.
    - **Ruta del archivo de credenciales:** Seleccione el archivo de credenciales haciendo clic en Examinar y navegando hasta la ubicación del archivo.
  - **Almacén de claves**
    - **Nombre de credencial:** Introduzca un nombre único para la credencial.
    - **La ruta del archivo de credenciales:** Seleccione el archivo de credenciales haciendo clic en Examinar y navegando hasta la ubicación del archivo.
    - **Contraseña:** Introduzca la contraseña del almacén de claves para la credencial.
  - **Certificado de servidor**
    - **Certificado de servidor:** Haga clic en el certificado de la lista desplegable que desea utilizar.
  - **Proveedor de credenciales**

  - **Proveedor de credenciales:** Haga clic en el nombre del proveedor de credenciales en la lista desplegable.

- **Configuración de la directiva**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.
  - **Permitir al usuario eliminar la directiva:** Puede seleccionar cuándo los usuarios pueden eliminar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**. No disponible para iOS.

Configuración de macOS



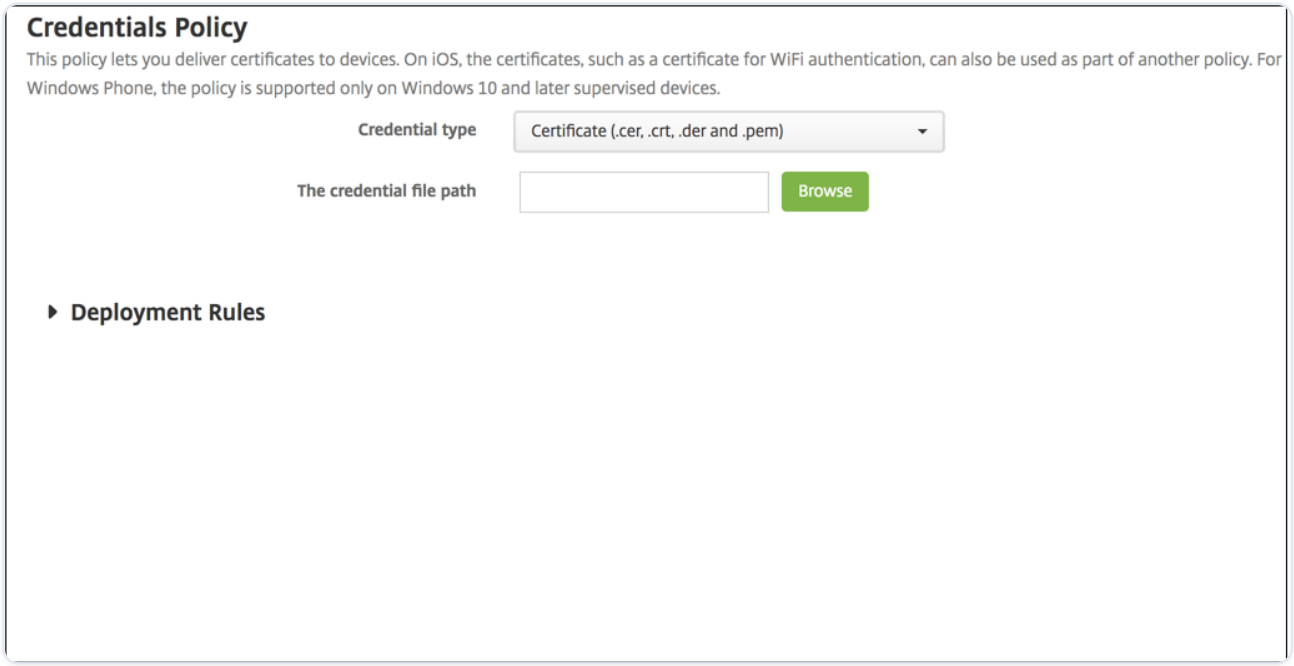
Configure los siguientes ajustes:

- **Tipo de credencial:** Haga clic en el tipo de credencial de la lista desplegable que desea utilizar con esta directiva y, a continuación, introduzca la siguiente información para la credencial seleccionada:

- **Certificado**
  - **Nombre de la credencial:** Introduzca un nombre único para la credencial.
  - **Ruta del archivo de credenciales:** Seleccione el archivo de credenciales haciendo clic en **Examinar** y navegando hasta la ubicación del archivo.
- **Almacén de claves**
  - **Nombre de la credencial:** Introduzca un nombre único para la credencial.
  - **Ruta del archivo de credenciales:** Seleccione el archivo de credenciales haciendo clic en **Examinar** y navegando hasta la ubicación del archivo.
  - **Contraseña:** Introduzca la contraseña del almacén de claves para la credencial.
- **Certificado de servidor**
  - **Certificado de servidor:** Haga clic en el certificado de la lista desplegable que desee utilizar.
- **Proveedor de credenciales**
  - **Proveedor de credenciales:** Haga clic en el nombre del proveedor de credenciales en la lista desplegable.

- **Configuración de directivas**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.
  - **Permitir al usuario eliminar la directiva:** Puede seleccionar cuándo los usuarios pueden eliminar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en macOS 10.7 y versiones posteriores.

Configuración de Android

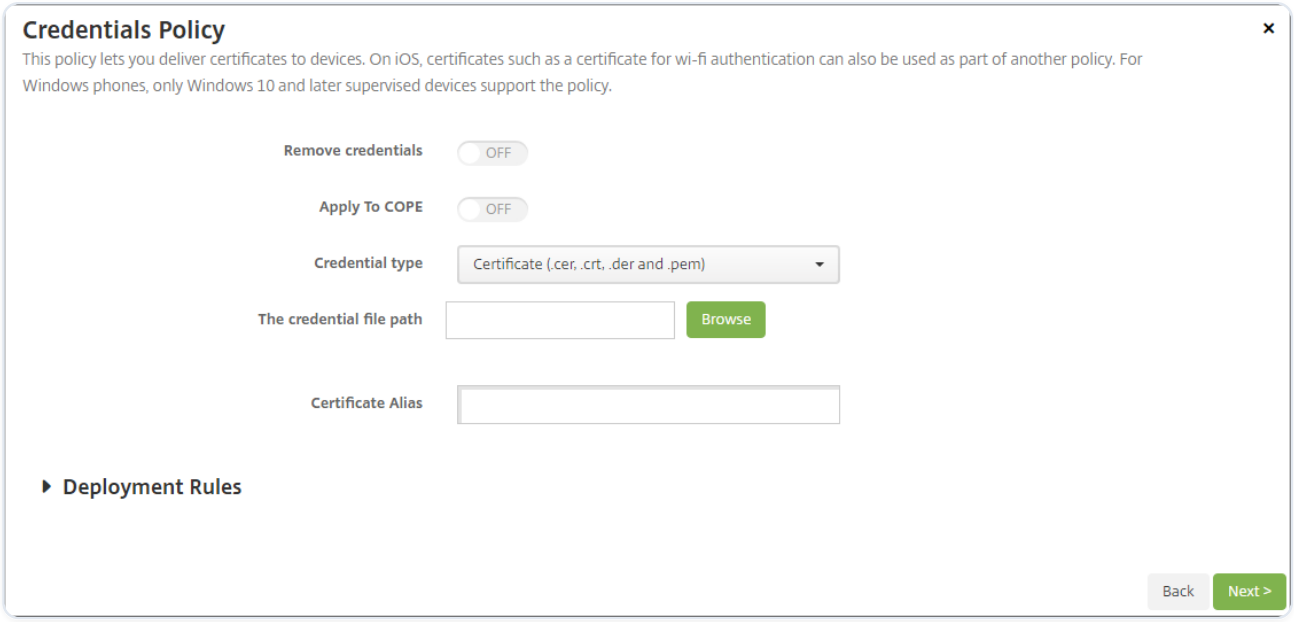


Configure los siguientes ajustes:

- **Tipo de credencial:** Haga clic en el tipo de credencial de la lista desplegable que desea usar con esta directiva y, a continuación, introduzca la siguiente información para la credencial seleccionada:
  - **Certificado**
    - **Nombre de la credencial:** Escriba un nombre único para la credencial.
    - **Ruta del archivo de credenciales:** Seleccione el archivo de credenciales haciendo clic en Examinar y, a continuación, navegando hasta la ubicación del archivo.
  - **Almacén de claves**
    - **Nombre de la credencial:** Escriba un nombre único para la credencial.
    - **Ruta del archivo de credenciales:** Seleccione el archivo de credenciales haciendo clic en **Examinar** y, a continuación, navegando hasta la ubicación del archivo.
    - **Contraseña:** Escriba la contraseña del almacén de claves para la credencial.
  - **Certificado de servidor**
    - **Certificado de servidor:** Haga clic en el certificado de la lista desplegable que desea usar.
  - **Proveedor de credenciales**

- **Proveedor de credenciales:** Haga clic en el nombre del proveedor de credenciales en la lista desplegable.

Configuración de Android Enterprise



Configure estos ajustes para determinar cómo se aplican los ajustes de credenciales:

- **Quitar credenciales:** Establezca en **Activado** para configurar los siguientes ajustes. El valor predeterminado es **Desactivado**.
  - **Quitar credenciales de usuario:** Quita los certificados del almacén de claves administrado. El valor predeterminado es **Desactivado**.
  - **Quitar certificados raíz de confianza:** Desinstala todos los certificados de CA que no son del sistema. El valor predeterminado es **Desactivado**.
- **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos corporativos:** Permite configurar los ajustes de la directiva de credenciales para dispositivos totalmente administrados con perfiles de trabajo. Cuando este ajuste está establecido en **Activado**, seleccione uno de estos ajustes. Esta directiva se aplica únicamente al perfil de trabajo en los dispositivos.

Configure los ajustes de credenciales:

- **Tipo de credencial:** Haga clic en el tipo de credencial de la lista desplegable que desea usar con esta directiva y, a continuación, introduzca la siguiente información para la credencial seleccionada:
  - **Certificado**

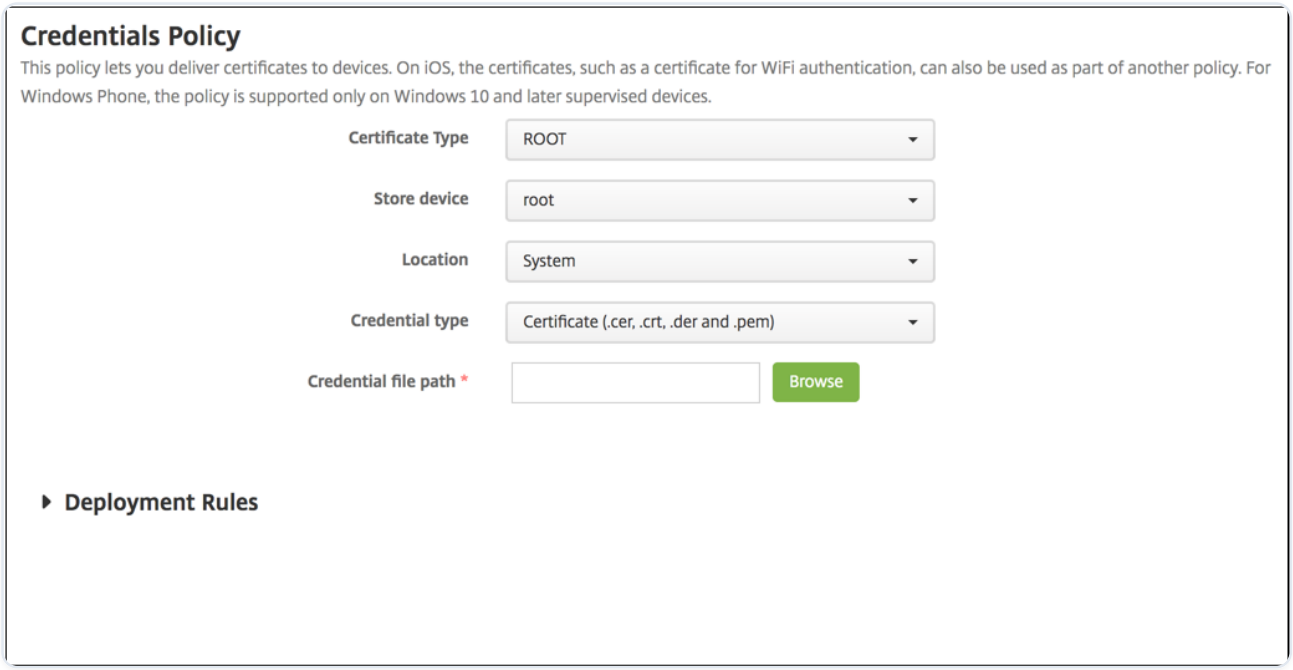
- **Nombre de la credencial:** Escriba un nombre único para la credencial.
- **Ruta del archivo de credenciales:** Seleccione el archivo de credenciales haciendo clic en **Examinar** y, a continuación, navegando hasta la ubicación del archivo.

- **Almacén de claves**
  - **Nombre de la credencial:** Escriba un nombre único para la credencial.
  - **Ruta del archivo de credenciales:** Seleccione el archivo de credenciales haciendo clic en **Examinar** y, a continuación, vaya a la ubicación del archivo.
  - **Contraseña:** Escriba la contraseña del almacén de claves para la credencial.
  - **Alias del certificado:** Un alias de certificado facilita a las aplicaciones el acceso al certificado. Configure un alias de certificado en la directiva de dispositivo de configuración administrada de Android Enterprise. A continuación, escriba el alias en el campo **Alias del certificado** de la directiva de dispositivo Credenciales. Las aplicaciones recuperan el certificado y autentican la VPN sin ninguna acción por parte de los usuarios.

- **Certificado de servidor**
  - **Certificado de servidor:** Haga clic en el certificado de la lista desplegable que quiera usar.

- **Proveedor de credenciales**
  - **Proveedor de credenciales:** Haga clic en el nombre del proveedor de credenciales de la lista desplegable.
  - **Aplicaciones para usar certificados:** Para especificar las aplicaciones que tienen acceso silencioso a las credenciales de este proveedor: Haga clic en **Agregar**, seleccione una aplicación y haga clic en **Guardar**.
  - **Alias del certificado:** Un alias de certificado facilita a las aplicaciones el acceso al certificado. Configure un alias de certificado en la directiva de dispositivo de configuración administrada de Android Enterprise. A continuación, escriba el alias en el campo **Alias del certificado** de la directiva de dispositivo Credenciales. Las aplicaciones recuperan el certificado y autentican la VPN sin ninguna acción por parte de los usuarios.

Configuración de equipos de escritorio/tabletas Windows



- **Tipo de certificado:** Haga clic en **ROOT** o **CLIENT** en la lista desplegable.
- Si hace clic en **ROOT**, configure estos parámetros:
  - **Almacenar dispositivo:** Haga clic en **root**, **My** o **CA** en la lista desplegable para la ubicación del almacén de certificados de la credencial. **My** almacena el certificado en los almacenes de certificados de los usuarios.
  - **Ubicación:** Para tabletas con Windows 10 y Windows 11, **Sistema** es la única ubicación.
  - **Tipo de credencial:** Para tabletas con Windows 10 y Windows 11, **Certificado** es el único tipo de credencial.
  - **Ruta de acceso del archivo de credenciales:** Seleccione el archivo de certificado haciendo clic en **Examinar** y navegando hasta la ubicación del archivo.
- Si hace clic en **CLIENTE**, configure estos ajustes:
- **Ubicación:** Para tabletas con Windows 10 y Windows 11, **Sistema** es la única ubicación.
- **Tipo de credencial:** Para tabletas con Windows 10 y Windows 11, **Almacén de claves** es el único tipo de credencial.
- **Nombre de la credencial:** Escriba el nombre de la credencial. Este campo es obligatorio.
- **Ruta de acceso del archivo de credenciales:** Seleccione el archivo de certificado haciendo clic en **Examinar** y navegando hasta la ubicación del archivo.
- **Contraseña:** Escriba la contraseña asociada a la credencial. Este campo es obligatorio.

Directiva de dispositivo XML personalizada

Puede crear directivas XML personalizadas en Citrix Endpoint Management para personalizar las siguientes funciones en los dispositivos Windows compatibles:

- Aprovisionamiento, que incluye la configuración del dispositivo y la habilitación o deshabilitación de funciones
- Configuración del dispositivo, que incluye permitir a los usuarios cambiar la configuración y los parámetros del dispositivo
- Actualizaciones de software, que incluyen el suministro de nuevo software o correcciones de errores para cargar en el dispositivo, incluidas las aplicaciones y el software del sistema
- Gestión de fallos, que incluye la recepción de informes de errores y estado del dispositivo

> **Nota:**

> Al crear su contenido XML, utilice el carácter \% con precaución. El carácter \% es un carácter reservado de XML, utilizado únicamente para escapar caracteres especiales de XML. Para usar \% en un nombre, codifíquelo como \%25.

> Para dispositivos Windows: Cree su configuración XML personalizada mediante la API Open Mobile Alliance Device Management (OMA DM) en Windows. La creación de XML personalizado con la API OMA DM está fuera del alcance de este tema. Para obtener más información sobre el uso de la API OMA DM, consulte Soporte del protocolo OMA DM en el sitio de Microsoft Developer Network.

Para dispositivos Android Enterprise: Cree su configuración XML personalizada mediante el sistema de administración MX (MXMS). La creación de XML personalizado con la API MXMS está fuera del alcance de este artículo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte (/es-es/citrix-endpoint-management/policies.html).

Configuración de equipos de escritorio/tabletas Windows

Contenido XML: Escriba o copie y pegue el código XML personalizado que desea agregar a la directiva.

Después de hacer clic en **Siguiente**, Citrix Endpoint Management comprueba la sintaxis del contenido XML. Cualquier error de sintaxis aparece debajo del cuadro de contenido. Corrija los errores antes de continuar.

Si no hay errores de sintaxis, aparece la página de asignación de la **directiva XML personalizada**.

Usar Windows AutoPilot para configurar dispositivos

Windows AutoPilot es un conjunto de tecnologías que se utilizan para configurar y preconfigurar dispositivos nuevos, preparándolos para un uso productivo. Puede usar Windows AutoPilot para restablecer, reasignar y recuperar dispositivos. AutoPilot ayuda a eliminar parte de la complejidad de la implementación actual de su sistema operativo. El uso de AutoPilot reduce la tarea a un conjunto de configuraciones y operaciones sencillas que pueden dejar sus dispositivos listos para usar de forma rápida y eficiente.

Para obtener una breve descripción general del uso de Windows AutoPilot con Citrix Endpoint Management, vea este vídeo.

<iframe src="https://www.youtube.com/embed/DFCeF68NXM0" width="720px" height="480px" frameborder="0" title="YouTube video player" allowfullscreen=""> </iframe>

Requisitos previos

- Marca de la empresa configurada en el portal de Azure Active Directory.
- La empresa tiene una suscripción a Azure Active Directory Premium P1 o P2.
- Configure Azure Active Directory como el tipo de IdP para Citrix Endpoint Management. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Proveedor de identidades (IdP)**.
- Conectividad de red a los servicios en la nube utilizados por Windows AutoPilot.
- Dispositivos con Windows 10 Professional, Enterprise o Education (versión 1703 o posterior) o Windows 11 Professional, Enterprise o Education preinstalado.
- Los dispositivos tienen acceso a Internet.

Para obtener más información sobre la configuración de los requisitos previos, consulte la documentación de Microsoft Windows sobre AutoPilot: `<https://docs.microsoft.com>`.

Para configurar la reimplementación automática de Windows en Citrix Endpoint Management para dispositivos AutoPilot

1. Siga los pasos para agregar una directiva XML personalizada en la Directiva de dispositivo XML personalizada. Agregue lo siguiente en **Contenido XML:**

```
<Add>
<CmdID>_cmdid_</CmdID>
<Item>
<Target>
<LocURI>./Vendor/MSFT/Policy/Config/CredentialProviders/
DisableAutomaticReDeploymentCredentials</LocURI>
</Target>
<Meta>
<Format xmlns="syncml:metinf">int</Format>
</Meta>
<Data>0</Data>
</Item>
</Add>
```

2. En la pantalla de bloqueo de Windows, escriba la combinación de teclas **CTRL + tecla de Windows + R**.
3. Inicie sesión con una cuenta de Azure Active Directory.
4. El dispositivo verifica que el usuario tiene derecho a volver a implementar el dispositivo. A continuación, el dispositivo se vuelve a implementar.
5. Después de que el dispositivo se actualice con la configuración de AutoPilot, el usuario puede iniciar sesión en el dispositivo recién configurado.

Implementar un quiosco de una sola aplicación en dispositivos Windows 11

> **Nota:**
>
> Los dispositivos Windows 11 solo admiten el modo Quiosco de una sola aplicación.

En el cuadro de texto **Contenido XML**, copie y pegue el siguiente script XML y, a continuación, reemplace las siguientes cadenas por su configuración:

- `your_username_here` (dos instancias): nombre de usuario que quiere crear en el dispositivo. Mantenga la misma configuración para ambas instancias.
- `your password_here`: contraseña del usuario.
- `your_UWP_app_id_here`: AUMID de la aplicación UMP que quiere implementar en el dispositivo.

Script XML:

```
<Add>
    <CmdID>_cmdid_</CmdID>
    <Item>
        <Target>
            <LocURI>./Device/Vendor/MSFT/Accounts/Users/
your_username_here/Password</LocURI>
        </Target>
        <Meta>
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data>your_password_here</Data>
```

```
    </Item>
</Add>
<Replace>
    <CmdID>_cmdid_</CmdID>
    <Item>
        <Target>
            <LocURI>./Device/Vendor/MSFT/AssignedAccess/Configuration</
LocURI>
        </Target>
        <Meta>
            <Format xmlns="syncml:metinf">chr</Format>
        </Meta>
        <Data><![CDATA[<AssignedAccessConfiguration
        xmlns="http://schemas.microsoft.com/AssignedAccess/2017/config"
        xmlns:rs5="http://schemas.microsoft.com/AssignedAccess/201810/
config">
            <Profiles>
                <Profile Id="{AFF9DA33-AE89-4039-B646-3A5706E92957}">
                    <KioskModeApp AppUserModelId="your_UWP_app_id_here"/>
                </Profile>
            </Profiles>
            <Configs>
                <Config>
```

```
                    <Account>your_username_here</Account>

                    <DefaultProfile Id="{AFF9DA33-AE89-4039-
B646-3A5706E92957}"/>

                </Config>

            </Configs>

        </AssignedAccessConfiguration>]]></Data>

    </Item>

</Replace>
```

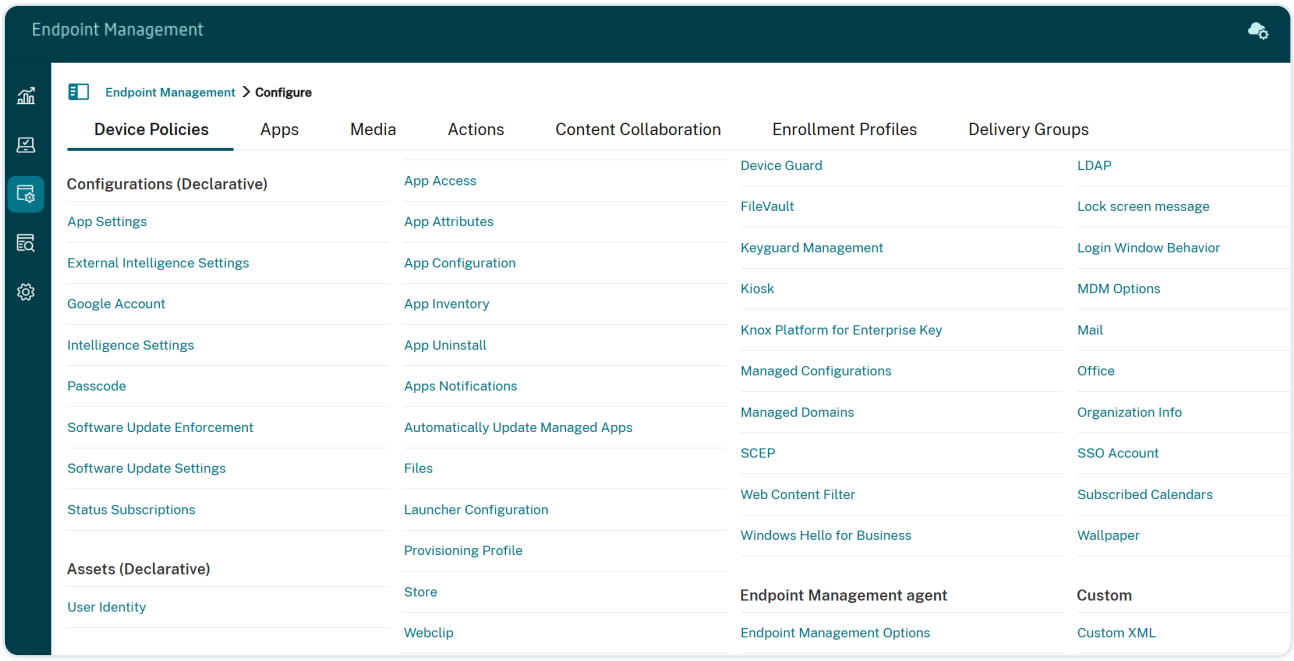
Directivas de gestión declarativa de dispositivos

Apple ha anunciado la gestión declarativa de dispositivos (DDM) en iOS 15, utilizando un paradigma de modelo de datos declarativo. Este paradigma permite a los servidores evitar los problemas comunes de rendimiento y escalabilidad asociados normalmente con la serialización de comandos y el sondeo de dispositivos a través de MDM. Para obtener más información, consulte Aprovechar el modelo de datos de gestión declarativa para escalar dispositivos.

Citrix Endpoint Management™ ahora es compatible con DDM para adoptar las últimas funciones que ofrece Apple.

Se admiten las siguientes directivas declarativas de dispositivos cuando habilita la función DDM:

- Configuración de aplicaciones
- Configuración de inteligencia externa
- Cuenta de Google
- Configuración de inteligencia
- Directiva de código de acceso del dispositivo
- Aplicación de actualizaciones de software
- Configuración de actualizaciones de software
- Suscripciones de estado
- Identidad de usuario



Política de dispositivo de configuración de aplicaciones

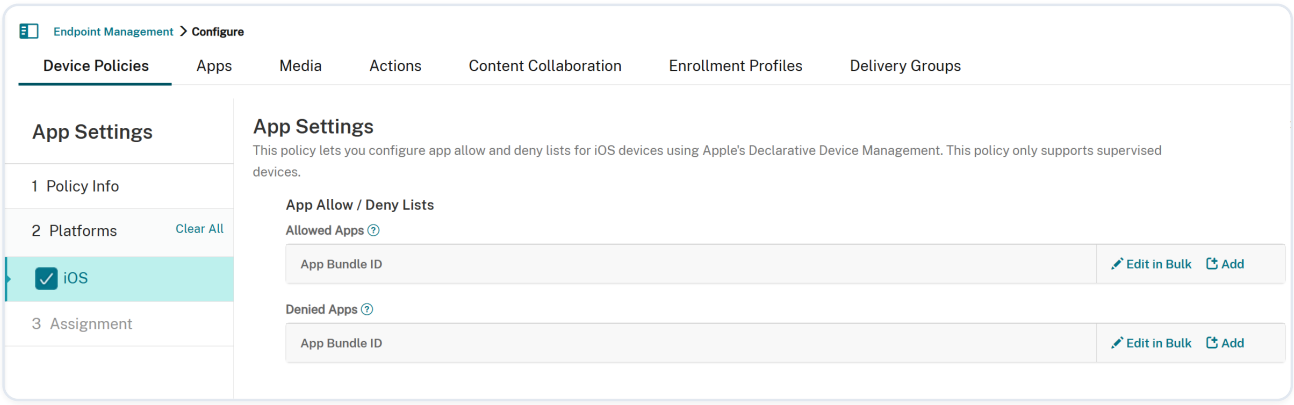
La política de dispositivo de configuración de aplicaciones le permite configurar listas de aplicaciones permitidas y denegadas mediante la gestión declarativa de dispositivos de Apple. Reemplaza las claves de restricción obsoletas `allowListedAppBundleIDs` y `blockedAppBundleIDs`. Esta política solo es compatible con dispositivos supervisados.

Para añadir o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

- La versión de CEM es igual o superior a la **26.8.0**.
- Disponible para **iOS 27** o posterior y **iPadOS 27** o posterior, solo es compatible con dispositivos supervisados.

Configuración de iOS



- **Listas de aplicaciones permitidas/denegadas**
  - **Aplicaciones permitidas:** Si está presente, el dispositivo solo muestra o inicia aplicaciones con ID de paquete en la lista. Incluya el valor `com.apple.webapp` para permitir todos los webclips. Esto se aplica a las aplicaciones de App Store, las aplicaciones de marketplace y las aplicaciones instaladas localmente (mediante Configurator, Xcode, etc.).
    - **ID de paquete de aplicación:** Para añadir un ID de paquete de aplicación, haga clic en **Añadir**, escriba un ID de paquete de aplicación y haga clic en **Guardar**. Repita ese proceso para cada ID de paquete de aplicación que desee añadir. También puede hacer clic en **Editar en bloque**, introducir o pegar ID de paquete de aplicación, uno por línea o separados por comas, y hacer clic en **Guardar**.
  - **Aplicaciones denegadas:** Si está presente, el dispositivo impide mostrar o iniciar aplicaciones con ID de paquete en la lista. Incluya el valor `com.apple.webapp` para restringir todos los webclips. Esto se aplica a las aplicaciones de App Store, las aplicaciones de marketplace y las aplicaciones instaladas localmente (mediante Configurator, Xcode, etc.).

> **Nota:**
>
> Denegar aplicaciones del sistema puede deshabilitar otras funcionalidades. Por ejemplo, denegar la aplicación App Store puede impedir que los usuarios acepten los términos y condiciones del Programa de compra por volumen (VPP) basado en el usuario. Le recomendamos que configure la lista de aplicaciones permitidas o la lista de aplicaciones denegadas, pero no ambas.

Política de dispositivo de configuración de inteligencia externa

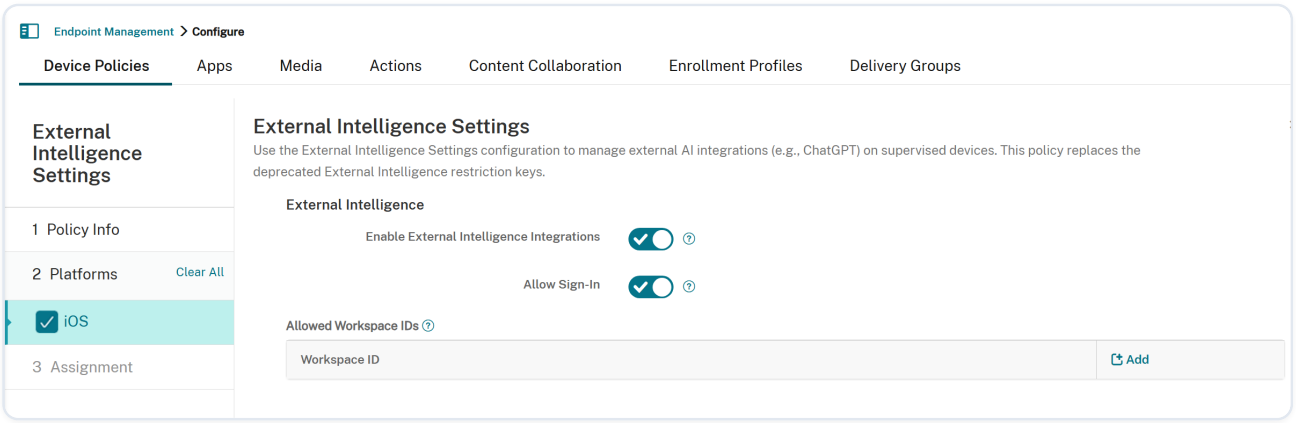
La política de dispositivo de configuración de inteligencia externa le permite gestionar integraciones de IA externas (por ejemplo, ChatGPT) mediante la gestión declarativa de dispositivos de Apple. Esta política reemplaza las claves de restricción de inteligencia externa obsoletas. Esta política solo es compatible con dispositivos supervisados.

Para añadir o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

- La versión de CEM es igual o superior a **26.8.0**.
- Disponible para **iOS 26.4** o posterior y **iPadOS 26.4** o posterior, solo es compatible con dispositivos supervisados.

Configuración de iOS



- **Inteligencia externa**
  - **Habilitar integraciones de inteligencia externa:** Si está en **Desactivado**, deshabilita las integraciones de inteligencia externa. El valor predeterminado es **Activado**.
  - **Permitir inicio de sesión:** Si está en **Desactivado**, deshabilita el inicio de sesión para las integraciones de inteligencia externa. El valor predeterminado es **Activado**.
  - **ID de espacios de trabajo permitidos:** Una matriz de cadenas, pero actualmente restringida a un solo elemento. Si está presente, Apple Intelligence permite el uso de solo el ID de espacio de trabajo de integración externa dado y requiere un inicio de sesión para realizar solicitudes. Se requiere que el usuario inicie sesión en las integraciones que admiten el inicio de sesión. Varios valores se combinan mediante una operación de intersección.
    - **ID de espacio de trabajo:** Para añadir un ID de espacio de trabajo de inteligencia externa, haga clic en **Añadir**, escriba un ID de espacio de trabajo y haga clic en **Guardar**. Repita ese proceso para cada ID de espacio de trabajo que desee añadir.

Política de dispositivo de cuenta de Google

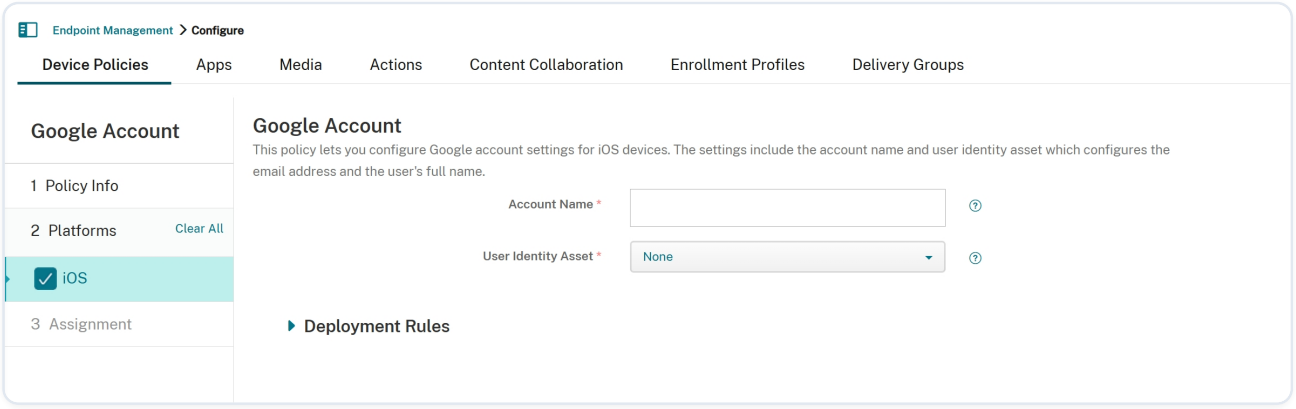
La política de dispositivo de cuenta de Google le permite configurar los ajustes de la cuenta de Google para dispositivos iOS. Los ajustes incluyen el nombre de la cuenta y el recurso de identidad de usuario que configura la dirección de correo electrónico y el nombre completo del usuario.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

- La versión de CEM es igual o superior a **25.5.0**.
- La política de identidad de usuario está configurada. Consulte Política de dispositivo de identidad de usuario.

Configuración de iOS



- **Nombre de la cuenta:** Escriba el nombre de la cuenta de Google.
- **Recurso de identidad de usuario:** En la lista, seleccione el recurso de identidad de usuario creado por la política de identidad de usuario, que contiene la dirección de correo electrónico y el nombre completo del usuario. El valor predeterminado es **Ninguno**.

Directiva de dispositivo de ajustes de inteligencia

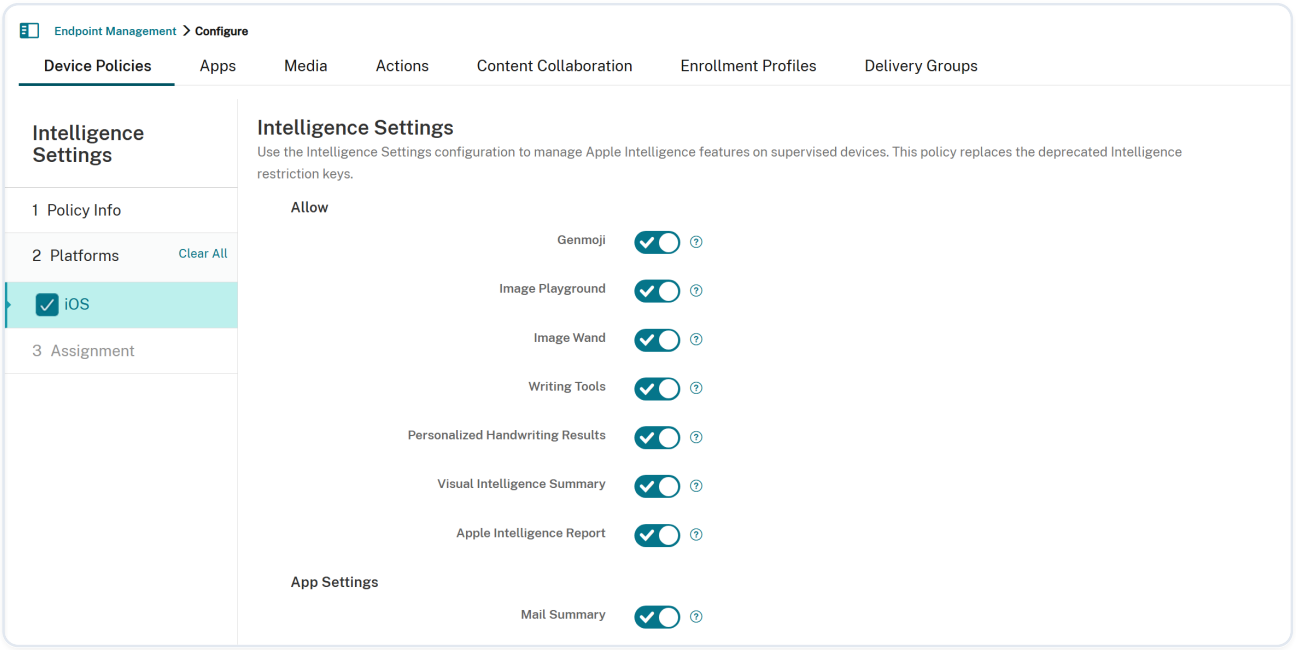
La directiva de dispositivo de ajustes de inteligencia le permite administrar las funciones de Apple Intelligence mediante la Administración declarativa de dispositivos de Apple. Esta directiva reemplaza las claves de restricción de inteligencia obsoletas. Esta directiva solo admite dispositivos supervisados.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

- La versión de CEM es igual o superior a **26.8.0**.
- Disponible para **iOS 26.4** o posterior y **iPadOS 26.4** o posterior, solo admite dispositivos supervisados.

Ajustes de iOS



- **Permitir**
  - **Genmoji:** Si está **Desactivado**, deshabilita Genmoji. El valor predeterminado es **Activado**.
  - **Image Playground:** Si está **Desactivado**, deshabilita Image Playground. El valor predeterminado es **Activado**.
  - **Image Wand:** Si está **Desactivado**, deshabilita Image Wand. El valor predeterminado es **Activado**.
  - **Writing Tools:** Si está **Desactivado**, deshabilita las herramientas de escritura de Apple Intelligence. El valor predeterminado es **Activado**.
  - **Resultados de escritura a mano personalizados:** Si está **Desactivado**, deshabilita los resultados de escritura a mano personalizados e impide que el sistema genere texto con la escritura del usuario. El valor predeterminado es **Activado**.
  - **Resumen de inteligencia visual:** Si está **Desactivado**, deshabilita la función de resumen de inteligencia visual. El valor predeterminado es **Activado**.
  - **Informe de Apple Intelligence:** Si está **Desactivado**, deshabilita el Informe de Apple Intelligence. El valor predeterminado es **Activado**.
- **Configuración de la aplicación**
  - **Resumen de correo:** Si está **Desactivado**, deshabilita el Resumen de correo. El valor predeterminado es **Activado**.
  - **Respuestas inteligentes de correo:** Si está **Desactivado**, deshabilita las Respuestas inteligentes de correo. El valor predeterminado es **Activado**.

  - **Transcripción de notas:** Si está **Desactivado**, deshabilita la Transcripción de notas. El valor predeterminado es **Activado**.
  - **Resumen de transcripción de notas:** Si está **Desactivado**, deshabilita el Resumen de transcripción de notas. El valor predeterminado es **Activado**.
  - **Resumen de Safari:** Si está **Desactivado**, deshabilita el Resumen de Safari. El valor predeterminado es **Activado**.

- **Forzar**
  - **Forzar dictado solo en el dispositivo:** Si está **Activado**, fuerza el dictado solo en el dispositivo. El valor predeterminado es **Desactivado**.
  - **Forzar traducción solo en el dispositivo:** Si está **Activado**, fuerza la traducción solo en el dispositivo. El valor predeterminado es **Desactivado**.

Política de dispositivo de código de acceso

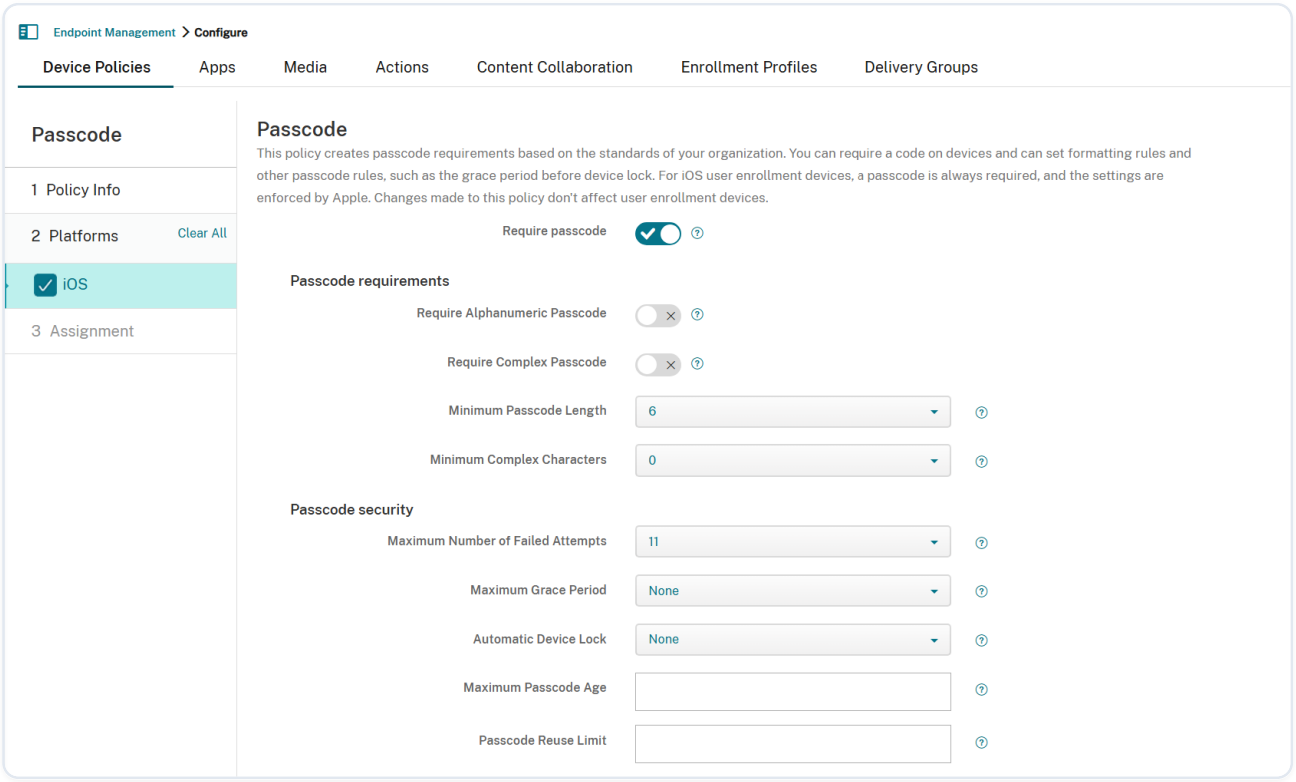
La política de dispositivo de código de acceso crea requisitos de código de acceso basados en los estándares de su organización. Puede exigir un código en los dispositivos y establecer reglas de formato y otras reglas de código de acceso, como el período de gracia antes del bloqueo del dispositivo.

Para agregar o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

- La versión de CEM es igual o superior a **25.5.0**.

Configuración de iOS



- **Requerir código de acceso:** Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una política de dispositivo de código de acceso de iOS. Si está en **Activado**, requiere que el usuario establezca un código de acceso sin requisitos sobre la longitud o la calidad del código de acceso, y la página se expande para permitirle configurar los ajustes de los requisitos y la seguridad del código de acceso. El valor predeterminado es **Activado**.
- **Requisitos del código de acceso**
  - **Requerir código de acceso alfanumérico:** Seleccione si desea que el código de acceso conste de al menos un carácter alfabético y al menos un número. El valor predeterminado es **Desactivado**.
  - **Requerir código de acceso complejo:** Seleccione si desea requerir un código de acceso complejo. Un código de acceso complejo es aquel que no contiene caracteres repetidos ni caracteres crecientes o decrecientes (como 123 o CBA), y debe contener al menos un carácter no numérico y no alfabético. El valor predeterminado es **Desactivado**.
  - **Longitud mínima del código de acceso:** Seleccione el número mínimo de caracteres que puede contener un código de acceso. El valor predeterminado es **6**.
  - **Caracteres complejos mínimos:** Seleccione el número mínimo de caracteres complejos en la contraseña. Un carácter complejo es un carácter que no es un número ni una letra, como &, %, $ y #. El valor predeterminado es **0**.

- **Seguridad del código de acceso**
  - **Número máximo de intentos fallidos:** Seleccione el número de intentos fallidos de código de acceso que el sistema permite al usuario antes de que iOS borre el dispositivo. Si no cambia esta configuración, después de seis intentos fallidos, el dispositivo impone un retraso de tiempo antes de que el usuario pueda volver a introducir un código de acceso. El retraso de tiempo aumenta con cada intento fallido. Después del último intento fallido, el sistema borra de forma segura todos los datos y configuraciones del dispositivo iOS. El retraso de tiempo del código de acceso comienza después del sexto intento, por lo que si este valor es seis o inferior, el sistema no tiene retraso de tiempo y activa el borrado o el bloqueo tan pronto como el usuario excede el límite. El valor predeterminado es **11**.
  - **Período máximo de gracia:** Seleccione el período máximo durante el cual el usuario puede desbloquear el dispositivo sin un código de acceso. Seleccione **inmediatamente** para no tener período de gracia, y el dispositivo requerirá un código de acceso de inmediato. El valor predeterminado es **Ninguno**, lo que significa que el usuario puede seleccionar cualquier período.
  - **Bloqueo automático del dispositivo:** Seleccione el período máximo durante el cual el dispositivo puede estar inactivo antes de que el sistema lo bloquee automáticamente. Cuando el dispositivo alcanza este límite, se bloquea y el usuario debe introducir el código de acceso para desbloquearlo. El valor predeterminado es **Ninguno**, lo que significa que el usuario puede seleccionar cualquier período.
  - **Antigüedad máxima del código de acceso:** Seleccione el número máximo de días que el código de acceso puede permanecer sin cambios. Después de este número de días, el sistema obliga al usuario a cambiar el código de acceso antes de que desbloquee el dispositivo. Los valores válidos son 0–730. Un valor de **0** fuerza un cambio inmediato del código de acceso. El valor predeterminado está vacío, lo que significa que no hay restricción de antigüedad del código de acceso.
  - **Límite de reutilización del código de acceso:** Seleccione el número de entradas de código de acceso históricas que el sistema comprueba al validar un nuevo código de acceso. El dispositivo rechaza un nuevo código de acceso si coincide con un código de acceso utilizado anteriormente dentro del rango de historial de códigos de acceso especificado. Los valores válidos son 1–50. El valor predeterminado está **vacío**, lo que significa que el sistema no realiza ninguna comprobación histórica.

Nota:

> Si la misma configuración se envía como un perfil MDM y una configuración declarativa a un dispositivo, se aplican las mismas reglas que si la configuración se hubiera entregado mediante varios perfiles. Por ejemplo, si las directivas de código de acceso se configuran mediante un perfil (a través de la directiva de código de acceso) y una configuración (a través de la directiva de código de acceso declarativa), las directivas se fusionan y se aplican las configuraciones más estrictas.

Directiva de dispositivo de aplicación de actualizaciones de software

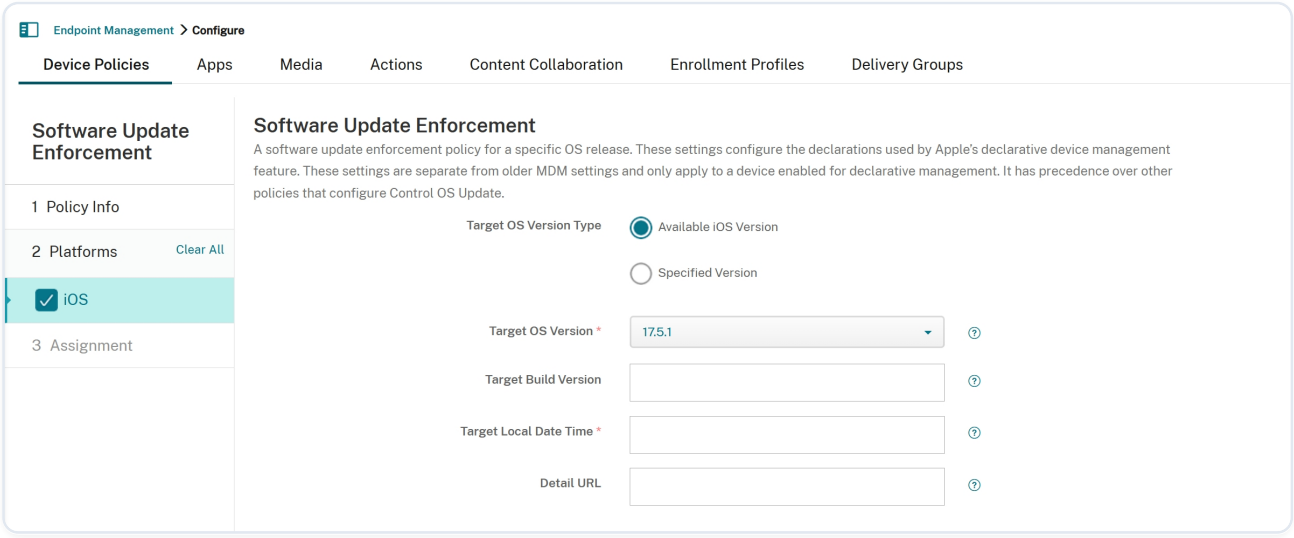
La directiva de dispositivo de aplicación de actualizaciones de software para una versión específica del sistema operativo permite a los administradores de TI gestionar las actualizaciones de dispositivos iOS, lo que les permite controlar qué actualizaciones se aplican y establecer plazos para completar todas las actualizaciones. Estos ajustes configuran las declaraciones utilizadas por la función de gestión declarativa de dispositivos de Apple. Estos ajustes son independientes de los ajustes MDM anteriores y solo se aplican a un dispositivo habilitado para la gestión declarativa. Tiene prioridad sobre la directiva Control OS Update para el mismo ajuste.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

- La versión de CEM es igual o superior a **25.5.0**.
- Disponible para **iOS 17.0** o posterior y **iPadOS 17.0** o posterior.

Configuración de iOS



- **Tipo de versión del SO de destino:** Especifique cómo configurar la versión del SO de destino. El valor predeterminado es **Versión de iOS disponible**.

  - **Versión de iOS disponible:** Si está **activado**, enumere las versiones de SO de destino disponibles en **Versión de SO de destino**.
  - **Versión especificada:** Si está **activado**, introduzca manualmente la versión del SO con el formato sugerido.

- **Versión del SO de destino: (Obligatorio)** Seleccione o escriba la versión del SO de destino a la que se actualizará el dispositivo en el momento adecuado. Este es el número de versión del SO, por ejemplo, 17.7. También puede incluir un identificador de versión suplementario, por ejemplo, 17.7.2.
- **Versión de compilación de destino:** Escriba la versión de compilación de destino a la que se actualizará el dispositivo en el momento adecuado, por ejemplo, 20A242. El sistema utiliza la versión de compilación para las pruebas durante los períodos de siembra. La versión de compilación puede incluir un identificador de versión suplementario, por ejemplo, 20A242a. Si la versión de compilación no es coherente con la versión del SO de destino especificada en la clave TargetOSVersion, la versión del SO de destino tiene prioridad.
- **Fecha y hora local de destino: (Obligatorio)** Escriba el valor de fecha y hora local que especifica cuándo forzar la instalación de la actualización de software. Utilice el formato aaaa-mm-ddThh:mm:ss, que se deriva de RFC3339 pero no incluye un desplazamiento de zona horaria. Si el usuario no activa la actualización de software antes de esta hora, el dispositivo la instala forzosamente.
- **URL de detalles:** Escriba la URL de una página web que muestre los detalles que la organización proporciona sobre la actualización forzada.

Nota:

Tanto la directiva de aplicación de actualizaciones de software como la directiva de control de actualizaciones del SO pueden gestionar las actualizaciones del SO en los dispositivos. Sin embargo, la directiva de aplicación de actualizaciones de software tiene prioridad sobre la directiva de control de actualizaciones del SO. Si ambas directivas se implementan con la misma configuración, la configuración de la directiva de control de actualizaciones del SO se anulará y no surtirá efecto. Para obtener más información, consulte Transición a la administración declarativa de dispositivos.

Además, existen algunas diferencias entre la directiva de aplicación de actualizaciones de software y la directiva de control de actualizaciones del SO.

TIPO DE DIRECTIVA	APLICACIÓN DE ACTUALIZACIONES DE SOFTWARE	CONTROL DE ACTUALIZACIONES DEL SO
Tipo de dispositivo	Dispositivo supervisado o no supervisado	Dispositivo supervisado
Aplicar una fecha límite de actualización	✓	✗
Introducir una URL de ayuda	✓	✗
Especificar el número de versión de compilación	✓	✗
Implementar automáticamente la última actualización	✗	✓
Versión mínima admitida	iOS 17.0	iOS 10.3 (supervisado)

Política de dispositivo de configuración de actualización de software

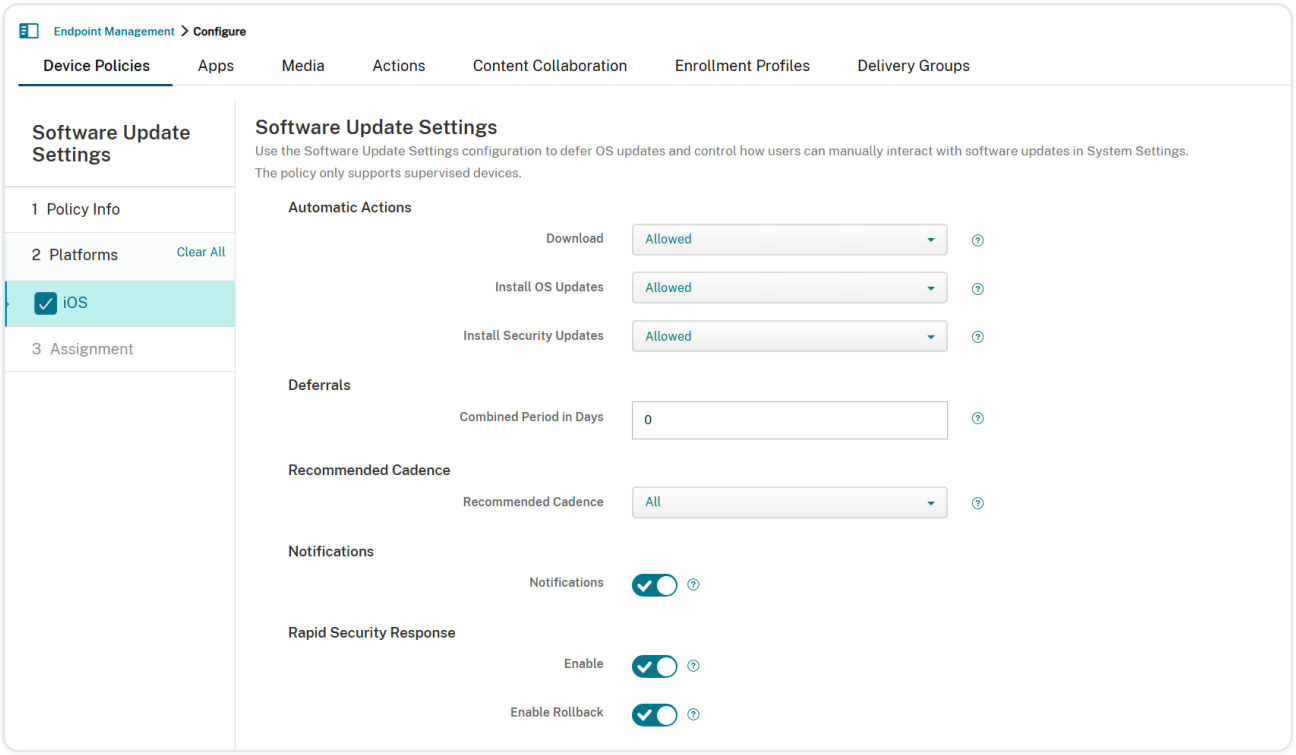
La política de dispositivo de configuración de actualización de software se puede utilizar para aplazar las actualizaciones del sistema operativo y controlar cómo los usuarios pueden interactuar manualmente con las actualizaciones de software en la Configuración del sistema. La política solo admite dispositivos supervisados.

Para añadir o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

- La versión de CEM es igual o superior a **25.5.0**.
- Disponible para **iOS 18.0** o posterior y **iPadOS 18.0** o posterior, solo admite dispositivos supervisados.

Configuración de iOS



- **Acciones automáticas**
  - **Descarga:** Especifique si el usuario puede controlar las descargas automáticas de las actualizaciones disponibles. El valor predeterminado es **Permitido**.
    - **Permitido** - el usuario puede habilitar o deshabilitar las descargas automáticas.
    - **Siempre activado** - las descargas automáticas siempre están habilitadas.
    - **Siempre desactivado** - las descargas automáticas siempre están deshabilitadas.
  - **Instalar actualizaciones del sistema operativo:** Especifique si el usuario puede controlar la instalación automática de las actualizaciones disponibles. El valor predeterminado es **Permitido**.
    - **Permitido** - el usuario puede habilitar o deshabilitar la instalación automática.
    - **AlwaysOn** - las instalaciones automáticas siempre están habilitadas.
    - **AlwaysOff** - las instalaciones automáticas siempre están deshabilitadas.
  - **Instalar actualizaciones de seguridad:** Especifique si el usuario puede controlar la instalación automática de las actualizaciones de seguridad disponibles. El valor predeterminado es **Permitido**.
    - **Permitido** - el usuario puede habilitar o deshabilitar la instalación automática.
    - **AlwaysOn** - las instalaciones automáticas siempre están habilitadas.

    - **AlwaysOff** - las instalaciones automáticas siempre están deshabilitadas.

- **Aplazamientos**

    - **Período combinado en días:** Especifique el número de días para aplazar una actualización de software del sistema operativo principal o secundario en el dispositivo. Cuando se establece, las actualizaciones de software solo aparecen después del retraso especificado, tras el lanzamiento de la actualización de software. Disponible en iOS 18 y versiones posteriores. Los valores válidos son 0–90. El valor predeterminado es **0**, lo que significa que no se espera ningún retraso.

- **Cadencia recomendada**

    - **Cadencia recomendada:** Especifique cómo el dispositivo muestra las actualizaciones de software al usuario. Cuando hay más de una actualización disponible, el dispositivo se comporta de la siguiente manera. El valor predeterminado es **Todas**.

        - **Todas** - Muestra todas las versiones de actualización de software.
        - **Más antigua** - Muestra solo la versión de actualización de software más antigua (con el número más bajo).
        - **Más reciente** - Muestra solo la versión de actualización de software más reciente (con el número más alto).

- **Notificaciones**

    - **Notificaciones:** Si está **Activado**, el dispositivo muestra todas las notificaciones de aplicación de actualizaciones de software. Si está **Desactivado**, el dispositivo solo muestra las notificaciones activadas una hora antes de la fecha límite de aplicación y la notificación de cuenta atrás para el reinicio. El valor predeterminado es **Activado**.

- **Respuesta de seguridad rápida**

    - **Habilitar:** Si está **Desactivado**, no se ofrecen respuestas de seguridad rápidas para la instalación del usuario. El sistema aún puede instalar respuestas de seguridad rápidas con configuraciones `com.apple.configuration.softwareupdate.enforcement.specific`. Si está **Activado**, el sistema ofrece respuestas de seguridad rápidas al usuario. El valor predeterminado es **Activado**.
    - **Habilitar reversión:** Si está **Desactivado**, el sistema no ofrece reversiones de respuesta de seguridad rápida al usuario. Si está **Activado**, el sistema ofrece reversiones de respuesta de seguridad rápida al usuario. El valor predeterminado es **Activado**.

Directiva de dispositivo de suscripciones de estado

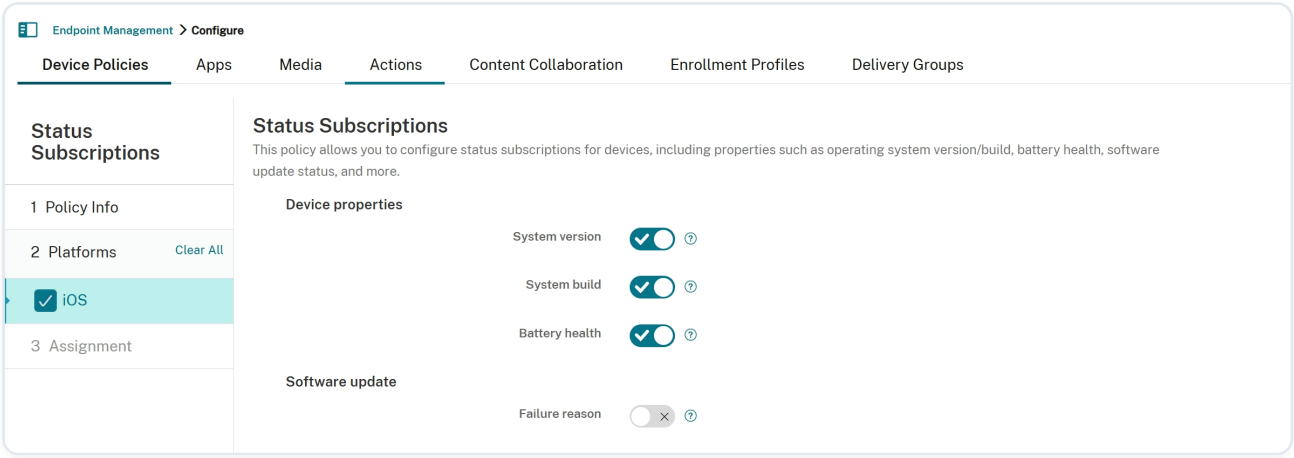
La directiva de dispositivo de suscripciones de estado le permite configurar suscripciones de estado para los dispositivos, incluidas propiedades como la versión/compilación del sistema operativo, el estado de la batería, el estado de las actualizaciones de software y mucho más.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

- La versión de CEM es igual o superior a la **25.5.0**.

Configuración de iOS



- **Propiedades del dispositivo**
  - **Versión del sistema:** Si está **Activado**, el dispositivo informará de la versión del sistema operativo (por ejemplo, 18.0), que se mostrará en la sección Información del sistema de las Propiedades del dispositivo. Esto es útil porque el dispositivo lo informará automáticamente cuando se produzca una actualización de versión. El valor predeterminado es **Activado**. Disponible para iOS 15 y versiones posteriores.
  - **Compilación del sistema:** Si está **Activado**, el dispositivo informará de la versión de compilación del sistema operativo (por ejemplo, 18F132), que se mostrará en la sección Información del sistema de las Propiedades del dispositivo. Esto es útil porque el dispositivo lo informará automáticamente cuando se produzca una actualización de versión. El valor predeterminado es **Activado**. Disponible para iOS 15 y versiones posteriores.
  - **Estado de la batería:** Si está **Activado**, se agrega una nueva configuración **Estado de la batería** a las Propiedades del dispositivo. Esta configuración permite a los administradores ver el estado de la batería de los dispositivos iOS inscritos navegando a **Administrar >**

Dispositivos > Propiedades > Batería > Estado de la batería. El valor predeterminado es **Activado**. Disponible para iOS 17 y versiones posteriores.

- **Actualización de software**
  - **Motivo del error:** Si está **Activado**, el dispositivo informará del motivo de un error de actualización del sistema operativo, que se mostrará en la sección de información de Actualizaciones de software de las Propiedades del dispositivo. El valor predeterminado es **Desactivado**. Disponible para iOS 17 y versiones posteriores.

Política de dispositivo de identidad de usuario

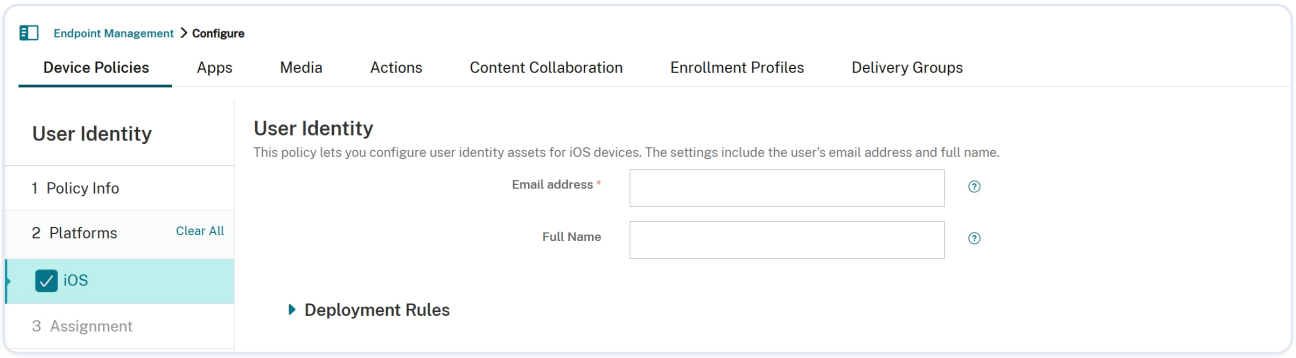
La política de dispositivo de identidad de usuario le permite configurar activos de identidad de usuario para dispositivos iOS. La configuración incluye la dirección de correo electrónico y el nombre completo del usuario.

Para agregar o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

- La versión de CEM es igual o superior a **25.5.0**.

Configuración de iOS



- **Dirección de correo electrónico:** Escriba la dirección de correo electrónico del usuario. Este campo es obligatorio.
- **Nombre completo:** Escriba el nombre completo del usuario.

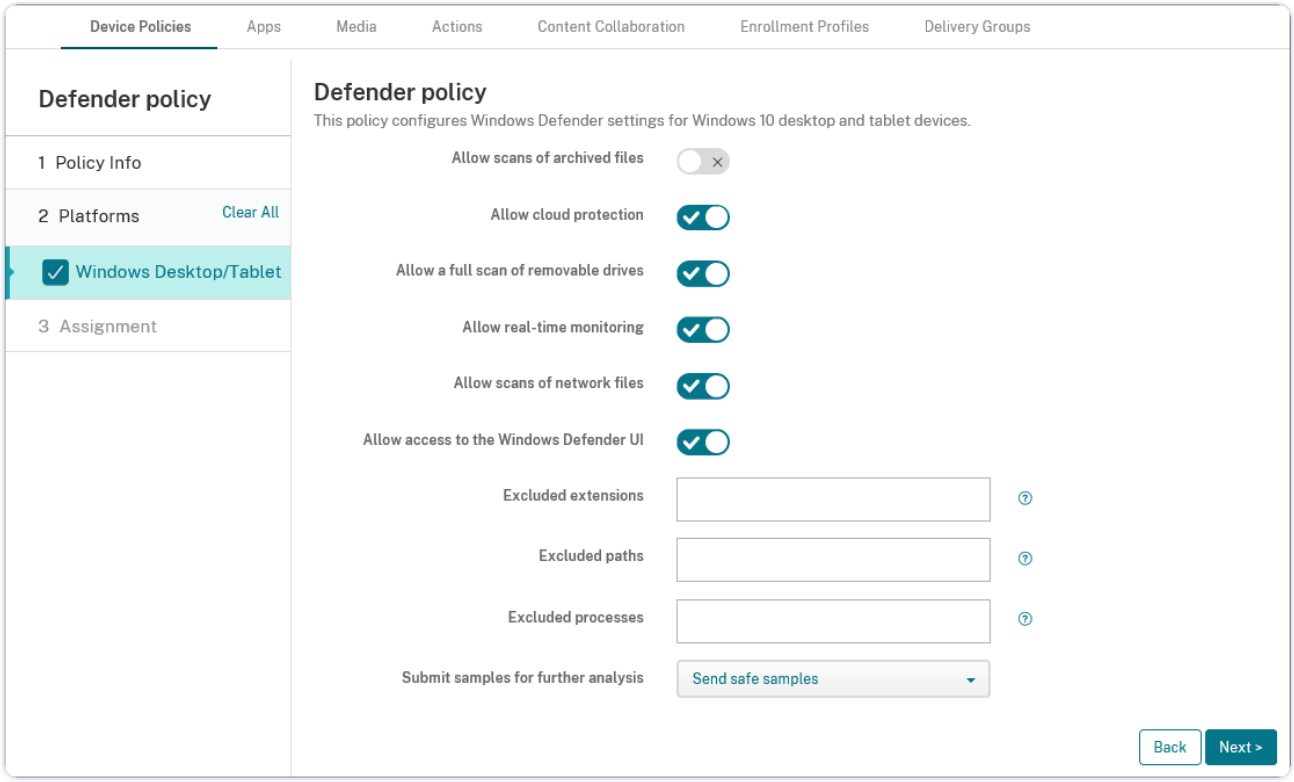
Directiva de dispositivo de Defender

Windows Defender es una protección contra malware incluida en Windows 10 y Windows 11. Puede usar la directiva de dispositivo de Citrix Endpoint Management, Defender, para configurar la

directiva de Microsoft Defender para dispositivos de escritorio y tabletas con Windows 10 y Windows 11.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de escritorio y tableta de Windows



- **Permitir el análisis de archivos archivados:** Permite o bloquea que Defender analice archivos archivados. El valor predeterminado es **Desactivado**.
- **Permitir la protección en la nube:** Permite o bloquea que Defender envíe información a Microsoft sobre la actividad de malware. El valor predeterminado es **Activado**.
- **Permitir un análisis completo de unidades extraíbles:** Permite o bloquea que Defender analice unidades extraíbles, como memorias USB. El valor predeterminado es **Activado**.
- **Permitir la supervisión en tiempo real:** El valor predeterminado es **Activado**.
- **Permitir análisis de archivos de red:** Permite o bloquea que Defender analice archivos de red. El valor predeterminado es **Activado**.
- **Permitir el acceso a la interfaz de usuario de Windows Defender:** Especifica si los usuarios pueden acceder a la interfaz de usuario de Windows Defender. Esta configuración surte efecto la próxima vez que se inicie el dispositivo del usuario. Si esta configuración está establecida en **Desactivado**, los usuarios no recibirán ninguna notificación de Windows Defender. El valor predeterminado es **Activado**.

- **Extensiones excluidas:** Las extensiones que se excluirán de los análisis en tiempo real o programados. Para separar las extensiones, utilice el carácter `|`. Por ejemplo, `lib\|obj`.
- **Rutas excluidas:** Las rutas que se excluirán de los análisis en tiempo real o programados. Para separar las rutas, utilice el carácter `|`. Por ejemplo, `C:\Example|C:\Example1`.
- **Procesos excluidos:** Los procesos que se excluirán de los análisis en tiempo real o programados. Para separar los procesos, utilice el carácter `|`. Por ejemplo, `C:\Example.exe|C:\Example1.exe`.
- **Enviar muestras para un análisis posterior:** Controla si se envían a Microsoft archivos que puedan requerir un análisis posterior para determinar si son maliciosos. Opciones: **Preguntar siempre**, **Enviar muestras seguras**, **Nunca enviar**, **Enviar todas las muestras**. El valor predeterminado es **Enviar muestras seguras**.

Directiva de dispositivo Device Guard

Device Guard es una función de seguridad disponible con Windows 10 y Windows 11. Esta función habilita la seguridad basada en virtualización mediante el uso del **Hipervisor de Windows** para admitir servicios de seguridad en el dispositivo. La directiva Device Guard habilita funciones de seguridad como el arranque seguro, el bloqueo UEFI y la virtualización.

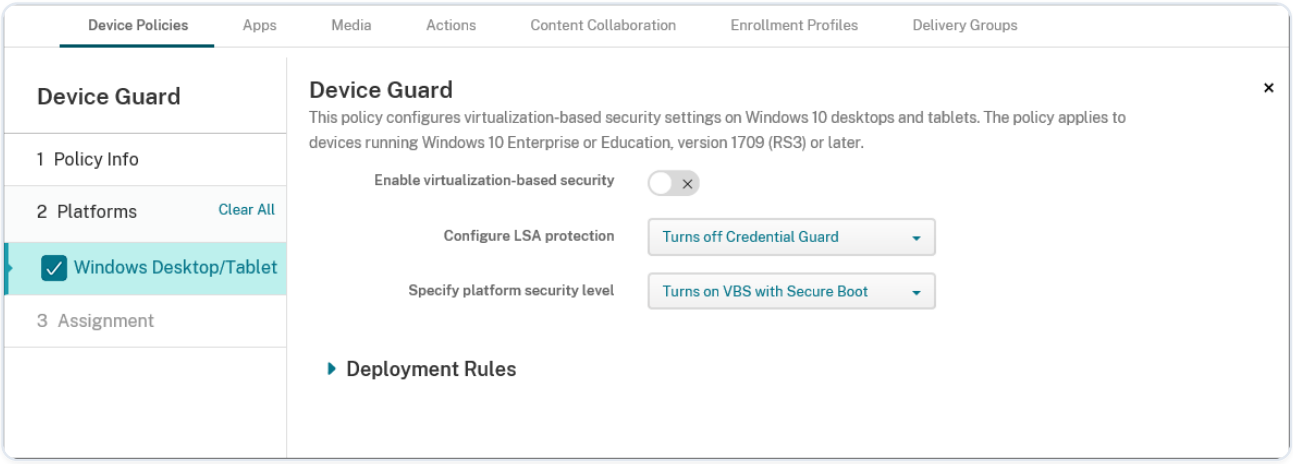
Requisitos previos

- Equipos de escritorio y tabletas con Windows 10 y Windows 11 con una licencia Enterprise o Education
- Device Guard habilitado en Windows

  Para obtener más información sobre Device Guard, consulte `<https://docs.microsoft.com/es-es/windows/access-protection/credential-guard/credential-guard-manage>`.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de equipos de escritorio y tabletas Windows



- **Habilitar la seguridad basada en virtualización:** Deshabilita o habilita las funciones de seguridad basadas en virtualización. La seguridad basada en virtualización utiliza el Hipervisor de Windows para admitir servicios de seguridad.
- **Configurar la protección LSA:** Permite configurar Credential Guard. Esta configuración permite a los usuarios activar Credential Guard con seguridad basada en virtualización para ayudar a proteger las credenciales en el siguiente reinicio. Las opciones son **Desactiva Credential Guard**, **Activa Credential Guard con bloqueo UEFI** y **Activa Credential Guard sin bloqueo UEFI**. El valor predeterminado es **Desactiva Credential Guard**.
- **Especificar el nivel de seguridad de la plataforma:** Permite especificar el nivel de seguridad de la plataforma en el siguiente reinicio. Las opciones son **Activa VBS con arranque seguro** y **Activa VBS con arranque seguro y acceso directo a memoria**. El valor predeterminado es **Activa VBS con arranque seguro**.

Citrix Endpoint Management consulta un dispositivo para determinar si la configuración de seguridad basada en virtualización coincide con la configuración del servidor. Si la configuración de seguridad coincide, Citrix Endpoint Management no implementa esta directiva en el dispositivo. Si la configuración de seguridad no coincide, Citrix Endpoint Management implementa la directiva.

Política de dispositivo de atestación de estado del dispositivo

En Citrix Endpoint Management, puede exigir que los dispositivos Windows 10 y Windows 11 informen sobre su estado de salud. Para informar sobre su estado de salud, los dispositivos envían datos específicos e información de tiempo de ejecución al Servicio de atestación de estado (HAS) para su análisis. El HAS crea y devuelve un Certificado de atestación de estado que el dispositivo envía a Citrix Endpoint Management. Citrix Endpoint Management utiliza el contenido

del Certificado de atestación de estado para implementar las acciones automáticas que haya configurado.

Los datos verificados por el HAS son:

- AIK presente
- Estado de BitLocker
- Depuración de arranque habilitada
- Versión de la lista de revisión del Administrador de arranque
- Integridad del código habilitada
- Versión de la lista de revisión de integridad del código
- Política del programa de implementación de Apple
- Controlador ELAM cargado
- Fecha de emisión
- Depuración del kernel habilitada
- PCR
- Recuento de reinicios
- Recuento de reinicios
- Modo seguro habilitado
- Hash SBCP
- Arranque seguro habilitado
- Firma de prueba habilitada
- VSM habilitado
- WinPE habilitado

Para obtener más información, consulte la página de Microsoft Device HealthAttestation CSP.

Puede configurar DHA mediante Microsoft Cloud o un servidor DHA de Windows local, de la siguiente manera:

- Para configurar DHA mediante Microsoft Cloud: Agregue una directiva de atestación de estado del dispositivo y configúrela como se describe en este artículo.
- Para configurar DHA mediante un servidor DHA de Windows local: Configure un servidor DHA. Luego, agregue una directiva de atestación de estado del dispositivo y configúrela como se describe en este artículo.

Para configurar un servidor DHA, instale la función de servidor DHA en una máquina que ejecute Windows Server 2016 Technical Preview 5 o posterior. Para obtener instrucciones, consulte Configurar un servidor de atestación de estado del dispositivo local.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de Windows Desktop/Tablet

Si configura DHA mediante Microsoft Cloud

- **Habilitar la atestación de estado del dispositivo:** Seleccione si desea requerir la atestación de estado del dispositivo. El valor predeterminado es **Desactivado**.

Si configura DHA mediante un servidor DHA de Windows local

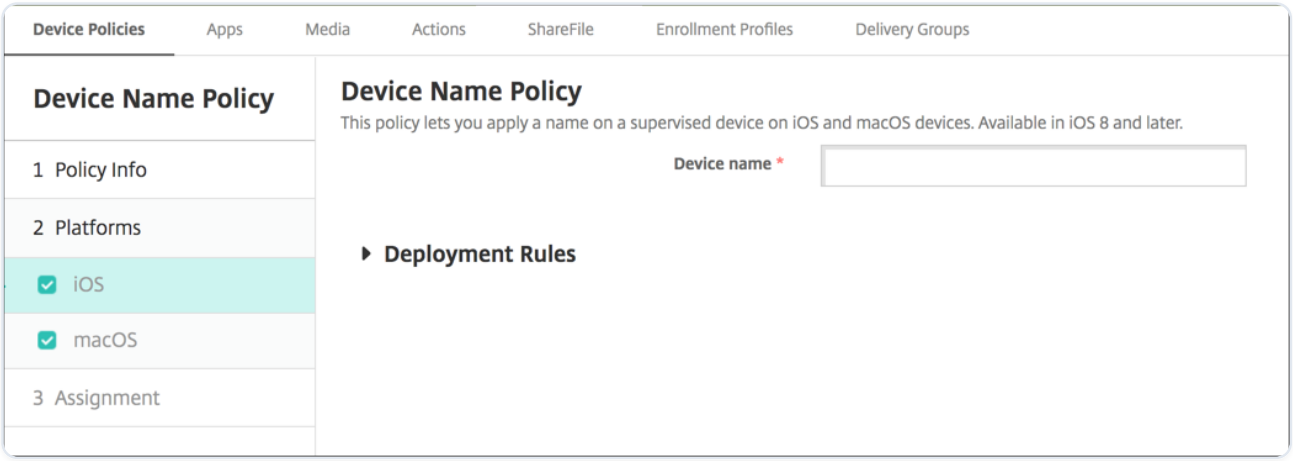
- **Habilitar la atestación de estado del dispositivo:** Establezca en **Activado**.
- **Configurar el servicio de atestación de estado local:** Establezca en **Activado**.
- **FQDN del servicio DHA local:** Escriba el nombre de dominio completo del servidor DHA que configuró.
- **Versión de la API de DHA local:** Seleccione la versión del servicio DHA instalado en el servidor DHA.

Política de nombres de dispositivos

Puede establecer los nombres en dispositivos iOS y macOS supervisados para poder identificar fácilmente los dispositivos. Puede usar macros, texto o una combinación de ambos para definir el nombre del dispositivo. Por ejemplo, para establecer el nombre del dispositivo como el número de serie del dispositivo, puede usar ${device.serialnumber}. Para establecer el nombre del dispositivo como una combinación del nombre de usuario y su dominio, puede usar ${user.username}@example.com. Para obtener más información sobre las macros, consulte Macros en Citrix Endpoint Management.

Para agregar o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS y macOS



- **Nombre del dispositivo:** Escriba la macro, una combinación de macros o una combinación de macros y texto para nombrar cada dispositivo de forma única. Por ejemplo, use ${device.serialnumber} para establecer los nombres de los dispositivos como el número de serie de cada dispositivo, o use ${device.serialnumber} ${ user.username } para incluir el ID de Apple del usuario en el nombre del dispositivo.

Directiva de dispositivo de configuración educativa

La directiva de dispositivo de configuración educativa define:

- La configuración de la aplicación Apple Classroom para dispositivos de instructores.
- Los certificados utilizados para la autenticación de cliente entre dispositivos de instructores y alumnos.

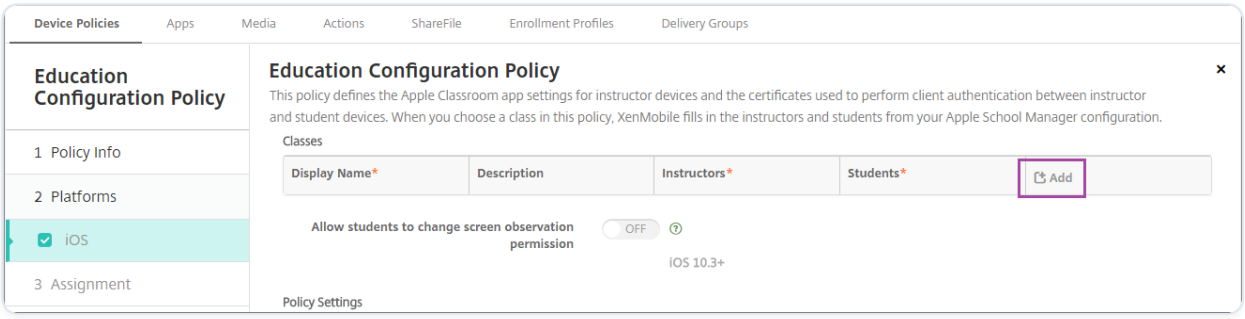
La directiva de dispositivo de configuración educativa es compatible con dispositivos iOS (iPadOS).

Cuando elige una clase en esta directiva, la consola de Citrix Endpoint Management rellena los instructores y alumnos de su configuración de Apple School Manager. Cree una directiva si la configuración de la aplicación Apple Classroom en esta directiva es la misma para todas las clases.

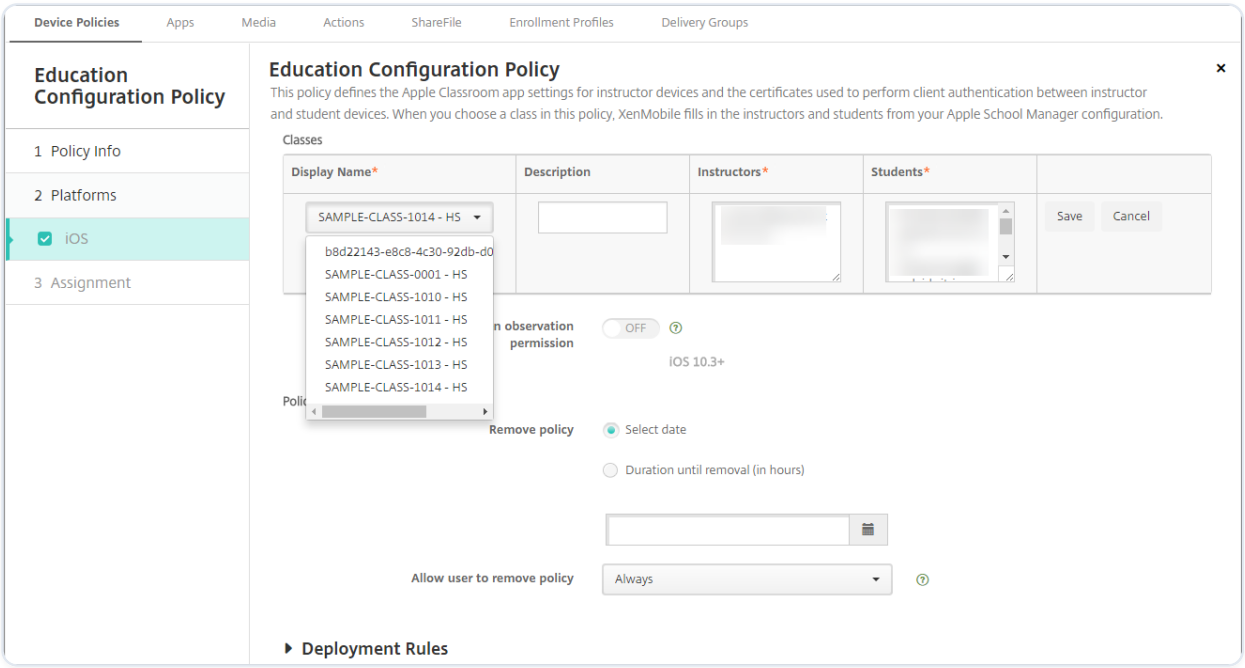
Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

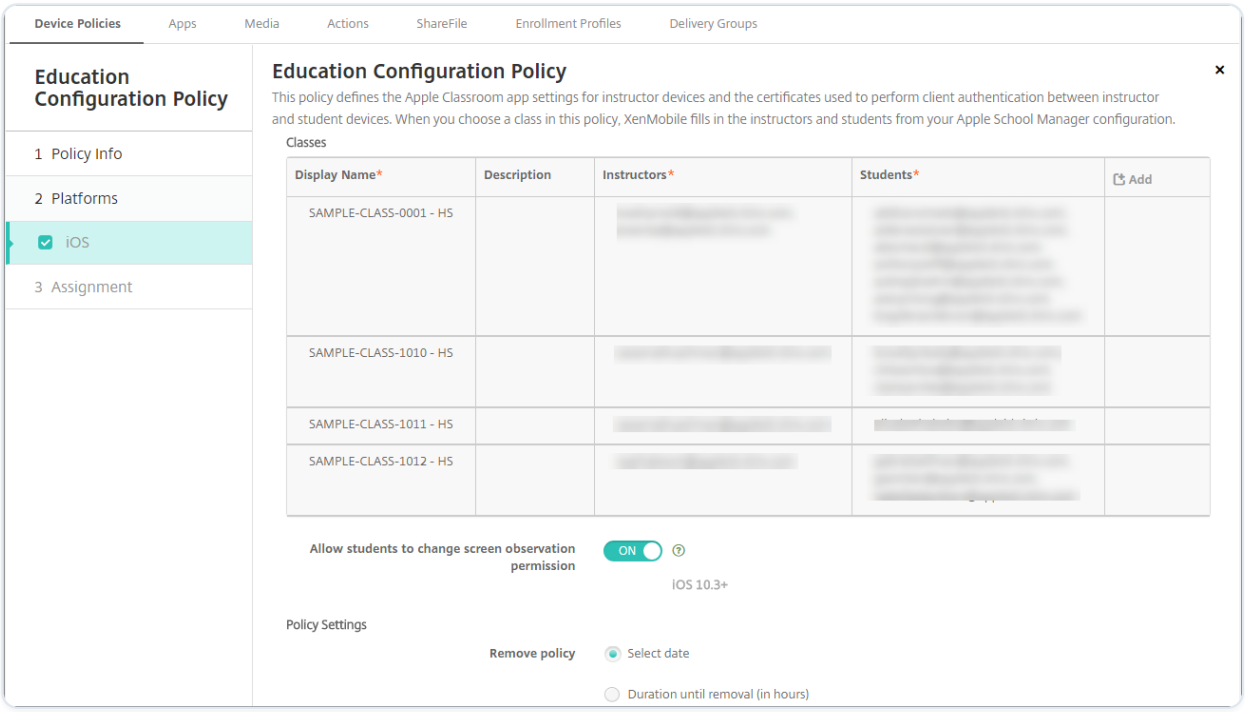
- **Clases:** Para agregar una clase, haga clic en **Agregar**.



A continuación, haga clic en la lista **Nombre para mostrar**. Aparece una lista de clases obtenidas de su cuenta de Apple School Manager conectada.



Cuando elige una clase de **Nombre para mostrar**, Citrix Endpoint Management rellena los instructores y alumnos. Continúe agregando clases.

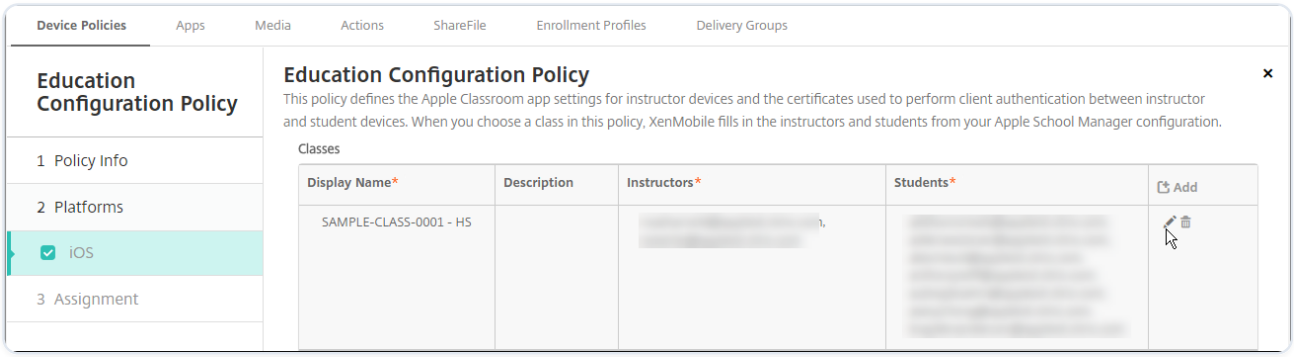


- **Permitir a los alumnos cambiar el permiso de observación de pantalla:** Si está **Activado**, los alumnos inscritos en clases administradas pueden elegir si permiten a su profesor observar las pantallas de sus dispositivos. El valor predeterminado es **Desactivado**.
- **Configuración de la directiva**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.

Para editar la información de la clase en la directiva

Puede agregar una descripción a una clase (el "Nombre para mostrar" en la aplicación Classroom). También puede agregar o eliminar instructores y alumnos. Citrix Endpoint Management no guarda estos cambios en su cuenta de Apple School Manager. Para obtener más información, consulte "Administrar datos de instructores, alumnos y clases" en Integrar con las funciones de Apple Education.

Pase el ratón por la columna **Agregar** de la clase que desea editar y, a continuación, haga clic en el icono del lápiz.



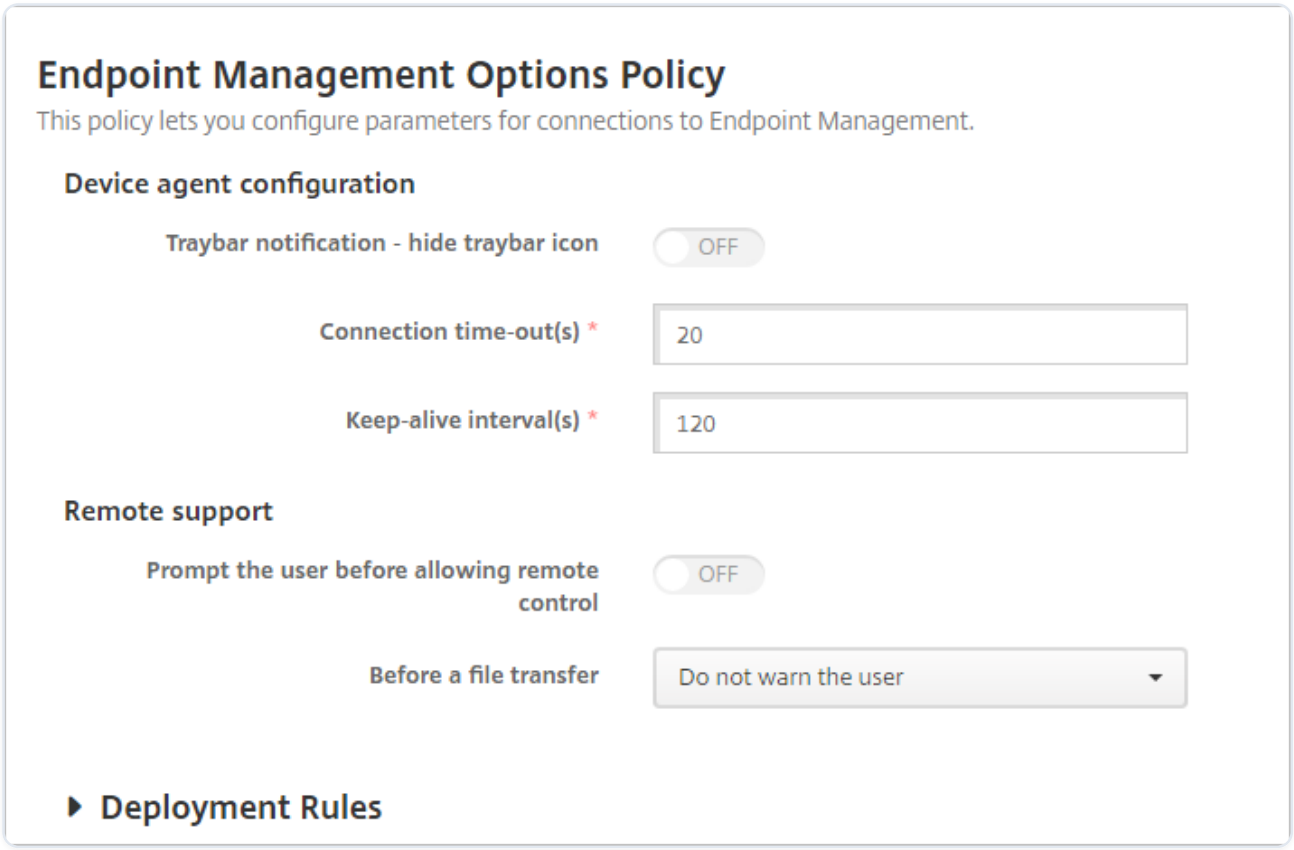
Para eliminar una clase de la directiva, pase el ratón por la columna **Agregar** de la clase que desea eliminar y, a continuación, haga clic en el icono de la papelera.

Directiva de dispositivo de opciones de Endpoint Management

Agregue una directiva de opciones de Endpoint Management para configurar el comportamiento de Citrix Secure Hub al conectarse a Citrix Endpoint Management desde dispositivos Android.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

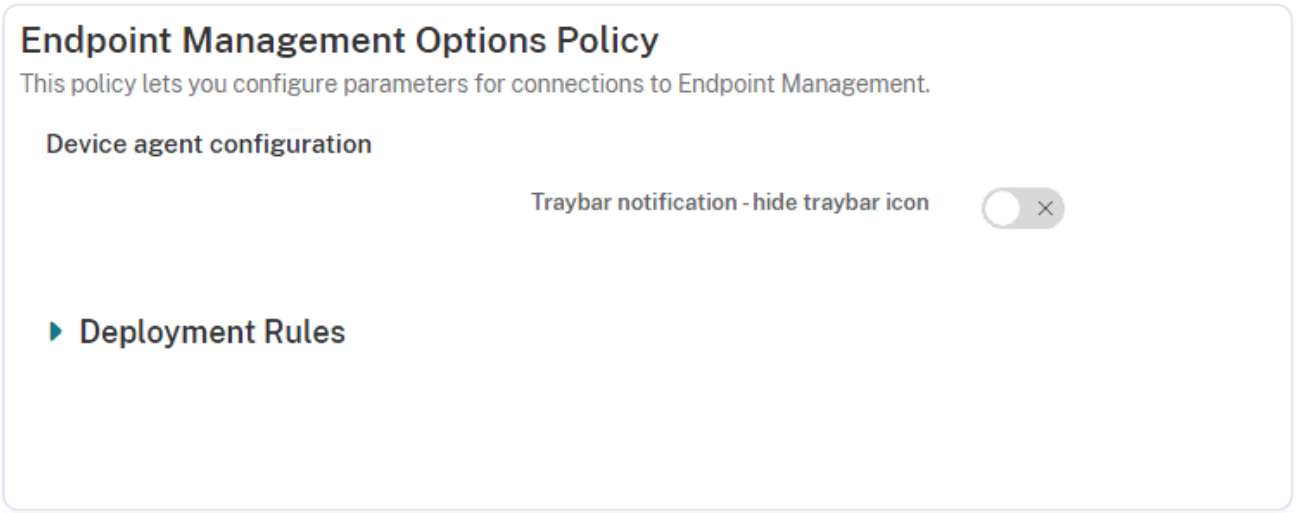
Configuración de Android



- **Notificación de la barra de tareas - ocultar icono de la barra de tareas:** Seleccione si el icono de la barra de tareas está oculto o visible. El valor predeterminado es **Desactivado**.

- **Conexión: tiempos de espera:** Escriba la duración en segundos que una conexión puede estar inactiva antes de que la conexión agote el tiempo de espera. El valor predeterminado es 20 segundos.
- **Intervalos de Keep-alive:** Escriba la duración en segundos para mantener una conexión abierta. El valor predeterminado es 120 segundos.
- **Solicitar al usuario antes de permitir el control remoto:** Seleccione si se debe solicitar al usuario antes de permitir el control de soporte remoto. El valor predeterminado es **Desactivado**.
- **Antes de una transferencia de archivos:** Haga clic para advertir al usuario sobre una transferencia de archivos o para pedirle permiso en la lista desplegable. Valores disponibles: **No advertir al usuario**, **Advertir al usuario** y **Pedir permiso al usuario**. El valor predeterminado es **No advertir al usuario**.

Configuración de Android Enterprise



Compatible a partir de la versión 7 de Android.

Notificación de la barra de tareas - ocultar icono de la barra de tareas: Seleccione si el icono de la barra de tareas está oculto o visible. El valor predeterminado es **Desactivado**.

> **Nota:**
>
> Si desea habilitar el servicio VPN para dispositivos que ejecutan Android Enterprise, puede habilitar la opción **Habilitar VPN siempre activa** en la **política de dispositivo VPN**. Si ya ha habilitado la opción **Habilitar VPN siempre activa** en la **política de dispositivo de opciones de Endpoint Management** en una versión anterior, asegúrese de habilitarla de nuevo en la **política de dispositivo VPN**.

Directiva de desinstalación de dispositivos de Citrix Endpoint Management

Puede añadir una directiva de dispositivo en Citrix Endpoint Management para desinstalar Citrix Endpoint Management de los dispositivos Android. Cuando se implementa, esta directiva elimina Citrix Endpoint Management de todos los dispositivos del grupo de implementación.

Para añadir o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de Android

- **Desinstalar Citrix Endpoint Management de los dispositivos:** Seleccione si desea desinstalar Citrix Endpoint Management de cada dispositivo al que implemente esta directiva. El valor predeterminado es **Desactivado**.

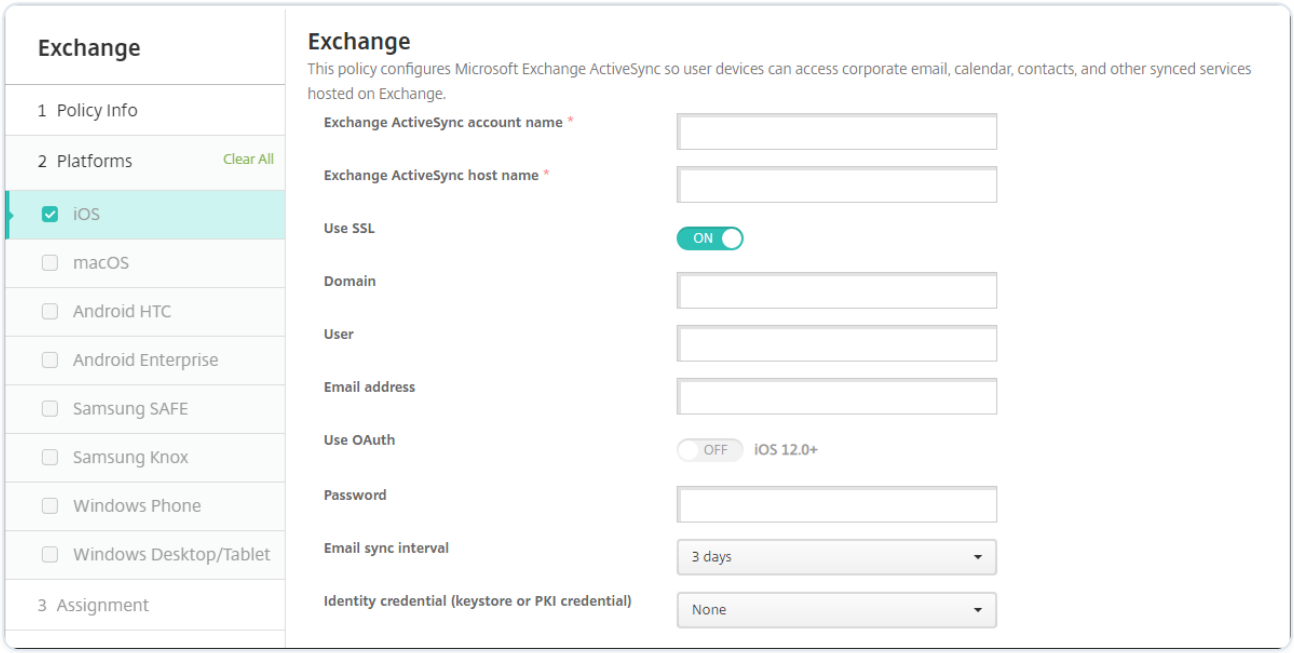
Directiva de dispositivo Exchange

Puede utilizar la directiva de dispositivo Exchange ActiveSync para configurar un cliente de correo electrónico en los dispositivos de los usuarios y permitirles acceder a su correo electrónico corporativo alojado en Exchange. Cada plataforma requiere un conjunto diferente de valores, que se describen en detalle en las siguientes secciones.

Para crear esta directiva, necesita el nombre de host o la dirección IP del servidor Exchange. Para obtener información sobre la configuración de ActiveSync, consulte el artículo de Microsoft, ActiveSync CSP.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS



- **Nombre de cuenta de Exchange ActiveSync:** Escriba la descripción de la cuenta de correo electrónico que se muestra en los dispositivos de los usuarios.
- **Nombre de host de Exchange ActiveSync:** Escriba la dirección del servidor de correo electrónico.
- **Usar SSL:** Seleccione si desea proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. El valor predeterminado es **Activado**.
- **Dominio:** Introduzca el dominio en el que se encuentra el servidor Exchange. Puede utilizar la macro del sistema `$user.domainname` en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **Usuario:** Especifique el nombre de usuario de la cuenta de usuario de Exchange. Puede utilizar la macro del sistema `$user.username` en este campo para buscar automáticamente los nombres de usuario.
- **Dirección de correo electrónico:** Especifique la dirección de correo electrónico completa. Puede utilizar la macro del sistema `$user.mail` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Usar OAuth:** Si se establece en **Activado**, la conexión utiliza OAuth para la autenticación. El valor predeterminado es **Desactivado**. Esta opción se aplica a iOS 12.0 y versiones posteriores.
- **Contraseña:** Introduzca una contraseña opcional para la cuenta de usuario de Exchange. Esta configuración no aparece cuando **Usar OAuth** está **Activado**.

- **Intervalo de sincronización de correo electrónico:** En la lista, elija la frecuencia con la que se sincroniza el correo electrónico con el servidor Exchange. El valor predeterminado es **3 días**.
- **Credencial de identidad (almacén de claves o PKI):** Haga clic en una credencial de identidad opcional en la lista desplegable si ha configurado un proveedor de identidades para Citrix Endpoint Management. Este campo solo es obligatorio cuando Exchange requiere una autenticación de certificado de cliente. El valor predeterminado es **Ninguno**.
- **Autorizar el movimiento de correo electrónico entre cuentas:** Seleccione si desea permitir a los usuarios:
  - mover el correo electrónico de esta cuenta a otra
  - reenviar correo electrónico desde una cuenta diferente
  - responder desde una cuenta diferente.

  El valor predeterminado es **Desactivado**.
- **Enviar correo electrónico solo desde la aplicación de correo electrónico:** Seleccione si desea restringir a los usuarios a la aplicación de correo de iOS para enviar correos electrónicos. El valor predeterminado es **Desactivado**.
- **Impedir que los usuarios sincronicen direcciones recientes:** Seleccione si desea impedir que los usuarios sincronicen direcciones recientes. El valor predeterminado es **Desactivado**.
- **Permitir Mail Drop:** Seleccione si desea permitir que la cuenta use Mail Drop. El valor predeterminado es **Desactivado**.
- **Habilitar la firma S/MIME:** Seleccione si esta cuenta admite la firma S/MIME. El valor predeterminado es **Activado**. Cuando se establece en **Activado**, aparecen los siguientes campos.
  - **Credencial de identidad de firma:** Elija la credencial de firma que desea usar.
  - **El usuario puede anular la firma S/MIME:** Si se establece en **Activado**, los usuarios pueden activar y desactivar la firma S/MIME en la configuración de sus dispositivos. El valor predeterminado es **Desactivado**. Esta opción se aplica a iOS 12.0 y versiones posteriores.
  - **El usuario puede anular el UUID del certificado de firma S/MIME:** Si se establece en **Activado**, los usuarios pueden seleccionar, en la configuración de sus dispositivos, la credencial de firma que desean usar. El valor predeterminado es **Desactivado**. Esta opción se aplica a iOS 12.0 y versiones posteriores.

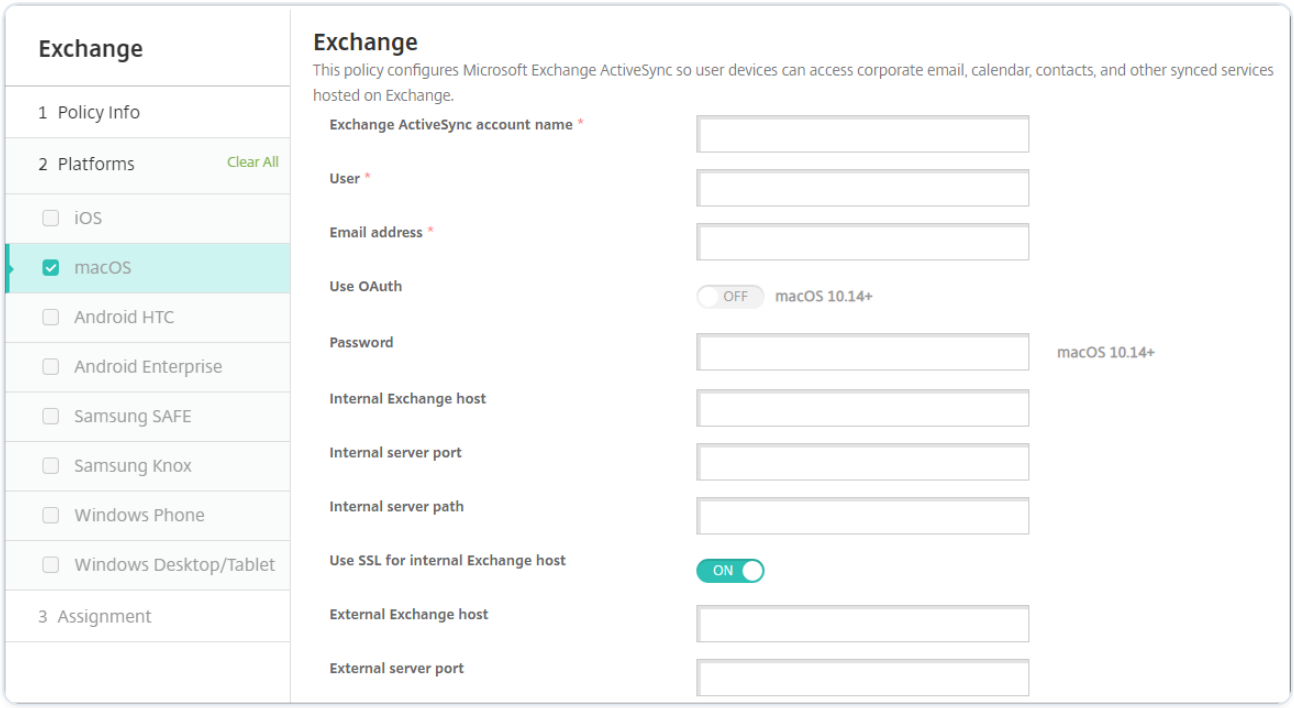
- **Habilitar el cifrado S/MIME:** Seleccione si esta cuenta admite el cifrado S/MIME. El valor predeterminado es **Desactivado**. Cuando se establece en **Activado**, aparecen los siguientes campos.
    - **Credencial de identidad de cifrado:** Elija la credencial de cifrado que desea usar.
    - **Habilitar el interruptor S/MIME por mensaje:** Cuando se establece en **Activado**, muestra a los usuarios una opción para activar o desactivar el cifrado S/MIME para cada mensaje que redactan. El valor predeterminado es **Desactivado**.
    - **El usuario puede anular el cifrado S/MIME:** Si se establece en **Activado**, los usuarios pueden, en la configuración de sus dispositivos, seleccionar si S/MIME está activado de forma predeterminada. El valor predeterminado es **Desactivado**. Esta opción se aplica a iOS 12.0 y versiones posteriores.
    - **El usuario puede anular el UUID del certificado de cifrado S/MIME:** Si se establece en **Activado**, los usuarios pueden activar y desactivar la identidad y el cifrado S/MIME en la configuración de sus dispositivos. El valor predeterminado es **Desactivado**. Esta opción se aplica a iOS 12.0 y versiones posteriores.
- **Configuración de la directiva**
    - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
        - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
        - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.

Servicios de Exchange sincronizados

La configuración de Servicios de Exchange sincronizados le permite elegir si desea sincronizar las siguientes funciones:

- Calendarios
- Contactos
- Correo
- Notas
- Recordatorios

Configuración de macOS

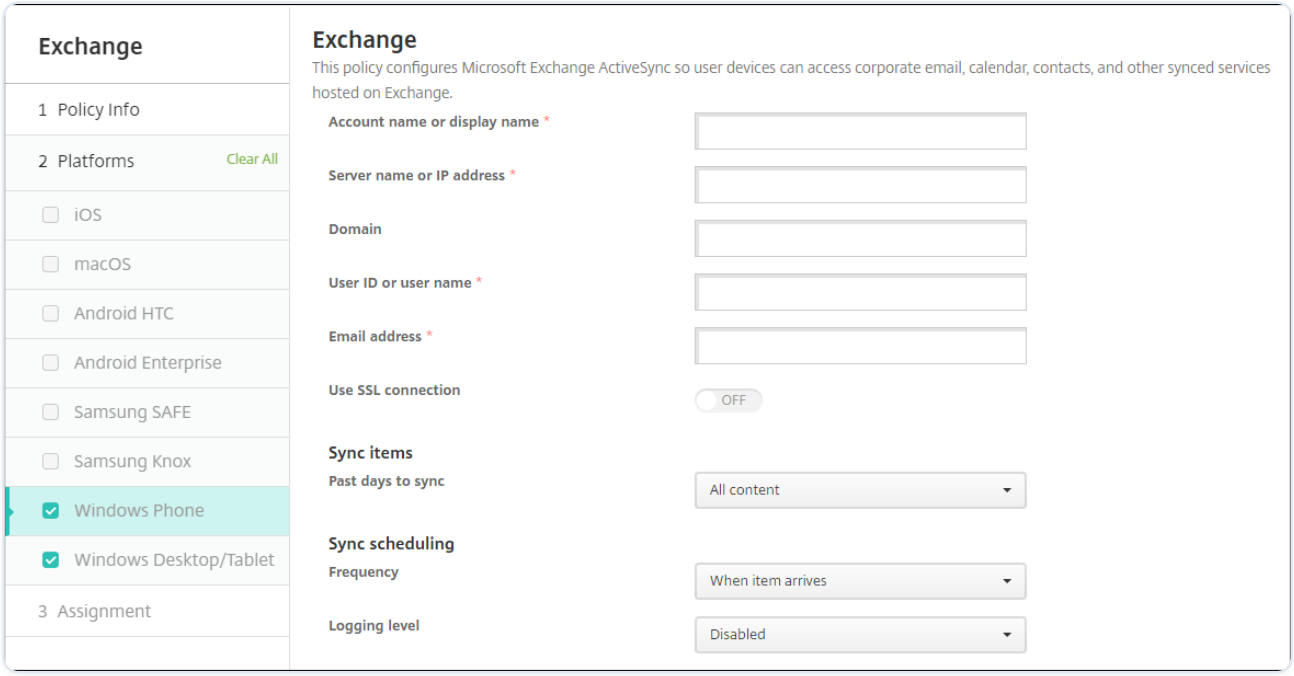


- **Nombre de cuenta de Exchange ActiveSync:** Escriba la descripción de la cuenta de correo electrónico que se muestra en los dispositivos de los usuarios.
- **Usuario:** Especifique el nombre de usuario de la cuenta de usuario de Exchange. Puede usar la macro del sistema `$user.username` en este campo para buscar automáticamente los nombres de usuario.
- **Dirección de correo electrónico:** Especifique la dirección de correo electrónico completa. Puede usar la macro del sistema `$user.mail` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Usar OAuth:** Si se establece en **Activado**, la conexión utiliza OAuth para la autenticación. El valor predeterminado es **Desactivado**. Esta opción se aplica a macOS 10.14 y versiones posteriores.
- **URL de inicio de sesión de OAuth:** Especifica la URL que se cargará en una vista web para autenticarse mediante OAuth cuando no utilice el servicio AutoDiscovery. Este campo aparece cuando **Usar OAuth** está establecido en **Activado**.
- **Contraseña:** Introduzca una contraseña opcional para la cuenta de usuario de Exchange. Esta configuración no aparece cuando **Usar OAuth** está **Activado**.
- **Host de Exchange interno:** Si desea que los nombres de host de Exchange internos y externos sean diferentes, escriba un nombre de host de Exchange interno opcional.

- **Puerto del servidor interno:** Si desea que los puertos del servidor de Exchange internos y externos sean diferentes, escriba un número de puerto del servidor de Exchange interno opcional.
- **Ruta del servidor interno:** Si desea que las rutas del servidor de Exchange internas y externas sean diferentes, escriba una ruta del servidor de Exchange interna opcional.
- **Usar SSL para el host de Exchange interno:** Seleccione si desea proteger las conexiones entre los dispositivos de los usuarios y el host de Exchange interno. El valor predeterminado es **Activado**.
- **Host de Exchange externo:** Si desea que los nombres de host de Exchange internos y externos sean diferentes, escriba un nombre de host de Exchange externo opcional.
- **Puerto del servidor externo:** Si desea que los puertos del servidor de Exchange internos y externos sean diferentes, escriba un número de puerto del servidor de Exchange externo opcional.
- **Ruta del servidor externo:** Si desea que las rutas del servidor de Exchange internas y externas sean diferentes, escriba una ruta del servidor de Exchange externa opcional.
- **Usar SSL para el host de Exchange externo:** Seleccione si desea proteger las conexiones entre los dispositivos de los usuarios y el host de Exchange interno. El valor predeterminado es **Activado**.
- **Permitir Mail Drop:** Seleccione si desea permitir a los usuarios compartir archivos de forma inalámbrica entre dos Mac, sin tener que conectarse a una red existente. El valor predeterminado es **Desactivado**.
- **Configuración de la directiva**
    - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
        - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
        - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.
    - **Permitir al usuario eliminar la directiva:** Puede seleccionar cuándo los usuarios pueden eliminar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**.

- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en macOS 10.7 y versiones posteriores.

Configuración de Windows de escritorio/tableta



Nota:

Esta directiva no le permite establecer la contraseña del usuario. Los usuarios deben establecer ese parámetro desde sus dispositivos después de que usted implemente la directiva.

- **Nombre de cuenta o nombre para mostrar:** Escriba el nombre de la cuenta de Exchange ActiveSync.
- **Nombre del servidor o dirección IP:** Escriba el nombre de host o la dirección IP del servidor de Exchange.
- **Dominio:** Introduzca el dominio en el que se encuentra el servidor de Exchange. Puede usar la macro del sistema `$user.domainname` en este campo para buscar automáticamente los nombres de dominio de usuario.
- **ID de usuario o nombre de usuario:** Especifique el nombre de usuario para la cuenta de usuario de Exchange. Puede usar la macro del sistema `$user.username` en este campo para buscar automáticamente los nombres de usuario.

- **Dirección de correo electrónico:** Especifique la dirección de correo electrónico completa. Puede usar la macro del sistema `$user.mail` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Usar conexión SSL:** Seleccione si desea proteger las conexiones entre los dispositivos de los usuarios y el servidor de Exchange. El valor predeterminado es **Desactivado**.
- **Días anteriores para sincronizar:** En la lista, haga clic en cuántos días anteriores desea sincronizar todo el contenido del dispositivo con el servidor de Exchange. El valor predeterminado es **Todo el contenido**.
- **Frecuencia:** Haga clic en la programación de la lista desplegable que quiere usar al sincronizar los datos que se envían al dispositivo desde el servidor de Exchange. El valor predeterminado es **Cuando llega el elemento**.
- **Nivel de registro:** Haga clic en **Deshabilitado**, **Básico** o **Avanzado** en la lista desplegable para especificar el nivel de detalle al registrar la actividad de Exchange. El **valor predeterminado es Deshabilitado**.

Directiva de archivos de dispositivo

Puede agregar e implementar archivos para que los usuarios accedan a ellos en sus dispositivos Android y Android Enterprise. Especifique el directorio donde desea almacenar el archivo en el dispositivo. Por ejemplo, si desea que los usuarios reciban un documento de la empresa o un archivo .pdf. Implemente el archivo en los dispositivos e informe a los usuarios dónde se encuentra el archivo.

Los dispositivos Android no admiten la ejecución de scripts de forma nativa. Los usuarios necesitan software de terceros para ejecutar scripts.

Puede agregar los siguientes tipos de archivo con esta directiva:

- Archivos de texto (.xml, .html, .py, etc.)
- Otros archivos, como documentos, imágenes, hojas de cálculo o presentaciones

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivos**. Para obtener más información, consulte Directivas de dispositivos.

Configuración de Android Enterprise

- **Archivo a importar:** Para seleccionar el archivo a importar, haga clic en **Examinar** y navegue hasta la ubicación del archivo.

- **Carpeta de destino:** En la lista, seleccione la ubicación donde desea almacenar el archivo cargado, o seleccione **Agregar nuevo** para especificar una ubicación de archivo. Seleccione la macro `%Flash Storage%\` o `%XenMobile Storage%\` para indicar dónde almacenar el archivo cargado. La macro se expande a la ubicación aplicable en cada dispositivo.
  - `%XenMobile Storage%\` se expande a `Android/data/com.zenprise/` en el directorio de almacenamiento interno.
  - Para Android 9.0 y versiones anteriores, `%Flash Storage%\` guarda el archivo en el directorio de almacenamiento externo.
  - Para Android 10.0 y versiones posteriores, `%Flash Storage%\` guarda el archivo en la carpeta **Descargas** del directorio de almacenamiento interno.
  - Para Android 11.0 y versiones posteriores, `%XenMobile Storage%\` ya no se aplica debido a las restricciones impuestas por Google en el acceso a la ubicación de destino.
- **Nombre de archivo de destino:** Opcional. Si debe cambiar un nombre de archivo antes de implementarlo en un dispositivo, escriba el nombre del archivo.
- **Si el archivo existe:** En la lista, seleccione si desea copiar un archivo existente. El valor predeterminado es **Copiar archivo solo si es diferente**.

> **Importante:**
>
> La directiva de dispositivo de Archivos ya no admite la adición de scripts en Android Enterprise. Si una directiva existente tiene un script, se muestra un mensaje de error al seleccionar la directiva y puede volver a agregar la directiva para resolver el problema.

Configuración de Android

- **Archivo a importar:** Para seleccionar el archivo a importar, haga clic en **Examinar** y navegue hasta la ubicación del archivo.
- **Tipo de archivo:** Seleccione **Archivo** o **Script**.
- **Ejecutar inmediatamente:** Cuando selecciona **Script**, aparece la opción **Ejecutar inmediatamente**. No ocurre nada cuando habilita esta configuración. Los usuarios deben ejecutar el script manualmente.
- **Reemplazar expresiones de macro:** Seleccione si desea reemplazar los nombres de los tokens de macro en un script con una propiedad de dispositivo o de usuario. Para la sintaxis de las macros, consulte Macros. El valor predeterminado es **Desactivado**.

- **Carpeta de destino:** En la lista, seleccione la ubicación donde desea almacenar el archivo cargado, o seleccione **Agregar nuevo** para especificar una ubicación de archivo. Seleccione la macro `%Flash Storage%\` o `%XenMobile Storage%\` para indicar dónde almacenar el archivo cargado. La macro se expande a la ubicación aplicable en cada dispositivo.
  - `%XenMobile Storage%\` se expande a `Android/data/com.zenprise/` en el directorio de almacenamiento interno.
  - Para Android 9.0 y versiones anteriores, `%Flash Storage%\` guarda el archivo en el directorio de almacenamiento externo.
  - Para Android 10.0 y versiones posteriores, `%Flash Storage%\` guarda el archivo en la carpeta **Descargas** del directorio de almacenamiento interno.
  - Para Android 11.0 y versiones posteriores, `%XenMobile Storage%\` ya no se aplica debido a las restricciones impuestas por Google en el acceso a la ubicación de destino.
- **Nombre de archivo de destino:** Opcional. Si debe cambiar un nombre de archivo antes de implementarlo en un dispositivo, escriba el nombre del archivo.
- **Si el archivo existe:** En la lista, seleccione si desea copiar un archivo existente. El valor predeterminado es **Copiar archivo solo si es diferente**.

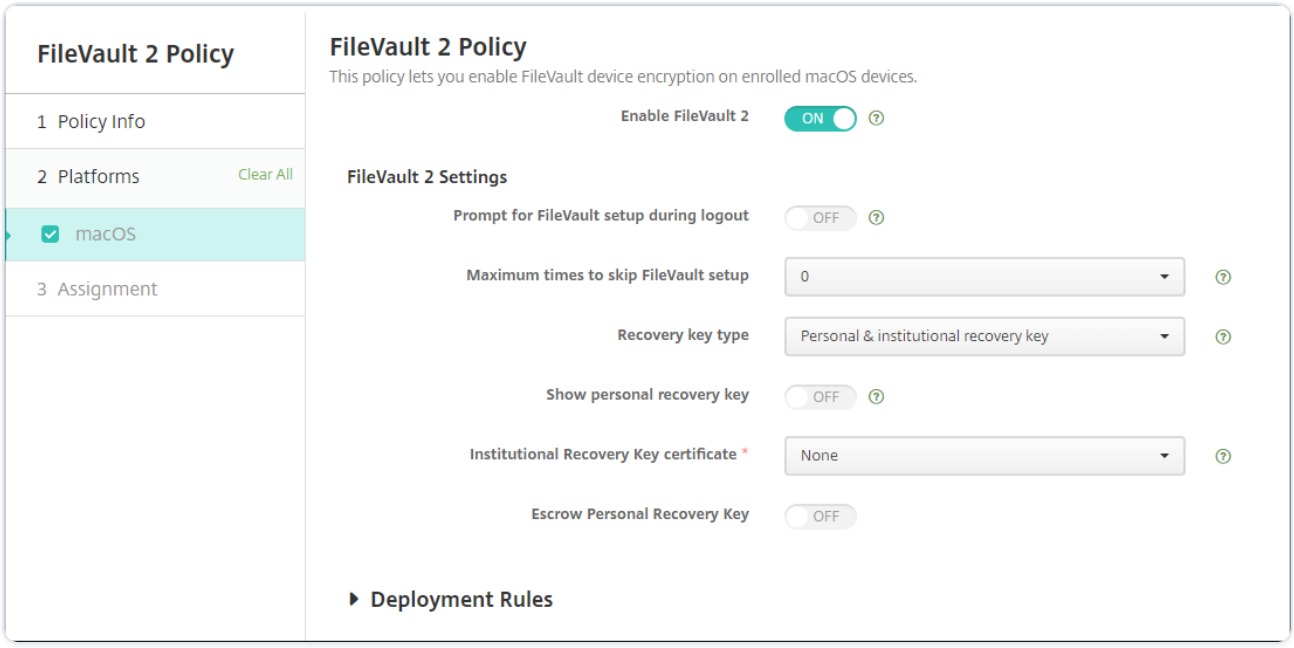
Política de dispositivo FileVault

La función de cifrado de disco completo (FileVault 2) de macOS FileVault protege el volumen del sistema cifrando su contenido. Un usuario inicia sesión en un dispositivo macOS habilitado para FileVault con la contraseña de su cuenta cada vez que el dispositivo se inicia. Si el usuario pierde su contraseña, una clave de recuperación le permite desbloquear el disco y restablecer su contraseña.

Esta política de dispositivo habilita las pantallas de configuración de usuario de FileVault y configura ajustes como las claves de recuperación. Para obtener más información sobre FileVault, consulte el sitio de soporte de Apple.

Para agregar la política de FileVault, vaya a **Configurar > Directivas de dispositivo**.

Configuración de macOS



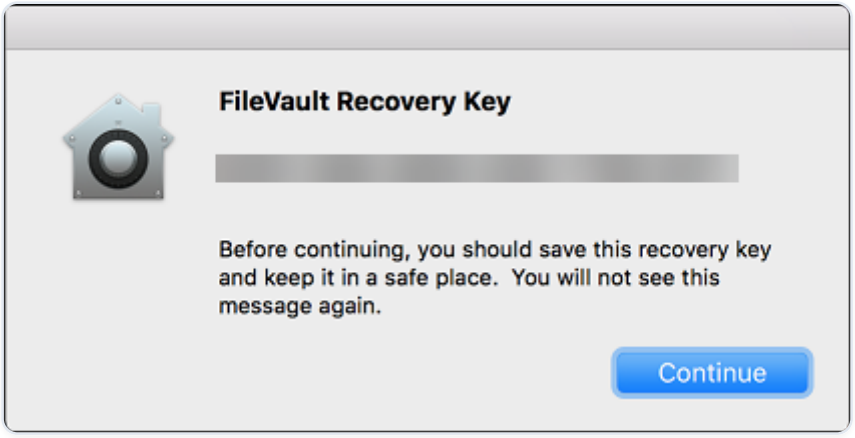
- **Habilitar FileVault:** Si esta opción está configurada como **Activado**, se le pedirá al usuario que habilite FileVault durante los próximos N cierres de sesión, según lo especificado por la opción **Número máximo de veces para omitir la configuración de FileVault**. Si está **Desactivado**, los usuarios no recibirán una solicitud para habilitar FileVault, pero aún pueden habilitarlo por su cuenta.
- **Solicitar configuración de FileVault durante el cierre de sesión:** Si está **Activado**, los usuarios verán una solicitud para habilitar FileVault al cerrar sesión.
- **Número máximo de veces para omitir la configuración de FileVault:** El número máximo de veces que el usuario puede omitir la configuración de FileVault. Cuando el usuario alcanza el máximo, debe configurar FileVault para iniciar sesión. Si es **0**, el usuario debe habilitar FileVault durante el primer intento de inicio de sesión. El valor predeterminado es **0**.
- **Tipo de clave de recuperación:** Un usuario que olvida su contraseña puede introducir una clave de recuperación para desbloquear el disco y restablecer su contraseña. Opciones de clave de recuperación:
    - **Clave de recuperación personal:** Una clave de recuperación personal es única para un usuario. Durante la configuración de FileVault, un usuario elige si crear una clave de recuperación o permitir que su cuenta de iCloud desbloquee su disco. Para mostrar la clave de recuperación al usuario una vez completada la configuración de FileVault, habilite **Mostrar clave de recuperación personal**. Mostrar la clave permite al usuario registrarla para uso futuro. Para permitir que los usuarios busquen su clave si la pierden, habilite **Custodiar clave de recuperación personal**.

Puede rotar las claves de recuperación personales mediante acciones de seguridad. Para obtener más información sobre cómo rotar las claves de recuperación personales, consulte Acciones de seguridad.

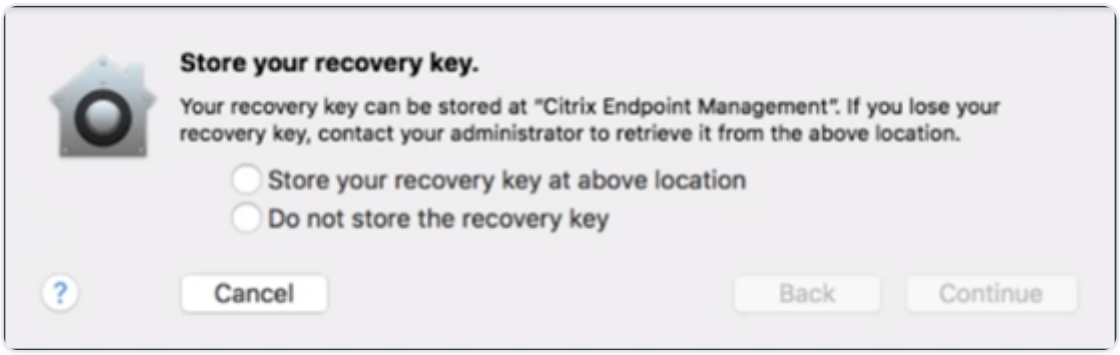
Para obtener información sobre la administración de claves de recuperación, consulte el sitio de soporte de Apple.

- **Clave de recuperación institucional:** Puede crear una clave de recuperación institucional (o principal) y un certificado de FileVault, que luego utilizará para desbloquear los dispositivos de los usuarios. Para obtener información, consulte el sitio de soporte de Apple. Utilice Citrix Endpoint Management para implementar el certificado de FileVault en los dispositivos. Para obtener información, consulte Certificados y autenticación.
- **Clave de recuperación personal e institucional:** Al habilitar ambos tipos de claves de recuperación, solo debe desbloquear un dispositivo de usuario si este pierde su clave de recuperación personal.

- **Certificado de clave de recuperación institucional:** Si selecciona **Clave de recuperación institucional** o **Clave de recuperación personal e institucional** como **Tipo de clave de recuperación**, seleccione el certificado de clave de recuperación para esa clave.
- **Mostrar clave de recuperación personal:** Si está en **Activado**, el dispositivo de usuario muestra la clave de recuperación personal al usuario después de configurar FileVault. El valor predeterminado es **Desactivado**.

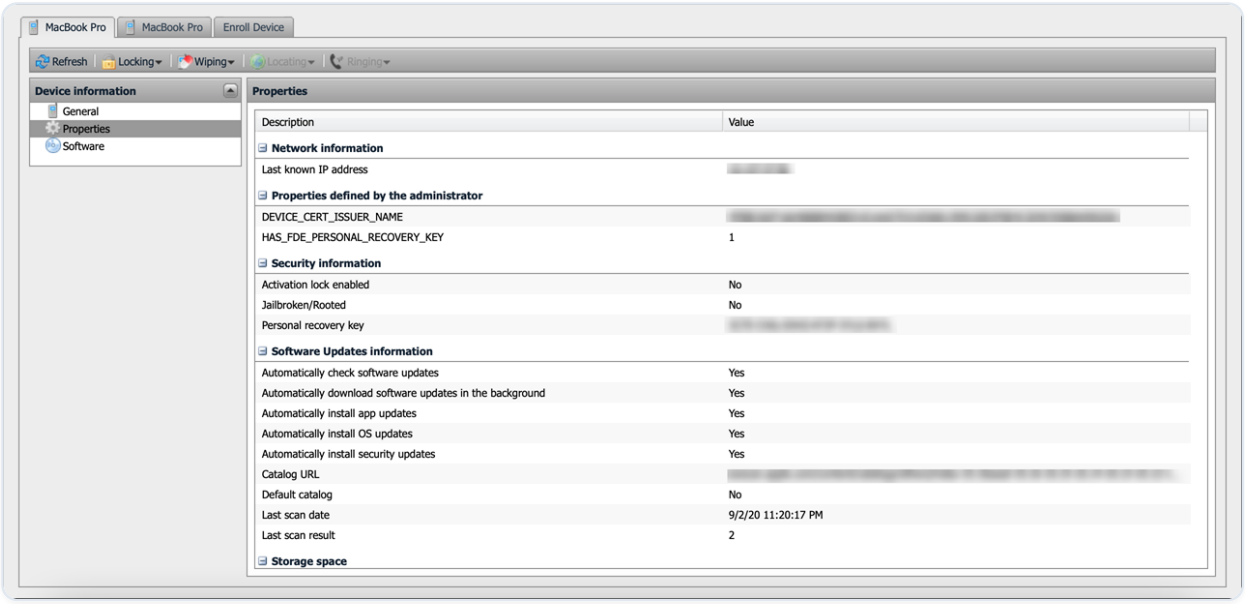


- **Custodiar clave de recuperación personal:** Cuando está habilitado, los usuarios pueden almacenar una copia de la clave de recuperación personal para cada dispositivo con Citrix Endpoint Management.



Para acceder a la clave desde Citrix Endpoint Management, vaya a **Administrar > Dispositivos**, seleccione el dispositivo macOS y haga clic en **Editar**. Luego, vaya a **Detalles del dispositivo > General** y localice la **Clave de recuperación personal**.

Para permitir que los usuarios vean su clave de recuperación desde el portal de autoservicio, habilite **Custodiar clave de recuperación personal** y **Mostrar clave de recuperación personal al usuario**. La clave aparece en el portal de autoservicio en la página **Propiedades** en **Información de seguridad**. Para obtener más información sobre el portal de autoservicio, consulte Portal de autoservicio.



Puede habilitar la configuración **Custodiar clave de recuperación personal** incluso si no habilita la configuración **Habilitar FileVault**. Si deshabilita la configuración **Habilitar FileVault**, los usuarios aún pueden habilitar FileVault por su cuenta. En esta situación, habilite **Custodiar clave de recuperación personal** para permitir que los usuarios almacenen una copia de su clave con Citrix Endpoint Management.

Si un usuario habilita FileVault antes de inscribir el dispositivo en Citrix Endpoint Management, Citrix Endpoint Management no almacena su clave de recuperación. El dispositivo aparece como habilitado para FileVault en la consola.

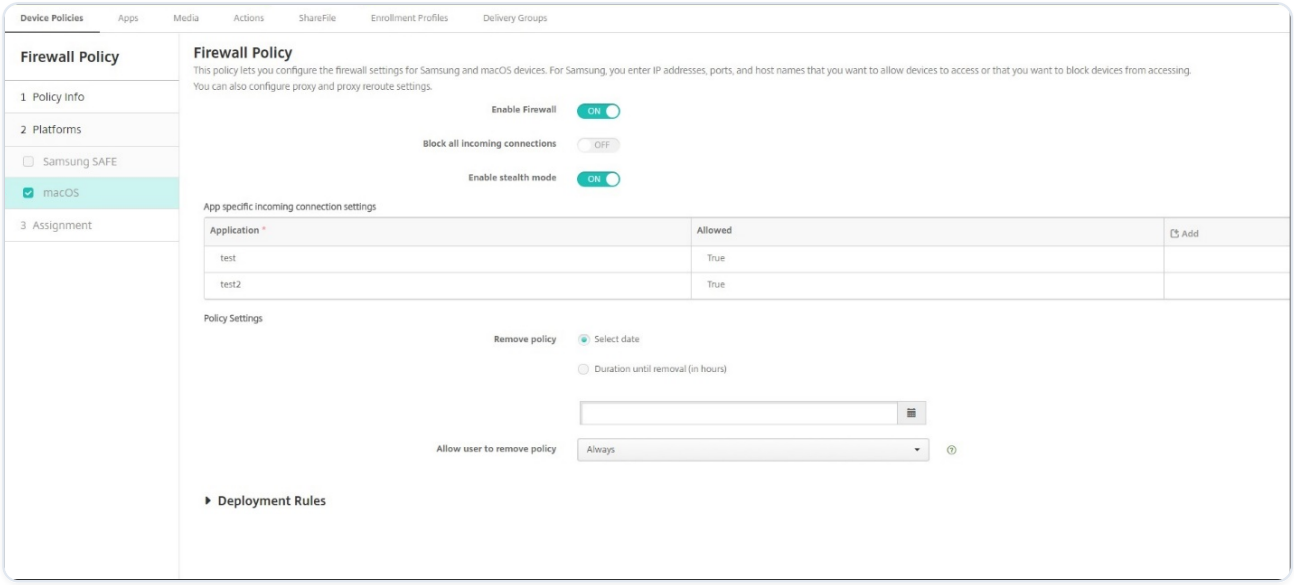
Política de dispositivo de firewall

Esta política le permite configurar los ajustes del firewall para dispositivos Samsung, macOS y Windows.

Para añadir o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de macOS

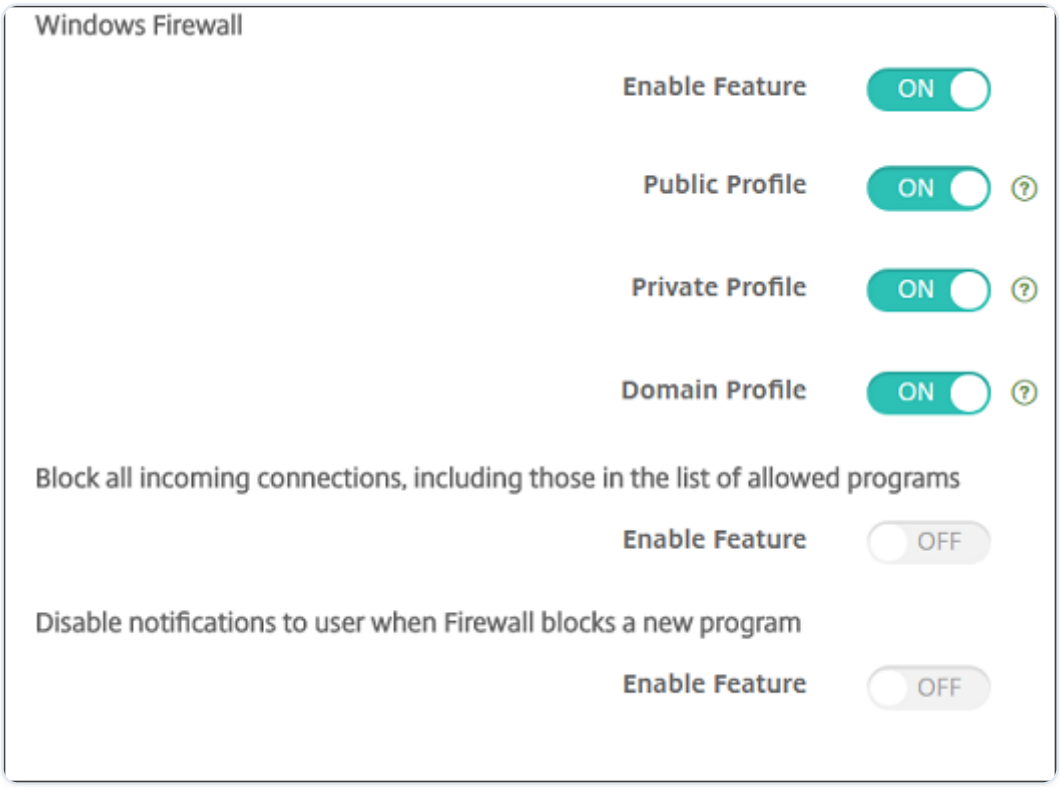
Requiere macOS 10.12 y versiones posteriores.



- **Habilitar firewall**. Para habilitar el firewall, establezca esta opción en **Activado**.
- **Bloquear todas las conexiones entrantes**. Cuando esta opción está establecida en **Activado**, bloquea todas las conexiones entrantes, excepto las conexiones necesarias para los servicios básicos.
- **Habilitar modo sigiloso**. En el modo sigiloso, el dispositivo no responde ni reconoce los intentos de acceso desde la red por parte de aplicaciones de prueba que utilizan ICMP, como Ping. Para habilitar el modo sigiloso, establezca esta opción en **Activado**.
- **Configuración de conexión entrante específica de la aplicación**. Para permitir que aplicaciones específicas reciban conexiones, añada las aplicaciones y establezca **Permitido** en **Verdadero**.

Configuración de Windows Desktop y Tablet

Requiere dispositivos Windows Desktop y Tablet que ejecuten Windows 10 (versión 1709 o posterior) o Windows 11.



- **Habilitar función:** Controla el tráfico entrante y saliente en los equipos a los que se implementa esta política. El valor predeterminado es **Activado**.
- **Perfil público:** Controla el Firewall de Windows mientras los equipos están conectados a redes no confiables en lugares públicos, como un aeropuerto o una cafetería. El valor predeterminado es **Activado**.
- **Perfil privado:** Controla el Firewall de Windows mientras los equipos están conectados a redes de confianza, como su red doméstica. El valor predeterminado es **Activado**.
- **Perfil de dominio:** Controla el Firewall de Windows mientras los equipos están conectados a las redes de dominio, como en su lugar de trabajo. El valor predeterminado es **Activado**.
- **Bloquear todas las conexiones entrantes, incluidas las de la lista de programas permitidos:** El valor predeterminado es **Desactivado**.
- **Deshabilitar las notificaciones al usuario cuando el Firewall bloquea un nuevo programa:** El valor predeterminado es **Desactivado**.

Directiva de dispositivo de fuente

Puede agregar una directiva de dispositivo en Citrix Endpoint Management para añadir más fuentes a los dispositivos iOS y macOS. Las fuentes deben ser TrueType (`.ttf`) u OpenType (`.oft`). Las colecciones de fuentes (`.ttc` o `.otc`) no son compatibles.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

- **Nombre visible para el usuario:** Escriba el nombre que los usuarios ven en sus listas de fuentes.
- **Archivo de fuente:** Para seleccionar el archivo de fuente que se agregará a los dispositivos de los usuarios, haga clic en **Examinar** y, a continuación, vaya a la ubicación del archivo.
- **Configuración de la directiva**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.

Configuración de macOS

- **Nombre visible para el usuario:** Escriba el nombre que los usuarios ven en sus listas de fuentes.
- **Archivo de fuente:** Para seleccionar el archivo de fuente que se agregará a los dispositivos de los usuarios, haga clic en **Examinar** y, a continuación, vaya a la ubicación del archivo.
- **Configuración de la directiva**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.
  - **Permitir al usuario eliminar la directiva:** Puede seleccionar cuándo los usuarios pueden eliminar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**.

- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en macOS 10.7 y versiones posteriores.

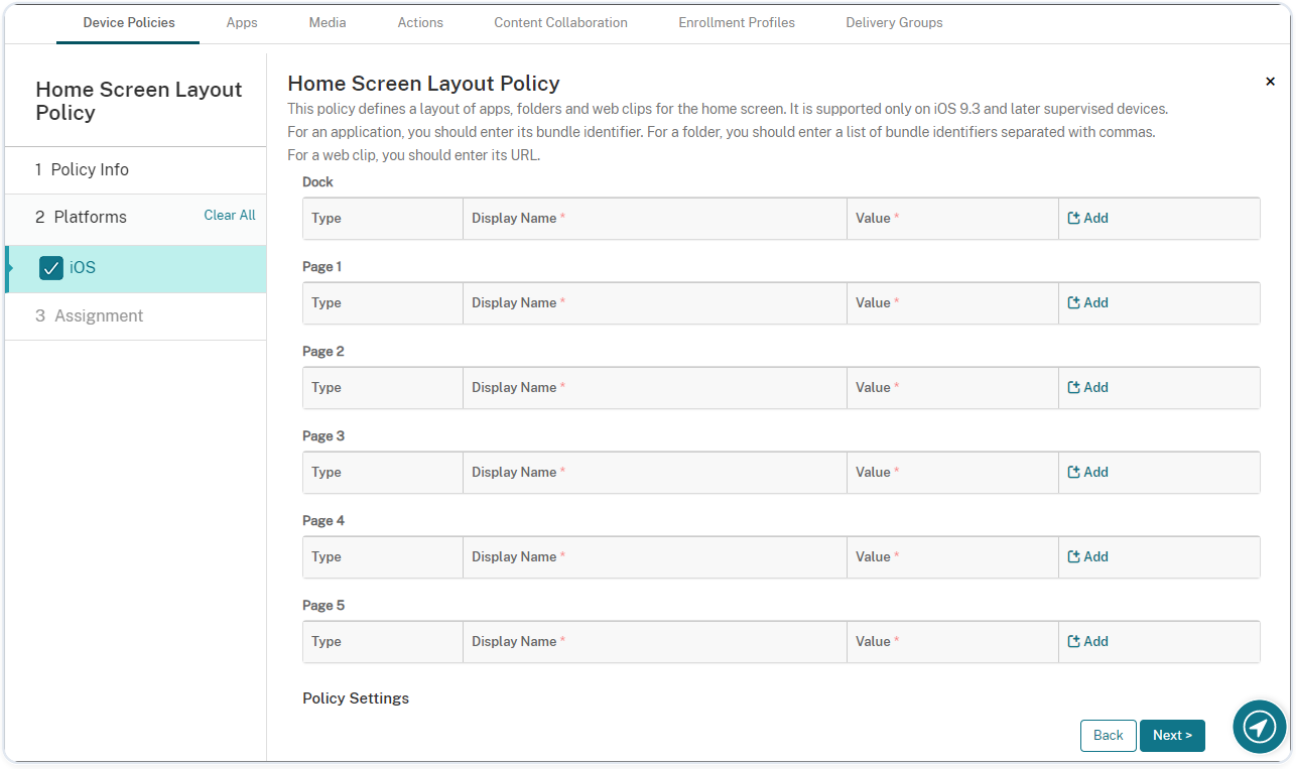
Política de dispositivo de diseño de pantalla de inicio

La política de dispositivo **Diseño de pantalla de inicio** le permite especificar el diseño de las aplicaciones y carpetas para la pantalla de inicio de iOS de los dispositivos iOS supervisados.

> **Importante:**
>
> La implementación de varias políticas de diseño de pantalla de inicio en un dispositivo provoca un error de iOS en el dispositivo. Esta limitación se aplica tanto si define la pantalla de inicio a través de esta política de Citrix Endpoint Management como a través de Apple Configurator.

> Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

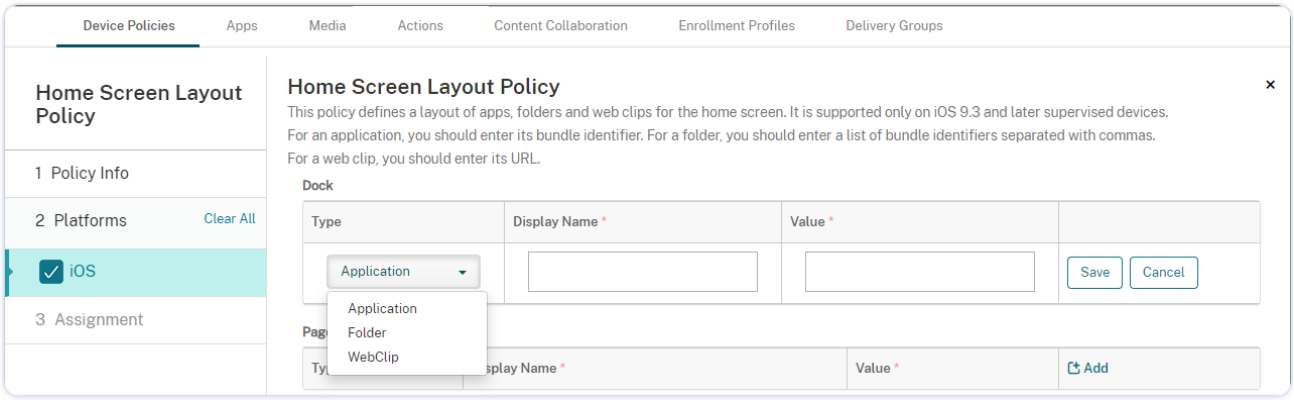
Configuración de iOS



- Para cada una de las áreas de pantalla que desee configurar (como **Dock** o **Página 1**), haga clic en **Agregar**.
- **Tipo:** Elija **Aplicación**, **Carpeta** o **Web Clip**.

  La configuración **Uso restringido de aplicaciones > Permitir solo algunas aplicaciones** en la política de dispositivo de restricciones puede impedir que los web clips aparezcan correctamente en la pantalla de inicio. Para que los web clips aparezcan correctamente, haga lo siguiente:

  - Establezca **Uso restringido de aplicaciones** en **Permitir todas las aplicaciones** o **No permitir algunas aplicaciones**.
  - Con **Uso restringido de aplicaciones** establecido en **Permitir solo algunas aplicaciones**, agregue una aplicación con el ID de paquete `com.apple.webapp` para permitir los web clips.



- **Nombre para mostrar:** El nombre que aparecerá en la pantalla de inicio para la aplicación o carpeta.
- **Valor:** Para las aplicaciones, escriba el identificador de paquete. Para las carpetas, escriba una lista de identificadores de paquete, separados por comas. Para los web clips, escriba el ID de paquete `com.apple.webClip.managed` y configure la URL del web clip en la política de web clips. Si existe más de un valor de Web Clip con la misma URL, el comportamiento no está definido en dispositivos iOS 11.3 y posteriores.
- **Configuración de la directiva**

  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**

    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.

    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.

  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en iOS 9.3 y versiones posteriores.

Importar política de dispositivo de perfil de iOS y macOS

Puede importar archivos XML de configuración de dispositivos para dispositivos iOS y macOS en Citrix Endpoint Management. El archivo contiene políticas de seguridad y restricciones de dispositivos que prepara con Apple Configurator 2 o Profile Creator. El archivo XML de configuración puede contener macros. Para obtener más información, consulte Macros.

Casos de uso

Importe las siguientes configuraciones creadas fuera de Citrix Endpoint Management para dispositivos macOS mediante Profile Creator:

- **Control de políticas del sistema:** La política identifica las aplicaciones firmadas por desarrolladores certificados de Apple y permite a los usuarios descargar aplicaciones verificadas de Mac App Store.

  Al configurar la política:

  - Seleccione **Habilitar Gatekeeper** para asegurarse de que los usuarios ejecuten solo software verificado y de confianza.
  - Seleccione **Permitir desarrolladores identificados** para asegurarse de que los usuarios instalen solo aplicaciones firmadas por desarrolladores certificados de Apple.

- **Control de políticas de preferencias de privacidad:** La política le permite conceder o restringir el acceso entre aplicaciones a determinados archivos o funciones, como los servicios de ubicación, la cámara y la captura de pantalla.

  Configure los ajustes que planea implementar. Para obtener más información, consulte Configuración de la carga útil de Control de políticas de preferencias de privacidad.

- **Política de extensiones de kernel:** La política permite a los usuarios instalar extensiones de aplicaciones que amplían las capacidades nativas del sistema operativo. Las extensiones de kernel se ejecutan a nivel de kernel.

Configure los ajustes que planea implementar. Para obtener más información, consulte Configuración de la carga útil de la política de extensiones de kernel.

- **Política de configuración de Ethernet:** La política le permite administrar la conexión de red Ethernet.

  Configure los ajustes que planea implementar. Para obtener más información, consulte Configuración de Ethernet.

Utilice Apple Configurator 2 o Profile Creator para configurar las siguientes políticas para dispositivos macOS e iOS:

- **Política de Wi-Fi:** La política le permite gestionar cómo los usuarios conectan sus dispositivos a una red Wi-Fi.

  Al configurar la política:

  - Añada el SSID de destino a la parte superior de la lista de prioridades.
  - Elija el modo de conexión que se utilizará cuando el usuario se una a una red. Si selecciona **Sistema**, el dispositivo utiliza las credenciales del sistema para autenticar al usuario. Si selecciona **Ventana de inicio de sesión**, el dispositivo utiliza las mismas credenciales introducidas en la ventana de inicio de sesión para autenticar al usuario.

  Para obtener más información, consulte Configuración de Wi-Fi.
- **Política de restricciones:** La política permite o restringe el uso de ciertas funciones en los dispositivos de los usuarios.

  Configure los ajustes que planea implementar. Para obtener más información, consulte Descripción general de las restricciones.
- **Política de VPN:** La política proporciona una conexión cifrada a nivel de dispositivo a redes privadas.

  Configure los ajustes que planea implementar. Para obtener más información, consulte la Descripción general de VPN.

Crear un perfil de configuración con Apple Configurator 2

1. Instale Apple Configurator 2 desde la App Store de Apple.
2. Inicie Apple Configurator 2 y vaya a **Archivo > Nuevo perfil**. Aparece una nueva ventana de configuración.

3. En el panel de configuración **General**, escriba un nombre y un identificador para su perfil, y luego añada cualquier opción de carga útil adicional.
4. En el panel izquierdo, seleccione una carga útil, haga clic en **Configurar** e introduzca los ajustes. No firme su perfil, ya que los perfiles firmados no son compatibles.

   Para añadir varias cargas útiles dentro de un único perfil, seleccione una carga útil y haga clic en el botón **Añadir carga útil** en la esquina superior derecha.
5. Vaya a **Archivo > Guardar**, elija un nombre y una ubicación para guardar el archivo XML y haga clic en **Guardar**.

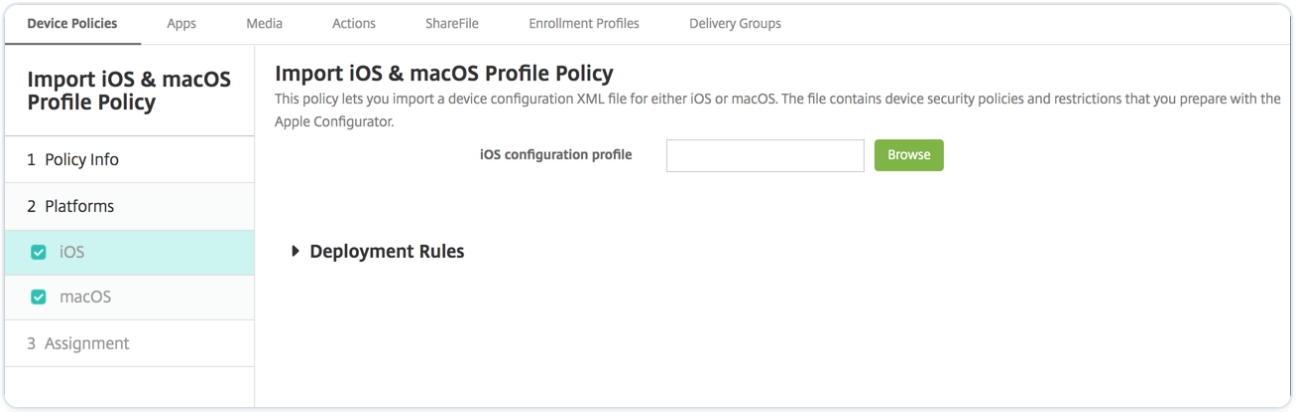
Crear un perfil de configuración con Profile Creator

1. Instale Profile Creator desde GitHub.
2. Inicie Profile Creator y vaya a **Archivo > Nuevo**. Aparece una nueva ventana de configuración.
3. En el panel de configuración **General**, escriba un nombre y una descripción para su perfil y, a continuación, agregue cualquier opción de carga útil adicional.
   - Recomendación: Seleccione **Impedir que los usuarios eliminen este perfil**.
   - Establezca **Ámbito de carga útil** en **Sistema** o **Usuario**.
4. En el panel izquierdo, elija la directiva, configure los ajustes y haga clic en **Agregar** en la esquina superior derecha.

   Para configurar varias directivas dentro de un único perfil, seleccione una directiva y haga clic en el botón **Agregar**.
5. Vaya a **Archivo > Exportar**, elija un nombre y una ubicación para guardar el archivo XML y haga clic en **Guardar**.

Para importar un archivo de configuración para la directiva de dispositivos de perfil de iOS y macOS en la consola de Citrix Endpoint Management, vaya a **Configurar > Directivas de dispositivos**. Para obtener más información, consulte Directivas de dispositivos.

Configuración de iOS y macOS



- **Perfil de configuración de iOS** o **perfil de configuración de macOS:** Para seleccionar el archivo de configuración que se va a importar, haga clic en **Examinar** y, a continuación, vaya a la ubicación del archivo.

Aplicación del cumplimiento para dispositivos Android (versión preliminar técnica)

> **Nota:**
>
> Las funciones de la versión preliminar técnica están disponibles para su uso en entornos de no producción o de producción limitada, y para ofrecer a los clientes la oportunidad de compartir sus comentarios. Citrix® no acepta casos de soporte para funciones en versión preliminar técnica, pero agradece los comentarios para mejorarlas. Puede enviar sus comentarios sobre esta función haciendo clic en **Envíenos sus comentarios**. Citrix podría actuar en función de los comentarios según su gravedad, criticidad e importancia.

Para los dispositivos Android inscritos en el modo *Propietario del dispositivo*, el administrador del cliente puede gestionar el cumplimiento del dispositivo. Pueden definir reglas personalizadas para evaluar el cumplimiento, incluyendo:

- Garantizar que la solidez de la contraseña del dispositivo cumpla con los estándares especificados.
- Verificar la instalación de todas las aplicaciones requeridas.
- Confirmar la eliminación de cualquier aplicación prohibida.

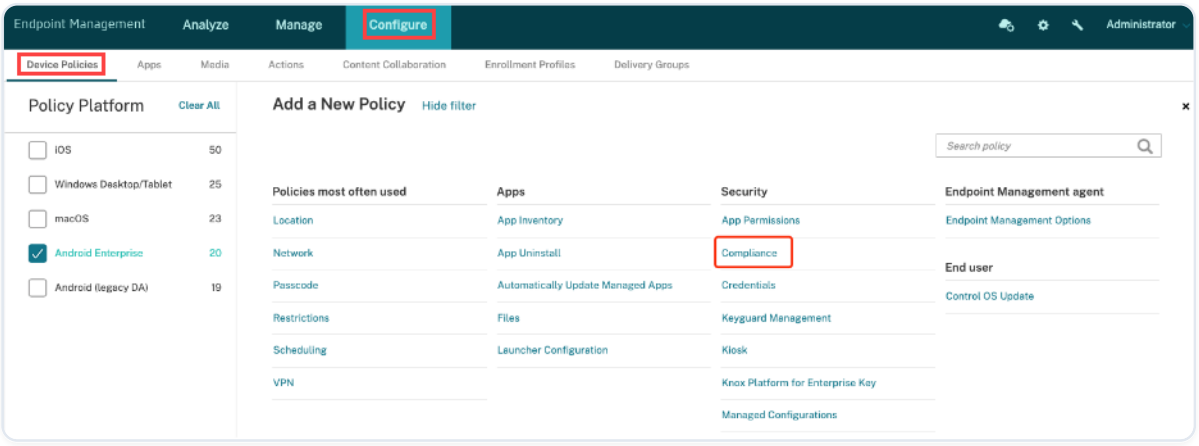
En los casos en que se detecte que los dispositivos no cumplen las normas, los clientes pueden pedir a los usuarios que rectifiquen los problemas. Además, hay disponibles medidas más estrictas, como la congelación de aplicaciones en el dispositivo para restringir el acceso del usuario hasta que se logre el cumplimiento. Para habilitar esta funcionalidad, son necesarios dos requisitos previos, ya que se requieren cambios tanto en el lado del servidor como en el del cliente:

- Actualice el servidor CEM a la versión 24.8.0.
- Actualice Secure Hub a la versión 24.8.0.

Procedimiento de gestión del cumplimiento de dispositivos Android

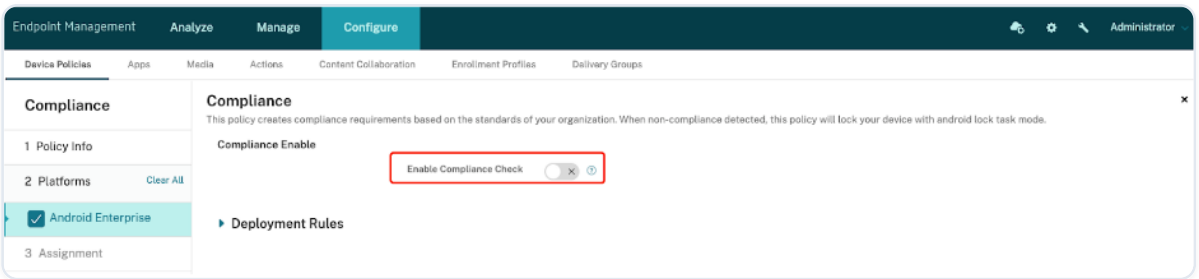
1. Active el indicador de función `afw.policy.compliance` específicamente para el servidor CEM.
2. Agregue e implemente la política de cumplimiento.

    a. En la ficha **Configurar**, seleccione **Directivas de dispositivo** y haga clic en **Cumplimiento**.

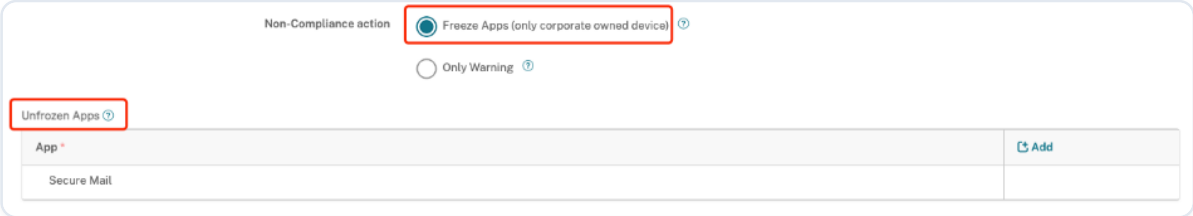


    b. Configure la política con los siguientes ajustes:

        - Habilitar **Comprobación de cumplimiento**: Este ajuste controla si los dispositivos se someten a comprobaciones de cumplimiento. Para revocar una política de cumplimiento implementada, deshabilite esta opción y vuelva a implementar la política. Simplemente eliminar la política del grupo de entrega no será efectivo.



- Acción de incumplimiento: Elija entre **Solo advertencia** y **Congelar aplicaciones (solo dispositivos corporativos)**. Seleccionar **Solo advertencia** notificará a los usuarios en Secure Hub sobre los elementos no conformes y les pedirá que solucionen estos problemas. Elegir **Congelar aplicaciones (solo dispositivos corporativos)** bloquea todas las aplicaciones del dispositivo, pero los administradores pueden personalizar una lista de aplicaciones no congeladas para eximir aplicaciones específicas, como Secure Hub (para mostrar y resolver elementos no conformes), Google Play Store (para instalar las aplicaciones necesarias), Ajustes (para restablecimientos de fábrica) y SMS (para comunicación de emergencia). La opción **Congelar aplicaciones (solo dispositivos corporativos)** solo es aplicable a dispositivos corporativos.



- verificar Cumplimiento de código de acceso: Comprueba si los códigos de acceso del dispositivo cumplen con los estándares especificados. Se utiliza normalmente con políticas de código de acceso.
- verificar Aplicaciones requeridas: Muestra una lista de aplicaciones obligatorias. Garantiza que estas aplicaciones estén instaladas en el dispositivo.

Nota:

- Las aplicaciones enumeradas en **Aplicaciones requeridas** también deben incluirse en la sección de aplicaciones requeridas del grupo de entrega para garantizar su funcionalidad. De lo contrario, no serán efectivas.
- Dado que las aplicaciones requeridas podrían no estar disponibles en Google Play administrado, los usuarios finales permanecerán en modo bloqueado.



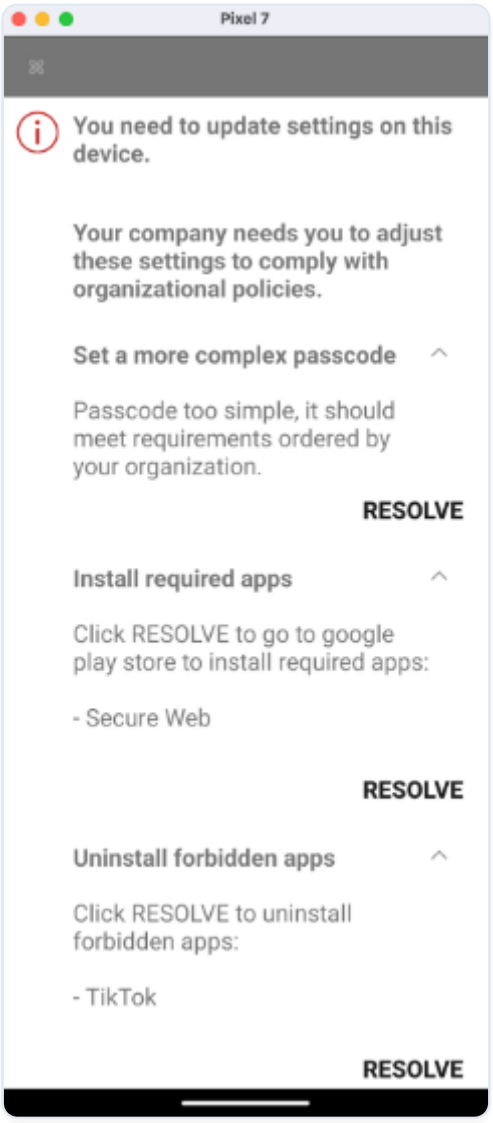
- verificar Aplicaciones prohibidas: Muestra una lista de aplicaciones prohibidas. Garantiza que ninguna de estas aplicaciones esté instalada.

> **Nota:**
>
> Los administradores deben abstenerse de añadir aplicaciones preinstaladas del sistema a la lista de **Aplicaciones prohibidas**, ya que los usuarios finales no tienen permiso para eliminarlas.

3. Implementar política.

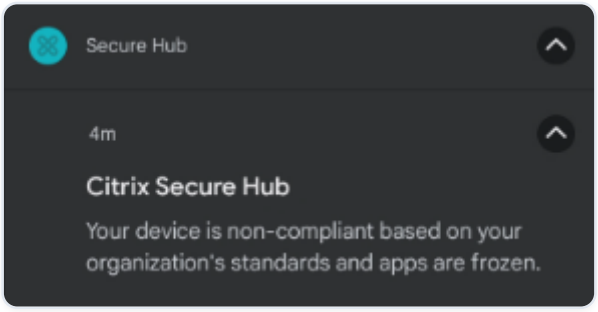
   a. En Secure Hub, haga clic en Actualizar política o espere a que la sincronización periódica de 6 horas implemente la política en los dispositivos.

   b. Tras la implementación, se activa inmediatamente una comprobación de cumplimiento. Los dispositivos no conformes en modo Congelar aplicaciones restringen tanto el dispositivo como sus aplicaciones hasta que se cumpla la conformidad.



Si el administrador configura la Acción de no conformidad para Congelar aplicaciones, tanto Secure Hub como el propio dispositivo restringirán el uso de las aplicaciones. En concreto:

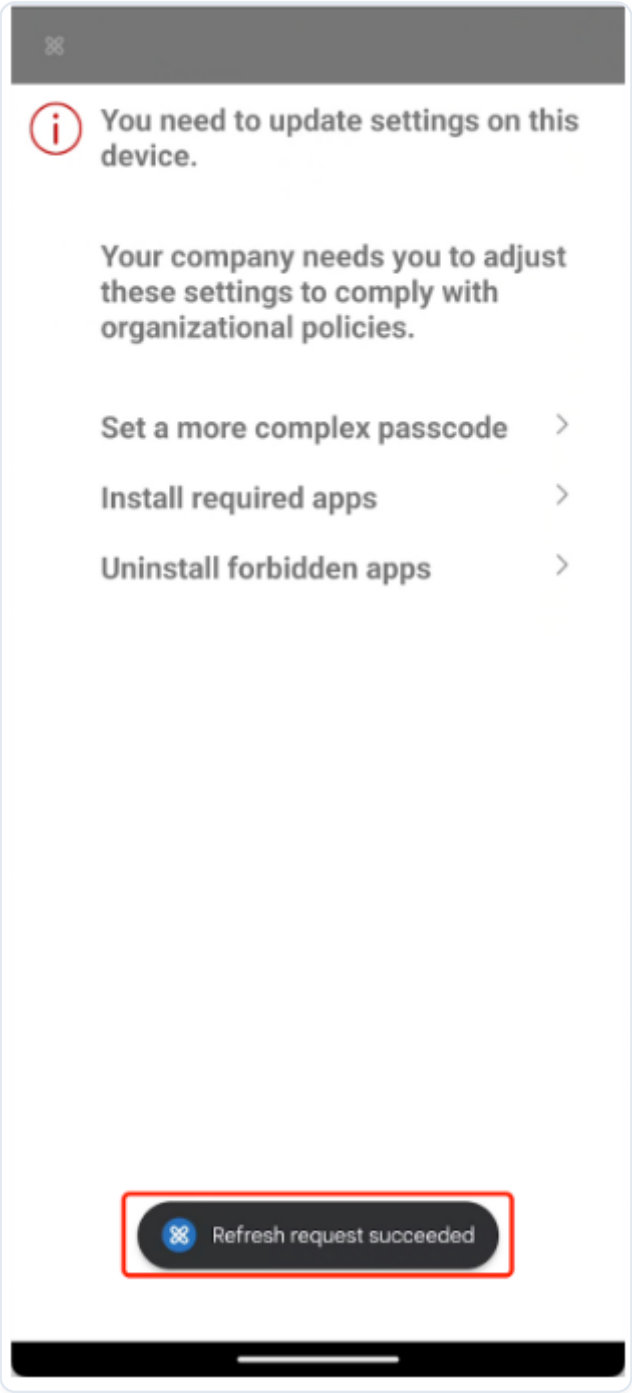
- Aparecerá una notificación persistente en la barra de notificaciones, recordando al usuario que las aplicaciones se han congelado.



- Las aplicaciones, excluidas las que figuran como permitidas por defecto o en la lista de **Aplicaciones descongeladas**, se congelarán y no responderán al hacer clic en ellas.
- Este estado persiste hasta que el dispositivo cumple con la conformidad. Incluso después de reiniciar o de una actualización del sistema, el dispositivo volverá inmediatamente a este estado congelado (excepto durante las actualizaciones de Secure Hub, que requieren un inicio manual por parte del usuario).

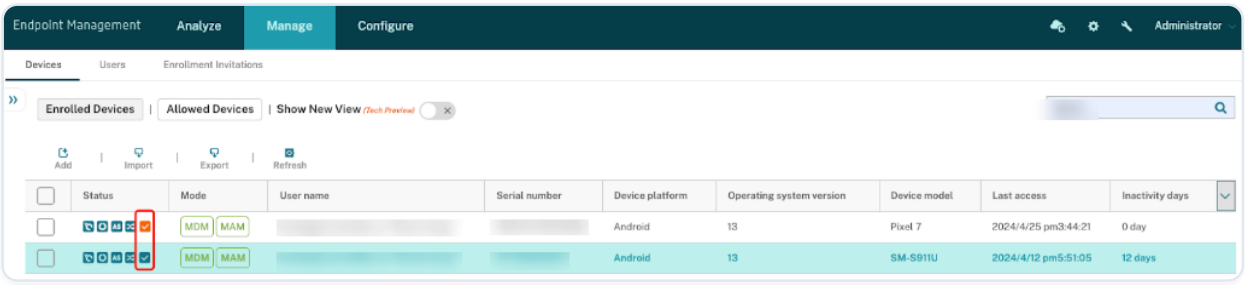
4. Resolución de no conformidad:

- Cuando un dispositivo no es conforme, Secure Hub no puede actualizar la política mediante el método habitual (haciendo clic en el botón **Actualizar política** en la página de **Información del dispositivo**).
- En su lugar, se proporciona una solución alternativa deslizando hacia abajo la página que muestra los elementos no conformes, y el resultado de la actualización se comunica mediante una notificación emergente.

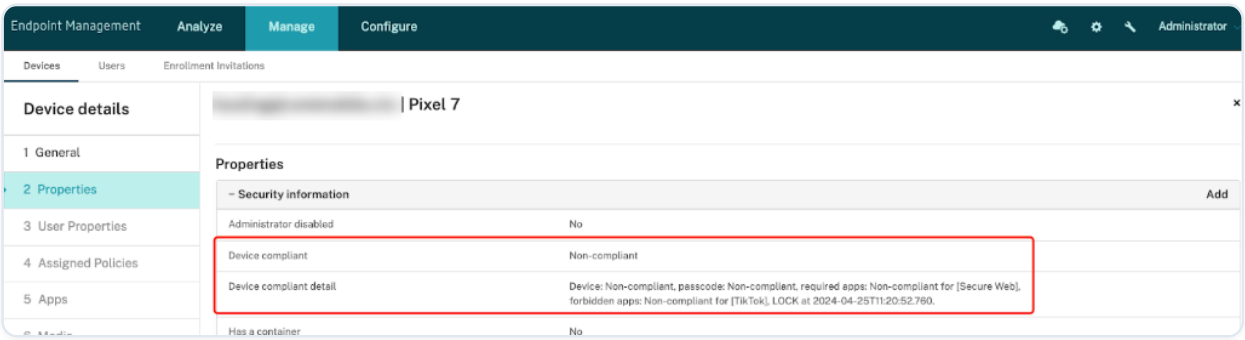


- Acciones específicas para los usuarios:
  - Establecer un código de acceso más complejo para cumplir los estándares.
  - Instalar las aplicaciones necesarias desde Google Play Store.
  - Desinstalar aplicaciones prohibidas.

5. Supervisión del cumplimiento
   - Ver el estado de cumplimiento: Un nuevo icono de estado de cumplimiento en **Administrar** -> **Dispositivos** -> **Estado**. El verde indica cumplimiento, mientras que el naranja indica incumplimiento.

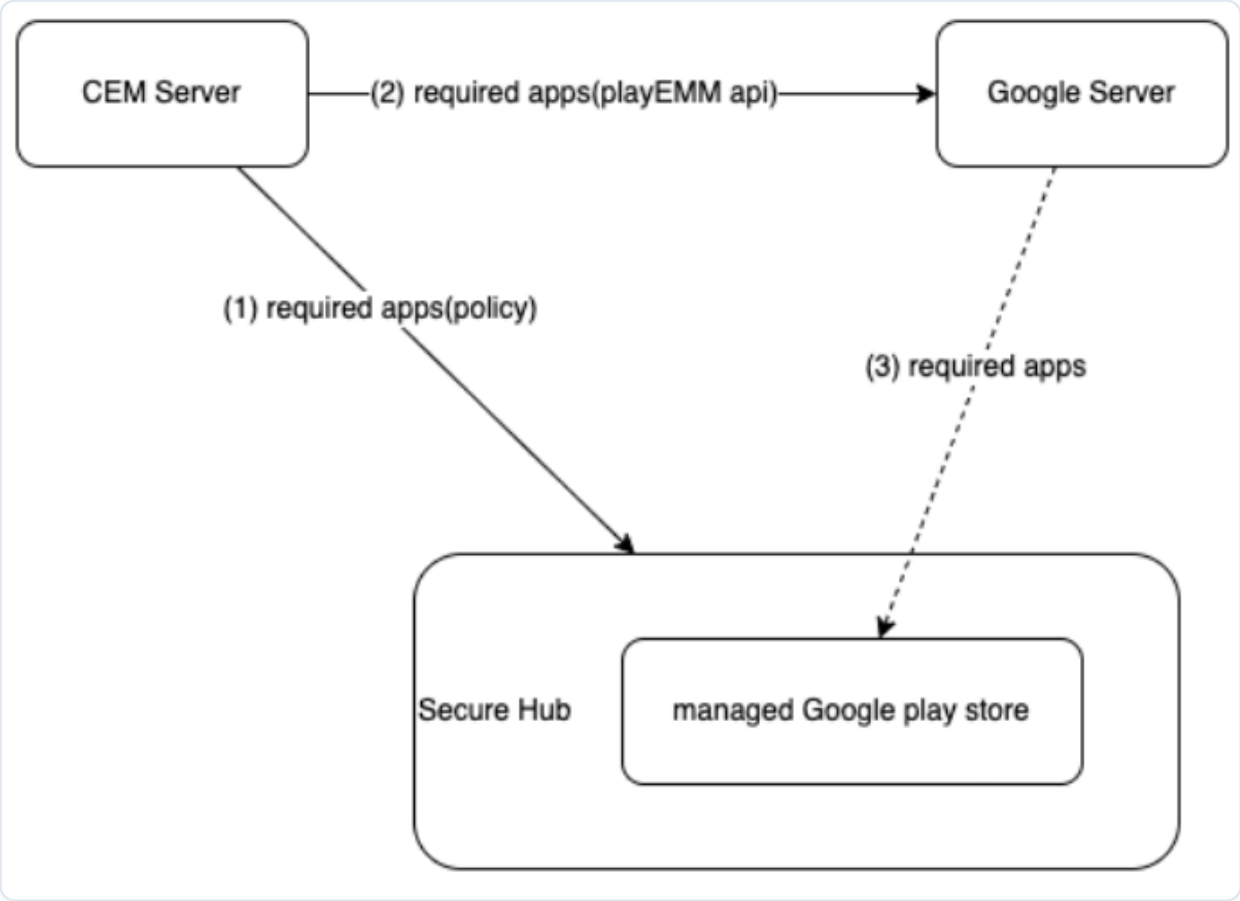


- Estado de cumplimiento detallado disponible en **Administrar** -> **Dispositivos** -> **Detalles del dispositivo** -> **Propiedades** -> **Información de seguridad**.



Solución de problemas

1. La aplicación requerida configurada no se encuentra en Google Play Store, lo que provoca que el dispositivo no cumpla las normas y no pueda resolver el problema. Esto es un fallo de diseño.



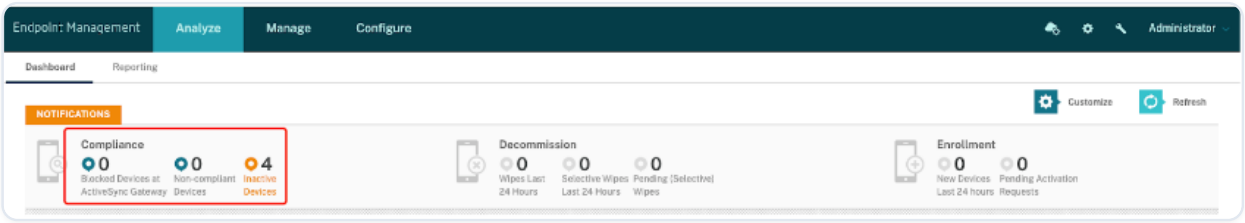
El servidor CEM envía las aplicaciones requeridas a Secure Hub y a los servidores de Google a través de los enlaces 1 y 2, pero el enlace 3 está fuera de nuestro control. Cuando Secure Hub comprueba las aplicaciones requeridas mediante el enlace 1, no podemos garantizar que Google Play Store administrado tenga estas aplicaciones disponibles. Esta discrepancia significa que, si bien la política de cumplimiento requiere que Secure Hub instale estas aplicaciones, es posible que no se encuentren en la tienda de inmediato. Normalmente, los servidores de Google envían las aplicaciones requeridas al dispositivo en un plazo de 24 horas mediante el enlace 3.

2. Antes de actualizar Secure Hub, el dispositivo no cumplía las normas y las aplicaciones estaban congeladas. Sin embargo, después de actualizar Secure Hub, todas las aplicaciones se descongelaron. Esto ocurrió porque durante el proceso de actualización, la operación de Secure Hub se interrumpió, lo que impidió que mantuviera la congelación de las aplicaciones. Este problema es conocido y actualmente no tiene solución. Estamos trabajando activamente con Google para abordarlo y esperamos mejoras en futuras versiones. Una vez completada la actualización, los usuarios pueden iniciar Secure Hub manualmente para iniciar el proceso y restaurar las aplicaciones a su estado congelado.
3. ¿Cómo descongelar aplicaciones? El método más común es que los usuarios resuelvan todos los problemas de incumplimiento, lo que hace que el dispositivo cumpla las normas y

descongele automáticamente todas las aplicaciones. Si no es factible lograr el cumplimiento rápidamente, se pueden seguir los siguientes pasos:

- Agregue las aplicaciones relacionadas a la lista de aplicaciones descongeladas y realice una actualización deslizando hacia abajo.
- Cambie la acción de incumplimiento a Advertencia y realice una actualización deslizando hacia abajo.
- Deshabilite el interruptor de verificación correspondiente a los elementos no conformes o el interruptor maestro, luego realice una actualización deslizando hacia abajo.
- Si ninguno de los métodos anteriores funciona, habilite la marca de función `afw.locktaskmode.disable` para el servidor CEM específico y realice una actualización manual. Esta acción desbloquea forzosamente todas las aplicaciones, pero Secure Hub permanece bloqueado de forma similar a cuando la Acción de incumplimiento se establece en **Advertencia**.
- Deshabilite la marca de función `afw.policy.compliance` para el servidor CEM específico y realice una actualización manual.
- En el peor de los casos, si Secure Hub no puede conectarse al servidor CEM, realice un restablecimiento de fábrica desde Ajustes.

4. El estado de cumplimiento que se muestra en Analizar -> Panel de control es un tipo de cumplimiento diferente en Citrix Endpoint Management™ al que se hace referencia en esta política. Esta función aún no se ha desarrollado y se mejorará en futuras versiones.



5. Esta función no se aplica a los dispositivos registrados mediante los modos COSU/WPCOD/BYOD. Actualmente, solo es compatible con dispositivos registrados en el modo Propietario del dispositivo (DO).

Política de dispositivos de administración de Keyguard

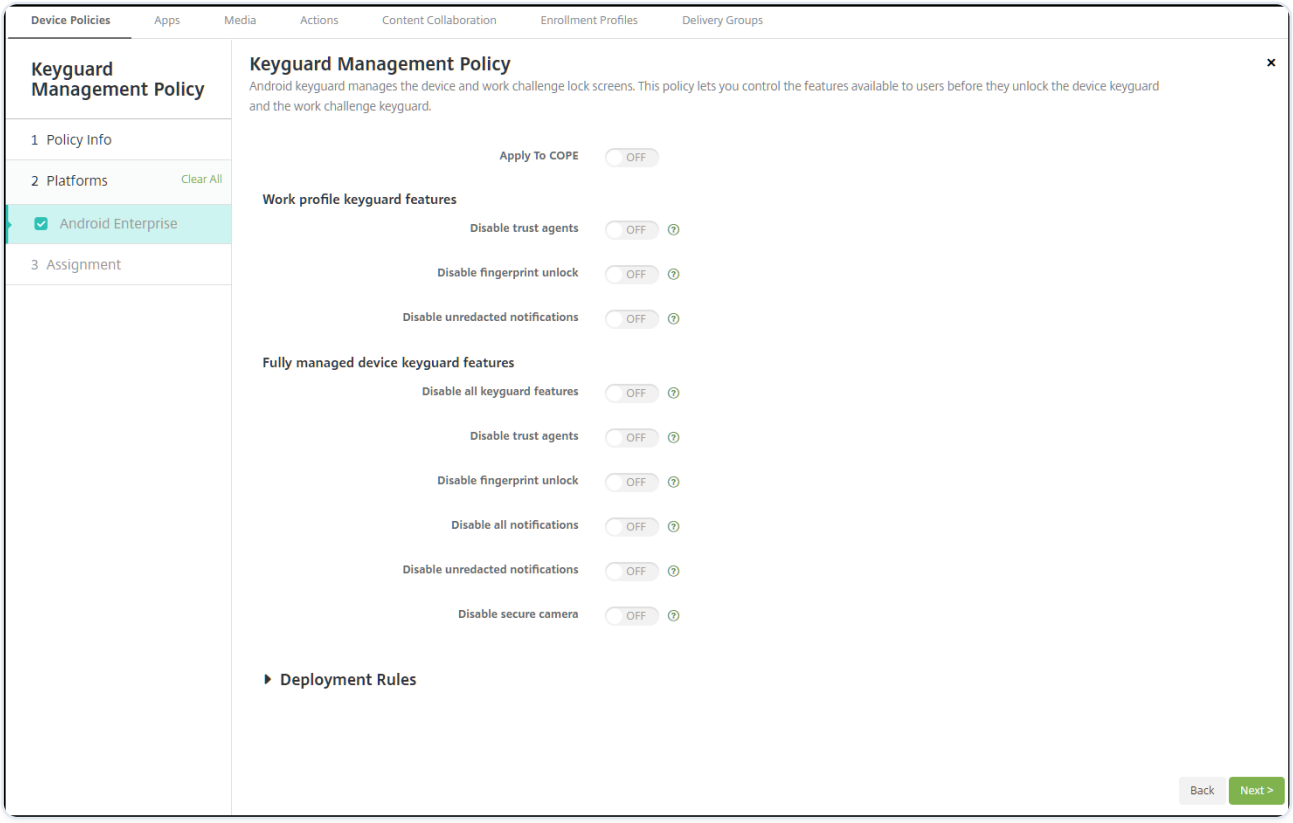
El keyguard de Android gestiona las pantallas de bloqueo del dispositivo y del desafío de trabajo. Esta política le permite gestionar las funciones del keyguard del perfil de trabajo de Android Enterprise y del keyguard avanzado del dispositivo. Puede controlar:

- Administración de Keyguard en dispositivos con perfil de trabajo. Puede especificar las funciones disponibles para los usuarios antes de que desbloqueen el keyguard del dispositivo y el keyguard del desafío de trabajo. Por ejemplo, de forma predeterminada, los usuarios pueden usar el desbloqueo por huella dactilar y ver notificaciones sin censura en la pantalla de bloqueo.
- Administración de Keyguard en dispositivos totalmente administrados y dedicados. Puede especificar las funciones disponibles, como agentes de confianza y cámara segura, antes de que desbloqueen la pantalla de Keyguard. O bien, puede optar por deshabilitar todas las funciones de Keyguard.
- Administración de Keyguard en dispositivos totalmente administrados con perfiles de trabajo. Estos dispositivos se conocían anteriormente como dispositivos COPE (propiedad de la empresa, habilitados para uso personal). Puede usar una política de administración de Keyguard para aplicar configuraciones separadas al dispositivo y al perfil de trabajo.

Para agregar o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Vea este vídeo para obtener más información:

Configuración de Android Enterprise



- **Aplicar a COPE:** Le permite configurar los ajustes de la política de dispositivos de administración de Keyguard para dispositivos totalmente administrados con perfiles de trabajo.

  Cuando esta configuración está **Activada**, puede aplicar configuraciones separadas al dispositivo y al perfil de trabajo en dispositivos totalmente administrados con perfiles de trabajo.

  Cuando esta configuración está **Desactivada**, puede aplicar configuraciones a dispositivos con perfil de trabajo o a dispositivos totalmente administrados. Las configuraciones que establezca para los perfiles de trabajo solo se aplican a los dispositivos con perfil de trabajo. Las configuraciones que establezca para los dispositivos totalmente administrados solo se aplican a los dispositivos totalmente administrados.

  El valor predeterminado es **Desactivado**.
- **Funciones de Keyguard del perfil de trabajo:** Controla si las siguientes funciones están disponibles antes de que un usuario desbloquee el keyguard del perfil de trabajo (pantalla de bloqueo).
  - **Deshabilitar agentes de confianza:** Si está **Desactivado**, los agentes de confianza pueden operar en pantallas de bloqueo seguras cuando se establece un desafío en el perfil de trabajo. Establézcalo en **Activado** para deshabilitar todos los agentes de confianza en el perfil de trabajo. El valor predeterminado es **Desactivado**.
  - **Deshabilitar autenticación biométrica:** Si está **Desactivado**, la autenticación biométrica está disponible en pantallas de bloqueo seguras cuando se establece un desafío en el perfil de trabajo. Establézcalo en **Activado** para deshabilitar la autenticación biométrica en el perfil de trabajo. Esta configuración deshabilita el desbloqueo por huella dactilar, la autenticación facial y la autenticación por iris. El valor predeterminado es **Desactivado**. Para Android 9.0 y versiones posteriores.
  - **Deshabilitar desbloqueo por huella dactilar:** Si está **Desactivado**, el desbloqueo por huella dactilar está disponible en pantallas de bloqueo seguras cuando se establece un desafío en el perfil de trabajo. Establézcalo en **Activado** para deshabilitar el desbloqueo por huella dactilar en el perfil de trabajo. El valor predeterminado es **Desactivado**.
  - **Deshabilitar autenticación facial:** Si está **Desactivado**, la autenticación facial está disponible en pantallas de bloqueo seguras cuando se establece un desafío en el perfil de trabajo. Establézcalo en **Activado** para deshabilitar la autenticación facial en el perfil de trabajo. El valor predeterminado es **Desactivado**. Para Android 9.0 y versiones posteriores.

  - **Deshabilitar autenticación por iris:** Si está **Desactivado**, la autenticación por iris está disponible en pantallas de bloqueo seguras cuando se establece un desafío en el perfil de trabajo. Establézcalo en **Activado** para deshabilitar la autenticación por iris en el perfil de trabajo. El valor predeterminado es **Desactivado**. Para Android 9.0 y versiones posteriores.
  - **Deshabilitar notificaciones no redactadas:** Si está **Desactivado**, tanto las notificaciones redactadas como las no redactadas aparecen en las pantallas de bloqueo seguras. Establézcalo en **Activado** para deshabilitar las notificaciones no redactadas y mostrar solo las notificaciones redactadas. El valor predeterminado es **Desactivado**.

- **Funciones de bloqueo de pantalla del dispositivo totalmente administrado:** Controla si las siguientes funciones están disponibles antes de que un usuario desbloquee la pantalla de bloqueo del dispositivo. Estas funciones se aplican a dispositivos totalmente administrados o dedicados.

  - **Deshabilitar todas las funciones de bloqueo de pantalla:** Si está **Desactivado**, todas las personalizaciones de bloqueo de pantalla actuales y futuras están disponibles en las pantallas de bloqueo seguras. Establézcalo en **Activado** para deshabilitar todas las personalizaciones de bloqueo de pantalla. El valor predeterminado es **Desactivado**.
  - **Deshabilitar agentes de confianza:** Si está **Desactivado**, los agentes de confianza pueden operar en pantallas de bloqueo seguras. Establézcalo en **Activado** para deshabilitar los agentes de confianza. El valor predeterminado es **Desactivado**.
  - **Deshabilitar autenticación biométrica:** Si está **Desactivado**, la autenticación biométrica está disponible en pantallas de bloqueo seguras cuando se establece un desafío en el dispositivo. Establézcalo en **Activado** para deshabilitar la autenticación biométrica en el dispositivo. Las funciones de autenticación biométrica deshabilitadas son el desbloqueo por huella dactilar, la autenticación facial y la autenticación por iris. El valor predeterminado es **Desactivado**. Para Android 9.0 y versiones posteriores.
  - **Deshabilitar desbloqueo por huella dactilar:** Si está **Desactivado**, el desbloqueo por huella dactilar está disponible en pantallas de bloqueo seguras cuando se establece un desafío en el dispositivo. Establézcalo en **Activado** para deshabilitar el desbloqueo por huella dactilar en el dispositivo. El valor predeterminado es **Desactivado**.
  - **Deshabilitar autenticación facial:** Si está **Desactivado**, la autenticación facial está disponible en pantallas de bloqueo seguras cuando se establece un desafío en el dispositivo. Establézcalo en **Activado** para deshabilitar la autenticación facial en el dispositivo. El valor predeterminado es **Desactivado**. Para Android 9.0 y versiones posteriores.

- **Deshabilitar autenticación por iris:** Si está **Desactivado**, la autenticación por iris está disponible en pantallas de bloqueo seguras cuando se establece un desafío en el dispositivo. Establézcalo en **Activado** para deshabilitar la autenticación por iris en el dispositivo. El valor predeterminado es **Desactivado**. Para Android 9.0 y versiones posteriores.
- **Deshabilitar todas las notificaciones:** Si está **Desactivado**, todas las notificaciones aparecen en las pantallas de bloqueo seguras. Establézcalo en **Activado** para mostrar todas las notificaciones. El valor predeterminado es **Desactivado**.
- **Deshabilitar notificaciones no redactadas:** Si está **Desactivado**, tanto las notificaciones redactadas como las no redactadas aparecen en las pantallas de bloqueo seguras. Establézcalo en **Activado** para deshabilitar las notificaciones no redactadas y mostrar solo las notificaciones redactadas. El valor predeterminado es **Desactivado**.
- **Deshabilitar cámara segura:** Si está en **Desactivado**, la cámara segura está disponible en las pantallas de bloqueo seguras. Establezca en **Activado** para deshabilitar la cámara segura. El valor predeterminado es **Desactivado**.

Directiva de quiosco

La directiva de quiosco le permite restringir los dispositivos al modo quiosco limitando las aplicaciones que se pueden ejecutar. Citrix Endpoint Management no controla qué parte del dispositivo se bloquea en el modo quiosco. El dispositivo administra la configuración del modo quiosco después de implementar la directiva.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Para configurar iPads para que se ejecuten en modo quiosco, utilice la directiva de dispositivo de bloqueo de aplicaciones. Para obtener información sobre cómo configurar iPads como quioscos, consulte Configurar un iPad como quiosco. También puede configurar un iPad para que abra solo un sitio web. Para obtener información, consulte la directiva de Webclip.

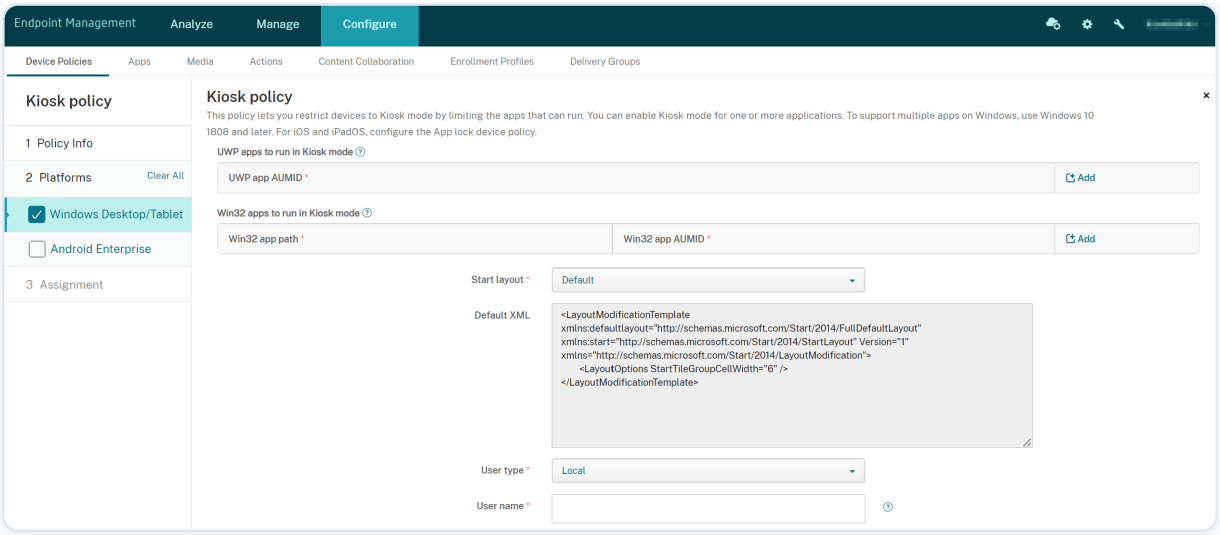
Configuración de Windows Desktop y Tablet

Para dispositivos Windows Desktop y Tablet, la directiva de quiosco se aplica solo a los usuarios locales y a los usuarios inscritos en Azure AD.

Una sola aplicación o varias aplicaciones pueden ejecutarse en modo quiosco en dispositivos Windows Desktop y Tablet.

Nota:

La directiva de dispositivo de quiosco se aplica solo a dispositivos Windows 10. Para implementar un quiosco de una sola aplicación en dispositivos Windows 11, puede usar la directiva de dispositivo XML personalizada para implementar el script XML que proporcionamos en los dispositivos. Para obtener más información, consulte Implementar un quiosco de una sola aplicación en dispositivos Windows 11.



- **AUMID de aplicación UWP:** Haga clic en **Agregar**, seleccione la aplicación de Plataforma universal de Windows (UWP) e introduzca el ID de modelo de usuario de aplicación (AUMID) para cada aplicación UWP. Por ejemplo, introduzca el siguiente AUMID:
  - `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`
- **Ruta de aplicación Win32** y **AUMID de aplicación Win32**: Haga clic en **Agregar**, seleccione la aplicación de escritorio de Windows (`Win32`) e introduzca la ruta y el AUMID para cada aplicación `Win32`. Por ejemplo, introduzca la siguiente ruta y AUMID:
  - `%windir%\system32\mspaint.exe` o `C:\Windows\System32\mspaint.exe`
  - `{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe`
- **Diseño de inicio:** Solo está disponible la pantalla de inicio predeterminada para las aplicaciones.
- **XML predeterminado:** Solo está disponible el script XML predeterminado.
- **Seleccionar tipo de usuario:** Especifique el tipo de usuario que recibirá la directiva de quiosco. Sus opciones:

  - **Local:** Citrix Endpoint Management crea un usuario para el dispositivo de destino o agrega un usuario existente.
  - **Azure AD:** Citrix Endpoint Management agrega usuarios inscritos en Azure AD.

- **Nombre de usuario:** Introduzca el nombre de usuario que recibirá la directiva de quiosco.
  - Para crear un nombre de usuario local en el dispositivo de destino, introduzca el nombre. Asegúrese de que su nombre de usuario local no tenga el dominio. Si introduce un nombre existente, Citrix Endpoint Management no crea un usuario ni cambia la contraseña actual.
  - Para agregar un usuario de Azure AD, introduzca el nombre en el formato `azuread\user`. La parte `user` puede ser el **Nombre** introducido al crear un usuario en Azure AD, o el **Nombre de usuario** introducido al crear un usuario en Azure AD. El usuario asignado no puede ser un administrador de Azure AD.
- **Contraseña:** No hay configuración de contraseña para los usuarios de Azure AD. Escriba la contraseña solo para el nombre de usuario local.
- **Mostrar barra de tareas:** Habilite la barra de tareas para proporcionar a los usuarios una forma sencilla de ver y administrar aplicaciones. El valor predeterminado es **Desactivado**.
- Haga clic en **Siguiente** y guarde los cambios.

Para una aplicación UWP que desee permitir en modo Quiosco, debe proporcionar el AUMID. Para obtener una lista de los AUMID de todas las aplicaciones de Microsoft Store instaladas para el usuario actual del dispositivo, ejecute el siguiente comando de PowerShell:

```
$installedapps = get-AppxPackage



$aumidList = @()

foreach ($app in $installedapps)

{

    foreach ($id in (Get-AppxPackageManifest
$app).package.applications.application.id)

    {

        $aumidList += $app.packagefamilyname + "!"+ $id
```

```
    }
}

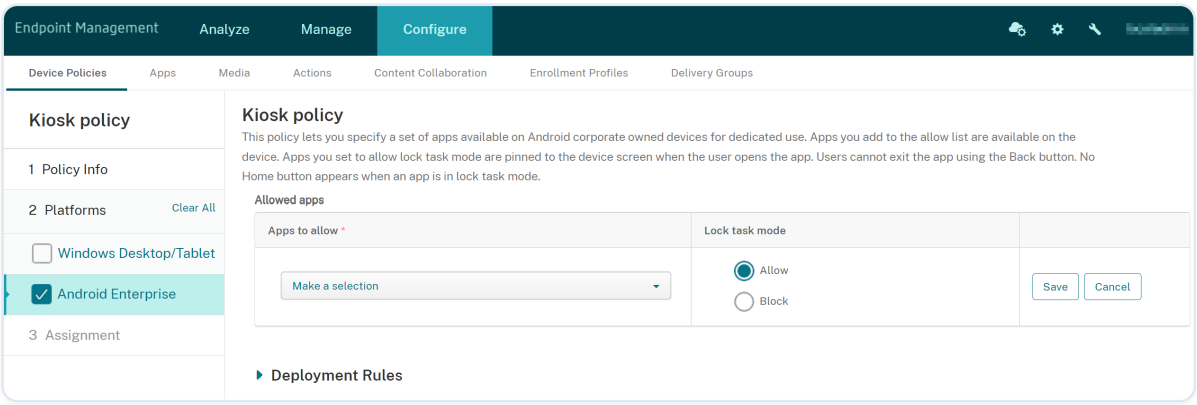

$aumidList
```

Configuración de Android Enterprise

Puede permitir aplicaciones y establecer el modo de bloqueo de tareas para dispositivos Android Enterprise dedicados, también conocidos como dispositivos de un solo uso propiedad de la empresa (COSU).

Para permitir una aplicación, haga clic en **Agregar**. Puede agregar varias aplicaciones a la lista de permitidas. Para obtener más información, consulte Android Enterprise.

- **Aplicaciones permitidas:** Introduzca el nombre del paquete de la aplicación que quiere permitir o seleccione la aplicación de la lista.
    - Haga clic en **Agregar nuevo** para introducir el nombre del paquete de la aplicación permitida en la lista.
    - Seleccione la aplicación existente de la lista. La lista muestra las aplicaciones que se han cargado en Citrix Endpoint Management. De forma predeterminada, Citrix Secure Hub y Google Play services están en la lista de permitidos.



- **Modo de bloqueo de tareas:** Elija **Permitir** para fijar la aplicación a la pantalla del dispositivo cuando el usuario la inicie. Elija **Bloquear** para que la aplicación no se fije. El valor predeterminado es **Permitir**.

Cuando una aplicación está en modo de bloqueo de tareas, la aplicación se fija a la pantalla del dispositivo cuando el usuario la abre. No aparece ningún botón de Inicio y el botón de **Atrás** está

deshabilitado. El usuario sale de la aplicación mediante una acción programada en la aplicación, como cerrar sesión.

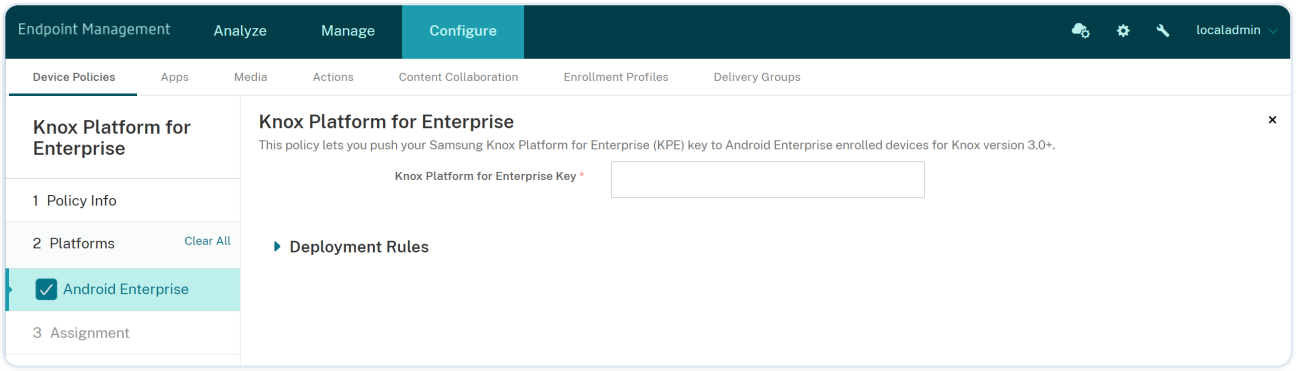
Política de clave de Knox Platform for Enterprise

Esta política le permite proporcionar la información de licencia necesaria de Samsung Knox Platform for Enterprise (KPE).

Para agregar o configurar esta política, vaya a **Configurar** > **Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de Android Enterprise

Esta política proporciona la información de licencia necesaria de Samsung Knox Platform for Enterprise (KPE). Para Android 12 o anterior, debe solicitar una licencia premium de KPE para usar las funciones premium de Knox. Para Android 13 o posterior, la licencia premium de KPE se proporciona de forma predeterminada.



Clave de Knox Platform for Enterprise: Introduzca la clave de Samsung Knox Platform for Enterprise (KPE) que desea enviar al dispositivo Android Enterprise. Solicite una clave de licencia de KPE en Clave de Samsung Knox Platform for Enterprise (KPE).

Política de dispositivo de configuración de Launcher

Citrix Launcher le permite personalizar la experiencia del usuario para dispositivos Android Enterprise y dispositivos Android heredados implementados por Citrix Endpoint Management.

Utilice una política de configuración de Launcher para controlar estas funciones de Citrix Launcher:

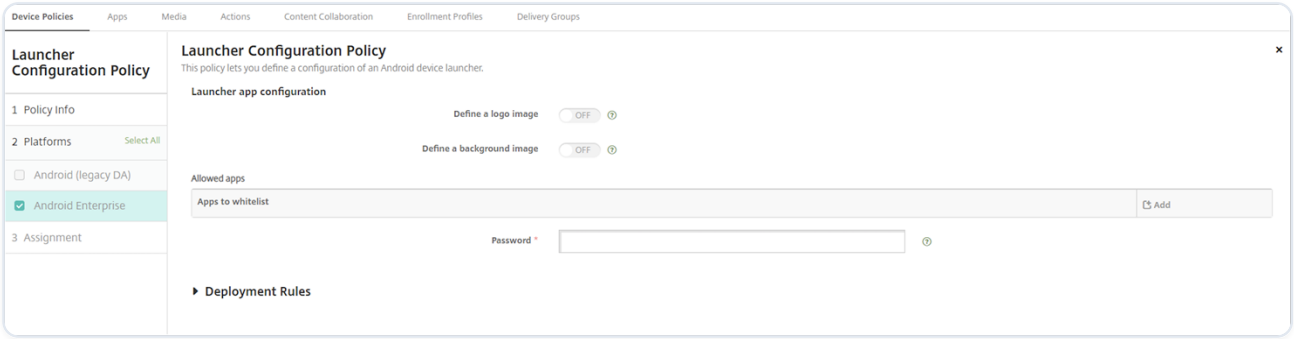
- Administre dispositivos Android Enterprise y dispositivos Android heredados para que los usuarios solo puedan acceder a las aplicaciones que usted especifique.

- Opcionalmente, especifique una imagen de logotipo personalizada para el icono de Citrix Launcher y una imagen de fondo personalizada para Citrix Launcher.
- Especifique una contraseña que los usuarios deben escribir para salir del iniciador.

Citrix Launcher no está diseñado para ser una capa de seguridad adicional sobre lo que ya proporciona la plataforma del dispositivo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de Android Enterprise y Android



- **Definir una imagen de logotipo:** Seleccione si desea usar una imagen de logotipo personalizada para el icono de Citrix Launcher. El valor predeterminado es **Desactivado**.
- **Imagen de logotipo:** Cuando habilite **Definir una imagen de logotipo**, seleccione el archivo de imagen haciendo clic en **Examinar** y navegando a la ubicación del archivo. Los tipos de archivo admitidos son PNG, JPG, JPEG y GIF.
- **Definir una imagen de fondo:** Seleccione si desea usar una imagen personalizada para el fondo de Citrix Launcher. El valor predeterminado es **Desactivado**.
- **Imagen de fondo:** Cuando habilite **Definir una imagen de fondo**, seleccione el archivo de imagen haciendo clic en **Examinar** y navegando a la ubicación del archivo. Los tipos de archivo admitidos son PNG, JPG, JPEG y GIF.
- **Aplicaciones permitidas:** Para cada aplicación que desee permitir en Citrix Launcher, haga clic en **Agregar** y, a continuación, haga lo siguiente:
  - **Nueva aplicación para añadir:** Introduzca el nombre completo de la aplicación que desea añadir. Por ejemplo, com.android.calendar para la aplicación de calendario de Android.
  - Haga clic en **Guardar** para añadir la aplicación o haga clic en **Cancelar** para cancelar la adición de la aplicación.
- **Contraseña:** La contraseña que un usuario debe introducir para salir de Citrix Launcher.

Directiva de dispositivo LDAP

Cree una directiva LDAP para dispositivos iOS en Citrix Endpoint Management para proporcionar información sobre un servidor LDAP que se va a utilizar, incluida la información de cuenta necesaria. La directiva también proporciona un conjunto de directivas de búsqueda LDAP para usar al consultar el servidor LDAP.

Necesita el nombre de host LDAP antes de configurar esta directiva.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

- **Descripción de la cuenta:** Introduzca una descripción opcional de la cuenta.
- **Nombre de usuario de la cuenta:** Introduzca un nombre de usuario opcional.
- **Contraseña de la cuenta:** Introduzca una contraseña opcional. Utilice este campo solo con perfiles cifrados.
- **Nombre de host LDAP:** Introduzca el nombre de host del servidor LDAP. Este campo es obligatorio.
- **Usar SSL:** Seleccione si desea utilizar una conexión Secure Socket Layer al servidor LDAP. El valor predeterminado es **Activado**.
- **Configuración de búsqueda:** Agregue la configuración de búsqueda que se utilizará al consultar el servidor LDAP. Puede introducir tantas configuraciones de búsqueda como desee, pero debe agregar al menos una configuración de búsqueda para que la cuenta sea útil. Haga clic en **Agregar** y, a continuación, haga lo siguiente:
    - **Descripción:** Introduzca una descripción de la configuración de búsqueda. Este campo es obligatorio.
    - **Ámbito:** Elija **Base**, **Un nivel** o **Subárbol** para definir la profundidad de la búsqueda en el árbol LDAP. El valor predeterminado es **Base**.
        - **Base** busca el nodo al que apunta la base de búsqueda.
        - **Un nivel** busca el nodo Base y un nivel por debajo de él.
        - **Subárbol** busca en el nodo base, más todos sus hijos, independientemente de la profundidad.
    - **Base de búsqueda:** Introduzca la ruta al nodo donde desea iniciar la búsqueda. Por ejemplo, ou=people o 0=example corp. Este campo es obligatorio.

    - Haga clic en **Guardar** para agregar la configuración de búsqueda o haga clic en **Cancelar** para cancelar la adición de la configuración de búsqueda.
    - Repita estos pasos para cada configuración de búsqueda que desee agregar.

- **Configuración de directiva**
    - **Quitar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
        - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
        - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.

Configuración de macOS

- **Descripción de la cuenta:** Introduzca una descripción opcional de la cuenta.
- **Nombre de usuario de la cuenta:** Introduzca un nombre de usuario opcional.
- **Contraseña de la cuenta:** Introduzca una contraseña opcional. Utilice este campo solo con perfiles cifrados.
- **Nombre de host LDAP:** Introduzca el nombre de host del servidor LDAP. Este campo es obligatorio.
- **Usar SSL:** Seleccione si desea usar una conexión Secure Socket Layer al servidor LDAP. El valor predeterminado es **Activado**.
- **Configuración de búsqueda:** Agregue la configuración de búsqueda que se utilizará al consultar el servidor LDAP. Puede introducir tantas configuraciones de búsqueda como desee, pero debe agregar al menos una configuración de búsqueda para que la cuenta sea útil. Haga clic en **Agregar** y, a continuación, haga lo siguiente:
    - **Descripción:** Introduzca una descripción de la configuración de búsqueda. Este campo es obligatorio.
    - **Ámbito:** Elija **Base**, **Un nivel** o **Subárbol** para definir la profundidad de la búsqueda en el árbol LDAP. El valor predeterminado es **Base**.
        - **Base** busca el nodo al que apunta la base de búsqueda.
        - **Un nivel** busca el nodo Base y un nivel por debajo de él.
        - **Subárbol** busca el nodo Base, más todos sus elementos secundarios, independientemente de la profundidad.

- **Base de búsqueda:** Introduzca la ruta al nodo donde desea iniciar la búsqueda. Por ejemplo, ou=people o 0=example corp. Este campo es obligatorio.
- Haga clic en **Guardar** para agregar la configuración de búsqueda o haga clic en **Cancelar** para anular la adición de la configuración de búsqueda.
- Repita estos pasos para cada configuración de búsqueda que desee agregar.

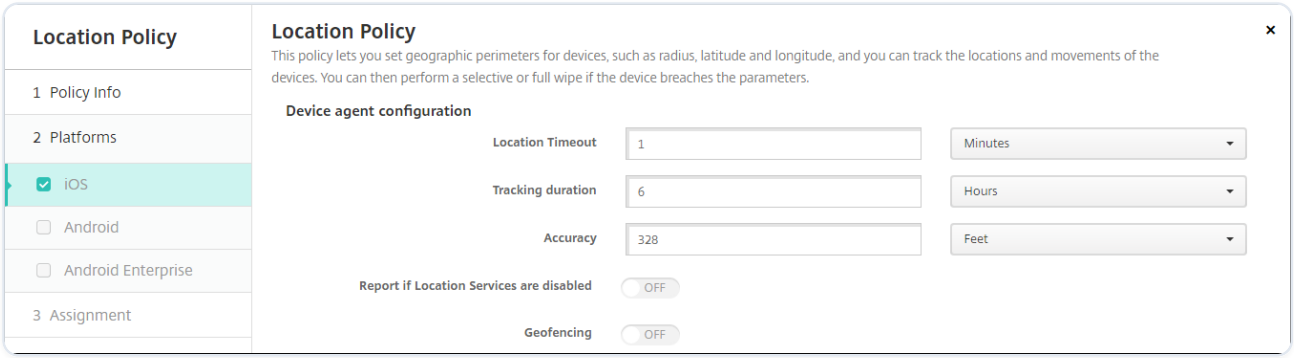
- **Configuración de directivas**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.
  - **Permitir al usuario eliminar la directiva:** Puede seleccionar cuándo los usuarios pueden eliminar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en macOS 10.7 y versiones posteriores.

Política de dispositivo de ubicación

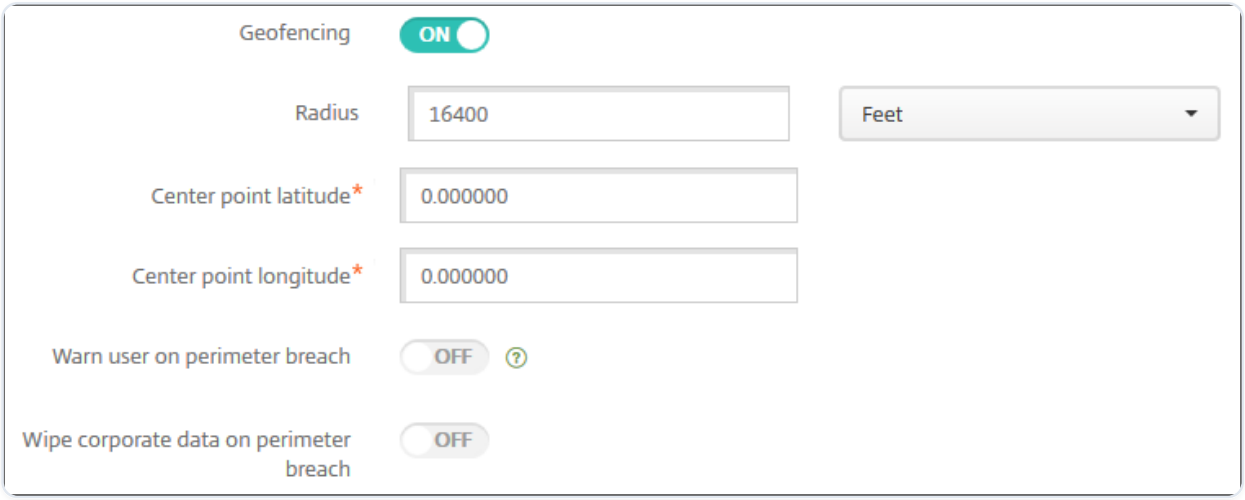
Usted crea políticas de dispositivo de ubicación en Citrix Endpoint Management para aplicar límites geográficos. Cuando los usuarios traspasan el límite definido, también llamado *geocerca*, Citrix Endpoint Management puede realizar ciertas acciones. Por ejemplo, puede configurar la política para emitir un mensaje de advertencia a los usuarios cuando traspasan el perímetro definido. También puede configurar la política para borrar los datos corporativos de los usuarios cuando traspasan un perímetro, de inmediato o después de un retraso. Para obtener información sobre las acciones de seguridad, como habilitar el seguimiento y localizar un dispositivo, consulte Acciones de seguridad.

Para agregar o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS



- **Tiempo de espera de ubicación:** Escriba un número y, a continuación, haga clic en **Segundos** o **Minutos** para establecer la frecuencia con la que Citrix Endpoint Management intenta fijar la ubicación del dispositivo. Los valores válidos son de 60 a 900 segundos o de 1 a 15 minutos. El valor predeterminado es **1 minuto**.
- **Duración del seguimiento:** Escriba un número y, a continuación, haga clic en **Horas** o **Minutos** para establecer el tiempo durante el cual Citrix Endpoint Management rastrea el dispositivo. Los valores válidos son de 1 a 10 horas o de 10 a 600 minutos. El valor predeterminado es **6 horas**.
- **Precisión:** Escriba un número y, a continuación, haga clic en **Metros**, **Pies** o **Yardas** para establecer la proximidad con la que Citrix Endpoint Management rastrea el dispositivo. Los valores válidos son de 10 a 5000 yardas, de 30 a 15000 pies o de 10 a 5000 metros. El valor predeterminado es **328 pies** (**100 metros**).
- **Informar si los servicios de ubicación están deshabilitados:** Seleccione si el dispositivo envía un informe a Citrix Endpoint Management cuando el usuario desactiva el GPS. El valor predeterminado es **Desactivado**.
- **Geocercado**

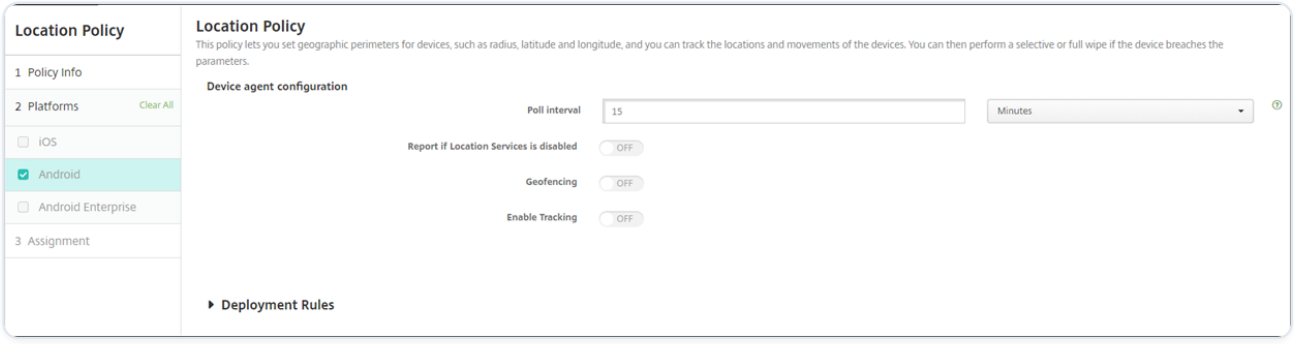


Cuando habilite Geocercado, configure estos ajustes:

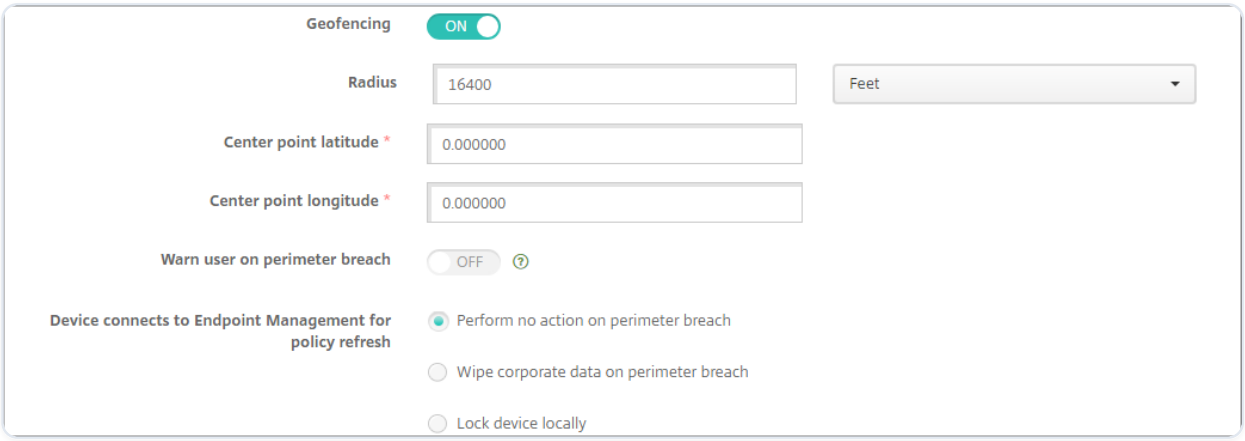
- **Radio:** Escriba un número y, a continuación, haga clic en las unidades que se utilizarán para medir el radio. El valor predeterminado es **16400 pies** (**5000 metros**). Los valores válidos para el radio son:
  - 164–16400 pies
  - 50–50000 metros
  - 54–54680 yardas
  - 1–31 millas
- **Latitud del punto central:** Escriba una latitud, como 37.787454, para definir la latitud del punto central de la geocerca.
- **Longitud del punto central:** Escriba una longitud, como 122.402952, para definir la longitud del punto central de la geocerca.
- **Advertir al usuario si se infringe el perímetro:** Seleccione si desea emitir un mensaje de advertencia cuando los usuarios infrinjan el perímetro definido. El valor predeterminado es **Desactivado**. No se requiere conexión a Citrix Endpoint Management para mostrar el mensaje de advertencia.
- **Borrar datos corporativos si se infringe el perímetro:** Seleccione si desea borrar los dispositivos de los usuarios cuando infrinjan el perímetro. El valor predeterminado es **Desactivado**. Cuando habilita esta opción, aparece el campo **Retraso en el borrado local**.
  - Escriba un número y, a continuación, haga clic en **Segundos** o **Minutos** para establecer el tiempo de retraso antes de borrar los datos corporativos de los dispositivos de los usuarios. El retraso da a los usuarios la oportunidad de volver a la ubicación permitida antes de que Citrix Endpoint Management borre selectivamente sus dispositivos. El valor predeterminado es **0 segundos**.

Configuración de Android (DA heredado)

El seguimiento de ubicación de Android requiere Android 9 o posterior.



- **Intervalo de sondeo:** Escriba un número y, a continuación, haga clic en **Minutos**, **Horas** o **Días** para establecer la frecuencia con la que Citrix Endpoint Management intenta determinar la ubicación del dispositivo. Los valores válidos son 15–1440 minutos, 1–24 horas o cualquier número de días. El valor predeterminado es **15 minutos**.
- **Informar si los servicios de ubicación están inhabilitados:** Seleccione si el dispositivo envía un informe a Citrix Endpoint Management cuando el usuario desactiva el GPS. El valor predeterminado es **Desactivado**.
- **Geocercas**



Cuando habilite las geocercas, configure estos ajustes:

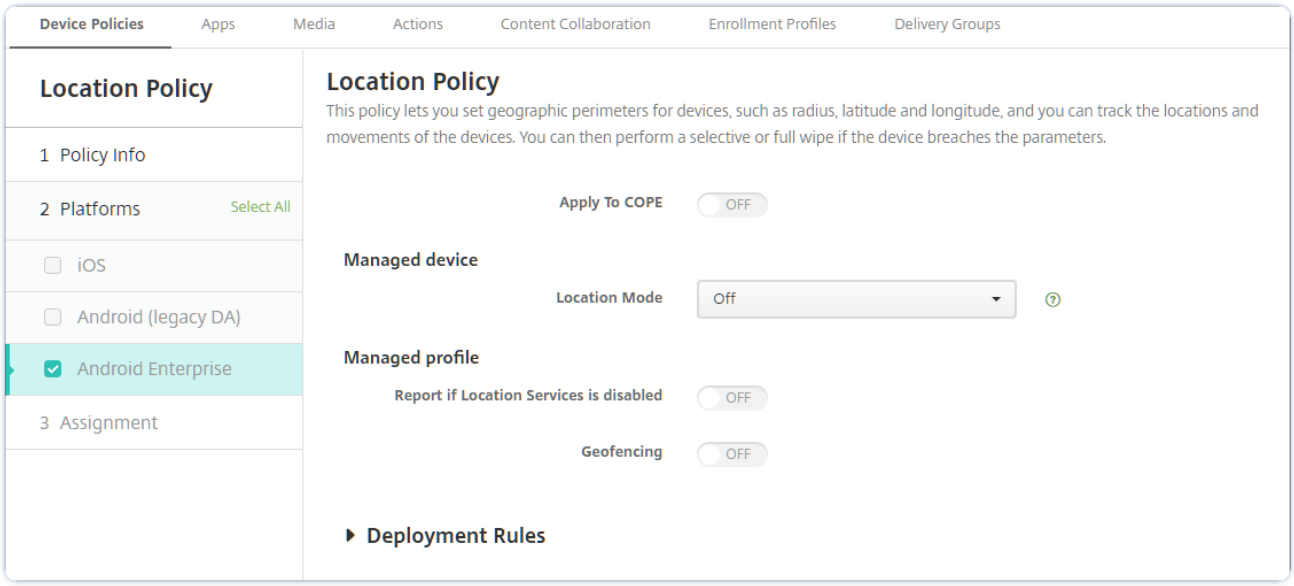
- **Radio:** Escriba un número y, a continuación, haga clic en las unidades que se utilizarán para medir el radio. El valor predeterminado es **16400 pies** (**5000 metros**). Los valores válidos para el radio son:
  - 164–164000 pies
  - 1–50 kilómetros
  - 50–50000 metros
  - 54–54680 yardas
  - 1–31 millas
- **Latitud del punto central:** Escriba una latitud, como 37.787454, para definir la latitud del punto central de la geocerca.
- **Longitud del punto central:** Escriba una longitud, como 122.402952, para definir la longitud del punto central de la geocerca.
- **Advertir al usuario si se infringe el perímetro:** Seleccione si desea emitir un mensaje de advertencia cuando los usuarios infrinjan el perímetro definido. El valor predeterminado es **Desactivado**. No se requiere conexión a Citrix Endpoint Management para mostrar el mensaje de advertencia.

- **El dispositivo se conecta a Citrix Endpoint Management para actualizar la directiva:** Seleccione una de las siguientes opciones para cuando los usuarios infrinjan el perímetro:
  - **No realizar ninguna acción si se infringe el perímetro:** No hacer nada. Esta es la opción predeterminada.
  - **Borrar datos corporativos si se infringe el perímetro:** Borrar datos corporativos después de un período de tiempo especificado. Al habilitar esta opción, aparece el campo **Retraso en el borrado local**.
    - Escriba un número y, a continuación, haga clic en **Segundos** o **Minutos** para establecer el tiempo de retraso antes de borrar los datos corporativos de los dispositivos de los usuarios. El retraso da a los usuarios la oportunidad de volver a la ubicación permitida antes de que Citrix Endpoint Management borre selectivamente sus dispositivos. El valor predeterminado es **0 segundos**.
  - **Bloquear dispositivo localmente:** Bloquear los dispositivos de los usuarios después de un período de tiempo especificado. Al habilitar esta opción, aparece el campo **Retraso en el bloqueo**.
    - Escriba un número y, a continuación, haga clic en **Segundos** o **Minutos** para establecer el tiempo de retraso antes de bloquear los dispositivos de los usuarios. El retraso da a los usuarios la oportunidad de volver a la ubicación permitida antes de que Citrix Endpoint Management bloquee sus dispositivos. El valor predeterminado es **0 segundos**.
- **Habilitar seguimiento:** Seleccione si el dispositivo rastrea la ubicación del usuario. El valor predeterminado es **Desactivado**.

Configuración de Android Enterprise

Para que el seguimiento de ubicación de Android funcione, asegúrese de que se cumplan los siguientes requisitos:

- Android 9 o posterior
- La configuración Permitir compartir ubicación habilitada en la directiva de dispositivo Restricciones para Android Enterprise
- Programación de conexión (se recomienda Firebase Cloud Messaging)



Aplicar a dispositivos totalmente administrados con un perfil de trabajo

Para dispositivos totalmente administrados con perfiles de trabajo (anteriormente conocidos como dispositivos COPE), solo está disponible la configuración del modo de ubicación.

- **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos corporativos:** Permite configurar el modo de ubicación para dispositivos totalmente administrados con perfiles de trabajo. Cuando esta configuración está activada, configure los ajustes para el perfil de trabajo:
  - **Informar si los servicios de ubicación están deshabilitados:** Seleccione si el dispositivo envía un informe a Citrix Endpoint Management cuando el usuario desactiva el GPS. El valor predeterminado es **Desactivado**.
  - **Geocercas:** Consulte la configuración de este artículo en Dispositivo administrado.

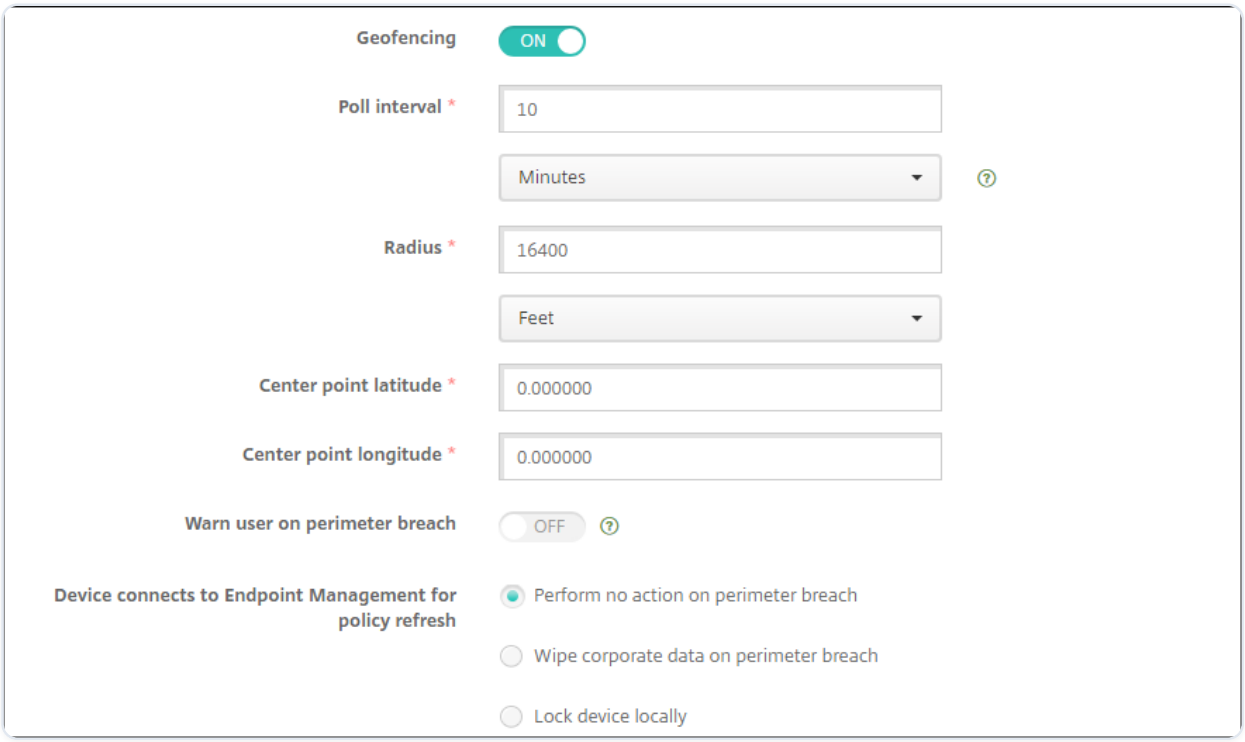
Cuando **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos corporativos** está desactivado, la configuración se aplica al dispositivo administrado y al perfil de trabajo como se muestra en las siguientes secciones. El valor predeterminado es **Desactivado**.

Dispositivo administrado

- **Modo de ubicación:** Especifique el grado de detección de ubicación que desea habilitar. Puede usar la acción de seguridad Localizar solo cuando el modo de ubicación esté configurado en **Alta precisión** o **Ahorro de batería**. El valor predeterminado es **Alta precisión**.

- **Alta precisión:** Habilita todos los métodos de detección de ubicación, incluidos GPS, redes y otros sensores.
- **Solo sensores:** Habilita solo el GPS y otros sensores.
- **Ahorro de batería:** Habilita solo el proveedor de ubicación de red.
- **Desactivado:** Deshabilita la detección de ubicación.

- **Geocercado:**



Cuando habilite **Geocercado**, configure estos ajustes:

- **Intervalo de sondeo:** Escriba un número y, a continuación, haga clic en **Minutos**, **Horas** o **Días** para establecer la frecuencia con la que Citrix Endpoint Management intenta fijar la ubicación del dispositivo. Los valores válidos son 1–1440 minutos, 1–24 horas o cualquier número de días. El valor predeterminado es **10 minutos**. Establecer este valor en menos de 10 minutos podría afectar negativamente la duración de la batería del dispositivo.
- **Radio:** Escriba un número y, a continuación, haga clic en las unidades que se utilizarán para medir el radio. El valor predeterminado es **16400 pies** (**5000 metros**). Los valores válidos para el radio son:
  - 164–164000 pies
  - 1–50 kilómetros
  - 50–50000 metros
  - 54–54680 yardas

    - 1–31 millas

- **Latitud del punto central:** Escriba una latitud, como 37.787454, para definir la latitud del punto central del geocercado. Para buscar el valor, vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Proteger** y, a continuación, haga clic en **Localizar**. Después de localizar el dispositivo, Citrix Endpoint Management informa de la ubicación del dispositivo en la página **Detalles del dispositivo > General**, en **Seguridad**.
- **Longitud del punto central:** Escriba una longitud, como 122.402952, para definir la longitud del punto central de la geocerca.
- **Advertir al usuario si se infringe el perímetro:** Seleccione si desea emitir un mensaje de advertencia cuando los usuarios infrinjan el perímetro definido. El valor predeterminado es **Desactivado**. No se requiere conexión a Citrix Endpoint Management para mostrar el mensaje de advertencia.
- **El dispositivo se conecta a Citrix Endpoint Management para actualizar la directiva:** Seleccione una de las siguientes opciones para cuando los usuarios infrinjan el perímetro:

    - **No realizar ninguna acción si se infringe el perímetro:** No hacer nada. Esta configuración es la predeterminada.
    - **Borrar datos corporativos si se infringe el perímetro:** Borre los datos corporativos después de un período de tiempo especificado. Cuando habilita esta opción, aparece el campo **Retraso en el borrado local**.

        - Escriba un número y, a continuación, haga clic en **Segundos** o **Minutos** para establecer el tiempo de retraso antes de borrar los datos corporativos de los dispositivos de los usuarios. El retraso da a los usuarios la oportunidad de volver a la ubicación permitida antes de que Citrix Endpoint Management borre selectivamente sus dispositivos. El valor predeterminado es **0 segundos**.

    - **Bloquear el dispositivo localmente:** Bloquee los dispositivos de los usuarios después de un período de tiempo especificado. Cuando habilita esta opción, aparece el campo **Retraso en el bloqueo**.

        - Escriba un número y, a continuación, haga clic en **Segundos** o **Minutos** para establecer el tiempo de retraso antes de bloquear los dispositivos de los usuarios. El retraso da a los usuarios la oportunidad de volver a la ubicación permitida antes de que Citrix Endpoint Management bloquee sus dispositivos. El valor predeterminado es **0 segundos**.

Perfil de trabajo

- **Informar si los servicios de ubicación están deshabilitados:** Seleccione si el dispositivo envía un informe a Citrix Endpoint Management cuando el usuario desactiva el GPS. El valor predeterminado es **Desactivado**.
- **Geocercado:** Consulte la configuración de este artículo en Dispositivo administrado.

Directiva de dispositivo de mensaje de pantalla de bloqueo

La directiva **Mensaje de pantalla de bloqueo** le permite configurar mensajes para que aparezcan en los siguientes dispositivos iOS cuando se pierden:

- La ventana de inicio de sesión de los iPads compartidos
- La pantalla de bloqueo de los dispositivos iOS supervisados

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

- **Información de etiqueta de recurso para el dispositivo:** La etiqueta de recurso para el dispositivo. Los dispositivos Apple truncan las cadenas largas, así que asegúrese de probar una cadena antes de implementar la directiva en producción. La longitud de la cadena depende del modelo de dispositivo Apple y de la configuración de Apple, que pueden cambiar.
- **Nota al pie de la ventana de inicio de sesión y la pantalla de bloqueo:** Información para ayudar a devolver el dispositivo, como una dirección u otra información de contacto. Por ejemplo, su mensaje podría tener el formato "Si se pierde, devolver a". Los dispositivos Apple truncan las cadenas largas, así que asegúrese de probar una cadena antes de implementar la directiva en producción. La longitud de la cadena depende del modelo de dispositivo Apple y de la configuración de Apple, que pueden cambiar.
- **Configuración de la directiva**
    - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
        - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.

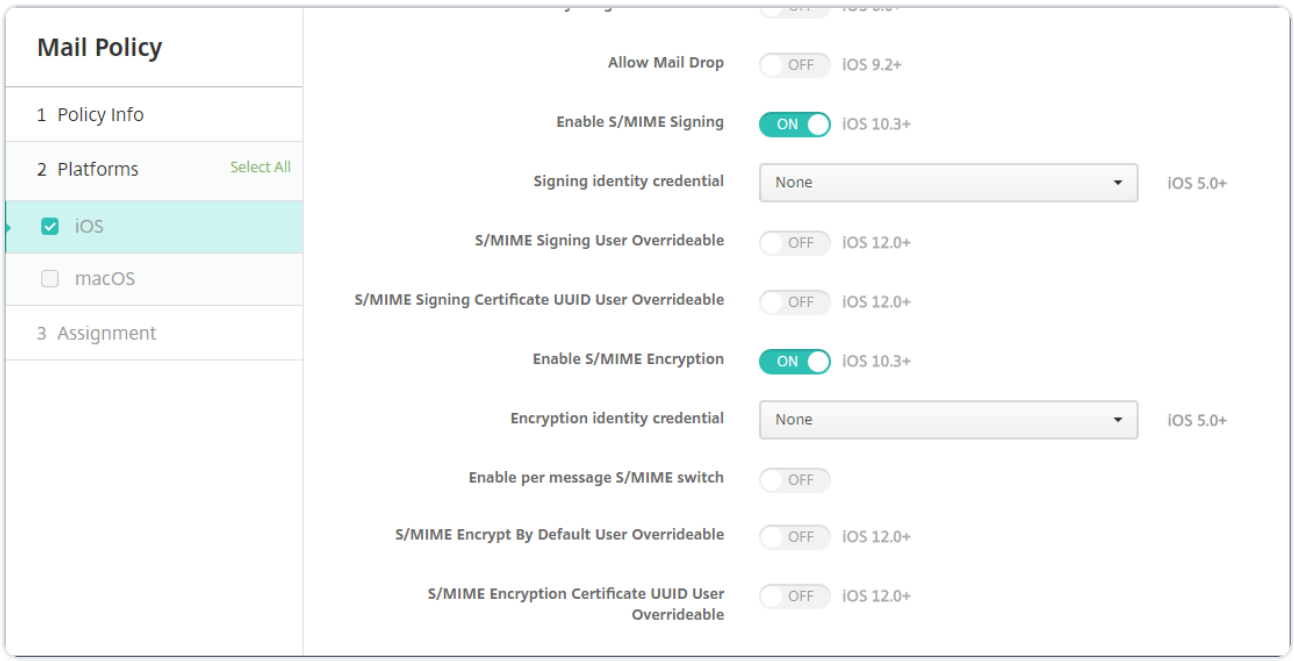
- **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva. Solo disponible para iOS 6.0 y versiones posteriores.

Directiva de dispositivo de correo

Puede agregar una directiva de dispositivo de correo en Citrix Endpoint Management para configurar una cuenta de correo electrónico en dispositivos iOS o macOS.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS y macOS



- **Descripción de la cuenta:** Escriba una descripción de la cuenta que aparecerá en las aplicaciones Mail y Ajustes. Este campo es obligatorio.
- **Tipo de cuenta:** Elija **IMAP** o **POP** para seleccionar el protocolo que se utilizará para las cuentas de usuario. El valor predeterminado es **IMAP**. Cuando selecciona **POP**, la siguiente opción de prefijo de **Ruta** desaparece.
- **Prefijo de ruta:** Escriba **INBOX** o el prefijo de ruta de su cuenta de correo IMAP. Este campo es obligatorio.
- **Nombre para mostrar del usuario:** Escriba el nombre de usuario completo que se utilizará para los mensajes y otros fines. Este campo es obligatorio.
- **Dirección de correo electrónico:** Escriba la dirección de correo electrónico completa de la cuenta. Este campo es obligatorio.

- **Configuración de correo electrónico entrante**
  - **Nombre de host del servidor de correo electrónico:** Escriba el nombre de host o la dirección IP del servidor de correo entrante. Este campo es obligatorio.
  - **Puerto del servidor de correo electrónico:** Escriba el número de puerto del servidor de correo entrante. El valor predeterminado es **143**. Este campo es obligatorio.
  - **Nombre de usuario:** Escriba el nombre de usuario de la cuenta de correo electrónico. Este nombre suele ser el mismo que la dirección de correo electrónico hasta el carácter @. Este campo es obligatorio.
  - **Tipo de autenticación:** Elija el tipo de autenticación que se utilizará. El valor predeterminado es **Contraseña**. Cuando se selecciona **Ninguno**, el siguiente campo **Contraseña** desaparece.
  - **Contraseña:** Escriba una contraseña opcional para el servidor de correo entrante.
  - **Usar SSL:** Seleccione si el servidor de correo entrante utiliza autenticación Secure Socket Layer. El valor predeterminado es **Desactivado**.
- **Configuración de correo electrónico saliente**
  - **Nombre de host del servidor de correo electrónico:** Escriba el nombre de host o la dirección IP del servidor de correo saliente. Este campo es obligatorio.
  - **Puerto del servidor de correo electrónico:** Escriba el número de puerto del servidor de correo saliente. Si no introduce un número de puerto, se utiliza el puerto predeterminado para el protocolo dado.
  - **Nombre de usuario:** Escriba el nombre de usuario de la cuenta de correo electrónico. Este nombre suele ser el mismo que la dirección de correo electrónico hasta el carácter @. Este campo es obligatorio.
  - **Tipo de autenticación:** Elija el tipo de autenticación que desea utilizar. El valor predeterminado es **Contraseña**.
  - **Contraseña:** Escriba una contraseña opcional para el servidor de correo saliente.
  - **Contraseña de salida igual que la de entrada:** Seleccione si las contraseñas de entrada y salida son las mismas. El valor predeterminado es **Desactivado**, lo que significa que las contraseñas son diferentes.
  - **Usar SSL:** Seleccione si el servidor de correo saliente utiliza autenticación Secure Socket Layer. El valor predeterminado es **Desactivado**.
- **Directiva**

- **Autorizar el movimiento de correo electrónico entre cuentas:** Seleccione si desea permitir a los usuarios:
  - mover correo electrónico de esta cuenta a otra cuenta
  - reenviar correo electrónico desde una cuenta diferente
  - responder desde una cuenta diferente.

  El valor predeterminado es **Desactivado**.
- **Enviar correo electrónico solo desde la aplicación de correo:** Seleccione si desea restringir a los usuarios a la aplicación de correo de iOS para enviar correos electrónicos.
- **Deshabilitar la sincronización de correos recientes:** Seleccione si desea evitar que los usuarios sincronicen direcciones recientes. El valor predeterminado es **Desactivado**. Esta opción solo se aplica a iOS 6.0 y versiones posteriores.
- **Permitir Mail Drop:** Seleccione si desea permitir el uso de Apple Mail Drop para dispositivos con iOS 9.2 y versiones posteriores. El valor predeterminado es **Desactivado**.
- **Habilitar la firma S/MIME:** Seleccione si esta cuenta admite la firma S/MIME. El valor predeterminado es **Activado**. Cuando se establece en **Activado**, aparecen los siguientes campos.
  - **Credencial de identidad de firma:** Elija la credencial de firma que desea utilizar.
  - **Firma S/MIME anulable por el usuario:** Si se establece en **Activado**, los usuarios pueden activar y desactivar la firma S/MIME en la configuración de sus dispositivos. El valor predeterminado es **Desactivado**. Esta opción se aplica a iOS 12.0 y versiones posteriores.
  - **UUID del certificado de firma S/MIME anulable por el usuario:** Si se establece en **Activado**, los usuarios pueden seleccionar, en la configuración de sus dispositivos, la credencial de firma que desean utilizar. El valor predeterminado es **Desactivado**. Esta opción se aplica a iOS 12.0 y versiones posteriores.
- **Habilitar el cifrado S/MIME:** Seleccione si esta cuenta admite el cifrado S/MIME. El valor predeterminado es **Desactivado**. Cuando se establece en **Activado**, aparecen los siguientes campos.
  - **Credencial de identidad de cifrado:** Elija la credencial de cifrado que desea utilizar.
  - **Habilitar el interruptor S/MIME por mensaje:** Cuando se establece en **Activado**, muestra a los usuarios una opción para activar o desactivar el cifrado S/MIME para cada mensaje que redacten. El valor predeterminado es **Desactivado**.

  - **Cifrado S/MIME predeterminado anulable por el usuario:** Si se establece en **Activado**, los usuarios pueden, en la configuración de sus dispositivos, seleccionar si S/MIME está activado de forma predeterminada. El valor predeterminado es **Desactivado**. Esta opción se aplica a iOS 12.0 y versiones posteriores.
  - **UUID del certificado de cifrado S/MIME anulable por el usuario:** Si se establece en **Activado**, los usuarios pueden activar y desactivar la identidad de cifrado S/MIME y el cifrado en la configuración de sus dispositivos. El valor predeterminado es **Desactivado**. Esta opción se aplica a iOS 12.0 y versiones posteriores.

- **Configuración de la directiva**
  - **Eliminar directiva:** Para eliminar la directiva más tarde, configure este ajuste para eliminar la directiva en una **Fecha seleccionada** o para una **Duración hasta la eliminación (en horas)**.
  - **Permitir al usuario eliminar la directiva:** Permitir a los usuarios eliminar la directiva de correo **Siempre**, solo con una **Contraseña requerida**, o **Nunca**. Solo disponible para macOS.
  - **Ámbito del perfil:** Solo para macOS, elija si la directiva se aplica a nivel de **Usuario** o en todo el **Sistema**.

Directiva de configuraciones administradas

La directiva de dispositivo de configuraciones administradas controla varias opciones de configuración de aplicaciones y restricciones de aplicaciones. Cree esta directiva para cada aplicación de Android Enterprise que desee controlar.

El desarrollador de la aplicación define las opciones y la información sobre herramientas disponibles para una aplicación. Si la información sobre herramientas menciona el uso de un "valor de plantilla", utilice la macro de Citrix Endpoint Management correspondiente en su lugar. Para obtener más información, consulte Información general sobre la configuración remota (en el sitio para desarrolladores de Android) y Macros.

La configuración de la aplicación puede incluir elementos como:

- Ajustes de correo
- Permitir o bloquear URL para un explorador web
- Opción para controlar la sincronización del contenido de la aplicación a través de una conexión de datos móviles o solo mediante una conexión Wi-Fi

Para obtener información sobre la configuración que aparece para sus aplicaciones, póngase en contacto con el desarrollador de la aplicación.

> **Nota:**
>
> Citrix SSO para Android ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación para reflejar este cambio de nombre.

Requisitos previos

- Complete las tareas de configuración de Android Enterprise en Google y conecte Android Enterprise a Google Play administrado. Para obtener más información, consulte Android Enterprise.
- Agregue aplicaciones de Android Enterprise a Citrix Endpoint Management. Para obtener más información, consulte Agregar aplicaciones a Citrix Endpoint Management.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos para VPN por aplicación

Para crear una VPN por aplicación para AE, debe realizar pasos adicionales además de configurar la política de dispositivo de configuraciones administradas. Además, debe verificar que se cumplen los siguientes requisitos previos:

- NetScaler Gateway local
- Las siguientes aplicaciones están instaladas en el dispositivo:
  - Citrix SSO
  - Citrix Secure Hub

Un flujo de trabajo general para configurar una VPN por aplicación para dispositivos AE es el siguiente:

1. Configure un perfil VPN como se describe en este artículo.
2. Configure Citrix ADC para aceptar tráfico de la VPN por aplicación. Para obtener más información, consulte Configuración completa de VPN en NetScaler Gateway.

Limitaciones

Las siguientes son las limitaciones para la VPN por aplicación en el entorno de Android Enterprise en dispositivos Android 11+ debido a las restricciones de visibilidad de paquetes introducidas en Android 11:

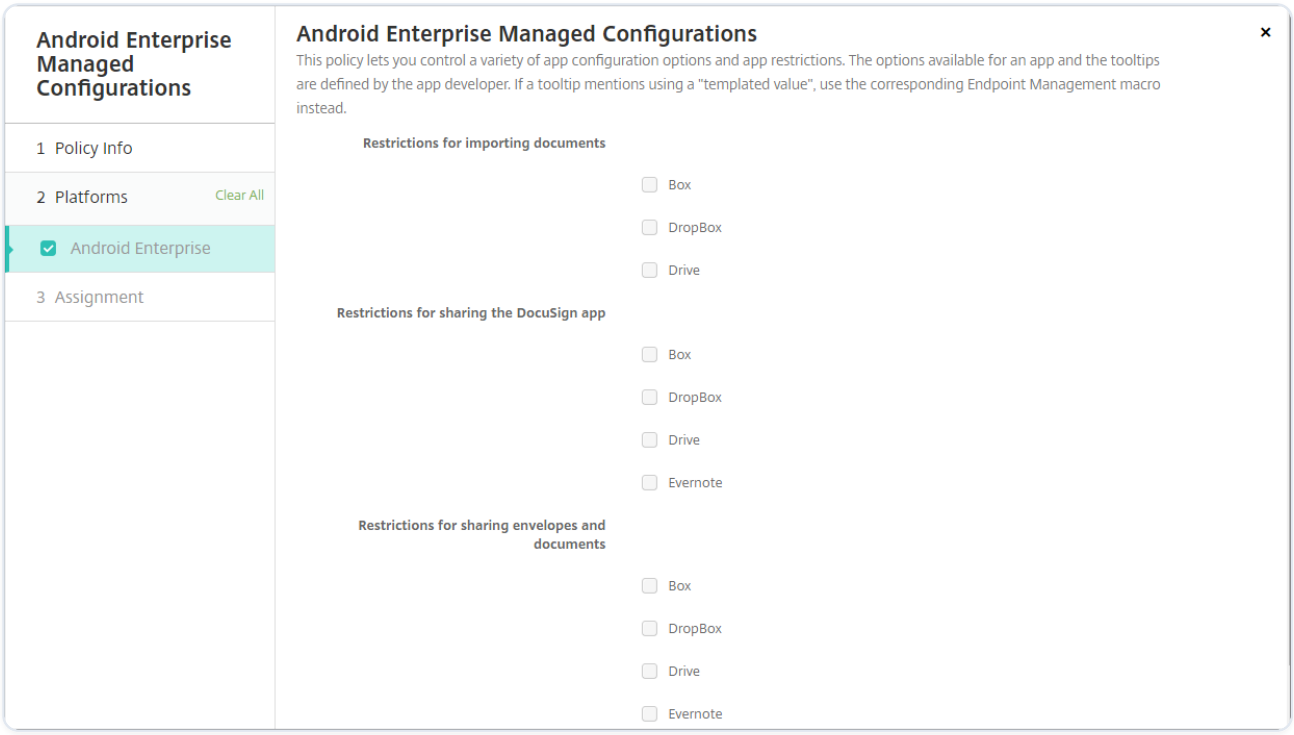
- Si una aplicación que forma parte de la lista de permitidas/denegadas se implementa en un dispositivo después de que se haya iniciado la sesión VPN, el usuario final debe reiniciar la sesión VPN para que la aplicación enrute su tráfico a través de la sesión VPN.
- Si se utiliza una VPN por aplicación a través de una sesión VPN Always On, después de instalar una nueva aplicación en el dispositivo, el usuario final debe reiniciar el perfil de trabajo o reiniciar el dispositivo para que el tráfico de la aplicación se enrute a través de la sesión VPN.

> **Nota:**
>
> Estas limitaciones no son aplicables si utiliza Citrix SSO para Android 23.8.1 o versiones posteriores. Para obtener más información, consulte Reinicio automático de VPN Always On.

Configuración de Android Enterprise

Después de elegir añadir una política de dispositivo de configuraciones administradas, aparece un mensaje para seleccionar una aplicación. Si no hay aplicaciones de Android Enterprise añadidas a Citrix Endpoint Management, no puede continuar.

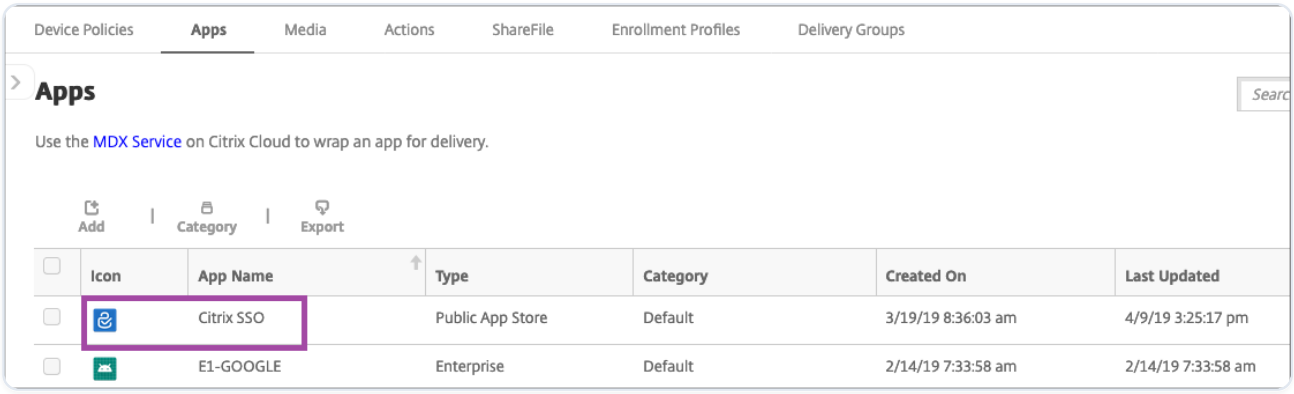
Después de seleccionar una aplicación, configure los ajustes de la política. Los ajustes son específicos para cada aplicación.



Configurar perfiles VPN para Android Enterprise

Ponga los perfiles VPN a disposición de los dispositivos Android Enterprise mediante la aplicación Citrix SSO con la política de dispositivo de configuraciones administradas.

Empiece por añadir Citrix SSO a la consola de Citrix Endpoint Management como una aplicación de Google Play Store. Consulte Agregar una aplicación de tienda de aplicaciones pública.



Vea este vídeo para obtener más información:

Crear una configuración administrada de Android Enterprise para Citrix SSO

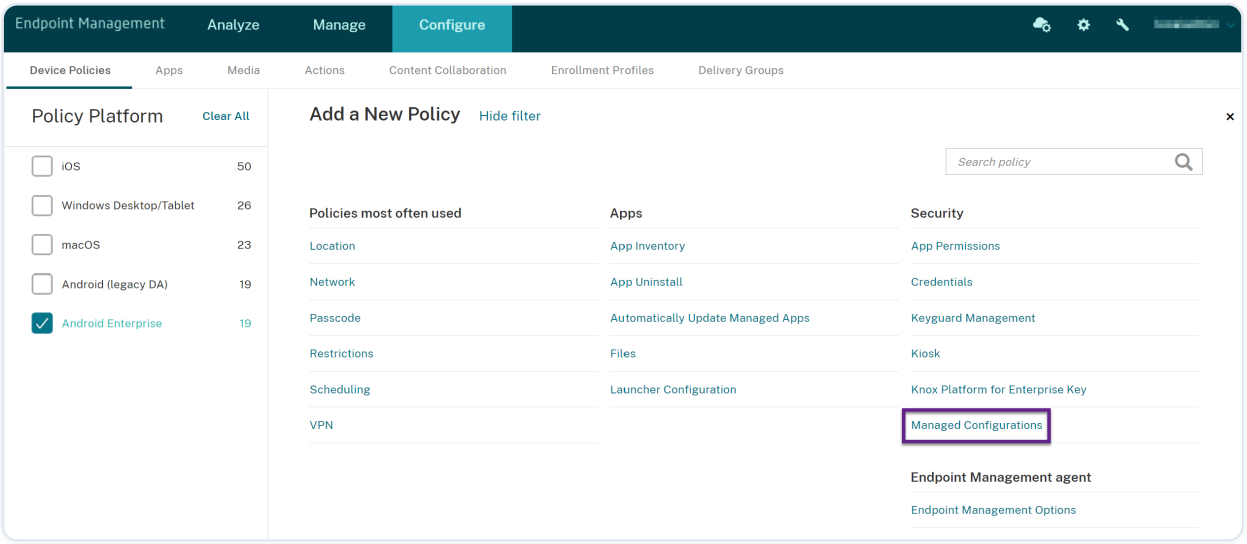
Configure la política de dispositivo de configuraciones administradas para Citrix SSO para crear perfiles VPN. Los dispositivos que tienen la aplicación Citrix SSO instalada y la política implementada pueden acceder a los perfiles VPN que cree.

Citrix Endpoint Management utiliza el certificado de usuario en el almacén de claves del dispositivo si:

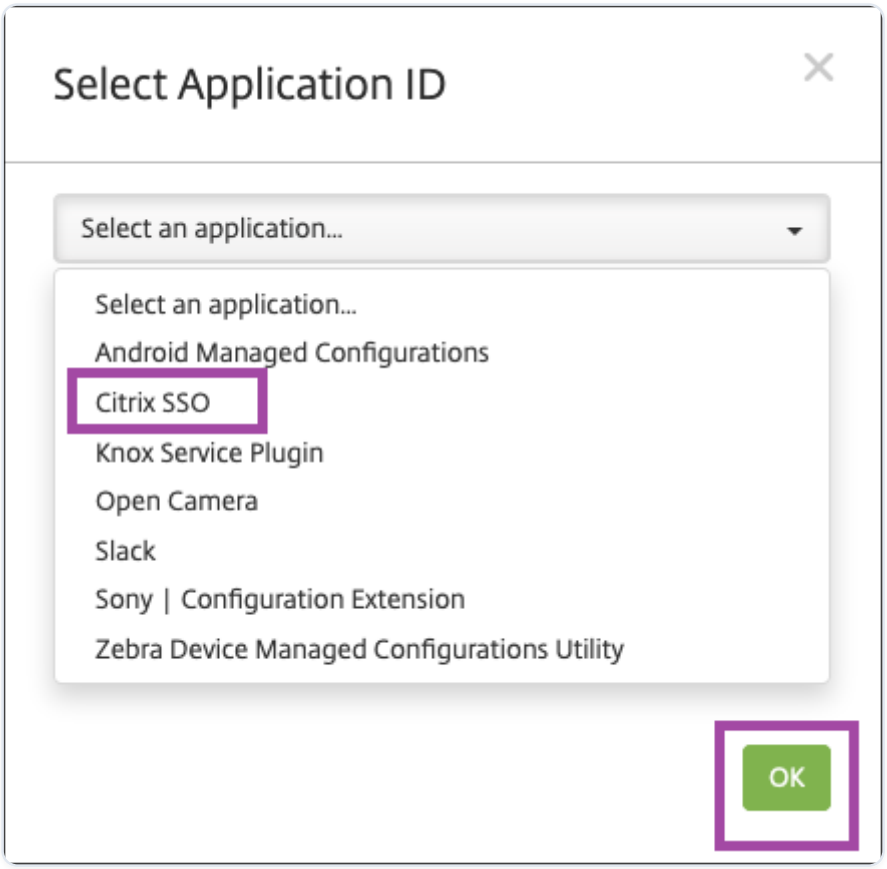
- NetScaler Gateway está configurado para la autenticación basada en certificados.
- **Entregar certificado de usuario para autenticación** está habilitado en la página de Citrix Endpoint Management **Configuración > NetScaler Gateway**.

Necesita el FQDN y el puerto de su NetScaler Gateway.

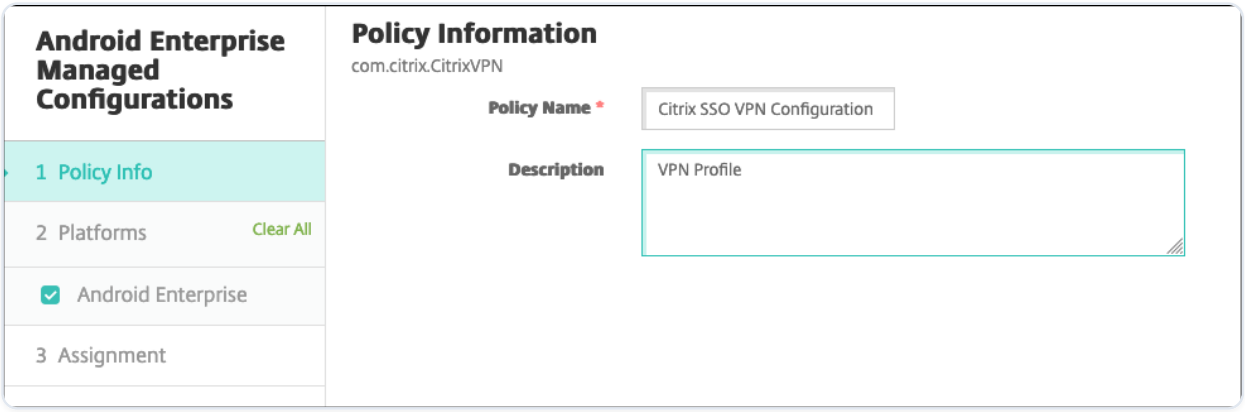
1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Directivas de dispositivo**. Haga clic en **Agregar**.
2. Seleccione **Android Enterprise**. Haga clic en **Configuraciones administradas**.



3. Cuando aparezca la ventana **Seleccionar ID de aplicación**, elija **Citrix SSO** de la lista y haga clic en **Aceptar**.



4. Escriba un nombre y una descripción para su configuración VPN de Citrix SSO. Haga clic en **Siguiente**.



5. Configure los parámetros del perfil VPN.

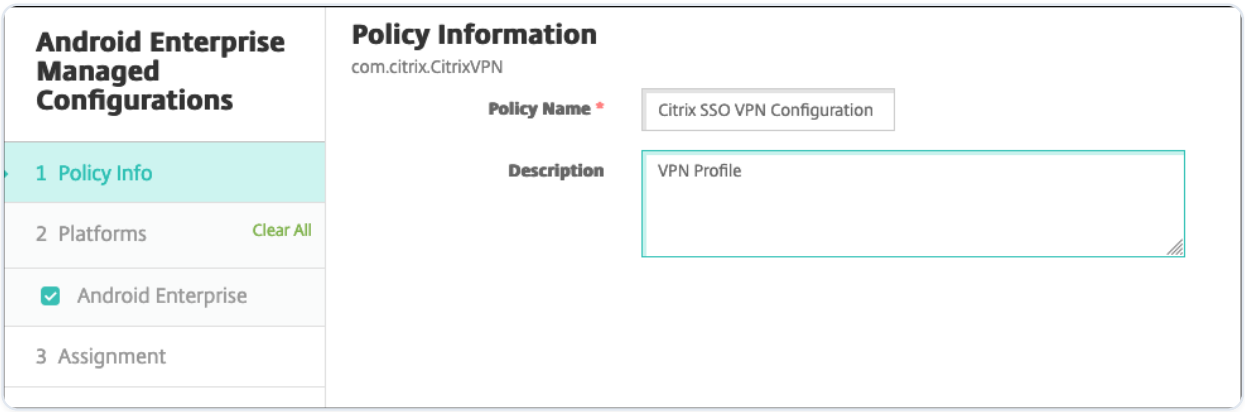
   - **Nombre del perfil VPN:** Escriba un nombre para el perfil VPN. Si va a crear más de un perfil VPN, use un nombre único para cada uno. Si no proporciona un nombre, la dirección que introduzca en el campo **Dirección del servidor** se utilizará como nombre del perfil VPN.
   - **Dirección del servidor(*):** Escriba el FQDN de su NetScaler Gateway. Si el puerto de su NetScaler Gateway no es 443, escriba también el puerto. Utilice el formato URL. Por ejemplo, `https://gateway.mycompany.com:8443`.

- **Nombre de usuario (opcional):** Proporcione el nombre de usuario que los usuarios finales utilizan para autenticarse en NetScaler Gateway. Puede usar la macro de Citrix Endpoint Management {user.username} para este campo. (Consulte Macros). Si no proporciona un nombre de usuario, se pedirá a los usuarios que lo hagan cuando se conecten a NetScaler Gateway.
- **Contraseña (opcional):** Proporcione la contraseña que los usuarios finales utilizan para autenticarse en NetScaler Gateway. Si no proporciona una contraseña, se pedirá a los usuarios que lo hagan cuando se conecten a NetScaler Gateway.
- **Alias de certificado (opcional):** Escriba un alias de certificado. El alias de certificado facilita a la aplicación el acceso al certificado. Cuando se utiliza el mismo alias de certificado con la directiva de dispositivo de credenciales, la aplicación recupera el certificado y autentica la VPN sin ninguna acción por parte de los usuarios.
- **Anclajes de certificado de Gateway (opcional):** Objeto JSON que describe los anclajes de certificado utilizados para NetScaler Gateway. Valor de ejemplo: `{"hash-alg" : "sha256", "pinset" : ["AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=", "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB="]}`. Para obtener más información, consulte Anclaje de certificados de NetScaler Gateway con Android Citrix SSO.
- **Tipo de VPN por aplicación (opcional):** Si utiliza una VPN por aplicación para restringir qué aplicaciones usan esta VPN, puede configurar este ajuste. Si selecciona **Permitir**, el tráfico de red para los nombres de paquete de aplicaciones que aparecen en la **lista de aplicaciones PerAppVPN** se enruta a través de la VPN. El tráfico de red de todas las demás aplicaciones se enruta fuera de la VPN. Si selecciona **Denegar**, el tráfico de red para los nombres de paquete de aplicaciones que aparecen en la **lista de aplicaciones PerAppVPN** se enruta fuera de la VPN. El tráfico de red de todas las demás aplicaciones se enruta a través de la VPN. El valor predeterminado es **Permitir**.
- **Lista de aplicaciones de PerAppVPN:** Una lista de aplicaciones cuyo tráfico está permitido o bloqueado en la VPN, según el valor de **Tipo de VPN por aplicación**. Enumere los nombres de los paquetes de aplicaciones separados por comas o puntos y comas. Los nombres de los paquetes de aplicaciones distinguen entre mayúsculas y minúsculas y deben aparecer en esta lista exactamente como aparecen en Google Play Store. Esta lista es opcional. Mantenga esta lista vacía para aprovisionar una VPN para todo el dispositivo.
- **Perfil VPN predeterminado:** Escriba el nombre del perfil VPN que se utilizará cuando los usuarios toquen el interruptor de conexión en la aplicación Citrix SSO en lugar de un perfil específico. Si este campo se deja vacío, se utiliza el perfil principal para la conexión. Si

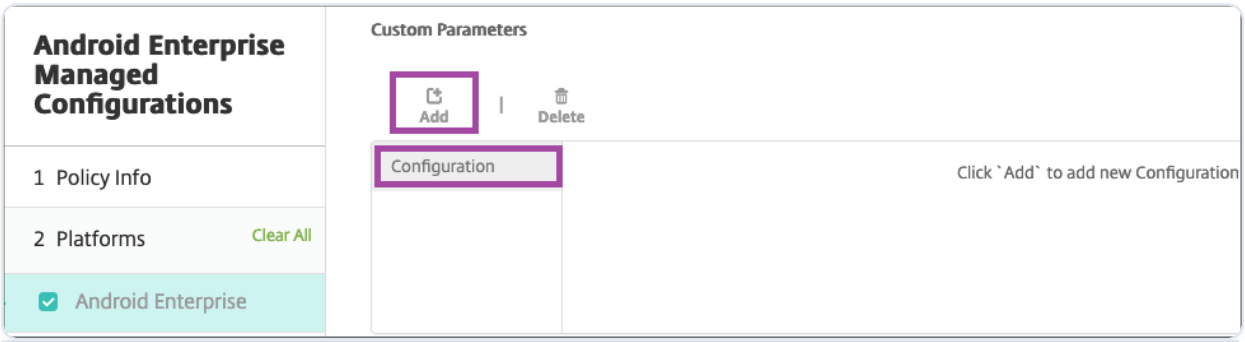
solo se configura un perfil, se marca como el perfil predeterminado. Para la VPN siempre activa, este campo debe establecerse con el nombre del perfil VPN que se utilizará para establecer una VPN siempre activa.

- **VPN siempre activa (opcional):** Este atributo indica si el perfil VPN está configurado como un perfil de VPN siempre activa. Cuando se establece en **true**, significa que el perfil VPN es un perfil de VPN siempre activa. El valor predeterminado es **false**. Esta propiedad solo se puede asignar al perfil VPN principal. Habilitar esta propiedad es esencial para garantizar el funcionamiento fiable de la VPN siempre activa.
- **Deshabilitar perfiles de usuario:** Si esta configuración está activada, los usuarios no pueden crear sus propias VPN en sus dispositivos. Si esta configuración está desactivada, los usuarios pueden crear sus propias VPN en sus dispositivos. El valor predeterminado es Desactivado.
- **Bloquear servidores no confiables:** Esta configuración está desactivada en cualquiera de los siguientes escenarios:
  - Cuando utiliza un certificado autofirmado para NetScaler Gateway
  - Cuando el certificado raíz de la CA que emite el certificado de NetScaler Gateway no está en la lista de CA del sistema.

  Si esta configuración está activada, el sistema operativo Android valida el certificado de NetScaler Gateway. Si la validación falla, no se permite la conexión. El valor predeterminado es Activado.



6. Opcionalmente, cree parámetros personalizados. Se admiten los parámetros personalizados **XenMobileDeviceId** y **UserAgent**. Seleccione la configuración VPN actual y haga clic en **Agregar**.



NOMBRE DEL PARÁMETRO	DESCRIPCIÓN	VALOR
XenMobileDeviceId	Este campo es el ID de dispositivo que se utilizará para la comprobación de acceso a la red basada en la inscripción de dispositivos en Citrix Endpoint Management. Si Citrix Endpoint Management inscribe y administra el dispositivo, se permite la conexión VPN. De lo contrario, la autenticación se deniega en el momento del establecimiento de la VPN.	Para que Citrix Endpoint Management determine el estado de inscripción y administración de los dispositivos, el valor de XenMobileDeviceID se establece en `DeviceID_${device.id}`.
UserAgent	Este texto se añade al encabezado HTTP User-Agent para realizar una comprobación adicional en NetScaler Gateway. El valor de este texto se añade al encabezado HTTP User-Agent por la aplicación Citrix SSO al comunicarse con NetScaler Gateway.	Escriba el texto que desea añadir al encabezado HTTP User-Agent. Este texto debe ajustarse a las especificaciones del encabezado HTTP User-Agent.
EnableDebugLogging	Habilite el registro de depuración en la aplicación Citrix SSO para ayudar a solucionar problemas de conectividad VPN en caso	**True**: Habilita el registro de depuración. Valor predeterminado: **False**

NOMBRE DEL PARÁMETRO	DESCRIPCIÓN	VALOR
	de VPN siempre activa. Puede habilitarlo en cualquiera de las configuraciones VPN administradas. El registro de depuración surte efecto cuando se procesan las configuraciones administradas.	
DisableLogoutFromStoreOnExplicitDisconnect	Controla el cierre de sesión de la tienda cuando el usuario final desconecta explícitamente la sesión VPN de la interfaz de usuario de la aplicación. Aplicable solo a implementaciones de Citrix Secure Private Access.	**True**: Deshabilita el cierre de sesión de la tienda de Secure Private Access y deja la sesión de Secure Private Access intacta, solo desconecta la sesión de la aplicación Citrix Secure Access. Valor predeterminado: **False**.

Asistente de configuración administrada de Android Enterprise (/en-us/citrix-endpoint-management/media/citrixsso-custom-params-xmdeviceid.png)

Para crear otro parámetro personalizado, haga clic de nuevo en **Agregar**.

7. Opcionalmente, cree más configuraciones de perfil VPN. Haga clic en **Agregar** debajo de la lista de configuraciones. Aparecerá una nueva configuración en la lista. Seleccione la nueva configuración y repita el paso 5 y, opcionalmente, el paso 6.

   Asistente de configuración administrada de Android Enterprise (/en-us/citrix-endpoint-management/media/citrixsso-add-more-vpns.png)
8. Cuando haya creado todos los perfiles VPN que desee, haga clic en **Siguiente**.
9. Configure las reglas de implementación para esta configuración administrada para Citrix SSO.
10. Haga clic en **Guardar**.

Esta configuración administrada para Citrix SSO aparece ahora en su lista de directivas de dispositivo configuradas.

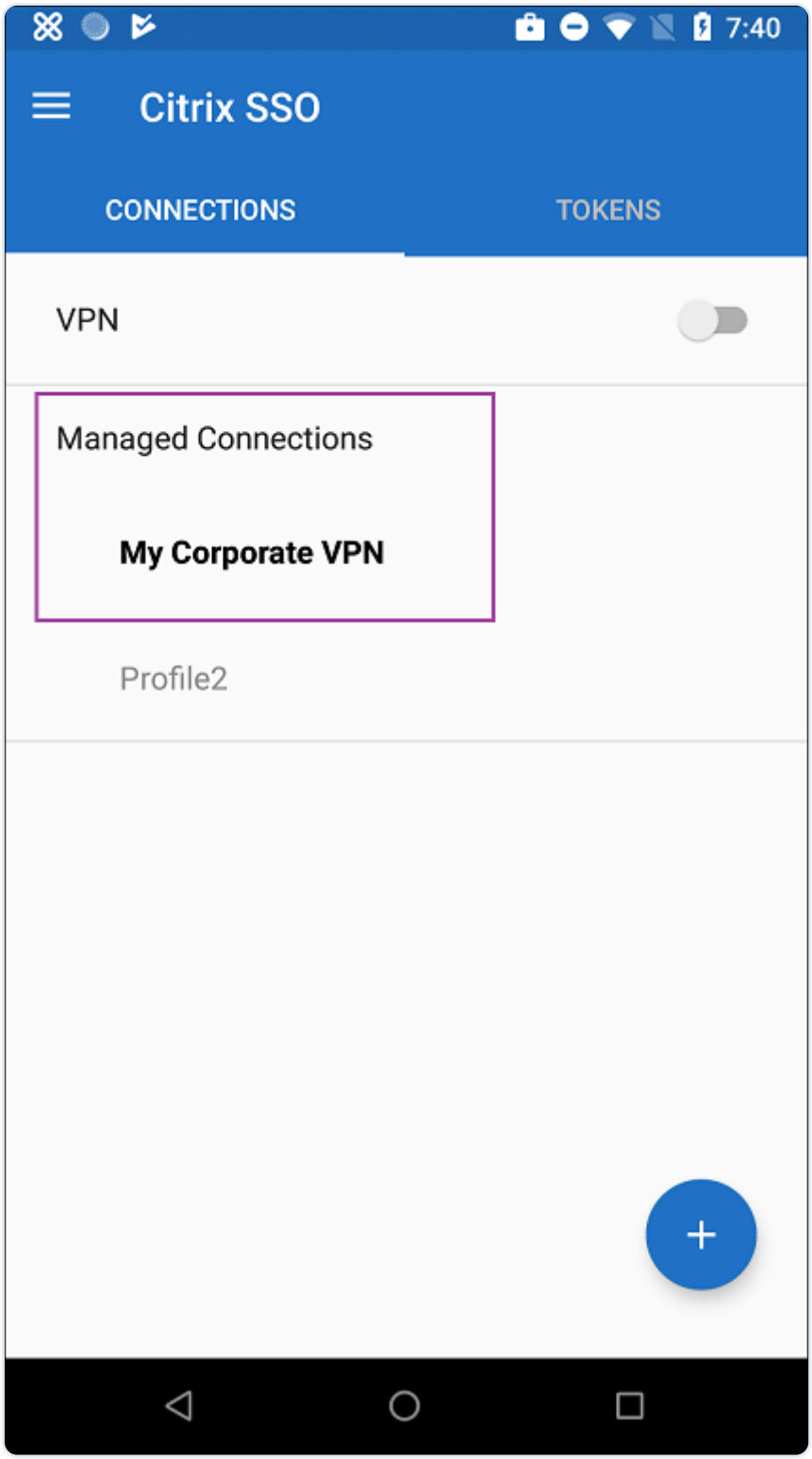
Para habilitar la conexión permanente para los perfiles VPN que configuró, establezca la directiva de dispositivo de opciones de Citrix Endpoint Management (/es-es/citrix-endpoint-management/policies/options-policy.html#android-enterprise-settings).

> **Nota:**
>
> Se requiere Citrix Secure Hub 19.5.5 o una versión posterior para la VPN siempre activa en Android Enterprise.

Acceso a los perfiles VPN desde el dispositivo

Para acceder a los perfiles VPN que creó, los usuarios de Android Enterprise instalan Citrix SSO desde la tienda administrada de Google Play.

El perfil o los perfiles VPN que configuró aparecen en el área **Conexiones administradas** de la aplicación. Los usuarios tocan el perfil VPN para conectarse mediante ese perfil VPN.



Después de que los usuarios se hayan autenticado y conectado, aparece una marca de verificación junto al perfil VPN. El icono de la llave indica que la VPN está conectada.

Administrar dispositivos Android Zebra con Zebra OEMConfig

Administre dispositivos Android Zebra mediante la herramienta administrativa Zebra Technologies OEMConfig. Para obtener información sobre la aplicación Zebra OEMConfig, consulte el sitio web de Zebra Technologies.

Citrix Endpoint Management es compatible con Zebra OEMConfig versión 9.2 y posteriores. Para obtener información sobre los requisitos del sistema para instalar Zebra OEMConfig en los dispositivos, consulte OEMConfig Setup en el sitio web de Zebra Technologies.

Actualmente admitimos los siguientes dispositivos Zebra:

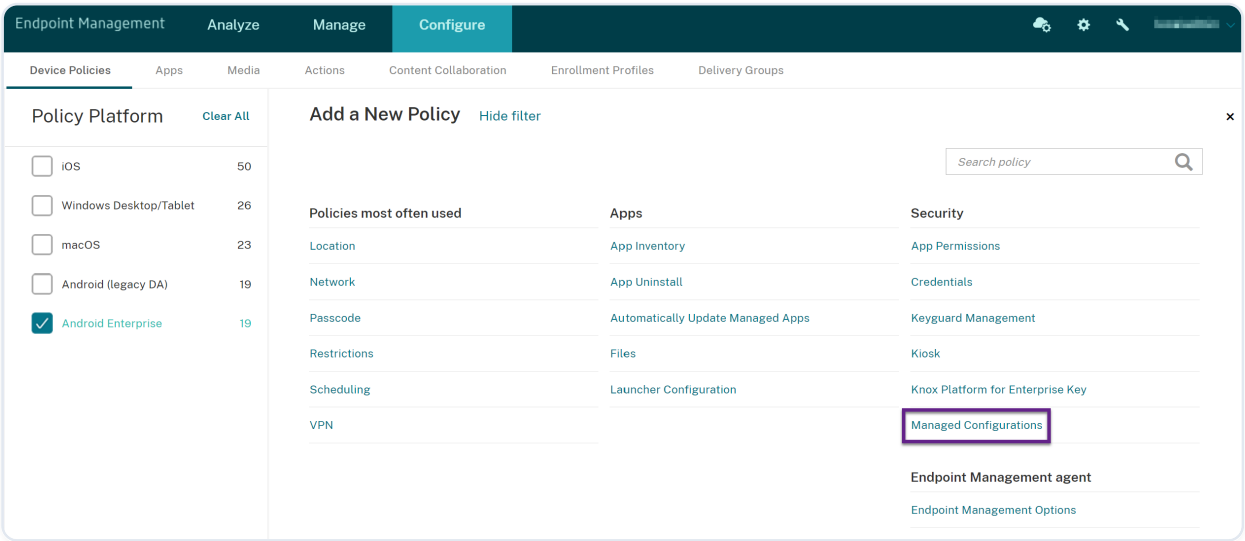
- EC50, EC55, ET56
- TC52x, TC52x-HC
- TC52ax, TC52ax-HC
- TC57x

Para empezar: En la consola de Citrix Endpoint Management, añada la aplicación Zebra OEMConfig como una aplicación de Google Play Store. Consulte Agregar una aplicación de tienda de aplicaciones pública.

Crear una configuración administrada de Android Enterprise para la aplicación Zebra OEMConfig

Configure la directiva de dispositivos de configuraciones administradas para la aplicación Zebra OEMConfig. La directiva se aplica a los dispositivos Zebra que tienen la aplicación Zebra OEMConfig instalada y la directiva implementada.

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Directivas de dispositivos**. Haga clic en **Agregar**.
2. Seleccione **Android Enterprise**. Haga clic en **Configuraciones administradas**.



3. Cuando aparezca la ventana **Seleccionar ID de aplicación**, elija **ZebraOEMConfig powered by MX** de la lista y haga clic en **Aceptar**.

4. Escriba un nombre y una descripción para su configuración de Zebra OEMConfig. Haga clic en **Siguiente**.
5. Escriba un nombre para la configuración de Zebra OEMConfig.
6. Configure los parámetros disponibles. Por ejemplo:
    - Para deshabilitar la cámara frontal del dispositivo, seleccione **Configuración de la cámara** y establezca **Uso de la cámara frontal** en **Desactivado**.
    - Para cambiar el formato de hora de los dispositivos, seleccione **Configuración del reloj** y establezca **Formato de hora** en **12** (12 horas) o **24** (24 horas).

Para obtener una lista y descripciones de todas las configuraciones disponibles, consulte Zebra Managed Configurations en el sitio web de Zebra Technologies.

1. Opcionalmente, cree más configuraciones de Zebra OEMConfig. Haga clic en **Agregar** debajo de la lista de configuraciones. Aparecerá una nueva configuración en la lista. Seleccione la nueva configuración y configure los parámetros.
2. Cuando haya creado todas las configuraciones de Zebra OEMConfig que desee, haga clic en **Siguiente**.
3. Configure las reglas de implementación para esta configuración administrada para Zebra OEMConfig.
4. Haga clic en **Guardar**.

Administrar Chrome Browser con marcadores predefinidos

Aquí tiene un ejemplo de cómo administrar Chrome Browser con marcadores predefinidos:

```
[



{ "toplevel_name": "My managed bookmarks folder" }

,



{ "name": "Google", "url": "[google.com|http://google.com/]" }

,
```

```
{ "name": "Youtube", "url": "[youtube.com|http://youtube.com/]" }

,

{

"nested_links": [



{ "name": "Chromium", "url": "[chromium.org|http://chromium.org/]" }

,



{ "name": "Chromium Developers", "url": "[dev.chromium.org|http://
dev.chromium.org/]" }

],

"name": "Chrome links"

}

]
```

Soporte para comentarios de configuraciones administradas (Vista previa técnica)

Para obtener más información sobre la función de soporte para comentarios de configuraciones administradas, consulte Support managed configurations feedback.

Directiva de dispositivos de dominios administrados

Puede definir dominios administrados que se aplican al correo electrónico y al navegador Safari. Los dominios administrados le ayudan a proteger los datos corporativos controlando qué aplicaciones pueden abrir documentos descargados de dominios mediante Safari.

Para los dispositivos iOS supervisados, especifique:

- URL o subdominios para controlar cómo los usuarios pueden abrir documentos, archivos adjuntos y descargas desde el navegador.
- URL desde las que los usuarios pueden guardar contraseñas en Safari.

Para conocer los pasos para configurar un dispositivo iOS en modo supervisado, consulte Implementar dispositivos con Apple Configurator 2.

Cuando un usuario envía un correo electrónico a un destinatario cuyo dominio no está en la lista de dominios de correo electrónico administrados, el mensaje se marca en el dispositivo del usuario para advertirle de que está enviando un mensaje a alguien ajeno a su dominio corporativo.

Para elementos como documentos, archivos adjuntos o descargas: Cuando un usuario abre un elemento mediante Safari desde un dominio web que está en la lista de dominios web administrados, la aplicación corporativa adecuada abre el elemento. Si el elemento no procede de un dominio web de la lista de dominios web administrados, el usuario no puede abrirlo con una aplicación corporativa. Debe usar una aplicación personal no administrada.

Para dispositivos supervisados, incluso si no especifica dominios de autocompletado de contraseñas de Safari: Si el dispositivo está configurado como multiusuario efímero, los usuarios no pueden guardar contraseñas. Sin embargo, si el dispositivo no está configurado como multiusuario efímero, los usuarios pueden guardar todas las contraseñas.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivos**. Para obtener más información, consulte Directivas de dispositivos.

Configuración de iOS

Para especificar dominios:

FORMATO	DESCRIPCIÓN
`example.com`	Tratar cualquier ruta bajo `example.com` como gestionada, pero no `site.example.com/`.
`foo.example.com`	Tratar cualquier ruta bajo `foo.example.com` como gestionada, pero no `example.com/` ni `bar.example.com/`.

FORMATO	DESCRIPCIÓN
`*.example.com`	Tratar cualquier ruta bajo `foo.example.com` o `bar.example.com` como gestionada, pero no `example.com/`.
`example.com/sub`	Tratar `example.com/sub` y cualquier ruta bajo ella como gestionada, pero no `example.com/`.
`foo.example.com/sub`	Tratar cualquier ruta bajo `foo.example.com/sub` como gestionada, pero no `example.com`, `example.com/sub`, `foo.example.com/` ni `bar.example.com/sub`.
`*.example.com/sub`	Tratar cualquier ruta bajo `foo.example.com/sub` o `bar.example.com/sub` como gestionada, pero no `example.com` ni `foo.example.com/`.

Reglas:

- Los prefijos "www." y las barras finales en las URL se ignoran al comparar dominios.
- Si una entrada tiene un número de puerto, solo las direcciones que especifican ese número de puerto se consideran gestionadas. De lo contrario, solo los puertos estándar se consideran gestionados (puerto 80 para http y puerto 443 para https). Por ejemplo, el patrón `*.example.com:8080` coincide con `https://site.example.com:8080/page.html`, pero no con `https://site.example.com/page.html`, pero el patrón `*.example.com` coincide con `https://site.example.com/page.html` y `https://site.example.com/page.html`, pero no con `https://site.example.com:8080/page.html`.
- Las definiciones de dominios web gestionados de Safari son acumulativas. Los patrones definidos por todas las cargas de dominios web gestionados de Safari se utilizan para hacer coincidir una solicitud de URL.

Configuración:

- **Dominios administrados**
  - **Dominios de correo electrónico sin marcar:** Para cada dominio de correo electrónico que desee incluir en la lista, haga clic en **Agregar** y, a continuación, haga lo siguiente:

    - **Dominio de correo electrónico administrado:** Escriba el dominio de correo electrónico.
    - Haga clic en **Guardar** para guardar el dominio de correo electrónico o haga clic en **Cancelar** para no guardar el dominio de correo electrónico.
  - **Dominios web de Safari administrados:** Para cada dominio web que desee incluir en la lista, haga clic en **Agregar** y, a continuación, haga lo siguiente:
    - **Dominio web administrado:** Escriba el dominio web.
    - Haga clic en **Guardar** para guardar el dominio web o haga clic en **Cancelar** para no guardar el dominio web.
  - **Dominios de autorrelleno de contraseñas de Safari:** Para cada dominio de autorrelleno que desee incluir en la lista, haga clic en **Agregar** y, a continuación, haga lo siguiente:
    - **Dominio de autorrelleno de contraseñas de Safari:** Escriba el dominio de autorrelleno.
    - Haga clic en **Guardar** para guardar el dominio de autorrelleno o haga clic en **Cancelar** para no guardar el dominio de autorrelleno.
- **Configuración de directivas**
  - **Quitar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva. Solo disponible para iOS 6.0 y versiones posteriores.

Política de dispositivo de usuarios residentes máximos

La política de dispositivo de usuarios residentes máximos es para dispositivos compartidos que ejecutan iOS (iPadOS). Para obtener más información sobre los iPad compartidos, consulte (/es-es/citrix-endpoint-management/device-management/apple/integrate-with-apple-education.html).

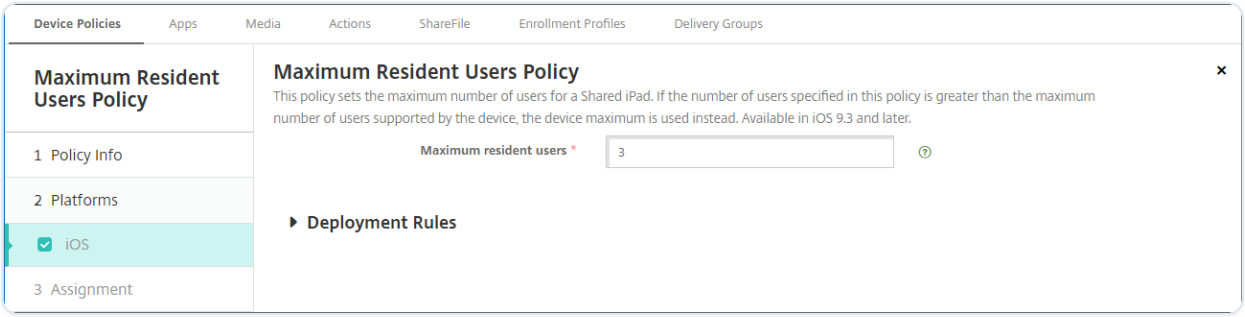
Esta política debe implementarse cuando el iPad se encuentra en la fase de "espera de configuración" durante el Asistente de Configuración. Apple no permite que esta política se implemente después de que los iPad compartidos se inscriban.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte (/es-es/citrix-endpoint-management/policies.html).

Configuración de iOS

- **Usuarios residentes máximos:** El número máximo de usuarios para un iPad compartido. Si el número de usuarios especificado en esta política es mayor que el número máximo de usuarios admitidos por el dispositivo, Citrix Endpoint Management utiliza el máximo del dispositivo en su lugar. El valor predeterminado es **5** usuarios.

  Apple recomienda mantener el valor de Usuarios residentes máximos lo más bajo posible. Un valor bajo maximiza la cantidad de almacenamiento del iPad para cada usuario. Además, un valor bajo minimiza la comunicación con iCloud y proporciona una experiencia de inicio de sesión más rápida. Para obtener información sobre cómo Apple gestiona el almacenamiento compartido en un iPad, consulte `<https://developer.apple.com/education/shared-ipad/>`.



Política de dispositivo de opciones de MDM

La política de dispositivo de opciones de MDM gestiona el bloqueo de activación de Buscar mi iPhone/iPad en dispositivos iOS supervisados. Para conocer los pasos para configurar un dispositivo iOS en modo supervisado, consulte (/es-es/citrix-endpoint-management/device-management/apple/ios-bulk-enrollment.html#deploy-devices-using-apple-configurator-2).

El Bloqueo de activación es una función de Buscar mi iPhone/iPad que impide la reactivación de un dispositivo supervisado perdido o robado. El Bloqueo de activación requiere el ID de Apple y la contraseña del usuario antes de que nadie pueda desactivar Buscar mi iPhone/iPad, borrar el dispositivo o reactivarlo. Para los dispositivos que posee su organización, es necesario omitir un Bloqueo de activación para, por ejemplo, restablecer o reasignar dispositivos.

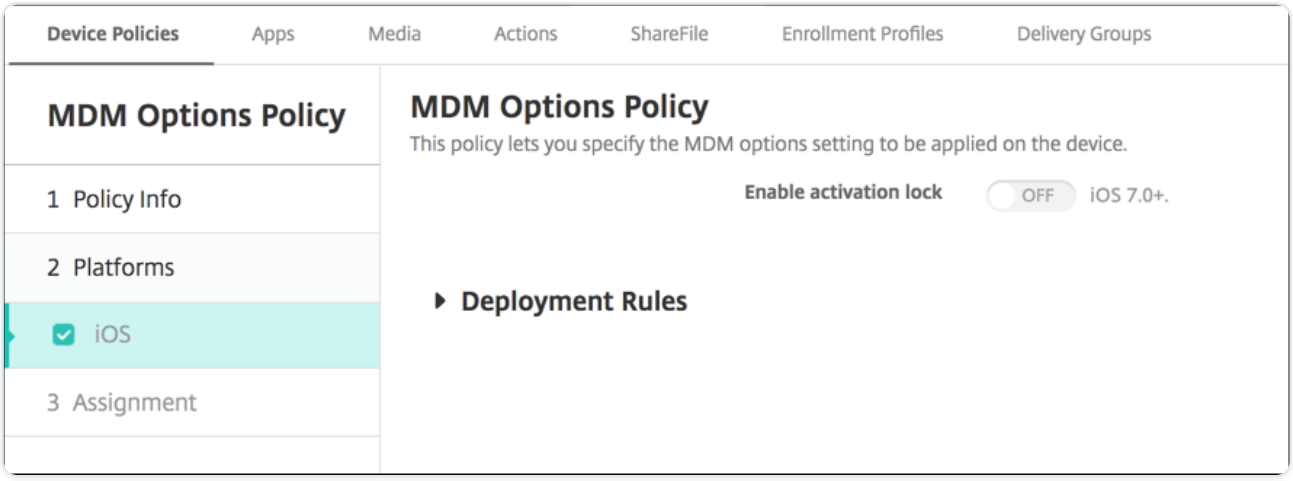
Para habilitar el Bloqueo de activación, configure e implemente la política de dispositivo de opciones de MDM de Citrix Endpoint Management. A continuación, puede administrar un dispositivo desde la consola de Citrix Endpoint Management sin las credenciales de Apple del

usuario. Para omitir el requisito de credenciales de Apple de un Bloqueo de activación, emita la acción de seguridad Omisión de Bloqueo de activación desde la consola de Citrix Endpoint Management.

Por ejemplo, si el usuario devuelve un teléfono perdido o para configurar el dispositivo antes o después de un borrado completo: Cuando el teléfono solicite la credencial de la cuenta de Apple App Store, puede omitir ese paso emitiendo la acción de seguridad Omisión de Bloqueo de activación desde la consola de Citrix Endpoint Management.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte (/es-es/citrix-endpoint-management/policies.html).

Configuración de iOS



- **Habilitar Bloqueo de activación:** Seleccione si desea habilitar el Bloqueo de activación en los dispositivos a los que implementa esta directiva. El valor predeterminado es **Desactivado**.

Después de habilitar el Bloqueo de activación implementando la política de dispositivo de opciones de MDM: La acción de seguridad **Omisión de Bloqueo de activación** aparece cuando selecciona esos dispositivos en la página **Administrar > Dispositivos** y hace clic en **Seguridad**. Una omisión de Bloqueo de activación le permite eliminar el Bloqueo de activación de los dispositivos supervisados antes de la activación del dispositivo sin conocer el ID de Apple y la contraseña de los usuarios del dispositivo. Puede enviar una omisión de Bloqueo de activación a un dispositivo antes o después de un borrado completo. Para obtener más información, consulte (/es-es/citrix-endpoint-management/device-management/apple/ios.html#bypass-an-ios-activation-lock).

Directiva de dispositivos de red

La directiva de dispositivos de red le permite administrar cómo los usuarios conectan sus dispositivos a las redes Wi-Fi definiendo los siguientes elementos:

- Nombres y tipos de red
- Directivas de autenticación y seguridad
- Uso del servidor proxy
- Otros detalles relacionados con Wi-Fi

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivos**. Para obtener más información, consulte Directivas de dispositivos.

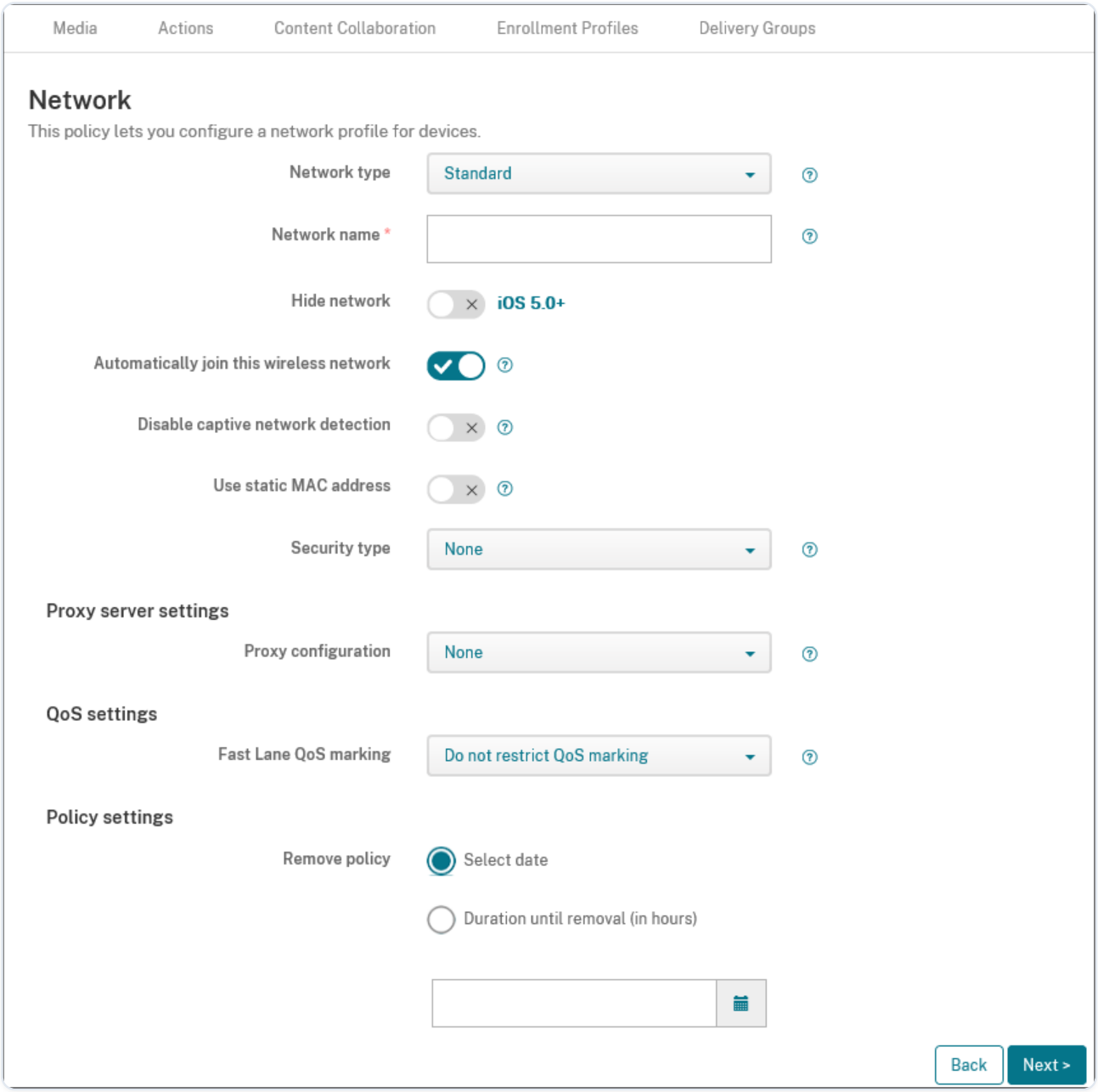
Requisitos previos

Antes de crear una directiva, complete lo siguiente:

- Cree los grupos de entrega que planee usar.
- Conozca el nombre y el tipo de red.
- Conozca los tipos de autenticación o seguridad que planea usar.
- Conozca cualquier información del servidor proxy que pueda necesitar.
- Instale los certificados de CA necesarios.
- Tenga las claves compartidas necesarias.
- Cree la entidad PKI para la autenticación basada en certificados.
- Configure los proveedores de credenciales.

Para obtener más información, consulte Autenticación y sus subartículos.

Configuración de iOS



- **Tipo de red:** En la lista, elija **Estándar**, **Punto de acceso heredado** o **Punto de acceso 2.0** para establecer el tipo de red que piensa utilizar.
- **Nombre de red:** Escriba el SSID que se ve en la lista de redes disponibles para el dispositivo. No se aplica a **Hotspot 2.0**.
- **Ocultar red:** Elija si la red está oculta.
- **Unirse automáticamente a esta red inalámbrica:** Elija si un dispositivo se une a la red automáticamente. Si un dispositivo está conectado a otra red, no se une a esta red. El usuario debe desconectar de la red anterior antes de que el dispositivo se conecte automáticamente. El valor predeterminado es **Activado**.

- **Inhabilitar la detección de redes cautivas:** El asistente de redes cautivas ayuda a los usuarios a acceder a redes de suscripción o de puntos de acceso Wi-Fi. Normalmente, estas redes se encuentran en cafeterías, hoteles y otros lugares públicos. Si está **Activado**, los dispositivos pueden seguir conectándose a redes cautivas, pero el usuario debe abrir un explorador e iniciar sesión manualmente. El valor predeterminado es **Desactivado**.
- **Usar dirección MAC estática:** Las direcciones MAC son identificadores únicos que un dispositivo transmite dentro de una red. Para aumentar la privacidad, los dispositivos iOS y iPadOS pueden usar una dirección MAC diferente cada vez que se conectan a una red. Si está **Activado**, el dispositivo siempre usa la misma dirección MAC al conectarse a esta red. Si está **Desactivado**, el dispositivo usa una dirección MAC diferente cada vez que se conecta a esta red. El valor predeterminado es **Desactivado**.
- **Tipo de seguridad:** En la lista, elija el tipo de seguridad que piensa utilizar. No se aplica a **Hotspot 2.0**.
    - Ninguno: No requiere más configuración.
    - WEP
    - WPA/WPA2/WPA3 Personal
    - Cualquiera (Personal)
    - WEP Enterprise
    - WPA/WPA2/WPA3 Enterprise: Para la última versión de Windows 10, configure el Protocolo de inscripción de certificados simple (SCEP) para usar WPA-2 Enterprise. Citrix Endpoint Management puede enviar el certificado a los dispositivos para autenticarse en el servidor Wi-Fi. Para configurar SCEP, vaya a la página Distribución de **Parámetros > Proveedores de credenciales**. Para obtener más información, consulte Proveedores de credenciales.
    - Cualquiera (Empresarial)

  En las siguientes secciones se enumeran las opciones que se configuran para cada uno de los tipos de conexión anteriores.
- **Configuración del servidor proxy**
    - **Configuración del proxy:** En la lista, elija **Ninguno**, **Manual** o **Automático** para establecer cómo la conexión VPN se enruta a través de un servidor proxy y, a continuación, configure cualquier opción adicional. El valor predeterminado es **Ninguno**, lo que no requiere ninguna configuración adicional.
    - Si elige **Manual**, configure estos parámetros:

    - **Nombre de host o dirección IP:** Escriba el nombre de host o la dirección IP del servidor proxy.
    - **Puerto:** Escriba el número de puerto del servidor proxy.
    - **Nombre de usuario:** Escriba un nombre de usuario opcional para autenticarse en el servidor proxy.
    - **Contraseña:** Escriba una contraseña opcional para autenticarse en el servidor proxy.
  - Si elige **Automático**, configure estos parámetros:
    - **URL del servidor:** Escriba la URL del archivo PAC que define la configuración del proxy.
    - **Permitir conexión directa si el PAC no es accesible:** Elija si desea permitir a los usuarios conectarse directamente al destino si el archivo PAC no es accesible. El valor predeterminado es **Activado**.
- **Marcado QoS de Fast Lane:** Si no restringe el marcado QoS para una red Wi-Fi compatible con Cisco Fast Lane QoS, todas las aplicaciones pueden usar el marcado L2 y L3. Si restringe el marcado QoS, especifique las aplicaciones que pueden usar el marcado L2 y L3.
  - **Habilitar marcado QoS:** Si restringe el marcado QoS, use esta configuración para deshabilitarlo por completo o para marcar solo ciertas aplicaciones. Si está en **Desactivado**, deshabilita el marcado QoS por completo. Si está en **Activado**, configure una lista de aplicaciones que puedan usar el marcado QoS. El valor predeterminado es **Activado**.
  - **Permitir llamadas de audio/vídeo de Apple:** Elija si las aplicaciones de llamadas de audio y vídeo pueden usar el marcado QoS. Si está en **Desactivado**, la calidad de las llamadas de vídeo y audio puede verse afectada.
  - **Permitir aplicaciones específicas:** Agregue un ID de paquete de aplicación a esta lista para permitir que la aplicación use el marcado QoS.
- **Configuración de Hotspot 2.0**
  - **Nombre del operador mostrado:** El nombre descriptivo transmitido por el dispositivo Hotspot. Los usuarios ven este nombre en su lista de redes Wi-Fi disponibles.
  - **Nombre de dominio:** El nombre de dominio utilizado para la negociación de Hotspot 2.0.
  - **Permitir la conexión a redes de socios de itinerancia:** Si está en **Activado**, los dispositivos que se desplazan fuera de su red doméstica pueden conectarse a redes de socios.

  - **Identificadores de organización de consorcio de itinerancia (OI):** Agregue una lista de identificadores de organización a los que el dispositivo puede acceder. Un OI de consorcio de itinerancia pertenece a una organización con métodos de autenticación compartidos. Si el Hotspot que configura no está disponible, el dispositivo se conecta a un OI de consorcio de itinerancia que aparece aquí.
  - **Nombres de dominio de identificador de acceso a la red (NAI):** Configure una lista de nombres de dominio utilizados para identificar a los usuarios en una red de itinerancia. Un NAI se transmite en el formato `user@realm`.
  - **Códigos de país de móvil (MCC) y configuraciones de red móvil (MNC):** Un Código de País de Móvil consta de tres dígitos que identifican el país de una red. El Código de Red Móvil consta de 2 o 3 dígitos únicos. Cuando se usan juntos, el MCC/MNC identifica de forma única a un operador o proveedor de red móvil.

- **Configuración de directivas**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.
  - **Permitir al usuario eliminar la directiva:** Puede seleccionar cuándo pueden los usuarios eliminar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**. No disponible para iOS.

Configuración de WPA, WPA Personal, Cualquiera (Personal) para iOS

Contraseña: Escriba una contraseña opcional. Si deja este campo en blanco, es posible que se pida a los usuarios sus contraseñas al iniciar sesión.

Configuración de WEP Enterprise, WPA Enterprise, WPA2 Enterprise, WPA3 Enterprise, Cualquiera (Enterprise) para iOS

Cuando elige cualquiera de estos tipos de seguridad, la configuración de **EAP** aparece después de la **Configuración de QoS**.

> **Importante:**
>
> Si selecciona el tipo de seguridad **WPA2 Enterprise**, debe permitir al menos un protocolo EAP.

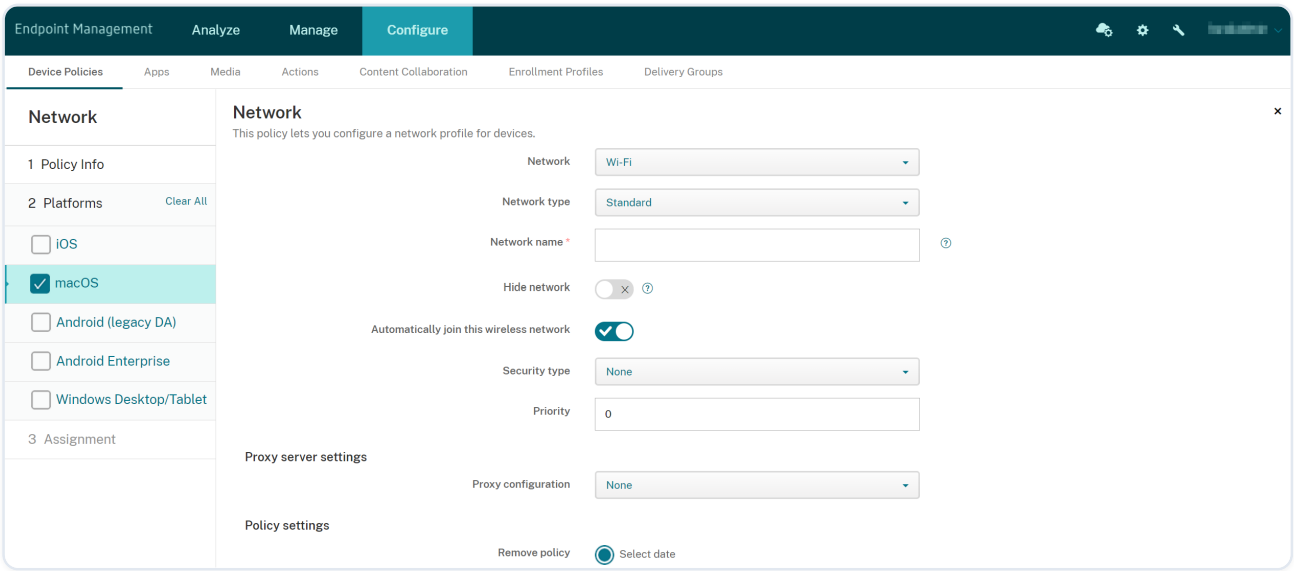
- **Protocolos EAP permitidos:** Habilite los tipos de EAP que quiera admitir y, a continuación, configure los ajustes asociados. El valor predeterminado es **Desactivado** para cada uno de los tipos de EAP disponibles.
- **Autenticación interna (TTLS):** *Obligatorio solo cuando habilita TTLS*. En la lista, elija el método de autenticación interna que desea usar. Las opciones son: **PAP**, **CHAP**, **MSCHAP** o **MSCHAPv2**. El valor predeterminado es **MSCHAPv2**.
- **EAP-FAST con PAC:** Elija si desea usar credenciales de acceso protegidas (PAC).
    - Si elige **Usar PAC**, elija si desea usar un PAC de aprovisionamiento.
        - Si elige **PAC de aprovisionamiento**, elija si desea permitir un protocolo de enlace TLS anónimo entre el cliente del usuario final y Citrix Endpoint Management.
            - **Aprovisionamiento de PAC de forma anónima**
- **Autenticación:**
    - **Nombre de usuario:** Escriba un nombre de usuario.
    - **Contraseña por conexión:** Elija si desea solicitar una contraseña cada vez que los usuarios inicien sesión.
    - **Contraseña:** Escriba una contraseña opcional. Si deja este campo en blanco, es posible que se les pida a los usuarios sus contraseñas cuando inicien sesión.
    - **Credencial de identidad (almacén de claves o credencial PKI):** En la lista, elija el tipo de credencial de identidad. El valor predeterminado es **Ninguno**.
    - **Identidad externa:** *Obligatorio solo cuando habilita* **PEAP**, **TTLS** *o* **EAP-FAST**. Escriba el nombre de usuario visible externamente. Puede aumentar la seguridad escribiendo un término genérico como "anónimo" para que el nombre de usuario no sea visible.
    - **Requerir un certificado TLS:** Elija si desea requerir un certificado TLS.
- **Confianza**
    - **Certificados de confianza:** Para agregar un certificado de confianza, haga clic en **Agregar** y, para cada certificado que desee agregar, haga lo siguiente:

- **Aplicación:** En la lista, elija la aplicación que desea agregar.
- Haga clic en **Guardar** para guardar el certificado o haga clic en **Cancelar**.

- **Nombres de certificados de servidor de confianza:** Para agregar nombres comunes de certificados de servidor de confianza, haga clic en **Agregar** y, para cada nombre que desee agregar, haga lo siguiente:
  - **Certificado:** Escriba el nombre del certificado del servidor. Puede usar caracteres comodín para especificar el nombre, como wpa.*.example.com.
  - Haga clic en **Guardar** para guardar el nombre del certificado o haga clic en **Cancelar**.

- **Permitir excepciones de confianza:** Elija si el cuadro de diálogo de confianza del certificado aparece en los dispositivos de los usuarios cuando un certificado no es de confianza. El valor predeterminado es **Activado**.

Configuración de macOS



- **Red:** En la lista, elija la opción de red que tiene previsto utilizar. El valor predeterminado es **Wi-Fi**.
  - Wi-Fi
  - Ethernet global
  - Primera Ethernet activa
  - Segunda Ethernet activa
  - Tercera Ethernet activa
  - Primera Ethernet

  - Segunda Ethernet
  - Tercera Ethernet

- **Tipo de red:** En la lista, elija **Estándar**, **Zona interactiva heredada** o **Hotspot 2.0** para establecer el tipo de red que tiene previsto utilizar.
- **Nombre de red:** Escriba el SSID que aparece en la lista de redes disponibles para el dispositivo. No se aplica a **Hotspot 2.0**.
- **Ocultar red:** Elija si la red está oculta.
- **Unirse automáticamente a esta red inalámbrica:** Elija si la red se une automáticamente. Si un dispositivo ya está conectado a otra red, no se unirá a esta red. El usuario debe desconectar de la red anterior antes de que el dispositivo se conecte automáticamente. El valor predeterminado es **Activado**.
- **Tipo de seguridad:** En la lista, elija el tipo de seguridad que tiene previsto utilizar. No se aplica a **Hotspot 2.0**.

  - Ninguno - No requiere más configuración.
  - WEP
  - WPA/WPA2 Personal
  - Cualquiera (Personal)
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - Cualquiera (Enterprise)

  Las siguientes secciones enumeran las opciones que se configuran para cada uno de los tipos de conexión anteriores.
- **Prioridad:** Para varias redes, escriba un número para definir la prioridad de la conexión de red. El dispositivo se conecta primero a la red con el número de prioridad más bajo. Se aceptan números negativos. El valor predeterminado es **0**.
- **Configuración del servidor proxy**

  - **Configuración del proxy:** En la lista, elija **Ninguno**, **Manual** o **Automático** para establecer cómo se enruta la conexión VPN a través de un servidor proxy y, a continuación, configure las opciones adicionales. El valor predeterminado es **Ninguno**, lo que no requiere más configuración.
  - Si elige **Manual**, configure estos parámetros:

        - **Nombre de host o dirección IP:** Escriba el nombre de host o la dirección IP del servidor proxy.
        - **Puerto:** Escriba el número de puerto del servidor proxy.
        - **Nombre de usuario:** Escriba un nombre de usuario opcional para autenticarse en el servidor proxy.
        - **Contraseña:** Escriba una contraseña opcional para autenticarse en el servidor proxy.
    - Si elige **Automático**, configure estos ajustes:
        - **URL del servidor:** Escriba la URL del archivo PAC que define la configuración del proxy.
        - **Permitir conexión directa si el PAC no está disponible:** Elija si permite a los usuarios conectarse directamente al destino si el archivo PAC no está disponible. El valor predeterminado es **Activado**.

- **Configuración de Hotspot 2.0**
    - **Nombre del operador mostrado:** El nombre descriptivo difundido por el dispositivo Hotspot. Los usuarios ven este nombre en su lista de redes Wi-Fi disponibles.
    - **Nombre de dominio:** El nombre de dominio utilizado para la negociación de Hotspot 2.0.
    - **Permitir la conexión a redes de socios de itinerancia:** Si está **Activado**, los dispositivos que se desplazan fuera de su red doméstica pueden conectarse a redes de socios.
    - **Identificadores de organización (OI) del consorcio de itinerancia:** Agregue una lista de identificadores de organización a los que el dispositivo puede acceder. Un OI del consorcio de itinerancia pertenece a una organización con métodos de autenticación compartidos. Si el Hotspot que configura no está disponible, el dispositivo se conecta a un OI del consorcio de itinerancia que aparece aquí.
    - **Nombres de dominio de identificador de acceso a la red (NAI):** Configure una lista de nombres de dominio utilizados para identificar a los usuarios en una red de itinerancia. Un NAI se transmite en el formato `user@realm`.
    - **Códigos de país de móvil (MCC) y configuraciones de red móvil (MNC):** Un código de país de móvil consta de tres dígitos que identifican el país de una red. El código de red móvil consta de 2 o 3 dígitos únicos. Cuando se usan juntos, el MCC/MNC identifica de forma única a un operador de red móvil.

- **Configuración de directivas**

- **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
  - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
  - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.
- **Permitir al usuario eliminar la directiva:** Puede seleccionar cuándo los usuarios pueden eliminar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**.
- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en macOS 10.7 y versiones posteriores.

Configuración de WPA, WPA Personal, WPA 2 Personal, Cualquiera (Personal) para macOS

- **Contraseña:** Escriba una contraseña opcional. Si deja este campo en blanco, es posible que se pida a los usuarios sus contraseñas al iniciar sesión.

Configuración de WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Cualquiera (Enterprise) para macOS

- **Modo de conexión:** Si está en **Activado**, elija el modo de conexión que se utilizará cuando el usuario se una a la red. El valor predeterminado es **Desactivado**.
  - **Sistema:** Si está marcada, el dispositivo utiliza las credenciales del sistema para autenticar al usuario. El valor predeterminado está desmarcado.
  - **Ventana de inicio de sesión:** Si está marcada, el dispositivo utiliza las mismas credenciales introducidas en la ventana de inicio de sesión para autenticar al usuario. El valor predeterminado está desmarcado.

Cuando elige cualquiera de estos tipos de seguridad, la configuración de **EAP** aparece después de la configuración de **QoS**.

> **Importante:**

> Si selecciona el tipo de seguridad **WPA2 Enterprise**, debe permitir al menos un protocolo EAP.

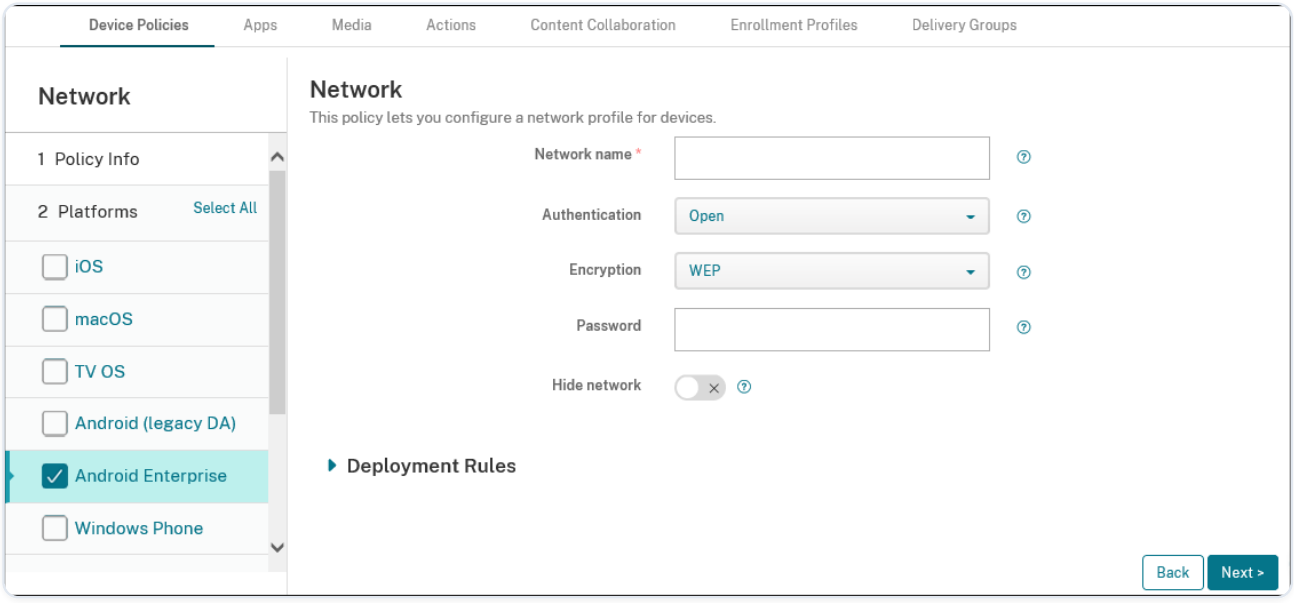
- **Protocolos EAP permitidos:** Habilite los tipos de EAP que desea admitir y, a continuación, configure los ajustes asociados. El valor predeterminado es **Desactivado** para cada uno de los tipos de EAP disponibles.
- **Autenticación interna (TTLS):** *Obligatorio solo cuando habilita TTLS*. En la lista, elija el método de autenticación interna que desea utilizar. Las opciones son: **PAP**, **CHAP**, **MSCHAP** o **MSCHAPv2**. El valor predeterminado es **MSCHAPv2**.
- **EAP-FAST con PAC:** Elija si desea utilizar credenciales de acceso protegido (PAC).
    - Si selecciona **Usar PAC**, elija si desea utilizar un PAC de aprovisionamiento.
        - Si elige **PAC de aprovisionamiento**, elija si desea permitir un protocolo de enlace TLS anónimo entre el cliente del usuario final y Citrix Endpoint Management.
            - **Aprovisionamiento de PAC de forma anónima**
- **Autenticación:**
    - **Usar autenticación de Active Directory:** Elija si quiere habilitar la autenticación de Active Directory. Disponible para macOS 10.7 y versiones posteriores. Para que esta opción esté disponible, complete lo siguiente:
        - Establezca **PEAP** como protocolo EAP.
        - Establezca el ámbito del perfil en **Sistema**. Puede usar esta opción de configuración solo cuando aplique la directiva a todo el sistema.
    - **Nombre de usuario:** Escriba un nombre de usuario.
    - **Contraseña por conexión:** Elija si quiere exigir una contraseña cada vez que los usuarios inicien sesión.
    - **Contraseña:** Escriba una contraseña opcional. Si deja este campo en blanco, es posible que se pida a los usuarios sus contraseñas cuando inicien sesión.
    - **Credencial de identidad (almacén de claves o credencial PKI):** En la lista, elija el tipo de credencial de identidad. El valor predeterminado es **Ninguno**.
    - **Identidad externa:** *Obligatorio solo si habilita* **PEAP**, **TTLS** *o* **EAP-FAST**. Escriba el nombre de usuario visible externamente. Puede aumentar la seguridad escribiendo un término genérico como "anónimo" para que el nombre de usuario no sea visible.

- **Requerir un certificado TLS:** Elija si quiere requerir un certificado TLS.

- **Confianza**
  - **Certificados de confianza:** Para agregar un certificado de confianza, haga clic en **Agregar** y, para cada certificado que quiera agregar, haga lo siguiente:
    - **Aplicación:** En la lista, elija la aplicación que quiere agregar.
    - Haga clic en **Guardar** para guardar el certificado o haga clic en **Cancelar**.
  - **Nombres de certificados de servidor de confianza:** Para agregar nombres comunes de certificados de servidor de confianza, haga clic en **Agregar** y, para cada nombre que desee agregar, haga lo siguiente:
    - **Certificado:** Escriba el nombre del certificado de servidor que desea agregar. Puede usar caracteres comodín para especificar el nombre, como wpa.*.example.com.
    - Haga clic en **Guardar** para guardar el nombre del certificado o haga clic en **Cancelar**.

- **Permitir excepciones de confianza:** Elija si el cuadro de diálogo de confianza del certificado aparece en los dispositivos de usuario cuando un certificado no es de confianza. El valor predeterminado es **Activado**.

Configuración de Android Enterprise



- **Nombre de red:** Escriba el SSID que se encuentra en la lista de redes disponibles en el dispositivo del usuario.
- **Autenticación:** En la lista, elija el tipo de seguridad que se utilizará con la conexión Wi-Fi.
  - Abierta

- Compartida
- WPA
- WPA-PSK
- WPA2
- WPA2-PSK
- 802.1x EAP

Las siguientes secciones enumeran las opciones que se configuran para cada uno de los tipos de conexión anteriores. El valor predeterminado es **Abrir**.

Abrir, Configuración compartida para Android Enterprise

- **Cifrado:** En la lista, elija **Deshabilitado** o **WEP**. El valor predeterminado es **WEP**.
- **Contraseña:** Escriba una contraseña opcional.
- **Ocultar red:** Elija si la red está oculta.

Configuración de WPA, WPA-PSK, WPA2, WPA2-PSK para Android Enterprise

- **Cifrado:** En la lista, elija **TKIP** o **AES**. El valor predeterminado es **TKIP**.
- **Contraseña:** Escriba una contraseña opcional.
- **Ocultar red:** Elija si la red está oculta.

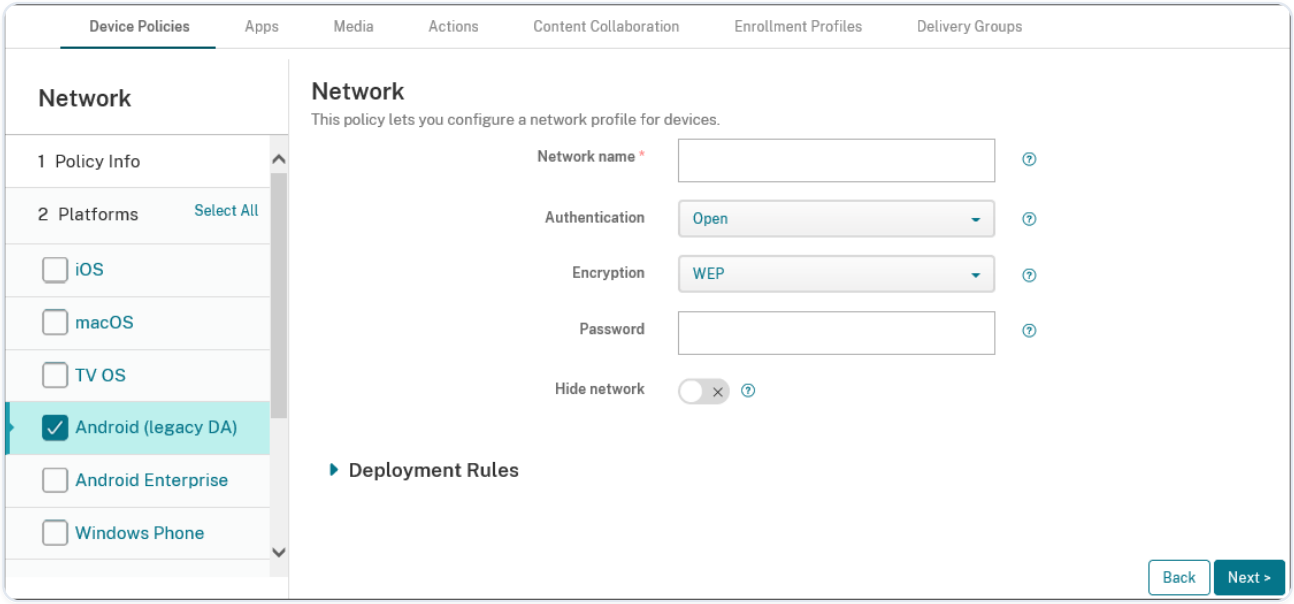
Configuración 802.1x para Android Enterprise

- **Tipo de EAP:** En la lista, elija **PEAP**, **TLS** o **TTLS**. El valor predeterminado es **PEAP**.
- **Contraseña:** Escriba una contraseña opcional.
- **Fase de autenticación 2:** En la lista, elija **Ninguno**, **PAP**, **MSCHAP**, **MSCHAPPv2** o **GTC**. El valor predeterminado es **PAP**.
- **Identidad:** Escriba el nombre de usuario y el dominio opcionales.
- **Anónimo:** Escriba el nombre de usuario opcional y visible externamente. Puede aumentar la seguridad escribiendo un término genérico como «anónimo» para que el nombre de usuario no sea visible.
- **Certificado de CA:** En la lista, elija el certificado que desea usar.
- **Dominio:** Escriba el nombre de dominio requerido. Para obtener más información, consulte Dominio.

> **Nota:**
>
> Al configurar la directiva de Wi-Fi en dispositivos con Android 13 o posterior, los campos **Certificado de CA** y **Dominio** deben actualizarse obligatoriamente. Si no se actualizan, la configuración falla.

- **Credencial de identidad:** En la lista, elija la credencial de identidad que desea usar. El valor predeterminado es **Ninguno**.
- **Ocultar red:** Elija si la red está oculta.

Configuración de Android (DA heredado)



- **Nombre de red:** Escriba el SSID que se encuentra en la lista de redes disponibles en el dispositivo del usuario.
- **Autenticación:** En la lista, elija el tipo de seguridad que desea usar con la conexión Wi-Fi.
  - Abierta
  - Compartida (solo Android Enterprise)
  - WPA (solo Android Enterprise)
  - WPA-PSK (solo Android Enterprise)
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

En las siguientes secciones se enumeran las opciones que se configuran para cada uno de los tipos de conexión anteriores.

Configuración abierta y compartida para Android

- **Cifrado:** En la lista, elija **Deshabilitado** o **WEP**. El valor predeterminado es **WEP**.
- **Contraseña:** Escriba una contraseña opcional.
- **Ocultar red:** Elija si la red está oculta.

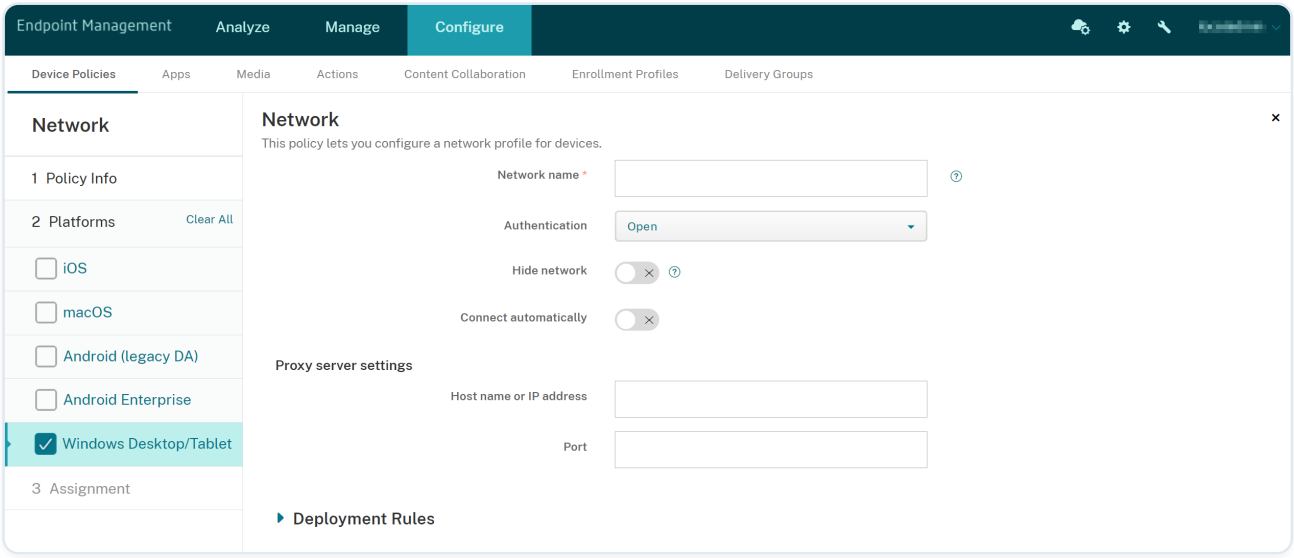
Configuración de WPA, WPA-PSK, WPA2, WPA2-PSK para Android

- **Cifrado:** En la lista, elija **TKIP** o **AES**. El valor predeterminado es **TKIP**.
- **Contraseña:** Escriba una contraseña opcional.
- **Ocultar red:** Elija si la red está oculta.

Configuración de 802.1x para Android

- **Tipo de EAP:** En la lista, elija **PEAP**, **TLS** o **TTLS**. El valor predeterminado es **PEAP**.
- **Contraseña:** Escriba una contraseña opcional.
- **Fase 2 de autenticación:** En la lista, elija **Ninguno**, **PAP**, **MSCHAP**, **MSCHAPPv2** o **GTC**. El valor predeterminado es **PAP**.
- **Identidad:** Escriba el nombre de usuario y el dominio opcionales.
- **Anónimo:** Escriba el nombre de usuario opcional y visible externamente. Puede aumentar la seguridad escribiendo un término genérico como "anónimo" para que el nombre de usuario no sea visible.
- **Certificado de CA:** En la lista, elija el certificado que desea utilizar.
- **Credencial de identidad:** En la lista, elija la credencial de identidad que desea utilizar. El valor predeterminado es **Ninguno**.
- **Ocultar red:** Elija si la red está oculta.

Configuración de Windows Desktop/Tablet



- **Nombre de red:** El SSID que se ve en la lista de redes disponibles.
- **Autenticación:** Haga clic en el tipo de seguridad de la lista desplegable que desea utilizar con la conexión Wi-Fi.
  - Abierta
  - WPA Personal
  - WPA-2 Personal
  - WPA Enterprise
  - WPA-2 Enterprise: Para la última versión de Windows 10, configure SCEP para usar WPA-2 Enterprise. La configuración de SCEP permite a Citrix Endpoint Management enviar el certificado a los dispositivos para autenticarse en el servidor Wi-Fi. Para configurar SCEP, vaya a la página **Distribución** de **Parámetros > Proveedores de credenciales**. Para obtener más información, consulte Proveedores de credenciales.

Las siguientes secciones enumeran las opciones que se configuran para cada uno de los tipos de conexión anteriores.

Abrir la configuración para Windows 10 y Windows 11

- **Ocultar red:** Elija si la red está oculta.
- **Conectar automáticamente:** Elija si desea conectarse a la red automáticamente.

Configuración de WPA Personal, WPA-2 Personal para Windows 10 y Windows 11

- **Cifrado:** En la lista, elija **AES** o **TKIP** para establecer el tipo de cifrado. El valor predeterminado es **AES**.

- **Clave compartida:** Proporcione la clave de cifrado para el método que seleccionó.
- **Ocultar red:** Elija si la red está oculta.
- **Conectar automáticamente:** Elija si desea conectarse a la red automáticamente.

Configuración de WPA-2 Enterprise para Windows 10 y Windows 11

- **Cifrado:** En la lista, elija **AES** o **TKIP** para establecer el tipo de cifrado. El valor predeterminado es **AES**.
- **Tipo de EAP:** en la lista, elija **PEAP-MSCHAPv2** o **TLS** para establecer el tipo de EAP. El valor predeterminado es **PEAP-MSCHAPv2**.
- **Ocultar red:** Elija si la red está oculta.
- **Conectar automáticamente:** Elija si desea conectarse a la red automáticamente.
- **¿Habilitar SCEP?:** Elija si desea enviar el certificado a los dispositivos de usuario mediante SCEP.
- **Proveedor de credenciales para SCEP:** En la lista, elija el proveedor de credenciales de SCEP. El valor predeterminado es **Ninguno**.

Directiva de dispositivo de uso de red

Puede establecer reglas de uso de red para especificar cómo los dispositivos iOS utilizan las redes, como las redes de datos móviles. Las reglas se aplican a las aplicaciones administradas y a las SIM especificadas. Las aplicaciones administradas son aplicaciones que implementa en los dispositivos de los usuarios a través de Citrix Endpoint Management. No incluyen las aplicaciones que los usuarios han descargado directamente en sus dispositivos si no se implementan a través de Citrix Endpoint Management. Tampoco incluyen las aplicaciones ya instaladas en los dispositivos cuando estos se inscribieron en Citrix Endpoint Management. Esta directiva se aplica a las SIM de los dispositivos iOS 13. Puede configurar reglas de aplicación, reglas de SIM o ambas. Las reglas de SIM se aplican a todas las aplicaciones administradas de ese dispositivo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

- **Reglas de aplicación**

- **Permitir datos móviles en itinerancia:** Seleccione si las aplicaciones especificadas pueden usar una conexión de datos móviles mientras están en itinerancia. El valor predeterminado es **Desactivado**.
- **Permitir datos móviles:** Seleccione si las aplicaciones especificadas pueden usar una conexión de datos móviles. El valor predeterminado es **Desactivado**.
- **Coincidencias de identificador de aplicación:** Para cada aplicación que quiera agregar a la lista, haga clic en **Agregar** y, a continuación, configure lo siguiente:
  - **Identificador de aplicación:** Escriba un identificador de aplicación.
- Haga clic en **Guardar** para guardar la aplicación en la lista o en **Cancelar** para no guardar la aplicación en la lista.

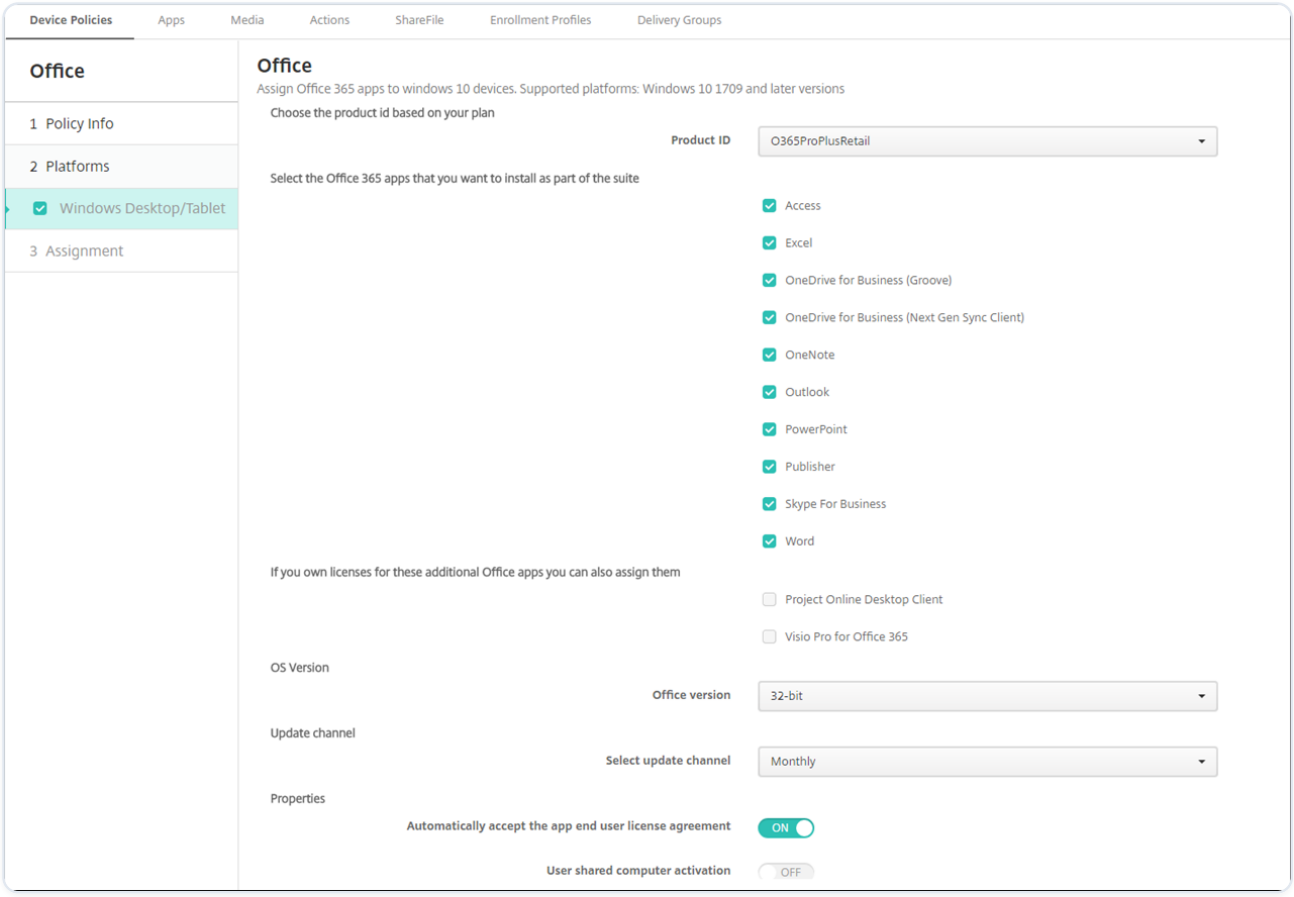
- **Reglas de SIM**
  - **Directiva de asistencia de Wi-Fi de SIM:** Al habilitar **Cambiar de Wi-Fi deficiente**, la directiva de asistencia de Wi-Fi cambia de Wi-Fi deficiente a conexiones móviles de forma más agresiva. Esta configuración puede aumentar el uso de datos móviles y afectar la duración de la batería.
  - **ICCID de SIM:** Para cada SIM que quiera agregar a la lista, haga clic en **Agregar** y, a continuación, configure lo siguiente:
    - **ICCID:** Escriba el número de 19 o 20 dígitos de la tarjeta SIM que quiere agregar.

Directiva de dispositivo de Office

Citrix Endpoint Management le permite implementar productos de Microsoft Office 365 mediante el proveedor de servicios de configuración (CSP) de Office. Al configurar la directiva de dispositivo de Office, puede implementar aplicaciones de Microsoft Office en cualquier dispositivo que ejecute Windows 10 (versión 1709 o posterior) o Windows 11.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de escritorio/tableta de Windows



- **ID de producto:** Seleccione un ID de producto según su plan de Office 365. Las opciones son **O365ProPlusRetail, O365BusinessRetail** o **O365SmallBusPremRetail**.
- **Aplicaciones de Office 365:** Seleccione las aplicaciones de Office 365 que desea implementar. Todas las aplicaciones están seleccionadas de forma predeterminada.
- **Aplicaciones de Office adicionales:** Si posee licencias para **Project Online Desktop Client** o **Visio Pro para Office 365**, puede seleccionar estas aplicaciones para instalarlas.
- **Versión de Office:** Seleccione si desea instalar la versión de Office de **32 bits** o de **64 bits**.
- **Canal de actualización:** Elija la frecuencia con la que desea que se realicen las actualizaciones. Las opciones son **Mensual**, **Mensual (dirigido)**, **Semestral** o **Semestral (dirigido)**.
- **Propiedades:**
  - **Aceptar automáticamente el contrato de licencia de usuario final de la aplicación:** Seleccione **Activado** o **Desactivado**. El valor predeterminado es **Activado**.
  - **Activación de equipo compartido por el usuario:** Seleccione si el equipo es compartido o no. Las opciones son **Activado** o **Desactivado**. El valor predeterminado es **Desactivado**.

- **Idioma de Office:** Office se instala automáticamente en cualquier idioma que Windows ya tenga instalado. Puede seleccionar idiomas adicionales para instalar.

Directiva de dispositivo de información de la organización

La directiva de dispositivo de información de la organización especifica la información de su organización para los mensajes de alerta que se envían desde Citrix Endpoint Management a los dispositivos iOS.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

- **Nombre:** Escriba el nombre de la organización que ejecuta Citrix Endpoint Management.
- **Dirección:** Escriba la dirección de la organización.
- **Teléfono:** Escriba el número de teléfono de soporte de la organización.
- **Correo electrónico:** Escriba la dirección de correo electrónico de soporte.
- **Mágico:** Escriba una palabra o frase que describa los servicios gestionados por la organización.

Directiva de dispositivo de actualización del SO

La directiva de dispositivo de actualización del SO le permite implementar:

- Las últimas actualizaciones del SO en dispositivos iOS supervisados.

  La directiva de dispositivo de actualización del SO solo funciona para dispositivos supervisados inscritos en el Programa de implementación de Apple.
- Las últimas actualizaciones del SO y de las aplicaciones en dispositivos macOS inscritos en el Programa de implementación de Apple que ejecutan macOS 10.11.5 y versiones posteriores.

> **Nota:**
>
> Actualmente, Apple limita las actualizaciones del SO solo a las versiones principales. Los administradores no pueden actualizar versiones secundarias. Para obtener más información, consulte este artículo en la documentación de Apple.

- Las últimas actualizaciones del SO en dispositivos de escritorio y tabletas supervisados que ejecutan Windows 10 o Windows 11.

  También puede usar la directiva de actualización del SO para administrar la configuración de optimización de entrega para equipos de escritorio y tabletas que ejecutan Windows 10 (versión 1607 o posterior) o Windows 11. La optimización de entrega es un servicio de actualización de cliente punto a punto proporcionado por Microsoft para las actualizaciones de Windows 10 y Windows 11. El objetivo de la optimización de entrega es reducir los problemas de ancho de banda durante el proceso de actualización. La reducción del ancho de banda se logra compartiendo la tarea de descarga entre varios dispositivos. Para obtener más información, consulte el artículo de Microsoft, Configurar la optimización de entrega para las actualizaciones de Windows 10.

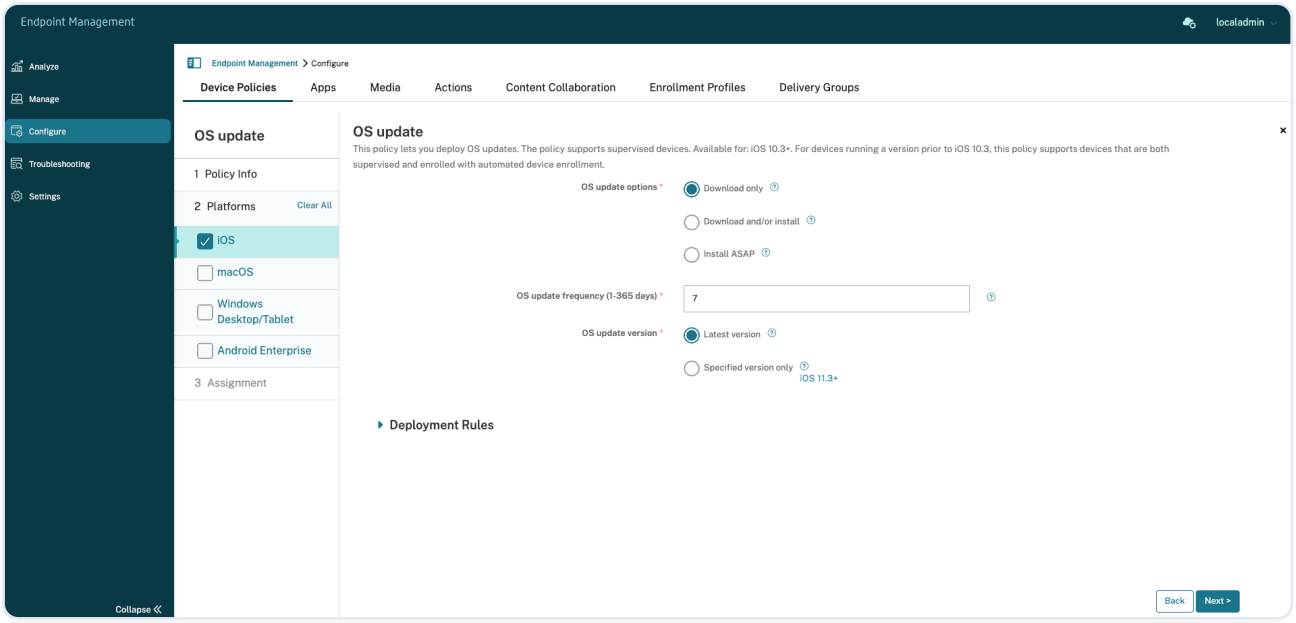
- Las últimas actualizaciones del SO en dispositivos Android Enterprise administrados (Android 7.0 y versiones posteriores).

Importante:

La directiva de actualización del SO no permite deshabilitar las actualizaciones por completo. Para retrasar las actualizaciones hasta 90 días, cree una directiva de restricción. Consulte (/es-es/citrix-endpoint-management/policies/restrictions-policy.html).

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte (/es-es/citrix-endpoint-management/policies.html).

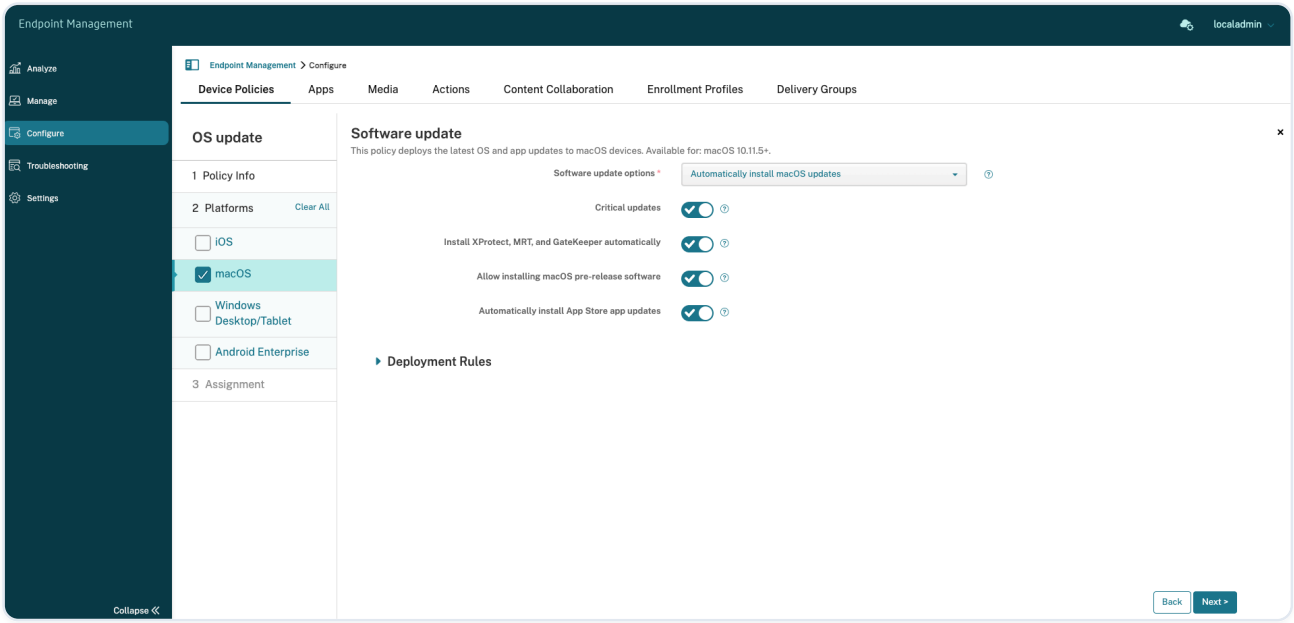
Configuración de iOS



Las siguientes configuraciones son para dispositivos iOS supervisados.

- **Opciones de actualización del SO:** Ambas opciones descargan las últimas actualizaciones del SO en los dispositivos supervisados según la **frecuencia de actualización del SO**. El dispositivo solicita a los usuarios que instalen las actualizaciones. La solicitud es visible después de que el usuario desbloquea el dispositivo.
- **Frecuencia de actualización del SO:** Determina la frecuencia con la que Citrix Endpoint Management comprueba y actualiza el SO del dispositivo. El valor predeterminado es **7** días.
- **Versión de las actualizaciones del SO:** Especifica la versión que se utilizará para actualizar los dispositivos iOS supervisados. El valor predeterminado es **Última versión**.
    - **Última versión:** Seleccione para actualizar a la última versión del SO.
    - **Solo versión específica:** Seleccione para actualizar a una versión específica del SO y, a continuación, escriba el número de versión.

Configuración de macOS



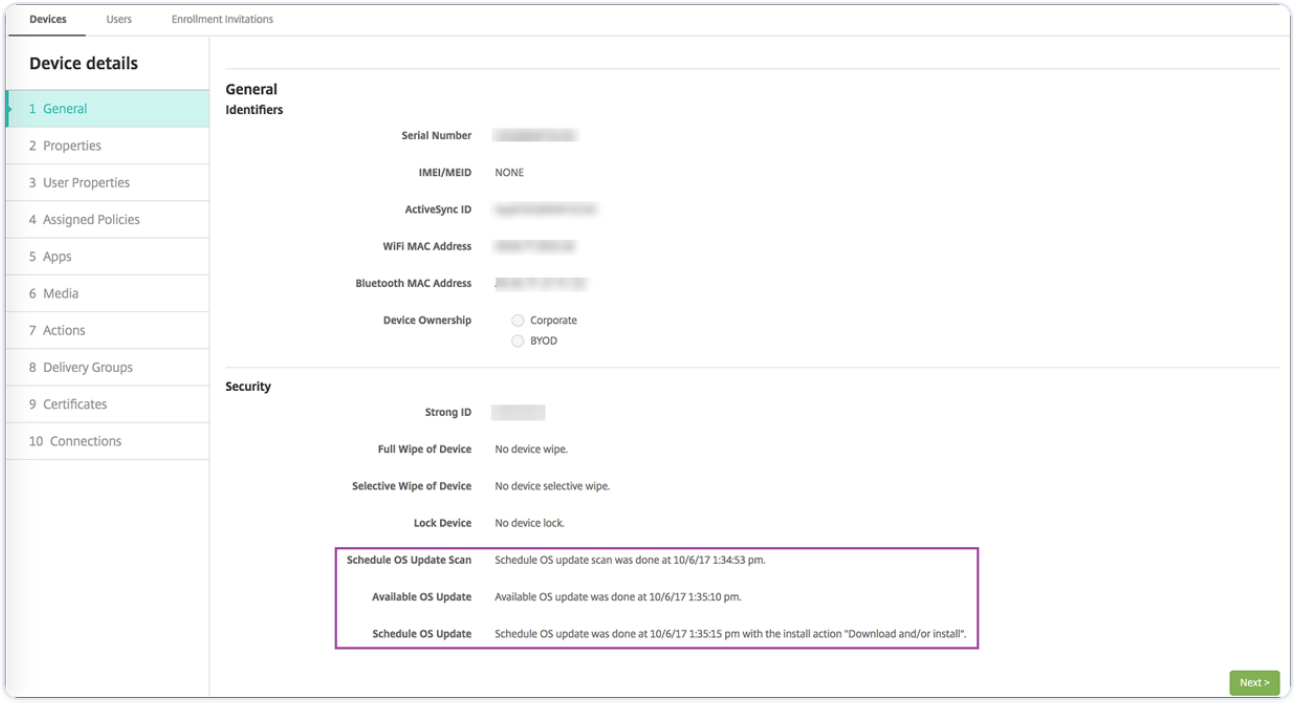
- **Opciones de actualizaciones de software:** Controla cómo los dispositivos macOS comprueban e instalan las actualizaciones. Seleccione entre las siguientes opciones:
  - **Instalar automáticamente las actualizaciones de macOS:** Las actualizaciones se descargan e instalan automáticamente.
  - **Descargar nuevas actualizaciones cuando estén disponibles:** Las actualizaciones se descargan, pero requieren instalación manual.
  - **Buscar actualizaciones:** Comprueba si existen actualizaciones, pero no las descarga ni las instala automáticamente.
  - **No buscar actualizaciones:** No buscar nuevas actualizaciones, ni descargarlas ni instalarlas automáticamente. Los usuarios pueden seguir instalando las actualizaciones manualmente.
- **Actualizaciones críticas:** Permite la instalación automática de actualizaciones críticas de macOS.
- **Instalar automáticamente las actualizaciones de xProtect, MRT y GateKeeper:** Permite que los dispositivos macOS instalen automáticamente las actualizaciones del software de seguridad.
- **Permitir la instalación de software preliminar de macOS:** Permitir a los usuarios instalar versiones preliminares del software de macOS.
- **Instalar automáticamente las actualizaciones de aplicaciones de App Store:** Permitir que las aplicaciones de App Store se actualicen automáticamente.

Obtener el estado de las acciones de actualización de iOS y macOS

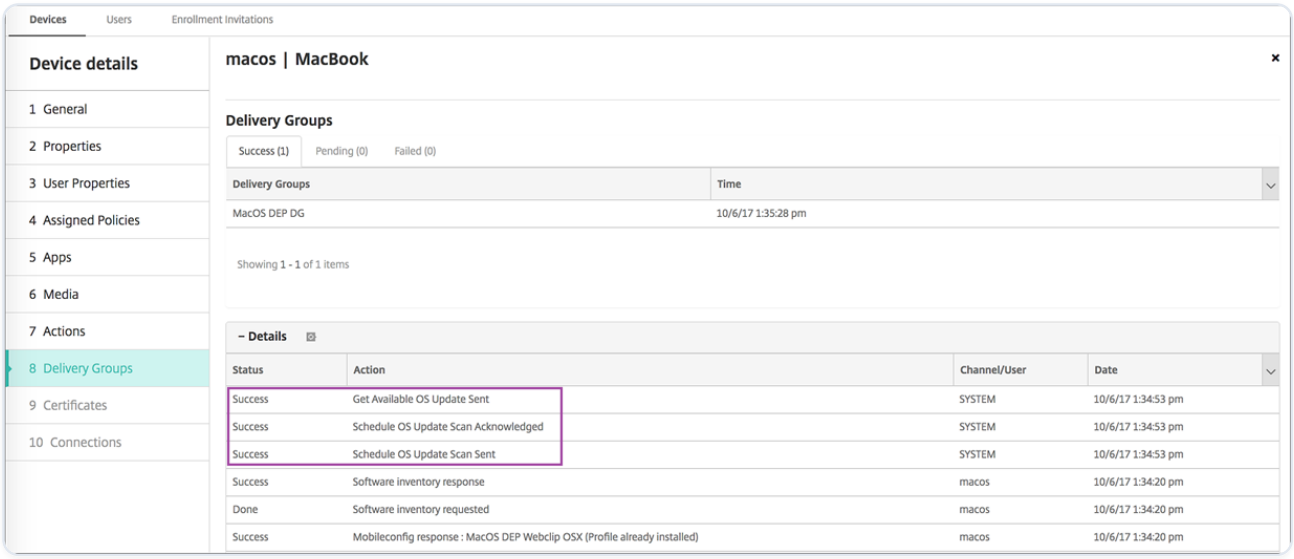
Para iOS y macOS, Citrix Endpoint Management no implementa la directiva Control OS Update en los dispositivos. En su lugar, Citrix Endpoint Management utiliza la directiva para enviar estos comandos MDM a los dispositivos:

- Programar análisis de actualizaciones del SO: Solicita que el dispositivo realice un análisis en segundo plano en busca de actualizaciones del SO. (Opcional para iOS)
- Actualizaciones del SO disponibles: Consulta el dispositivo para obtener una lista de las actualizaciones del SO disponibles.
- Programar actualización del SO: Solicita que el dispositivo realice actualizaciones de macOS, actualizaciones de aplicaciones o ambas. Por lo tanto, el SO del dispositivo determina cuándo descarga o instala las actualizaciones del SO y de las aplicaciones.

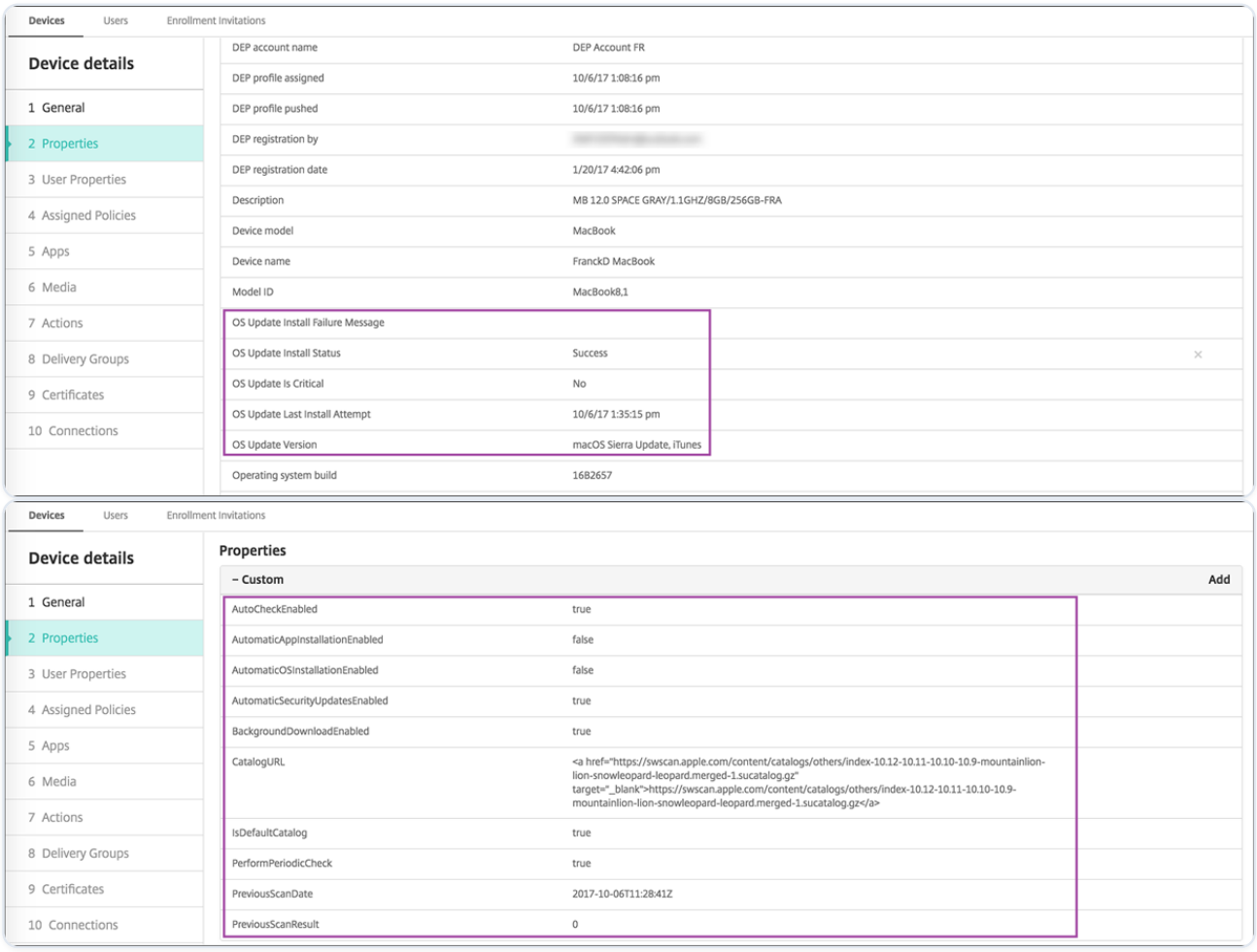
La página **Administrar > Dispositivos > Detalles del dispositivo (General)** muestra el estado de los análisis de actualizaciones del SO programados y disponibles, y las actualizaciones programadas de macOS y aplicaciones.



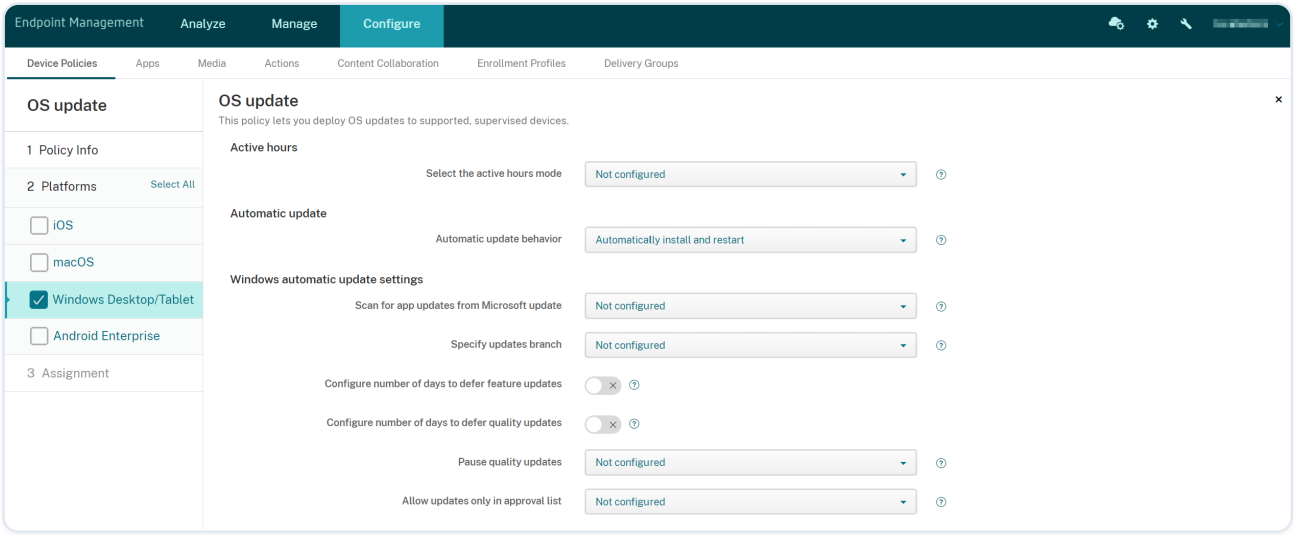
Para obtener más detalles sobre el estado de las acciones de actualización, vaya a la página **Administrar > Dispositivos > Detalles del dispositivo (Grupos de entrega)**.



Para obtener detalles como las actualizaciones del SO disponibles y el último intento de instalación, vaya a la página **Administrar > Dispositivos > Detalles del dispositivo (Propiedades)**.



Configuración de Windows Desktop y Tablet



- **Seleccionar modo de horas activas:** Seleccione un modo para configurar las horas activas para realizar actualizaciones del sistema operativo. Puede especificar un rango de horas o una hora de inicio y fin. Después de seleccionar un modo, aparecen más configuraciones: **Especificar rango máximo de horas activas** o **Inicio de horas activas** y **Fin de horas activas**. **No configurado** permite que Windows realice actualizaciones del sistema operativo en cualquier momento. El valor predeterminado es **No configurado**.
- **Comportamiento de actualización automática:** Configura el comportamiento de descarga, instalación y reinicio del servicio de actualización de Windows en los dispositivos de usuario. El valor predeterminado es **Instalación y reinicio automáticos**.
    - **Notificar al usuario antes de descargar la actualización:** Windows notifica a los usuarios cuando hay actualizaciones disponibles. Windows no descarga ni instala actualizaciones automáticamente. Los usuarios deben iniciar las acciones de descarga e instalación.
    - **Instalación automática y notificación para programar el reinicio del dispositivo:** Windows descarga actualizaciones automáticamente en redes no medidas. Windows instala actualizaciones durante el Mantenimiento automático cuando el dispositivo no está en uso y no funciona con batería. Si el Mantenimiento automático no puede instalar actualizaciones durante dos días, Windows Update instala las actualizaciones inmediatamente. Si la instalación requiere un reinicio, Windows solicita al usuario que programe la hora de reinicio. El usuario tiene hasta siete días para programar el reinicio. Después de siete días, Windows fuerza el reinicio del dispositivo. Permitir que el usuario controle la hora de inicio reduce el riesgo de pérdida accidental de datos causada por aplicaciones que no se cierran correctamente al reiniciar.

  - **Instalación y reinicio automáticos:** Configuración predeterminada. Windows descarga actualizaciones automáticamente en redes no medidas. Windows instala actualizaciones durante el Mantenimiento automático cuando el dispositivo no está en uso y no funciona con batería. Si el Mantenimiento automático no puede instalar actualizaciones durante dos días, Windows Update instala las actualizaciones inmediatamente. Si la instalación requiere un reinicio, Windows reinicia automáticamente el dispositivo cuando este está inactivo.
  - **Instalación y reinicio automáticos a una hora especificada:** Al elegir esta opción, aparecen más configuraciones para que pueda especificar el día y la hora. El valor predeterminado es las 3:00 AM diariamente. La instalación automática se realiza a la hora especificada y el reinicio del dispositivo ocurre después de una cuenta atrás de 15 minutos. Cuando Windows está listo para reiniciar, un usuario que haya iniciado sesión puede interrumpir la cuenta atrás de 15 minutos para retrasar el reinicio.
  - **Instalación y reinicio automáticos sin control del usuario final:** Windows descarga actualizaciones automáticamente en redes no medidas. Windows instala actualizaciones durante el Mantenimiento automático cuando el dispositivo no está en uso y no funciona con batería. Si el Mantenimiento automático no puede instalar actualizaciones durante dos días, Windows Update instala las actualizaciones inmediatamente. Si la instalación requiere un reinicio, Windows reinicia automáticamente el dispositivo cuando este está inactivo. Esta opción también establece el panel de control del usuario en solo lectura.
  - **Desactivar actualizaciones automáticas:** Deshabilita las actualizaciones automáticas de Windows en el dispositivo.

- **Buscar actualizaciones de aplicaciones de Microsoft Update:** Especifica si Windows acepta actualizaciones para otras aplicaciones de Microsoft del servicio de actualización de Microsoft. El valor predeterminado es **No configurado**.

  - **No configurado:** Utilice esta configuración si no desea configurar el comportamiento. Windows no cambia la interfaz de usuario relacionada en los dispositivos de usuario. Los usuarios pueden aceptar o rechazar actualizaciones para otras aplicaciones de Microsoft.
  - **Sí:** Windows permite que las actualizaciones de aplicaciones se instalen desde el servicio de actualización de Windows. La configuración relacionada en el dispositivo del usuario está inactiva, por lo que el usuario no puede modificarla.
  - **No:** Windows no permite que las actualizaciones de aplicaciones se instalen desde el servicio de actualización de Windows. La configuración relacionada en el dispositivo del usuario está inactiva, por lo que el usuario no puede modificarla.

- **Especificar rama de actualizaciones:** Especifica qué rama del servicio de actualización de Windows usar para las actualizaciones. El valor predeterminado es **No configurado**.
    - **No configurado:** Utilice esta configuración si no desea configurar el comportamiento. Windows no cambia la interfaz de usuario relacionada en los dispositivos de usuario. Los usuarios pueden elegir una rama del servicio de actualización de Windows.
    - **Current Branch:** Windows recibe actualizaciones de Current Branch. La configuración relacionada en el dispositivo del usuario está inactiva, por lo que el usuario no puede modificarla.
    - **Current Branch for Business:** Windows recibe actualizaciones de Current Branch for Business. La configuración relacionada en el dispositivo del usuario está inactiva, por lo que el usuario no puede modificarla.
- **Configurar el número de días para aplazar las actualizaciones de características:** Si está **Activado**, Windows aplaza las actualizaciones de características el número de días especificado y el usuario no puede cambiar la configuración. Si está **Desactivado**, el usuario puede cambiar el número de días para aplazar las actualizaciones de características. El valor predeterminado es **Desactivado**.
- **Configurar el número de días para aplazar las actualizaciones de calidad:** Si está **Activado**, Windows aplaza las actualizaciones de calidad el número de días especificado y el usuario no puede cambiar la configuración. Si está **Desactivado**, el usuario puede cambiar el número de días para aplazar las actualizaciones de calidad. El valor predeterminado es **Desactivado**.
- **Pausar actualizaciones de calidad:** Especifica si se deben pausar las actualizaciones de calidad durante 35 días. El valor predeterminado es **No configurado**.
    - **No configurado:** Utilice esta configuración si no desea configurar el comportamiento. Windows no cambia la interfaz de usuario relacionada en los dispositivos de los usuarios. Los usuarios pueden optar por pausar las actualizaciones de calidad durante 35 días.
    - **Sí:** Windows pausa la instalación de actualizaciones de calidad del Servicio de Windows Update durante 35 días. La configuración relacionada en el dispositivo del usuario está inactiva, por lo que el usuario no puede modificarla.
    - **No:** Windows no pausa la instalación de actualizaciones de calidad del Servicio de Windows Update. La configuración relacionada en el dispositivo del usuario está inactiva, por lo que el usuario no puede modificarla.

- **Permitir actualizaciones solo de la lista de aprobación:** Especifica si se deben instalar solo las actualizaciones que aprueba un servidor MDM. Citrix Endpoint Management no admite la configuración de una lista de actualizaciones aprobadas. El valor predeterminado es **No configurado**.
    - **No configurado:** Utilice esta configuración si no desea configurar el comportamiento. Windows no cambia la interfaz de usuario relacionada en los dispositivos de los usuarios. Los usuarios pueden elegir qué actualizaciones permitir.
    - **Sí, instalar solo actualizaciones aprobadas:** Permite la instalación solo de actualizaciones aprobadas.
    - **No, instalar todas las actualizaciones aplicables:** Permite la instalación de cualquier actualización aplicable en el dispositivo.
- **Usar servidor de actualizaciones interno:** Especifica si se deben obtener actualizaciones del servicio de Windows Update o de un servidor de actualizaciones interno a través de Windows Server Update Services (WSUS). Si está **Desactivado**, los dispositivos utilizan el servicio de Windows Update. Si está **Activado**, los dispositivos se conectan al servidor WSUS especificado para las actualizaciones. El valor predeterminado es **Desactivado**.
    - **Aceptar actualizaciones firmadas por entidades distintas de Microsoft:** Especifica si se deben aceptar actualizaciones firmadas por entidades de terceros distintas de Microsoft. Esta función requiere que el dispositivo confíe en el certificado del proveedor de terceros. El valor predeterminado es **Desactivado**.
    - **Permitir conexión al servicio de actualizaciones de Microsoft:** Permite que Windows Update en el dispositivo se conecte periódicamente al servicio de actualizaciones de Microsoft, incluso si el dispositivo está configurado para obtener actualizaciones de un servidor WSUS. El valor predeterminado es **Activado**.
    - **Servidor WSUS:** Especifique la URL del servidor WSUS.
    - **Servidor de intranet alternativo para alojar actualizaciones:** Especifique una URL de servidor de intranet alternativa para alojar actualizaciones y recibir información de informes.
- **Configurar la optimización de la entrega:** Si se debe usar la optimización de la entrega para las actualizaciones de Windows 10 y Windows 11. El valor predeterminado es **Desactivado**.
- **Tamaño de la caché:** El tamaño máximo de la caché de optimización de la entrega. Un valor de **0** significa una caché ilimitada. El valor predeterminado es **10** GB.

- **Permitir el almacenamiento en caché entre pares de VPN:** Si se permite que los dispositivos participen en el almacenamiento en caché entre pares cuando están conectados a la red de dominio a través de VPN. Cuando está **Activado**, el dispositivo puede descargar o cargar desde otros dispositivos de la red de dominio, ya sea en VPN o en la red de dominio corporativa. El valor predeterminado es **Desactivado**.
- **Método de descarga:** El método de descarga que la optimización de la entrega puede usar para las descargas de actualizaciones de Windows, aplicaciones y actualizaciones de aplicaciones. El valor predeterminado es **HTTP combinado con intercambio de pares detrás de la misma NAT**. Las opciones son:
  - **Solo HTTP, sin intercambio de pares:** Deshabilita el almacenamiento en caché de igual a igual, pero permite que la optimización de la entrega descargue contenido de los servidores de Windows Update o de los servidores de Windows Server Update Services (WSUS).
  - **HTTP combinado con intercambio de pares detrás de la misma NAT:** Habilita el uso compartido entre pares en la misma red. El servicio en la nube de optimización de la entrega encuentra otros clientes que se conectan a Internet utilizando la misma IP pública que el cliente de destino. Estos clientes intentan conectarse a otros pares en la misma red utilizando su IP de subred privada.
  - **HTTP combinado con intercambio de pares en un grupo privado:** Selecciona automáticamente un grupo en función del sitio de Active Directory Domain Services (AD DS) del dispositivo o del dominio al que se autentica el dispositivo. El intercambio de pares se produce en subredes internas, entre dispositivos que pertenecen al mismo grupo, incluidos los dispositivos en oficinas remotas.
  - **HTTP combinado con intercambio de pares de Internet:** Habilita las fuentes de pares de Internet para la optimización de la entrega.
  - **Modo de descarga simple sin intercambio de pares:** Deshabilita el uso de los servicios en la nube de optimización de la entrega. La optimización de la entrega cambia a este modo automáticamente en estas condiciones: cuando los servicios en la nube de optimización de la entrega no están disponibles, no son accesibles o cuando el tamaño del archivo de contenido es inferior a 10 MB. En este modo, la optimización de la entrega proporciona una experiencia de descarga fiable, sin almacenamiento en caché de igual a igual.
  - **No usar la optimización de la entrega y usar BITS en su lugar:** Permite a los clientes usar BranchCache. Para obtener más información, consulte el artículo de Microsoft, BranchCache.

- **Ancho de banda máximo de descarga:** El ancho de banda máximo de descarga en KB/segundo. El valor predeterminado es **0**, lo que significa ajuste dinámico del ancho de banda.
- **Porcentaje del ancho de banda máximo de descarga:** El ancho de banda máximo de descarga que la optimización de la entrega puede usar en todas las actividades de descarga simultáneas. El valor es un porcentaje del ancho de banda de descarga disponible. El valor predeterminado es **0**, lo que significa ajuste dinámico.
- **Ancho de banda máximo de carga:** El ancho de banda máximo de carga en KB/segundo. El valor predeterminado es **0**. Un valor de **0** significa ancho de banda ilimitado.
- **Límite de datos de carga mensual:** El tamaño máximo en GB que la optimización de entrega puede cargar a pares de Internet en cada mes natural. El valor predeterminado es 20 GB. Un valor de **0** significa cargas mensuales ilimitadas.

Cómo Citrix Endpoint Management gestiona las actualizaciones aprobadas para dispositivos Windows de escritorio y tabletas

Puede especificar si desea instalar solo las actualizaciones aprobadas. Citrix Endpoint Management gestiona las actualizaciones de la siguiente manera:

- Para una actualización de seguridad, como las definiciones de Windows Defender, Citrix Endpoint Management aprueba automáticamente la actualización y envía un comando de instalación al dispositivo durante la siguiente sincronización.
- Para todos los demás tipos de actualización, Citrix Endpoint Management espera su aprobación antes de enviar el comando de instalación al dispositivo.

Requisitos previos

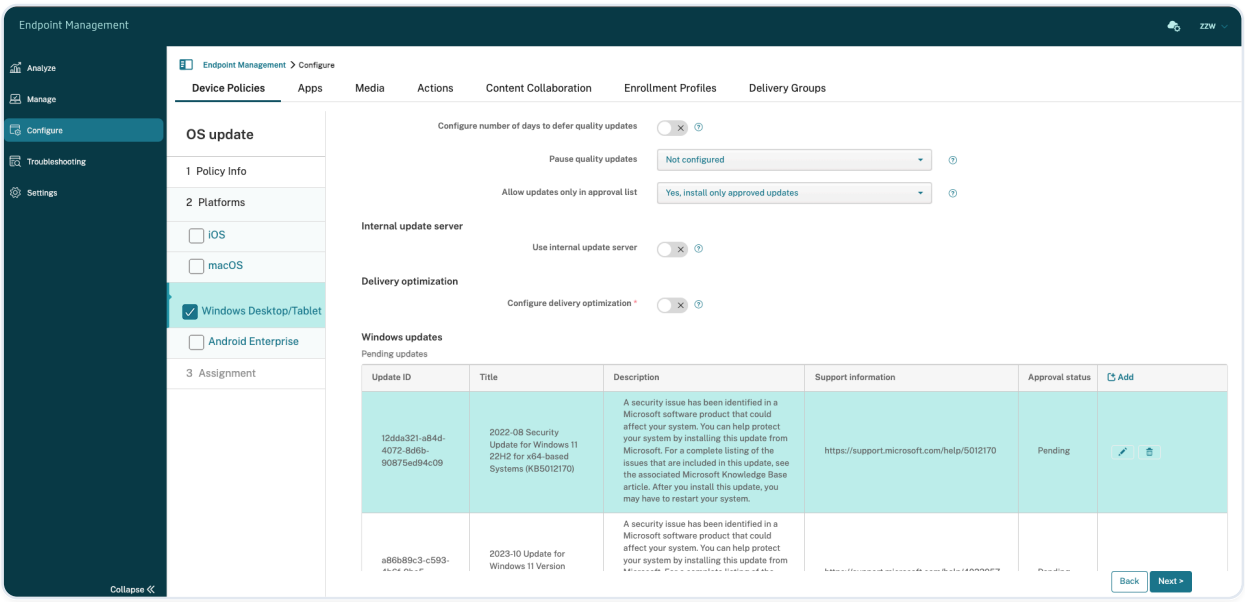
- Debe cargar el certificado raíz de Microsoft en el servidor de Citrix Endpoint Management como certificado de servidor.
- Para obtener información sobre cómo importar un certificado de servidor, consulte "Para importar un certificado" en Certificados y autenticación.

Para instalar solo las actualizaciones aprobadas

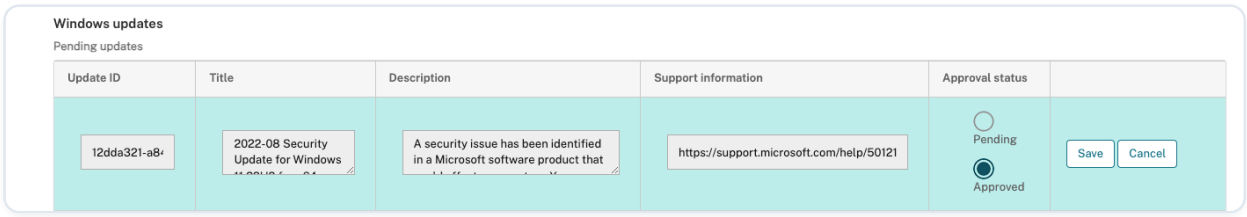
1. Vaya a **Configurar > Directivas de dispositivo** y abra la directiva de dispositivo Actualización del SO.
2. Cambie la configuración **Permitir actualizaciones solo en la lista de aprobación** a **Sí, instalar solo actualizaciones aprobadas**.

Para aprobar una actualización

1. En la directiva de dispositivo Actualización del SO, desplácese hasta la tabla **Actualizaciones pendientes**. Citrix Endpoint Management obtiene las actualizaciones que aparecen en la tabla de los dispositivos.
2. Busque actualizaciones con un **Estado de aprobación** de **Pendiente**.
3. Haga clic en la fila de la actualización que desea aprobar y, a continuación, haga clic en el icono de edición de esa fila (en la columna **Agregar**).



4. Para aprobar la actualización, haga clic en **Aprobado** y, a continuación, en **Guardar**.



Nota:

Aunque la tabla de actualizaciones pendientes incluye comandos para agregar y eliminar, esos comandos no producen ningún cambio en la base de datos de Citrix Endpoint Management. La edición del estado de aprobación es la única acción disponible para las actualizaciones pendientes.

Para ver el estado de las actualizaciones de Windows de un dispositivo, vaya a **Administrar > Dispositivos > Propiedades**.



Cuando se publica una actualización, el **ID de actualización** aparece en la primera columna con un estado (Correcto o Error). Puede crear un informe o una acción automatizada para los dispositivos con actualizaciones fallidas. También aparece la fecha y la hora de la publicación.

Cómo funcionan las actualizaciones para las implementaciones iniciales y posteriores

El efecto de la directiva de dispositivo de actualización del SO en los dispositivos difiere entre una implementación inicial y una implementación después de que los dispositivos reciban actualizaciones.

- Para que Citrix Endpoint Management consulte un dispositivo en busca de actualizaciones, debe configurar y asignar a un grupo de entrega al menos una directiva de dispositivo de actualización del SO.

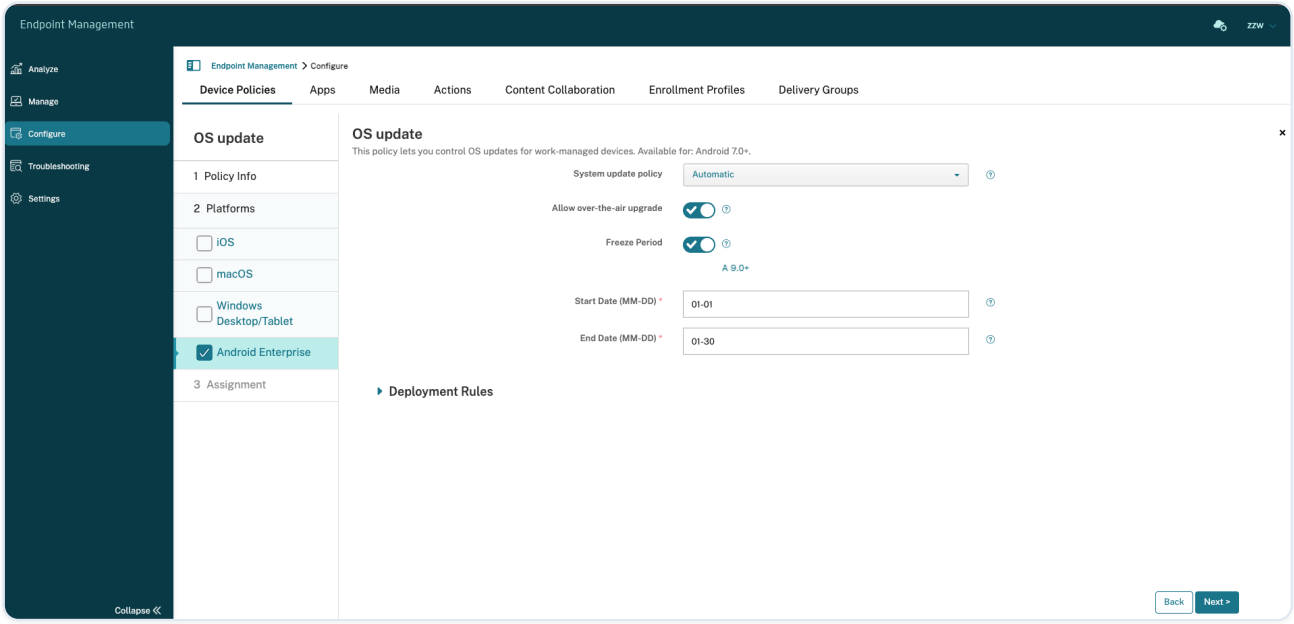
  Citrix Endpoint Management consulta un dispositivo en busca de actualizaciones instalables durante una sincronización MDM del dispositivo.
- Después de la primera implementación de la directiva de dispositivo de actualización del SO, la lista de actualizaciones de Windows está vacía porque ningún dispositivo ha informado todavía.
- Cuando los dispositivos del grupo de entrega asignado informan de las actualizaciones, Citrix Endpoint Management guarda esas actualizaciones en su base de datos. Para aprobar las actualizaciones notificadas, edite la directiva de nuevo.

  La aprobación de la actualización se aplica solo a la directiva que está editando. Las actualizaciones aprobadas en una directiva no aparecen como aprobadas en otra directiva. La próxima vez que un dispositivo se sincronice, Citrix Endpoint Management enviará un comando al dispositivo para indicar que la actualización está aprobada.
- Para una segunda política de dispositivo de actualización del SO, la lista de actualizaciones contiene las actualizaciones almacenadas en la base de datos de Citrix Endpoint Management. Apruebe las actualizaciones para cada política.

  Durante cada sincronización de dispositivos, Citrix Endpoint Management consulta el dispositivo para conocer el estado de actualización aprobado hasta que el dispositivo informa de que se ha instalado una actualización. Para las actualizaciones que requieren un reinicio después de la instalación, Citrix Endpoint Management consulta el estado de la actualización hasta que el dispositivo informa de que la actualización se ha instalado.

- Citrix Endpoint Management no restringe las actualizaciones que se muestran en la página de configuración de la política por grupo de entrega o dispositivo. Todas las actualizaciones notificadas por los dispositivos aparecen en la lista.

Configuración de Android Enterprise



- **Política de actualización del sistema:** Determina cuándo se producen las actualizaciones del sistema.
  - **Automático:** Instala una actualización cuando está disponible.
  - **Con ventana:** Instala una actualización automáticamente dentro de la ventana de mantenimiento diaria especificada en **Hora de inicio** y **Hora de finalización**.
    - **Hora de inicio:** El inicio de la ventana de mantenimiento, medido como el número de minutos (**0** - **1440**) desde la medianoche en la hora local del dispositivo. El valor predeterminado es **0**.
    - **Hora de finalización:** El final de la ventana de mantenimiento, medido como el número de minutos (**0** - **1440**) desde la medianoche en la hora local del dispositivo. El valor predeterminado es **120**.
  - **Posponer:** Permite al usuario posponer una actualización hasta 30 días.
  - **Predeterminado:** Establece la política de actualización en la predeterminada del sistema.
- **Permitir actualización inalámbrica:** Si está deshabilitado, los dispositivos de usuario no pueden recibir actualizaciones de software de forma inalámbrica. El valor predeterminado es **Activado**.

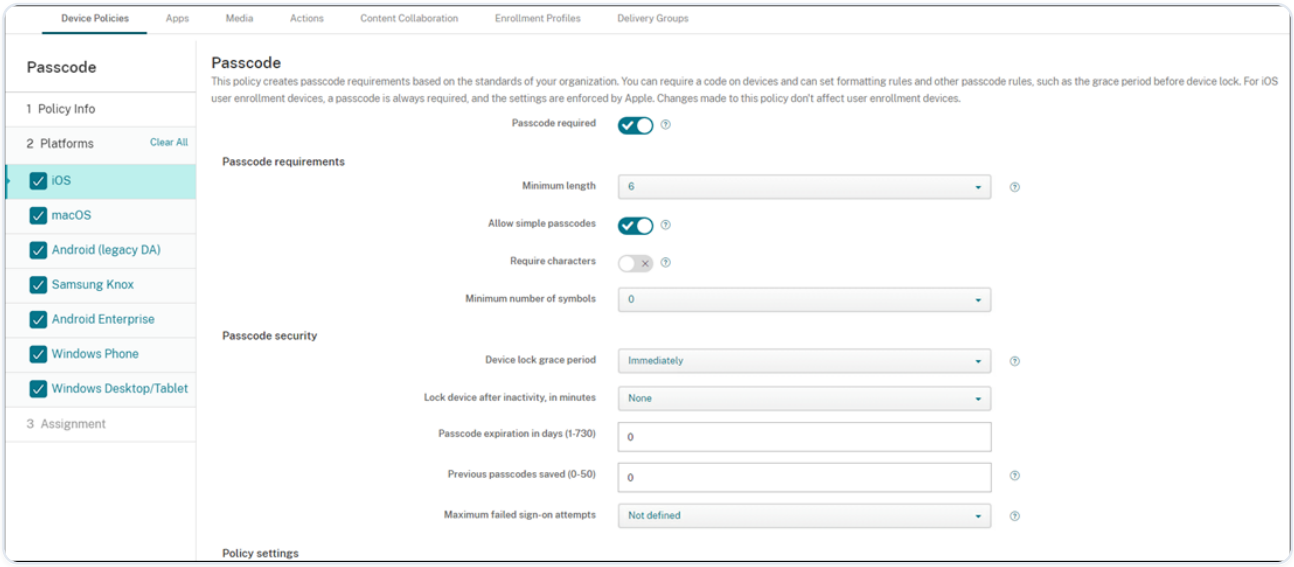
- **Período de congelación:** Si está **Activado**, las actualizaciones del SO no se instalan en el dispositivo durante el rango de fechas especificado para las políticas de actualización **Automático**, **Posponer** y **Con ventana**. Solo se puede establecer un período de congelación por dispositivo a la vez. La duración del período de congelación no puede exceder los 90 días.
    - **Fecha de inicio/Fecha de finalización:** El rango de fechas en el que no se instalan las actualizaciones del SO si el **Período de congelación** está habilitado.
- **Período de congelación:** Si está **Activado**, no se instalan actualizaciones del SO en el dispositivo durante el intervalo de fechas especificado para las políticas de actualización **Automática**, **Aplazar** y **Ventana**. Solo se puede establecer un período de congelación para un dispositivo a la vez. La duración del período de congelación no puede exceder los 90 días.
    - **Fecha de inicio/Fecha de fin:** El intervalo de fechas en el que no se instalan actualizaciones del SO si el **Período de congelación** está activado.

Directiva de código de acceso del dispositivo

Cree una directiva de código de acceso en Citrix Endpoint Management según los estándares de su organización. Puede exigir códigos de acceso en los dispositivos de los usuarios y establecer varias reglas de formato y código de acceso. Cree directivas para iOS, macOS, Android, Android Enterprise y equipos de escritorio/tabletas con Windows. Cada plataforma requiere un conjunto diferente de valores, que se describen en este artículo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivos**. Para obtener más información, consulte Directivas de dispositivos.

Configuración de iOS



- **Código de acceso obligatorio:** Seleccione esta opción para exigir un código de acceso y para mostrar las opciones de configuración de una directiva de dispositivo con código de acceso de iOS. La página se expande para permitirle configurar los ajustes de los requisitos del código de acceso, la seguridad del código de acceso y la configuración de la directiva.
- **Requisitos del código de acceso**
  - **Longitud mínima:** Haga clic en la longitud mínima del código de acceso en la lista desplegable. El valor predeterminado es **6**.
  - **Permitir códigos de acceso simples:** Seleccione si desea permitir códigos de acceso simples. Los códigos de acceso simples son un conjunto de caracteres repetidos o secuenciales. El valor predeterminado es **Activado**.
  - **Caracteres obligatorios:** Seleccione si desea que los códigos de acceso tengan al menos una letra. El valor predeterminado es **Desactivado**.
  - **Número mínimo de símbolos:** En la lista, haga clic en el número de símbolos que debe tener el código de acceso. El valor predeterminado es **0**.
- **Seguridad del código de acceso**
  - **Período de gracia de bloqueo del dispositivo:** En la lista, haga clic en el período de tiempo antes de que los usuarios deban introducir un código de acceso para desbloquear un dispositivo bloqueado. El valor predeterminado es **Inmediatamente**.
  - **Bloquear dispositivo después de la inactividad:** En el cuadro, introduzca el período de tiempo que un dispositivo puede estar inactivo antes de que se bloquee. El valor puede estar entre 1 y 15 minutos. Establezca el valor en **Ninguno** para deshabilitar la directiva. El valor predeterminado es **Ninguno**.
  - **Caducidad del código de acceso en días (1-730):** Escriba el número de días después de los cuales caduca el código de acceso. Los valores válidos son 1–730. El valor predeterminado es **0**, lo que significa que el código de acceso nunca caduca.
  - **Contraseñas anteriores guardadas (0-50):** Escriba el número de contraseñas usadas que se deben guardar. Los usuarios no pueden usar ninguna contraseña que se encuentre en esta lista. Los valores válidos son 0-50. El valor predeterminado es **0**, lo que significa que los usuarios pueden reutilizar contraseñas.
  - **Intentos máximos de inicio de sesión fallidos:** En la lista, haga clic en el número de veces que un usuario puede fallar al iniciar sesión.
    - Si establece este número en más de 6, después del sexto intento, el dispositivo impone un retardo de tiempo entre los intentos. El retardo de tiempo aumenta con cada intento

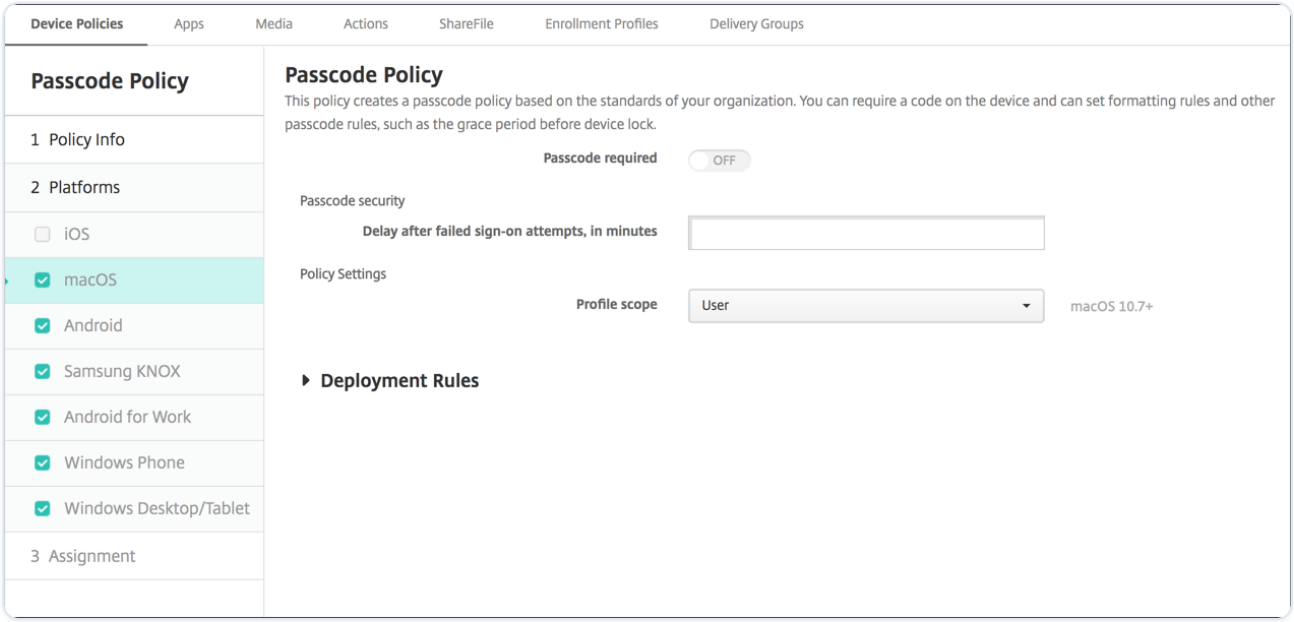
fallido. Después del último intento, todos los datos y la configuración se borran de forma segura.

- Si establece el número en 6 o menos, el dispositivo se borra sin implementar un retardo de tiempo.
- Si selecciona **No definido**, después de 6 intentos, el dispositivo impone un límite de tiempo creciente entre los intentos, pero no se borra.

El valor predeterminado es **No definido**.

- **Configuración de la directiva**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva. Solo disponible para iOS 6.0 y versiones posteriores.

Configuración de macOS



- **Se requiere código de acceso:** Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una directiva de dispositivo de código de acceso de iOS. La página se expande para permitirle configurar los ajustes de los requisitos del código de acceso, la seguridad del código de acceso y la configuración de la directiva.

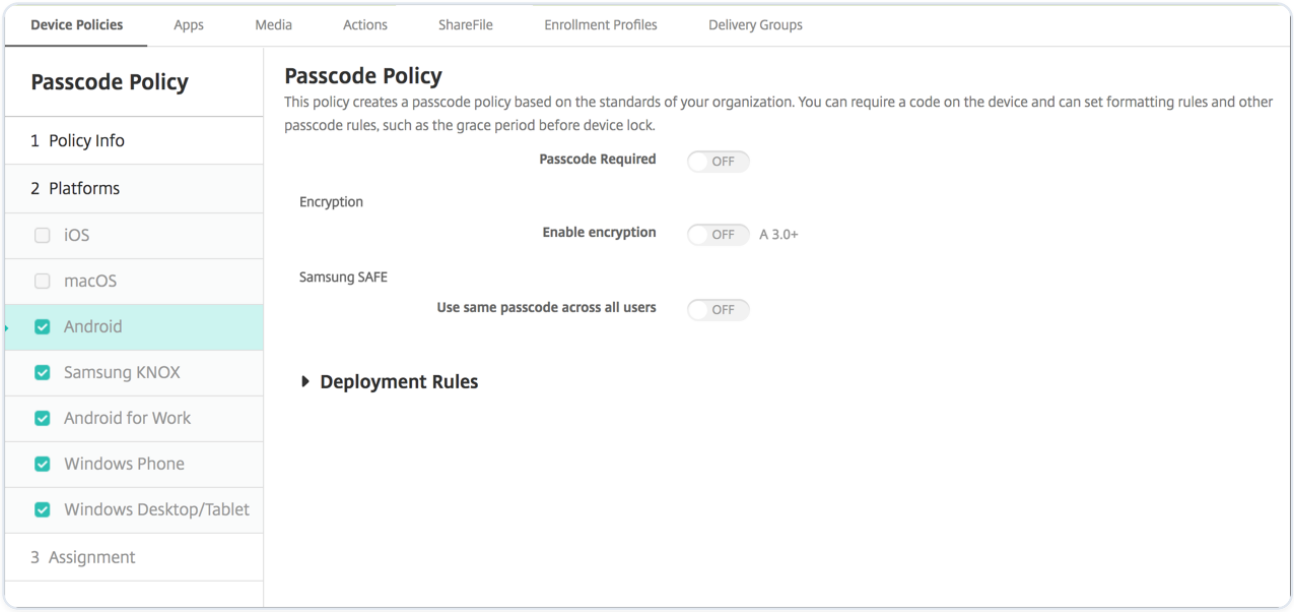
- Si **Se requiere código de acceso** está deshabilitado, junto a **Retraso después de intentos de inicio de sesión fallidos, en minutos**, escriba el número de minutos de retraso antes de permitir a los usuarios volver a introducir sus códigos de acceso.
- Si habilita **Se requiere código de acceso**, configure los siguientes ajustes:
- **Requisitos de código de acceso**
    - **Longitud mínima:** Haga clic en la longitud mínima del código de acceso en la lista desplegable. El valor predeterminado es **6**.
    - **Permitir códigos de acceso simples:** Seleccione si desea permitir códigos de acceso simples. Los códigos de acceso simples son un conjunto de caracteres repetidos o secuenciales. El valor predeterminado es **Activado**.
    - **Caracteres obligatorios:** Seleccione si desea que los códigos de acceso tengan al menos una letra. El valor predeterminado es **Desactivado**.
    - **Número mínimo de símbolos:** En la lista, haga clic en el número de símbolos que debe tener el código de acceso. El valor predeterminado es **0**.
- **Seguridad del código de acceso**
    - **Período de gracia de bloqueo del dispositivo:** En la lista, haga clic en el período de tiempo antes de que los usuarios deban introducir un código de acceso para desbloquear un dispositivo bloqueado. El valor predeterminado es **Ninguno**.
    - **Bloquear dispositivo después de inactividad:** En la lista, haga clic en el período de tiempo que un dispositivo puede estar inactivo antes de que se bloquee. El valor puede estar entre 1 y 5 minutos. Establezca el valor en **Ninguno** para deshabilitar la directiva. El valor predeterminado es **Ninguno**.
    - **Caducidad del código de acceso en días (1-730):** Escriba el número de días después de los cuales caduca el código de acceso. Los valores válidos son 1–730. El valor predeterminado es **0**, lo que significa que el código de acceso nunca caduca.
    - **Contraseñas anteriores guardadas (0-50):** Escriba el número de contraseñas usadas que se deben guardar. Los usuarios no pueden usar ninguna contraseña que se encuentre en esta lista. Los valores válidos son 0–50. El valor predeterminado es **0**, lo que significa que los usuarios pueden reutilizar contraseñas.
    - **Número máximo de intentos de inicio de sesión fallidos:** En la lista, haga clic en el número de veces que un usuario puede fallar al iniciar sesión.

    - Si establece este número en más de 6, después del sexto intento, el dispositivo impone un retardo de tiempo entre los intentos. El retardo de tiempo aumenta con cada intento fallido. Después del último intento, el dispositivo se bloquea.
    - Si establece el número en 6 o menos, el dispositivo se bloquea sin implementar un retardo de tiempo.
    - Si selecciona **No definido**, después de 6 intentos, el dispositivo impone un límite de tiempo creciente entre los intentos, pero no se bloquea.

  El valor predeterminado es **No definido**.
- **Retraso después de intentos de inicio de sesión fallidos, en minutos:** Escriba el número de minutos antes de que aparezca la ventana de inicio de sesión después de que un usuario alcance el número máximo de intentos fallidos.
- **Forzar restablecimiento de código de acceso:** Si está en **Desactivado**, los usuarios no necesitan restablecer su código de acceso la próxima vez que se autentiquen después de que su dispositivo reciba esta directiva. El valor predeterminado es **Activado**.

- **Configuración de directivas**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.
  - **Permitir al usuario eliminar la directiva:** Puede seleccionar cuándo los usuarios pueden eliminar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en macOS 10.7 y versiones posteriores.

Configuración de Android (DA heredado)



> **Nota:**
>
> La configuración predeterminada para Android es **Desactivado**.

- **Se requiere código de acceso:** Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una directiva de dispositivo de código de acceso de Android. La página se expande para permitirle configurar los ajustes de requisitos de código de acceso, seguridad de código de acceso y cifrado.
- **Requisitos de código de acceso**
  - **Longitud mínima:** Haga clic en la longitud mínima del código de acceso en la lista desplegable. El valor predeterminado es 6.
  - **Reconocimiento biométrico:** Seleccione si desea habilitar el reconocimiento biométrico. Si habilita esta opción, el campo Caracteres obligatorios se oculta. El valor predeterminado es **Desactivado**.
  - **Caracteres obligatorios:** En la lista, haga clic en **Sin restricciones**, **Números y letras**, **Solo números** o **Solo letras** para configurar cómo se componen los códigos de acceso. El valor predeterminado es **Sin restricciones**.
  - **Reglas avanzadas:** Seleccione si desea aplicar reglas avanzadas para códigos de acceso. El valor predeterminado es **Desactivado**.

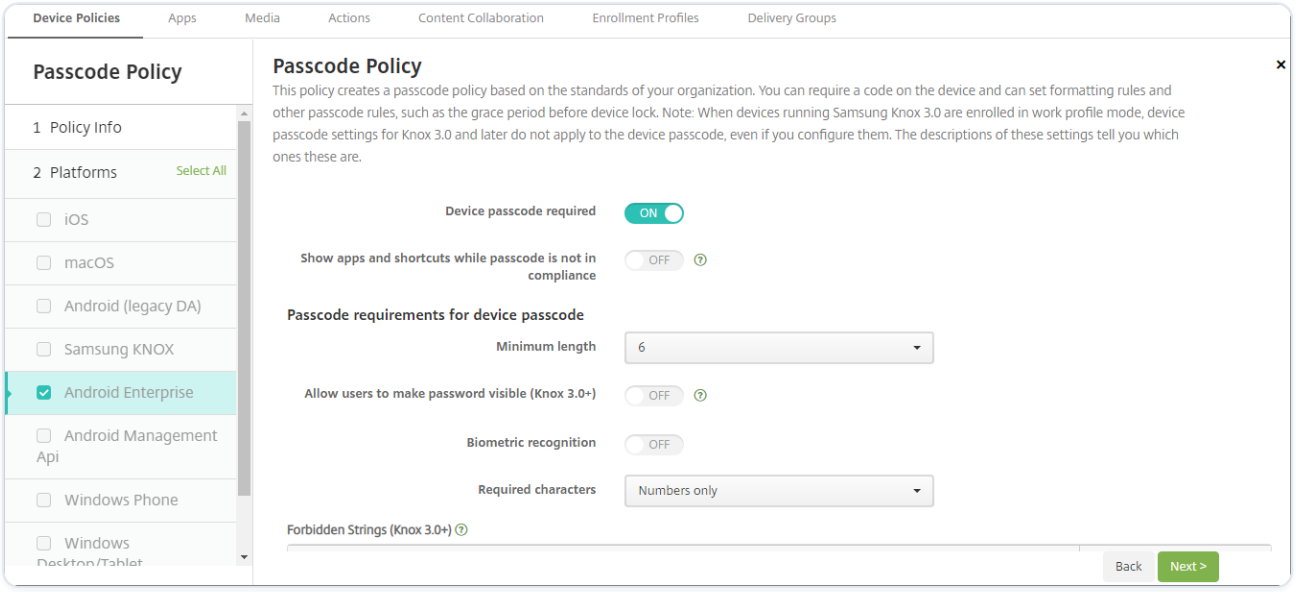
- Cuando habilite las **Reglas avanzadas**, en cada una de las siguientes listas, haga clic en el número mínimo de cada tipo de carácter que debe tener un código de acceso:
  - **Símbolos:** El número mínimo de símbolos.
  - **Letras:** El número mínimo de letras.
  - **Letras minúsculas:** El número mínimo de letras minúsculas.
  - **Letras mayúsculas:** El número mínimo de letras mayúsculas.
  - **Números o símbolos:** El número mínimo de números o símbolos.
  - **Números:** El número mínimo de números.

- **Seguridad del código de acceso**
  - **Bloquear dispositivo tras inactividad:** En la lista, haga clic en el período de tiempo que un dispositivo puede estar inactivo antes de que se bloquee. El valor predeterminado es **Ninguno**
  - **Caducidad del código de acceso en días (1-730):** Escriba el número de días después de los cuales caduca el código de acceso. Los valores válidos son 1–730. El valor predeterminado es **0**, lo que significa que el código de acceso nunca caduca.
  - **Contraseñas anteriores guardadas (0-50):** Escriba el número de contraseñas usadas que se deben guardar. Los usuarios no pueden usar ninguna contraseña que se encuentre en esta lista. Los valores válidos son 0–50. El valor predeterminado es **0**, lo que significa que los usuarios pueden reutilizar las contraseñas.
  - **Número máximo de intentos de inicio de sesión fallidos:** En la lista, haga clic en el número de veces que un usuario puede fallar al iniciar sesión correctamente antes de que se borre el dispositivo. El valor predeterminado es **No definido**.

- **Cifrado**
  - **Habilitar cifrado:** Seleccione si desea habilitar el cifrado. La opción está disponible independientemente de la configuración de **Contraseña obligatoria**.

    Para cifrar sus dispositivos, los usuarios deben empezar con la batería cargada y mantener el dispositivo enchufado hasta que se complete el cifrado. El proceso puede tardar una hora o más. Si interrumpen el proceso de cifrado, pueden perder parte o la totalidad de los datos de sus dispositivos. Una vez cifrado un dispositivo, el proceso no se puede revertir, excepto realizando un restablecimiento de fábrica, lo que borra todos los datos del dispositivo.

Configuración de Android Enterprise



Para los dispositivos Android Enterprise, puede exigir una contraseña para el dispositivo o un desafío de seguridad para el perfil de trabajo de Android Enterprise, o ambos.

- **Contraseña del dispositivo obligatoria:** Requiere una contraseña en el dispositivo. Cuando esta opción está **Activada**, configure los ajustes en **Requisitos de contraseña para la contraseña del dispositivo** y **Seguridad de contraseña para la contraseña del dispositivo**. El valor predeterminado es **Desactivado**.
- **Mostrar aplicaciones y accesos directos cuando la contraseña no cumple los requisitos:** Cuando esta opción está **Activada**, las aplicaciones y los accesos directos del dispositivo no se ocultan, incluso cuando la contraseña no cumple los requisitos. Cuando esta opción está **Desactivada**, las aplicaciones y los accesos directos se ocultan cuando la contraseña no cumple los requisitos. Si habilita esta opción, Citrix® recomienda crear una acción automatizada para marcar el dispositivo como no conforme cuando la contraseña no cumpla los requisitos. El valor predeterminado es **Desactivado**.
- **Requisitos de contraseña para la contraseña del dispositivo:**
  - **Longitud mínima:** Especifica la longitud mínima de la contraseña. El valor predeterminado es 6.
  - **Reconocimiento biométrico:** Habilita el reconocimiento biométrico. Si esta opción está **Activada**, el campo **Caracteres obligatorios** está oculto. El valor predeterminado es **Desactivado**.
  - **Caracteres obligatorios:** Especifica los tipos de caracteres obligatorios para las contraseñas. En la lista, elija **Sin restricciones**, **Números y letras**, **Solo números** o **Solo letras**. Utilice **Sin restricciones** solo para dispositivos con Android 7.0. Android 7.1 y

versiones posteriores no respetan la configuración de **Sin restricciones**. El valor predeterminado es **Números y letras**.

- **Reglas avanzadas:** Aplica reglas avanzadas para los tipos de caracteres que pueden aparecer en las contraseñas. Cuando esta opción está **Activada**, configure los ajustes en **Número mínimo de** y **Número máximo de**. Esta opción no está disponible para dispositivos Android anteriores a Android 5.0. El valor predeterminado es **Desactivado**.
- **Número mínimo de:**
  - **Símbolos:** Especifica el número mínimo de símbolos. El valor predeterminado es **0**.
  - **Letras:** Especifica el número mínimo de letras. El valor predeterminado es **0**.
  - **Letras minúsculas:** Especifica el número mínimo de letras minúsculas. El valor predeterminado es **0**.
  - **Letras mayúsculas:** Especifica el número mínimo de letras mayúsculas. El valor predeterminado es **0**.
  - **Números o símbolos:** Especifica el número mínimo de números o símbolos. El valor predeterminado es **0**.
  - **Números:** Especifica el número mínimo de números. El valor predeterminado es **0**.
  - **Caracteres cambiados:** Para dispositivos con Samsung Knox 3.0 o posterior que tengan una clave de licencia de Knox válida configurada. Solo para dispositivos totalmente administrados. Esta configuración no se aplica a los dispositivos inscritos como dispositivos de perfil de trabajo. Especifica el número de caracteres que los usuarios deben cambiar de su código de acceso anterior. El valor predeterminado es **0**.
- **Número máximo de:** Para dispositivos con Samsung Knox 3.0 o posterior que tengan una clave de licencia de Knox válida configurada. Solo para dispositivos totalmente administrados. Esta configuración no se aplica a los dispositivos inscritos como dispositivos de perfil de trabajo.
  - **Veces que un carácter puede aparecer:** Especifica el número máximo de veces que un carácter puede aparecer en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.
  - **Longitud de secuencia alfabética:** Especifica la longitud máxima de una secuencia alfabética en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.

    - **Longitud de secuencia numérica:** Especifica la longitud máxima de una secuencia numérica en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.

- **Complejidad del código de acceso para el código de acceso del dispositivo (Android 12+):**

    - **Aplicar complejidad del código de acceso:** Requiere una contraseña con un nivel de complejidad definido por la plataforma, en lugar de un requisito de contraseña personalizado. Solo para dispositivos con Android 12+ y que utilicen Citrix Secure Hub 22.9 o posterior.
    - **Nivel de complejidad:** Niveles predefinidos de complejidad de la contraseña.
        - **Ninguno:** No se requiere contraseña.
        - **Bajo:** Las contraseñas pueden ser:
            - Un patrón
            - Un PIN con un mínimo de cuatro números
        - **Media:** Las contraseñas pueden ser:
            - Un PIN sin secuencias repetidas (4444) ni secuencias ordenadas (1234), y un mínimo de cuatro números
            - Alfabética con un mínimo de cuatro caracteres
            - Alfanumérica con un mínimo de cuatro caracteres
        - **Alta:** Las contraseñas pueden ser:
            - Un PIN sin secuencias repetidas (4444) ni secuencias ordenadas (1234), y un mínimo de ocho números
            - Alfabética con un mínimo de seis caracteres
            - Alfanumérica con un mínimo de seis caracteres

> **Nota:**
>
> Para los dispositivos BYOD, la configuración del código de acceso, como la longitud mínima, los caracteres obligatorios, el reconocimiento biométrico y las reglas avanzadas, no se aplica en Android 12+. En su lugar, utilice la complejidad del código de acceso.

- **Seguridad del código de acceso para el código de acceso del dispositivo:**
  - **Borrar el dispositivo después de (intentos de inicio de sesión fallidos):** Especifica el número de veces que un usuario puede fallar al iniciar sesión, después de lo cual el dispositivo se borra por completo. El valor predeterminado es **No definido**.
  - **Bloquear el dispositivo después de la inactividad:** Especifica el número de minutos que un dispositivo puede estar inactivo antes de que se bloquee. Establezca el valor en 0 para deshabilitar la directiva.
  - **Caducidad del código de acceso en días (1-730):** Especifica el número de días tras los cuales caduca el código de acceso. Los valores válidos son 1–730. El valor predeterminado es **0**, lo que significa que el código de acceso nunca caduca.
  - **Contraseñas anteriores guardadas (0-50):** Especifica el número de contraseñas usadas que se deben guardar. Los usuarios no pueden usar ninguna contraseña que se encuentre en esta lista. Los valores válidos son 0–50. El valor predeterminado es **0**, lo que significa que los usuarios pueden reutilizar contraseñas.
- **Desafío de seguridad del perfil de trabajo:** Requiere que los usuarios completen un desafío de seguridad para acceder a las aplicaciones que se ejecutan en un perfil de trabajo de Android Enterprise. Para dispositivos con Android 7.0 y versiones posteriores. Cuando esta opción está **Activada**, configure los ajustes en **Requisitos de código de acceso para el desafío de seguridad del perfil de trabajo** y **Seguridad de código de acceso para el desafío de seguridad del perfil de trabajo**. El valor predeterminado es **Desactivado**.
- **Requisitos de código de acceso para el desafío de seguridad del perfil de trabajo:**
  - **Longitud mínima:** Especifica la longitud mínima del código de acceso. El valor predeterminado es 6.
  - **Reconocimiento biométrico:** Habilita el reconocimiento biométrico. Si esta opción está **Activada**, el campo **Caracteres obligatorios** se oculta. El valor predeterminado es **Desactivado**.
  - **Caracteres obligatorios:** Especifica los tipos de caracteres obligatorios para los códigos de acceso. En la lista, elija **Sin restricciones**, **Números y letras**, **Solo números** o **Solo letras**. Use **Sin restricciones** solo para dispositivos con Android 7.0. Android 7.1 y versiones posteriores no respetan la configuración **Sin restricciones**. El valor predeterminado es **Números y letras**.
  - **Reglas avanzadas:** Aplica reglas avanzadas para los tipos de caracteres que pueden aparecer en los códigos de acceso. Cuando esta opción está **Activada**, configure los ajustes en **Número mínimo de** y **Número máximo de**. Esta configuración no está

disponible para dispositivos Android anteriores a Android 5.0. El valor predeterminado es **Desactivado**.

- **Número mínimo de:**
  - **Símbolos:** Especifica el número mínimo de símbolos. El valor predeterminado es **0**.
  - **Letras:** Especifica el número mínimo de letras. El valor predeterminado es **0**.
  - **Letras minúsculas:** Especifica el número mínimo de letras minúsculas. El valor predeterminado es **0**.
  - **Letras mayúsculas:** Especifica el número mínimo de letras mayúsculas. El valor predeterminado es **0**.
  - **Números o símbolos:** Especifica el número mínimo de números o símbolos. El valor predeterminado es **0**.
  - **Números:** Especifica el número mínimo de números. El valor predeterminado es **0**.
  - **Caracteres modificados:** Para dispositivos con Knox 3.0 o posterior que tienen una clave de licencia de Knox válida configurada. Especifica el número de caracteres que los usuarios deben cambiar de su código de acceso anterior. El valor predeterminado es **0**.
- **Número máximo de:** Para dispositivos con Knox 3.0 o posterior que tienen una clave de licencia de Knox válida configurada.
  - **Veces que un carácter puede aparecer:** Especifica el número máximo de veces que un carácter puede aparecer en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.
  - **Longitud de secuencia alfabética:** Especifica la longitud máxima de una secuencia alfabética en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.
  - **Longitud de secuencia numérica:** Especifica la longitud máxima de una secuencia numérica en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.

- **Complejidad del código de acceso para el desafío de seguridad del perfil de trabajo (Android 12+):**
  - **Aplicar complejidad del código de acceso:** Requiere una contraseña con un nivel de complejidad definido por la plataforma, en lugar de un requisito de contraseña

personalizado. Solo para dispositivos con Android 12+ y que utilizan Citrix Secure Hub 22.9 o posterior.

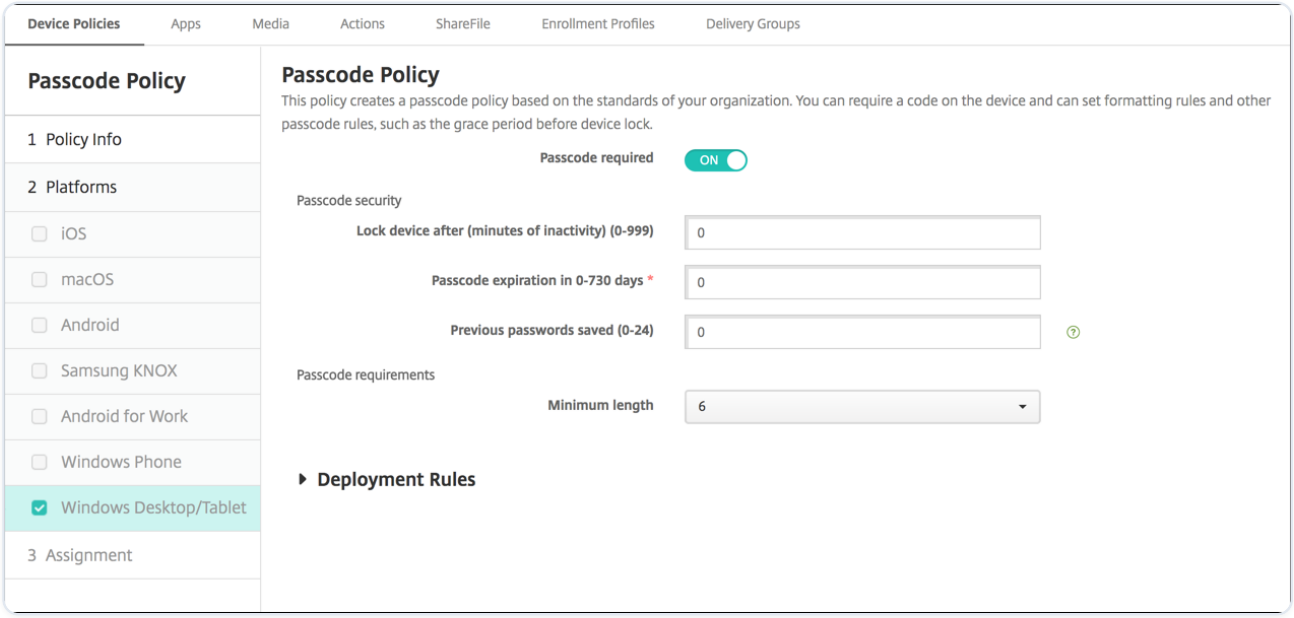
- **Nivel de complejidad:** Niveles predefinidos de complejidad de la contraseña.
  - **Ninguno:** No se requiere contraseña.
  - **Bajo:** Las contraseñas pueden ser:
    - Un patrón
    - Un PIN con un mínimo de cuatro números
  - **Medio:** Las contraseñas pueden ser:
    - Un PIN sin secuencias repetidas (4444) ni secuencias ordenadas (1234), y un mínimo de cuatro números
    - Alfabético con un mínimo de cuatro caracteres
    - Alfanumérico con un mínimo de cuatro caracteres
  - **Alto:** Las contraseñas pueden ser:
    - Un PIN sin secuencias repetidas (4444) ni secuencias ordenadas (1234), y un mínimo de ocho números
    - Alfabético con un mínimo de seis caracteres
    - Alfanumérico con un mínimo de seis caracteres

> **Nota:**
>
> Si habilita la complejidad del código de acceso para un perfil de trabajo, también debe habilitarla para el dispositivo.

- **Seguridad del código de acceso para el desafío de seguridad del perfil de trabajo**
  - **Borrar el contenedor después de (intentos de inicio de sesión fallidos):** Especifica el número de veces que un usuario puede fallar al iniciar sesión, después de lo cual el perfil de trabajo y sus datos se borran del dispositivo. Los usuarios deben volver a inicializar el perfil de trabajo después de que se produzca el borrado. El valor predeterminado es **No definido**.

- **Bloquear contenedor después de inactividad:** Especifica el número de minutos que un dispositivo puede estar inactivo antes de que se bloquee el perfil de trabajo. El valor puede estar entre 0 y 999 minutos. Establezca el valor en 0 para deshabilitar la directiva.
- **Caducidad del código de acceso en días (1-730):** Especifica el número de días después de los cuales caduca el código de acceso. Los valores válidos son 1–730. El valor predeterminado es **0**, lo que significa que el código de acceso nunca caduca.
- **Contraseñas anteriores guardadas (0-50):** Especifica el número de contraseñas usadas que se guardarán. Los usuarios no pueden usar ninguna contraseña que se encuentre en esta lista. Los valores válidos son 0–50. El valor predeterminado es **0**, lo que significa que los usuarios pueden reutilizar las contraseñas.

Configuración de Windows Desktop/Tablet



- **Se requiere código de acceso:** Seleccione esta opción para no requerir un código de acceso para los dispositivos Windows Desktop/Tablet. La configuración predeterminada es **Activado**, lo que requiere un código de acceso. La página se contrae y las siguientes opciones desaparecen cuando deshabilita esta configuración.
- **Seguridad del código de acceso**
  - **Bloquear dispositivo tras inactividad:** Escriba el número de minutos que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **0**.
  - **Caducidad del código de acceso en días (0-730):** Escriba el número de días tras los cuales caduca el código de acceso. Los valores válidos son 0-730. El valor predeterminado es **0**, lo que significa que el código de acceso nunca caduca.

- **Contraseñas anteriores guardadas (0-24):** Escriba el número de códigos de acceso usados que se deben guardar. Los usuarios no pueden usar ningún código de acceso que se encuentre en esta lista. Los valores válidos son 1-24. Introduzca un número entre 1 y 24 en este campo. El valor predeterminado es **0**.

- **Requisitos del código de acceso**

  - **Longitud mínima:** Haga clic en la longitud mínima del código de acceso en la lista desplegable. El valor predeterminado es **6**.

Directiva de dispositivo de período de gracia de bloqueo por código de acceso

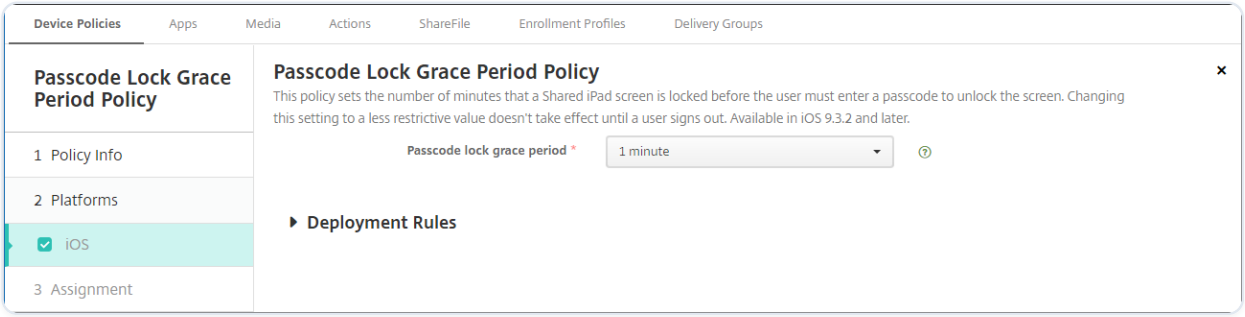
La directiva de dispositivo de período de gracia de bloqueo por código de acceso es para dispositivos compartidos que ejecutan iOS (iPadOS). Para obtener más información sobre los iPad compartidos, consulte (/es-es/citrix-endpoint-management/device-management/apple/integrate-with-apple-education.html).

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte (/es-es/citrix-endpoint-management/policies.html).

Configuración de iOS

- **Período de gracia de bloqueo por código de acceso:** El número de minutos que la pantalla de un iPad compartido permanece bloqueada antes de que el usuario deba introducir un código de acceso para desbloquear la pantalla. Cambiar esta configuración a un valor menos restrictivo no surte efecto hasta que un usuario cierra la sesión. El valor predeterminado es **Inmediatamente**.

  De forma predeterminada, el iPad compartido se bloquea automáticamente después de dos minutos de inactividad.



Directiva de dispositivo de punto de acceso personal

Puede permitir que los usuarios se conecten a Internet cuando no estén dentro del alcance de una red Wi-Fi utilizando la conexión de datos móviles a través de la funcionalidad de punto de acceso personal de sus dispositivos iOS.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

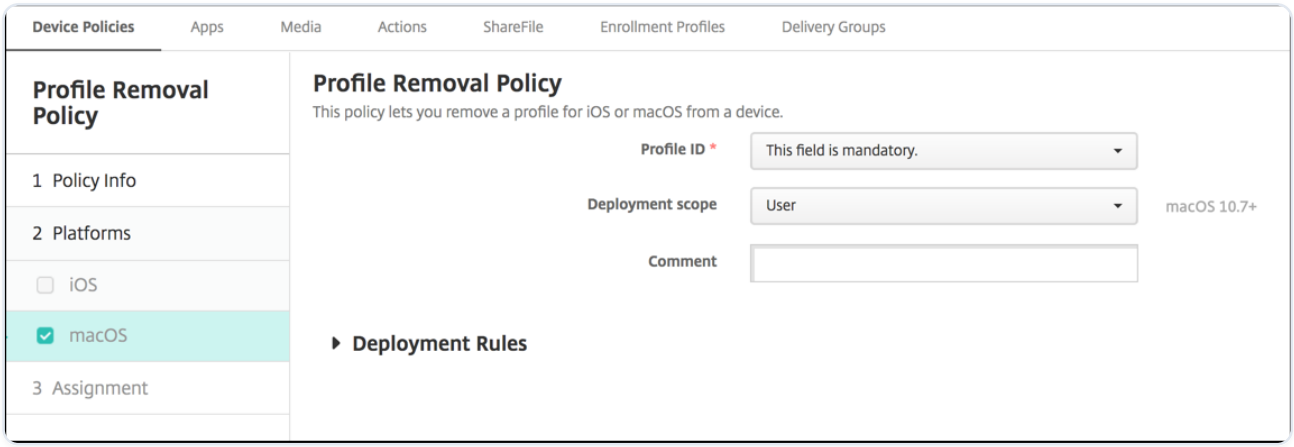
- **Deshabilitar punto de acceso personal:** Seleccione si desea deshabilitar la funcionalidad de punto de acceso personal en los dispositivos de los usuarios. El valor predeterminado es **Desactivado**, lo que desactiva el punto de acceso personal en los dispositivos de los usuarios. Esta directiva no deshabilita la funcionalidad. Los usuarios pueden seguir utilizando el punto de acceso personal en sus dispositivos, pero cuando se implementa la directiva, el punto de acceso personal se desactiva para que no permanezca activado de forma predeterminada.

Directiva de dispositivo de eliminación de perfiles

Puede crear una directiva de dispositivo de eliminación de perfiles de aplicaciones en Citrix Endpoint Management. Cuando se implementa, la directiva elimina el perfil de la aplicación de los dispositivos iOS o macOS de los usuarios.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de macOS



- **ID de perfil:** Haga clic en el ID de perfil de la aplicación en la lista desplegable. Este campo es obligatorio.

- **Ámbito de implementación:** Haga clic en **Usuario** o **Sistema** en la lista desplegable. El valor predeterminado es **Usuario**. Esta opción solo está disponible en macOS 10.7 y versiones posteriores.
- **Comentario:** Escriba un comentario opcional.

Política de dispositivo de perfil de aprovisionamiento

Cuando desarrolla y firma el código de una aplicación empresarial de iOS, normalmente incluye un perfil de aprovisionamiento de distribución empresarial, que Apple exige para que la aplicación se ejecute en un dispositivo iOS. Si falta un perfil de aprovisionamiento o ha caducado, la aplicación se bloquea cuando un usuario la toca para abrirla.

El problema principal con los perfiles de aprovisionamiento es que caducan un año después de su generación en el Portal para desarrolladores de Apple, y debe hacer un seguimiento de las fechas de caducidad de todos sus perfiles de aprovisionamiento en todos los dispositivos iOS registrados por sus usuarios. El seguimiento de las fechas de caducidad no solo implica hacer un seguimiento de las fechas de caducidad reales, sino también de qué usuarios están utilizando qué versión de la aplicación. Dos soluciones son enviar los perfiles de aprovisionamiento por correo electrónico a los usuarios o ponerlos en un portal web para su descarga e instalación. Estas soluciones funcionan, pero son propensas a errores porque requieren que los usuarios reaccionen a las instrucciones de un correo electrónico o que vayan al portal web, descarguen el perfil correcto y luego lo instalen.

Para que este proceso sea transparente para los usuarios, en Citrix Endpoint Management puede instalar y eliminar perfiles de aprovisionamiento con políticas de dispositivo. Los perfiles que faltan o han caducado se eliminan según sea necesario y los perfiles actualizados se instalan en los dispositivos de los usuarios, de modo que al tocar una aplicación, esta simplemente se abre para su uso.

Antes de poder crear una política de perfil de aprovisionamiento, debe crear un archivo de perfil de aprovisionamiento. Para obtener más información, consulte el artículo de Apple sobre cómo crear un perfil de aprovisionamiento de desarrollo en el sitio para desarrolladores de Apple.

Configuración de iOS

- **Perfil de aprovisionamiento de iOS:** Seleccione el archivo de perfil de aprovisionamiento para importar haciendo clic en **Examinar** y luego navegando hasta la ubicación del archivo.

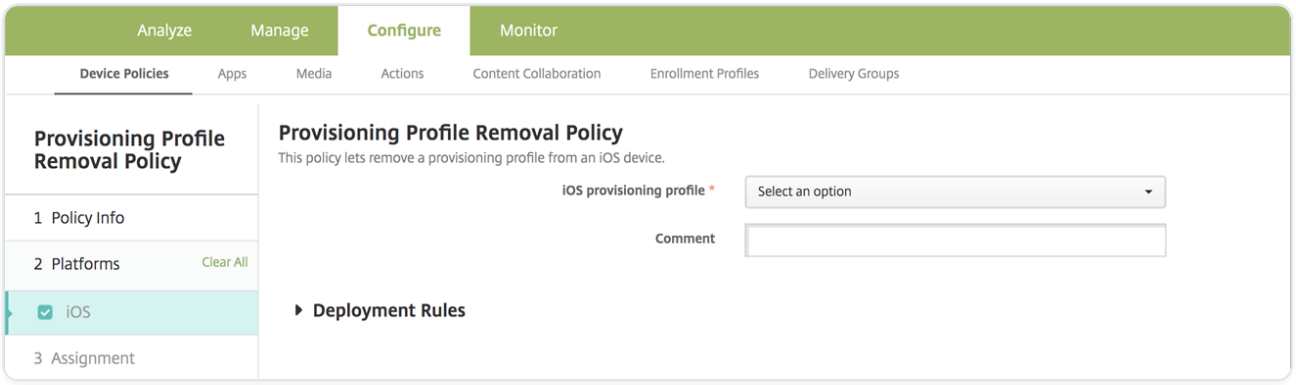
Política de dispositivo de eliminación de perfil de aprovisionamiento

Un perfil de aprovisionamiento le permite distribuir aplicaciones iOS a los dispositivos de los usuarios. Apple requiere que firme una aplicación utilizando un perfil de aprovisionamiento para autorizar que la aplicación se ejecute en dispositivos iOS. Para obtener más información, consulte Política de dispositivo de perfil de aprovisionamiento.

Para eliminar o reemplazar un perfil de aprovisionamiento antiguo, utilice la política de dispositivo de eliminación de perfil de aprovisionamiento.

Para añadir o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS



- **Perfil de aprovisionamiento de iOS:** Haga clic en el perfil de aprovisionamiento de la lista desplegable que desea eliminar.
- **Comentario:** Opcionalmente, añada un comentario.

Directiva de dispositivo proxy

La directiva de dispositivo proxy especifica la configuración global del proxy HTTP para los dispositivos iOS compatibles. Solo puede implementar una directiva global de proxy HTTP por dispositivo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisitos previos

Antes de implementar esta directiva, asegúrese de configurar todos los dispositivos iOS para los que desea establecer un proxy HTTP global en modo supervisado. Para obtener más información, consulte Implementar dispositivos con Apple Configurator 2 o Implementar dispositivos a través del programa de implementación de Apple.

Establezca reglas de implementación para inscribir dispositivos antes de enviar la directiva de proxy a los dispositivos.

Configuración de iOS

- **Configuración del proxy:** Haga clic en **Manual** o **Automático** para indicar cómo debe configurarse el proxy en los dispositivos de los usuarios.
    - Si hace clic en **Manual**, configure estos parámetros:
        - **Nombre de host o dirección IP del servidor proxy:** Escriba el nombre de host o la dirección IP del servidor proxy. Este campo es obligatorio.
        - **Puerto del servidor proxy:** Escriba el número de puerto del servidor proxy. Este campo es obligatorio.
        - **Nombre de usuario:** Escriba un nombre de usuario opcional para autenticarse en el servidor proxy.
        - **Contraseña:** Escriba una contraseña opcional para autenticarse en el servidor proxy.
    - Si hace clic en **Automático**, configure estos parámetros:
        - **URL de PAC del proxy:** Escriba la URL del archivo PAC que define la configuración del proxy.
        - **Permitir conexión directa si PAC no es accesible:** Seleccione si desea permitir a los usuarios conectarse directamente al destino si el archivo PAC no es accesible. El valor predeterminado es **Activado**.
- **Permitir omitir el proxy para acceder a redes cautivas:** Seleccione si desea permitir omitir el proxy para acceder a redes cautivas. El valor predeterminado es **Desactivado**.
- **Configuración de la directiva**
    - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**

- **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
- **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva. Solo disponible para iOS 6.0 y versiones posteriores.

Directiva de dispositivo de restricciones

> **Nota:**
>
> Cuando una actualización incluye nuevas configuraciones de directiva de dispositivo de restricciones, debe editar y guardar la directiva. Citrix Endpoint Management no implementa la directiva de dispositivo de restricciones actualizada hasta que la guarda.

La directiva de dispositivo de restricciones permite o restringe ciertas funciones o características en los dispositivos de los usuarios, como la cámara. Puede establecer restricciones de seguridad y restricciones en el contenido multimedia. También puede establecer restricciones sobre los tipos de aplicaciones que los usuarios pueden y no pueden instalar. La mayoría de las configuraciones de restricción están activadas de forma predeterminada (**Activado**), o *permiten*. Las principales excepciones son la función iOS Security - Force y todas las funciones de Windows Tablet, que están desactivadas de forma predeterminada (**Desactivado**), o *restringen*.

Cualquier opción para la que seleccione **Activado** significa que el usuario puede realizar la operación o usar la función. Por ejemplo:

- **Cámara:** Si está **Activado**, el usuario puede usar la cámara de su dispositivo. Si está **Desactivado**, el usuario no puede usar la cámara de su dispositivo.
- **Capturas de pantalla:** Si está **Activado**, el usuario puede hacer capturas de pantalla en su dispositivo. Si está **Desactivado**, el usuario no puede hacer capturas de pantalla en su dispositivo.

Si tiene configuradas tanto la directiva de dispositivo de restricciones como la directiva de dispositivo de quiosco, la directiva de dispositivo de restricciones tiene prioridad.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

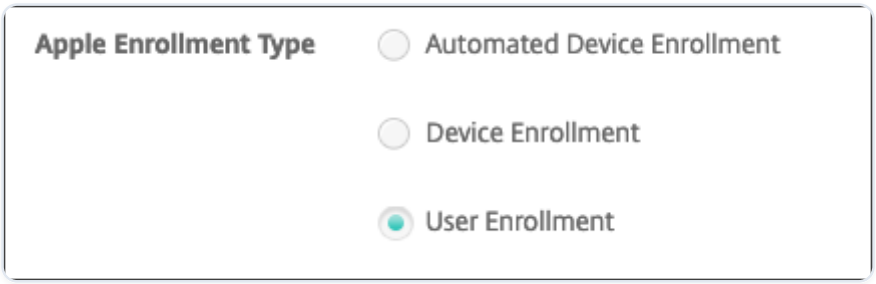


Algunas configuraciones de la directiva de restricciones de iOS solo se aplican a versiones específicas de iOS, como se indica aquí y en la página de la directiva de restricciones de la consola de Citrix Endpoint Management.

Estas configuraciones se aplican cuando el dispositivo está inscrito en modo de inscripción de usuario, modo no supervisado (MDM completo) o modo supervisado. La siguiente tabla muestra los modos de inscripción disponibles para cada configuración para iOS 13 y versiones posteriores.

- **Inscripción automatizada de dispositivos:** Dispositivos supervisados. Estos son los dispositivos que se inscriben mediante la inscripción masiva.
- **Inscripción de dispositivos:** Dispositivos no supervisados. Estos dispositivos se inscriben individualmente y todo el dispositivo es MDM completo.
- **Inscripción de usuario:** Dispositivos en los que solo se administran usuarios específicos. Para obtener más información sobre la inscripción de usuarios, consulte la documentación de Apple.

La configuración de la directiva de restricciones de iOS puede aplicarse cuando el dispositivo está inscrito en el modo de inscripción de usuario, el modo no supervisado (MDM completo) o el modo supervisado. La siguiente tabla muestra los modos de inscripción disponibles para cada configuración de directiva de restricciones para iOS 13 y versiones posteriores.



Como se indica en la tabla, algunas configuraciones que antes estaban disponibles en el modo no supervisado y supervisado solo están disponibles en el modo supervisado a partir de iOS 13. Se aplican las siguientes reglas:

- Si un dispositivo iOS 13+ supervisado se inscribe en Citrix Endpoint Management, la configuración se aplica al dispositivo.
- Si un dispositivo iOS 13+ no supervisado se inscribe en Citrix Endpoint Management, la configuración no se aplica al dispositivo.
- Si un dispositivo iOS 12 (o inferior) ya inscrito en Citrix Endpoint Management se actualiza a iOS 13, no hay cambios. La configuración se aplica al dispositivo como lo hacía antes de la actualización.

Para obtener información sobre cómo configurar un dispositivo iOS en modo supervisado, consulte Implementar dispositivos con Apple Configurator 2.

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
Permitir controles de hardware			
Cámara	No	Sí	Sí
FaceTime	No	No	Sí
Permitir el control remoto de FaceTime	No	No	Sí
Capturas de pantalla	Sí	No	Sí
Permitir que la aplicación Classroom observe de forma remota las	No	No	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
pantallas de los alumnos			
Permitir que la aplicación Classroom realice AirPlay y Ver pantalla sin preguntar	No	No	Sí
Streams de fotos	No	Sí	Sí
Streams de fotos compartidos	No	Sí	Sí
Permitir sesión temporal de iPad compartido	No	No	Sí
Marcación por voz	No	Sí	Sí
Siri	Sí	Sí	Sí
Permitir mientras el dispositivo está bloqueado	Sí	Sí	Sí
Filtro de blasfemias de Siri	No	No	Sí
Instalación de aplicaciones	No	No	Sí
Mercado de aplicaciones alternativo	No	No	Sí
Aplicaciones de distribución web	No	No	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
Permitir la recuperación global en segundo plano durante la itinerancia	No	Sí	Sí
Permitir aplicaciones			
iTunes Store	No	No	Sí
Compras dentro de la aplicación	No	Sí	Sí
Requerir contraseña de iTunes Store para compras	No	Sí	Sí
Safari	No	No	Sí
Autorrelleno	No	No	Sí
Forzar advertencia de fraude	Sí	Sí	Sí
Habilitar JavaScript	No	Sí	Sí
Bloquear elementos emergentes	No	Sí	Sí
Aceptar cookies	No	Sí	Sí
Red - Permitir acciones de iCloud			
Documentos y datos de iCloud	No	No	Sí
Copia de seguridad de iCloud	No	Sí	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
Llavero de fotos de iCloud	No	Sí	Sí
Fototeca de iCloud	No	Sí	Sí
Seguridad - Forzar			
Copias de seguridad cifradas	Sí	Sí	Sí
Seguimiento de anuncios limitado	No	Sí	Sí
Código de acceso en el primer emparejamiento de AirPlay	Sí	Sí	Sí
Apple Watch emparejado para usar la detección de muñeca	Sí	Sí	Sí
Compartir documentos administrados mediante AirDrop	Sí	Sí	Sí
Seguridad - Permitir			
Aceptar certificados SSL no confiables	No	Sí	Sí
Actualización automática de la configuración de confianza de certificados	No	Sí	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
Requerir portapapeles administrado	Sí	Sí	Sí
Documentos de aplicaciones administradas en aplicaciones no administradas	Sí	Sí	Sí
Las aplicaciones no administradas leen contactos administrados	No	No	Sí
Las aplicaciones administradas escriben contactos no administrados	No	No	Sí
Documentos de aplicaciones no administradas en aplicaciones administradas	Sí	Sí	Sí
Envío de diagnósticos a Apple	Sí	Sí	Sí
Touch ID para desbloquear el dispositivo	No	Sí	Sí
Desbloqueo automático	No	Sí	Sí
Notificaciones de Wallet cuando está bloqueado	No	Sí	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
Handoff	No	Sí	Sí
Sincronización de iCloud para aplicaciones administradas	Sí	Sí	Sí
Copia de seguridad para libros empresariales	Sí	Sí	Sí
Sincronización de notas y resaltados para libros empresariales	Sí	Sí	Sí
Resultados de Internet en Spotlight	No	Sí	Sí
Confianza en aplicaciones empresariales	No	Sí	Sí
Permitir publicidad personalizada de Apple	No	Sí	Sí
Configuración solo para dispositivos supervisados - Permitir			
Permitir la modificación de la eSIM	No	No	Sí
Conservar la eSIM al borrar	No	No	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
Borrar todo el contenido y la configuración	No	No	Sí
Tiempo de uso	No	No	Sí
Podcasts	No	No	Sí
Instalación de perfiles de configuración	No	No	Sí
Modificación de Touch ID y Face ID	No	No	Sí
Instalación de aplicaciones desde el dispositivo	No	No	Sí
Atajos de teclado	No	No	Sí
Apple Watch emparejado	No	No	Sí
Modificación de código de acceso	No	No	Sí
Modificación del nombre del dispositivo	No	No	Sí
Modificación del fondo de pantalla	No	No	Sí
Descarga automática de aplicaciones	No	No	Sí
AirDrop	No	No	Sí
iMessage	No	No	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
Contenido generado por el usuario de Siri	No	No	Sí
iBooks	No	No	Sí
Eliminar aplicaciones	No	Sí	Sí
Game Center	No	No	Sí
Añadir amigos	No	No	Sí
Juegos multijugador	No	No	Sí
Modificar la configuración de la cuenta	No	No	Sí
Modificar la configuración de datos móviles de la aplicación	No	No	Sí
Modificar la configuración de datos móviles de la aplicación	No	No	Sí
Permitir conexiones a unidades de red	No	No	Sí
Permitir conexiones de dispositivos USB	No	No	Sí
Permitir Buscar mi dispositivo	No	No	Sí
Permitir la configuración de Buscar a mis amigos	No	No	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
Modificar la configuración de Buscar a mis amigos	No	No	Sí
Emparejamiento con hosts que no son de Configurator	No	No	Sí
Teclados predictivos	No	No	Sí
Autocorrecciones del teclado	No	No	Sí
Corrector ortográfico del teclado	No	No	Sí
Permitir teclado QuickPath	No	No	Sí
Búsqueda de definiciones	No	No	Sí
ID de paquete de aplicación única	No	No	Sí
Noticias	No	No	Sí
Servicio Apple Music	No	No	Sí
Radio de Apple Music	No	No	Sí
Modificación de notificaciones	No	No	Sí
Uso restringido de aplicaciones	No	No	Sí
Modificación del envío de diagnósticos	No	No	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
Modificación de Bluetooth	No	No	Sí
Permitir dictado	No	No	Sí
Modificar si la Wi-Fi está activada o desactivada	No	No	Sí
Unirse solo a redes Wi-Fi instaladas por una directiva de red	No	No	Sí
Permitir que la aplicación Classroom realice AirPlay y Ver pantalla sin preguntar	No	No	Sí
Permitir que la aplicación Classroom se bloquee en una aplicación y bloquee el dispositivo sin preguntar	No	No	Sí
Unirse automáticamente a las clases de la aplicación Classroom sin preguntar	No	No	Sí
Permitir AirPrint	No	No	Sí
Permitir el almacenamiento de	No	No	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
credenciales de AirPrint en el llavero			
Permitir la detección de impresoras AirPrint mediante iBeacons	No	No	Sí
Permitir AirPrint solo a destinos con certificados de confianza	No	No	Sí
Agregar configuraciones de VPN	No	No	Sí
Modificar la configuración del plan de datos móviles	No	No	Sí
Eliminar aplicaciones del sistema	No	No	Sí
Configurar nuevos dispositivos cercanos	No	No	Sí
Permitir el modo restringido USB	No	No	Sí
Forzar actualizaciones de software retrasadas	No	No	Sí
Retraso forzado de la actualización de software	No	No	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
Forzar la solicitud de permiso del aula para abandonar las clases	No	No	Sí
Forzar la autenticación antes del autocompletado	No	No	Sí
Forzar fecha y hora automáticas	No	No	Sí
Autorrelleno de contraseñas	No	No	Sí
Solicitudes de proximidad de contraseña	No	No	Sí
Compartir contraseña	No	No	Sí
Permitir la modificación del punto de acceso personal	No	No	Sí
Permitir el arranque en recuperación por un dispositivo no emparejado	No	No	Sí
Instalar respuesta de seguridad rápida	No	No	Sí
Eliminar respuesta rápida de seguridad	No	No	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
Permitir protección de privacidad de correo	No	No	Sí
NFC	No	No	Sí
Permitir App clips	No	No	Sí
Genmoji	No	No	Sí
Image Playground	No	No	Sí
Image Wand	No	No	Sí
Duplicación de iPhone	No	No	Sí
Resultados de escritura a mano personalizados	No	No	Sí
Herramientas de escritura	No	No	Sí
Grabación de llamadas	No	No	Sí
Aplicaciones que se van a ocultar	No	No	Sí
Aplicaciones que se van a bloquear	No	No	Sí
Resumen de correo	No	No	Sí
Mensajería RCS	No	No	Sí
Permitir integraciones de inteligencia externa	No	No	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
Permitir iniciar sesión en integraciones de inteligencia externa	No	No	Sí
Permitir respuestas inteligentes de correo	No	No	Sí
Permitir transcripción de Notas	No	No	Sí
Permitir resumen de Safari	No	No	Sí
Permitir resumen de inteligencia visual	No	No	Sí
Permitir resumen de transcripción de Notas	No	No	Sí
Permitir informe de Apple Intelligence	No	No	Sí
Permitir la modificación de la aplicación de llamadas predeterminada	No	No	Sí
Permitir la modificación de la aplicación de mensajería predeterminada	No	No	Sí
Permitir ID de espacio de trabajo	No	No	Sí

CONFIGURACIÓN	INSCRIPCIÓN DE USUARIO	NO SUPERVISADO	SUPERVISADO
de inteligencia externa			
Modificación del navegador predeterminado	No	No	Sí
Permitir buzón de voz en vivo	No	No	Sí
Seguridad - Mostrar en la pantalla de bloqueo			
Centro de control	Sí	Sí	Sí
Notificación	Sí	Sí	Sí
Vista Hoy	Sí	Sí	Sí
Contenido multimedia - Permitir			
Música explícita, podcasts y material de iTunes U	No	No	Sí
Contenido sexual explícito en iBooks	No	Sí	Sí
Región de clasificaciones	No	Sí	Sí
Películas	No	Sí	Sí
Programas de TV	No	Sí	Sí
Aplicaciones	No	Sí	Sí

- **Permitir controles de hardware**

- **Cámara:** Permite a los usuarios usar la cámara en sus dispositivos.
  - **FaceTime:** Permite a los usuarios usar FaceTime en sus dispositivos. Para dispositivos iOS supervisados.
  - **Permitir control remoto de FaceTime:** Permite que una sesión remota de FaceTime solicite el control del dispositivo. Para dispositivos iOS supervisados. Disponible para iOS 18.4 y versiones posteriores.
- **Capturas de pantalla:** Permite a los usuarios hacer capturas de pantalla en sus dispositivos.
  - **Permitir que la aplicación Classroom observe de forma remota las pantallas de los alumnos:** Si esta restricción no está seleccionada, un instructor no puede usar la aplicación Classroom para observar de forma remota las pantallas de los alumnos. La configuración predeterminada está seleccionada, un instructor puede usar la aplicación Classroom para observar las pantallas de los alumnos. La configuración de **Permitir que la aplicación Classroom realice AirPlay y vea la pantalla sin preguntar** determina si los alumnos reciben una solicitud para dar permiso al instructor. Para dispositivos iOS supervisados.
  - **Permitir que la aplicación Classroom realice AirPlay y vea la pantalla sin preguntar:** Si esta restricción está seleccionada, el instructor puede realizar AirPlay y ver la pantalla en un dispositivo de un alumno, sin solicitar permiso. La configuración predeterminada no está seleccionada. Para dispositivos iOS supervisados.
- **Secuencias de fotos:** Permite a los usuarios usar MyPhotoStream para compartir fotos a través de iCloud con todos sus dispositivos iOS.
- **Secuencias de fotos compartidas:** Permite a los usuarios usar iCloud Photo Sharing para compartir fotos con compañeros de trabajo, amigos y familiares.
- **Permitir sesión temporal de iPad compartido:** Impide el acceso a sesiones temporales en iPads compartidos.
- **Marcación por voz:** Habilita la marcación por voz en los dispositivos de los usuarios.
- **Siri:** Permite a los usuarios usar Siri.
  - **Permitir con el dispositivo bloqueado:** Permite a los usuarios usar Siri mientras sus dispositivos están bloqueados.
  - **Filtro de blasfemias de Siri:** Habilita el filtro de blasfemias de Siri. La configuración predeterminada es restringir esta función, lo que significa que no se realiza ningún filtrado de blasfemias.

Para obtener más información sobre Siri y la seguridad, consulte Políticas de Siri y dictado.

- **Instalación de aplicaciones:** Permite a los usuarios instalar aplicaciones. Para dispositivos iOS supervisados.
- **Mercado de aplicaciones alternativo:** Impide la instalación de aplicaciones de mercados alternativos desde la web y evita que las aplicaciones de mercados alternativos ya instaladas instalen otras aplicaciones. Esta función está disponible a partir de iOS 17.4 y versiones posteriores. El valor predeterminado es **Activado**. Para dispositivos iOS supervisados.
- **Aplicaciones de distribución web:** Permite a los administradores de clientes bloquear las aplicaciones de terceros distribuidas por la web en dispositivos iOS. Esto es aplicable para las versiones de iOS 17.5 y posteriores. Para obtener más información, consulte Restricciones.
- **Permitir la recuperación global en segundo plano durante la itinerancia:** Permite que los dispositivos sincronicen automáticamente las cuentas de correo con iCloud mientras el dispositivo está en itinerancia. Cuando está **Desactivado**, deshabilita la actividad de recuperación global en segundo plano cuando un teléfono iOS está en itinerancia. El valor predeterminado es **Activado**.

- **Permitir aplicaciones**
  - **iTunes Store:** Permite a los usuarios acceder a iTunes Store. Para dispositivos iOS supervisados.
  - **Compras dentro de la aplicación:** Permite a los usuarios realizar compras dentro de la aplicación.
    - **Requerir contraseña de iTunes Store para las compras:** Requiere una contraseña para las compras dentro de la aplicación. El valor predeterminado es restringir esta función, lo que significa que no se requiere contraseña para las compras dentro de la aplicación.
  - **Safari:** Permite a los usuarios acceder a Safari. Para dispositivos iOS supervisados.
    - **Autorrelleno:** Permite a los usuarios configurar el autorrelleno para nombres de usuario y contraseñas en Safari.
    - **Forzar advertencia de fraude:** Si esta configuración está habilitada y los usuarios visitan un sitio web sospechoso de phishing, Safari les alerta. El valor predeterminado es restringir esta función, lo que significa que no se emiten advertencias.

    - **Habilitar JavaScript:** Permite que JavaScript se ejecute en Safari.
    - **Bloquear ventanas emergentes:** Bloquea las ventanas emergentes al ver sitios web. El valor predeterminado es restringir esta función, lo que significa que las ventanas emergentes no se bloquean.
  - **Aceptar cookies:** Establece en qué medida se aceptan las cookies. En la lista, elija una opción para permitir o restringir las cookies. La opción predeterminada es **Siempre**, que permite a todos los sitios web guardar cookies en Safari. Otras opciones son **Solo sitio web actual**, **Nunca** y **Solo de sitios visitados**.

- **Red - Permitir acciones de iCloud**
  - **Documentos y datos de iCloud:** Permite a los usuarios sincronizar documentos y datos con iCloud. Para dispositivos iOS supervisados.
  - **Copia de seguridad de iCloud:** Permite a los usuarios hacer copias de seguridad de sus dispositivos en iCloud.
  - **Llavero de iCloud:** Permite a los usuarios almacenar contraseñas, redes Wi-Fi, tarjetas de crédito y otra información en el Llavero de iCloud.
  - **Biblioteca de fotos en la nube:** Permite a los usuarios acceder a su biblioteca de fotos de iCloud.

- **Seguridad - Forzar**

  La configuración predeterminada es restringir las siguientes funciones, lo que significa que no hay funciones de seguridad habilitadas.

  - **Copias de seguridad cifradas:** Fuerza que las copias de seguridad en iCloud estén cifradas.
  - **Seguimiento de anuncios limitado:** Bloquea el seguimiento de anuncios dirigido.
  - **Código de acceso en el primer emparejamiento de AirPlay:** Requiere que los dispositivos habilitados para AirPlay se verifiquen con un código único en pantalla antes de que puedan usar AirPlay.
  - **Apple Watch emparejado para usar Detección de muñeca:** Requiere que un Apple Watch emparejado use **Detección de muñeca**.
  - **Compartir documentos administrados mediante AirDrop:** Al establecer esta opción en **Activado**, AirDrop aparece como un destino de entrega no administrado.

- **Seguridad - Permitir**

- **Aceptar certificados SSL no confiables:** Permite a los usuarios aceptar certificados SSL no confiables de sitios web.
- **Actualización automática de la configuración de confianza de certificados:** Permite que los certificados de confianza se actualicen automáticamente.
- **Requerir portapapeles administrado:** Permite que la funcionalidad de copiar y pegar siga las mismas restricciones que se aplican a **Documentos de aplicaciones administradas en aplicaciones no administradas** y **Documentos de aplicaciones no administradas en aplicaciones administradas**. Por ejemplo, configure lo siguiente:
  - **Requerir portapapeles administrado:** Activado
  - **Documentos de aplicaciones administradas en aplicaciones no administradas:** Desactivado
  - **Documentos de aplicaciones no administradas en aplicaciones administradas:** Activado Después de implementar la directiva en los dispositivos iOS, los usuarios no pueden copiar y pegar datos de aplicaciones administradas a aplicaciones no administradas, pero sí pueden copiar y pegar datos de aplicaciones no administradas a aplicaciones administradas.
- **Documentos de aplicaciones administradas en aplicaciones no administradas:** Permite a los usuarios mover datos de aplicaciones administradas (corporativas) a aplicaciones no administradas (personales).
- **Documentos de aplicaciones no administradas en aplicaciones administradas:** Permite a los usuarios mover datos de aplicaciones no administradas (personales) a aplicaciones administradas (corporativas).
- **Envío de diagnósticos a Apple:** Permite que se envíen a Apple datos de diagnóstico anónimos sobre los dispositivos de los usuarios.
- **Touch ID o Face ID para desbloquear el dispositivo:** Permite a los usuarios usar Touch ID o Face ID para desbloquear sus dispositivos.
- **Desbloqueo automático:** Si está en **Desactivado**, el usuario no puede usar el Apple Watch para desbloquear un iPhone emparejado. El valor predeterminado es **Activado**. Disponible para iOS 14.5 y versiones posteriores.
- **Notificaciones de Wallet cuando está bloqueado:** Permite que las notificaciones de Wallet aparezcan en la pantalla de bloqueo.
- **Handoff:** Permite a los usuarios transferir actividades de un dispositivo iOS a otro dispositivo iOS cercano.

- **Sincronización de iCloud para aplicaciones administradas:** Permite a los usuarios sincronizar aplicaciones administradas con iCloud.
- **Copia de seguridad de libros empresariales:** Permite que se haga una copia de seguridad de los libros empresariales en iCloud.
- **Sincronización de notas y resaltados para libros empresariales:** Permite que las notas y los resaltados que los usuarios han añadido a los libros empresariales se sincronicen con iCloud.
- **Confianza en aplicaciones empresariales:** Permite que las aplicaciones empresariales sean de confianza. Las aplicaciones empresariales son cualquier aplicación hecha a medida para su organización. Estas aplicaciones pueden ser creadas internamente o pueden ser desarrolladas y compradas a un proveedor externo. Para obtener información adicional, consulte Instalar aplicaciones empresariales personalizadas en iOS.
- **Resultados de Internet en Spotlight:** Permite que Spotlight muestre resultados de búsqueda de Internet además de los del dispositivo.
- **Las aplicaciones no administradas leen contactos administrados:** Opcional. Solo disponible si **Documentos de aplicaciones administradas en aplicaciones no administradas** está deshabilitado. Si esta política está habilitada, las aplicaciones no administradas pueden leer datos de los contactos de las cuentas administradas. El valor predeterminado es **Desactivado**. Disponible a partir de iOS 12.
- **Las aplicaciones administradas escriben contactos no administrados:** Opcional. Si está habilitado, permite que las aplicaciones administradas escriban contactos en los contactos de las cuentas no administradas. Si **Documentos de aplicaciones administradas en aplicaciones no administradas** está habilitado, esta restricción no tiene efecto. El valor predeterminado es **Desactivado**. Disponible a partir de iOS 12.
- **Permitir publicidad personalizada de Apple:** Si está **Desactivado**, la plataforma de publicidad de Apple no puede usar los datos de los usuarios para ofrecer anuncios personalizados. El valor predeterminado es **Activado**. Disponible para iOS 14.0 y versiones posteriores.

- **Configuración solo para dispositivos supervisados - Permitir**

  Esta configuración se aplica solo a los dispositivos supervisados. Para conocer los pasos para configurar un dispositivo iOS en modo supervisado, consulte Implementar dispositivos con Apple Configurator 2.

  - **Permitir la modificación de la eSIM:** Permite a los usuarios cambiar la configuración de la eSIM en su dispositivo.

- **Conservar eSIM al borrar:** Si está **Activado**, el sistema conserva la eSIM cuando borra el dispositivo debido a demasiados intentos fallidos de contraseña o a la opción Borrar contenido y configuración en **Ajustes > General > Restablecer**. El valor predeterminado es **Desactivado**.

> **Nota:**
>
> El sistema no conserva la eSIM si **Buscar mi** inicia el borrado del dispositivo.

- **Borrar contenido y configuración:** Permite a los usuarios borrar todo el contenido y la configuración de sus dispositivos.
- **Tiempo de uso:** Permite a los usuarios habilitar Tiempo de uso.
- **Podcasts:** Permite a los usuarios descargar y sincronizar podcasts.
- **Instalar perfiles de configuración:** Permite a los usuarios instalar un perfil de configuración distinto al implementado por usted.
- **Modificación de Touch ID y Face ID:** Permite a los usuarios cambiar o eliminar su Touch ID o Face ID.
- **Instalar aplicaciones desde el dispositivo:** Permite a los usuarios instalar aplicaciones. Deshabilitar esta configuración impide que los usuarios finales instalen nuevas aplicaciones. La App Store se deshabilita y su icono se elimina de la pantalla de inicio.
- **Atajos de teclado:** Permitir a los usuarios crear atajos de teclado personalizados para palabras o frases que usan con frecuencia.
- **Apple Watch emparejado:** Permitir a los usuarios emparejar un Apple Watch con un dispositivo supervisado.
- **Modificación de código de acceso:** Permitir a los usuarios cambiar el código de acceso en un dispositivo supervisado.
- **Modificación del nombre del dispositivo:** Permitir a los usuarios cambiar el nombre de su dispositivo.
- **Modificación del fondo de pantalla:** Permitir a los usuarios cambiar el fondo de pantalla en sus dispositivos.
- **Descarga automática de aplicaciones:** Permitir la descarga de aplicaciones.
- **AirDrop:** Permitir a los usuarios compartir fotos, vídeos, sitios web, ubicaciones y más con dispositivos iOS cercanos.

- **iMessage:** Permitir a los usuarios enviar mensajes de texto a través de Wi-Fi con iMessage.
- **Contenido generado por el usuario de Siri:** Permitir a Siri consultar contenido generado por el usuario de la web. Los consumidores, no los periodistas tradicionales, producen contenido generado por el usuario. Por ejemplo, el contenido que se encuentra en Twitter o Facebook es generado por el usuario.
- **iBooks:** Permitir a los usuarios usar la aplicación iBooks.
- **Eliminación de aplicaciones:** Permitir a los usuarios eliminar aplicaciones de sus dispositivos.
- **Game Center:** Permitir a los usuarios jugar a juegos en línea a través de Game Center en sus dispositivos.
  - **Añadir amigos:** Permitir a los usuarios enviar una notificación a un amigo para jugar a un juego.
  - **Juegos multijugador:** Permitir a los usuarios iniciar partidas multijugador en sus dispositivos.
- **Modificación de la configuración de la cuenta:** Permitir a los usuarios modificar la configuración de la cuenta de su dispositivo.
- **Modificación de la configuración de datos móviles de la aplicación:** Permite a los usuarios modificar cómo las aplicaciones usan los datos móviles.
- **Permitir conexiones a unidades de red:** Impide la conexión a unidades de red en la aplicación Archivos.
- **Permitir conexiones de dispositivos USB:** Impide la conexión a cualquier dispositivo USB conectado en la aplicación Archivos.
- **Permitir Buscar mi dispositivo:** Deshabilita la opción **Buscar mi dispositivo** en la aplicación Buscar.
- **Permitir la configuración de Buscar a mis amigos:** Deshabilita la opción **Buscar a mis amigos** en la aplicación Buscar.
- **Modificación de la configuración de Buscar a mis amigos:** Permite a los usuarios cambiar su configuración de Buscar a mis amigos.
- **Emparejamiento con hosts que no son de Configurator:** Permite al administrador controlar con qué dispositivos se puede emparejar un dispositivo de usuario. Deshabilitar esta opción impide el emparejamiento, excepto con el host supervisor que ejecuta Apple

Configurator. Si no se configura ningún certificado de host supervisor, se deshabilita todo el emparejamiento.

- **Teclados predictivos:** Permite a los dispositivos de usuario usar el teclado predictivo para sugerir palabras mientras escriben. Deshabilite esta opción en situaciones como la administración de pruebas estandarizadas en las que no desea que los usuarios tengan acceso a palabras sugeridas.
- **Correcciones automáticas del teclado:** Permite a los dispositivos de usuario usar la corrección automática del teclado. Deshabilite esta opción en situaciones como la administración de pruebas estandarizadas en las que no desea que los usuarios tengan acceso a la corrección automática.
- **Corrector ortográfico del teclado:** Permite a los dispositivos de usuario usar el corrector ortográfico mientras escriben. Deshabilite esta opción en situaciones como la administración de pruebas estandarizadas en las que no desea que los usuarios tengan acceso al corrector ortográfico.
- **Búsqueda de definiciones:** Permite a los dispositivos de usuario usar la búsqueda de definiciones mientras escriben. Deshabilite esta opción en situaciones como la administración de pruebas estandarizadas en las que no desea que los usuarios busquen definiciones mientras escriben.
- **ID de paquete de aplicación única:** Cree una lista de aplicaciones a las que se les permite mantener el control sobre el dispositivo e impedir la interacción con otras aplicaciones o funciones. Para agregar una aplicación, haga clic en **Agregar**, escriba un **Nombre de aplicación** y haga clic en **Guardar**. Repita ese proceso para cada aplicación que desee agregar.
- **Noticias:** Permite a los usuarios usar la aplicación Noticias.
- **Servicio Apple Music:** Permite a los usuarios usar el servicio Apple Music. Si no permite el servicio Apple Music, la aplicación Música se ejecuta en modo clásico. El valor predeterminado es **Activado**. Disponible para iOS 9.3 o posterior.
- **Apple Music Radio:** Permite a los usuarios usar Apple Music Radio. El valor predeterminado es **Activado**. Disponible para iOS 9.3 o posterior.
- **Modificación de notificaciones:** Permitir a los usuarios modificar la configuración de notificaciones.
- **Uso restringido de aplicaciones:** Permitir a los usuarios usar todas las aplicaciones o usar o no usar aplicaciones, según los ID de paquete que proporcione. Se aplica solo a

dispositivos supervisados. Si selecciona **Solo permitir algunas aplicaciones**, agregue una aplicación con el ID de paquete `com.apple.webapp` para permitir los clips web.

> **Nota:**
>
> A partir de iOS 11, Apple introdujo cambios en las directivas disponibles para las restricciones de aplicaciones. Apple ya no permite eliminar el acceso a la aplicación Ajustes y a la aplicación Teléfono restringiendo el paquete de aplicación iOS correspondiente.
>
> Después de configurar la directiva de dispositivo Restricciones para bloquear algunas aplicaciones y, a continuación, implementar la directiva: Si más tarde desea permitir algunas o todas esas aplicaciones, cambiar e implementar la directiva de dispositivo Restricciones no cambia las restricciones. En este caso, iOS no aplica los cambios al perfil de iOS. Para continuar, use la directiva de eliminación de perfiles para eliminar el perfil de iOS y, a continuación, implemente la directiva de dispositivo Restricciones actualizada.

Si cambia esta configuración a **Solo permitir algunas aplicaciones:** Antes de implementar esta directiva, aconseje a los usuarios de dispositivos inscritos mediante el Programa de implementación de Apple que inicien sesión en sus cuentas de Apple desde el Asistente de configuración. De lo contrario, es posible que los usuarios tengan que deshabilitar la autenticación de dos factores en sus dispositivos para iniciar sesión en sus cuentas de Apple y acceder a las aplicaciones permitidas.

- **Modificación del envío de diagnósticos:** Permitir a los usuarios modificar la configuración de envío de diagnósticos y análisis de aplicaciones en el panel **Ajustes > Diagnóstico y uso**.
- **Modificación de Bluetooth:** Permitir a los usuarios modificar la configuración de Bluetooth.
- **Permitir dictado:** Solo supervisado. Si esta restricción está establecida en **Desactivado**, no se permite la entrada de dictado, incluido el reconocimiento de voz a texto. La configuración predeterminada es **Activado**.
- **Modificar si Wi-Fi está activado o desactivado:** Impide que Wi-Fi se active o desactive en Ajustes o en el Centro de control. Activar el modo avión tampoco tiene efecto. Esta restricción no impide seleccionar qué red Wi-Fi usar.

- **Unirse solo a redes Wi-Fi instaladas por una directiva de red:** Opcional. Solo supervisado. Si esta restricción está establecida en **Activado**, el dispositivo solo puede unirse a redes Wi-Fi cuando se configuraron a través de un perfil de configuración. La configuración predeterminada es **Desactivado**.
- **Permitir que la aplicación Aula realice AirPlay y Ver pantalla sin preguntar:** Si se selecciona esta restricción, el instructor puede realizar AirPlay y Ver pantalla en un dispositivo de estudiante, sin pedir permiso. La configuración predeterminada no está seleccionada. Para dispositivos iOS supervisados.
- **Permitir que la aplicación Aula se bloquee en una aplicación y bloquee el dispositivo sin preguntar:** Si esta restricción está establecida en **Activado**, la aplicación Aula bloquea automáticamente los dispositivos de los usuarios en una aplicación y bloquea el dispositivo, sin preguntar a los usuarios. La configuración predeterminada es **Desactivado**. Para dispositivos supervisados que ejecutan iOS 11 (versión mínima).
- **Unirse automáticamente a las clases de la aplicación Aula sin preguntar:** Si esta restricción está establecida en **Activado**, la aplicación Aula une automáticamente a los usuarios a las clases, sin preguntar a los usuarios. La configuración predeterminada es **Desactivado**. Para dispositivos supervisados que ejecutan iOS 11 (versión mínima).
- **Permitir AirPrint:** Si esta restricción está establecida en **Desactivado**, los usuarios no pueden imprimir con AirPrint. La configuración predeterminada es **Activado**. Cuando esta restricción está **Activada**, aparecen estas restricciones adicionales. Para dispositivos supervisados que ejecutan iOS 11 (versión mínima).
  - **Permitir el almacenamiento de credenciales de AirPrint en el llavero:** Si esta restricción no está seleccionada, el nombre de usuario y la contraseña de AirPrint no se almacenan en el llavero. La configuración predeterminada está seleccionada. Para dispositivos supervisados que ejecutan iOS 11 (versión mínima).
  - **Permitir la detección de impresoras AirPrint mediante iBeacons:** Si esta restricción no está seleccionada, la detección de impresoras AirPrint mediante iBeacon está deshabilitada. Esta configuración evita que las balizas Bluetooth de AirPrint falsas realicen phishing para el tráfico de red. La configuración predeterminada está seleccionada. Para dispositivos supervisados que ejecutan iOS 11 (versión mínima).
  - **Permitir AirPrint solo a destinos con certificados de confianza:** Si esta restricción está seleccionada, los usuarios solo pueden usar AirPrint para imprimir en destinos con certificados de confianza. La configuración predeterminada no está seleccionada. Para dispositivos supervisados que ejecutan iOS 11 (versión mínima).

- **Adición de configuraciones de VPN:** Si esta restricción está establecida en **Desactivado**, los usuarios no pueden crear configuraciones de VPN. La configuración predeterminada es **Activado**. Para dispositivos supervisados que ejecutan iOS 11 (versión mínima).
- **Modificación de la configuración del plan de datos móviles:** Si esta restricción está establecida en **Desactivado**, los usuarios no pueden modificar la configuración del plan de datos móviles. La configuración predeterminada es **Activado**. Para dispositivos supervisados que ejecutan iOS 11 (versión mínima).
- **Eliminación de aplicaciones del sistema:** Si esta restricción está establecida en **Desactivado**, los usuarios no pueden eliminar aplicaciones del sistema de su dispositivo. La configuración predeterminada es **Activado**. Para dispositivos supervisados que ejecutan iOS 11 (versión mínima).
- **Configuración de nuevos dispositivos cercanos:** Si esta restricción está establecida en Desactivado, los usuarios no pueden configurar nuevos dispositivos cercanos. La configuración predeterminada es Activado. Para dispositivos supervisados que ejecutan iOS 11 (versión mínima).
- **Permitir el modo restringido USB:** Si está **Desactivado**, el dispositivo siempre puede conectarse a accesorios USB mientras está bloqueado. El valor predeterminado es **Activado**. Solo disponible para dispositivos iOS 11.3 y posteriores supervisados.
- **Forzar actualizaciones de software retrasadas:** Si está **Activado**, retrasa la visibilidad de las actualizaciones de software para el usuario. Con esta restricción, el usuario no ve una actualización de software hasta el número de días especificado después de la fecha de lanzamiento de la actualización de software. El valor predeterminado es **Desactivado**. Solo disponible para dispositivos iOS 11.3 y posteriores supervisados. La directiva de actualización del SO tiene más configuraciones para controlar la frecuencia con la que los dispositivos reciben actualizaciones. Consulte Directiva de dispositivo de actualización del SO.
- **Retraso forzado de la actualización de software (días):** Permite especificar el número de días para retrasar una actualización de software en el dispositivo. El retraso máximo es de **90** días. El valor predeterminado es de **30** días. Solo disponible para dispositivos iOS 11.3 y posteriores supervisados.
- **Forzar la solicitud de permiso de Classroom para abandonar las clases:** Si está **Activado**, un estudiante inscrito en un curso no administrado con Classroom debe solicitar permiso al profesor al intentar abandonar el curso. El valor predeterminado es **Desactivado**. Solo disponible para dispositivos iOS 11.3 y posteriores supervisados.

- **Forzar la autenticación antes del autorrelleno:** Obliga al usuario a autenticarse antes de poder usar la función de autorrelleno.
- **Forzar fecha y hora automáticas:** Permite establecer automáticamente la fecha y la hora en dispositivos supervisados. Si está **Activado**, los usuarios del dispositivo no pueden desmarcar **Establecer automáticamente** en **General > Fecha y hora**. La zona horaria del dispositivo solo se actualiza cuando el dispositivo puede determinar su ubicación. Es decir, cuando un dispositivo tiene una conexión de datos móviles o una conexión Wi-Fi con los servicios de ubicación habilitados. El valor predeterminado es **Desactivado**. Solo disponible para dispositivos iOS 12 y posteriores supervisados.
- **Autorrelleno de contraseñas:** Opcional. Si está deshabilitado, los usuarios no pueden usar las funciones de Autorrelleno de contraseñas o Contraseñas seguras automáticas. El valor predeterminado es **Activado**. Disponible a partir de iOS 12.
- **Solicitudes de proximidad de contraseñas:** Opcional. Si está deshabilitado, los dispositivos de los usuarios no solicitan contraseñas a los dispositivos cercanos. El valor predeterminado es **Activado**. Disponible a partir de iOS 12.
- **Compartir contraseñas:** Opcional. Si está desactivado, los usuarios no pueden compartir sus contraseñas mediante la función Contraseñas de AirDrop. El valor predeterminado es **Activado**. Disponible a partir de iOS 12.
- **Permitir la modificación del punto de acceso personal:** Impide que los usuarios cambien la configuración del punto de acceso personal.
- **Permitir el arranque en recuperación por un dispositivo no emparejado:** Si está **Activado**, permite que los dispositivos se inicien en modo de recuperación mediante un dispositivo no emparejado. El valor predeterminado es **Desactivado**. Disponible para iOS 14.5 y versiones posteriores.
- **Instalar respuesta de seguridad rápida:** Si está **Desactivado**, prohíbe la instalación de respuestas de seguridad rápidas. El valor predeterminado es **Activado**.
- **Eliminar respuesta de seguridad rápida:** Si está **Desactivado**, prohíbe la eliminación de respuestas de seguridad rápidas. El valor predeterminado es **Activado**.
- **Permitir la protección de la privacidad del correo:** Si está **Desactivado**, desactiva la Protección de la privacidad del correo en el dispositivo. El valor predeterminado es **Activado**. Disponible para iOS 15.2 y versiones posteriores.
- **NFC:** Si está **Desactivado**, desactiva NFC. El valor predeterminado es **Activado**. Disponible para iOS 14.2 y versiones posteriores.

- **Permitir App Clips**: Si está **Desactivado**, impide que un usuario añada App Clips y elimina cualquier App Clip existente en el dispositivo. El valor predeterminado es **Activado**. Disponible para iOS 14.0 y versiones posteriores.
- **Genmoji:** Si está **Desactivado**, prohíbe la creación de nuevos Genmoji. El valor predeterminado es **Activado**. Disponible para iOS 18 y versiones posteriores.
- **Image Playground:** Si está **Desactivado**, prohíbe el uso de la generación de imágenes. El valor predeterminado es **Activado**. Disponible para iOS 18 y versiones posteriores.
- **Image Wand:** Si está **Desactivado**, prohíbe el uso de Image Wand. El valor predeterminado es **Activado**. Disponible para iOS 18 y versiones posteriores.
- **Duplicación de iPhone:** Si está **Desactivado**, prohíbe el uso de la Duplicación de iPhone e impide que el iPhone se duplique en cualquier Mac. El valor predeterminado es **Activado**. Disponible para iOS 18 y versiones posteriores.
- **Resultados de escritura a mano personalizados:** Si está **Desactivado**, impide que el sistema genere texto con la escritura a mano del usuario. El valor predeterminado es **Activado**. Disponible para iOS 18 y versiones posteriores.
- **Herramientas de escritura:** Si está **Desactivado**, desactiva las herramientas de escritura de Apple Intelligence. El valor predeterminado es **Activado**. Disponible para iOS 18 y versiones posteriores.
- **Grabación de llamadas:** Si está **Desactivado**, desactiva la grabación de llamadas. El valor predeterminado es **Activado**. Disponible para iOS 18 y versiones posteriores.
- **Aplicaciones a ocultar:** Si está **Desactivado**, impide que el usuario oculte aplicaciones. No afecta la capacidad de dejar aplicaciones en la Biblioteca de Apps mientras se eliminan de la pantalla de inicio. El valor predeterminado es **Activado**. Disponible para iOS 18 y versiones posteriores.
- **Aplicaciones a bloquear:** Si está **Desactivado**, deshabilita la capacidad del usuario para bloquear aplicaciones. Dado que ocultar aplicaciones requiere bloquearlas, deshabilitar el bloqueo también deshabilita la ocultación. El valor predeterminado es **Activado**. Disponible para iOS 18 y versiones posteriores.
- **Resumen de Mail:** Si está **Desactivado**, deshabilita la capacidad de crear manualmente resúmenes de mensajes de correo electrónico. Esto no afecta la generación automática de resúmenes. El valor predeterminado es **Activado**. Disponible para iOS 18.1 y versiones posteriores.
- **Mensajería RCS:** Si está **Desactivado**, impide el uso de la mensajería RCS. El valor predeterminado es **Activado**. Disponible para iOS 18.1 y versiones posteriores.

- **Permitir integraciones de inteligencia externas:** Si está **Desactivado**, deshabilita el uso de servicios de inteligencia externos basados en la nube con Siri. El valor predeterminado es **Activado**. Disponible para iOS 18.2 y versiones posteriores.
- **Permitir iniciar sesión en integraciones de inteligencia externas:** Si está **Desactivado**, fuerza a los proveedores de inteligencia externos a un modo anónimo. Si un usuario ya ha iniciado sesión en un proveedor de inteligencia externo, aplicar esta restricción hará que se cierre la sesión cuando se intente la siguiente solicitud. El valor predeterminado es **Activado**. Disponible para iOS 18.2 y versiones posteriores.
- **Permitir respuestas inteligentes en Mail:** Si está **Desactivado**, deshabilita las respuestas inteligentes en Mail. El valor predeterminado es **Activado**. Disponible para iOS 18.2 y versiones posteriores.
- **Permitir transcripción en Notas:** Si está **Desactivado**, deshabilita la transcripción en Notas. El valor predeterminado es **Activado**. Disponible para iOS 18.2 y versiones posteriores.
- **Permitir resumen de Safari:** Si está **Desactivado**, el sistema deshabilita la capacidad de resumir contenido en Safari. El valor predeterminado es **Activado**. Disponible para iOS 18.4 y versiones posteriores.
- **Permitir resumen de inteligencia visual:** Si está **Desactivado**, el sistema deshabilita la función de resumen de inteligencia visual. El valor predeterminado es **Activado**. Disponible para iOS 18.3 y versiones posteriores.
- **Permitir resumen de transcripción de Notas:** Si está **Desactivado**, deshabilita el resumen de transcripciones en Notas. El valor predeterminado es **Activado**. Disponible para iOS 18.3 y versiones posteriores.
- **Permitir informe de Apple Intelligence:** Si está **Desactivado**, el sistema deshabilita los informes de Apple Intelligence. El valor predeterminado es **Activado**. Disponible para iOS 18.4 y versiones posteriores.
- **Permitir modificación de la aplicación de llamadas predeterminada:** Si está **Desactivado**, deshabilita la modificación de la preferencia de la aplicación de llamadas predeterminada. El comando de configuración MDM para establecer la preferencia de la aplicación de llamadas predeterminada sigue funcionando cuando se aplica esto. El valor predeterminado es **Activado**. Disponible para iOS 18.4 y versiones posteriores.
- **Permitir modificación de la aplicación de mensajería predeterminada:** Si está **Desactivado**, deshabilita la modificación de la preferencia de la aplicación de mensajería predeterminada. El comando de configuración MDM para establecer la preferencia de la

aplicación de mensajería predeterminada sigue funcionando cuando se aplica esto. El valor predeterminado es **Activado**. Disponible para iOS 18.4 y versiones posteriores.

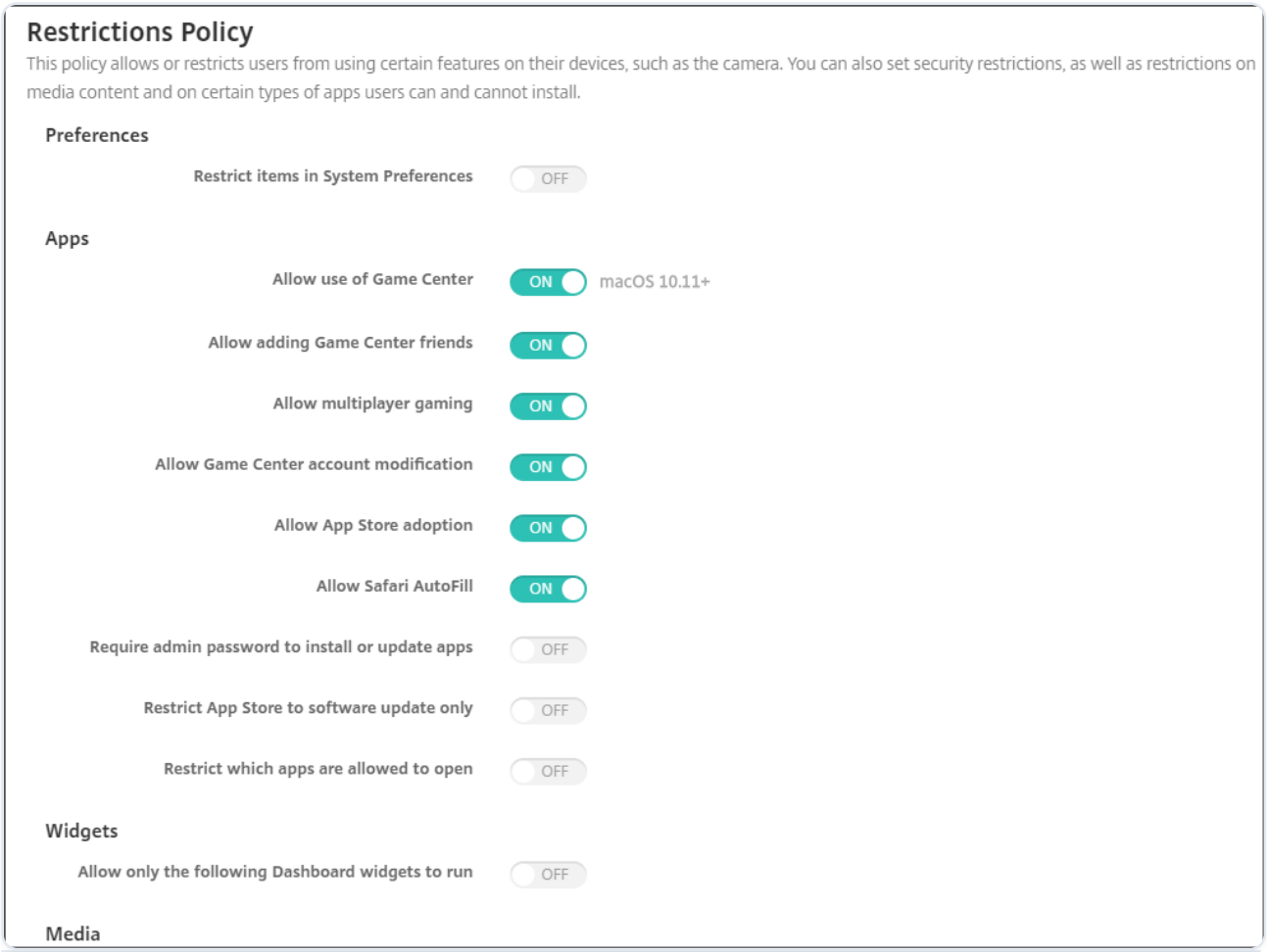
- **Permitir ID de espacio de trabajo de inteligencia externa:** Una matriz de cadenas, pero actualmente restringida a un solo elemento. Si está presente, Apple Intelligence solo permite el uso del ID de espacio de trabajo de integración externa proporcionado y requiere un inicio de sesión para realizar solicitudes; se requerirá que el usuario inicie sesión en las integraciones que admitan el inicio de sesión. Múltiples cargas útiles se combinan utilizando una operación de intersección. Esto significa que el conjunto permitido de ID de espacio de trabajo puede convertirse en un conjunto vacío si se especifican valores conflictivos en varias cargas útiles. Disponible para iOS 18.3 y versiones posteriores.
  - **ID de espacio de trabajo de inteligencia externa:** Para añadir un ID de espacio de trabajo de inteligencia externa, haga clic en **Añadir**, escriba un **ID de espacio de trabajo de inteligencia externa** y haga clic en **Guardar**. Repita este proceso para cada ID de espacio de trabajo que desee añadir.
- **Modificación del navegador predeterminado:** Si está en **Desactivado**, deshabilita la modificación de la preferencia del navegador predeterminado. El comando de configuración de MDM para establecer la preferencia del navegador predeterminado seguirá funcionando cuando se aplique esto. El valor predeterminado es **Activado**. Disponible para iOS 18.2 y versiones posteriores.
- **Permitir buzón de voz en vivo:** Si está en **Desactivado**, el sistema deshabilita el buzón de voz en vivo en el dispositivo. El valor predeterminado es **Activado**. Disponible para iOS 17.2 y versiones posteriores.

- **Seguridad - Mostrar en la pantalla de bloqueo**
  - **Centro de control:** Permite el acceso al Centro de control en la pantalla de bloqueo. El Centro de control permite a los usuarios modificar fácilmente la configuración del Modo avión, Wi-Fi, Bluetooth, Modo No molestar y Bloquear rotación.
  - **Notificación:** Permite las notificaciones en la pantalla de bloqueo.
  - **Vista Hoy:** Permite la Vista Hoy, que agrega información como el tiempo y los elementos del calendario del día actual, en la pantalla de bloqueo.
- **Contenido multimedia - Permitir**
  - **Música, podcasts y material de iTunes U explícitos:** Permite material explícito en los dispositivos de los usuarios.

- **Contenido sexual explícito en iBooks:** Permite la descarga de material explícito de iBooks.
- **Región de clasificación:** Establezca la región de la que se obtienen las clasificaciones de control parental. En la lista, haga clic en un país para establecer la región de clasificación. El valor predeterminado es **Estados Unidos**.
- **Películas:** Establezca si se permiten películas en los dispositivos de los usuarios. Si se permiten películas, establezca opcionalmente el nivel de clasificación para las películas. En la lista, haga clic en una opción para permitir o restringir películas en el dispositivo. El valor predeterminado es Permitir todas las películas.
- **Programas de TV:** Establezca si se permiten programas de TV en los dispositivos de los usuarios. Si se permiten programas de TV, establezca opcionalmente el nivel de clasificación para los programas de TV. En la lista, haga clic en una opción para permitir o restringir programas de TV en el dispositivo. El valor predeterminado es Permitir todos los programas de TV.
- **Aplicaciones:** Establezca si se permiten aplicaciones en los dispositivos de los usuarios. Si se permiten aplicaciones, establezca opcionalmente el nivel de clasificación para las aplicaciones. En la lista, haga clic en una opción para permitir o restringir aplicaciones en el dispositivo. El valor predeterminado es Permitir todas las aplicaciones.

- **Configuración de la directiva**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva. Solo disponible para iOS 6.0 y versiones posteriores.
  - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en iOS 9.3 y versiones posteriores.

Configuración de macOS



CONFIGURACIÓN	NO SUPERVISADO	SUPERVISADO
Aplicaciones		
Permitir el uso de Game Center	No	Sí
Permitir añadir amigos de Game Center	No	Sí
Permitir juegos multijugador	No	Sí
Permitir la modificación de la cuenta de Game Center	Sí	Sí
Permitir la adopción de App Store	Sí	Sí
Permitir el autorrelleno de Safari	No	Sí

CONFIGURACIÓN	NO SUPERVISADO	SUPERVISADO
Requerir contraseña de administrador para instalar o actualizar aplicaciones	Sí	Sí
Restringir App Store solo a actualizaciones de software	Sí	Sí
Restringir qué aplicaciones se pueden abrir	Sí	Sí
Multimedia		
Permitir AirDrop	No	Sí
Funcionalidad		
Bloquear imagen de escritorio	No	Sí
Permitir el uso de la cámara	No	Sí
Permitir Apple Music	No	Sí
Permitir sugerencias de Spotlight	Sí	Sí
Permitir Buscar	Sí	Sí
Permitir el uso de la contraseña de iCloud para cuentas locales	Sí	Sí
Permitir documentos y datos de iCloud	Sí	Sí
Permitir Escritorio y Documentos de iCloud	No	Sí
Permitir sincronización de Llavero de iCloud	No	Sí
Permitir Mail de iCloud	Sí	Sí

CONFIGURACIÓN	NO SUPERVISADO	SUPERVISADO
Permitir Contactos de iCloud	Sí	Sí
Permitir Calendarios de iCloud	Sí	Sí
Permitir Recordatorios de iCloud	Sí	Sí
Permitir Marcadores de iCloud	Sí	Sí
Permitir Notas de iCloud	Sí	Sí
Permitir Fotos de iCloud	Sí	Sí
Permitir Desbloqueo Automático	Sí	Sí
Permitir Touch ID para desbloquear Mac	Sí	Sí
Forzar actualizaciones de software retrasadas	No	Sí
Autorrelleno de contraseñas	No	Sí
Solicitudes de proximidad de contraseña	No	Sí
Compartir contraseña	Sí	Sí
Image Playground	No	Sí
Duplicación de iPhone	No	Sí
Herramientas de escritura	No	Sí
Permitir modificación de uso compartido de medios	Sí	Sí

- **Preferencias**

- **Restringir elementos en Preferencias del Sistema:** Permite o restringe el acceso de los usuarios a Preferencias del Sistema. El valor predeterminado es **Desactivado**, lo que permite a los usuarios acceso completo a Preferencias del Sistema. Si está activado, configure los siguientes ajustes.
  - **Panel de Preferencias del Sistema:** Seleccione si los ajustes que seleccione están activados o desactivados. El valor predeterminado es activar todos los ajustes, que están **Activados** de forma predeterminada.
    - Usuarios y grupos
    - General
    - Accesibilidad
    - App Store
    - Actualización de software
    - Bluetooth
    - CD y DVD
    - Fecha y hora
    - Escritorio y salvapantallas
    - Pantallas
    - Dock
    - Ahorro de energía
    - Extensiones
    - FibreChannel
    - iCloud
    - Tinta
    - Cuentas de Internet
    - Teclado
    - Idioma y Texto
    - Mission Control
    - Ratón
    - Red
    - Notificaciones

    - Controles parentales
    - Impresoras y Escáneres
    - Perfiles
    - Seguridad y Privacidad
    - Compartir
    - Sonido
    - Dictado y voz
    - Spotlight
    - Disco de arranque
    - Time Machine
    - Trackpad
    - Xsan

- **Aplicaciones**
    - **Permitir el uso de Game Center:** Permite a los usuarios jugar a juegos en línea a través de Game Center. El valor predeterminado es **Activado**.
    - **Permitir añadir amigos en Game Center:** Permite a los usuarios enviar una notificación a un amigo para jugar a un juego. El valor predeterminado es **Activado**.
    - **Permitir juegos multijugador:** Permite a los usuarios iniciar partidas multijugador. El valor predeterminado es **Activado**.
    - **Permitir la modificación de la cuenta de Game Center:** Permite a los usuarios modificar la configuración de su cuenta de Game Center. El valor predeterminado es **Activado**.
    - **Permitir la adopción de App Store:** Permite o restringe que App Store adopte aplicaciones preexistentes en OS X. El valor predeterminado es **Activado**.
    - **Permitir el autorrelleno de Safari:** Permite que Safari rellene automáticamente los campos de los sitios web con contraseñas, direcciones y otra información básica que haya almacenado. El valor predeterminado es **Activado**.
    - **Requerir contraseña de administrador para instalar o actualizar aplicaciones:** Requiere una contraseña de administrador para instalar o actualizar aplicaciones. El valor predeterminado es **Desactivado**, lo que significa que no se requiere ninguna contraseña de administrador.
    - **Restringir App Store solo a actualizaciones de software:** Restringe la App Store solo a las actualizaciones, lo que deshabilita todas las pestañas de la App Store excepto la de

Actualizaciones. El valor predeterminado es **Desactivado**, lo que permite el acceso completo a la App Store.

- **Restringir qué aplicaciones se pueden abrir:** Restringe o permite las aplicaciones que los usuarios pueden usar. El valor predeterminado es Desactivado, lo que permite usar todas las aplicaciones. Si está habilitado, configure los siguientes ajustes:
  - **Aplicaciones permitidas:** Haga clic en **Agregar**, introduzca el nombre y el ID de paquete de una aplicación que se permita iniciar y, a continuación, haga clic en **Guardar**. Para las aplicaciones de productividad móvil de Citrix, utilice el ID del campo **ID de paquete** al agregar la aplicación. Repita este paso para cada aplicación que se permita iniciar.
  - **Carpetas no permitidas:** Haga clic en **Agregar**, escriba la ruta de archivo de una carpeta a la que quiera restringir el acceso de los usuarios (por ejemplo, /Applications/Utilities) y, a continuación, haga clic en **Guardar**. Repita este paso para todas las carpetas a las que no quiera que los usuarios puedan acceder.
  - **Carpetas permitidas:** Haga clic en **Agregar**, escriba la ruta de archivo de una carpeta a la que quiera conceder acceso a los usuarios y, a continuación, haga clic en **Guardar**. Repita este paso para todas las carpetas a las que quiera que los usuarios puedan acceder.

- **Widgets**
  - **Permitir que solo se ejecuten los siguientes widgets de Dashboard:** Si está **Activado**, los usuarios solo pueden ejecutar los widgets de Dashboard configurados en este ajuste. El valor predeterminado es **Desactivado**, lo que permite a los usuarios ejecutar todos los widgets. Si está habilitado, configure el siguiente ajuste:
    - **Widgets permitidos:** Haga clic en **Agregar**, escriba el nombre y el ID de un widget que se permita ejecutar y, a continuación, haga clic en **Guardar**. Repita este paso para cada widget que quiera ejecutar en el Dashboard.
- **Multimedia**
  - **Permitir AirDrop:** Permite a los usuarios compartir fotos, vídeos, sitios web, ubicaciones y mucho más con dispositivos iOS cercanos.
- **Compartir**
  - **Habilitar automáticamente nuevos servicios para compartir:** Seleccione si desea habilitar automáticamente los servicios para compartir.

- **Correo:** Seleccione si desea permitir un buzón compartido.
- **Facebook:** Seleccione si desea permitir una cuenta de Facebook compartida.
- **Servicios de vídeo - Flickr, Vimeo, Tudou y Youku:** Seleccione si desea permitir los servicios de vídeo compartidos.
- **Añadir a Aperture:** Seleccione si desea permitir la capacidad compartida de añadir a Aperture.
- **Sina Weibo:** Seleccione si desea permitir una cuenta compartida de Sina Weibo.
- **Twitter:** Seleccione si desea permitir una cuenta compartida de Twitter.
- **Mensajes:** Seleccione si desea permitir el acceso compartido a los mensajes.
- **Añadir a iPhoto:** Seleccione si desea permitir la capacidad compartida de añadir a iPhoto.
- **Añadir a la lista de lectura:** Seleccione si desea permitir la capacidad compartida de añadir a la lista de lectura.
- **AirDrop:** Seleccione si desea permitir una cuenta compartida de AirDrop.

- **Funcionalidad**
  - **Bloquear imagen de escritorio:** Seleccione si los usuarios pueden cambiar la imagen de escritorio. El valor predeterminado es **Desactivado**, lo que significa que los usuarios pueden cambiar la imagen de escritorio.
  - **Permitir el uso de la cámara:** Seleccione si los usuarios pueden usar la cámara en sus Mac. El valor predeterminado es **Desactivado**, lo que significa que los usuarios no pueden usar la cámara.
  - **Permitir Apple Music:** Permita a los usuarios usar el servicio Apple Music (macOS 10.12 y posterior). Si no permite el servicio Apple Music, la aplicación Música se ejecuta en modo clásico. Se aplica solo a dispositivos supervisados. El valor predeterminado es **Activado**.
  - **Permitir sugerencias de Spotlight:** Seleccione si los usuarios pueden usar las sugerencias de Spotlight para buscar en su Mac y para proporcionar sugerencias de Spotlight desde Internet y la App Store. El valor predeterminado es **Desactivado**, lo que impide que los usuarios usen las sugerencias de Spotlight.
  - **Permitir búsqueda:** Seleccione si los usuarios pueden buscar las definiciones de palabras con el menú contextual o el menú de búsqueda de Spotlight. El valor predeterminado es Off, lo que impide que los usuarios usen la búsqueda en sus Mac.
  - **Permitir el uso de la contraseña de iCloud para cuentas locales:** Seleccione si los usuarios pueden usar su ID de Apple y su contraseña de iCloud para iniciar sesión en sus Mac. Habilitar esta política significa que los usuarios usan solo un ID y una contraseña

para *todas* las pantallas de inicio de sesión en sus Mac. El valor predeterminado es **Activado**, lo que permite a los usuarios usar su ID de Apple y su contraseña de iCloud para acceder a sus Mac.

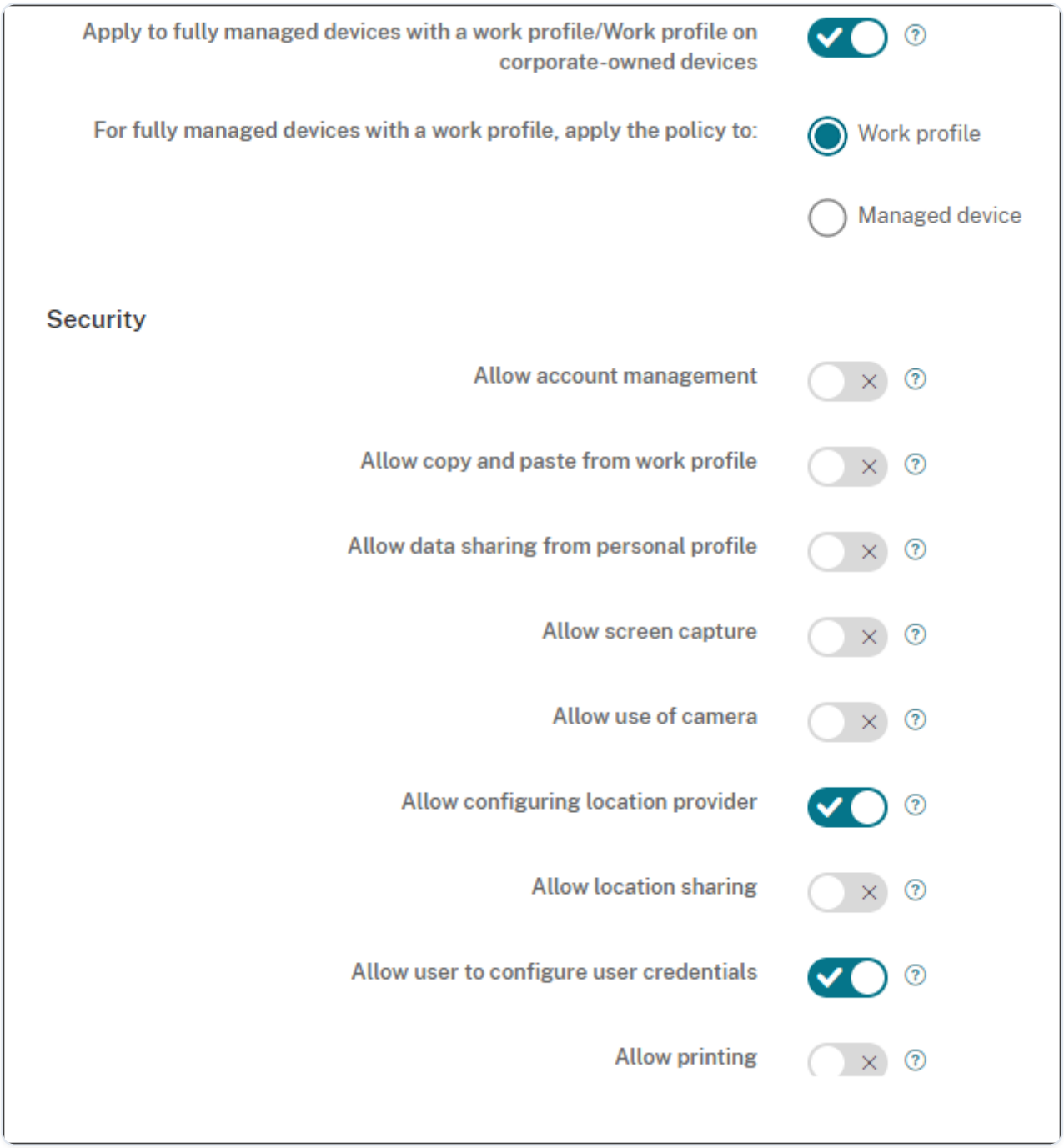
- **Permitir documentos y datos de iCloud:** Seleccione si desea permitir a los usuarios acceder a documentos y datos almacenados en iCloud en sus Mac. El valor predeterminado es **Activado**, lo que impide a los usuarios usar documentos y datos de iCloud en sus Mac.
  - **Permitir Escritorio y Documentos de iCloud:** (macOS 10.12.4 y posterior) El valor predeterminado está seleccionado.
- **Permitir sincronización de Llavero de iCloud:** Permitir la sincronización del Llavero de iCloud (macOS 10.12 y posterior). El valor predeterminado es **Activado**.
- **Permitir Mail de iCloud:** Permitir a los usuarios usar Mail de iCloud (macOS 10.12 y posterior). El valor predeterminado es **Activado**.
- **Permitir Contactos de iCloud:** Permitir a los usuarios usar Contactos de iCloud (macOS 10.12 y posterior). El valor predeterminado es **Activado**.
- **Permitir Calendarios de iCloud:** Permitir a los usuarios usar Calendarios de iCloud (macOS 10.12 y posterior). El valor predeterminado es **Activado**.
- **Permitir Recordatorios de iCloud:** Permitir a los usuarios usar Recordatorios de iCloud (macOS 10.12 y posterior). El valor predeterminado es **Activado**.
- **Permitir Marcadores de iCloud:** Permitir a los usuarios sincronizar con Marcadores de iCloud (macOS 10.12 y posterior). El valor predeterminado es **Activado**.
- **Permitir Notas de iCloud:** Permitir a los usuarios usar Notas de iCloud (macOS 10.12 y posterior). El valor predeterminado es **Activado**.
- **Permitir Fotos de iCloud:** Si cambia esta configuración a **Desactivado**, cualquier foto que no se haya descargado completamente de la Fototeca de iCloud se eliminará del almacenamiento local del dispositivo (macOS 10.12 y posterior). El valor predeterminado es **Activado**.
- **Permitir Desbloqueo Automático:** Para obtener información sobre esta opción y el Apple Watch, consulte https://www.imore.com/auto-unlock (macOS 10.12 y posterior). El valor predeterminado es **Activado**.
- **Permitir Touch ID para desbloquear Mac:** (macOS 10.12.4 y posterior). El valor predeterminado es **Activado**.

- **Forzar actualizaciones de software retrasadas:** Si está **Activado**, esta configuración retrasa la visibilidad de las actualizaciones de software para el usuario. Los usuarios no ven una actualización de software hasta el número de días especificado después de la fecha de lanzamiento de la actualización de software. El valor predeterminado es **Desactivado**. Disponible solo para dispositivos supervisados que ejecutan macOS 10.13.4 y posterior. La directiva de actualización del SO tiene más configuraciones para controlar la frecuencia con la que los dispositivos reciben actualizaciones. Consulte Directiva de dispositivo de actualización del SO.
- **Retraso forzado de la actualización de software (días):** Especifica cuántos días se debe retrasar una actualización de software en el dispositivo. El máximo es de 90 días. El valor predeterminado es **30**. Disponible solo para dispositivos supervisados que ejecutan macOS 10.13.4 y posterior.
- **Autorrelleno de contraseñas:** Opcional. Si está deshabilitado, los usuarios no pueden usar las funciones de Autorrelleno de contraseñas o Contraseñas seguras automáticas. El valor predeterminado es **Activado**. (macOS 10.14 y posterior)
- **Solicitudes de proximidad de contraseña:** Opcional. Si está deshabilitado, los dispositivos de los usuarios no solicitan contraseñas de dispositivos cercanos. El valor predeterminado es **Activado**. (macOS 10.14 y versiones posteriores)
- **Compartir contraseña:** Opcional. Si está deshabilitado, los usuarios no pueden compartir sus contraseñas mediante la función Contraseñas de AirDrop. El valor predeterminado es **Activado**. (macOS 10.14 y versiones posteriores)
- **Image Playground:** Si está **Desactivado**, prohíbe el uso de la generación de imágenes. El valor predeterminado es **Activado**. Disponible solo para dispositivos supervisados que ejecuten macOS 15 y versiones posteriores.
- **Duplicación de iPhone:** Si está **Desactivado**, prohíbe el uso de la duplicación de iPhone. Cuando se usa en macOS, esto evita que el Mac duplique cualquier iPhone. El valor predeterminado es **Activado**. Disponible solo para dispositivos supervisados que ejecuten macOS 15 y versiones posteriores.
- **Herramientas de escritura:** Si está **Desactivado**, deshabilita las herramientas de escritura de Apple Intelligence. El valor predeterminado es **Activado**. Disponible solo para dispositivos supervisados que ejecuten macOS 15 y versiones posteriores.
- **Permitir modificación de uso compartido de medios:** Si está **Desactivado**, impide la modificación de la configuración de uso compartido de medios. El valor predeterminado es **Activado**. Disponible para macOS 15.1 y versiones posteriores.

Configuración de Android

- **Cámara:** Permite a los usuarios usar la cámara en sus dispositivos. Si está **Desactivado**, la cámara se deshabilita. El valor predeterminado es **Activado**.

Configuración de Android Enterprise



Cuando un dispositivo Android nuevo o restablecido de fábrica se inscribe en el modo de perfil de trabajo, los dispositivos que ejecutan Android 9.0-10.x se inscriben como dispositivos totalmente administrados con un perfil de trabajo. Los dispositivos que ejecutan Android 11+ se inscriben

como perfil de trabajo en dispositivos propiedad de la empresa. La directiva de restricciones se puede aplicar al perfil de trabajo del dispositivo o al dispositivo administrado.

En los dispositivos inscritos en el modo de perfil de trabajo en dispositivos propiedad de la empresa, las siguientes restricciones no funcionan:

- Permitir servicio de copia de seguridad
- Habilitar aplicaciones del sistema
- Evitar que el bloqueo de pantalla bloquee el dispositivo
- Permitir el uso de la barra de estado
- Mantener la pantalla del dispositivo encendida
- Permitir al usuario controlar la configuración de la aplicación
- Permitir al usuario configurar las credenciales de usuario
- Permitir la configuración de VPN
- Permitir el almacenamiento masivo USB
- Permitir el restablecimiento de fábrica
- Permitir la desinstalación de aplicaciones
- Permitir aplicaciones que no sean de Google Play
- Permitir copiar y pegar entre perfiles
- Habilitar la verificación de aplicaciones
- Permitir la administración de cuentas
- Permitir la impresión
- Permitir NFC
- Permitir añadir usuarios

De forma predeterminada, las opciones **Depuración USB y Orígenes desconocidos** están inhabilitadas en un dispositivo cuando se inscribe en Android Enterprise en el modo de perfil de trabajo.

Vea este vídeo para obtener más información:



- **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos corporativos:** Permite configurar los ajustes de la directiva de restricciones

para dispositivos totalmente administrados con perfiles de trabajo. Estos dispositivos también se conocen como dispositivos COPE (propiedad de la empresa, habilitados para uso personal). Cuando esta opción está en **On**, seleccione uno de estos ajustes:

- **Perfil de trabajo:** Los ajustes de restricciones que configure se aplican solo al perfil de trabajo del dispositivo.
- **Dispositivo administrado:** Los ajustes de restricciones que configure se aplican solo al dispositivo.

Cuando esta opción está en **Off**, los ajustes de credenciales que configure se aplican al dispositivo, excepto los ajustes que se aplican explícitamente al perfil de trabajo. El valor predeterminado es **Off**.

Cuando **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos corporativos** está desactivado, configure los siguientes ajustes:

- **Seguridad**
  - **Permitir la administración de cuentas:** Permite agregar una cuenta a los dispositivos administrados y al perfil de trabajo. El valor predeterminado es **Off**.
  - **Permitir copiar y pegar desde el perfil de trabajo:** Si está en **On**, los usuarios pueden copiar y pegar datos de las aplicaciones del perfil de trabajo a las aplicaciones del perfil personal. El valor predeterminado es **Off**.
  - **Permitir el uso compartido de datos desde el perfil personal:** Si está en **On**, los usuarios pueden copiar, pegar y compartir archivos y datos de las aplicaciones del perfil personal a las aplicaciones del perfil de trabajo. El valor predeterminado es **Off**.
  - **Permitir captura de pantalla:** Permite a los usuarios grabar o tomar una captura de pantalla del dispositivo. El valor predeterminado es **Off**.
  - **Permitir el uso de la cámara:** Permite a los usuarios tomar fotografías y grabar vídeos con la cámara del dispositivo. El valor predeterminado es **Off**.
  - **Permitir la configuración de VPN:** Permite a los usuarios crear configuraciones de VPN. Para dispositivos con perfil de trabajo con Android 6 y versiones posteriores y para dispositivos totalmente administrados. El valor predeterminado es **On**.
  - **Permitir servicio de copia de seguridad:** Permite a los usuarios hacer copias de seguridad de los datos de las aplicaciones y del sistema en sus dispositivos. El valor predeterminado es **Activado**.

- **Permitir NFC:** Permite a los usuarios enviar páginas web, fotos, vídeos u otro contenido desde sus dispositivos a otro dispositivo mediante la comunicación de campo cercano (NFC). Para MDM 4.0 y versiones posteriores. El valor predeterminado es **Activado**.
- **Permitir configurar el proveedor de ubicación:** Permite a los usuarios activar el GPS en sus dispositivos. Para Android API 28 y versiones posteriores. El valor predeterminado es **Activado**.
- **Permitir compartir ubicación:** Para los perfiles administrados, el propietario del dispositivo puede anular esta configuración. El valor predeterminado es **Desactivado**.

> **Sugerencia:**
>
> Puede crear directivas de dispositivo de ubicación en Citrix Endpoint Management para aplicar límites geográficos. Consulte Directiva de dispositivo de ubicación.

- **Permitir al usuario configurar credenciales de usuario:** Especifica si los usuarios pueden configurar credenciales en el almacén de claves administrado. El valor predeterminado es **Activado**.
- **Permitir impresión:** Si está **Activado**, la configuración permite a los usuarios imprimir en cualquier impresora accesible desde el dispositivo de usuario. El valor predeterminado es **Desactivado**. Disponible para: Android 9 y versiones posteriores.
- **Permitir depuración USB:** El valor predeterminado es **Desactivado**.

- **Aplicaciones**
  - **Habilitar aplicaciones del sistema:** Permite a los usuarios ejecutar aplicaciones de dispositivo preinstaladas. El valor predeterminado es **Desactivado**. Para habilitar aplicaciones específicas, haga clic en **Agregar** en la tabla **Lista de aplicaciones del sistema**.
    - **Lista de aplicaciones del sistema:** Una lista de las aplicaciones del sistema que desea habilitar en el dispositivo. Establezca **Habilitar aplicaciones del sistema** en **Activado** y agregue el nombre del paquete de la aplicación. Para buscar el nombre del paquete de una aplicación del sistema, puede usar Android Debug Bridge (`adb`) para llamar al comando del administrador de paquetes de Android (`pm`). Por ejemplo, `adb shell "pm list packages -f name"`, donde "name" forma parte del nombre del paquete. Para obtener más información, consulte `<https://developer.android.com/studio/command-line/adb>`. Para dispositivos Android

Enterprise, puede restringir los permisos de las aplicaciones mediante la directiva Permisos de aplicaciones de Android Enterprise.

- **Inhabilitar aplicaciones:** Bloquea una lista especificada de aplicaciones para que no se ejecuten en los dispositivos. El valor predeterminado es **Desactivado**. Para inhabilitar una aplicación instalada, cambie la configuración a **Activado** y, a continuación, haga clic en **Agregar** en la tabla **Lista de aplicaciones**.
  - **Lista de aplicaciones:** Una lista de las aplicaciones que desea bloquear. Establezca **Inhabilitar aplicaciones** en **Activado** y agregue la aplicación. Escriba el nombre del paquete de la aplicación. Al cambiar e implementar una lista de aplicaciones, se sobrescribe la lista de aplicaciones anterior. Por ejemplo: Si inhabilita com.example1 y com.example2, y luego cambia la lista a com.example1 y com.example3, Citrix Endpoint Management habilita com.example.2.
- **Aplicaciones de administrador de credenciales:** Controla si una aplicación puede actuar como proveedor de credenciales. El valor predeterminado es **Desactivado**. Si esta configuración está **Activada**, los usuarios pueden elegir un tipo de directiva de paquete y, a continuación, hacer clic en **Agregar** en la tabla **Lista de aplicaciones de proveedor de credenciales** para agregar una aplicación por nombre de paquete. Esta función está disponible en Android 14 y versiones posteriores y requiere Secure Hub versión 26.5.0 o posterior.
  - **Tipo de política de paquete:** Especifica qué proveedores de credenciales están permitidos o bloqueados. La opción predeterminada es **Permitir lista y paquetes del sistema**, que permite el acceso desde los proveedores de credenciales predeterminados del OEM y la lista de permitidos de proveedores de credenciales. Otras opciones son **Solo lista de permitidos**, que limita los proveedores de credenciales que los usuarios pueden usar a los paquetes de la política, y **Lista de bloqueados**, que impide que los usuarios utilicen los proveedores de credenciales enumerados en la política.
  - **Lista de aplicaciones de proveedor de credenciales:** Para permitir o bloquear una aplicación como proveedor de credenciales según el tipo de política de paquete, haga clic en **Agregar**, escriba el nombre del paquete de la aplicación y haga clic en **Guardar**. Repita el proceso para cada aplicación que desee agregar.
- **Habilitar verificación de aplicaciones:** Permite que el sistema operativo escanee las aplicaciones para detectar comportamientos maliciosos. El valor predeterminado es **Activado**.

- **Habilitar aplicaciones de Google:** Permite a los usuarios descargar aplicaciones de Google Mobile Services en el dispositivo. El valor predeterminado es **Activado**.
- **Permitir aplicaciones que no sean de Google Play:** Permite la instalación de aplicaciones de tiendas que no sean Google Play. El valor predeterminado es **Desactivado**.
- **Permitir aplicaciones que no sean de Google Play para todos los perfiles:** Si está **Activado**, los usuarios pueden instalar aplicaciones de tiendas que no sean Google Play en todos los perfiles del dispositivo. El valor predeterminado es **Desactivado**.
- **Permitir control de usuario de la configuración de aplicaciones:** Permite a los usuarios desinstalar aplicaciones, deshabilitar aplicaciones, borrar caché y datos, forzar la detención de cualquier aplicación y borrar valores predeterminados. Los usuarios realizan estas acciones desde la aplicación Configuración. El valor predeterminado es **Desactivado**.
- **Permitir desinstalación de aplicaciones:** Permite a los usuarios desinstalar aplicaciones desde Managed Google Play Store. El valor predeterminado es **Desactivado**.

- **Perfil de trabajo BYOD**
  - **Habilitar aplicaciones conectadas:** Si está habilitado, los usuarios pueden seleccionar aplicaciones que pueden comunicarse entre perfiles de trabajo y personales, utilizando datos tanto de trabajo como personales. Después de habilitar, haga clic en **Agregar**, seleccione las aplicaciones deseadas y luego haga clic en **Guardar**. Se requiere un perfil de trabajo para habilitar esta función. El valor predeterminado es **Desactivado**.
  - **Permitir widgets de aplicaciones de perfil de trabajo en la pantalla de inicio:** Si esta configuración está **Activada**, los usuarios pueden colocar widgets de aplicaciones de perfil de trabajo en la pantalla de inicio del dispositivo. Si esta configuración está **Desactivada**, los usuarios no pueden colocar widgets de aplicaciones de perfil de trabajo en la pantalla de inicio del dispositivo. El valor predeterminado es **Desactivado**.
    - **Aplicaciones con widgets permitidos:** Una lista de las aplicaciones que desea permitir en la pantalla de inicio. Establezca **Permitir widgets de aplicaciones de perfil de trabajo en la pantalla de inicio** en **Activado** y agregue la aplicación. Haga clic en **Agregar** y seleccione una aplicación cuyos widgets desea permitir en la pantalla de inicio de la lista. Haga clic en **Guardar**. Repita ese proceso para permitir más widgets de aplicaciones.
  - **Permitir contactos del perfil de trabajo en los contactos del dispositivo:** Muestra los contactos del perfil de Android Enterprise administrado en el perfil principal, para llamadas entrantes (Android 7.0 y posterior). El valor predeterminado es **Desactivado**.

- **Solo dispositivo totalmente administrado**
  - **Permitir agregar usuarios:** Permite a los usuarios agregar nuevos usuarios en un dispositivo. El valor predeterminado es **Activado**.
  - **Permitir itinerancia de datos:** Permite a los usuarios usar datos móviles en itinerancia. El valor predeterminado es Desactivado, lo que deshabilita la itinerancia en los dispositivos de los usuarios. El valor predeterminado es **Desactivado**.
  - **Permitir SMS:** Permite a los usuarios enviar y recibir mensajes SMS. El valor predeterminado es **Desactivado**.
  - **Permitir el uso de la barra de estado:** Si está **Activado**, esta opción habilita la barra de estado en los dispositivos administrados y los dispositivos dedicados (también conocidos como dispositivos COSU). Esta opción deshabilita las notificaciones, la configuración rápida y otras superposiciones de pantalla que permiten salir del modo de pantalla completa. Los usuarios pueden ir a la configuración del sistema y ver las notificaciones. Para Android 6.0 y versiones posteriores. El valor predeterminado es **Desactivado**.
  - **Permitir Bluetooth:** Permite a los usuarios usar Bluetooth. El valor predeterminado es **Activado**.
    - **Permitir compartir por Bluetooth:** Si no está seleccionada, los usuarios no pueden establecer el uso compartido saliente de Bluetooth en su dispositivo. El valor predeterminado es seleccionado.
  - **Permitir configurar fecha y hora:** Permite a los usuarios cambiar la fecha y la hora en sus dispositivos. El valor predeterminado es **Activado**.
  - **Permitir restablecimiento de fábrica:** Permite a los usuarios realizar un restablecimiento de fábrica en sus dispositivos. El valor predeterminado es **Activado**.
  - **Mantener la pantalla del dispositivo encendida:** Si esta opción está configurada en **Activado**, la pantalla del dispositivo permanece encendida cuando el dispositivo está enchufado. El valor predeterminado es **Desactivado**.
  - **Permitir almacenamiento masivo USB:** Permite la transferencia de archivos de datos grandes entre los dispositivos de los usuarios y un equipo a través de una conexión USB. El valor predeterminado es **Activado**.
  - **Permitir micrófono:** Permite a los usuarios usar el micrófono en sus dispositivos. El valor predeterminado es **Activado**.
  - **Permitir anclaje a red:** Permite a los usuarios configurar puntos de acceso portátiles y anclar datos. El valor predeterminado es **Desactivado**.

- **Evitar que el bloqueo de pantalla bloquee el dispositivo:** Si está **Activado**, esta opción deshabilita el bloqueo de pantalla en la pantalla de bloqueo de los dispositivos administrados y los dispositivos dedicados (también conocidos como dispositivos COSU). El valor predeterminado es **Desactivado**.
- **Permitir cambios de Wi-Fi:** Si está **Activado**, los usuarios pueden activar o desactivar Wi-Fi y conectarse a redes Wi-Fi. El valor predeterminado es **Activado**.
- **Permitir transferencia de archivos:** Permite transferencias de archivos a través de USB. El valor predeterminado es **Desactivado**.

- **Samsung**
  - **Habilitar TIMA Keystore:** El TIMA Keystore proporciona almacenamiento seguro de claves basado en TrustZone para las claves simétricas. Los pares de claves RSA y los certificados se dirigen al proveedor de almacén de claves predeterminado para su almacenamiento. El valor predeterminado es **Desactivado**.
  - **Permitir lista de compartir:** Permite a los usuarios compartir contenido entre aplicaciones en la lista Compartir mediante. El valor predeterminado es **Activado**.
  - **Habilitar registro de auditoría:** Permite la creación de registros de auditoría de eventos para el análisis forense de un dispositivo. El valor predeterminado es **Desactivado**.

- **Samsung: Solo dispositivos totalmente administrados**
  - **Permitir solo llamadas de emergencia:** Permite a los usuarios habilitar el modo Solo llamadas de emergencia en sus dispositivos. El valor predeterminado es **Desactivado**.
  - **Permitir recuperación de firmware:** Permite a los usuarios recuperar el firmware de sus dispositivos. El valor predeterminado es **Activado**.
  - **Permitir cifrado rápido:** Permite el cifrado solo del espacio de memoria utilizado. Este cifrado contrasta con el cifrado de disco completo, que cifra todos los datos. Esos datos incluyen configuraciones, datos de aplicaciones, archivos y aplicaciones descargados, medios y otros archivos. El valor predeterminado es **Activado**.
  - **Habilitar modo de Criterios Comunes:** Pone el dispositivo en modo de Criterios Comunes. La configuración de Criterios Comunes aplica procesos de seguridad estrictos. El valor predeterminado es **Activado**.
  - **Habilitar banner de reinicio:** Muestra un mensaje de notificación o banner de uso del sistema aprobado por el DoD cuando se reinician los dispositivos de los usuarios. El valor predeterminado es **Desactivado**.

- **Permitir cambios de configuración:** Permite a los usuarios cambiar la configuración en sus dispositivos totalmente administrados. El valor predeterminado es **Activado**.
- **Habilitar uso de datos en segundo plano:** Permite que las aplicaciones sincronicen datos en segundo plano. Para dispositivos totalmente administrados. El valor predeterminado es **Activado**.
- **Permitir portapapeles:** Permite a los usuarios copiar datos al portapapeles de sus dispositivos.
  - **Permitir compartir portapapeles:** Permite a los usuarios compartir contenido del portapapeles entre sus dispositivos y un equipo (MDM 4.0 y posterior).
- **Permitir tecla de inicio:** Permite a los usuarios usar la tecla **Inicio** en sus dispositivos totalmente administrados. El valor predeterminado es **Activado**.
- **Permitir ubicación simulada:** Permite a los usuarios falsificar su ubicación GPS. Para dispositivos totalmente administrados. El valor predeterminado es **Desactivado**.
- **NFC:** Permite a los usuarios usar NFC en sus dispositivos totalmente administrados (MDM 3.0 y versiones posteriores). El valor predeterminado es **Activado**.
- **Permitir apagar:** Permite a los usuarios apagar sus dispositivos totalmente administrados (MDM 3.0 y versiones posteriores). El valor predeterminado es **Activado**.
- **Permitir Wi-Fi Direct:** Permite a los usuarios conectarse directamente a otro dispositivo a través de su conexión Wi-Fi. El valor predeterminado es **Activado**. Si está **Activado**, debe habilitar la configuración **Permitir cambios de Wi-Fi**.
- **Permitir tarjeta SD:** Permite a los usuarios usar una tarjeta SD, si está disponible, con sus dispositivos. El valor predeterminado es **Activado**.
- **Permitir almacenamiento de host USB:** Permite que los dispositivos de los usuarios actúen como host USB cuando un dispositivo USB se conecta a sus dispositivos. Los dispositivos de los usuarios suministran energía al dispositivo USB. El valor predeterminado es **Activado**.
- **Permitir marcador de voz:** Permite a los usuarios usar el marcador de voz en sus dispositivos (MDM 4.0 y versiones posteriores). El valor predeterminado es **Activado**.
- **Permitir S Beam:** Permite a los usuarios compartir contenido con otros mediante NFC y Wi-Fi Direct (MDM 4.0 y versiones posteriores). El valor predeterminado es **Activado**.
- **Permitir S Voice:** Permite a los usuarios usar el asistente personal inteligente y el navegador de conocimientos en sus dispositivos (MDM 4.0 y versiones posteriores). El valor predeterminado es **Activado**.

- **Permitir anclaje a red USB:** Permite a los usuarios compartir una conexión de datos móviles con otro dispositivo mediante su conexión USB. El valor predeterminado es **Desactivado**. Si está **Activado**, la configuración **Permitir anclaje a red** también debe estar **Activada**.
- **Permitir anclaje a red Bluetooth:** Permite a los usuarios compartir una conexión de datos móviles con otro dispositivo mediante su conexión Bluetooth. El valor predeterminado es **Desactivado**. Si está **Activado**, la configuración **Permitir anclaje a red** también debe estar **Activada**.
  - **Permitir compartir por Bluetooth:** Si no está seleccionada, los usuarios no pueden establecer el uso compartido saliente de Bluetooth en su dispositivo. El valor predeterminado es seleccionado.
- **Permitir anclaje a red Wi-Fi:** Permite a los usuarios compartir una conexión de datos móviles con otro dispositivo mediante su conexión Wi-Fi. El valor predeterminado es **Desactivado**. Si está **Activado**, la configuración **Permitir anclaje a red** también debe estar **Activada**.
- **Permitir MMS entrantes:** Permite a los usuarios recibir mensajes MMS. El valor predeterminado es **Desactivado**. Si está **Activado**, debe activar la configuración **Permitir SMS**.
- **Permitir MMS salientes:** Permite a los usuarios enviar mensajes MMS. El valor predeterminado es **Desactivado**. Si está **Activado**, debe activar la configuración **Permitir SMS**.
- **Permitir SMS entrantes:** Permite a los usuarios recibir mensajes SMS. El valor predeterminado es **Desactivado**. Si está **Activado**, debe activar la configuración **Permitir SMS**.
- **Permitir SMS salientes:** Permite a los usuarios enviar mensajes SMS. El valor predeterminado es **Desactivado**. Si está **Activado**, debe activar la configuración **Permitir SMS**.
- **Configurar redes móviles:** Permite a los usuarios usar su conexión de datos móviles. El valor predeterminado es **Desactivado**.
- **Límite diario (MB):** Introduzca el número de MB de datos móviles que los usuarios pueden usar cada día. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y posterior).

- **Límite semanal (MB):** Introduzca el número de MB de datos móviles que los usuarios pueden usar cada semana. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y posterior).
- **Límite mensual (MB):** Introduzca el número de MB de datos móviles que los usuarios pueden usar cada mes. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y posterior).
- **Permitir solo conexiones VPN seguras:** Permite a los usuarios usar solo conexiones seguras (MDM 4.0 y posterior). El valor predeterminado es **Activado**.
- **Permitir grabación de audio:** Permite a los usuarios grabar audio con sus dispositivos (MDM 4.0 y posterior). El valor predeterminado es **Activado**. Si está **Activado**, debe activar la configuración **Permitir micrófono**.
- **Permitir grabación de vídeo:** Permite a los usuarios grabar vídeo con sus dispositivos (MDM 4.0 y posterior). El valor predeterminado es **Desactivado**. Si está **Activado**, debe activar la configuración **Permitir el uso de la cámara**.
- **Permitir mensajes push en itinerancia:** Permite a los usuarios usar datos móviles para el envío de notificaciones. El valor predeterminado es **Desactivado**. Si está **Activado**, debe habilitar la configuración **Permitir itinerancia de datos**.
- **Permitir sincronización automática en itinerancia:** Permite a los usuarios usar datos móviles para la sincronización. El valor predeterminado es **Desactivado**. Si está **Activado**, debe habilitar la configuración **Permitir itinerancia de datos**.
- **Permitir llamadas de voz en itinerancia:** Permite a los usuarios usar datos móviles para llamadas de voz. El valor predeterminado es **Desactivado**. Si está **Activado**, debe habilitar la configuración **Permitir itinerancia de datos**.

Cuando **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos corporativos** está activado y **Para dispositivos totalmente administrados con un perfil de trabajo, aplicar la directiva a** está establecido en **Perfil de trabajo**, configure estos ajustes:

- **Seguridad**
  - **Permitir administración de cuentas:** Permite agregar una cuenta al perfil de trabajo y a los dispositivos administrados. El valor predeterminado es **Desactivado**.
  - **Permitir copiar y pegar entre perfiles:** Si está **Activado**, los usuarios pueden copiar y pegar entre aplicaciones del perfil de Android Enterprise y aplicaciones del área personal. El valor predeterminado es **Desactivado**.

- **Permitir captura de pantalla:** Permite a los usuarios grabar o hacer una captura de pantalla del dispositivo. El valor predeterminado es **Desactivado**.
- **Permitir el uso de la cámara:** Permite a los usuarios tomar fotos y grabar vídeos con la cámara del dispositivo. El valor predeterminado es **Desactivado**.
- **Permitir la configuración del proveedor de ubicación:** Permite a los usuarios activar el GPS en sus dispositivos. Para Android API 28 y posteriores. El valor predeterminado es **Activado**.
- **Permitir compartir la ubicación:** Para los perfiles administrados, el propietario del dispositivo puede anular esta configuración. El valor predeterminado es **Desactivado**.

> **Sugerencia:**
>
> Puede crear directivas de dispositivo de ubicación en Citrix Endpoint Management para aplicar límites geográficos. Consulte Directiva de dispositivo de ubicación.

- **Permitir al usuario configurar las credenciales de usuario:** Especifica si los usuarios pueden configurar credenciales en el almacén de claves administrado. El valor predeterminado es **Activado**.
- **Permitir impresión:** Si está **Activado**, la configuración permite a los usuarios imprimir en cualquier impresora accesible desde el dispositivo del usuario. El valor predeterminado es **Desactivado**. Disponible para: Android 9 y posteriores.

- **Aplicaciones**
  - **Habilitar aplicaciones del sistema:** Permite a los usuarios ejecutar aplicaciones preinstaladas en el dispositivo. El valor predeterminado es **Desactivado**. Para habilitar aplicaciones específicas, haga clic en **Agregar** en la tabla **Lista de aplicaciones del sistema**.
    - **Lista de aplicaciones del sistema:** Una lista de las aplicaciones del sistema que desea habilitar en el dispositivo. Establezca **Habilitar aplicaciones del sistema** en **Activado** y agregue el nombre del paquete de la aplicación. Para buscar el nombre del paquete de una aplicación del sistema, puede usar Android Debug Bridge (`adb`) para llamar al comando del administrador de paquetes de Android (`pm`). Por ejemplo, `adb shell "pm list packages -f name"`, donde "nombre" forma parte del nombre del paquete. Para obtener más información, consulte `<https://developer.android.com/studio/command-line/adb>`. Para dispositivos Android

Enterprise, puede restringir los permisos de las aplicaciones mediante la directiva Permisos de aplicaciones de Android Enterprise.

- **Inhabilitar aplicaciones:** Bloquea una lista específica de aplicaciones para que no se ejecuten en los dispositivos. El valor predeterminado es **Desactivado**. Para inhabilitar una aplicación instalada, cambie la configuración a **Activado** y, a continuación, haga clic en **Agregar** en la tabla **Lista de aplicaciones**.
  - **Lista de aplicaciones:** Una lista de las aplicaciones que desea bloquear. Establezca **Inhabilitar aplicaciones** en **Activado** y agregue la aplicación. Escriba el nombre del paquete de la aplicación. Al cambiar e implementar una lista de aplicaciones, se sobrescribe la lista de aplicaciones anterior. Por ejemplo: Si inhabilita com.example1 y com.example2, y luego cambia la lista a com.example1 y com.example3, Citrix Endpoint Management habilita com.example.2.
- **Aplicaciones de administrador de credenciales:** Controla si una aplicación puede actuar como proveedor de credenciales. El valor predeterminado es **Desactivado**. Si esta configuración está **Activada**, los usuarios pueden elegir un tipo de directiva de paquete y, a continuación, hacer clic en **Agregar** en la tabla **Lista de aplicaciones de proveedor de credenciales** para agregar una aplicación por nombre de paquete. Esta función está disponible en Android 14 y versiones posteriores y requiere Secure Hub versión 26.5.0 o posterior.
  - **Tipo de directiva de paquete:** Especifica qué proveedores de credenciales están permitidos o bloqueados. La opción predeterminada es **Lista de permitidos y paquetes del sistema**, que permite el acceso de los proveedores de credenciales predeterminados del OEM y la lista de permitidos de proveedores de credenciales. Otras opciones son **Solo lista de permitidos**, que limita los proveedores de credenciales que los usuarios pueden usar a los paquetes de la directiva, y **Lista de bloqueados**, que bloquea el uso por parte de los usuarios de los proveedores de credenciales enumerados en la directiva.
  - **Lista de aplicaciones de proveedor de credenciales:** Para permitir o bloquear una aplicación como proveedor de credenciales según el tipo de política de paquete, haga clic en **Agregar**, escriba el nombre del paquete de la aplicación y haga clic en **Guardar**. Repita este proceso para cada aplicación que desee agregar.
- **Habilitar verificación de aplicaciones:** Permite que el sistema operativo analice las aplicaciones para detectar comportamientos maliciosos. El valor predeterminado es **Activado**.

- **Habilitar aplicaciones de Google:** Permite a los usuarios descargar aplicaciones de Google Mobile Services en el dispositivo. El valor predeterminado es **Activado**.
- **Permitir aplicaciones que no sean de Google Play:** Permite la instalación de aplicaciones de tiendas que no sean Google Play. El valor predeterminado es **Desactivado**.
- **Permitir al usuario controlar la configuración de las aplicaciones:** Permite a los usuarios desinstalar aplicaciones, deshabilitar aplicaciones, borrar la caché y los datos, forzar la detención de cualquier aplicación y borrar los valores predeterminados. Los usuarios realizan estas acciones desde la aplicación Configuración. El valor predeterminado es **Desactivado**.
- **Permitir desinstalación de aplicaciones:** Permite a los usuarios desinstalar aplicaciones desde Managed Google Play Store. El valor predeterminado es **Desactivado**.

- **Perfil de trabajo BYOD**
  - **Permitir widgets de aplicaciones de perfil de trabajo en la pantalla de inicio:** Si esta opción está **Activada**, los usuarios pueden colocar widgets de aplicaciones de perfil de trabajo en la pantalla de inicio del dispositivo. Si esta opción está **Desactivada**, los usuarios no pueden colocar widgets de aplicaciones de perfil de trabajo en la pantalla de inicio del dispositivo. El valor predeterminado es **Desactivado**.
    - **Aplicaciones con widgets permitidos:** Una lista de las aplicaciones que desea permitir en la pantalla de inicio. Establezca **Permitir widgets de aplicaciones de perfil de trabajo en la pantalla de inicio** en **Activado** y agregue la aplicación. Haga clic en **Agregar** y seleccione una aplicación cuyos widgets desee permitir en la pantalla de inicio de la lista. Haga clic en **Guardar**. Repita ese proceso para permitir más widgets de aplicaciones.
  - **Permitir contactos del perfil de trabajo en los contactos del dispositivo:** Muestra los contactos del perfil administrado de Android Enterprise en el perfil principal, para llamadas entrantes (Android 7.0 y versiones posteriores). El valor predeterminado es **Desactivado**.
- **Samsung**
  - **Habilitar TIMA Keystore:** TIMA Keystore proporciona almacenamiento seguro de claves basado en TrustZone para las claves simétricas. Los pares de claves RSA y los certificados se dirigen al proveedor de almacén de claves predeterminado para su almacenamiento. El valor predeterminado es **Desactivado**.

- **Permitir lista de compartir:** Permite a los usuarios compartir contenido entre aplicaciones en la lista Compartir mediante. El valor predeterminado es **Activado**.
- **Habilitar registro de auditoría:** Permite la creación de registros de auditoría de eventos para el análisis forense de un dispositivo. El valor predeterminado es **Desactivado**.

Cuando **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos corporativos** está activado y **Para dispositivos totalmente administrados con un perfil de trabajo, aplicar la política a** está establecido en **Dispositivo administrado**, configure estos ajustes:

- **Seguridad**
  - **Permitir la administración de cuentas:** Permite agregar una cuenta al perfil de trabajo y a los dispositivos administrados. El valor predeterminado es **Desactivado**.
  - **Permitir copiar y pegar entre perfiles:** Si está en **Activado**, los usuarios pueden copiar y pegar entre aplicaciones del perfil de Android Enterprise y aplicaciones del área personal. El valor predeterminado es **Desactivado**.
  - **Permitir la captura de pantalla:** Permite a los usuarios grabar o tomar una captura de pantalla del dispositivo. El valor predeterminado es **Desactivado**.
  - **Permitir el uso de la cámara:** Permite a los usuarios tomar fotos y grabar vídeos con la cámara del dispositivo. El valor predeterminado es **Desactivado**.
  - **Permitir la configuración de VPN:** Permite a los usuarios crear configuraciones de VPN. Para dispositivos con perfil de trabajo que ejecutan Android 6 y versiones posteriores, y para dispositivos totalmente administrados. El valor predeterminado es **Activado**.
  - **Permitir el servicio de copia de seguridad:** Permite a los usuarios hacer copias de seguridad de las aplicaciones y los datos del sistema en sus dispositivos. El valor predeterminado es **Activado**.
  - **Permitir NFC:** Permite a los usuarios enviar páginas web, fotos, vídeos u otro contenido de sus dispositivos a otro dispositivo mediante la comunicación de campo cercano (NFC). Para MDM 4.0 y versiones posteriores. El valor predeterminado es **Activado**.
  - **Permitir la configuración del proveedor de ubicación:** Permite a los usuarios activar el GPS en sus dispositivos. Para Android API 28 y versiones posteriores. El valor predeterminado es **Activado**.
  - **Permitir compartir ubicación:** Para perfiles administrados, el propietario del dispositivo puede anular esta configuración. El valor predeterminado es **Desactivado**.

> **Sugerencia:**
>
> Puede crear directivas de dispositivo de ubicación en Citrix Endpoint Management para aplicar límites geográficos. Consulte Directiva de dispositivo de ubicación.

- **Permitir al usuario configurar credenciales de usuario:** Especifique si los usuarios pueden configurar credenciales en el almacén de claves administrado. El valor predeterminado es **Activado**.
- **Permitir la impresión:** Si está en **Activado**, la configuración permite a los usuarios imprimir en cualquier impresora accesible desde el dispositivo del usuario. El valor predeterminado es **Desactivado**. Disponible para: Android 9 y versiones posteriores.
- **Permitir la depuración USB:** El valor predeterminado es **Desactivado**.

- **Aplicaciones**
  - **Habilitar aplicaciones del sistema:** Permite a los usuarios ejecutar aplicaciones preinstaladas en el dispositivo. El valor predeterminado es **Desactivado**. Para habilitar aplicaciones específicas, haga clic en **Agregar** en la tabla **Lista de aplicaciones del sistema**.
    - **Lista de aplicaciones del sistema:** Una lista de las aplicaciones del sistema que desea habilitar en el dispositivo. Establezca **Habilitar aplicaciones del sistema** en **Activado** y agregue el nombre del paquete de la aplicación. Para buscar el nombre del paquete de una aplicación del sistema, puede usar Android Debug Bridge (`adb`) para llamar al comando del administrador de paquetes de Android (`pm`). Por ejemplo, `adb shell "pm list packages -f name"`, donde "nombre" forma parte del nombre del paquete. Para obtener más información, consulte `<https://developer.android.com/studio/command-line/adb>`. Para dispositivos Android Enterprise, puede restringir los permisos de las aplicaciones mediante la directiva Permisos de aplicaciones de Android Enterprise.
  - **Inhabilitar aplicaciones:** Bloquea la ejecución de una lista especificada de aplicaciones en los dispositivos. El valor predeterminado es **Desactivado**. Para inhabilitar una aplicación instalada, cambie la configuración a **Activado** y, a continuación, haga clic en **Agregar** en la tabla **Lista de aplicaciones**.
    - **Lista de aplicaciones:** Una lista de las aplicaciones que desea bloquear. Establezca **Inhabilitar aplicaciones** en **Activado** y agregue la aplicación. Escriba el nombre del

paquete de la aplicación. Cambiar e implementar una lista de aplicaciones sobrescribe la lista de aplicaciones anterior. Por ejemplo: Si inhabilita com.example1 y com.example2, y luego cambia la lista a com.example1 y com.example3, Citrix Endpoint Management habilita com.example.2.

- **Habilitar verificación de aplicaciones:** Permite al sistema operativo escanear aplicaciones para detectar comportamientos maliciosos. El valor predeterminado es **Activado**.
- **Habilitar aplicaciones de Google:** Permite a los usuarios descargar aplicaciones de Google Mobile Services en el dispositivo. El valor predeterminado es **Activado**.
- **Permitir aplicaciones que no sean de Google Play:** Permite la instalación de aplicaciones de tiendas que no sean Google Play. El valor predeterminado es **Desactivado**.
- **Permitir control de usuario de la configuración de aplicaciones:** Permite a los usuarios desinstalar aplicaciones, inhabilitar aplicaciones, borrar caché y datos, forzar la detención de cualquier aplicación y borrar valores predeterminados. Los usuarios realizan estas acciones desde la aplicación Configuración. El valor predeterminado es **Desactivado**.
- **Permitir desinstalación de aplicaciones:** Permite a los usuarios desinstalar aplicaciones desde Managed Google Play Store. El valor predeterminado es **Desactivado**.

- **Solo dispositivos totalmente administrados**
  - **Permitir agregar usuarios:** Permite a los usuarios agregar nuevos usuarios en un dispositivo. El valor predeterminado es **Activado**.
  - **Permitir itinerancia de datos:** Permite a los usuarios usar datos móviles mientras están en itinerancia. El valor predeterminado es Desactivado, lo que inhabilita la itinerancia en los dispositivos de los usuarios. El valor predeterminado es **Desactivado**.
  - **Permitir SMS:** Permite a los usuarios enviar y recibir mensajes SMS. El valor predeterminado es **Desactivado**.
  - **Permitir el uso de la barra de estado:** Si está **Activado**, esta configuración habilita la barra de estado en dispositivos administrados y dispositivos dedicados (también conocidos como dispositivos COSU). Esta configuración inhabilita las notificaciones, la configuración rápida y otras superposiciones de pantalla que permiten salir del modo de pantalla completa. Los usuarios pueden ir a la configuración del sistema y ver las notificaciones. Para Android 6.0 y versiones posteriores. El valor predeterminado es **Desactivado**.
  - **Permitir Bluetooth:** Permite a los usuarios usar Bluetooth. El valor predeterminado es **Activado**.

    - **Permitir compartir Bluetooth:** Si no está seleccionada, los usuarios no pueden establecer el uso compartido de Bluetooth saliente en su dispositivo. El valor predeterminado es seleccionado.

  - **Permitir configurar fecha y hora:** Permite a los usuarios cambiar la fecha y la hora en sus dispositivos. El valor predeterminado es **Activado**.
  - **Permitir restablecimiento de fábrica:** Permite a los usuarios realizar un restablecimiento de fábrica en sus dispositivos. El valor predeterminado es **Activado**.
  - **Permitir protección de restablecimiento de fábrica:** Si se establece en **Activado**, cuando el dispositivo se restablece mediante el modo de recuperación, el usuario debe proporcionar las credenciales de la cuenta que estaba en el dispositivo antes del restablecimiento. También pueden proporcionar el bloqueo del dispositivo si se estableció uno antes del restablecimiento. Si se establece en **Desactivado**, no se requiere autenticación después de un restablecimiento. El valor predeterminado es **Activado**.
  - **Mantener la pantalla del dispositivo encendida:** Si esta configuración se establece en **Activado**, la pantalla del dispositivo permanece encendida cuando el dispositivo está enchufado. El valor predeterminado es **Desactivado**.
  - **Permitir almacenamiento masivo USB:** Permite la transferencia de archivos de datos grandes entre los dispositivos de los usuarios y un equipo a través de una conexión USB. El valor predeterminado es **Activado**.
  - **Permitir micrófono:** Permite a los usuarios usar el micrófono en sus dispositivos. El valor predeterminado es **Activado**.
  - **Permitir anclaje a red:** Permite a los usuarios configurar puntos de acceso portátiles y anclar datos. El valor predeterminado es **Desactivado**. Cuando esta configuración está activada, estas configuraciones están disponibles para dispositivos Samsung:
  - **Evitar que el bloqueo de pantalla bloquee el dispositivo:** Si está **Activado**, esta configuración deshabilita el bloqueo de pantalla en la pantalla de bloqueo en dispositivos administrados y dispositivos dedicados (también conocidos como dispositivos COSU). El valor predeterminado es **Desactivado**.
  - **Permitir cambios de Wi-Fi:** Si está **Activado**, los usuarios pueden activar o desactivar Wi-Fi y conectarse a redes Wi-Fi. El valor predeterminado es **Activado**.
  - **Permitir transferencia de archivos:** Permite transferencias de archivos a través de USB. El valor predeterminado es **Desactivado**.

- **Samsung**

- **Habilitar TIMA Keystore:** El TIMA Keystore proporciona almacenamiento seguro de claves basado en TrustZone para las claves simétricas. Los pares de claves RSA y los certificados se dirigen al proveedor de almacén de claves predeterminado para su almacenamiento. El valor predeterminado es **Desactivado**.
- **Permitir lista de compartir:** Permite a los usuarios compartir contenido entre aplicaciones en la lista Compartir a través de. El valor predeterminado es **Activado**.
- **Habilitar registro de auditoría:** Permite la creación de registros de auditoría de eventos para el análisis forense de un dispositivo. El valor predeterminado es **Desactivado**.

- **Samsung: Solo dispositivos totalmente administrados**
  - **Permitir solo llamadas de emergencia:** Permite a los usuarios habilitar el modo Solo llamadas de emergencia en sus dispositivos. El valor predeterminado es **Desactivado**.
  - **Permitir recuperación de firmware:** Permite a los usuarios recuperar el firmware en sus dispositivos. El valor predeterminado es **Activado**.
  - **Permitir cifrado rápido:** Permite el cifrado solo del espacio de memoria utilizado. Este cifrado contrasta con el cifrado de disco completo, que cifra todos los datos. Esos datos incluyen configuraciones, datos de aplicaciones, archivos y aplicaciones descargados, medios y otros archivos. El valor predeterminado es **Activado**.
  - **Habilitar modo Common Criteria:** Pone el dispositivo en modo Common Criteria. La configuración de Common Criteria aplica procesos de seguridad estrictos. El valor predeterminado es **Activado**.
  - **Habilitar banner de reinicio:** Muestra un mensaje o banner de notificación de uso del sistema aprobado por el DoD cuando se reinician los dispositivos de los usuarios. El valor predeterminado es **Desactivado**.
  - **Permitir cambios de configuración:** Permite a los usuarios cambiar la configuración en sus dispositivos totalmente administrados. El valor predeterminado es **Activado**.
  - **Habilitar uso de datos en segundo plano:** Permite que las aplicaciones sincronicen datos en segundo plano para dispositivos totalmente administrados. El valor predeterminado es **Activado**.
  - **Permitir portapapeles:** Permite a los usuarios copiar datos al portapapeles en sus dispositivos. El valor predeterminado es **Activado**.
    - **Permitir compartir portapapeles:** Permite a los usuarios compartir contenido del portapapeles entre sus dispositivos y un equipo (MDM 4.0 y posterior).

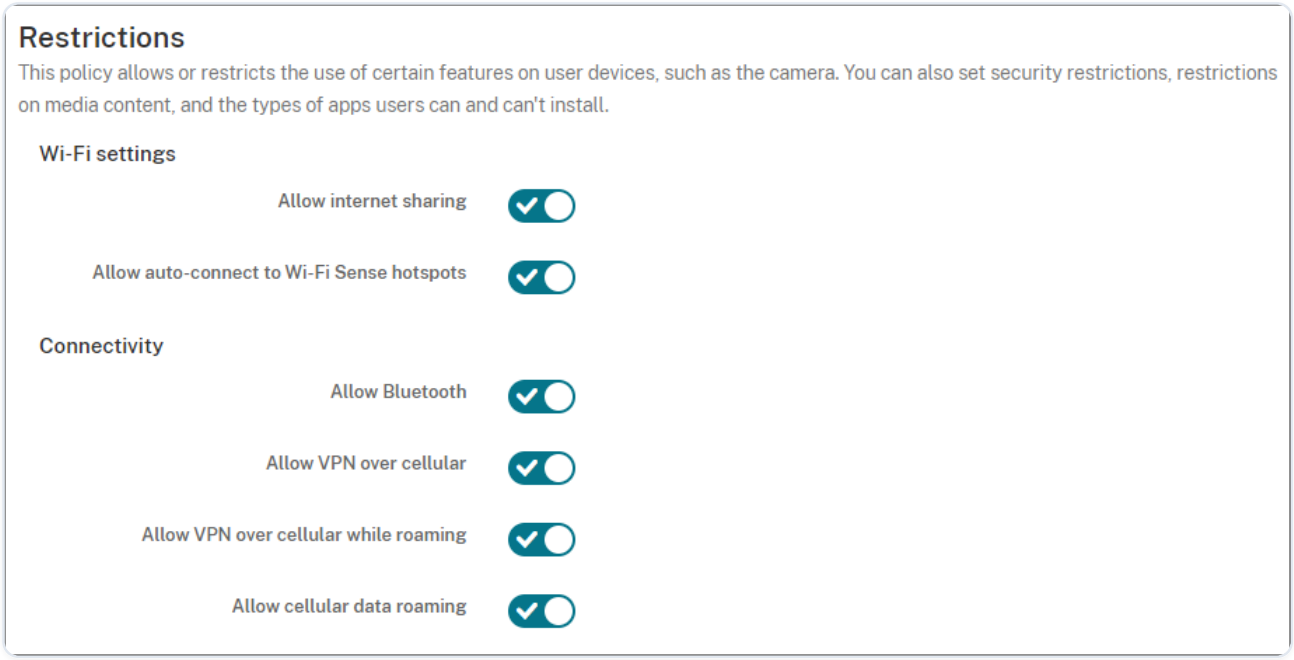
- **Permitir tecla de inicio:** Permite a los usuarios usar la tecla **Inicio** en sus dispositivos totalmente administrados. El valor predeterminado es **Activado**.
- **Permitir ubicación simulada:** Permite a los usuarios falsificar su ubicación GPS. Para dispositivos totalmente administrados. El valor predeterminado es **Desactivado**.
- **NFC:** Permite a los usuarios usar NFC en sus dispositivos totalmente administrados (MDM 3.0 y posterior). El valor predeterminado es **Activado**.
- **Permitir apagar:** Permite a los usuarios apagar sus dispositivos totalmente administrados (MDM 3.0 y posterior). El valor predeterminado es **Activado**.
- **Permitir Wi-Fi Direct:** Permite a los usuarios conectarse directamente a otro dispositivo a través de su conexión Wi-Fi. El valor predeterminado es **Activado**. Si está **Activado**, debe habilitar la configuración **Permitir cambios de Wi-Fi**.
- **Permitir tarjeta SD:** Permite a los usuarios usar una tarjeta SD, si está disponible, con sus dispositivos. El valor predeterminado es **Activado**.
- **Permitir almacenamiento de host USB:** Permite que los dispositivos de los usuarios actúen como host USB cuando un dispositivo USB se conecta a sus dispositivos. Los dispositivos de los usuarios suministran energía al dispositivo USB. El valor predeterminado es **Activado**.
- **Permitir marcador de voz:** Permite a los usuarios usar el marcador de voz en sus dispositivos (MDM 4.0 y posterior). El valor predeterminado es **Activado**.
- **Permitir S Beam:** Permite a los usuarios compartir contenido con otros mediante NFC y Wi-Fi Direct (MDM 4.0 y posterior). El valor predeterminado es **Activado**.
- **Permitir S Voice:** Permite a los usuarios usar el asistente personal inteligente y el navegador de conocimientos en sus dispositivos (MDM 4.0 y posterior). El valor predeterminado es **Activado**.
- **Permitir anclaje a red USB:** Permite a los usuarios compartir una conexión de datos móviles con otro dispositivo mediante su conexión USB. El valor predeterminado es **Desactivado**. Si está **Activado**, la configuración **Permitir anclaje a red** también debe estar **Activada**.
- **Permitir anclaje a red Bluetooth:** Permite a los usuarios compartir una conexión de datos móviles con otro dispositivo mediante su conexión Bluetooth. El valor predeterminado es **Desactivado**. Si está **Activado**, la configuración **Permitir anclaje a red** también debe estar **Activada**.
- **Permitir anclaje a red Wi-Fi:** Permite a los usuarios compartir una conexión de datos móviles con otro dispositivo mediante su conexión Wi-Fi. El valor predeterminado es

Desactivado. Si está **Activado**, la configuración **Permitir anclaje a red** también debe estar **Activada**.

- **Permitir MMS entrantes:** Permite a los usuarios recibir mensajes MMS. El valor predeterminado es **Desactivado**. Si está **Activado**, debe activar la configuración **Permitir SMS**.
- **Permitir MMS salientes:** Permite a los usuarios enviar mensajes MMS. El valor predeterminado es **Desactivado**. Si está **Activado**, debe activar la configuración **Permitir SMS**.
- **Permitir SMS entrantes:** Permite a los usuarios recibir mensajes SMS. El valor predeterminado es **Desactivado**. Si está **Activado**, debe activar la configuración **Permitir SMS**.
- **Permitir SMS salientes:** Permite a los usuarios enviar mensajes SMS. El valor predeterminado es **Desactivado**. Si está **Activado**, debe activar la configuración **Permitir SMS**.
- **Configurar redes móviles:** Permite a los usuarios usar su conexión de datos móviles. El valor predeterminado es **Desactivado**.
- **Límite diario (MB):** Introduzca la cantidad de MB de datos móviles que los usuarios pueden usar cada día. El valor predeterminado es 0, lo que deshabilita esta función (MDM 4.0 y posterior).
- **Límite por semana (MB):** Introduzca el número de MB de datos móviles que los usuarios pueden usar cada semana. El valor predeterminado es 0, lo que deshabilita esta función (MDM 4.0 y posterior).
- **Límite por mes (MB):** Introduzca el número de MB de datos móviles que los usuarios pueden usar cada mes. El valor predeterminado es 0, lo que deshabilita esta función (MDM 4.0 y posterior).
- **Permitir solo conexiones VPN seguras:** Permite a los usuarios usar solo conexiones seguras (MDM 4.0 y posterior). El valor predeterminado es **Activado**.
- **Permitir grabación de audio:** Permite a los usuarios grabar audio con sus dispositivos (MDM 4.0 y posterior). El valor predeterminado es **Activado**. Si está **Activado**, debe activar la configuración **Permitir micrófono**.
- **Permitir grabación de vídeo:** Permite a los usuarios grabar vídeo con sus dispositivos (MDM 4.0 y posterior). El valor predeterminado es **Desactivado**. Si está **Activado**, debe activar la configuración **Permitir uso de la cámara**.

- **Permitir mensajes push en itinerancia:** Permite a los usuarios usar datos móviles para enviar mensajes. El valor predeterminado es **Desactivado**. Si está **Activado**, debe habilitar la configuración **Permitir itinerancia de datos**.
- **Permitir sincronización automática en itinerancia:** Permite a los usuarios usar datos móviles para sincronizar. El valor predeterminado es **Desactivado**. Si está **Activado**, debe habilitar la configuración **Permitir itinerancia de datos**.
- **Permitir llamadas de voz en itinerancia:** Permite a los usuarios usar datos móviles para llamadas de voz. El valor predeterminado es **Desactivado**. Si está **Activado**, debe habilitar la configuración **Permitir itinerancia de datos**.

Configuración de escritorio/tableta de Windows



- **Configuración de Wi-Fi**
  - **Permitir compartir Internet:** Permite que un dispositivo comparta su conexión a Internet con otros dispositivos convirtiéndolo en un punto de acceso Wi-Fi.
- **Conectividad**
  - **Permitir Bluetooth:** Permite que el dispositivo se conecte a través de Bluetooth.
  - **Permitir VPN a través de datos móviles:** Permite que el dispositivo se conecte a través de VPN a una red móvil.
  - **Permitir VPN a través de datos móviles en itinerancia:** Permitir que el dispositivo se conecte a través de VPN cuando el dispositivo esté en itinerancia a través de redes móviles.

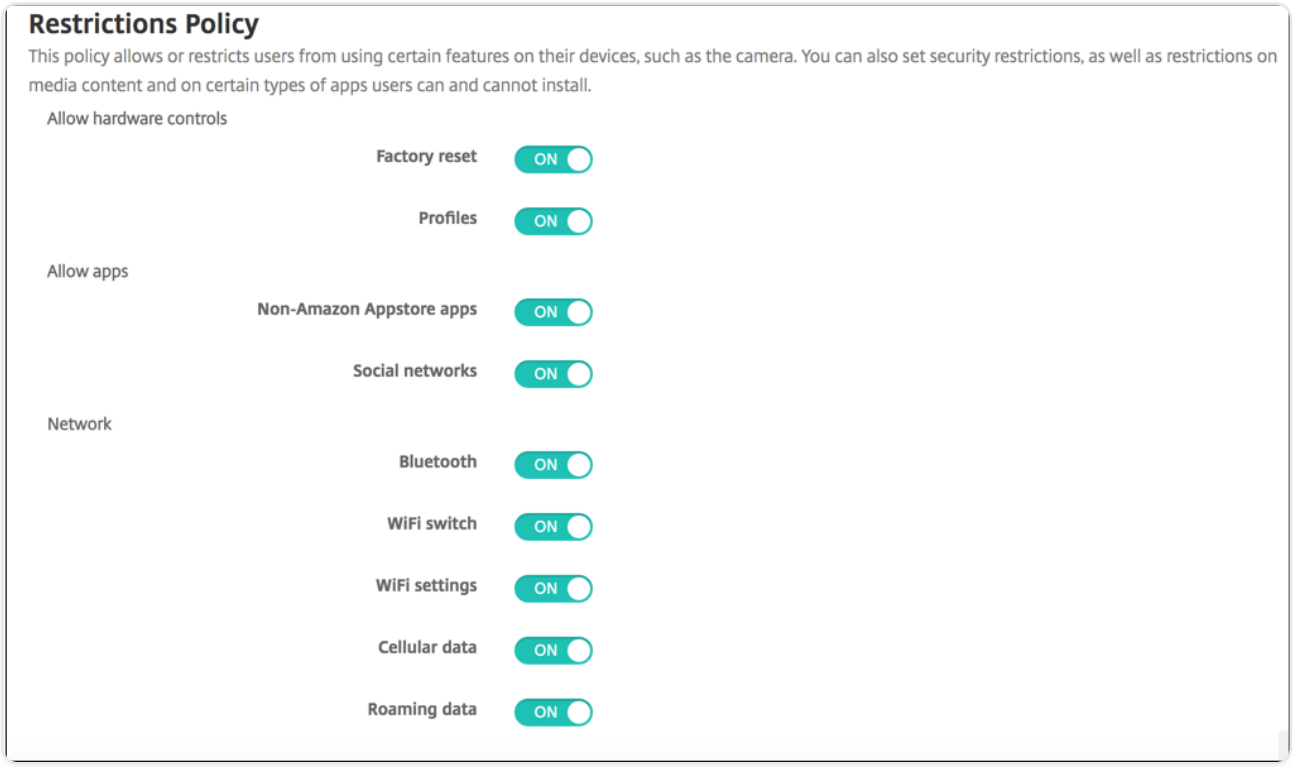
  - **Permitir itinerancia de datos móviles:** Permitir a los usuarios usar datos móviles mientras están en itinerancia.

- **Cuentas**
  - **Permitir conexión de cuenta de Microsoft:** Permitir que el dispositivo use una cuenta de Microsoft para la autenticación y los servicios de conexión no relacionados con el correo electrónico.
  - **Permitir correo electrónico que no sea de Microsoft:** Permitir al usuario agregar cuentas de correo electrónico que no sean de Microsoft.
- **Sistema**
  - **Permitir tarjeta de almacenamiento:** Permitir que el dispositivo use una tarjeta de almacenamiento.
  - **Telemetría:** Haga clic en una opción de la lista desplegable para permitir o restringir que el dispositivo envíe información de telemetría. El valor predeterminado es **Permitido**. Otras opciones son **No permitido** y **Permitido, excepto para solicitudes de datos secundarios**.
  - **Permitir acceso de aplicaciones al servicio de ubicación:** Permitir el acceso de las aplicaciones a los servicios de ubicación.
  - **Permitir vista previa de compilaciones internas:** Permitir a los usuarios previsualizar compilaciones internas de Microsoft.
- **Cámara:** Solo para Windows Desktop/Tablet
  - **Permitir el uso de la cámara:** Permitir a los usuarios usar la cámara de su dispositivo.
- **Bluetooth:** Solo para Windows Desktop/Tablet
  - **Permitir modo detectable:** Permitir que los dispositivos Bluetooth encuentren el dispositivo local.
  - **Nombre del dispositivo local:** Un nombre para el dispositivo local.
- **Experiencia:** Solo Windows de escritorio/tableta
  - **Permitir Cortana:** Permite a los usuarios acceder a Cortana, el asistente personal inteligente y navegador de conocimientos.
  - **Permitir detección de dispositivos:** Permite la detección de red del dispositivo.

  - **Permitir anulación manual de la inscripción MDM:** Permite a los usuarios anular manualmente la inscripción de su dispositivo en el MDM de Citrix Endpoint Management.
  - **Permitir sincronización de la configuración del dispositivo:** Permite a los usuarios sincronizar la configuración entre dispositivos Windows 10 y Windows 11 cuando están en itinerancia.

- **Por encima del bloqueo:** Solo Windows de escritorio/tableta
  - **Permitir notificaciones flotantes en la pantalla de bloqueo:** Permite notificaciones flotantes en la pantalla de bloqueo. Solo Windows de escritorio/tableta
- **Aplicaciones**
  - **Permitir actualizaciones automáticas de la tienda de aplicaciones:** Permite que las aplicaciones de la tienda de aplicaciones se actualicen automáticamente. Solo Windows de escritorio/tableta.
- **Privacidad:** Solo Windows de escritorio/tableta
  - **Permitir personalización de entrada:** Permite que se ejecute el servicio de personalización de entrada. El servicio de personalización de entrada mejora las entradas predictivas, como el lápiz y el teclado táctil, basándose en lo que escribe un usuario.
- **Configuración:** Solo Windows de escritorio/tableta.
  - **Permitir reproducción automática:** Permite a los usuarios cambiar la configuración de reproducción automática.
  - **Permitir Data Sense:** Permite a los usuarios cambiar la configuración de Data Sense.
  - **Permitir fecha y hora:** Permite a los usuarios cambiar la configuración de fecha y hora.
  - **Permitir idioma:** Permite a los usuarios cambiar la configuración de idioma.
  - **Permitir suspensión de energía:** Permite a los usuarios cambiar la configuración de energía y suspensión.
  - **Permitir región:** Permite a los usuarios cambiar la configuración de región.
  - **Permitir opciones de inicio de sesión:** Permite a los usuarios cambiar la configuración de inicio de sesión.
  - **Permitir lugar de trabajo:** Permite a los usuarios cambiar la configuración del lugar de trabajo.
  - **Permitir su cuenta:** Permite a los usuarios cambiar la configuración de la cuenta.

Configuración de Amazon



- **Permitir controles de hardware**
  - **Restablecimiento de fábrica:** Permite a los usuarios realizar un restablecimiento de fábrica en sus dispositivos.
  - **Perfiles:** Permite a los usuarios cambiar el perfil de hardware en sus dispositivos.
- **Permitir aplicaciones**
  - **Aplicaciones que no son de Amazon Appstore:** Permite a los usuarios instalar aplicaciones que no son de Amazon Appstore en sus dispositivos.
  - **Redes sociales:** Permite a los usuarios acceder a redes sociales desde sus dispositivos.
- **Red**
  - **Bluetooth:** Permitir a los usuarios usar Bluetooth.
  - **Conmutador de Wi-Fi:** Permitir que las aplicaciones cambien el estado de conectividad Wi-Fi.
  - **Configuración de Wi-Fi:** Permitir a los usuarios cambiar la configuración de Wi-Fi.
  - **Configurar redes móviles:** Permitir a los usuarios usar su conexión de datos móviles.
  - **Datos de itinerancia:** Permitir a los usuarios usar datos móviles mientras están en itinerancia.

    - **Servicios de ubicación:** Permitir a los usuarios usar el GPS.

- **Acciones USB:**

    - **Depuración:** Permitir que los dispositivos de los usuarios se conecten a un equipo a través de USB para la depuración.

Directiva de itinerancia de dispositivos

Puede agregar una directiva de dispositivo en Citrix Endpoint Management para configurar si se permite la itinerancia de voz y datos en los dispositivos iOS compatibles. Cuando la itinerancia de voz está inhabilitada, la itinerancia de datos se inhabilita automáticamente.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

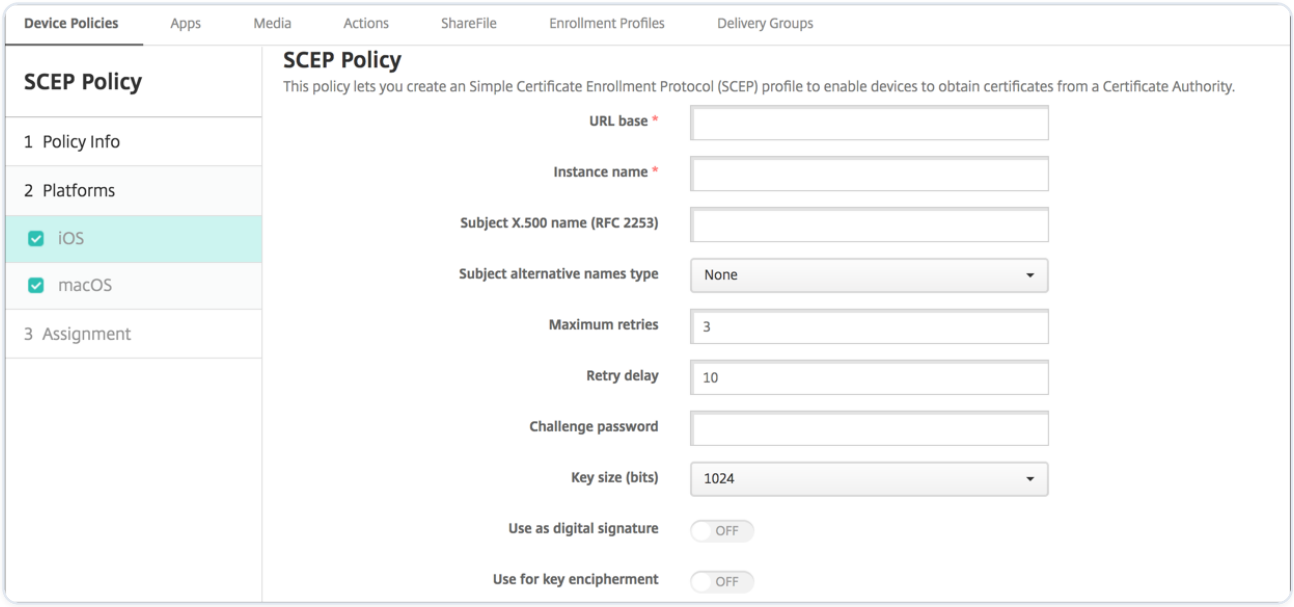
- **Inhabilitar itinerancia de voz:** Seleccione si quiere inhabilitar la itinerancia de voz. Cuando esta opción está habilitada, la itinerancia de datos se inhabilita automáticamente. El valor predeterminado es **Desactivado**, lo que permite la itinerancia de voz.
- **Inhabilitar itinerancia de datos:** Seleccione si quiere inhabilitar la itinerancia de datos. Esta opción solo está disponible cuando la itinerancia de voz está habilitada. El valor predeterminado es **Desactivado**, lo que permite la itinerancia de datos.

Directiva de dispositivo SCEP

Esta directiva le permite configurar dispositivos iOS y macOS para recuperar un certificado de un servidor SCEP externo a través del Protocolo simple de inscripción de certificados (SCEP). Para entregar un certificado a los dispositivos mediante SCEP desde una PKI conectada a Citrix Endpoint Management, cree una entidad PKI y un proveedor PKI en modo distribuido. Para obtener más información, consulte Entidades PKI.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

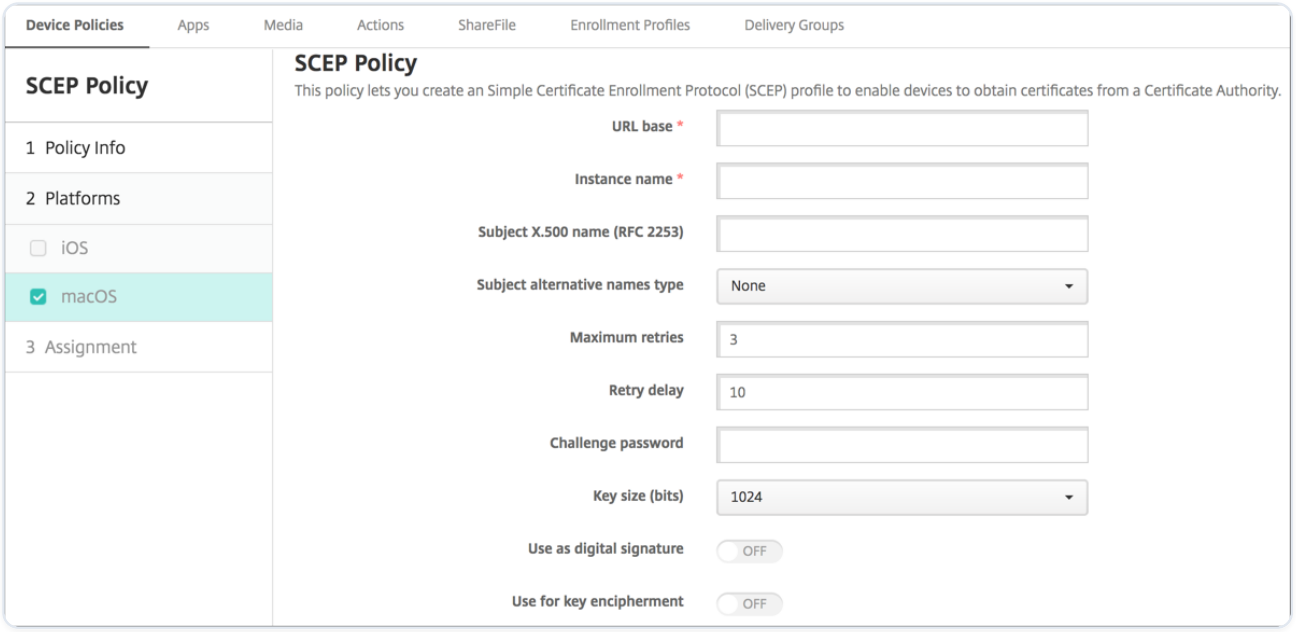
Configuración de iOS



- **URL base:** Escriba la dirección del servidor SCEP para definir dónde se envían las solicitudes SCEP, a través de HTTP o HTTPS. La clave privada no se envía con la solicitud de firma de certificado (CSR), por lo que podría ser seguro enviar la solicitud sin cifrar. Si la contraseña de un solo uso está configurada para su reutilización, utilice HTTPS para proteger la contraseña. Este paso es obligatorio.
- **Nombre de instancia:** Escriba cualquier cadena que el servidor SCEP reconozca. Por ejemplo, puede ser un nombre de dominio como example.org. Si una CA tiene varios certificados de CA, puede utilizar este campo para distinguir el dominio requerido. Este paso es obligatorio.
- **Nombre de sujeto X.500 (RFC 2253):** Escriba la representación de un nombre X.500 como una matriz de identificador de objeto (OID) y valor. Por ejemplo, `/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar`, que se traduce como: `[ [ [“C”, “US”] ], [ [“O”, “Apple Inc.”] ], …, [ [“1.2.5.3”, “bar” ] ] ]`. Puede representar los OID como números separados por puntos con accesos directos para país (C), localidad (L), estado (ST), organización (O), unidad organizativa (OU) y nombre común (CN).
- **Tipo de nombres alternativos del sujeto:** Seleccione un tipo de nombre alternativo. Un tipo de nombre alternativo opcional puede proporcionar los valores requeridos por la CA para emitir un certificado. Puede especificar **Ninguno**, **Nombre RFC 822**, **Nombre DNS** o **URI**.
- **Número máximo de reintentos:** Escriba el número de veces que un dispositivo debe reintentar cuando el servidor SCEP envía una respuesta PENDIENTE. El valor predeterminado es **3**.
- **Retraso de reintento:** Escriba el número de segundos que se deben esperar entre reintentos posteriores. El primer reintento se realiza sin demora. El valor predeterminado es **10**.

- **Contraseña de desafío:** Introduzca un secreto precompartido.
- **Tamaño de clave (bits):** Seleccione **2048** o superior como tamaño de clave en bits.
- **Usar como firma digital:** Elija si desea utilizar el certificado como firma digital. El servidor SCEP verifica el uso del certificado como firma digital antes de utilizar la clave pública para descifrar el hash.
- **Usar para cifrado de clave:** Elija si desea utilizar el certificado para el cifrado de clave. Un servidor primero comprueba si el certificado proporcionado por un cliente está permitido para el cifrado de clave. Luego, el servidor utiliza la clave pública de un certificado para verificar que un fragmento de datos se cifró utilizando la clave privada. Si no, la operación falla.
- **Huella digital SHA-256 (cadena hexadecimal):** Si su CA utiliza HTTP, use este campo para proporcionar la huella digital del certificado de la CA. El dispositivo utiliza la huella digital para confirmar la autenticidad de la respuesta de la CA durante la inscripción. Puede proporcionar una huella digital SHA-256 o puede seleccionar un certificado para importar su firma.
- **Configuración de la política**
    - **Eliminar política:** Elija un método para programar la eliminación de la política. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
        - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
        - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la política. Solo disponible para iOS 6.0 y versiones posteriores.

Configuración de macOS



- **URL base:** Escriba la dirección del servidor SCEP para definir dónde se envían las solicitudes SCEP, a través de HTTP o HTTPS. La clave privada no se envía con la Solicitud de firma de certificado (CSR), por lo que podría ser seguro enviar la solicitud sin cifrar. Si la contraseña de un solo uso está configurada para su reutilización, use HTTPS para proteger la contraseña. Este paso es obligatorio.
- **Nombre de instancia:** Escriba cualquier cadena que el servidor SCEP reconozca. Por ejemplo, puede ser un nombre de dominio como example.org. Si una CA tiene varios certificados de CA, puede usar este campo para distinguir el dominio requerido. Este paso es obligatorio.
- **Nombre de sujeto X.500 (RFC 2253):** Escriba la representación de un nombre X.500 como una matriz de Identificador de objeto (OID) y valor. Por ejemplo, `/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar`, que se traduce como: `[ [ [“C”, “US”] ], [ [“O”, “Apple Inc.”] ], …, [ [“1.2.5.3”, “bar” ] ] ]`. Puede representar los OID como números separados por puntos con atajos para país (C), localidad (L), estado (ST), organización (O), unidad organizativa (OU) y nombre común (CN).
- **Tipo de nombres alternativos del sujeto:** Seleccione un tipo de nombre alternativo. Un tipo de nombre alternativo opcional puede proporcionar los valores requeridos por la CA para emitir un certificado. Puede especificar **Ninguno**, **Nombre RFC 822**, **Nombre DNS** o **URI**.
- **Número máximo de reintentos:** Escriba el número de veces que un dispositivo debe reintentar cuando el servidor SCEP envía una respuesta PENDIENTE. El valor predeterminado es **3**.

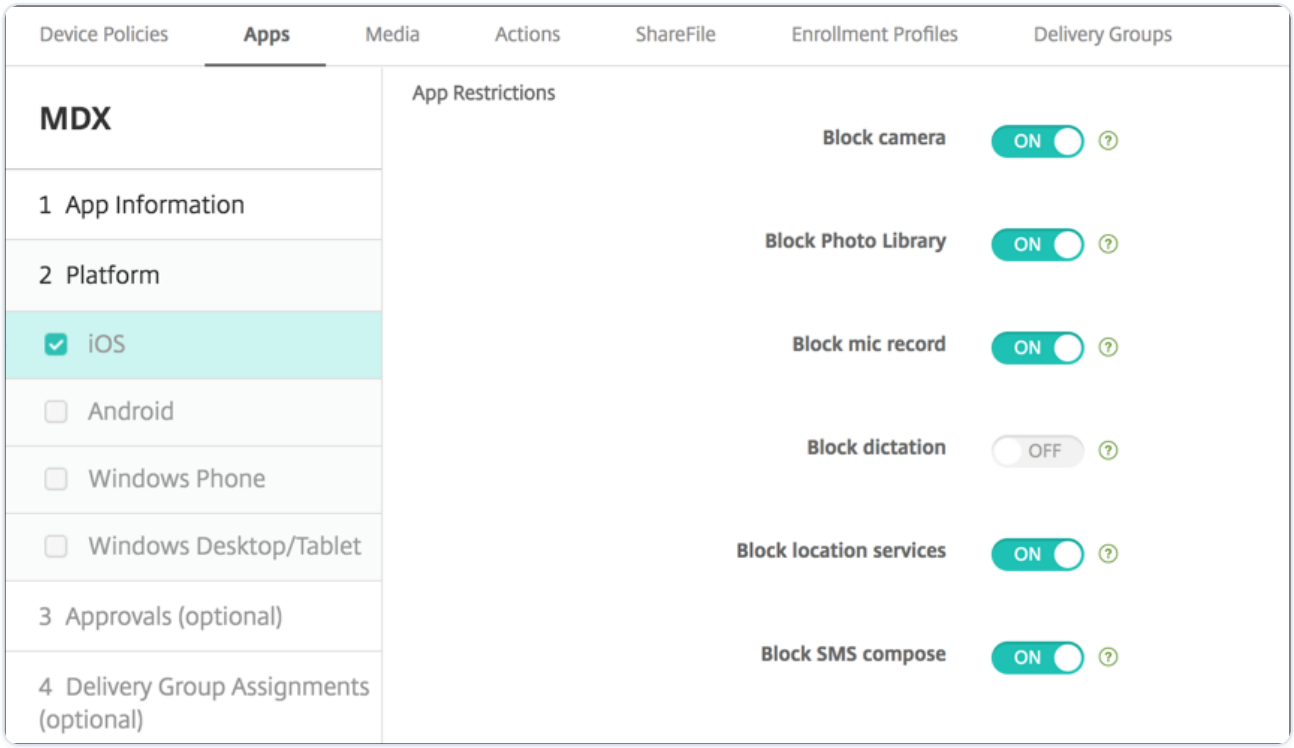
- **Retraso de reintento:** Escriba el número de segundos que debe esperar entre reintentos posteriores. El primer reintento se realiza sin demora. El valor predeterminado es **10**.
- **Contraseña de desafío:** Escriba un secreto precompartido.
- **Tamaño de clave (bits):** Seleccione **2048** o superior como tamaño de clave en bits.
- **Usar como firma digital:** Elija si desea usar el certificado como firma digital. El servidor SCEP verifica el uso del certificado como firma digital antes de usar la clave pública para descifrar el hash.
- **Usar para cifrado de clave:** Elija si desea usar el certificado para cifrado de clave. Un servidor comprueba primero si el certificado proporcionado por un cliente está permitido para el cifrado de clave. Luego, el servidor usa la clave pública de un certificado para verificar que un fragmento de datos se cifró con la clave privada. Si no, la operación falla.
- **Huella digital SHA-256 (cadena hexadecimal):** Si su CA utiliza HTTP, use este campo para proporcionar la huella digital del certificado de CA. El dispositivo usa la huella digital para confirmar la autenticidad de la respuesta de la CA durante la inscripción. Puede proporcionar una huella digital SHA-256 o seleccionar un certificado para importar su firma.
- **Configuración de directivas**
    - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
        - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
        - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.
    - **Permitir al usuario eliminar la directiva:** Puede seleccionar cuándo los usuarios pueden eliminar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**.
    - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en macOS 10.7 y versiones posteriores.

Políticas de Siri y dictado

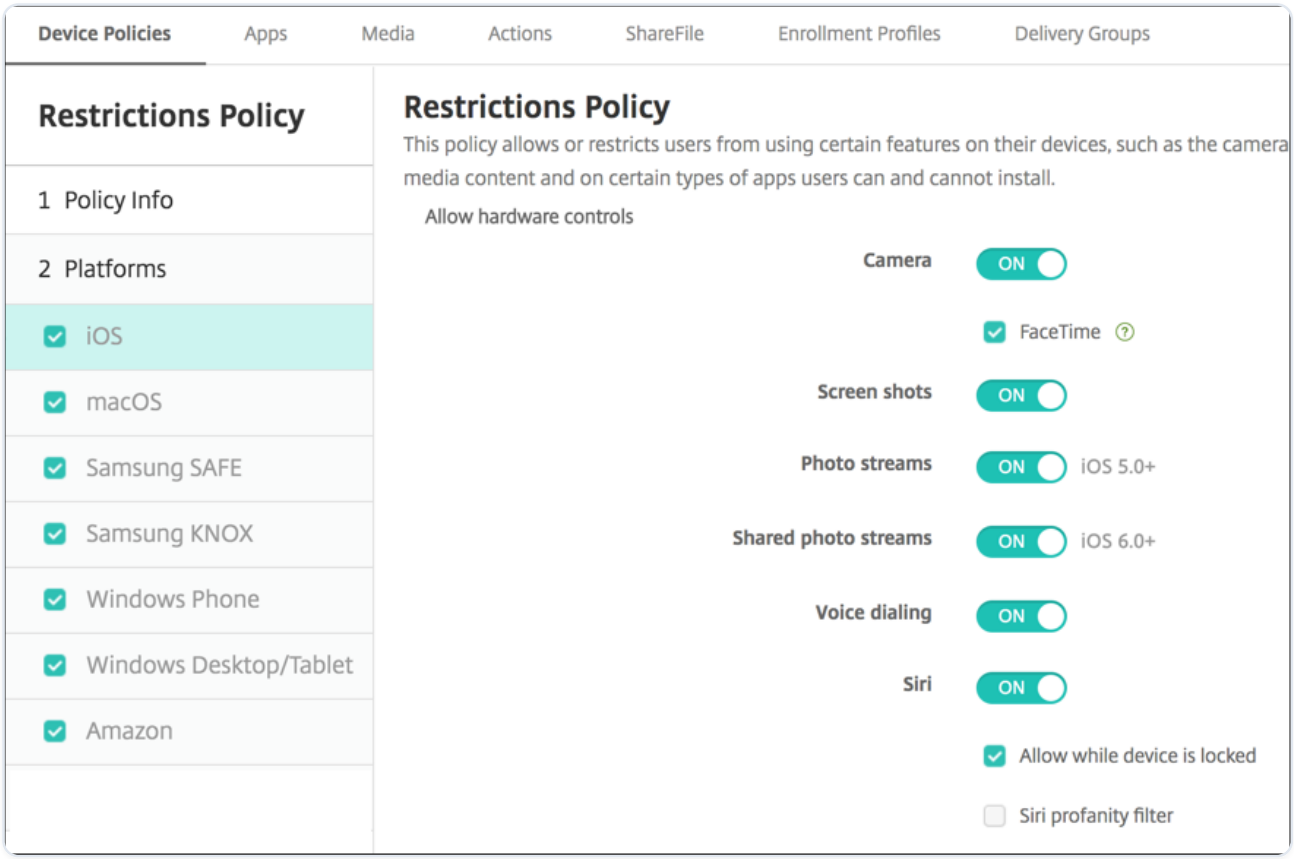
Cuando los usuarios preguntan algo a Siri o dictan texto en dispositivos iOS administrados, Apple recopila los datos de voz con el fin de mejorar Siri. Los datos de voz pasan por los servicios basados en la nube de Apple y, por lo tanto, existen fuera del contenedor seguro de Citrix Endpoint Management. Sin embargo, el texto resultante del dictado permanece dentro del contenedor.

Citrix Endpoint Management le permite bloquear los servicios de Siri y dictado, según lo requieran sus necesidades de seguridad.

En las implementaciones de MAM, la directiva **Bloquear dictado** para cada aplicación está **Activada** de forma predeterminada, lo que deshabilita el micrófono del dispositivo. Establézcala en **Desactivado** si desea permitir el dictado. Puede encontrar la directiva en la consola de Citrix Endpoint Management en **Configurar > Aplicaciones**. Seleccione la aplicación, haga clic en **Editar** y, a continuación, haga clic en **iOS**.



En las implementaciones de MDM, también puede inhabilitar Siri con la directiva de Siri en **Configurar > Directivas de dispositivo**. El uso de Siri está permitido de forma predeterminada.



Algunos puntos a tener en cuenta al decidir si permitir Siri y el dictado:

- Según la información que Apple ha hecho pública, Apple conserva los datos de los clips de voz de Siri y dictado durante un máximo de dos años. A los datos se les asigna un número aleatorio para representar al usuario, y los archivos de voz se asocian con este número aleatorio.
- Puede revisar la política de privacidad de Apple yendo a **Ajustes > General > Teclados** en cualquier dispositivo iOS y tocando el enlace debajo de **Activar dictado**.

Directiva de dispositivo de cuenta SSO

La directiva de dispositivo de cuenta SSO le permite crear cuentas de inicio de sesión único (SSO) en Citrix Endpoint Management. Esas cuentas permiten a los usuarios iniciar sesión una sola vez para acceder a Citrix Endpoint Management y a los recursos internos de su empresa desde varias aplicaciones. Los usuarios no necesitan almacenar ninguna credencial en el dispositivo. Las credenciales de usuario empresarial de la cuenta SSO se utilizan en todas las aplicaciones, incluidas las de App Store. Esta directiva está diseñada para funcionar con un back-end de autenticación Kerberos.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

- **Nombre de cuenta:** Introduzca el nombre de la cuenta SSO de Kerberos que aparece en los dispositivos de los usuarios. Este campo es obligatorio.
- **Nombre principal de Kerberos:** Introduzca el nombre principal de Kerberos. Este campo es obligatorio.
- **Credencial de identidad (almacén de claves o credencial PKI):** Haga clic en una credencial de identidad opcional en la lista desplegable que se puede utilizar para renovar la credencial de Kerberos sin la interacción del usuario.
- **Dominio de Kerberos:** Introduzca el dominio de Kerberos para esta directiva. Este valor suele ser el nombre de su dominio en mayúsculas (por ejemplo, EXAMPLE.COM). Este campo es obligatorio.
- **URL permitidas:** Para cada URL para la que quiera requerir SSO, haga clic en **Agregar** y, a continuación, haga lo siguiente:
  - **URL permitida:** Introduzca una URL para la que quiera requerir SSO cuando un usuario visite la URL desde el dispositivo iOS.

    Por ejemplo, cuando un usuario intenta navegar a un sitio y el sitio web inicia un desafío de Kerberos: Si ese sitio no está en la lista de URL, el dispositivo iOS no intenta el SSO proporcionando el token de Kerberos que Kerberos podría haber almacenado en caché en el dispositivo de un inicio de sesión de Kerberos anterior. La coincidencia debe ser exacta en la parte del host de la URL. Por ejemplo, `https://shopping.apple.com` es válido, pero `https://*.apple.com` no lo es.

    Además, si Kerberos no se activa en función de la coincidencia de host, la URL sigue recurriendo a una llamada HTTP estándar. Esto puede significar casi cualquier cosa, incluido un desafío de contraseña estándar o un error HTTP si la URL solo está configurada para SSO mediante Kerberos.
  - Haga clic en **Agregar** para añadir la URL o haga clic en **Cancelar** para cancelar la adición de la URL.
- **Identificadores de aplicación:** Para cada aplicación a la que se le permite usar este inicio de sesión, haga clic en **Agregar** y, a continuación, haga lo siguiente:
  - **Identificador de aplicación:** Introduzca un identificador de aplicación para una aplicación a la que se le permite usar este inicio de sesión. Si no agrega ningún identificador de aplicación, este inicio de sesión coincide con **todos** los identificadores de aplicación.

- **Configuración de la política**
  - **Eliminar política:** Elija un método para programar la eliminación de la política. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la política. Solo disponible para iOS 6.0 y versiones posteriores.

Directiva de dispositivo de tienda

Puede crear una directiva en Citrix Endpoint Management para especificar si los dispositivos muestran un clip web de la tienda de aplicaciones en la pantalla de inicio.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS, Android y Windows Desktop/Tablet

Para cada plataforma que configure, seleccione si un clip web de la tienda de aplicaciones aparece en los dispositivos de los usuarios. El valor predeterminado es **Activado**.

Directiva de dispositivo de calendarios suscritos

Puede agregar una directiva de dispositivo en Citrix Endpoint Management para añadir un calendario suscrito a la lista de calendarios en dispositivos iOS. La lista de calendarios públicos a los que puede suscribirse está disponible en el sitio de soporte de Apple, en Descargas.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Requisito previo

Debe haberse suscrito a un calendario antes de poder agregarlo a la lista de calendarios suscritos en los dispositivos de usuario.

Parámetros de iOS

- **Descripción:** Introduzca una descripción del calendario. Este campo es obligatorio.

- **URL:** Introduzca la URL del calendario. Puede introducir una URL `webcal://` o un enlace `https://` a un archivo iCalendar (.ics). Este campo es obligatorio.
- **Nombre de usuario:** Introduzca el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Introduzca una contraseña de usuario opcional.
- **Usar SSL:** Seleccione si desea utilizar una conexión Secure Socket Layer al calendario. El valor predeterminado es **Desactivado**.
- **Configuración de directiva**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva. Solo disponible para iOS 6.0 y versiones posteriores.

Política de dispositivo de términos y condiciones

Puede crear políticas de dispositivo de términos y condiciones en Citrix Endpoint Management cuando desee que los usuarios acepten las políticas específicas de su empresa que rigen las conexiones a la red corporativa. Cuando los usuarios inscriben sus dispositivos en Citrix Endpoint Management, se les presentan los términos y condiciones y deben aceptarlos para inscribir sus dispositivos. Rechazar los términos y condiciones cancela el proceso de inscripción.

Puede crear diferentes políticas de términos y condiciones en distintos idiomas si su empresa tiene usuarios internacionales y desea que acepten los términos y condiciones en sus idiomas nativos. Debe proporcionar un archivo para cada combinación de plataforma e idioma que planee implementar. Para dispositivos Android e iOS, debe proporcionar archivos PDF. Para dispositivos Windows, debe proporcionar archivos de texto (.txt) y archivos de imagen adjuntos.

Para agregar o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS y Android

- **Archivo a importar:** Seleccione el archivo de términos y condiciones que desea importar haciendo clic en **Examinar** y, a continuación, navegando hasta la ubicación del archivo.

- **Términos y condiciones predeterminados:** Seleccione si este archivo es el documento predeterminado para los usuarios que son miembros de varios grupos con diferentes términos y condiciones. El valor predeterminado es **Desactivado**.

> **Nota:**
>
> Los términos y condiciones no se muestran si un dispositivo iOS se inscribe a través del Programa de inscripción de dispositivos (DEP).

Configuración de tabletas Windows

- **Archivo a importar:** Seleccione el archivo de términos y condiciones que desea importar haciendo clic en **Examinar** y, a continuación, navegando hasta la ubicación del archivo.
- **Imagen:** Seleccione el archivo de imagen que desea importar haciendo clic en **Examinar** y, a continuación, navegando hasta la ubicación del archivo.
- **Términos y condiciones predeterminados:** Seleccione si este archivo es el documento predeterminado para los usuarios que son miembros de varios grupos con diferentes términos y condiciones. El valor predeterminado es **Desactivado**.

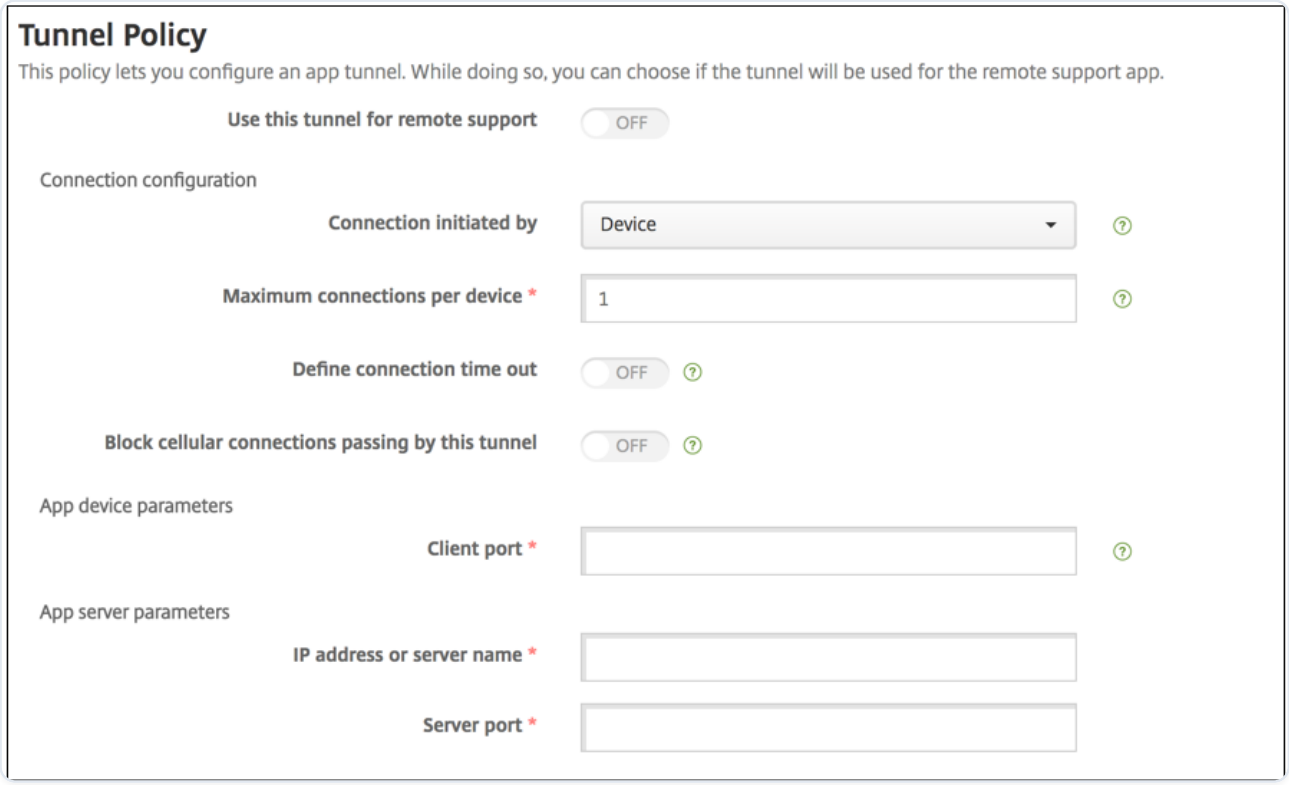
Directiva de dispositivo de túnel

Los túneles de aplicación (túneles de apps) están diseñados para aumentar la continuidad del servicio y la fiabilidad de la transferencia de datos para sus aplicaciones móviles. Los túneles de aplicación definen los parámetros de proxy entre el componente cliente de cualquier aplicación de dispositivo móvil y el componente de servidor de la aplicación. Puede configurar la directiva de túnel para dispositivos Android.

Todo el tráfico de aplicaciones enviado a través de un túnel que defina en esta directiva pasa por Citrix Endpoint Management antes de ser redirigido al servidor que ejecuta la aplicación.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de Android



- **Conexión iniciada por:** Haga clic en **Dispositivo** o **Servidor** para especificar el origen que inicia la conexión.
- **Número máximo de conexiones por dispositivo:** Escriba un número para especificar cuántas conexiones TCP simultáneas puede establecer la aplicación. Este campo solo se aplica a las conexiones iniciadas por el dispositivo.
- **Definir tiempo de espera de conexión:** Seleccione si desea establecer un período de tiempo durante el cual una aplicación puede estar inactiva antes de que se cierre el túnel.
    - **Tiempo de espera de conexión:** Si establece **Definir tiempo de espera de conexión** en **Activado**, escriba la duración en segundos que una aplicación puede estar inactiva antes de que se cierre el túnel.
- **Bloquear conexiones móviles que pasen por este túnel:** Seleccione si este túnel se bloquea durante la itinerancia. Las conexiones Wi-Fi y USB no se bloquean.
- **Puerto de cliente:** Escriba el número de puerto de cliente. Normalmente, este valor es el mismo que el del puerto del servidor.
- **Dirección IP o nombre del servidor:** Escriba la dirección IP o el nombre del servidor de aplicaciones. Este campo solo se aplica a las conexiones iniciadas por el dispositivo.
- **Puerto del servidor:** Escriba el número de puerto del servidor.

Política de dispositivos VPN

La política de dispositivos VPN configura los ajustes de red privada virtual (VPN) que permiten a los dispositivos de los usuarios conectarse de forma segura a los recursos corporativos. Puede configurar la política de dispositivos VPN para las siguientes plataformas. Cada plataforma requiere un conjunto diferente de valores, que se describen en detalle en este artículo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivos**. Para obtener más información, consulte Directivas de dispositivos.

> **Nota:**
>
> Citrix SSO para Android e iOS ahora se llama Citrix Secure Access. Estamos actualizando nuestra documentación para reflejar este cambio de nombre.

Requisitos para VPN por aplicación

Puede configurar la función de VPN por aplicación para las siguientes plataformas a través de las directivas VPN:

- iOS
- macOS
- Android (DA heredado)

Para Android Enterprise, utilice la directiva de dispositivos de configuraciones administradas para configurar perfiles VPN.

Las opciones de VPN por aplicación están disponibles para ciertos tipos de conexión. La siguiente tabla indica cuándo están disponibles las opciones de VPN por aplicación.

PLATAFORMA	TIPO DE CONEXIÓN	OBSERVACIÓN
iOS	Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix SSO o Custom SSL.	
macOS	Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL	

PLATAFORMA	TIPO DE CONEXIÓN	OBSERVACIÓN
	Mobile Connect, Ariba VIA o Custom SSL.	
Android (DA heredado)	Citrix SSO	

Para crear una VPN por aplicación para dispositivos iOS y Android (DA heredado) mediante la aplicación Citrix SSO, debe realizar pasos adicionales, además de la configuración de la directiva VPN. Además, debe verificar que se cumplen los siguientes requisitos previos:

- NetScaler Gateway local
- Las siguientes aplicaciones están instaladas en el dispositivo:
  - Citrix SSO
  - Citrix Secure Hub

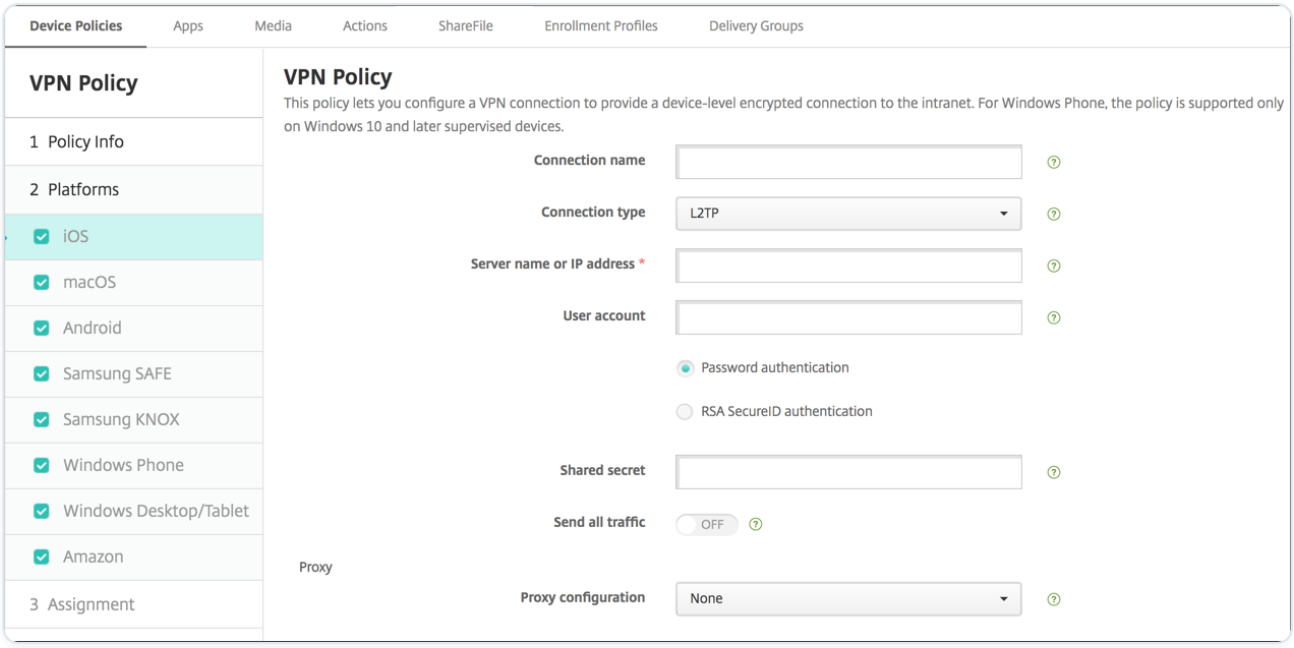
Un flujo de trabajo general para configurar una VPN por aplicación para dispositivos iOS y Android mediante la aplicación Citrix SSO es el siguiente:

1. Configure una directiva de dispositivo VPN como se describe en este artículo.
   - Para iOS, consulte Configurar el protocolo Citrix SSO para iOS. Después de configurar el protocolo Citrix SSO para iOS mediante una directiva de dispositivo VPN, también debe crear una directiva de atributos de aplicación para asociar una aplicación a la directiva VPN por aplicación. Para obtener más información, consulte Configurar una VPN por aplicación.
     - Para el campo **Tipo de autenticación para la conexión**, si selecciona **Certificado**, primero debe configurar la autenticación basada en certificados para Citrix Endpoint Management. Consulte Certificado de cliente o certificado más autenticación de dominio.
   - Para Android (DA heredado), consulte Configurar el protocolo Citrix SSO para Android.
     - En el campo **Tipo de autenticación para la conexión**, si selecciona **Certificado** o **Contraseña y certificado**, primero debe configurar la autenticación basada en certificados para Citrix Endpoint Management. Consulte Certificado de cliente o certificado más autenticación de dominio.
2. Configure Citrix ADC para aceptar el tráfico de la VPN por aplicación. Para obtener más información, consulte Configuración completa de VPN en NetScaler Gateway.

Configuración de iOS

El tipo de conexión VPN de Citrix en la directiva de dispositivo VPN para iOS no es compatible con iOS 12. Siga estos pasos para eliminar la directiva de dispositivo VPN existente y crear una directiva de dispositivo VPN con el tipo de conexión Citrix SSO:

1. Elimine su directiva de dispositivo VPN para iOS.
2. Agregue una directiva de dispositivo VPN para iOS con la siguiente configuración:
    - **Tipo de conexión: Citrix SSO**
    - **Habilitar VPN por aplicación: Activado**
    - **Tipo de proveedor: Túnel de paquetes**
3. Agregue una directiva de dispositivo de atributos de aplicación para iOS. En **Identificador de VPN por aplicación**, elija **iOS_VPN**.



- **Nombre de conexión:** Escriba un nombre para la conexión.
- **Tipo de conexión:** En la lista, seleccione el protocolo que se utilizará para esta conexión. El valor predeterminado es **L2TP**.
    - **L2TP:** Protocolo de tunelización de capa 2 con autenticación de clave precompartida.
    - **PPTP:** Tunelización punto a punto.
    - **IPSec:** Conexión VPN corporativa.
    - **Cisco Legacy AnyConnect:** Este tipo de conexión requiere que el cliente VPN Cisco Legacy AnyConnect esté instalado en el dispositivo del usuario. Cisco está eliminando

gradualmente el cliente Cisco Legacy AnyConnect que se basaba en un marco VPN ahora obsoleto.

Para utilizar el cliente Cisco AnyConnect actual, utilice un **Tipo de conexión** de **SSL personalizado**. Para conocer la configuración necesaria, consulte “Configurar el protocolo SSL personalizado” en esta sección.

- **Juniper SSL:** Cliente VPN SSL de Juniper Networks.
- **F5 SSL:** Cliente VPN SSL de F5 Networks.
- **SonicWALL Mobile Connect:** Cliente VPN unificado de Dell para iOS.
- **Ariba VIA:** Cliente de acceso a Internet virtual de Ariba Networks.
- **IKEv2 (solo iOS):** Intercambio de claves de Internet versión 2 solo para iOS.
- **AlwaysOn IKEv2:** Acceso permanente mediante IKEv2.
- **AlwaysOn IKEv2 Dual Configuration:** Acceso permanente mediante configuración dual de IKEv2.
- **Citrix SSO:** Cliente Citrix SSO para iOS 12 y versiones posteriores.
- **SSL personalizado:** Capa de sockets seguros personalizada. Este tipo de conexión es necesario para el cliente Cisco AnyConnect que tiene un ID de paquete de **com.cisco.anyconnect**. Especifique un **Nombre de conexión** de **Cisco AnyConnect**. También puede implementar la directiva VPN y habilitar un filtro de control de acceso a la red (NAC) para dispositivos iOS. El filtro bloquea una conexión VPN para los dispositivos que tienen aplicaciones no conformes instaladas. La configuración requiere ajustes específicos para la directiva VPN de iOS, como se describe en la siguiente sección de iOS. Para obtener más información sobre otros ajustes necesarios para habilitar el filtro NAC, consulte Control de acceso a la red.

Las siguientes secciones enumeran las opciones de configuración para cada uno de los tipos de conexión anteriores.

Configurar el protocolo L2TP para iOS

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- Seleccione **Autenticación de contraseña** o **Autenticación RSA SecurID**.
- **Secreto compartido:** Escriba la clave secreta compartida de IPsec.

- **Enviar todo el tráfico:** Seleccione si desea enviar todo el tráfico a través de la VPN. El valor predeterminado es **Desactivado**.

Configurar el protocolo PPTP para iOS

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- Seleccione **Autenticación de contraseña** o **Autenticación RSA SecurID**.
- **Nivel de cifrado:** En la lista, seleccione un nivel de cifrado. El valor predeterminado es **Ninguno**.
    - **Ninguno:** No usar cifrado.
    - **Automático:** Utilice el nivel de cifrado más seguro compatible con el servidor.
    - **Máximo (128 bits):** Utilice siempre el cifrado de 128 bits.
- **Enviar todo el tráfico:** Seleccione si desea enviar todo el tráfico a través de la VPN. El valor predeterminado es **Desactivado**.

Configurar el protocolo IPsec para iOS

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Secreto compartido** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Secreto compartido**.
- Si habilita **Secreto compartido**, configure estos ajustes:
    - **Nombre del grupo:** Escriba un nombre de grupo opcional.
    - **Secreto compartido:** Escriba una clave de secreto compartido opcional.
    - **Usar autenticación híbrida:** Seleccione si desea usar la autenticación híbrida. Con la autenticación híbrida, el servidor se autentica primero con el cliente y, a continuación, el cliente se autentica con el servidor. El valor predeterminado es **Desactivado**.
    - **Solicitar contraseña:** Seleccione si desea solicitar a los usuarios sus contraseñas cuando se conecten a la red. El valor predeterminado es **Desactivado**.
- Si habilita **Certificado**, configure estos ajustes:

- **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea usar. El valor predeterminado es **Ninguno**.
- **Solicitar PIN al conectar:** Seleccione si desea exigir a los usuarios que introduzcan su PIN al conectarse a la red. El valor predeterminado es **Desactivado**.
- **Habilitar VPN a petición:** Seleccione si desea habilitar la activación de una conexión VPN cuando los usuarios se conecten a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los ajustes cuando **Habilitar VPN a petición** está **Activado**, consulte Configurar los ajustes de Habilitar VPN a petición para iOS.

- **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**.
- **Aplicación de coincidencia a petición habilitada:** Seleccione si las conexiones VPN por aplicación se activan automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red. El valor predeterminado es **Desactivado**.
- **Dominios de Safari:** Haga clic en **Agregar** para añadir un nombre de dominio de Safari.

Configurar el protocolo Cisco AnyConnect heredado para iOS

Para pasar del cliente Cisco AnyConnect heredado al nuevo cliente Cisco AnyConnect, utilice el protocolo SSL personalizado.

- **Identificador de paquete del proveedor:** Para el cliente Legacy AnyConnect, el ID de paquete es com.cisco.anyconnect.gui.
- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Grupo:** Escriba un nombre de grupo opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, configure estos ajustes:
    - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea utilizar. El valor predeterminado es **Ninguno**.

    - **Solicitar PIN al conectar:** Seleccione si desea solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
    - **Habilitar VPN a petición:** Seleccione si desea habilitar la activación de una conexión VPN cuando los usuarios se conecten a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los ajustes cuando **Habilitar VPN a petición** está **Activado**, consulte Configurar los ajustes de Habilitar VPN a petición para iOS.

- **Incluir todas las redes:** Seleccione si desea permitir que todas las redes utilicen esta conexión. El valor predeterminado es **Desactivado**.
- **Excluir redes locales:** Seleccione si desea excluir las redes locales de usar la conexión o permitirlas. El valor predeterminado es **Desactivado**.
- **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si habilita esta opción, configure estos ajustes:
    - **Coincidencia de aplicación bajo demanda habilitada:** Seleccione si las conexiones VPN por aplicación se activan automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red. El valor predeterminado es **Desactivado**.
    - **Tipo de proveedor:** Seleccione si la VPN por aplicación se proporciona como un **proxy de aplicación** o como un **túnel de paquetes**. El valor predeterminado es **proxy de aplicación**.
    - **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que desee incluir, haga clic en **Agregar** y realice lo siguiente:
        - **Dominio:** Escriba el dominio que se va a agregar.
        - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo SSL de Juniper para iOS

- **Identificador de paquete del proveedor:** Si su perfil VPN por aplicación tiene el identificador de paquete de una aplicación con varios proveedores VPN del mismo tipo, especifique aquí el proveedor que desea utilizar.
- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.

- **Dominio:** Escriba un nombre de dominio opcional.
- **Rol:** Escriba un nombre de rol opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
- Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
- Si habilita **Certificado**, configure estos ajustes:
  - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea utilizar. El valor predeterminado es **Ninguno**.
  - **Solicitar PIN al conectar:** Seleccione si desea solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
  - **Habilitar VPN a petición:** Seleccione si desea habilitar la activación de una conexión VPN cuando los usuarios se conecten a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los ajustes cuando **Habilitar VPN a petición** está **Activado**, consulte Configurar los ajustes de Habilitar VPN a petición para iOS.
  - **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si habilita esta opción, configure los siguientes ajustes:
  - **Aplicación de coincidencia a petición habilitada:** Seleccione si las conexiones VPN por aplicación se activan automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red. El valor predeterminado es **Desactivado**.
  - **Tipo de proveedor:** Seleccione si la VPN por aplicación se proporciona como un **Proxy de aplicación** o como un **Túnel de paquetes**. El valor predeterminado es **Proxy de aplicación**.
  - **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que desee incluir, haga clic en **Agregar** y realice lo siguiente:
  - **Dominio:** Escriba el dominio que desea agregar.
- Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo F5 SSL para iOS

- **Identificador de paquete del proveedor:** Si su perfil VPN por aplicación tiene el identificador de paquete de una aplicación con varios proveedores VPN del mismo tipo, especifique aquí el proveedor que desea utilizar.

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
    - Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
    - Si habilita **Certificado**, configure los siguientes ajustes:
        - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea usar. El valor predeterminado es **Ninguno**.
        - **Solicitar PIN al conectar:** Seleccione si se debe solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
        - **Habilitar VPN a petición:** Seleccione si se debe habilitar la activación de una conexión VPN cuando los usuarios se conecten a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los ajustes cuando **Habilitar VPN a petición** está **Activado**, consulte Configurar los ajustes de Habilitar VPN a petición para iOS.
- **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si habilita esta opción, configure estos ajustes:
    - **Aplicación de coincidencia a petición habilitada:** Seleccione si las conexiones VPN por aplicación se activan automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red.
    - **Tipo de proveedor:** Seleccione si la VPN por aplicación se proporciona como un **proxy de aplicación** o como un **túnel de paquetes**. El valor predeterminado es **proxy de aplicación**.
    - **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que desee incluir, haga clic en **Agregar** y haga lo siguiente:
        - **Dominio:** Escriba el dominio que desea agregar.
        - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardar el dominio.

Configurar el protocolo SonicWALL para iOS

- **Identificador de paquete del proveedor:** Si su perfil VPN por aplicación tiene el identificador de paquete de una aplicación con varios proveedores VPN del mismo tipo, especifique aquí el proveedor que desea usar.
- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Grupo o dominio de inicio de sesión:** Escriba un grupo o dominio de inicio de sesión opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
    - Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
    - Si habilita **Certificado**, configure estos ajustes:
        - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea usar. El valor predeterminado es **Ninguno**.
        - **Solicitar PIN al conectar:** Seleccione si desea solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
        - **Habilitar VPN a petición:** Seleccione si desea habilitar la activación de una conexión VPN cuando los usuarios se conecten a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los ajustes cuando **Habilitar VPN a petición** está **Activado**, consulte (#configure-enable-vpn-on-demand-options-for-ios).
- **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si establece esta opción en Activado, configure estos ajustes:
    - **Aplicación de coincidencia a petición habilitada:** Seleccione si las conexiones VPN por aplicación se activan automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red.
    - **Tipo de proveedor:** Seleccione si la VPN por aplicación se proporciona como un **Proxy de aplicación** o como un **Túnel de paquetes**. El valor predeterminado es **Proxy de aplicación**.

- **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que desee incluir, haga clic en **Agregar** y haga lo siguiente:
  - **Dominio:** Escriba el dominio que desea agregar.
  - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo Ariba VIA para iOS

- **Identificador de paquete del proveedor:** Si su perfil VPN por aplicación tiene el identificador de paquete de una aplicación con varios proveedores de VPN del mismo tipo, especifique aquí el proveedor que desea usar.
- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, configure estos parámetros:
    - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que quiere usar. El valor predeterminado es **Ninguno**.
    - **Solicitar PIN al conectar:** Seleccione si quiere solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
    - **Habilitar VPN a petición:** Seleccione si quiere habilitar la activación de una conexión VPN cuando los usuarios se conecten a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los parámetros cuando **Habilitar VPN a petición** está **Activado**, consulte Configurar los parámetros de Habilitar VPN a petición para iOS.
- **Habilitar VPN por aplicación:** Seleccione si quiere habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si habilita esta opción, configure estos parámetros:
  - **Aplicación de coincidencia a petición habilitada:** Seleccione si las conexiones VPN por aplicación se activan automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red.

- **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que quiera incluir, haga clic en **Agregar** y haga lo siguiente:
  - **Dominio:** Escriba el dominio que quiere agregar.
  - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardarlo.

Configurar protocolos IKEv2 para iOS

Esta sección incluye los parámetros utilizados para los protocolos IKEv2, Always On IKEv2 y Always On IKEv2 Dual Configuration. Para el protocolo Always On IKEv2 Dual Configuration, configure todos estos parámetros para redes móviles y Wi-Fi.

- **Permitir al usuario deshabilitar la conexión automática:** Para los protocolos Always On. Seleccione si quiere permitir a los usuarios deshabilitar la conexión automática a la red en sus dispositivos. El valor predeterminado es **Desactivado**.
- **Nombre de host o dirección IP del servidor:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Identificador local:** El FQDN o la dirección IP del cliente IKEv2. Este campo es obligatorio.
- **Identificador remoto:** El FQDN o la dirección IP del servidor VPN. Este campo es obligatorio.
- **Autenticación de dispositivo:** Elija **Secreto compartido**, **Certificado** o **Certificado de dispositivo basado en identificador de dispositivo** para el tipo de autenticación de esta conexión. El valor predeterminado es **Secreto compartido**.
  - Si elige **Secreto compartido**, escriba una clave de secreto compartido opcional.
  - Si elige **Certificado**, elija una **Credencial de identidad** para usar. El valor predeterminado es **Ninguno**.
  - Si elige **Certificado de dispositivo basado en identificador de dispositivo**, elija el **Tipo de identidad de dispositivo** que desea usar. El valor predeterminado es **IMEI**. Para usar esta opción, importe certificados de forma masiva mediante la API de REST. Consulte (/es-es/citrix-endpoint-management/authentication/upload-renew-certificates.html#upload-certificates-in-bulk-using-the-rest-api). Solo disponible cuando selecciona **IKEv2 siempre activo**.
- **Autenticación extendida habilitada:** Seleccione si desea habilitar el Protocolo de autenticación extendida (EAP). Si está **Activado**, escriba la **Cuenta de usuario** y la **Contraseña de autenticación**.

- **Intervalo de detección de pares inactivos:** Elija la frecuencia con la que se contacta con un dispositivo par para asegurarse de que el dispositivo par siga siendo accesible. El valor predeterminado es **Ninguno**. Las opciones son:
  - **Ninguno:** Deshabilita la detección de pares inactivos.
  - **Bajo:** Contacta con el par cada 30 minutos.
  - **Medio:** Contacta con el par cada 10 minutos.
  - **Alto:** Contacta con el par cada 1 minuto.
- **Deshabilitar movilidad y multihoming:** Elija si desea deshabilitar esta función.
- **Usar atributos de subred interna IPv4/IPv6:** Elija si desea habilitar esta función.
- **Deshabilitar redireccionamientos:** Elija si desea deshabilitar los redireccionamientos.
- **Habilitar reserva:** Si está habilitada, esta configuración permite que un túnel a través de datos móviles transporte tráfico que sea apto para Wi-Fi Assist y requiera una VPN. El valor predeterminado es **Desactivado**.
- **Habilitar NAT keepalive mientras el dispositivo está inactivo:** Para los protocolos Always On. Los paquetes keepalive mantienen las asignaciones NAT para las conexiones IKEv2. El chip envía estos paquetes a intervalos regulares cuando el dispositivo está activo. Si esta configuración está activada, el chip envía paquetes keepalive incluso mientras el dispositivo está inactivo. El intervalo predeterminado es de 20 segundos a través de Wi-Fi y 110 segundos a través de datos móviles. Puede cambiar el intervalo mediante el parámetro de intervalo de NAT keepalive.
- **Intervalo de NAT keepalive (segundos):** El valor predeterminado es 20 segundos.
- **Habilitar secreto perfecto hacia adelante:** Elija si desea habilitar esta función.
- **Direcciones IP del servidor DNS:** Opcional. Una lista de cadenas de direcciones IP del servidor DNS. Estas direcciones IP pueden incluir una mezcla de direcciones IPv4 e IPv6. Haga clic en **Agregar** para escribir una dirección.
- **Nombre de dominio:** Opcional. El dominio principal del túnel.
- **Dominios de búsqueda:** Opcional. Una lista de cadenas de dominio utilizadas para calificar completamente los nombres de host de etiqueta única.
- **Anexar dominios de coincidencia suplementarios a la lista del resolvedor:** Opcional. Determina si se debe agregar la lista de dominios de coincidencia suplementarios a la lista de dominios de búsqueda del resolvedor. El valor predeterminado es **Activado**.
- **Dominios de coincidencia suplementarios:** Opcional. Una lista de cadenas de dominio utilizadas para determinar qué consultas DNS deben usar la configuración del resolvedor DNS

que se encuentra en las direcciones del servidor DNS. Esta clave crea una configuración de DNS dividido donde solo los hosts en ciertos dominios se resuelven utilizando el resolvedor DNS del túnel. Los hosts que no están en uno de los dominios de esta lista se resuelven utilizando el resolvedor predeterminado del sistema.

Si este parámetro tiene una cadena vacía, esa cadena es el dominio predeterminado. Como resultado, una configuración de túnel dividido puede dirigir todas las consultas DNS a los servidores DNS de la VPN antes que a los servidores DNS principales. Si el túnel VPN es la ruta predeterminada de la red, los servidores DNS enumerados se convierten en el resolvedor predeterminado. En ese caso, la lista de dominios de coincidencia suplementarios se ignora.

- **Parámetros de SA de IKE** y **Parámetros de SA secundaria:** Configure estos ajustes para cada opción de parámetros de Asociación de seguridad (SA):
  - **Algoritmo de cifrado:** En la lista, seleccione el algoritmo de cifrado IKE que desea usar. El valor predeterminado es **3DES**.
  - **Algoritmo de integridad:** En la lista, seleccione el algoritmo de integridad que desea usar. El valor predeterminado es **SHA-256**.
  - **Grupo Diffie Hellman:** En la lista, seleccione el número de grupo Diffie Hellman. El valor predeterminado es **2**.
  - **Tiempo de vida de IKE en minutos:** Escriba un número entero entre 10 y 1440 que represente el tiempo de vida de la SA (intervalo de nueva clave). El valor predeterminado es **1440** minutos.
- **Excepciones de servicio:** Para los protocolos Always On. Las excepciones de servicio son servicios del sistema que están exentos de la VPN Always On. Configure estos ajustes de excepciones de servicio:
  - **Buzón de voz:** En la lista, seleccione cómo gestionar la excepción del buzón de voz. El valor predeterminado es **Permitir tráfico a través del túnel**.
  - **AirPrint:** En la lista, seleccione cómo gestionar la excepción de AirPrint. El valor predeterminado es **Permitir tráfico a través del túnel**.
  - **Permitir tráfico desde la hoja web cautiva fuera del túnel VPN:** Seleccione si desea permitir a los usuarios conectarse a puntos de acceso públicos fuera del túnel VPN. El valor predeterminado es **Desactivado**.
  - **Permitir tráfico de todas las aplicaciones de red cautivas fuera del túnel VPN:** Seleccione si desea permitir todas las aplicaciones de red de puntos de acceso fuera del túnel VPN. El valor predeterminado es **Desactivado**.

    - **Identificadores de paquete de aplicaciones de red cautivas:** Para cada identificador de paquete de aplicación de red de punto de acceso al que los usuarios pueden acceder, haga clic en **Agregar** y escriba el **Identificador de paquete** de la aplicación de red de punto de acceso. Haga clic en **Guardar** para guardar el identificador de paquete de la aplicación.

- **VPN por aplicación:** Configure estos ajustes para los tipos de conexión IKEv2.
    - **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**.
    - **Aplicación de coincidencia bajo demanda habilitada:** Seleccione si las conexiones VPN por aplicación se activan automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red. El valor predeterminado es **Desactivado**.
    - **Dominios de Safari:** Haga clic en **Agregar** para añadir un nombre de dominio de Safari.
- **Configuración de proxy:** Elija cómo la conexión VPN se enruta a través de un servidor proxy. El valor predeterminado es **Ninguno**.

Configurar el protocolo Citrix SSO para iOS

El cliente Citrix SSO está disponible en la Apple Store.

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
    - Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
    - Si habilita **Certificado**, configure estos parámetros:
        - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que quiere usar. El valor predeterminado es **Ninguno**.
        - **Solicitar PIN al conectar:** Seleccione si quiere solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
        - **Habilitar VPN a petición:** Seleccione si quiere habilitar la activación de una conexión VPN cuando los usuarios se conecten a la red. El valor predeterminado es

Desactivado. Para obtener información sobre cómo configurar los parámetros cuando **Habilitar VPN a petición** está **Activado**, consulte Configurar los parámetros de Habilitar VPN a petición para iOS.

- **Habilitar VPN por aplicación:** Seleccione si quiere habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si establece esta opción en Activado, configure los siguientes parámetros:
  - **Aplicación de coincidencia a petición habilitada:** Seleccione si las conexiones VPN por aplicación se activan automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red.
  - **Tipo de proveedor:** Seleccione si la VPN por aplicación se proporciona como un **proxy de aplicación** o como un **túnel de paquetes**. El valor predeterminado es **proxy de aplicación**.
  - **Tipo de proveedor:** Establezca en **Túnel de paquetes**.
  - **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que quiera incluir, haga clic en **Agregar** y haga lo siguiente:
    - **Dominio:** Escriba el dominio que quiere agregar.
    - Haga clic en **Guardar** para guardar el dominio o en **Cancelar** para no guardarlo.
- **XML personalizado:** Para cada parámetro XML personalizado que quiera agregar, haga clic en **Agregar** y especifique los pares clave/valor. Los parámetros disponibles son:
  - **disableL3:** Deshabilita la VPN a nivel de sistema. Solo permite la VPN por aplicación. No se necesita ningún **Valor**.
  - **agente de usuario:** Asocia a esta directiva de dispositivo cualquier directiva de NetScaler Gateway dirigida a clientes de complemento VPN. Para las solicitudes iniciadas por el complemento, el **Valor** de esta clave se añade automáticamente al complemento VPN.

Configurar el protocolo SSL personalizado para iOS

Para pasar del cliente Cisco Legacy AnyConnect al cliente Cisco AnyConnect:

1. Configure la directiva de dispositivo VPN con el protocolo SSL personalizado. Implemente la directiva en los dispositivos iOS.
2. Cargue el cliente Cisco AnyConnect desde `<https://apps.apple.com/us/app/cisco-secure-client/id1135064690>`, añada la aplicación a Citrix Endpoint Management y, a continuación, implemente la aplicación en los dispositivos iOS.

3. Quite la directiva de dispositivo VPN antigua de los dispositivos iOS.

Configuración:

- **Identificador SSL personalizado (formato DNS inverso):** Establézcalo en el identificador de paquete. Para el cliente Cisco AnyConnect, use **com.cisco.anyconnect**.
- **Identificador de paquete del proveedor:** Si la aplicación especificada en **Identificador SSL personalizado** tiene varios proveedores VPN del mismo tipo (proxy de aplicación o túnel de paquetes), especifique este identificador de paquete. Para el cliente Cisco AnyConnect, use **com.cisco.anyconnect**.
- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
    - Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
    - Si habilita **Certificado**, configure estos ajustes:
        - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea usar. El valor predeterminado es **Ninguno**.
        - **Solicitar PIN al conectar:** Seleccione si desea solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
        - **Habilitar VPN a petición:** Seleccione si desea habilitar la activación de una conexión VPN cuando los usuarios se conecten a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los ajustes cuando **Habilitar VPN a petición** está **Activado**, consulte Configurar los ajustes de Habilitar VPN a petición para iOS.
- **Incluir todas las redes:** Seleccione si desea permitir que todas las redes utilicen esta conexión. El valor predeterminado es **Desactivado**.
- **Excluir redes locales:** Seleccione si desea excluir las redes locales del uso de la conexión o permitir las redes. El valor predeterminado es **Desactivado**.
- **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si establece esta opción en Activado, configure los siguientes ajustes:

- **Aplicación de coincidencia a petición habilitada:** Seleccione si las conexiones VPN por aplicación se activan automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red.
- **Tipo de proveedor:** Un tipo de proveedor indica si el proveedor es un servicio VPN o un servicio proxy. Para el servicio VPN, elija **Túnel de paquetes**. Para el servicio proxy, elija **Proxy de aplicación**. Para el cliente Cisco AnyConnect, elija **Túnel de paquetes**.
- **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que desee incluir, haga clic en **Agregar** y haga lo siguiente:
  - **Dominio:** Escriba el dominio que desea agregar.
  - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardarlo.

- **XML personalizado:** Para cada parámetro XML personalizado que desee agregar, haga clic en **Agregar** y haga lo siguiente:
  - **Nombre del parámetro:** Escriba el nombre del parámetro que desea agregar.
  - **Valor:** Escriba el valor asociado al **Nombre del parámetro**.
  - Haga clic en **Guardar** para guardar el parámetro o haga clic en **Cancelar** para no guardarlo.

Configurar la directiva de dispositivo VPN para admitir NAC

1. El **tipo de conexión** de **SSL personalizado** es necesario para configurar el filtro NAC.
2. Especifique un **nombre de conexión** de **VPN**.
3. Para **identificador SSL personalizado**, escriba **com.citrix.NetScalerGateway.ios.app**
4. Para **identificador de paquete de proveedor**, escriba **com.citrix.NetScalerGateway.ios.app.vpnplugin**

Los valores de los pasos 3 y 4 provienen de la instalación de Citrix SSO necesaria para el filtrado NAC. No configure una contraseña de autenticación. Para obtener más información sobre el uso de la función NAC, consulte Control de acceso a la red.

Configurar las opciones de habilitación de VPN a petición para iOS

- **Dominio a petición:** Para cada dominio y la acción asociada que se debe realizar cuando los usuarios se conectan, haga clic en **Agregar** y haga lo siguiente:
- **Dominio:** Escriba el dominio que se va a agregar.

- **Acción:** En la lista, seleccione una de las acciones posibles:
  - **Establecer siempre:** El dominio siempre activa una conexión VPN.
  - **Nunca establecer:** El dominio nunca activa una conexión VPN.
  - **Establecer si es necesario:** El dominio activa un intento de conexión VPN si la resolución del nombre de dominio falla. El fallo ocurre cuando el servidor DNS no puede resolver el dominio, redirige a un servidor diferente o agota el tiempo de espera.
  - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardar el dominio.
- **Reglas a petición**
  - **Acción:** En la lista, seleccione la acción que se va a realizar. El valor predeterminado es **EvaluateConnection**. Las acciones posibles son:
    - **Permitir:** Permite que la VPN a petición se conecte cuando se active.
    - **Conectar:** Inicia una conexión VPN incondicionalmente.
    - **desconectar:** Elimina la conexión VPN y no se vuelve a conectar a petición mientras la regla coincida.
    - **EvaluateConnection:** Evalúa la matriz ActionParameters para cada conexión.
    - **Ignorar:** Mantiene cualquier conexión VPN existente, pero no se vuelve a conectar a petición mientras la regla coincida.
  - **DNSDomainMatch:** Para cada dominio con el que pueda coincidir la lista de dominios de búsqueda de un dispositivo que quiera agregar, haga clic en **Agregar** y haga lo siguiente:
    - **Dominio DNS:** Escriba el nombre de dominio. Puede usar el prefijo comodín "*" para que coincida con varios dominios. Por ejemplo, *.example.com coincide con mydomain.example.com, yourdomain.example.com y herdomain.example.com.
    - Haga clic en **Guardar** para guardar el dominio o en **Cancelar** para no guardarlo.
  - **DNSServerAddressMatch:** Para cada dirección IP con la que pueda coincidir cualquiera de los servidores DNS especificados de la red que quiera agregar, haga clic en **Agregar** y haga lo siguiente:
    - **Dirección del servidor DNS:** Escriba la dirección del servidor DNS que quiera agregar. Puede usar el sufijo comodín "*" para que coincida con los servidores DNS. Por ejemplo, 17.* coincide con cualquier servidor DNS de la subred de clase A.

    - Haga clic en **Guardar** para guardar la dirección del servidor DNS o en **Cancelar** para no guardar la dirección del servidor DNS.

- **InterfaceTypeMatch:** En la lista, seleccione el tipo de hardware de interfaz de red principal en uso. El valor predeterminado es **Sin especificar**. Los valores posibles son:
    - **Sin especificar:** Coincide con cualquier hardware de interfaz de red. Esta opción es la predeterminada.
    - **Ethernet:** Coincide solo con hardware de interfaz de red Ethernet.
    - **WiFi:** Coincide solo con hardware de interfaz de red Wi-Fi.
    - **Celular:** Coincide solo con el hardware de la interfaz de red celular.
- **SSIDMatch:** Para cada SSID que desee hacer coincidir con la red actual que desea agregar, haga clic en **Agregar** y haga lo siguiente.
    - **SSID:** Escriba el SSID que desea agregar. Si la red no es una red Wi-Fi, o si el SSID no aparece, la coincidencia falla. Deje esta lista vacía para que coincida con cualquier SSID.
    - Haga clic en **Guardar** para guardar el SSID o en **Cancelar** para no guardarlo.
- **URLStringProbe:** Escriba una URL para obtener. Si esta URL se obtiene correctamente sin redirección, esta regla coincide.
- **ActionParameters : Domains:** Para cada dominio que EvaluateConnection comprueba y que desea agregar, haga clic en **Agregar** y haga lo siguiente:
    - **Dominio:** Escriba el dominio que se va a agregar.
    - Haga clic en **Guardar** para guardar el dominio o en **Cancelar** para no guardarlo.
- **ActionParameters : DomainAction:** En la lista, seleccione el **comportamiento de VPN** para los dominios **ActionParameters : Domains** especificados. El valor predeterminado es **ConnectIfNeeded**. Las acciones posibles son:
    - **ConnectIfNeeded:** El dominio activa un intento de conexión VPN si la resolución del nombre de dominio falla. El fallo ocurre cuando el servidor DNS no puede resolver el dominio, redirige a un servidor diferente o agota el tiempo de espera.
    - **NeverConnect:** El dominio nunca activa una conexión VPN.
- **Parámetros de acción: RequiredDNSServers:** Para cada servidor DNS que se utilizará para resolver los dominios especificados, haga clic en **Agregar** y haga lo siguiente:

    - **Servidor DNS:** Válido solo cuando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Escriba la dirección IP del servidor DNS. Este servidor puede estar fuera de la configuración de red actual del dispositivo. Si el servidor DNS no es accesible, se establece una conexión VPN en respuesta. Asegúrese de que el servidor DNS sea un servidor DNS interno o un servidor DNS externo de confianza.
    - Haga clic en **Guardar** para guardar el servidor DNS o en **Cancelar** para no guardarlo.
  - **ActionParameters : RequiredURLStringProbe:** Opcionalmente, escriba una URL HTTP o HTTPS (preferida) para sondear, utilizando una solicitud GET. Si el nombre de host de la URL no se puede resolver, el servidor no es accesible o el servidor no responde, se establece una conexión VPN. Válido solo cuando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.
  - **OnDemandRules : Contenido XML:** Escriba, o copie y pegue, las reglas XML de configuración a petición.
    - Haga clic en **Comprobar diccionario** para validar el código XML. **XML válido** aparece debajo del cuadro de texto **Contenido XML** si el XML es válido. Si no es válido, un mensaje de error describe el error.

- **Proxy**
  - **Configuración del proxy:** En la lista, seleccione cómo la conexión VPN se enruta a través de un servidor proxy. El valor predeterminado es **Ninguno**.
    - Si habilita **Manual**, configure estos ajustes:
      - **Nombre de host o dirección IP del servidor proxy:** Escriba el nombre de host o la dirección IP del servidor proxy. Este campo es obligatorio.
      - **Puerto del servidor proxy:** Escriba el número de puerto del servidor proxy. Este campo es obligatorio.
      - **Nombre de usuario:** Escriba un nombre de usuario opcional para el servidor proxy.
      - **Contraseña:** Escriba una contraseña opcional para el servidor proxy.
    - Si configura **Automático**, configure este ajuste:
      - **URL del servidor proxy:** Escriba la URL del servidor proxy. Este campo es obligatorio.

- **Configuración de la directiva**

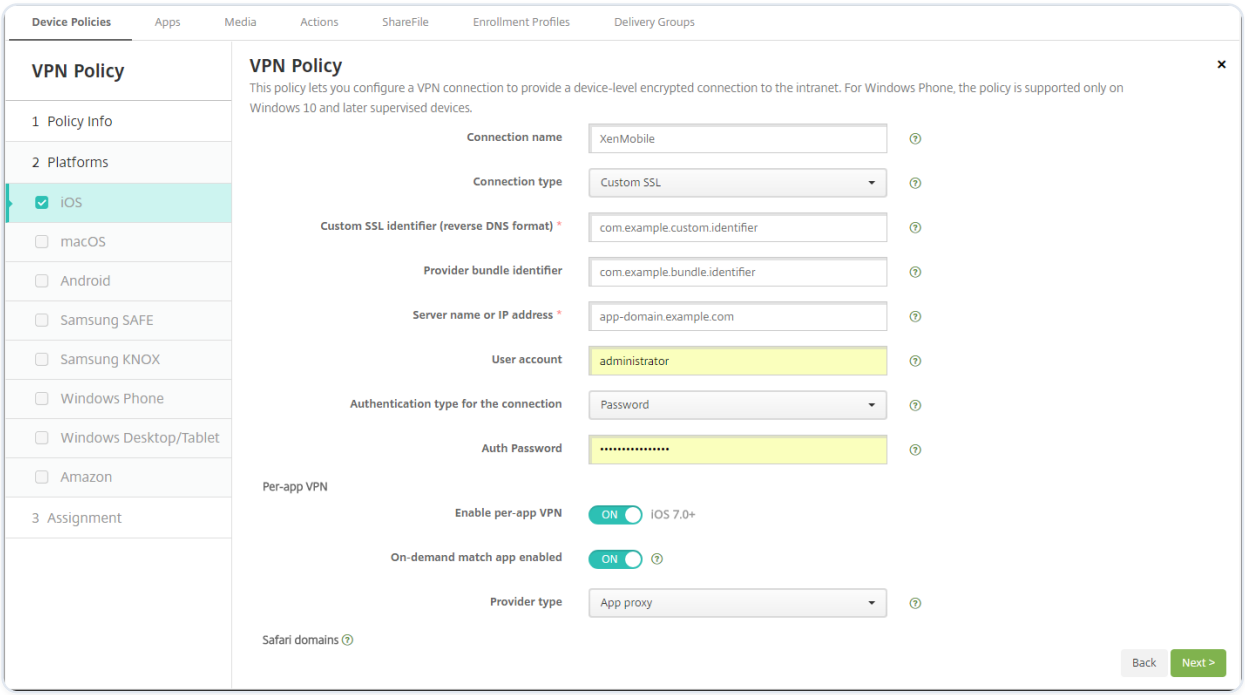
- **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
  - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
  - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva. Solo disponible para iOS 6.0 y versiones posteriores.

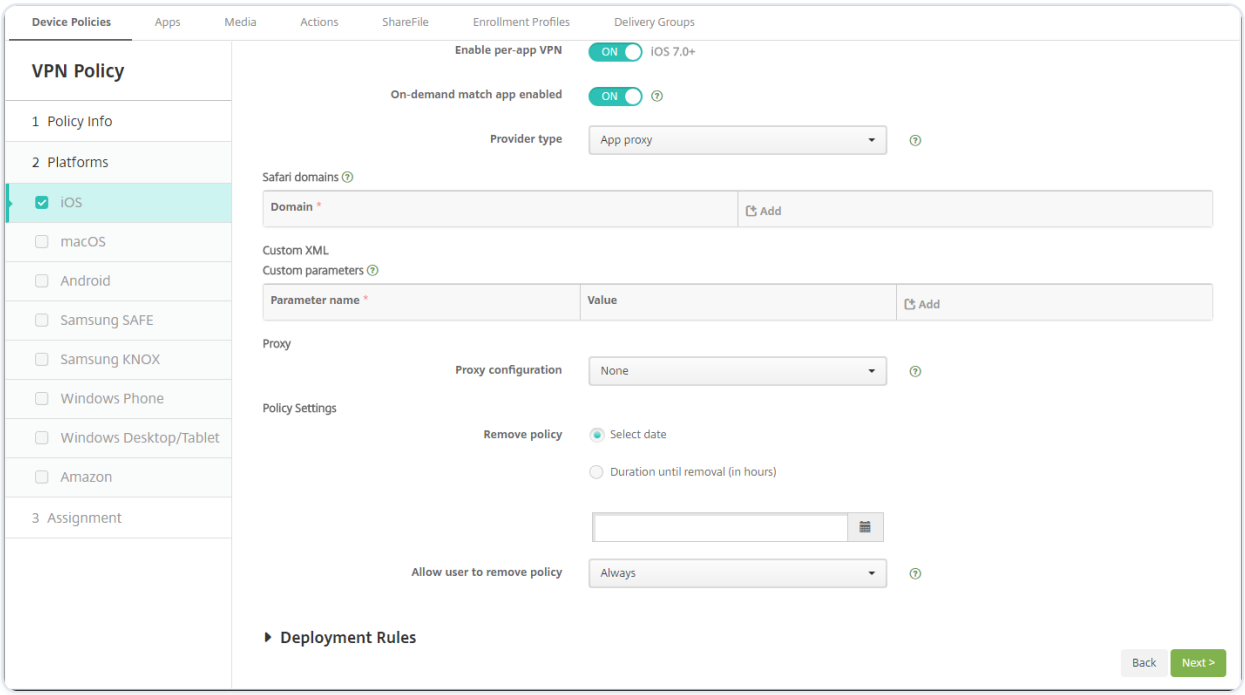
Configurar una VPN por aplicación

Las opciones de VPN por aplicación para iOS están disponibles para estos tipos de conexión: Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN, Citrix SSO y Custom SSL.

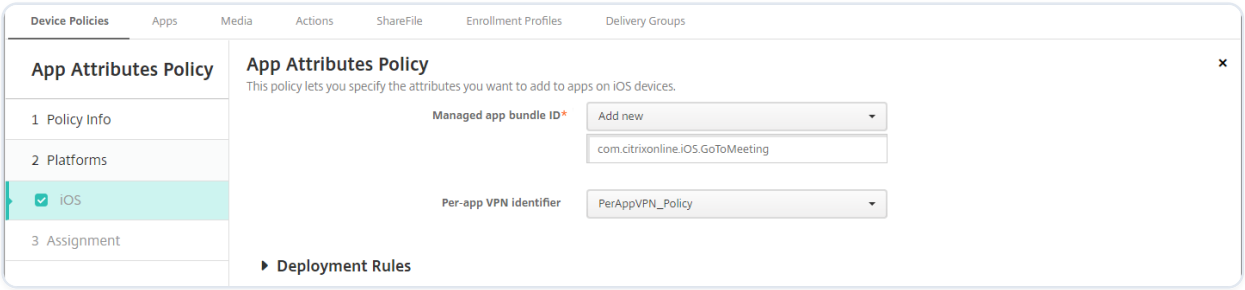
Para configurar una VPN por aplicación:

1. En **Configurar > Directivas de dispositivo**, cree una directiva VPN. Por ejemplo:

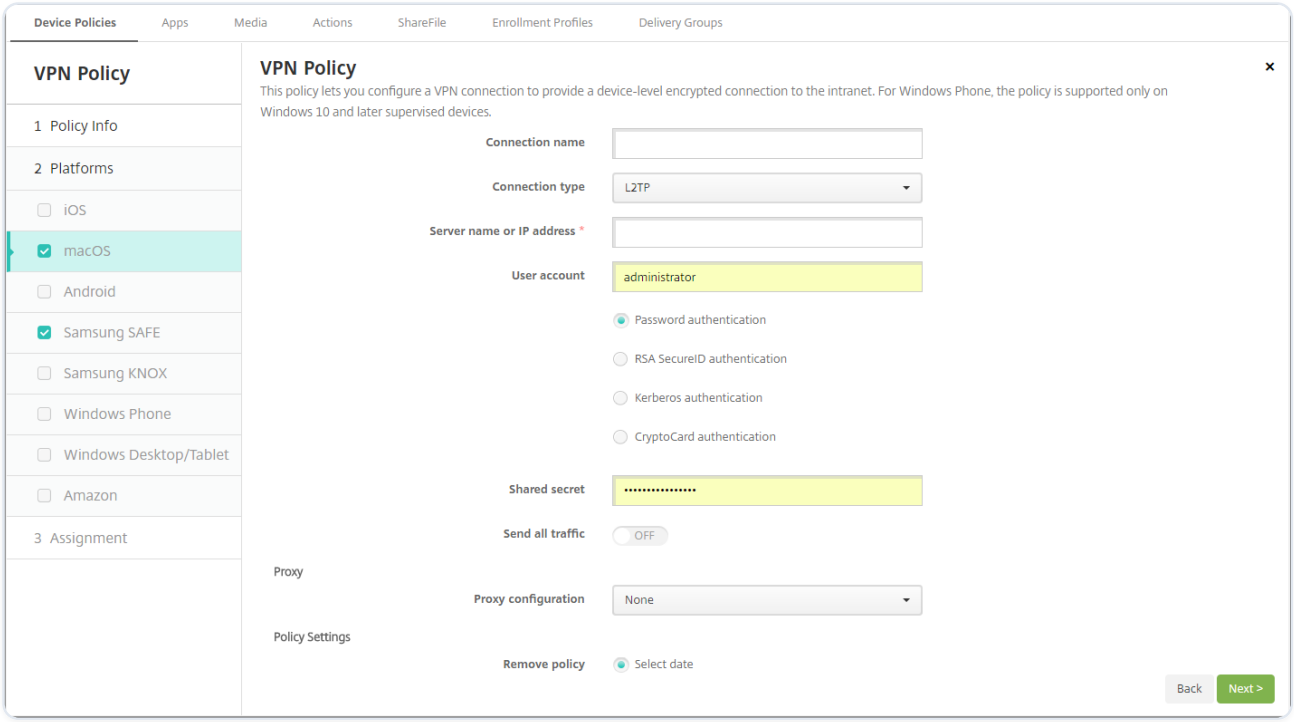




2. En **Configurar > Directivas de dispositivo**, cree una directiva de Atributos de aplicación para asociar una aplicación a la directiva VPN por aplicación. En **Identificador de VPN por aplicación**, elija el nombre de la directiva VPN creada en el paso 1. En **ID de paquete de aplicación administrada**, elija de la lista de aplicaciones o escriba el ID de paquete de aplicación. (Si implementa una directiva de inventario de aplicaciones iOS, la lista de aplicaciones contendrá las aplicaciones).



Configuración de macOS



- **Nombre de conexión:** Escriba un nombre para la conexión.
- **Tipo de conexión:** En la lista, seleccione el protocolo que se utilizará para esta conexión. El valor predeterminado es L2TP.
    - **L2TP:** Protocolo de tunelización de capa 2 con autenticación de clave precompartida.
    - **PPTP:** Tunelización punto a punto.
    - **IPSec:** Su conexión VPN corporativa.
    - **Cisco AnyConnect:** Cliente VPN Cisco AnyConnect.
    - **Juniper SSL:** Cliente VPN SSL de Juniper Networks.
    - **F5 SSL:** Cliente VPN SSL de F5 Networks.
    - **SonicWALL Mobile Connect:** Cliente VPN unificado de Dell para iOS.
    - **Ariba VIA:** Cliente de acceso a Internet virtual de Ariba Networks.
    - **Citrix VPN:** Cliente VPN de Citrix.
    - **SSL personalizado:** Capa de sockets seguros personalizada.

Las siguientes secciones enumeran las opciones de configuración para cada uno de los tipos de conexión anteriores.

Configurar el protocolo L2TP para macOS

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- Seleccione **Autenticación de contraseña**, **Autenticación RSA SecurID**, **Autenticación Kerberos** o **Autenticación CryptoCard**. La opción predeterminada es **Autenticación de contraseña**.
- **Secreto compartido:** Escriba la clave de secreto compartido de IPsec.
- **Enviar todo el tráfico:** Seleccione si desea enviar todo el tráfico a través de la VPN. La opción predeterminada es **Desactivado**.

Configurar el protocolo PPTP para macOS

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- Seleccione **Autenticación por contraseña**, **Autenticación RSA SecurID**, **Autenticación Kerberos** o **Autenticación CryptoCard**. El valor predeterminado es **Autenticación por contraseña**.
- **Nivel de cifrado:** Seleccione el nivel de cifrado deseado. El valor predeterminado es **Ninguno**.
  - **Ninguno:** No usar cifrado.
  - **Automático:** Usar el nivel de cifrado más seguro compatible con el servidor.
  - **Máximo** (128 bits): Usar siempre cifrado de 128 bits.
- **Enviar todo el tráfico:** Seleccione si desea enviar todo el tráfico a través de la VPN. El valor predeterminado es **Desactivado**.

Configurar el protocolo IPsec para macOS

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Secreto compartido** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Secreto compartido**.

- Si habilita la autenticación de **Secreto compartido**, configure estos ajustes:
  - **Nombre del grupo:** Escriba un nombre de grupo opcional.
  - **Secreto compartido:** Escriba una clave de secreto compartido opcional.
  - **Usar autenticación híbrida:** Seleccione si desea usar la autenticación híbrida. Con la autenticación híbrida, el servidor se autentica primero con el cliente y, a continuación, el cliente se autentica con el servidor. El valor predeterminado es **Desactivado**.
  - **Solicitar contraseña:** Seleccione si desea solicitar a los usuarios sus contraseñas cuando se conecten a la red. El valor predeterminado es **Desactivado**.
- Si habilita la autenticación por **Certificado**, configure estos ajustes:
  - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea usar. El valor predeterminado es **Ninguno**.
  - **Solicitar PIN al conectar:** Seleccione si desea exigir a los usuarios que introduzcan su PIN al conectarse a la red. El valor predeterminado es **Desactivado**.
  - **Habilitar VPN a petición:** Seleccione si desea habilitar la activación de una conexión VPN cuando los usuarios se conecten a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los ajustes cuando **Habilitar VPN a petición** está en **Activado**, consulte Configurar las opciones de Habilitar VPN a petición.

Configurar el protocolo Cisco AnyConnect para macOS

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Grupo:** Escriba un nombre de grupo opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, configure estos ajustes:
    - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea usar. El valor predeterminado es **Ninguno**.

- **Solicitar PIN al conectar:** Seleccione si desea solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
- **Habilitar VPN a petición:** Seleccione si desea habilitar la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los ajustes cuando **Habilitar VPN a petición** está **Activado**, consulte Configurar las opciones de Habilitar VPN a petición.

- **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si habilita esta opción, configure estos ajustes:
  - **Aplicación de coincidencia a petición habilitada:** Seleccione si una conexión VPN por aplicación se activa automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red. El valor predeterminado es **Desactivado**.
  - **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que desee incluir, haga clic en **Agregar** y haga lo siguiente:
    - **Dominio:** Escriba el dominio que se va a agregar.
    - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo SSL de Juniper para macOS

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Dominio:** Escriba un nombre de dominio opcional.
- **Rol:** Escriba un nombre de rol opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, configure estos ajustes:
    - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea usar. El valor predeterminado es **Ninguno**.

    - **Solicitar PIN al conectar:** Seleccione si desea solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
    - **Habilitar VPN a petición:** Seleccione si desea habilitar la activación de una conexión VPN cuando los usuarios se conecten a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los ajustes cuando **Habilitar VPN a petición** está **Activado**, consulte Configurar los ajustes de Habilitar VPN a petición.

- **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si habilita esta opción, configure los siguientes ajustes:
    - **Aplicación de coincidencia a petición habilitada:** Seleccione si una conexión VPN por aplicación se activa automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red. El valor predeterminado es **Desactivado**.
    - **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que desee incluir, haga clic en **Agregar** y realice lo siguiente:
        - **Dominio:** Escriba el dominio que se va a agregar.
        - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo F5 SSL para macOS

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
    - Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
    - Si habilita **Certificado**, configure estos ajustes:
        - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea usar. El valor predeterminado es **Ninguno**.
        - **Solicitar PIN al conectar:** Seleccione si desea solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.

    - **Habilitar VPN a petición:** Seleccione si desea habilitar la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los ajustes cuando **Habilitar VPN a petición** está **Activado**, consulte Configurar los ajustes de Habilitar VPN a petición.

- **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si habilita esta opción, configure estos ajustes:

    - **Aplicación de coincidencia a petición habilitada:** Seleccione si la conexión VPN por aplicación se activa automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red. El valor predeterminado es **Desactivado**.
    - **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que desee incluir, haga clic en **Agregar** y realice lo siguiente:

        - **Dominio:** Escriba el dominio que se va a agregar.
        - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo SonicWALL Mobile Connect para macOS

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Grupo de inicio de sesión o dominio:** Escriba un grupo de inicio de sesión o dominio opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.

    - Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
    - Si habilita **Certificado**, configure estos ajustes:

        - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea utilizar. El valor predeterminado es **Ninguno**.
        - **Solicitar PIN al conectar:** Seleccione si desea solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.

    - **Habilitar VPN bajo demanda:** Seleccione si desea habilitar la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los ajustes cuando **Habilitar VPN bajo demanda** está **Activado**, consulte Configurar los ajustes de Habilitar VPN bajo demanda.

- **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si habilita esta opción, configure estos ajustes:

    - **Aplicación de coincidencia bajo demanda habilitada:** Seleccione si la conexión VPN por aplicación se activa automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red. El valor predeterminado es **Desactivado**.
    - **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que desee incluir, haga clic en **Agregar** y realice lo siguiente:

        - **Dominio:** Escriba el dominio que se va a agregar.
        - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo Ariba VIA para macOS

- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.

    - Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
    - Si habilita **Certificado**, configure estos ajustes:

        - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea usar. El valor predeterminado es **Ninguno**.
        - **Solicitar PIN al conectar:** Seleccione si desea solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
        - **Habilitar VPN bajo demanda:** Seleccione si desea habilitar la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información sobre cómo configurar los ajustes cuando

Habilitar VPN bajo demanda está **Activado**, consulte Configurar los ajustes de Habilitar VPN bajo demanda.

- **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si habilita esta opción, configure los siguientes ajustes:
  - **Coincidencia de aplicación bajo demanda habilitada:** Seleccione si la conexión VPN por aplicación se activa automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red. El valor predeterminado es **Desactivado**.
  - **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que desee incluir, haga clic en **Agregar** y haga lo siguiente:
    - **Dominio:** Escriba el dominio que se va a agregar.
    - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo SSL personalizado para macOS

- **Identificador SSL personalizado (formato DNS inverso):** Escriba el identificador SSL en formato DNS inverso. Este campo es obligatorio.
- **Nombre del servidor o dirección IP:** Escriba el nombre del servidor o la dirección IP del servidor VPN. Este campo es obligatorio.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
  - **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
  - Si habilita **Contraseña**, escriba una contraseña de autenticación opcional en el campo **Contraseña de autenticación**.
  - Si habilita **Certificado**, configure los siguientes ajustes:
    - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que desea usar. El valor predeterminado es **Ninguno**.
    - **Solicitar PIN al conectar:** Seleccione si desea solicitar a los usuarios su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
    - **Habilitar VPN bajo demanda:** Seleccione si desea habilitar la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es

Desactivado. Para obtener información sobre cómo configurar los ajustes cuando **Habilitar VPN bajo demanda** está **Activado**, consulte Configurar los ajustes de Habilitar VPN bajo demanda.

- **VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. El valor predeterminado es **Desactivado**. Si habilita esta opción, configure los siguientes ajustes:
  - **Coincidencia de aplicación bajo demanda habilitada:** Seleccione si las conexiones VPN por aplicación se activan automáticamente cuando las aplicaciones vinculadas al servicio VPN por aplicación inician la comunicación de red.
  - **Dominios de Safari:** Para cada dominio de Safari que pueda activar una conexión VPN por aplicación que desee incluir, haga clic en **Agregar** y realice lo siguiente:
    - **Dominio:** Escriba el dominio que desea agregar.
    - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardar el dominio.

- **XML personalizado:** Para cada parámetro XML personalizado que desee agregar, haga clic en **Agregar** y realice lo siguiente:
  - **Nombre del parámetro:** Escriba el nombre del parámetro que desea agregar.
  - **Valor:** Escriba el valor asociado con **Nombre del parámetro**.
  - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardar el dominio.

Configurar opciones de habilitación de VPN a petición

- **Dominio a petición:** Para cada dominio y acción asociada que se realizará cuando los usuarios se conecten a ellos que desee agregar, haga clic en **Agregar** y realice lo siguiente:
  - **Dominio:** Escriba el dominio que desea agregar.
  - **Acción:** En la lista, seleccione una de las acciones posibles:
    - **Establecer siempre:** El dominio siempre activa una conexión VPN.
    - **Nunca establecer:** El dominio nunca activa una conexión VPN.
    - **Establecer si es necesario:** El dominio activa un intento de conexión VPN si la resolución del nombre de dominio falla. El fallo ocurre cuando el servidor DNS no puede resolver el dominio, redirige a un servidor diferente o agota el tiempo de espera.
  - Haga clic en **Guardar** para guardar el dominio o en **Cancelar** para no guardarlo.

- **Reglas a petición**
  - **Acción:** En la lista, seleccione la acción que se va a realizar. El valor predeterminado es **EvaluateConnection**. Las posibles acciones son:
    - **Permitir:** Permitir que la VPN a petición se conecte cuando se active.
    - **Conectar:** Iniciar incondicionalmente una conexión VPN.
    - **desconectar:** Eliminar la conexión VPN y no volver a conectar a petición mientras la regla coincida.
    - **EvaluateConnection:** Evaluar la matriz **ActionParameters** para cada conexión.
    - **Ignorar:** Mantener cualquier conexión VPN existente activa, pero no volver a conectar a petición mientras la regla coincida.
  - **DNSDomainMatch:** Para los dominios con los que puede coincidir la lista de dominios de búsqueda de un dispositivo, haga clic en **Agregar** y haga lo siguiente:
    - **Dominio DNS:** Escriba el nombre de dominio. Puede usar el prefijo comodín "*" para hacer coincidir varios dominios. Por ejemplo, *.example.com coincide con mydomain.example.com, yourdomain.example.com y herdomain.example.com.
    - Haga clic en **Guardar** para guardar el dominio o en **Cancelar** para no guardarlo.
  - **DNSServerAddressMatch:** Para cada dirección IP con la que pueda coincidir cualquiera de los servidores DNS especificados de la red que desee agregar, haga clic en **Agregar** y haga lo siguiente:
    - **Dirección del servidor DNS:** Escriba la dirección del servidor DNS que desea agregar. Puede usar el sufijo comodín "*" para hacer coincidir servidores DNS. Por ejemplo, 17.* coincide con cualquier servidor DNS de la subred de clase A.
    - Haga clic en **Guardar** para guardar la dirección del servidor DNS o en **Cancelar** para no guardar la dirección del servidor DNS.
  - **InterfaceTypeMatch:** En la lista, haga clic en el tipo de hardware de interfaz de red principal en uso. El valor predeterminado es **No especificado**. Los valores posibles son:
    - **Unspecified:** Coincide con cualquier hardware de interfaz de red. Esta opción es la predeterminada.
    - **Ethernet:** Coincide solo con hardware de interfaz de red Ethernet.
    - **WiFi:** Coincide solo con hardware de interfaz de red Wi-Fi.
    - **Cellular:** Coincide solo con hardware de interfaz de red celular.

- **SSIDMatch:** Para cada SSID que desee agregar para que coincida con la red actual, haga clic en **Agregar** y haga lo siguiente.
  - **SSID:** Escriba el SSID que desea agregar. Si la red no es una red Wi-Fi, o si el SSID no aparece, la coincidencia falla. Deje esta lista vacía para que coincida con cualquier SSID.
  - Haga clic en **Guardar** para guardar el SSID o haga clic en **Cancelar** para no guardar el SSID.
- **URLStringProbe:** Escriba una URL para obtener. Si esta URL se obtiene correctamente sin redirección, esta regla coincide.
- **ActionParameters : Domains:** Para cada dominio que EvaluateConnection comprueba y que desea agregar, haga clic en **Agregar** y haga lo siguiente:
  - **Dominio:** Escriba el dominio que desea agregar.
  - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardar el dominio.
- **ActionParameters : DomainAction:** En la lista, seleccione el **comportamiento de VPN** para los dominios **ActionParameters : Domains** especificados. El valor predeterminado es **ConnectIfNeeded**. Las acciones posibles son:
  - **ConnectIfNeeded:** El dominio activa un intento de conexión VPN si la resolución del nombre de dominio falla. El fallo ocurre cuando el servidor DNS no puede resolver el dominio, redirige a un servidor diferente o agota el tiempo de espera.
  - **NeverConnect:** El dominio nunca activa una conexión VPN.
- **Parámetros de acción: RequiredDNSServers:** Para cada servidor DNS que se utilizará para resolver los dominios especificados, haga clic en **Agregar** y haga lo siguiente:
  - **Servidor DNS:** Válido solo cuando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**. Escriba la dirección IP del servidor DNS que desea agregar. Este servidor puede estar fuera de la configuración de red actual del dispositivo. Si el servidor DNS no es accesible, se establece una conexión VPN en respuesta. Este servidor DNS debe ser un servidor DNS interno o un servidor DNS externo de confianza.
  - Haga clic en **Guardar** para guardar el servidor DNS o haga clic en **Cancelar** para no guardarlo.

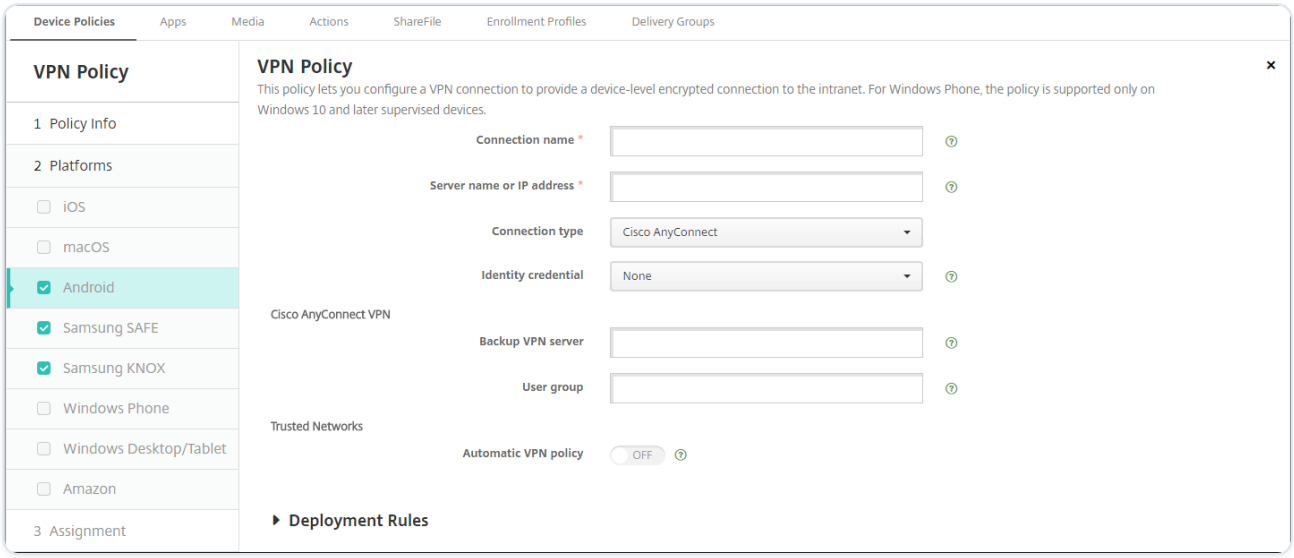
    - **ActionParameters : RequiredURLStringProbe:** Opcionalmente, escriba una URL HTTP o HTTPS (preferida) para sondear, utilizando una solicitud GET. Si el nombre de host de la URL no se puede resolver, el servidor no es accesible o el servidor no responde, se establece una conexión VPN. Válido solo cuando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.
    - **OnDemandRules : Contenido XML:** Escriba o copie y pegue las reglas XML de configuración a petición.
        - Haga clic en **Comprobar diccionario** para validar el código XML. **XML válido** aparece debajo del cuadro de texto **Contenido XML** si el XML es válido. Si no es válido, un mensaje de error describe el error.

- **Proxy**
    - **Configuración del proxy:** En la lista, seleccione cómo la conexión VPN se enruta a través de un servidor proxy. El valor predeterminado es **Ninguno**.
        - Si habilita **Manual**, configure estos ajustes:
            - **Nombre de host o dirección IP del servidor proxy:** Escriba el nombre de host o la dirección IP del servidor proxy. Este campo es obligatorio.
            - **Puerto del servidor proxy:** Escriba el número de puerto del servidor proxy. Este campo es obligatorio.
            - **Nombre de usuario:** Escriba un nombre de usuario opcional para el servidor proxy.
            - **Contraseña:** Escriba una contraseña opcional para el servidor proxy.
        - Si configura **Automático**, configure este ajuste:
            - **URL del servidor proxy:** Escriba la URL del servidor proxy. Este campo es obligatorio.

- **Configuración de la política**
    - **Eliminar política:** Elija un método para programar la eliminación de la política. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
        - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
        - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la política.

- **Permitir al usuario eliminar la política:** Puede seleccionar cuándo los usuarios pueden eliminar la política de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**.
- **Ámbito del perfil:** Seleccione si esta política se aplica a un **Usuario** o a un **Sistema** completo. El valor predeterminado es **Usuario**. Esta opción solo está disponible en macOS 10.7 y versiones posteriores.

Configuración de Android (DA heredado)



Configurar el protocolo VPN Cisco AnyConnect para Android

- **Nombre de la conexión:** Escriba un nombre para la conexión VPN de Cisco AnyConnect. Este campo es obligatorio.
- **Nombre del servidor o dirección IP:** Escriba el nombre o la dirección IP del servidor VPN. Este campo es obligatorio.
- **Credencial de identidad:** En la lista, seleccione una credencial de identidad.
- **Servidor VPN de respaldo:** Escriba la información del servidor VPN de respaldo.
- **Grupo de usuarios:** Escriba la información del grupo de usuarios.
- **Redes de confianza**
  - **Política VPN automática:** Habilite o deshabilite esta opción para configurar cómo reacciona la VPN a las redes de confianza y no de confianza. Si está habilitada, configure estos ajustes:

- **Política de red de confianza:** En la lista, seleccione la política deseada. El valor predeterminado es **desconectar**. Las opciones posibles son:
  - **desconectar:** El cliente finaliza la conexión VPN en la red de confianza. Esta configuración es la predeterminada.
  - **Conectar:** El cliente inicia una conexión VPN en la red de confianza.
  - **No hacer nada:** El cliente no realiza ninguna acción.
  - **Pausar:** Cuando un usuario establece una sesión VPN fuera de la red de confianza y luego entra en una red configurada como de confianza, la sesión VPN se suspende. Cuando el usuario vuelve a salir de la red de confianza, la sesión se reanuda. Esta configuración elimina la necesidad de establecer una nueva sesión VPN después de salir de una red de confianza.
- **Política de red no de confianza:** En la lista, seleccione la política deseada. El valor predeterminado es **Conectar**. Las opciones posibles son:
  - **Conectar:** El cliente inicia una conexión VPN en la red no de confianza.
  - **No hacer nada:** El cliente inicia una conexión VPN en la red no de confianza. Esta opción deshabilita la VPN siempre activa.

- **Dominios de confianza:** Para cada sufijo de dominio que tenga la interfaz de red cuando el cliente esté en la red de confianza, haga clic en **Agregar** para hacer lo siguiente:
  - **Dominio:** Escriba el dominio que se va a agregar.
  - Haga clic en **Guardar** para guardar el dominio o haga clic en **Cancelar** para no guardar el dominio.
- **Servidores de confianza:** Para cada dirección de servidor que tenga una interfaz de red cuando el cliente esté en la red de confianza, haga clic en **Agregar** y haga lo siguiente:
  - **Servidores:** Escriba el servidor que se va a agregar.
  - Haga clic en **Guardar** para guardar el servidor o haga clic en **Cancelar** para no guardar el servidor.

Configurar el protocolo Citrix SSO para Android

- **Nombre de la conexión:** Escriba un nombre para la conexión VPN. Este campo es obligatorio.
- **Nombre del servidor o dirección IP:** Escriba el FQDN o la dirección IP de NetScaler Gateway.

- **Tipo de autenticación para la conexión:** Elija un tipo de autenticación y complete cualquiera de los campos que aparezcan para ese tipo:
  - **Nombre de usuario** y **Contraseña:** Escriba sus credenciales VPN para los **tipos de autenticación** de **Contraseña** o **Contraseña y certificado**. Opcional. Si no proporciona las credenciales VPN, la aplicación Citrix VPN le pedirá un nombre de usuario y una contraseña.
  - **Credencial de identidad:** Aparece para los **tipos de autenticación** de **Certificado** o **Contraseña y certificado**. En la lista, seleccione una credencial de identidad.
- **Habilitar VPN por aplicación:** Seleccione si desea habilitar la VPN por aplicación. Si no habilita una VPN por aplicación, todo el tráfico pasa por el túnel VPN de Citrix. Si habilita una VPN por aplicación, especifique la siguiente configuración. El valor predeterminado es **Desactivado**.
  - **Lista de permitidos** o **Lista de bloqueados:** Si es **Lista de permitidos**, todas las aplicaciones de la lista de permitidos se conectan a través de esta VPN. Si es **Lista de bloqueados**, todas las aplicaciones, excepto las de la lista de bloqueados, se conectan a través de esta VPN.
  - **Lista de aplicaciones:** Las aplicaciones de una lista de permitidos o de una lista de bloqueados. Haga clic en **Agregar** y, a continuación, escriba una lista de nombres de paquetes de aplicaciones separados por comas.
- **XML personalizado:** Haga clic en **Agregar** y, a continuación, escriba los parámetros personalizados. Citrix Endpoint Management admite estos parámetros para Citrix VPN:
  - **DisableUserProfiles:** Opcional. Para habilitar este parámetro, escriba **Sí** para el **Valor**. Si está habilitado, Citrix Endpoint Management no muestra las conexiones VPN agregadas por el usuario y este no puede agregar una conexión. Esta configuración es una restricción global y se aplica a todos los perfiles VPN.
  - **userAgent:** Un valor de cadena. Puede especificar una cadena de agente de usuario personalizada para enviar en cada solicitud HTTP. La cadena de agente de usuario especificada se añade al agente de usuario VPN de Citrix existente.
  - **IsAlwaysOnVpn:** Opcional. Esta propiedad determina si el perfil VPN es un perfil VPN Always On o no. Establezca en **Sí** para indicar que el perfil VPN es un perfil VPN Always On; el valor predeterminado es **No**. Solo un perfil VPN puede tener esta propiedad establecida en **Sí** para que Always On VPN funcione de forma fiable.

Configurar VPN para admitir NAC

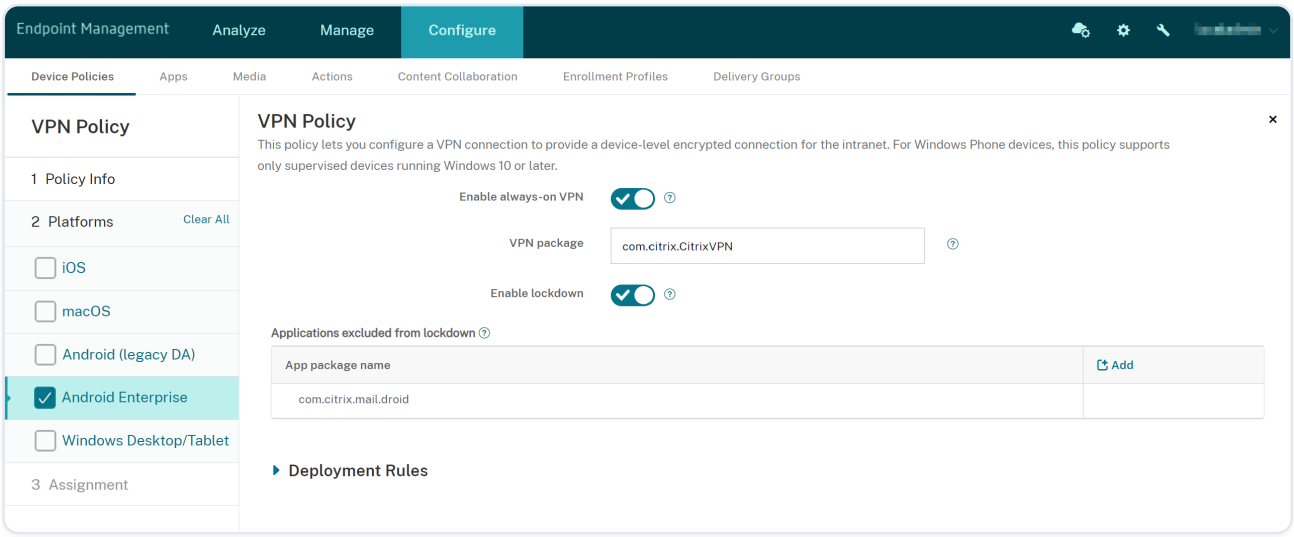
1. Utilice el **Tipo de conexión** de **SSL personalizado** para configurar el filtro NAC.
2. Especifique un **Nombre de conexión** de **VPN**.
3. Para **XML personalizado**, haga clic en **Agregar** y haga lo siguiente:

    - **Nombre del parámetro:** Escriba **XenMobileDeviceId**. Este campo es el ID de dispositivo que se utilizará para la comprobación NAC basada en la inscripción del dispositivo en Citrix Endpoint Management. Si Citrix Endpoint Management inscribe y administra el dispositivo, se permite la conexión VPN. De lo contrario, la autenticación se deniega en el momento del establecimiento de la VPN.
    - **Valor:** Escriba **DeviceID_${device.id}**, que es el valor del parámetro **XenMobileDeviceId**.
    - Haga clic en **Guardar** para guardar el parámetro.

Configurar VPN para Android Enterprise

Para configurar VPN para dispositivos Android Enterprise, cree una directiva de dispositivo de configuración administrada de Android Enterprise para la aplicación Citrix SSO. Consulte Configurar perfiles VPN para Android Enterprise.

Configuración de Android Enterprise

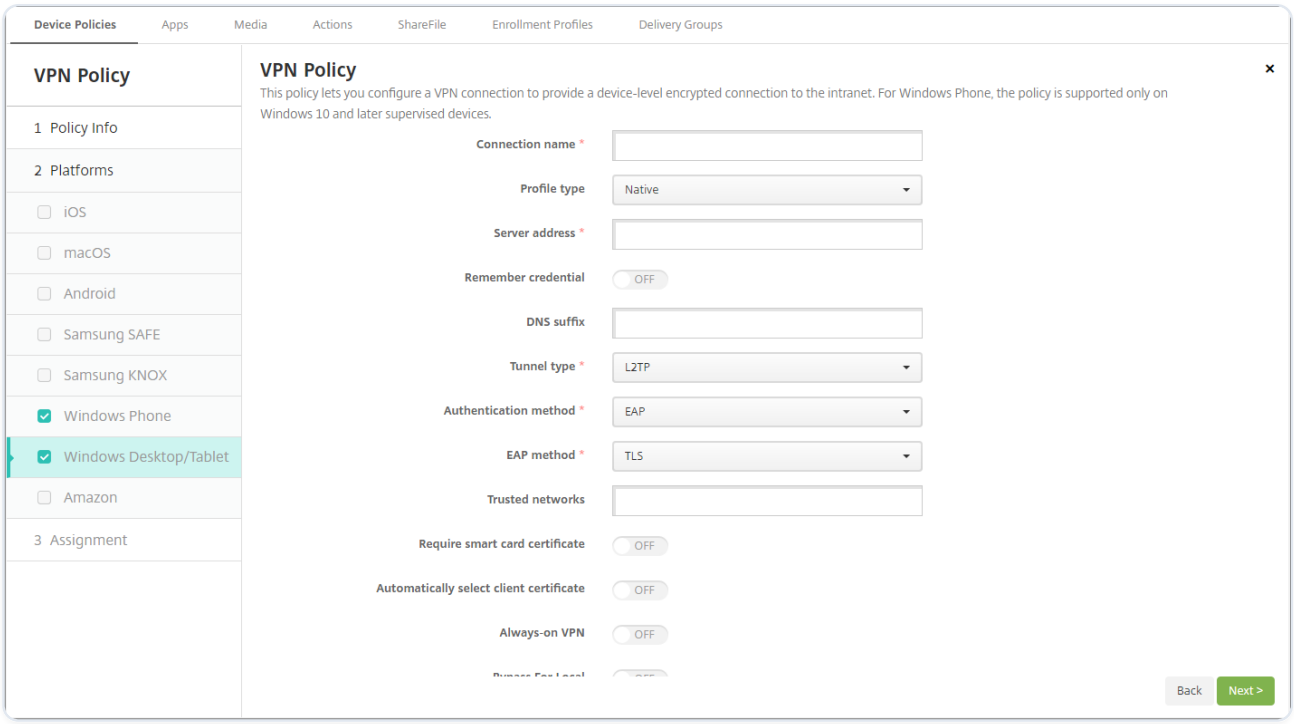


- **Habilitar VPN siempre activa:** Seleccione si la VPN está siempre activa. El valor predeterminado es **Desactivado**. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario la desconecta manualmente.
- **Paquete VPN** Escriba el nombre del paquete de la aplicación VPN que utilizan los dispositivos.
- **Habilitar bloqueo:** Si está deshabilitado, ninguna aplicación puede acceder a la red si no existe una conexión VPN. Si está habilitado, las aplicaciones que configure en la siguiente

configuración pueden acceder a la red, incluso si no existe una conexión VPN. Disponible para dispositivos Android 10 y posteriores.

- **Aplicaciones excluidas del bloqueo:** Haga clic en **Agregar** para escribir los nombres de los paquetes de las aplicaciones que desea que omitan la configuración de bloqueo.

Configuración de Windows Desktop/Tablet



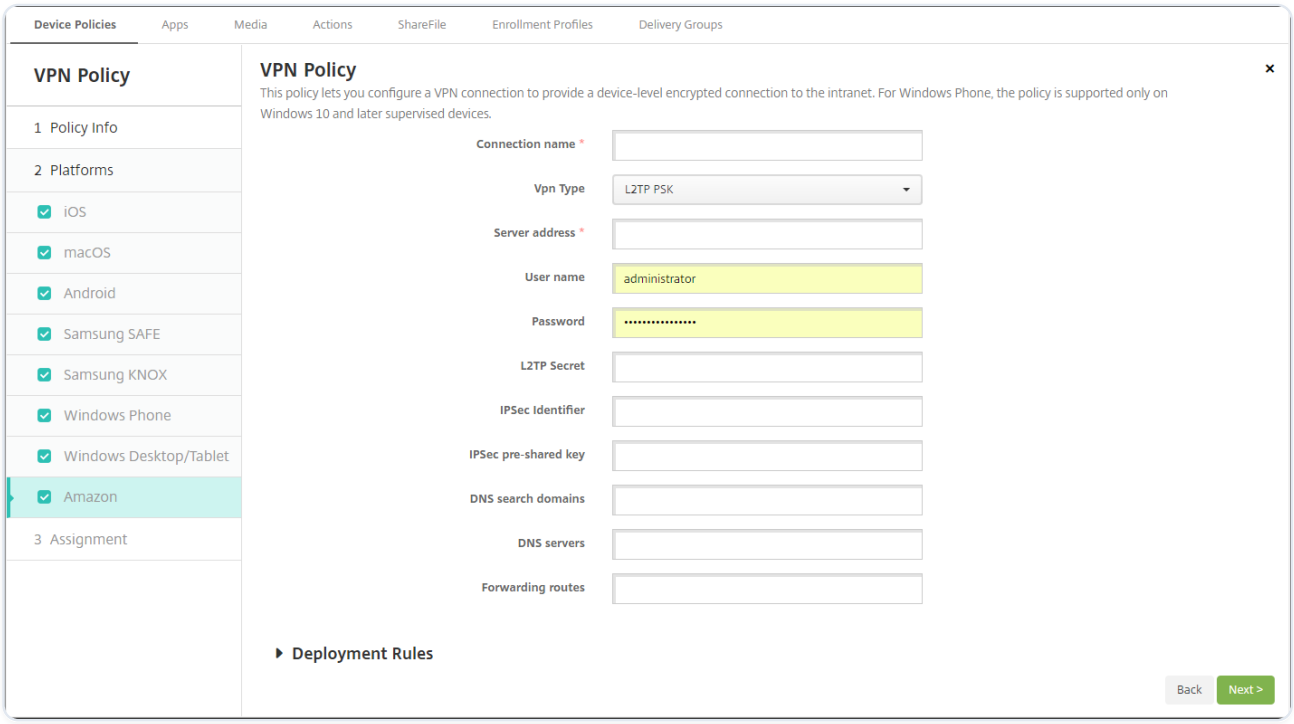
- **Nombre de la conexión:** Introduzca un nombre para la conexión. Este campo es obligatorio.
- **Tipo de perfil:** En la lista, seleccione **Nativo** o **Plugin**. El valor predeterminado es **Nativo**.
- **Configurar tipo de perfil nativo:** Estos parámetros se aplican a la VPN integrada en los dispositivos Windows de los usuarios.
    - **Dirección del servidor:** Escriba el FQDN o la dirección IP del servidor VPN. Este campo es obligatorio.
    - **Recordar credenciales:** Seleccione si desea almacenar en caché las credenciales. El valor predeterminado es **Desactivado**. Cuando está habilitado, las credenciales se almacenan en caché siempre que sea posible.
    - **Sufijo DNS:** Escriba el sufijo DNS.
    - **Tipo de túnel:** En la lista, seleccione el tipo de túnel VPN que desea utilizar. El valor predeterminado es **L2TP**. Las opciones posibles son:
        - **L2TP:** Protocolo de tunelización de capa 2 con autenticación de clave precompartida.
        - **PPTP:** Tunelización punto a punto.

    - **IKEv2:** Intercambio de claves de Internet versión 2.
  - **Método de autenticación:** En la lista, seleccione el método de autenticación que desea utilizar. El valor predeterminado es **EAP**. Las opciones posibles son:
    - **EAP:** Protocolo de autenticación extensible.
    - **MSChapV2:** Utilice el Protocolo de autenticación de desafío-respuesta de Microsoft para la autenticación mutua. Esta opción no está disponible si selecciona **IKEv2** como tipo de túnel.
  - **Método EAP:** En la lista, seleccione el método EAP que se va a utilizar. El valor predeterminado es **TLS**. Este campo no está disponible cuando la autenticación MSChapV2 está habilitada. Las opciones posibles son:
    - **TLS:** Seguridad de la capa de transporte
    - **PEAP:** Protocolo de autenticación extensible protegido
  - **Redes de confianza:** Escriba una lista de redes separadas por comas que no requieran una conexión VPN para el acceso. Por ejemplo, cuando los usuarios están en la red inalámbrica de su empresa, pueden acceder directamente a los recursos protegidos.
  - **Requerir certificado de tarjeta inteligente:** Seleccione si se requiere un certificado de tarjeta inteligente. El valor predeterminado es **Desactivado**.
  - **Seleccionar automáticamente el certificado de cliente:** Seleccione si se debe elegir automáticamente el certificado de cliente que se utilizará para la autenticación. El valor predeterminado es **Desactivado**. Esta opción no está disponible cuando se habilita **Requerir certificado de tarjeta inteligente**.
  - **VPN siempre activa:** Seleccione si la VPN está siempre activa. El valor predeterminado es **Desactivado**. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario la desconecta manualmente.
  - **Omitir para local:** Escriba la dirección y el número de puerto para permitir que los recursos locales omitan el servidor proxy.

- **Configurar tipo de perfil de complemento:** Estos ajustes se aplican a los complementos VPN obtenidos de la Tienda Windows e instalados en los dispositivos de los usuarios.
  - **Dirección del servidor:** Escriba el FQDN o la dirección IP del servidor VPN. Este campo es obligatorio.

- **Recordar credencial:** Seleccione si se debe almacenar en caché la credencial. El valor predeterminado es **Desactivado**. Cuando está habilitado, las credenciales se almacenan en caché siempre que sea posible.
- **Sufijo DNS:** Escriba el sufijo DNS.
- **ID de aplicación cliente:** Escriba el nombre de la familia de paquetes para el complemento VPN.
- **XML de perfil de complemento:** Seleccione el perfil de complemento VPN personalizado que se utilizará haciendo clic en **Examinar** y navegando a la ubicación del archivo. Póngase en contacto con el proveedor del complemento para obtener el formato y los detalles.
- **Redes de confianza:** Escriba una lista de redes separadas por comas que no requieran una conexión VPN para el acceso. Por ejemplo, cuando los usuarios están en la red inalámbrica de su empresa, pueden acceder directamente a los recursos protegidos.
- **VPN siempre activa:** Seleccione si la VPN está siempre activa. El valor predeterminado es **Desactivado**. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario la desconecta manualmente.
- **Omitir para local:** Escriba la dirección y el número de puerto para permitir que los recursos locales omitan el servidor proxy.

Configuración de Amazon



- **Nombre de la conexión:** Escriba un nombre para la conexión.

- **Tipo de VPN:** Seleccione el tipo de conexión. Las opciones posibles son:
  - **L2TP PSK:** Protocolo de tunelización de capa 2 con autenticación de clave precompartida. Esta configuración es la predeterminada.
  - **L2TP RSA:** Protocolo de tunelización de capa 2 con autenticación RSA.
  - **IPSEC XAUTH PSK:** Seguridad de protocolo de Internet con clave precompartida y autenticación extendida.
  - **IPSEC HYBRID RSA:** Seguridad de protocolo de Internet con autenticación RSA híbrida.
  - **PPTP:** Tunelización punto a punto.

Las siguientes secciones enumeran las opciones de configuración para cada uno de los tipos de conexión anteriores.

Configurar los ajustes de L2TP PSK para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Escriba una contraseña opcional.
- **Secreto L2TP:** Escriba la clave secreta compartida.
- **Identificador IPSec:** Escriba el nombre de la conexión VPN que los usuarios ven en sus dispositivos al conectarse.
- **Clave precompartida IPSec:** Escriba la clave secreta.
- **Dominios de búsqueda DNS:** Escriba los dominios con los que puede coincidir la lista de dominios de búsqueda de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se utilizarán para resolver los dominios especificados.
- **Rutas de reenvío:** Si su servidor VPN corporativo admite rutas de reenvío, para cada ruta de reenvío que desee usar, haga clic en **Agregar** y haga lo siguiente:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta o en **Cancelar** para no guardarla.

Configurar los ajustes L2TP RSA para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Escriba una contraseña opcional.

- **Secreto L2TP:** Escriba la clave secreta compartida.
- **Dominios de búsqueda DNS:** Escriba los dominios con los que puede coincidir la lista de dominios de búsqueda de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se utilizarán para resolver los dominios especificados.
- **Certificado de servidor:** En la lista, seleccione el certificado de servidor que se va a utilizar.
- **Certificado de CA:** En la lista, seleccione el certificado de CA que se va a utilizar.
- **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a utilizar.
- **Rutas de reenvío:** Si su servidor VPN corporativo admite rutas de reenvío, para cada ruta de reenvío que desee utilizar, haga clic en **Agregar** y realice lo siguiente:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta o haga clic en **Cancelar** para no guardar la ruta.

Configurar los parámetros de IPSEC XAUTH PSK para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Escriba una contraseña opcional.
- **Identificador de IPSec:** Escriba el nombre de la conexión VPN que los usuarios ven en sus dispositivos al conectarse.
- **Clave precompartida de IPSec:** Escriba la clave secreta compartida.
- **Dominios de búsqueda de DNS:** Escriba los dominios con los que puede coincidir la lista de dominios de búsqueda de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se utilizarán para resolver los dominios especificados.
- **Rutas de reenvío:** Si su servidor VPN corporativo admite rutas de reenvío, para cada ruta de reenvío que desee utilizar, haga clic en **Agregar** y realice lo siguiente:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta o haga clic en **Cancelar** para no guardar la ruta.

Configurar los ajustes de IPSEC AUTH RSA para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.

- **Contraseña:** Escriba una contraseña opcional.
- **Dominios de búsqueda DNS:** Escriba los dominios con los que puede coincidir la lista de dominios de búsqueda de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se utilizarán para resolver los dominios especificados.
- **Certificado de servidor:** En la lista, seleccione el certificado de servidor que se va a utilizar.
- **Certificado de CA:** En la lista, seleccione el certificado de CA que se va a utilizar.
- **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a utilizar.
- **Rutas de reenvío:** Si su servidor VPN corporativo admite rutas de reenvío, para cada ruta de reenvío que desee utilizar, haga clic en **Agregar** y realice lo siguiente:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta o haga clic en **Cancelar** para no guardar la ruta.

Configurar los ajustes de IPSEC HYBRID RSA para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Escriba una contraseña opcional.
- **Dominios de búsqueda DNS:** Escriba los dominios con los que puede coincidir la lista de dominios de búsqueda de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se utilizarán para resolver los dominios especificados.
- **Certificado de servidor:** En la lista, seleccione el certificado de servidor que se va a utilizar.
- **Certificado de CA:** En la lista, seleccione el certificado de CA que se va a utilizar.
- **Rutas de reenvío:** Si su servidor VPN corporativo admite rutas de reenvío, para cada ruta de reenvío que desee usar, haga clic en **Agregar** y haga lo siguiente:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta o haga clic en **Cancelar** para no guardarla.

Configurar la configuración de PPTP para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Escriba una contraseña opcional.

- **Dominios de búsqueda DNS:** Escriba los dominios con los que puede coincidir la lista de dominios de búsqueda de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se utilizarán para resolver los dominios especificados.
- **Cifrado PPP (MPPE):** Seleccione si desea habilitar el cifrado de datos con Microsoft Point-to-Point Encryption (MPPE). El valor predeterminado es **Desactivado**.
- **Rutas de reenvío:** Si su servidor VPN corporativo admite rutas de reenvío, para cada ruta de reenvío que desee utilizar, haga clic en **Agregar** y haga lo siguiente:
  - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
  - Haga clic en **Guardar** para guardar la ruta o haga clic en **Cancelar** para no guardar la ruta.

Directiva de dispositivo de fondo de pantalla

La directiva de dispositivo de fondo de pantalla le permite agregar un archivo .png o .jpg para establecer el fondo de pantalla en la pantalla de bloqueo, la pantalla de inicio o ambas de un dispositivo iOS. Esta directiva solo está disponible para dispositivos supervisados. Para usar diferentes fondos de pantalla en iPads y iPhones, debe crear diferentes directivas de fondo de pantalla e implementarlas en los usuarios adecuados.

La siguiente tabla enumera las dimensiones de imagen recomendadas por Apple para dispositivos iOS.

iPhone

DISPOSITIVO	DIMENSIONES DE IMAGEN EN PÍXELES
iPhone 12 Pro Max	2778 x 1284
iPhone 12 y iPhone 12 Pro	2532 x 1170
iPhone 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
iPhone XS Max	2688 x 1242

DISPOSITIVO	DIMENSIONES DE IMAGEN EN PÍXELES
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE 2.ª generación	1334 x 750
iPhone 7 Plus, 8 Plus	2208 x 1242
iPhone 7, 8	1334 x 750
iPhone 8 Plus	1334 x 750
iPhone 8	1334 x 750

iPad

DISPOSITIVO	DIMENSIONES DE LA IMAGEN EN PÍXELES
iPad Pro (1.ª, 2.ª y 3.ª generación de 12,9")	2732 x 2048
iPad Pro de 10,5 pulgadas	2224 x 1668
iPad Pro (9,7 pulgadas)	1536 x 2048
iPad Air 2	2048 x 1536

Para añadir o configurar esta política, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

- **Aplicar a:** En la lista, seleccione **Pantalla de bloqueo**, **Pantalla de inicio (lista de iconos)** o **Pantallas de bloqueo e inicio** para establecer dónde debe aparecer el fondo de pantalla.
- **Archivo de fondo de pantalla:** Para seleccionar el archivo de fondo de pantalla, haga clic en **Examinar** y, a continuación, vaya a la ubicación del archivo.

Política de dispositivo de filtro de contenido web

Puede filtrar el contenido web en dispositivos iOS mediante la función de filtro automático de Apple con sitios específicos que agregue a las listas de permitidos o bloqueados. La política de dispositivo de filtro de contenido web solo está disponible en dispositivos iOS en modo supervisado. Para obtener información sobre cómo poner un dispositivo iOS en modo supervisado, consulte Implementar dispositivos con Apple Configurator 2.

Nota:

- Los dispositivos Android no admiten el filtrado de contenido web.
- A partir de iOS versión 16.5 y posteriores, la política de dispositivo de filtro de contenido web deja de reconocer `https://localhost` en la lista de permitidos. Esto hace que algunas aplicaciones dejen de responder. Además, agregar un derivado de la URL, como `http://localhost:` , `http://localhost:*` , etc., a la lista de permitidos no resuelve el problema.

Para agregar o configurar esta política, vaya a **Configurar** > **Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

- **Tipo de filtro:** Haga clic en **Integrado** o **Plug-in** en la lista desplegable y, a continuación, siga los procedimientos que se indican para la opción que elija. El valor predeterminado es **Integrado**.

Tipo de filtro integrado

- **Filtro de contenido web**
  - **Filtro automático habilitado:** Si se debe usar la función de filtro automático de Apple para analizar sitios web en busca de contenido inapropiado. El valor predeterminado es **Desactivado**.
  - **URL permitidas:** Esta lista se ignora cuando **Filtro automático habilitado** está establecido en **Desactivado**. Cuando **Filtro automático habilitado** está establecido en **Activado**, los elementos de esta lista siempre son accesibles, independientemente de si el

filtro automático permite el acceso o no. Para cada URL que quiera agregar a la lista de permitidos, haga clic en **Agregar** y haga lo siguiente:

- Escriba la URL del sitio web permitido. Debe agregar `https://` o `https://` antes de la dirección web.
- Haga clic en **Guardar** para guardar el sitio web en la lista de permitidos o haga clic en **Cancelar** para no guardarlo.

- **URL bloqueadas:** Los elementos de esta lista siempre están bloqueados. Para cada URL que quiera agregar a la lista de bloqueados, haga clic en **Agregar** y haga lo siguiente:
  - Introduzca la URL del sitio web que desea bloquear. Debe añadir `https://` o `https://` antes de la dirección web.
  - Haga clic en **Guardar** para guardar el sitio web en la lista de bloqueo o haga clic en **Cancelar** para no guardarlo.

- **Lista de permitidos de marcadores**
  - **Lista de permitidos de marcadores:** Especifica los sitios a los que los usuarios pueden acceder. Para habilitar el acceso a los sitios web, añada su URL.
    - **URL:** La URL de cada sitio web al que los usuarios pueden acceder. Por ejemplo, para habilitar el acceso a la tienda de Citrix Secure Hub, añada la URL del servidor de Citrix Endpoint Management a la lista de **URL**. Debe añadir `https://` o `https://` antes de la dirección web. Este campo es obligatorio.
    - **Carpeta de marcadores:** Introduzca un nombre opcional para la carpeta de marcadores. Si este campo se deja en blanco, el marcador se añade al directorio de marcadores predeterminado.
    - **Título:** Introduzca un título descriptivo para el sitio web. Por ejemplo, escriba "Google" para la URL `https://google.com`.
    - Haga clic en **Guardar** para guardar el sitio web en la lista de permitidos o haga clic en **Cancelar** para no guardarlo.

Tipo de filtro de plug-in

- **Nombre del filtro:** Introduzca un nombre único para el filtro.
- **Identificador:** Introduzca el ID de paquete del plug-in que proporciona el servicio de filtrado.
- **Dirección del servicio:** Introduzca una dirección de servidor opcional. Los formatos válidos son dirección IP, nombre de host o URL.

- **Nombre de usuario:** Introduzca un nombre de usuario opcional para el servicio.
- **Contraseña:** Introduzca una contraseña opcional para el servicio.
- **Certificado:** Haga clic en un certificado de identidad opcional en la lista desplegable que se debe usar para autenticar al usuario en el servicio. El valor predeterminado es **Ninguno**.
- **Filtrar tráfico de WebKit:** Seleccione si desea filtrar el tráfico de WebKit.
- **Filtrar tráfico de socket:** Seleccione si desea filtrar el tráfico de socket.
- **Datos personalizados:** Para cada clave personalizada que quiera añadir al filtro web, haga clic en **Agregar** y, a continuación, haga lo siguiente:
  - **Clave:** Escriba la clave personalizada.
  - **Valor:** Escriba un valor para la clave personalizada.
  - Haga clic en **Guardar** para guardar la clave personalizada o haga clic en **Cancelar** para no guardarla.
- **Configuración de la directiva**
  - **Eliminar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva. Solo disponible para iOS 6.0 y versiones posteriores.

Directiva de dispositivo de clip web

Puede colocar accesos directos, o clips web, a sitios web para que aparezcan junto a las aplicaciones en los dispositivos de los usuarios. Puede especificar sus propios iconos para representar los clips web en dispositivos iOS, iPadOS, macOS y Android. Las tabletas Windows solo requieren una etiqueta y una URL. Para dispositivos iOS y iPadOS, configure la directiva de dispositivo de diseño de la pantalla de inicio para organizar los clips web que cree. Si restringe el acceso a las aplicaciones en iOS, asegúrese de configurar la directiva de dispositivo de restricción para permitir los clips web. Para obtener información sobre cómo configurar estas directivas, consulte Directiva de dispositivo de diseño de la pantalla de inicio y Directiva de dispositivo de restricciones.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de iOS

- **Etiqueta:** Escriba la etiqueta que aparecerá con el clip web.
- **URL:** Escriba la URL asociada al clip web. La URL debe comenzar con un protocolo, por ejemplo, `https://server`.
- **Extraíble:** Seleccione si los usuarios pueden quitar el clip web. El valor predeterminado es **Desactivado**. Esta opción no es compatible con iPads compartidos.
- **Icono que se va a actualizar:** Seleccione el icono que se utilizará para el clip web haciendo clic en **Examinar** y navegando a la ubicación del archivo.
- **Icono precompuesto:** Seleccione si el icono tiene efectos (esquinas redondeadas, sombra paralela y brillo reflectante) aplicados. El valor predeterminado es **Desactivado**, lo que añade los efectos.
- **Pantalla completa:** Seleccione si la página web vinculada se abre en modo de pantalla completa. Esta configuración también permite que un iPad abra solo un sitio web. Alternativamente, para configurar iPads para que se ejecuten en modo Quiosco, utilice la directiva de dispositivo de bloqueo de aplicaciones. Para obtener más información, consulte Configurar un iPad como quiosco. El valor predeterminado es **Desactivado**.
- **Configuración de directiva**
  - **Quitar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva. Solo disponible para iOS 6.0 y versiones posteriores.
  - **Ámbito del perfil:** Seleccione si la directiva se aplica a un usuario o a un sistema completo. El valor predeterminado es **Sistema**. Solo disponible para iOS 9.3 y versiones posteriores.

Configuración de macOS

- **Etiqueta:** Escriba la etiqueta que aparecerá con el clip web.

- **URL:** Escriba la URL asociada al clip web. La URL debe comenzar con un protocolo, por ejemplo, `https://server`.
- **Icono que se va a actualizar:** Seleccione el icono que se utilizará para el clip web haciendo clic en Examinar y navegando hasta la ubicación del archivo.
- **Configuración de la directiva**
  - **Quitar directiva:** Elija un método para programar la eliminación de la directiva. Las opciones disponibles son **Seleccionar fecha** y **Duración hasta la eliminación (en horas)**
    - **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de eliminación.
    - **Duración hasta la eliminación (en horas):** Escriba un número, en horas, hasta que se produzca la eliminación de la directiva.
  - **Permitir al usuario quitar la directiva:** Puede seleccionar cuándo los usuarios pueden quitar la directiva de su dispositivo. Seleccione **Siempre**, **Se requiere código de acceso** o **Nunca** en el menú. Si selecciona **Se requiere código de acceso**, escriba un código de acceso en el campo **Código de acceso de eliminación**.

Configuración de Android

- **Regla:** Seleccione si esta directiva agrega o quita un clip web. El valor predeterminado es **Agregar**.
- **Etiqueta:** Escriba la etiqueta que aparecerá con el clip web.
- **URL:** Escriba la URL asociada al clip web.
- **Definir un icono:** Seleccione si desea usar un archivo de icono. El valor predeterminado es **Desactivado**.
- **Archivo de icono:** Si **Definir un icono** está **Activado**, seleccione el archivo de icono que desea usar haciendo clic en **Examinar** y navegando hasta la ubicación del archivo.

Configuración de escritorio/tableta de Windows

- **Nombre:** Escriba la etiqueta que debe aparecer con el clip web.
- **URL:** Escriba la URL asociada al clip web.

Directiva de dispositivo de agente de Windows

Utilice la directiva de dispositivo de agente de Windows para ejecutar scripts de PowerShell en escritorios y tabletas Windows administrados. Puede apuntar a archivos de script cargados en Citrix Endpoint Management como una aplicación empresarial y a otros servidores que alojan scripts. Para obtener información sobre cómo agregar aplicaciones empresariales, consulte Agregar aplicaciones.

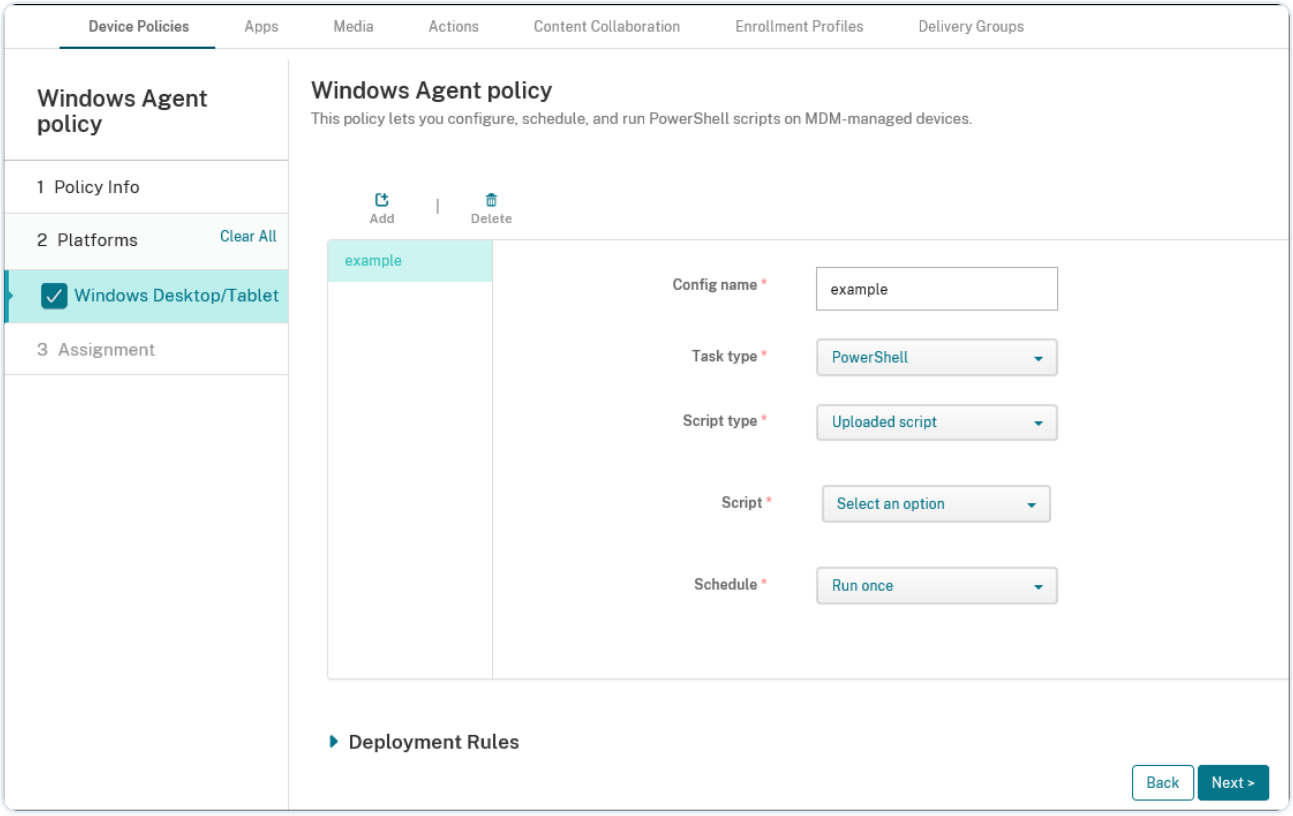
Todos los scripts se ejecutan con privilegios, no es necesario ejecutarlos como administrador.

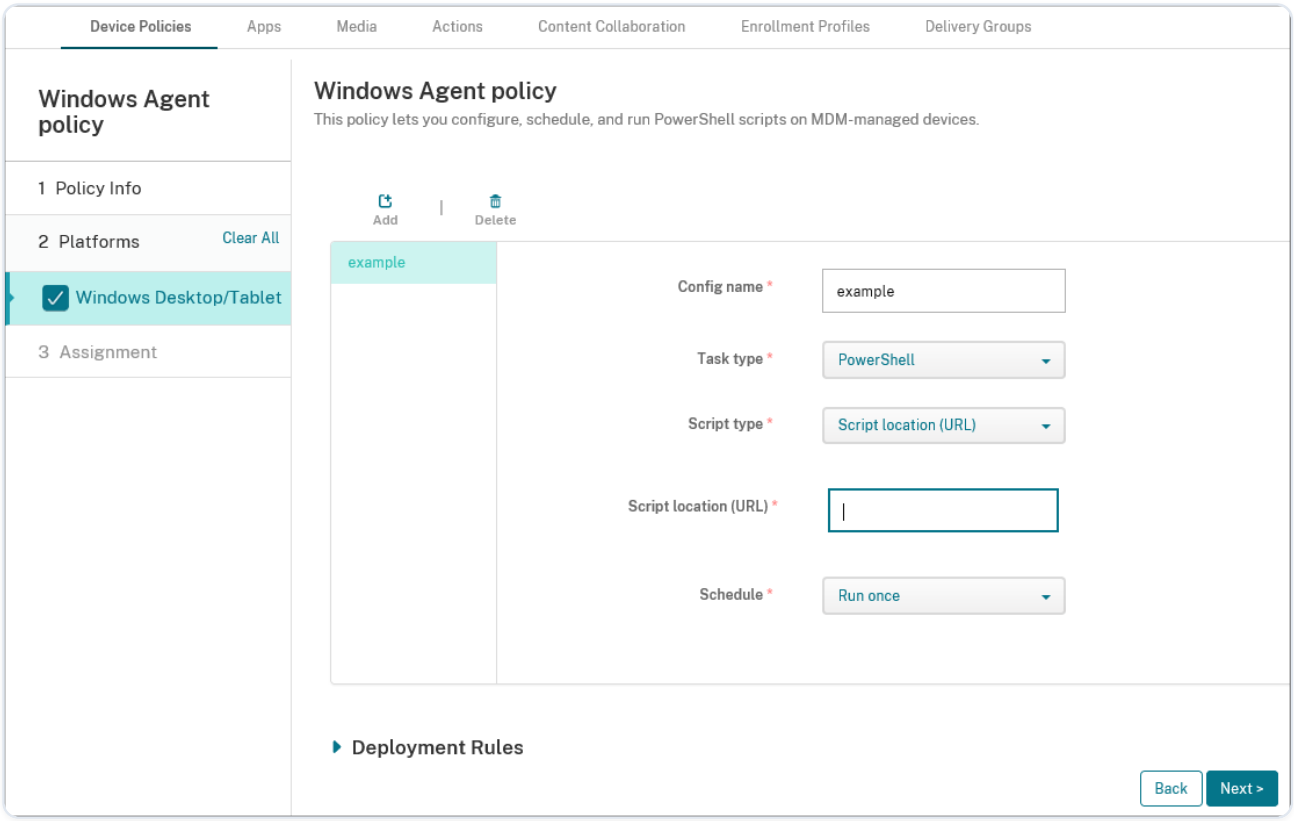
Después de implementar y ejecutar el script, puede configurar acciones automatizadas basadas en los resultados del script. Por ejemplo, ejecuta un script que supervisa una clave de registro y devuelve un resultado. Basándose en el resultado devuelto, se ejecuta una acción automatizada. La acción concede o deniega el acceso a una aplicación, marca el dispositivo como no conforme o tiene otros efectos.

También puede usar esta directiva para implementar instaladores MSI personalizados configurando un script de PowerShell que apunte a un archivo .msi y a un archivo .mst.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de escritorios y tabletas Windows





- **Nombre de configuración:** Escriba un nombre descriptivo para su configuración.
- **Tipo de tarea:** Seleccione **PowerShell**.
- **Tipo de script:** Seleccione **Script cargado** para scripts que haya cargado en Citrix Endpoint Management o seleccione **Ubicación del script (URL)** para scripts alojados externamente. Para obtener más información sobre cómo cargar un script en Citrix Endpoint Management, consulte Agregar aplicaciones `Win32` como aplicaciones empresariales.
  - **Seleccionar script:** Si eligió **Script cargado**, seleccione el script que desea ejecutar.
  - **Ubicación del script (URL):** Si eligió **Ubicación del script (URL)**, introduzca la ubicación del script que desea ejecutar. Esta URL debe entregar el script como una carga útil. Citrix Endpoint Management no admite URL que entreguen scripts como una descarga de JavaScript. El script también debe estar disponible públicamente.
- **Programación:** Seleccione **Ejecutar una vez** para ejecutar el script seleccionado una sola vez o seleccione **Ejecutar de forma recurrente** para ejecutar el script regularmente.
  - **Ejecutar cada (horas):** Escriba el número de horas entre ejecuciones de scripts.

Para comprobar el estado de un script, vaya a **Administrar > Dispositivos** en la consola. Seleccione el dispositivo en el que quiere comprobar el estado del script y haga clic en **Modificar**. En **Propiedades**, puede comprobar el estado de los scripts haciendo clic en **Descargar** en el encabezado **Windows Agent**.

Implementar un script de PowerShell para activar una acción automatizada

1. Cree un script de PowerShell para supervisar una clave de registro. El siguiente script de PowerShell comprueba si el firewall está habilitado.

```
$body = @{}

$firewallEnabled = Get-ItemPropertyValue HKLM:
\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPoli
cy\StandardProfile -Name EnableFirewall

if($firewallEnabled -eq 1){

$body["firewallEnabled"]="true"

} else {

$body["firewallEnabled"]="false"

}

$body | ConvertTo-Json -Depth 10
```

   Este script devuelve un valor de

```
{

    "firewallEnabled":  "true"

}
```

   o

```
{

    "firewallEnabled":  "false"

}
```

2. Cargue el script en la consola de Citrix Endpoint Management como una aplicación empresarial o aloje el script en una URL accesible.

3. Configure la directiva de dispositivo de Windows Agent descrita en este artículo. Asegúrese de que el script esté programado para ejecutarse inmediatamente.
4. Después de que se ejecute el script, determine el estado del script.
    a. Vaya a **Administrar > Dispositivos** en la consola.
    b. Seleccione el dispositivo para comprobar el estado de su script y, a continuación, haga clic en **Modificar**.
    c. Haga clic en **Descargar** en el encabezado **Windows Agent**.
5. Configure una acción automatizada según el estado recibido. Para obtener más información sobre cómo configurar acciones automatizadas, consulte Crear una acción automatizada basada en el resultado de una directiva de dispositivo de Windows Agent. Esa sección muestra las acciones automatizadas específicas creadas para el script de ejemplo y la directiva de dispositivo de Windows Agent.

Directiva de dispositivo de configuración de GPO de Windows

La directiva de dispositivo de configuración de GPO de Windows le permite:

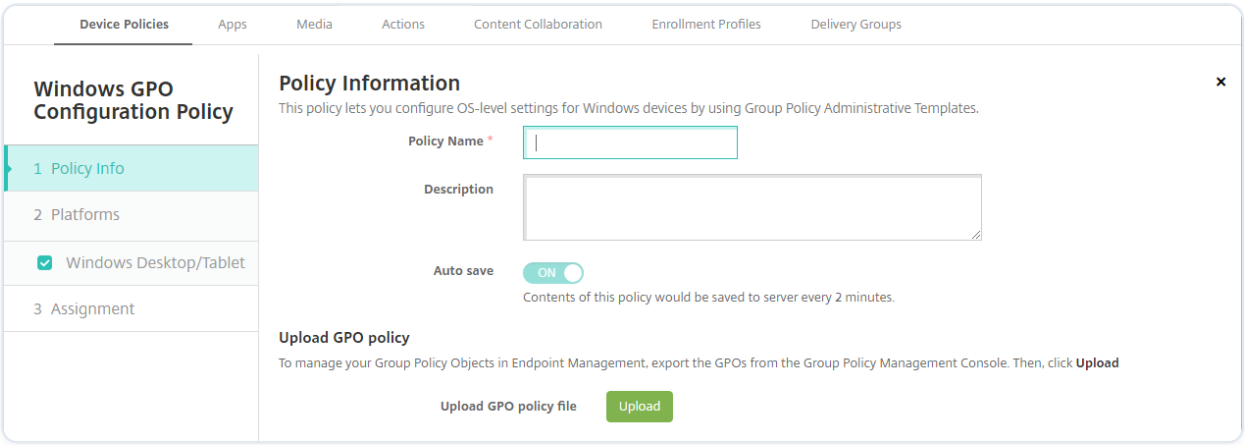
- Utilizar la consola de Citrix Endpoint Management para importar objetos de directiva de grupo (GPO) e implementarlos en dispositivos Windows 10 y Windows 11.
- Configurar GPO para cualquier dispositivo Windows compatible con Citrix Workspace Environment Management.
- Configurar GPO a nivel de dispositivo y de usuario.

Importar GPO para su implementación en dispositivos Windows 10 y Windows 11

En lugar de depender de un administrador de AD para que utilice la consola de administración de directivas de grupo para administrar los GPO, puede importar e implementar GPO a través de la consola de Citrix Endpoint Management.

Para crear una copia de seguridad de sus GPO en Citrix Endpoint Management:

1. Solicite a su administrador de AD que exporte los GPO desde la consola de administración de directivas de grupo y le proporcione los archivos.
2. En la consola de Citrix Endpoint Management, vaya a **Configurar > Directivas de dispositivo** y cree una directiva de **Configuración de GPO de Windows**.
3. Haga clic en **Cargar**, busque el archivo y, a continuación, haga clic en **Abrir** para importarlo.



Para obtener información sobre la configuración de GPO, consulte en este artículo, Configuración de escritorio y tabletas de Windows.

Configurar GPO para su implementación en Citrix Workspace Environment Management

La directiva de dispositivo de configuración de GPO de Windows le permite configurar GPO para cualquier dispositivo Windows compatible con Citrix Workspace Environment Management (WEM). Citrix Endpoint Management envía las directivas al servicio Citrix WEM. A continuación, el servicio WEM aplica los GPO a los dispositivos y sus aplicaciones mediante el agente WEM instalado en los dispositivos.

Para obtener información sobre la instalación del agente de Workspace Environment Management, consulte Instalar y configurar.

Esta directiva utiliza todos los archivos ADMX del sistema operativo Windows. Si quiere cargar un archivo ADMX de terceros, utilice la directiva de dispositivo de Configuración de aplicaciones. Para obtener más información sobre cómo cargar archivos ADMX de terceros, consulte Directiva de dispositivo de configuración de aplicaciones.

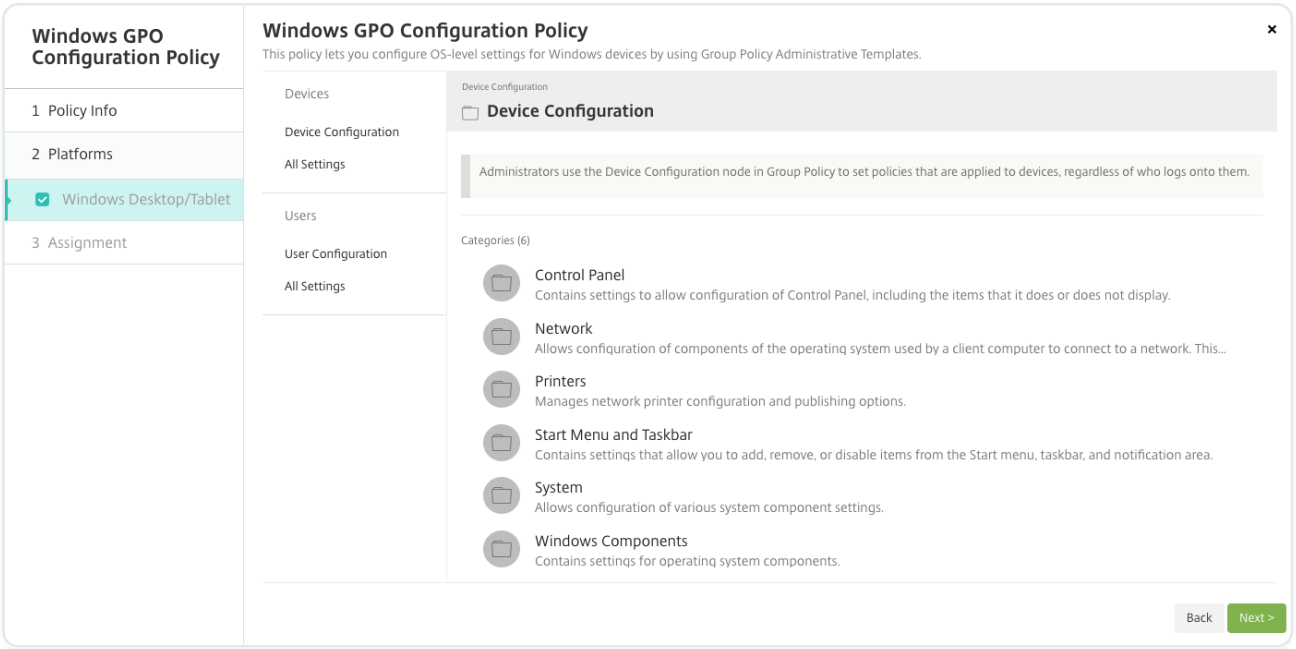
- Puede enviar configuraciones de GPO a cualquier dispositivo compatible con WEM, incluso si Citrix Endpoint Management no admite el dispositivo de forma nativa. Para obtener una lista de los dispositivos compatibles, consulte Requisitos del sistema operativo.
- Esta directiva requiere que un dispositivo tenga el agente de WEM instalado y configurado. No es necesario inscribir los dispositivos en MDM o MAM.
- Citrix Endpoint Management envía la configuración de GPO a través del canal WEM. (Microsoft no admite el envío de configuraciones a nivel de dispositivo a través del canal MDM). Los dispositivos que reciben la directiva de dispositivo de Configuración de GPO de Windows se ejecutan en el modo de Citrix Endpoint Management llamado WEM. En la lista de

dispositivos inscritos de **Administrar > Dispositivos**, la columna **Modo** de los dispositivos administrados por WEM muestra **WEM**.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte Directivas de dispositivo.

Configuración de escritorios y tabletas Windows

Esta directiva le permite configurar GPO a nivel de dispositivo y de usuario.



Seleccione y configure la GPO de Windows que quiere implementar en sus dispositivos Windows. Puede modificar la **Configuración del dispositivo** y la **Configuración del usuario**. Las directivas se muestran en una estructura de árbol. Haga clic en **Todas las configuraciones** para mostrar todas las configuraciones. Para obtener información sobre las configuraciones, descargue una hoja de referencia de GPO de Microsoft.

Para configurar un ajuste, primero debe habilitarlo. Durante la configuración, Citrix Endpoint Management guarda automáticamente los cambios para que esos ajustes persistan. Si intenta salir de la página antes de que se haya guardado un ajuste, aparecerá un mensaje emergente que indica que hay cambios sin guardar.

Si un ajuste tiene dos opciones, aparece una selección de botón de radio. Con más de dos opciones, aparece un menú.

> **Nota:**
>
> Si necesita comprobar qué configuraciones ha realizado, puede hacer lo siguiente.

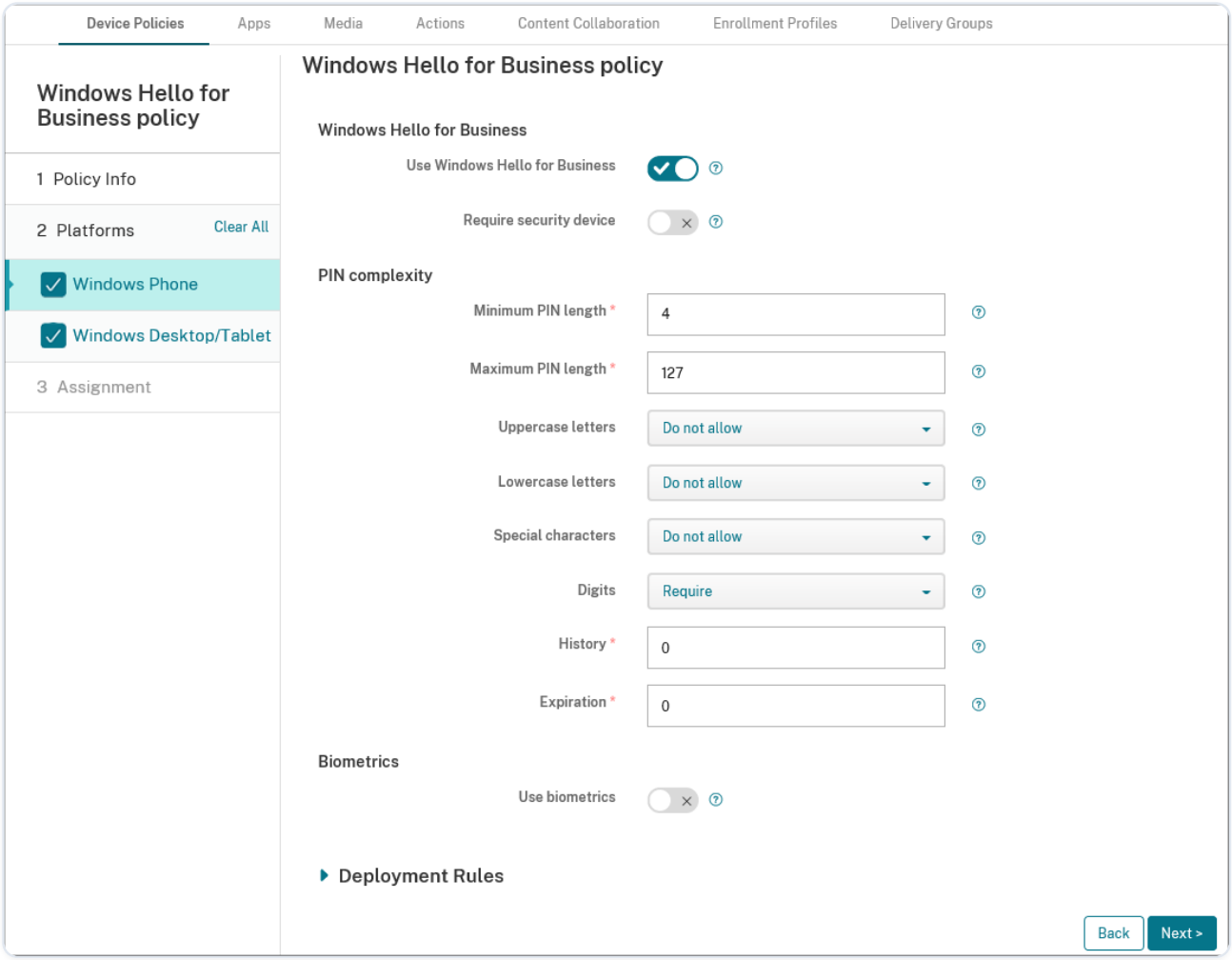
1. En la consola de Citrix Endpoint Management, abra la directiva **Configuración de GPO de Windows** que quiera editar.
2. En **Dispositivos** o **Usuarios**, seleccione **Todos los ajustes**.
3. Ordene la tabla por **Estado**, ascendente. Todas las directivas no configuradas tienen el estado **No configurado**. Las directivas que configure se enumeran en la parte superior.

Directiva de dispositivo de Windows Hello para empresas

Windows Hello para empresas permite a los usuarios iniciar sesión en dispositivos Windows mediante su cuenta de Active Directory o Azure Active Directory. Utilice la directiva de dispositivo **Windows Hello para empresas** para habilitar la función, de modo que los usuarios puedan aprovisionar Windows Hello para empresas en su dispositivo. La directiva también le permite configurar limitaciones de código de acceso y otras funciones de seguridad.

Vaya a **Configurar > Directivas de dispositivo** para agregar la directiva de dispositivo **Windows Hello para empresas**. Configure estos ajustes:

Configuración de Windows para equipos de escritorio/tabletas



- **Usar Windows Hello para empresas:** Habilite la función para permitir que los usuarios aprovisionen Windows Hello para empresas en su dispositivo.
- **Requerir dispositivo de seguridad:** Exija que los usuarios tengan un Módulo de plataforma segura (TPM) para iniciar sesión.
- **Longitud mínima/máxima del PIN:** Longitud mínima y máxima para los PIN de usuario. La **longitud mínima del PIN** predeterminada es **4**. La **longitud máxima del PIN** predeterminada es **127**.
- **Letras mayúsculas**, **letras minúsculas**, **caracteres especiales:** Seleccione si **Permitir**, **Requerir** o **No permitir** cada tipo de carácter. El valor predeterminado es **No permitir**.
- **Dígitos:** Si **Permitir**, **Requerir** o **No permitir** dígitos. El valor predeterminado es **Requerir**.
- **Historial:** El número de PIN anteriores que los usuarios no pueden reutilizar. El valor predeterminado es **0**, lo que significa que los usuarios pueden reutilizar todos los PIN.
- **Caducidad:** El número de días antes de que un usuario deba cambiar su PIN. El valor predeterminado es **0**, lo que significa que los PIN no caducan.

- **Usar datos biométricos:** Permite el uso de datos biométricos en lugar de PIN para el inicio de sesión del usuario.

Añadir aplicaciones

Añadir aplicaciones a Citrix Endpoint Management proporciona capacidades de administración de aplicaciones móviles (MAM). Citrix Endpoint Management ayuda con la entrega de aplicaciones, la concesión de licencias de software, la configuración y la administración del ciclo de vida de las aplicaciones.

La habilitación de aplicaciones con MDX es una parte importante de la preparación de algunos tipos de aplicaciones para su distribución a los dispositivos de los usuarios. Para una introducción a MDX, consulte Componentes de Citrix Endpoint Management y Información general sobre el SDK de MAM.

- Citrix recomienda el uso del SDK de MAM para habilitar aplicaciones con MDX. O bien, puede seguir encapsulando aplicaciones con MDX hasta que el MDX Toolkit quede obsoleto. Consulte Desuso.
- No puede usar el MDX Toolkit para encapsular las aplicaciones de productividad móvil de Citrix. Obtenga los archivos MDX de las aplicaciones de productividad móvil de las descargas de Citrix.

Cuando añade aplicaciones a la consola de Citrix Endpoint Management, usted:

- Configura los ajustes de la aplicación
- Opcionalmente, organiza las aplicaciones en categorías para organizarlas en Citrix Secure Hub
- Opcionalmente, define flujos de trabajo para requerir aprobación antes de permitir a los usuarios acceder a una aplicación
- Implementa aplicaciones para los usuarios

Este artículo cubre los flujos de trabajo generales para añadir aplicaciones. Consulte los siguientes artículos para conocer las especificidades de la plataforma:

- Distribuir aplicaciones de Android Enterprise
- Distribuir aplicaciones de Apple

> **Importante:**

> Citrix Endpoint Management admite la adición y el mantenimiento de hasta 300 aplicaciones. Superar este límite hace que el sistema se vuelva inestable.

Tipos y características de las aplicaciones

La siguiente tabla resume los tipos de aplicaciones que puede implementar con Citrix Endpoint Management.

TIPO DE APLICACIÓN	ORÍGENES	NOTAS	VER
MDX	Aplicaciones iOS y Android que desarrolla para sus usuarios. Aplicaciones de productividad móvil de Citrix.	Desarrolle aplicaciones iOS o Android con el SDK de MAM o encapsúlelas con el MDX Toolkit. Para las aplicaciones de productividad móvil, descargue los archivos MDX de la tienda pública desde las descargas de Citrix. Luego, agregue las aplicaciones a Citrix Endpoint Management.	Agregar una aplicación MDX
Tienda de aplicaciones pública	Aplicaciones gratuitas o de pago de tiendas de aplicaciones públicas como Google Play o Apple App Store.	Cargue las aplicaciones, habilite MDX en ellas y, a continuación, agregue las aplicaciones a Citrix Endpoint Management.	Agregar una aplicación de tienda de aplicaciones pública

TIPO DE APLICACIÓN	ORÍGENES	NOTAS	VER
Web y SaaS	Su red interna (aplicaciones web) o una red pública (SaaS).	Citrix Endpoint Management proporciona inicio de sesión único móvil para aplicaciones SaaS nativas desde dispositivos iOS y Android inscritos en MDM. O bien, utilice conectores de aplicaciones SAML (Security Assertion Markup Language).	Agregar una aplicación web o SaaS
Empresarial	Aplicaciones privadas, incluidas las aplicaciones Win32, que no están habilitadas para MDX. Aplicaciones privadas de Android Enterprise que están habilitadas para MDX. Las aplicaciones empresariales se encuentran en ubicaciones de Content Delivery Network o en servidores de Citrix Endpoint Management.	Agregue las aplicaciones a Citrix Endpoint Management.	Agregar una aplicación empresarial
Enlace web	Direcciones web de Internet, direcciones web de intranet o aplicaciones web que no requieren	Configure enlaces web en Citrix Endpoint Management.	Agregar un enlace web

TIPO DE APLICACIÓN	ORÍGENES	NOTAS	VER
	inicio de sesión único.		

Al planificar la distribución de aplicaciones, tenga en cuenta estas funciones:

- Acerca de las instalaciones silenciosas
- Acerca de las aplicaciones obligatorias y opcionales
- Acerca de las categorías de aplicaciones
- Entregar aplicaciones empresariales desde la CDN de Citrix
- Habilitar aplicaciones de Microsoft 365
- Aplicar flujos de trabajo
- Marca de la tienda de aplicaciones y de Citrix Secure Hub
- Citrix Virtual Apps and Desktops™ a través de la tienda de aplicaciones

Acerca de las instalaciones silenciosas

Citrix admite la instalación y actualización silenciosas de aplicaciones iOS, Android Enterprise y Samsung. La instalación silenciosa significa que no se solicita a los usuarios que instalen las aplicaciones que implementa en el dispositivo. Las aplicaciones se instalan automáticamente en segundo plano.

Requisitos previos para implementar la instalación silenciosa:

- Para iOS, ponga el dispositivo iOS administrado en modo supervisado. Para obtener más información, consulte Importar la directiva de dispositivo de perfil de iOS y macOS.
- Para Android Enterprise, las aplicaciones se instalan en el perfil de trabajo de Android en el dispositivo. Para obtener más información, consulte Android Enterprise.
- Para dispositivos Samsung, habilite Samsung Knox en el dispositivo.

  Para ello, configure la directiva de dispositivo de clave de licencia de Samsung MDM para generar códigos de acceso de licencia de Samsung ELM y Knox. Para obtener más información, consulte las directivas de dispositivo de clave de licencia de Samsung MDM.

Acerca de las aplicaciones obligatorias y opcionales

Al agregar aplicaciones a un grupo de entrega, elige si son opcionales u obligatorias. Citrix recomienda implementar las aplicaciones como **Obligatorias**.

- Las aplicaciones obligatorias se instalan silenciosamente en los dispositivos de los usuarios, minimizando la interacción. Tener esta función habilitada también permite que las aplicaciones se actualicen automáticamente.
- Las aplicaciones opcionales permiten a los usuarios elegir qué aplicaciones instalar, pero los usuarios deben iniciar la instalación manualmente a través de Citrix Secure Hub.

Para las aplicaciones marcadas como obligatorias, los usuarios pueden recibir actualizaciones rápidamente en situaciones como:

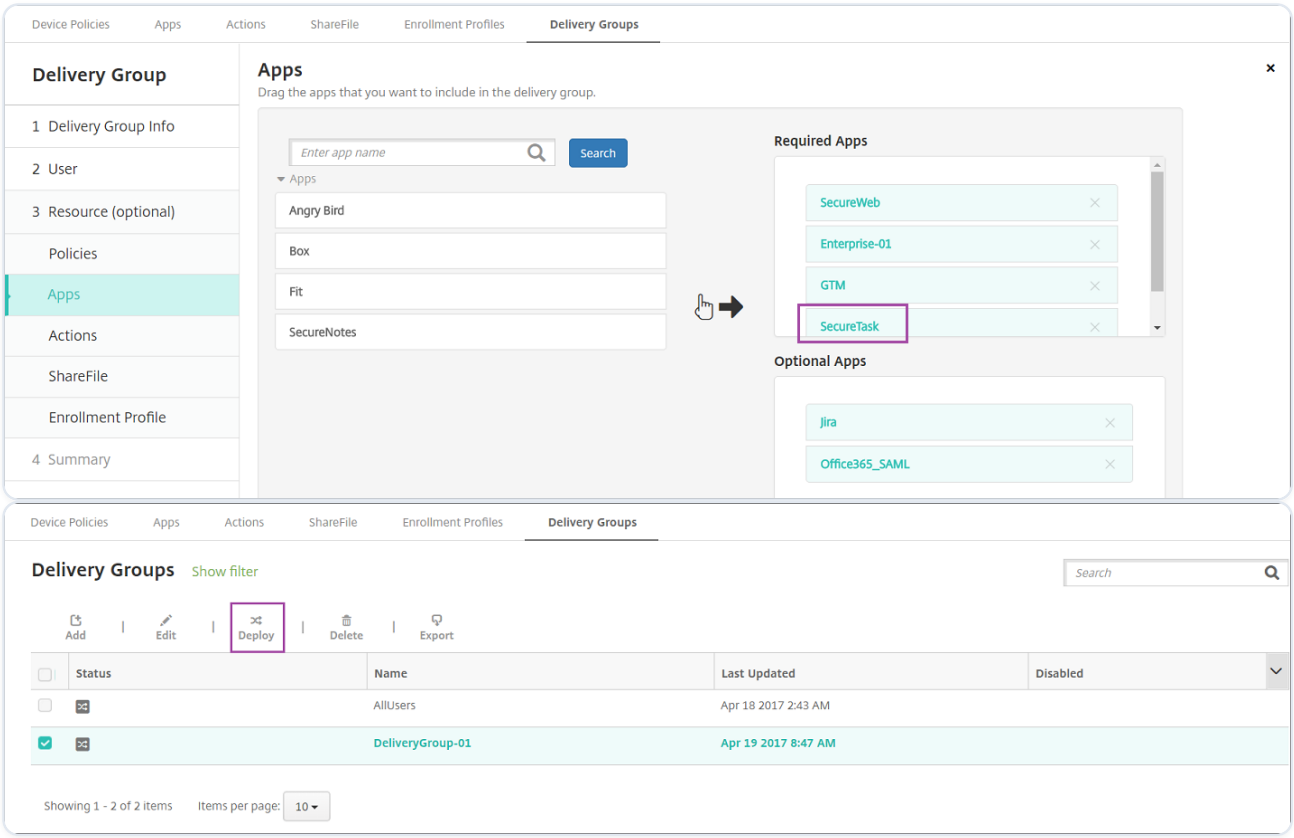
- Usted carga una nueva aplicación y la marca como obligatoria.
- Usted marca una aplicación existente como obligatoria.
- Un usuario elimina una aplicación obligatoria.
- Hay una actualización de Citrix Secure Hub disponible.

Requisitos para la implementación forzada de aplicaciones obligatorias

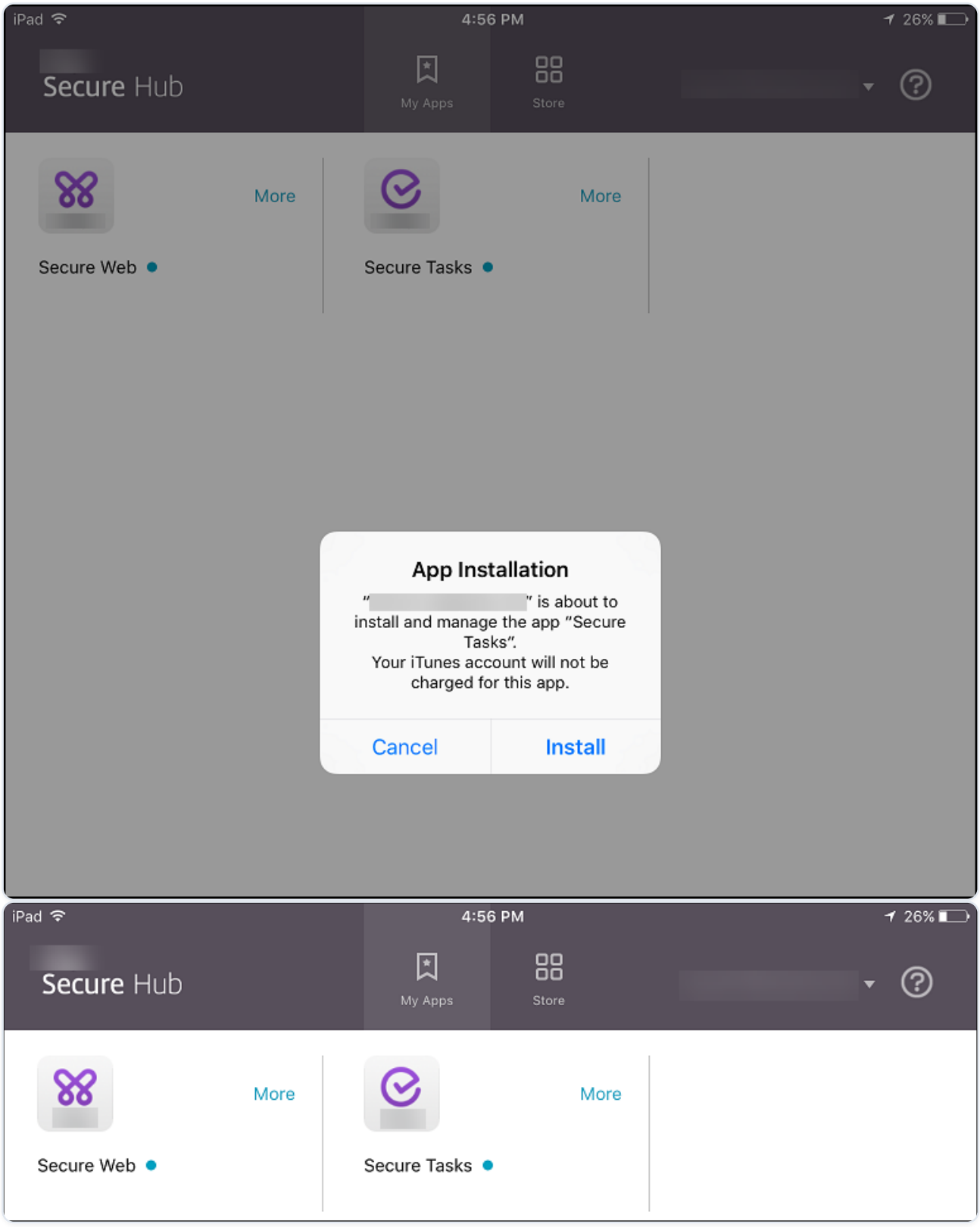
- Citrix Secure Hub 10.5.15 para iOS y 10.5.20 para Android (versiones mínimas)
- MAM SDK o MDX Toolkit 10.6 (versión mínima)
- Después de actualizar Citrix Endpoint Management y Citrix Secure Hub: Los usuarios con dispositivos inscritos deben cerrar sesión y volver a iniciarla en Citrix Secure Hub para obtener las actualizaciones de implementación de aplicaciones obligatorias.

Ejemplos

Los siguientes ejemplos muestran la secuencia de cómo agregar una aplicación llamada Secure Tasks a un grupo de entrega y, a continuación, implementar el grupo de entrega.



Después de que la aplicación de ejemplo, Secure Tasks, se implemente en el dispositivo del usuario, Citrix Secure Hub le pedirá al usuario que instale la aplicación.



Importante:

Las aplicaciones obligatorias habilitadas para MDX, incluidas las aplicaciones empresariales y las aplicaciones de tiendas de aplicaciones públicas, se actualizan inmediatamente. Esta

> actualización se produce incluso si configura una política MDX para un período de gracia de actualización de la aplicación y el usuario elige actualizar la aplicación más tarde.

Flujo de trabajo de aplicaciones obligatorias de iOS para aplicaciones empresariales y de tiendas públicas

1. Implemente la aplicación de productividad móvil durante la inscripción inicial. La aplicación obligatoria se instala en el dispositivo.
2. Actualice la aplicación en la consola de Citrix Endpoint Management.
3. Utilice la consola de Citrix Endpoint Management para implementar las aplicaciones obligatorias.
4. La aplicación de la pantalla de inicio se actualiza. Y, para las aplicaciones de tiendas públicas, la actualización se inicia automáticamente. No se solicita a los usuarios que actualicen.
5. Los usuarios abren la aplicación desde la pantalla de inicio. Las aplicaciones se actualizan inmediatamente, incluso si establece un período de gracia de actualización de la aplicación y el usuario toca para actualizar la aplicación más tarde.

Flujo de trabajo de aplicaciones obligatorias de Android para aplicaciones empresariales

1. Implemente la aplicación de productividad móvil durante la inscripción inicial. La aplicación obligatoria se instala en el dispositivo.
2. Utilice la consola de Citrix Endpoint Management para implementar las aplicaciones obligatorias.
3. La aplicación se actualiza. (Los dispositivos Nexus solicitan actualizaciones de instalación, pero los dispositivos Samsung realizan una instalación silenciosa.)
4. Los usuarios abren la aplicación desde la pantalla de inicio. Las aplicaciones se actualizan inmediatamente, incluso si establece un período de gracia de actualización de la aplicación y el usuario toca para actualizar la aplicación más tarde. (Los dispositivos Samsung realizan una instalación silenciosa.)

Flujo de trabajo de aplicación obligatoria de Android para aplicaciones de tiendas públicas

1. Implemente la aplicación de productividad móvil durante la inscripción inicial. La aplicación obligatoria se instala en el dispositivo.
2. Actualice la aplicación en la consola de Citrix Endpoint Management.

3. Utilice la consola de Citrix Endpoint Management para implementar las aplicaciones obligatorias. O bien, abra la tienda de Citrix Secure Hub en el dispositivo. El icono de actualización aparece en la tienda.
4. La actualización de la aplicación se inicia automáticamente. (Los dispositivos Nexus solicitan a los usuarios que instalen la actualización).
5. Abra la aplicación en la pantalla de inicio. La aplicación se actualiza. No se solicita a los usuarios un período de gracia. (Los dispositivos Samsung realizan una instalación silenciosa).

Desinstalar una aplicación cuando está configurada como obligatoria

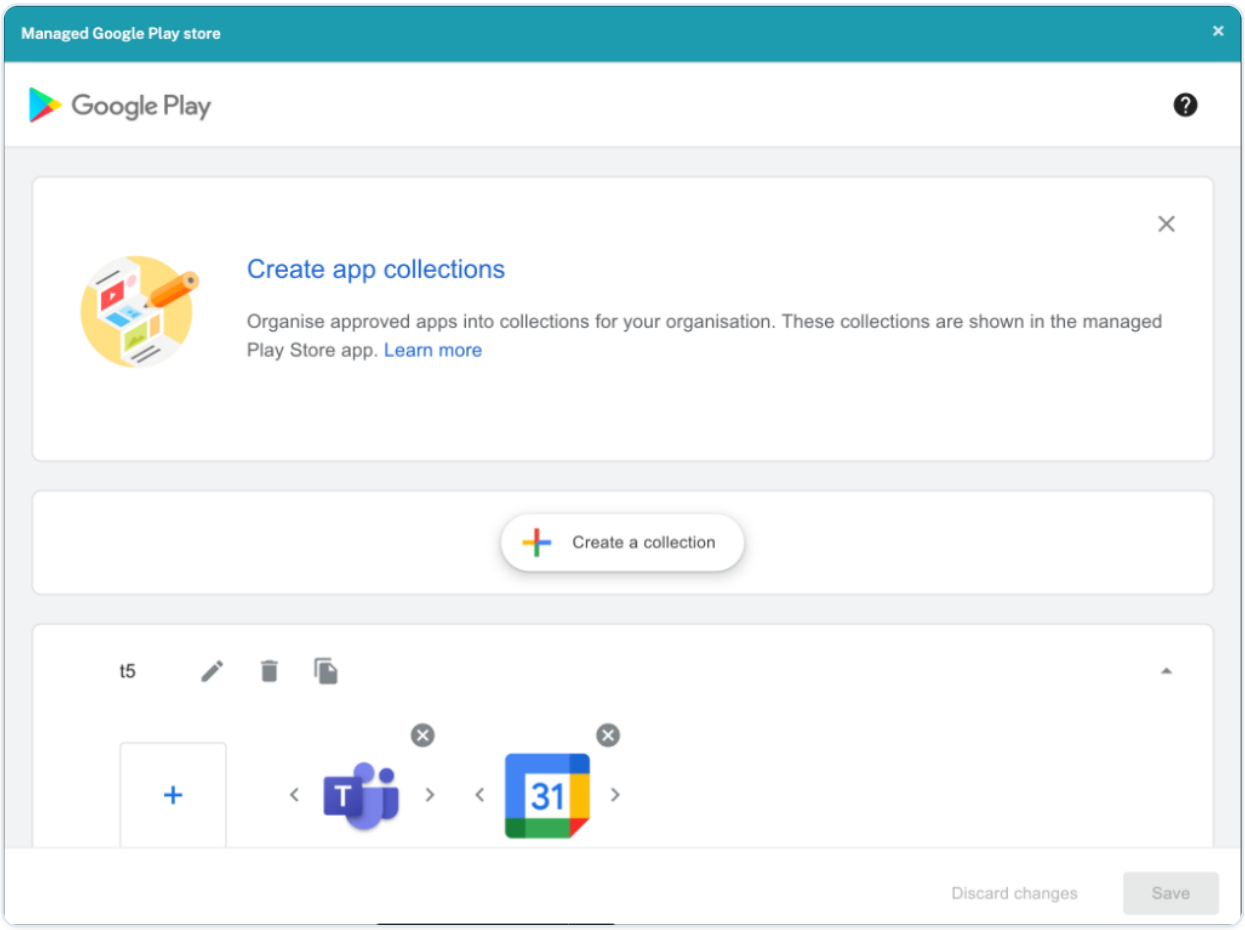
Puede permitir a los usuarios desinstalar una aplicación configurada como obligatoria. Vaya a **Configurar > Grupos de entrega** y mueva la aplicación de **Aplicaciones obligatorias** a **Aplicaciones opcionales**.

Recomendado: Utilice un grupo de entrega especial para cambiar temporalmente una aplicación a opcional, de modo que usuarios específicos puedan desinstalar la aplicación. A continuación, puede cambiar una aplicación obligatoria existente a opcional, implementar la aplicación en ese grupo de entrega y, a continuación, desinstalar la aplicación de esos dispositivos. Después de eso, si desea que las futuras inscripciones para ese grupo de entrega requieran la aplicación, puede volver a configurar la aplicación como obligatoria.

Organizar aplicaciones (Android Enterprise)

Cuando los usuarios inician sesión en Citrix Secure Hub, reciben una lista de las aplicaciones, enlaces web y tiendas que configuró en Citrix Endpoint Management. En Android Enterprise, puede organizar estas aplicaciones en colecciones para permitir a los usuarios acceder solo a ciertas aplicaciones, tiendas o enlaces web. Por ejemplo, puede crear una colección de Finanzas y, a continuación, agregar a esa colección aplicaciones que solo se refieran a finanzas. O bien, puede configurar una colección de Ventas a la que asigne aplicaciones de ventas.

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones > Organizar aplicaciones**. Aparece la ventana de **Managed Google Play store**.



2. Haga clic en **Crear una colección** y seleccione las aplicaciones que se agregarán a esa colección.
3. Cuando haya terminado de agregar colecciones, haga clic en **Guardar**.

> **Nota:**
>
> Los administradores de TI deben aprobar una aplicación antes de que pueda agregarse a una colección en la ventana de Google Play administrado. Un administrador de TI puede aprobar una aplicación yendo a `<https://play.google.com/work>`. En una versión futura, no necesitará aprobar una aplicación antes de agregarla a una colección.

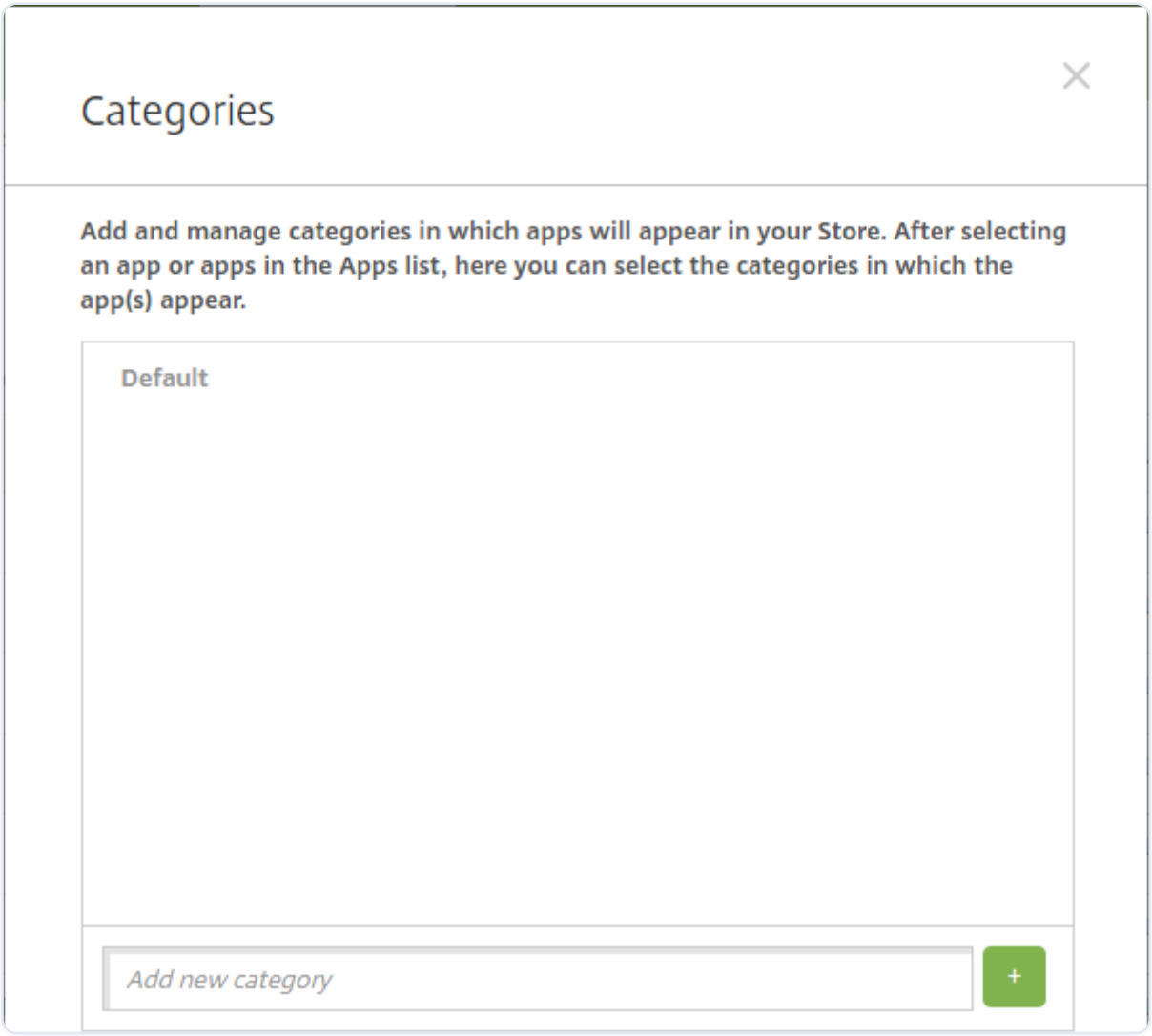
Acerca de las categorías de aplicaciones (iOS y MDX)

Cuando los usuarios inician sesión en Citrix Secure Hub, reciben una lista de las aplicaciones, enlaces web y tiendas que configuró en Citrix Endpoint Management. En iOS o MDX, puede usar categorías de aplicaciones para permitir que los usuarios accedan solo a ciertas aplicaciones, tiendas o enlaces web. Por ejemplo, puede crear una categoría de Finanzas y luego agregar

aplicaciones a esa categoría que solo se relacionen con las finanzas. O bien, puede configurar una categoría de Ventas a la que asigne aplicaciones de ventas.

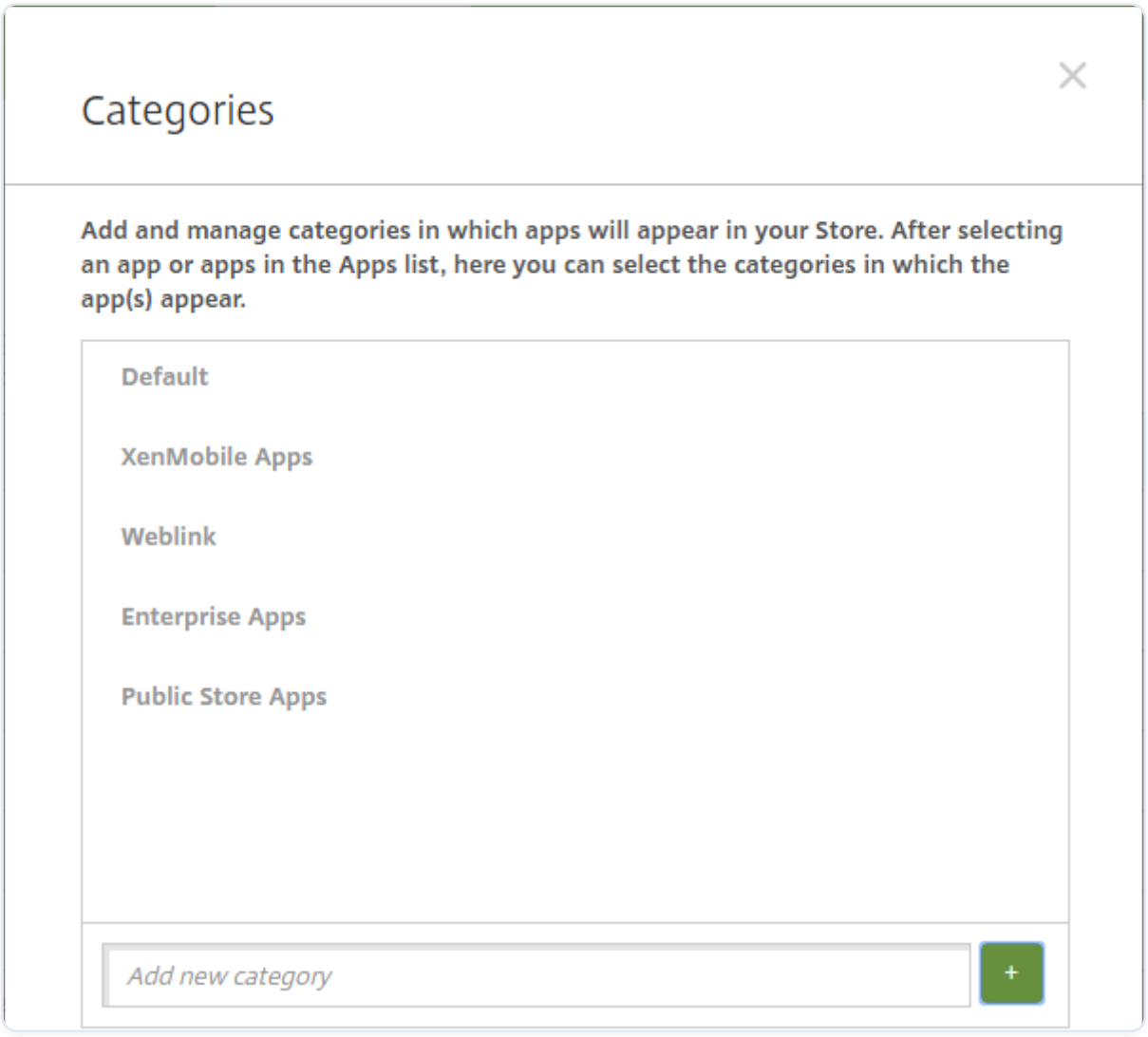
Cuando agrega o edita una aplicación, un enlace web o una tienda, puede agregar la aplicación a una o más de las categorías configuradas.

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones > Categoría**. Aparecerá el cuadro de diálogo **Categorías**.



2. Para cada categoría que quiera agregar, haga lo siguiente:

    - Escriba el nombre de la categoría que quiere agregar en el campo **Agregar una nueva categoría** en la parte inferior del cuadro de diálogo. Por ejemplo, puede escribir Aplicaciones empresariales para crear una categoría para aplicaciones empresariales.
    - Haga clic en el signo más (+) para agregar la categoría. La categoría recién creada se agrega y aparece en el cuadro de diálogo **Categorías**.



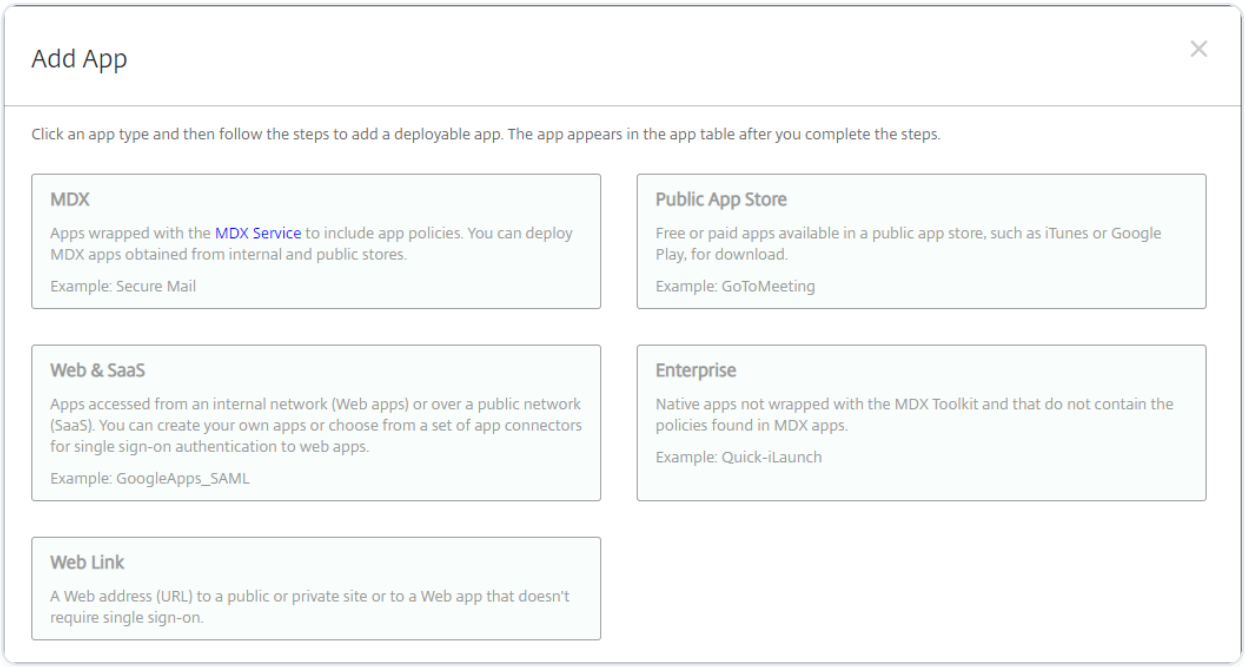
3. Cuando termine de agregar categorías, cierre el cuadro de diálogo **Categorías**.
4. En la página **Aplicaciones**, puede colocar una aplicación existente en una nueva categoría.
    - Seleccione la aplicación que quiere categorizar.
    - Haga clic en **Modificar**. Aparecerá la página **Información de la aplicación**.
    - En la lista **Categoría de aplicación**, aplique la nueva categoría seleccionando la casilla de verificación de la categoría. Desactive las casillas de verificación de cualquier categoría existente que no desee aplicar a la aplicación.
    - Haga clic en la pestaña **Asignaciones de grupos de entrega** o haga clic en **Siguiente** en cada una de las páginas siguientes para avanzar por las páginas restantes de configuración de la aplicación.
    - Haga clic en **Guardar** en la página **Asignaciones de grupos de entrega** para aplicar la nueva categoría. La nueva categoría se aplica a la aplicación y aparece en la tabla **Aplicaciones**.

Agregar una aplicación MDX

Cuando reciba un archivo MDX para una aplicación iOS o Android, puede cargar la aplicación en Citrix Endpoint Management. Después de cargar la aplicación, puede configurar los detalles de la aplicación y la configuración de las directivas. Para obtener información sobre las directivas de aplicación disponibles para cada tipo de plataforma de dispositivo, consulte:

- Información general de MAM SDK
- Directivas MDX de un vistazo

1. Para las aplicaciones de productividad móvil de Citrix, descargue los archivos MDX de la tienda pública: Vaya a `<https://www.citrix.com/downloads>`. Vaya a **Citrix Endpoint Management (XenMobile) > Aplicaciones de productividad de Citrix Endpoint Management**.
2. Para otros tipos de aplicaciones MDX, obtenga el archivo MDX.
3. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones > Agregar**. Aparece el cuadro de diálogo **Agregar aplicación**.



4. Haga clic en **MDX**. Aparece la página **Información de la aplicación MDX**.
5. En el panel **Información de la aplicación**, escriba la siguiente información:

   - **Nombre:** Escriba un nombre descriptivo para la aplicación. El nombre aparece en **Nombre de la aplicación** en la tabla **Aplicaciones**.
   - **Descripción:** Escriba una descripción opcional de la aplicación.

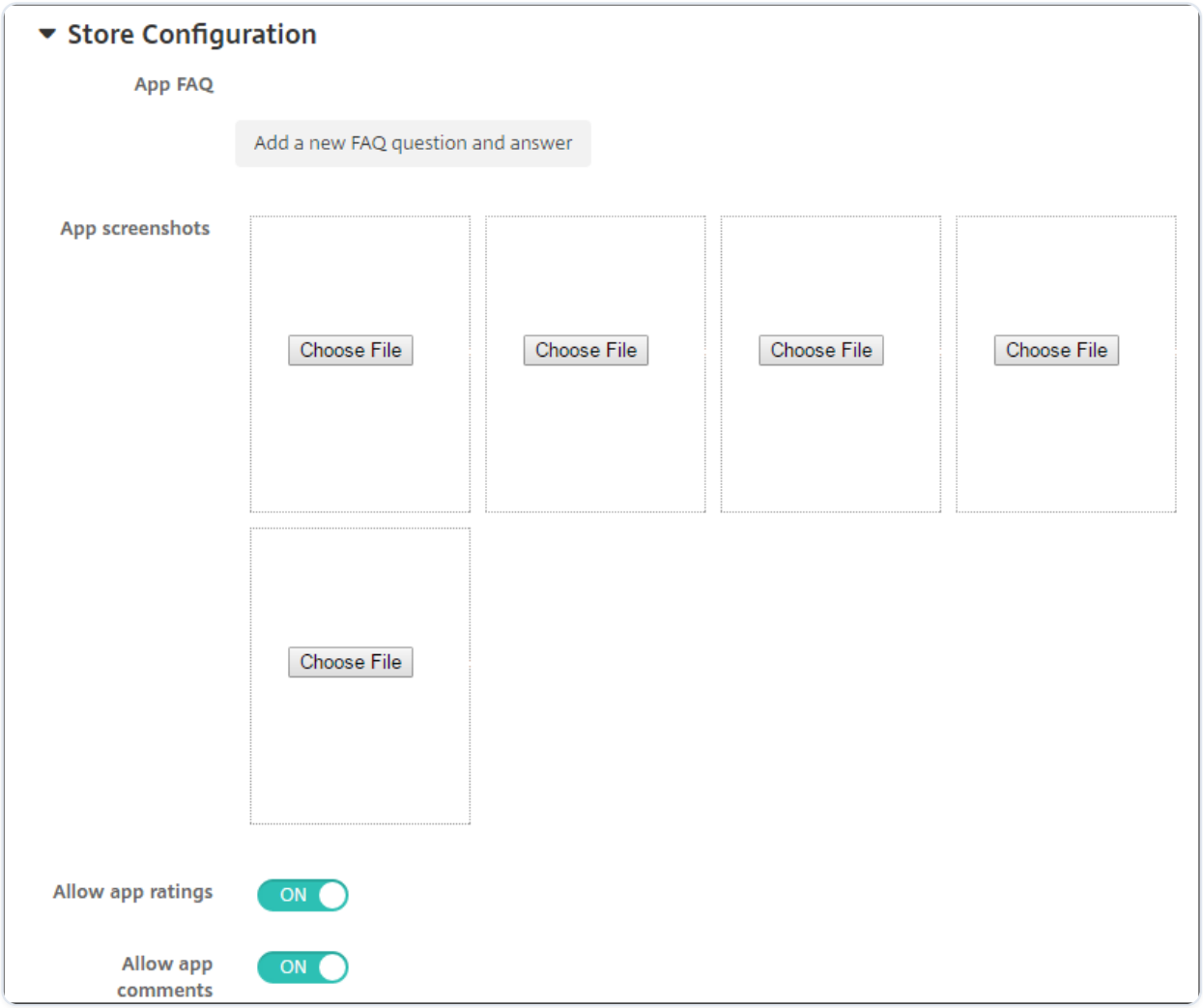
- **Categoría de la aplicación:** Opcionalmente, en la lista, haga clic en la categoría a la que desea añadir la aplicación. Para obtener más información sobre las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.

6. Haga clic en **Siguiente**. Aparece la página **Plataformas de aplicaciones**.
7. En **Plataformas**, seleccione las plataformas que desea añadir. Si solo va a configurar una plataforma, desactive las demás.
8. Para seleccionar un archivo MDX para cargar, haga clic en **Cargar** y vaya a la ubicación del archivo.
9. En la página **Detalles de la aplicación**, configure estos ajustes:

   - **Nombre de archivo:** Escriba el nombre de archivo asociado a la aplicación.
   - **Descripción de la aplicación:** Escriba una descripción para la aplicación.
   - **Versión de la aplicación:** Opcionalmente, escriba el número de versión de la aplicación.
   - **ID de paquete:** Escriba el ID de paquete de la aplicación desde Google Play Store administrado.
   - **Versión mínima del SO:** Opcionalmente, escriba la versión más antigua del sistema operativo que el dispositivo puede ejecutar para usar la aplicación.
   - **Versión máxima del SO:** Opcionalmente, escriba la versión más reciente del sistema operativo que el dispositivo debe ejecutar para usar la aplicación.
   - **Dispositivos excluidos:** Opcionalmente, escriba el fabricante o los modelos de dispositivos que no pueden ejecutar la aplicación.
   - **Eliminar aplicación si se elimina el perfil MDM:** Seleccione si desea eliminar la aplicación de un dispositivo iOS cuando se elimine el perfil MDM. El valor predeterminado es **Activado**.
   - **Impedir la copia de seguridad de los datos de la aplicación:** Seleccione si desea impedir que los usuarios realicen copias de seguridad de los datos de la aplicación en dispositivos iOS. El valor predeterminado es **Activado**.
   - **Pista de producto:** Especifique qué pista de producto desea enviar a los dispositivos iOS. Si tiene una pista diseñada para pruebas, puede seleccionarla y asignarla a sus usuarios. El valor predeterminado es **Producción**.
   - **Forzar la administración de la aplicación:** Para una aplicación que se instala como no administrada, seleccione si desea pedir a los usuarios que permitan que la aplicación se administre en dispositivos iOS no supervisados. El valor predeterminado es **Activado**.

- **Aplicación implementada mediante compra por volumen:** Seleccione si desea implementar la aplicación mediante la compra por volumen de Apple. Si está **Activado**, y usted implementa una versión MDX de la aplicación y utiliza la compra por volumen para implementarla, Citrix Secure Hub solo muestra la instancia de compra por volumen. El valor predeterminado es **Desactivado**.

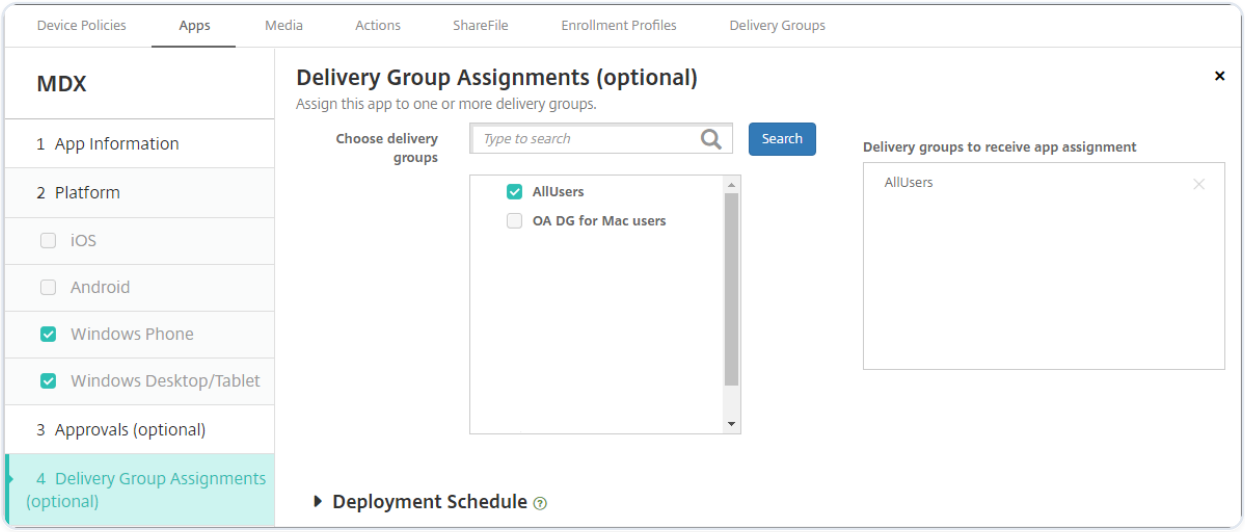
10. Configure las **directivas MDX**. Las directivas MDX varían según la plataforma e incluyen opciones para áreas de directivas, como la autenticación, la seguridad del dispositivo y las restricciones de aplicaciones. En la consola, cada una de las directivas tiene una información sobre herramientas que la describe.
11. Configure las reglas de implementación. Para obtener más información, consulte Configurar reglas de implementación.
12. Expanda **Configuración de la tienda**.



Opcionalmente, puede configurar lo siguiente:

- **Preguntas frecuentes de la aplicación:** Haga clic en **Agregar una nueva pregunta y respuesta de preguntas frecuentes** para crear una sección de preguntas frecuentes para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agregue capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir valoraciones de la aplicación:** Permita que los usuarios valoren la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de la aplicación:** Permita que los usuarios dejen comentarios sobre la aplicación en la tienda de aplicaciones.

13. Haga clic en **Siguiente**. Aparece la página **Asignación de grupos de entrega**.



14. Junto a **Elegir grupos de entrega**, escriba para buscar un grupo de entrega o seleccione uno o varios grupos en la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega para recibir la asignación de aplicaciones**.
15. Expanda **Programación de implementación** y, a continuación, configure los siguientes parámetros:

    - **Implementar:** Elija si quiere implementar la aplicación en los dispositivos. El valor predeterminado es **Activado**.
    - **Programación de implementación:** Elija si quiere implementar la aplicación **Ahora** o **Más tarde**. Si selecciona **Más tarde**, configure una fecha y hora para implementar la aplicación. El valor predeterminado es **Ahora**.
    - **Condición de implementación:** Elija **En cada conexión** para implementar la aplicación cada vez que el dispositivo se conecte. Elija **Solo cuando la implementación anterior ha fallado** para implementar la aplicación cuando el dispositivo no la recibió anteriormente. El valor predeterminado es **En cada conexión**.

La opción **Implementar para conexión siempre activa** se aplica cuando ha configurado la clave de implementación en segundo plano de programación en **Configuración > Propiedades del servidor**.

La opción siempre activa:

- No está disponible para dispositivos iOS
- No está disponible para clientes de Android y Android Enterprise que empezaron a usar Citrix Endpoint Management con la versión 10.18.19 o posterior
- No se recomienda para clientes de Android y Android Enterprise que empezaron a usar Citrix Endpoint Management antes de la versión 10.18.19

La programación de implementación que configure es la misma para todas las plataformas. Cualquier cambio que realice se aplica a todas las plataformas, excepto a **Implementar para conexión siempre activa**.

16. Haga clic en **Guardar**.

Agregar una aplicación de tienda de aplicaciones pública

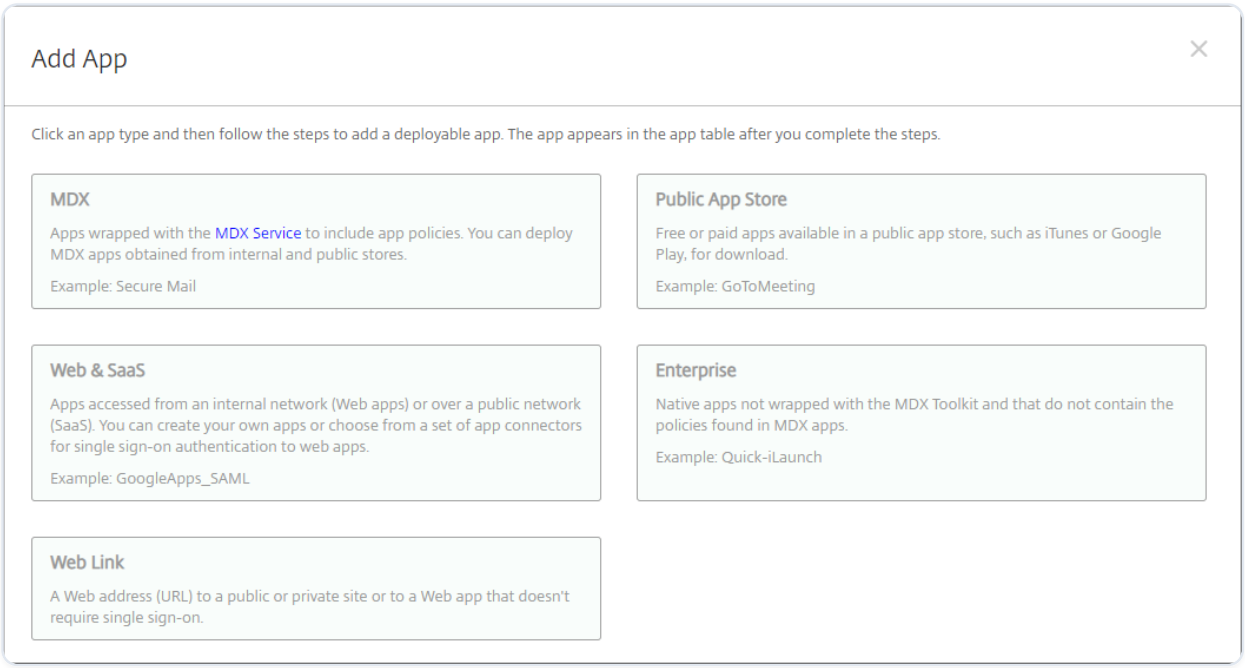
Puede agregar aplicaciones gratuitas o de pago a Citrix Endpoint Management que estén disponibles en una tienda de aplicaciones pública, como Apple App Store.

Puede configurar los ajustes para recuperar los nombres y las descripciones de las aplicaciones de Apple App Store. Cuando recupera la información de la aplicación de la tienda, Citrix Endpoint Management sobrescribe el nombre y la descripción existentes. Configure manualmente la información de la aplicación de Google Play Store.

> **Nota:**
>
> Google ya no admite las aplicaciones de pago para Android a través de Android Enterprise Managed Google Play. Para obtener más información, consulte documentación de ayuda de Managed Google Play.

Configure la información de la aplicación y elija las plataformas a las que desea entregarla:

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones > Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.



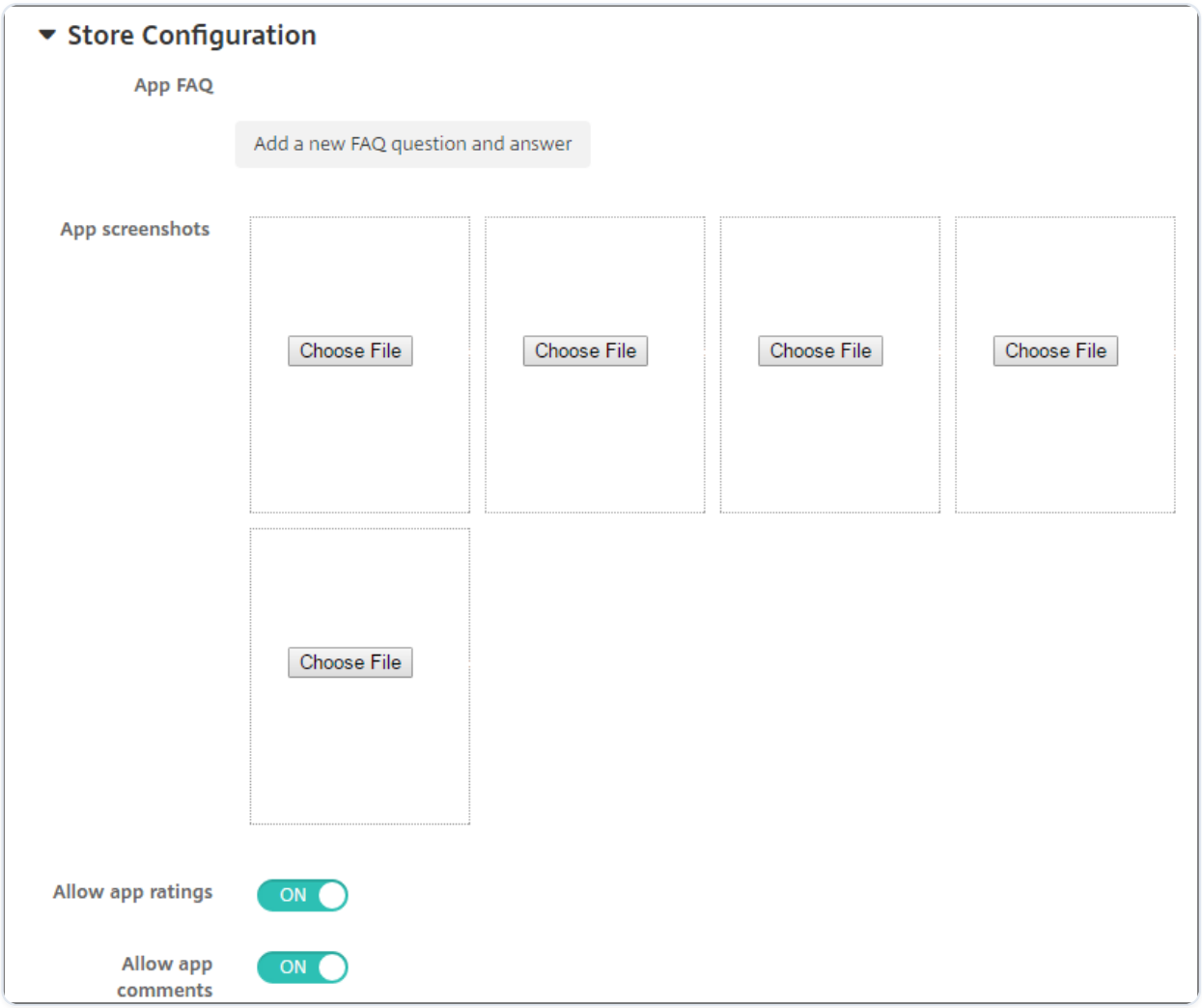
2. Haga clic en **Tienda de aplicaciones pública**. Aparecerá la página **Información de la aplicación**.
3. En el panel **Información de la aplicación**, escriba la siguiente información:
    - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre aparece en **Nombre de la aplicación** en la tabla **Aplicaciones**.
    - **Descripción:** Escriba una descripción opcional de la aplicación.
    - **Categoría de aplicación:** Opcionalmente, en la lista, haga clic en la categoría a la que desea agregar la aplicación. Para obtener más información sobre las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.
4. Haga clic en **Siguiente**. Aparecerá la página **Plataformas de aplicaciones**.
5. En **Plataformas**, seleccione las plataformas que desea agregar. Si solo va a configurar una plataforma, desactive las demás.

A continuación, configure los ajustes de la aplicación para cada plataforma. Consulte:

- Configurar los ajustes de las aplicaciones de Google Play
- Aplicaciones de la tienda de aplicaciones administradas
- Configurar los ajustes de las aplicaciones iOS

Cuando termine de configurar los ajustes de una plataforma, establezca las reglas de implementación de la plataforma y la configuración de la tienda de aplicaciones.

1. Configure las reglas de implementación. Para obtener más información, consulte Configurar reglas de implementación.
2. Expanda **Configuración de la tienda**.



Opcionalmente, puede configurar lo siguiente:

- **Preguntas frecuentes de la aplicación:** Haga clic en **Agregar una nueva pregunta y respuesta de preguntas frecuentes** para crear una sección de preguntas frecuentes para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agregue capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir valoraciones de la aplicación:** Permita que los usuarios valoren la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de la aplicación:** Permita que los usuarios dejen comentarios sobre la aplicación en la tienda de aplicaciones.

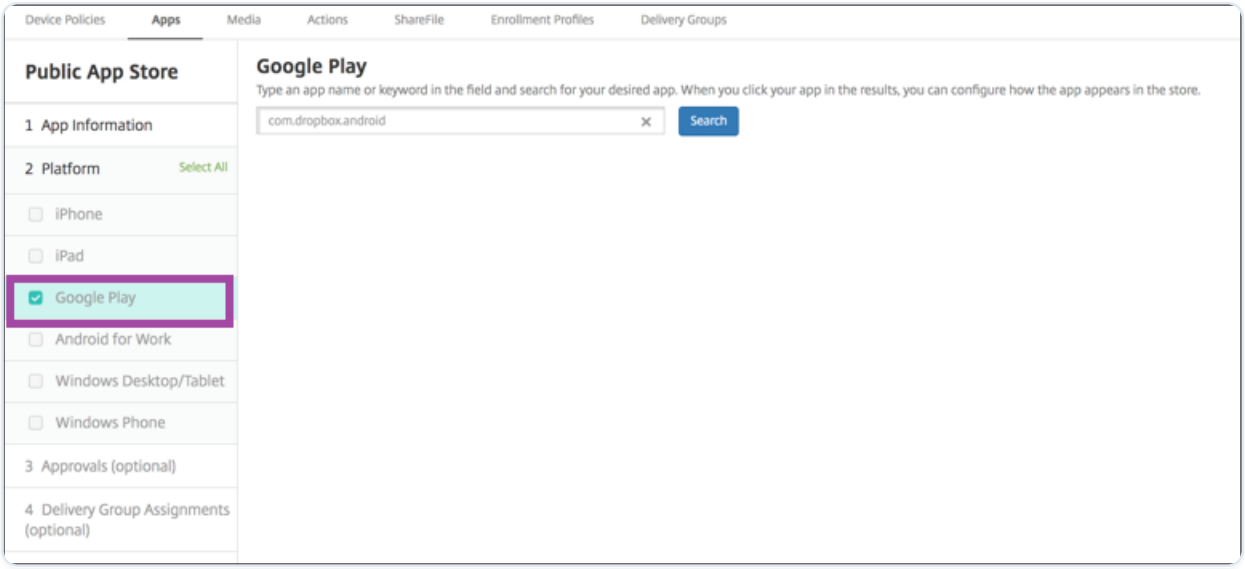
Configurar los ajustes de las aplicaciones de Google Play

Nota:

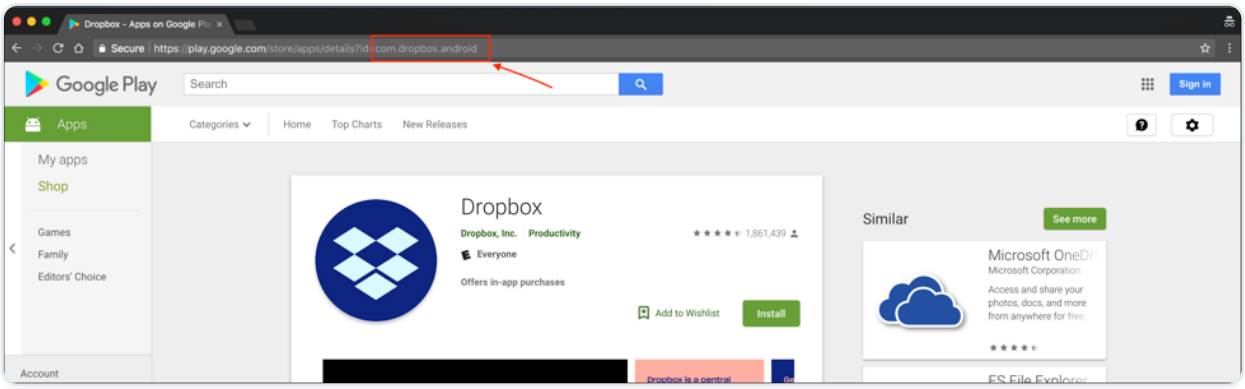
Para que todas las aplicaciones de Google Play Store sean accesibles desde Google Play administrado, utilice la propiedad de servidor **Acceder a todas las aplicaciones en la tienda de Google Play administrada**. (Consulte Propiedades del servidor.) Al establecer esta propiedad en **true**, todos los usuarios de Android Enterprise pueden acceder a las aplicaciones públicas de Google Play Store. A continuación, puede utilizar la directiva de dispositivo Restricciones para controlar el acceso a estas aplicaciones.

La configuración de los ajustes para las aplicaciones de Google Play Store requiere pasos diferentes a los de las aplicaciones para otras plataformas. Configure manualmente la información de la aplicación de Google Play Store.

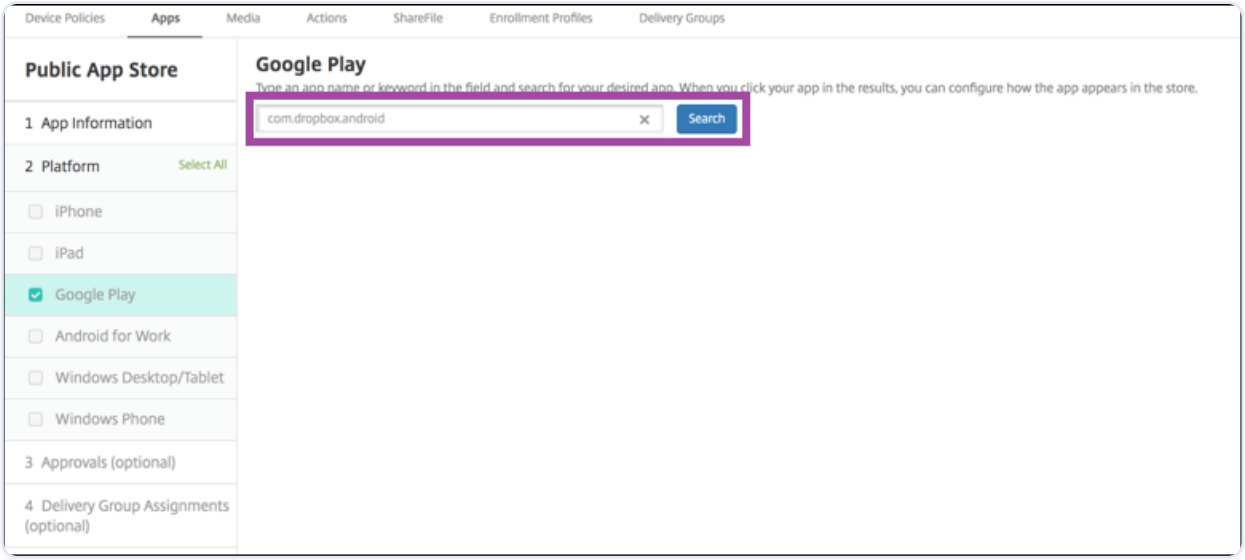
1. Asegúrese de que **Google Play** esté seleccionado en **Plataformas**.



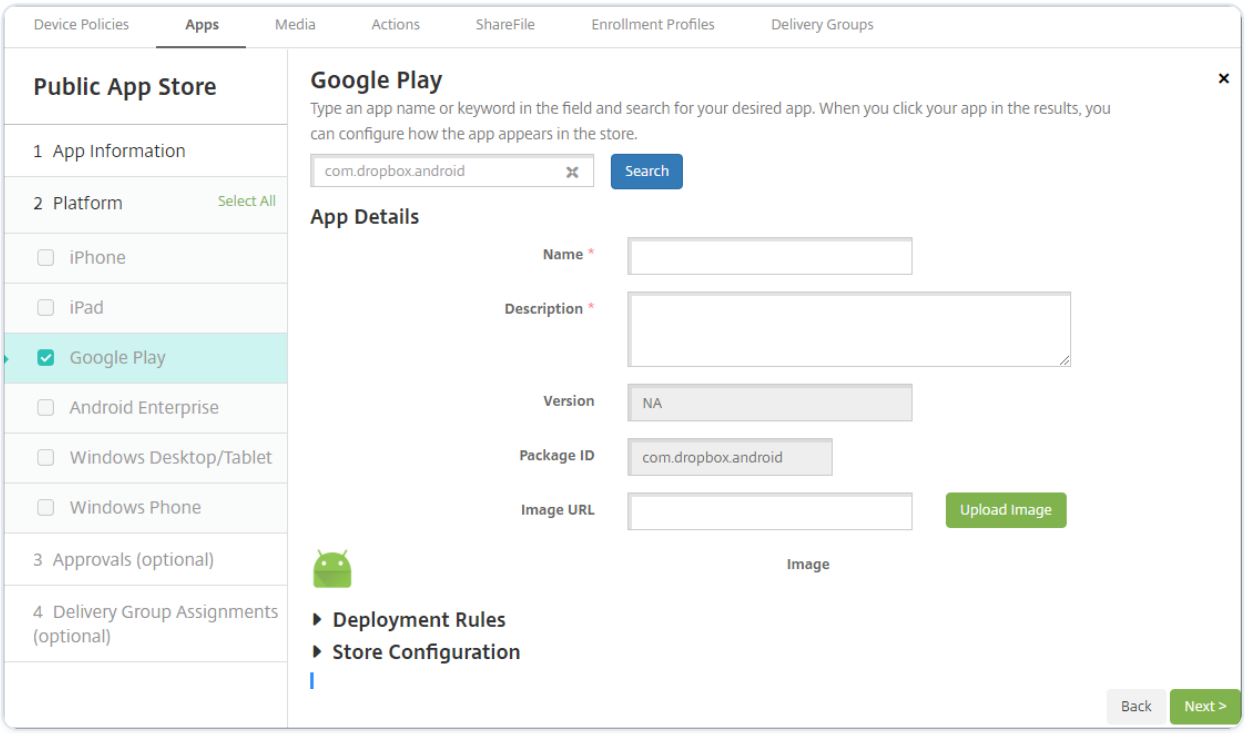
2. Vaya a Google Play Store. Desde Google Play Store, copie el ID del paquete. El ID se encuentra en la URL de la aplicación.



3. Al añadir una aplicación de tienda pública en la consola de Citrix Endpoint Management, pegue el ID del paquete en la barra de búsqueda. Haga clic en **Buscar**.



4. Si el ID del paquete es válido, aparece una interfaz de usuario que le permite introducir los detalles de la aplicación.



5. Puede configurar la URL de la imagen que aparecerá con la aplicación en la tienda. Para usar la imagen de Google Play Store:

   a. Vaya a Google Play Store. Haga clic con el botón derecho en la imagen de la aplicación y copie la dirección de la imagen.

   b. Pegue la dirección de la imagen en el campo **URL de la imagen**.

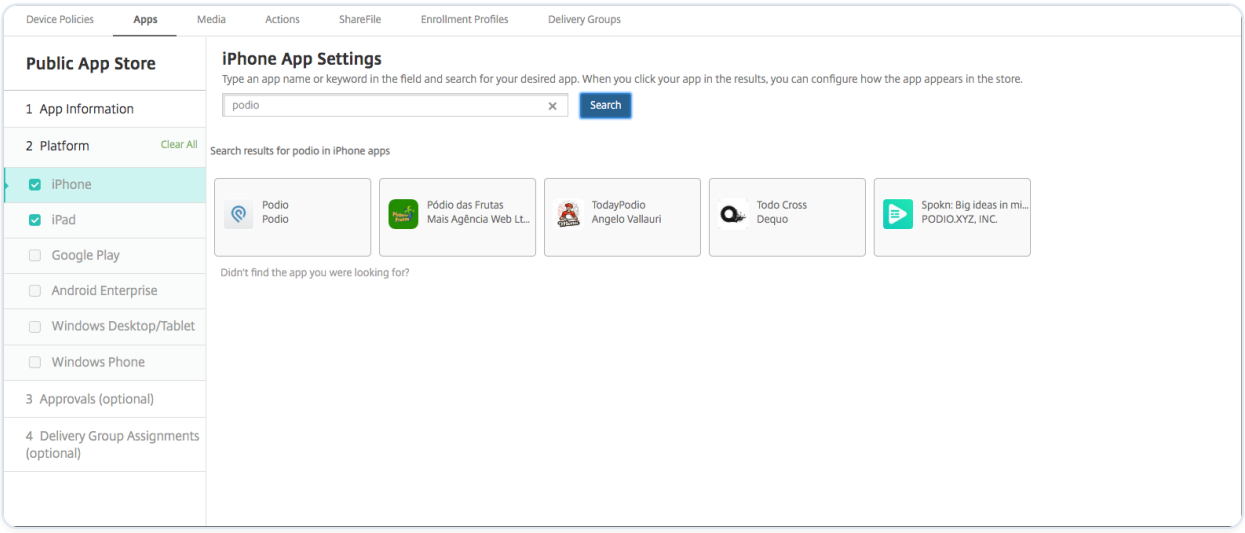
   c. Haga clic en **Cargar imagen**. La imagen aparece junto a **Imagen**.

Si no configura una imagen, la imagen genérica de Android aparece con la aplicación.

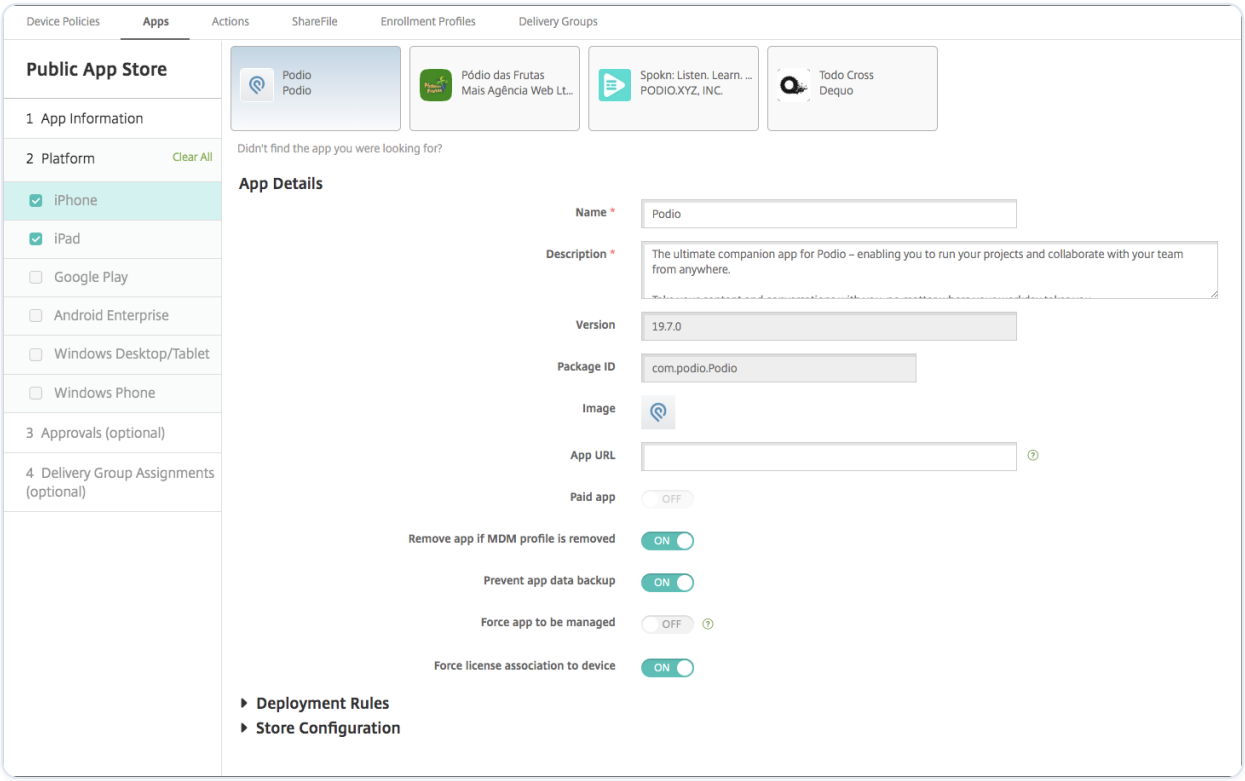
Configurar los ajustes de la aplicación para aplicaciones iOS

1. Escriba el nombre de la aplicación en el cuadro de búsqueda y haga clic en **Buscar**. Aparecen las aplicaciones que coinciden con los criterios de búsqueda. Aparecen las aplicaciones que coinciden con los criterios de búsqueda.

   La siguiente figura muestra el resultado de la búsqueda de **podio** en aplicaciones en un iPhone.



2. Haga clic en la aplicación que desea añadir.
3. Los campos de **Detalles de la aplicación** se rellenan automáticamente con información relacionada con la aplicación elegida (incluidos el nombre, la descripción, el número de versión y la imagen asociada).

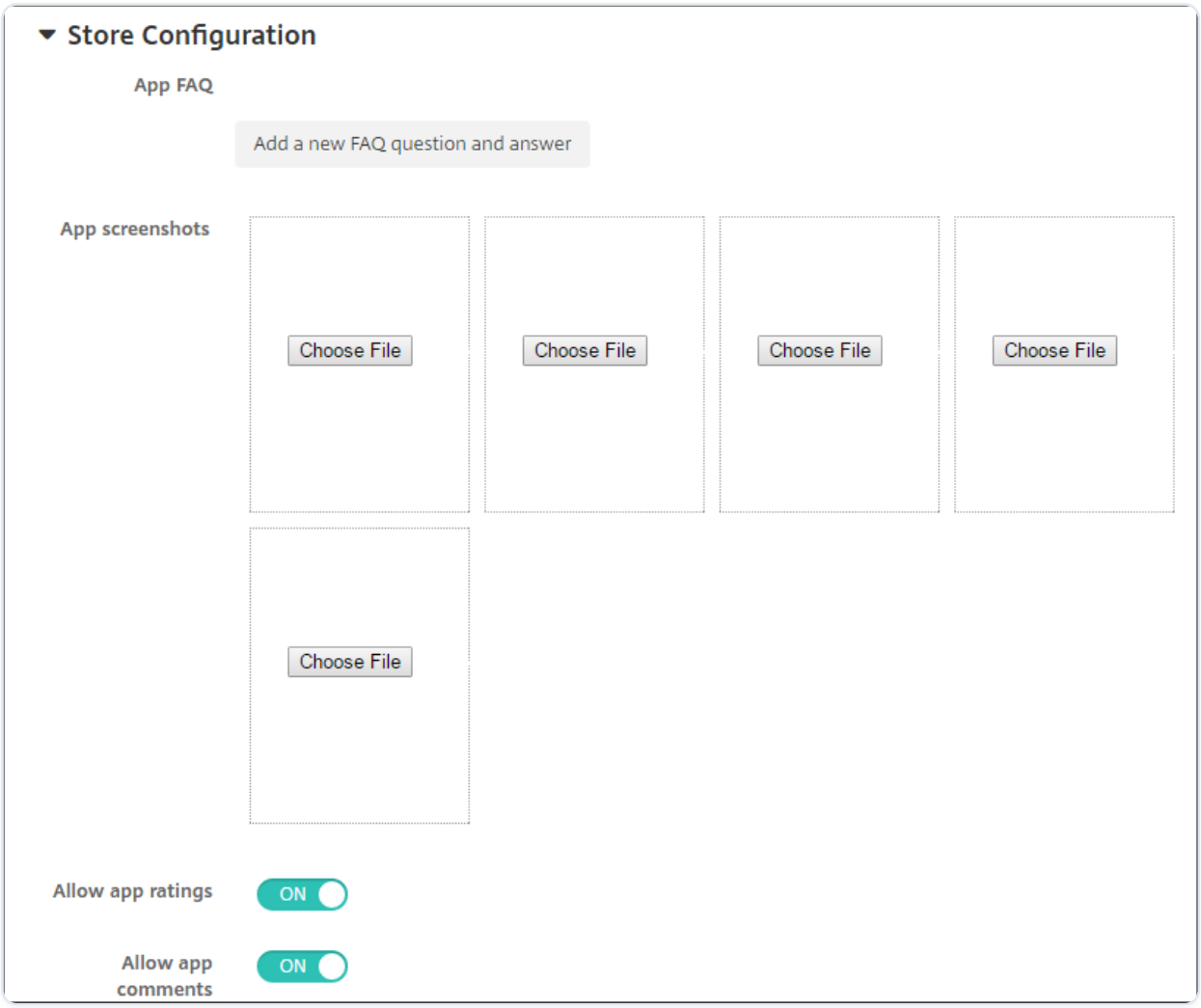


4. Configure los ajustes:

   - Si es necesario, cambie el nombre y la descripción de la aplicación.
   - **URL de la aplicación:** Introduzca una lista de URL separadas por comas para iniciar sus aplicaciones desde la aplicación Citrix Workspace. Este campo solo está disponible para dispositivos iPhone y iPad.
   - **Aplicación de pago:** Este campo está preconfigurado y no se puede cambiar.

- **Eliminar aplicación si se elimina el perfil MDM:** Seleccione si desea eliminar la aplicación si se elimina el perfil MDM. El valor predeterminado es **Activado**.
- **Impedir la copia de seguridad de datos de la aplicación:** Seleccione si desea impedir que la aplicación realice copias de seguridad de datos. El valor predeterminado es **Activado**.
- **Pista de producto:** Especifique qué pista de producto desea enviar a los dispositivos de los usuarios. Si tiene una pista diseñada para pruebas, puede seleccionarla y asignarla a sus usuarios. El valor predeterminado es **Producción**.
- **Forzar la administración de la aplicación:** Para una aplicación que se instala como no administrada, seleccione si desea pedir a los usuarios que permitan que la aplicación se administre en dispositivos iOS no supervisados. El valor predeterminado es **Desactivado**. Para los dispositivos iOS inscritos mediante la inscripción de usuarios, Citrix Endpoint Management no aplica esta configuración y no solicita a los usuarios que permitan la administración de aplicaciones.
- **Forzar la asociación de la licencia al dispositivo:** Seleccione si desea asociar una aplicación (desarrollada con la asociación de dispositivos habilitada) a un dispositivo en lugar de a un usuario. Si la aplicación que eligió no admite la asignación a un dispositivo, no puede cambiar esta configuración.

5. Configure las reglas de implementación. Para obtener más información, consulte Configurar reglas de implementación.
6. Expanda **Configuración de la tienda**.



Opcionalmente, puede configurar lo siguiente:

- **Preguntas frecuentes de la aplicación:** Haga clic en **Agregar una nueva pregunta y respuesta de preguntas frecuentes** para crear unas preguntas frecuentes para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agregue capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir valoraciones de la aplicación:** Permita que los usuarios valoren la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de la aplicación:** Permita que los usuarios dejen comentarios sobre la aplicación en la tienda de aplicaciones.

7. Para iPhone o iPad, expanda **Compra por volumen**.

   a. Para permitir que Citrix Endpoint Management aplique una licencia de compra por volumen para la aplicación: En la lista **Licencia de compra por volumen**, haga clic en **Cargar una licencia de compra por volumen**.

b. En el cuadro de diálogo que aparece, importe la licencia.

   La tabla Asignación de licencias muestra el número de licencias en uso para la aplicación, del total de licencias disponibles.

   Puede desasociar licencias de compra por volumen para un usuario individual. Al hacerlo, finalizan las asignaciones de licencias y se liberan licencias.

c. Cuando agregue su cuenta de compra por volumen, habilite **Actualización automática de la aplicación**. Esta configuración garantiza que las aplicaciones en los dispositivos de los usuarios se actualicen automáticamente cuando aparezca una actualización en la tienda de Apple. Si una aplicación tiene la configuración **Forzar la administración de la aplicación** habilitada, se actualiza sin pedir confirmación al usuario. La actualización se produce tanto si la aplicación es obligatoria como opcional.

8. Después de completar la configuración de **Compra por volumen**, haga clic en **Siguiente**. Aparece la página **Aprobaciones**.

   Para usar flujos de trabajo que requieran aprobación antes de permitir a los usuarios acceder a la aplicación, consulte Aplicar flujos de trabajo. Si no necesita un flujo de trabajo de aprobación, continúe con el siguiente paso.

9. Haga clic en **Siguiente**. Aparece la página **Asignación de grupos de entrega**.
10. Junto a **Elegir grupos de entrega**, escriba para buscar un grupo de entrega o seleccione uno o varios grupos de la lista. Los grupos que seleccione aparecen en la lista **Grupos de entrega que recibirán la asignación de la aplicación**.
11. Expanda **Programación de la implementación** y, a continuación, configure los siguientes parámetros:

    - **Implementar:** Elija si desea implementar la aplicación en los dispositivos. El valor predeterminado es **Activado**.
    - **Programación de implementación:** Elija si desea implementar la aplicación **Ahora** o **Más tarde**. Si selecciona **Más tarde**, configure una fecha y hora para implementar la aplicación. El valor predeterminado es **Ahora**.
    - **Condición de implementación:** Elija **En cada conexión** para implementar la aplicación cada vez que el dispositivo se conecte. Elija **Solo cuando la implementación anterior haya fallado** para implementar la aplicación cuando el dispositivo no la haya recibido anteriormente. El valor predeterminado es **En cada conexión**.

La opción **Implementar para conexión siempre activa** se aplica cuando ha configurado la clave de implementación en segundo plano de programación en **Parámetros > Propiedades del servidor**.

La opción siempre activa:

- No está disponible para dispositivos iOS
- No está disponible para clientes de Android y Android Enterprise que empezaron a usar Citrix Endpoint Management con la versión 10.18.19 o posterior
- No se recomienda para clientes de Android y Android Enterprise que empezaron a usar Citrix Endpoint Management antes de la versión 10.18.19

La programación de implementación que configure es la misma para todas las plataformas. Cualquier cambio que realice se aplica a todas las plataformas, excepto a **Implementar para conexión siempre activa**.

12. Haga clic en **Guardar**.

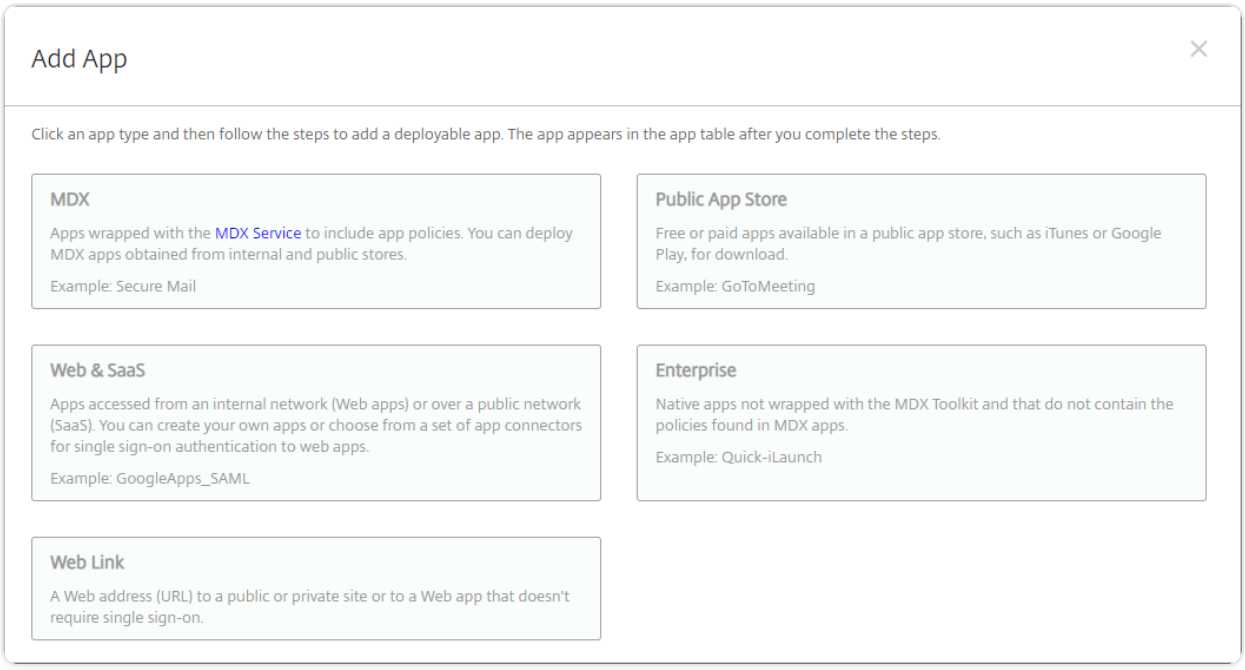
Agregar una aplicación web o SaaS

Con la consola de Citrix Endpoint Management, puede conceder a los usuarios autorización de inicio de sesión único (SSO) para sus aplicaciones empresariales, web y SaaS.

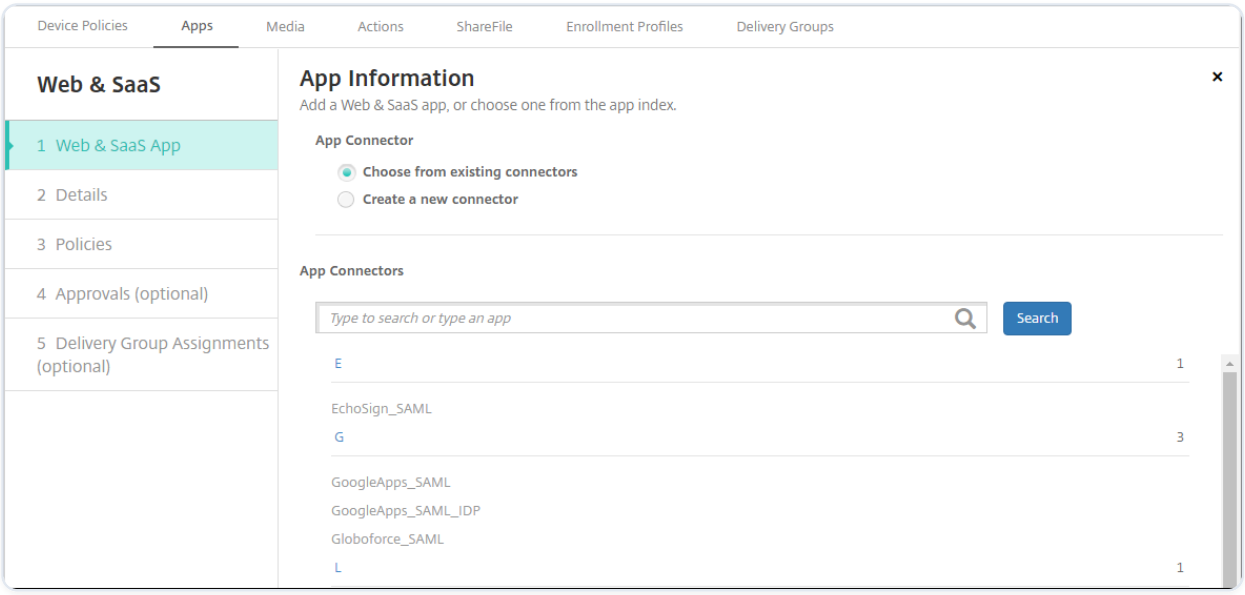
Puede crear su propio conector en Citrix Endpoint Management al agregar una aplicación web o SaaS. Para obtener una lista de los tipos de conectores disponibles en Citrix Endpoint Management, consulte Tipos de conectores de aplicaciones.

Si una aplicación solo está disponible para SSO: Después de guardar la configuración, la aplicación aparece en la ficha **Aplicaciones** en la consola de Citrix Endpoint Management.

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones > Agregar**. Aparece el cuadro de diálogo **Agregar aplicación**.



2. Haga clic en **Web y SaaS**. Aparece la página **Información de la aplicación**.



3. Configure un conector de aplicaciones existente o nuevo de la siguiente manera.

Para configurar un conector de aplicaciones existente

1. En la página **Información de la aplicación**, la opción **Elegir entre conectores existentes** ya está seleccionada, como se mostró anteriormente. Haga clic en el conector que desea usar en la lista **Conectores de aplicaciones**. Aparece la información del conector de aplicaciones.
2. Configure estos ajustes:
   - **Nombre de la aplicación:** Acepte el nombre rellenado previamente o escriba uno nuevo.
   - **Descripción de la aplicación:** Acepte la descripción rellenada previamente o escriba una propia.

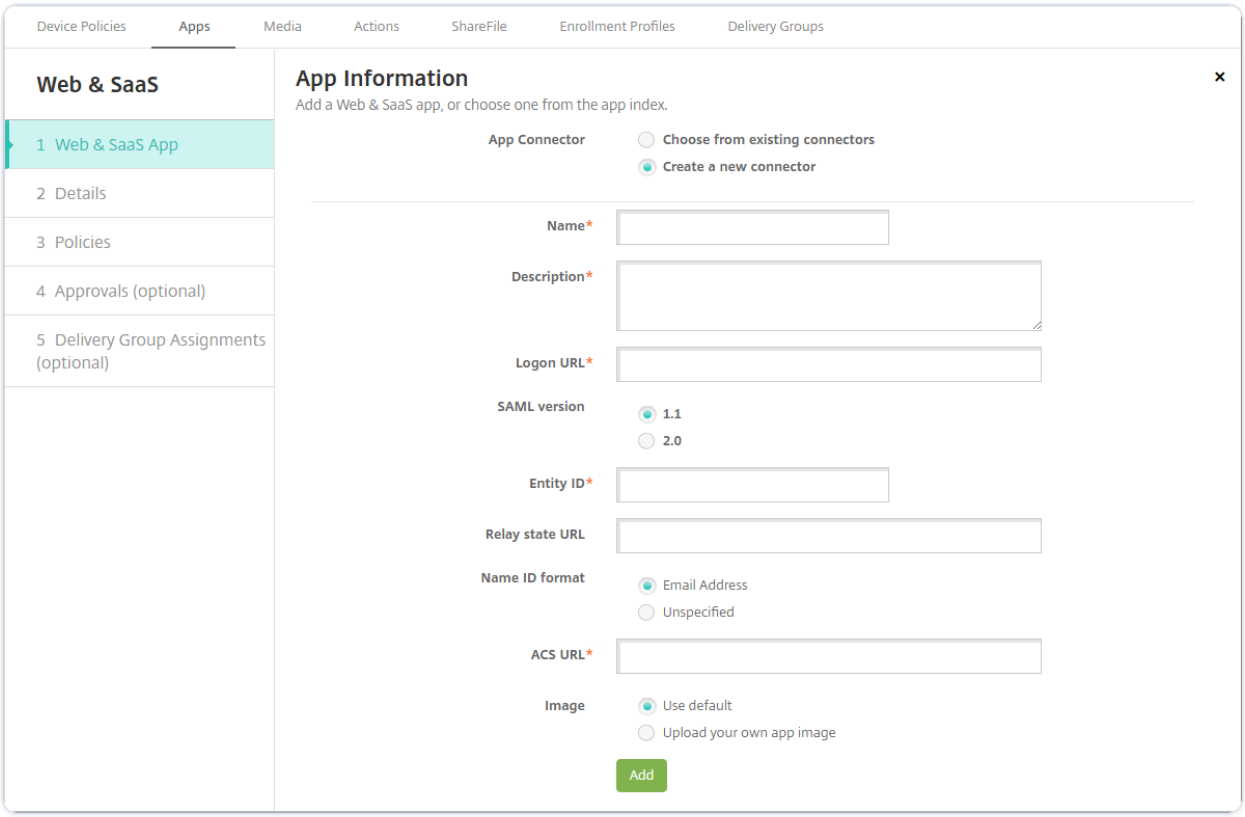
- **URL:** Acepte la URL rellenada previamente o escriba la dirección web de la aplicación. Dependiendo del conector que elija, este campo puede tener un marcador de posición que debe reemplazar antes de poder pasar a la página siguiente.
- **Nombre de dominio:** Si corresponde, escriba el nombre de dominio de la aplicación. Este campo es obligatorio.
- **La aplicación está alojada en la red interna:** Seleccione si la aplicación se ejecuta en un servidor de su red interna. Si los usuarios se conectan desde una ubicación remota a la aplicación interna, deben conectarse a través de NetScaler Gateway. Al establecer esta opción en **Activado**, se añade la palabra clave VPN a la aplicación y se permite a los usuarios conectarse a través de NetScaler Gateway. El valor predeterminado es **Desactivado**.
- **Categoría de la aplicación:** Haga clic en una categoría opcional de la lista desplegable para aplicarla a la aplicación.
- **Aprovisionamiento de cuentas de usuario:** Seleccione si desea crear cuentas de usuario para la aplicación. Si utiliza el conector Globoforce_SAML, debe habilitar esta opción para proporcionar una integración SSO sin problemas.
- Si habilita el **Aprovisionamiento de cuentas de usuario**, configure estos ajustes:
    - **Cuenta de servicio**
        - **Nombre de usuario:** Escriba el nombre del administrador de la aplicación. Este campo es obligatorio.
        - **Contraseña:** Escriba la contraseña del administrador de la aplicación. Este campo es obligatorio.
    - **Cuenta de usuario**
        - **Cuando finaliza el derecho de usuario:** Haga clic en la acción de la lista desplegable que se realizará cuando los usuarios ya no tengan acceso a la aplicación. El valor predeterminado es **Inhabilitar cuenta**.
    - **Regla de nombre de usuario**
        - Para cada regla de nombre de usuario que quiera agregar, haga lo siguiente:
            - **Atributos de usuario:** Haga clic en el atributo de usuario de la lista desplegable para agregarlo a la regla.

    - **Longitud (caracteres):** Haga clic en el número de la lista desplegable de caracteres del atributo de usuario que se utilizará en la regla de nombre de usuario. El valor predeterminado es **Todo**.
    - **Regla:** Cada atributo de usuario que agregue se anexará automáticamente a la regla de nombre de usuario.

- **Requisito de contraseña**
    - **Longitud:** Escriba la longitud mínima de la contraseña de usuario. El valor predeterminado es **8**.
- **Caducidad de la contraseña**
    - **Validez (días):** Escriba el número de días que la contraseña es válida. Los valores válidos son **0–90**. El valor predeterminado es 90.
    - **Restablecer automáticamente la contraseña después de que caduque:** Seleccione si desea restablecer la contraseña automáticamente cuando caduque. El valor predeterminado es **Desactivado**. Si no habilita este campo, los usuarios no podrán abrir la aplicación después de que caduquen sus contraseñas.

Para configurar un nuevo conector de aplicación

1. En la página **Información de la aplicación**, seleccione **Crear un nuevo conector**. Aparecen los campos del conector de aplicación.

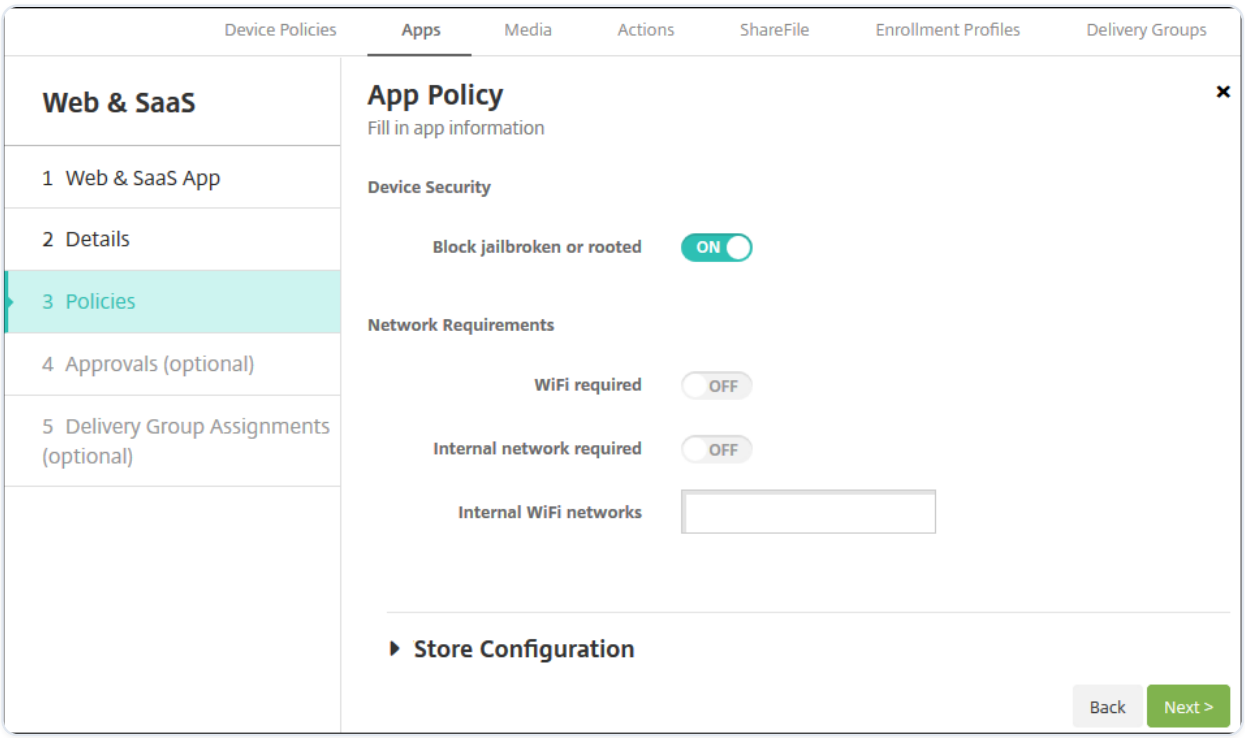


2. Configure estos ajustes:

- **Nombre:** Escriba un nombre para el conector. Este campo es obligatorio.
- **Descripción:** Escriba una descripción para el conector. Este campo es obligatorio.
- **URL de inicio de sesión:** Escriba o copie y pegue la URL donde los usuarios inician sesión en el sitio. Por ejemplo, si la aplicación que quiere agregar tiene una página de inicio de sesión, abra un explorador web y vaya a la página de inicio de sesión de la aplicación. Por ejemplo, podría ser `https://www.example.com/logon`. Este campo es obligatorio.
- **Versión de SAML:** Seleccione **1.1** o **2.0**. El valor predeterminado es **1.1**.
- **ID de entidad:** Escriba la identidad de la aplicación SAML.
- **URL de estado de retransmisión:** Escriba la dirección web de la aplicación SAML. La URL de estado de retransmisión es la URL de respuesta de la aplicación.
- **Formato de ID de nombre:** Seleccione **Dirección de correo electrónico** o **Sin especificar**. El valor predeterminado es **Dirección de correo electrónico**.
- **URL de ACS:** Escriba la URL del Servicio de consumidor de aserciones del proveedor de identidades o del proveedor de servicios. La URL de ACS proporciona a los usuarios la capacidad de inicio de sesión único (SSO).
- **Imagen:** Seleccione si desea usar la imagen predeterminada de Citrix o cargar su propia imagen de aplicación. El valor predeterminado es Usar predeterminada.

- Para cargar su propia imagen, haga clic en **Examinar** y vaya a la ubicación del archivo. El archivo debe ser un archivo .PNG. No puede cargar un archivo JPEG o GIF. Cuando agrega un gráfico personalizado, no puede cambiarlo más tarde.

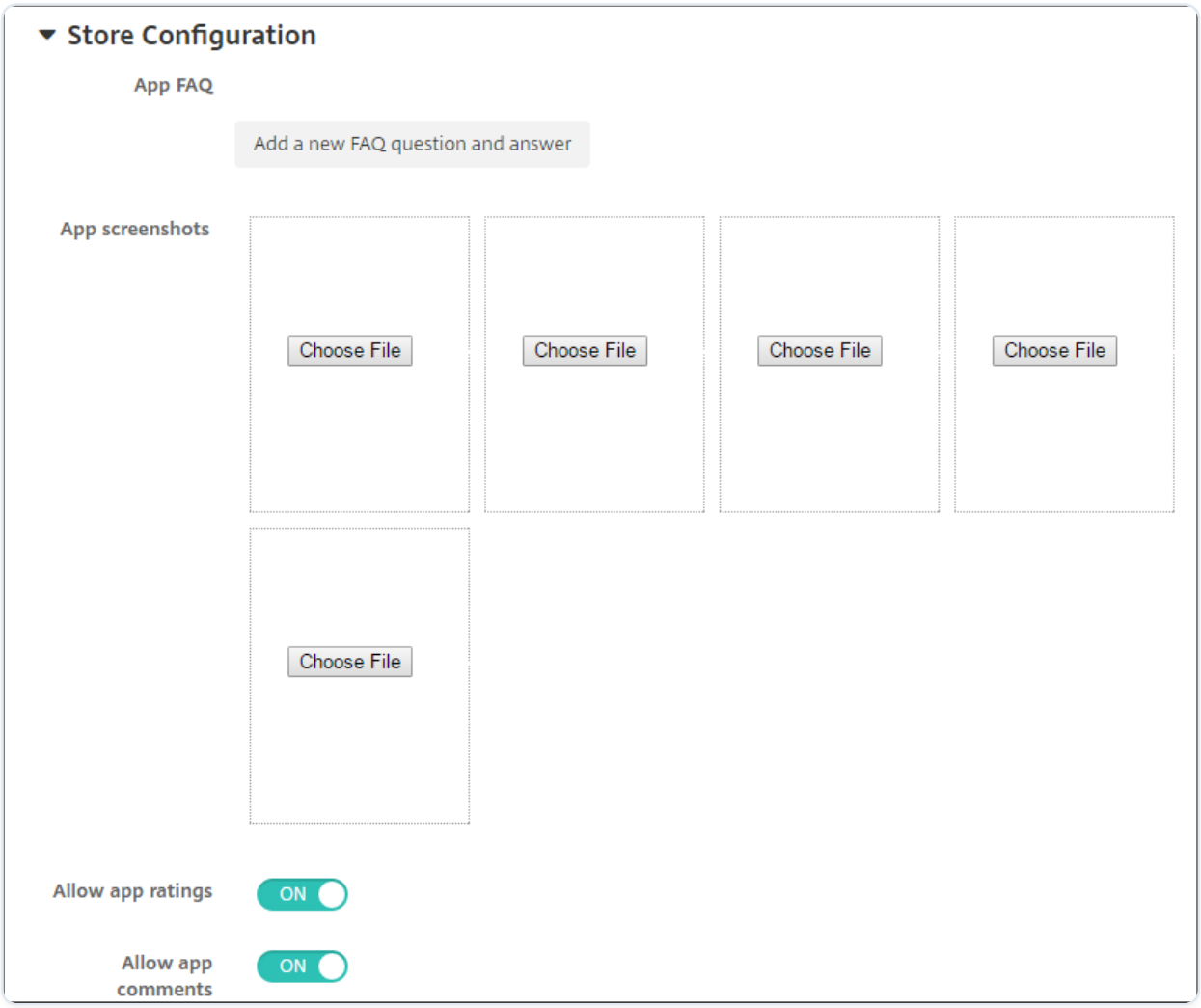
3. Cuando haya terminado, haga clic en **Agregar**. Aparece la página **Detalles**.
4. Haga clic en **Siguiente**. Aparecerá la página **Directiva de aplicaciones**.



5. Configure estos ajustes:

- **Seguridad del dispositivo**
- **Bloquear dispositivos con jailbreak o root:** Seleccione si desea bloquear el acceso a la aplicación a los dispositivos con jailbreak o root. El valor predeterminado es **Activado**.
- **Requisitos de red**
- **Se requiere WiFi:** Seleccione si se requiere una conexión Wi-Fi para ejecutar la aplicación. El valor predeterminado es **Desactivado**.
- **Se requiere red interna:** Seleccione si se requiere una red interna para ejecutar la aplicación. El valor predeterminado es **Desactivado**.
- **Redes WiFi internas:** Si ha habilitado **Se requiere Wi-Fi**, escriba la red Wi-Fi interna que desea utilizar.

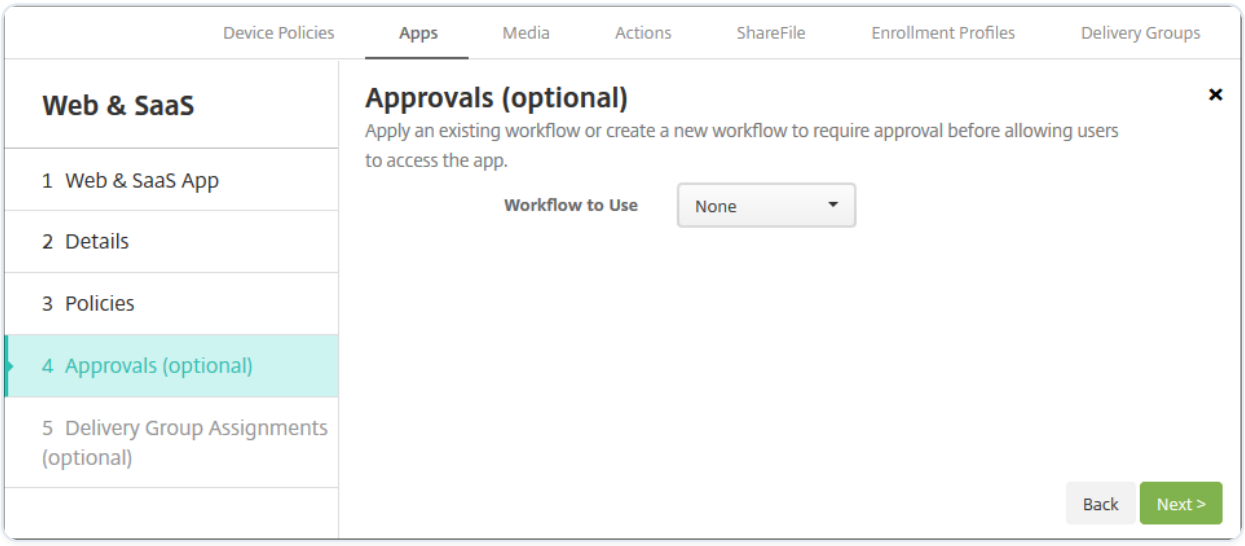
6. Expanda **Configuración de la tienda**.



Opcionalmente, puede configurar lo siguiente:

- **Preguntas frecuentes de la aplicación:** Haga clic en **Agregar una nueva pregunta y respuesta de preguntas frecuentes** para crear una sección de preguntas frecuentes para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agregue capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir valoraciones de la aplicación:** Permita que los usuarios valoren la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de la aplicación:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

7. Haga clic en **Siguiente**. Aparece la página **Aprobaciones**.



Para usar flujos de trabajo que requieran aprobación antes de permitir que los usuarios accedan a la aplicación, consulte Aplicar flujos de trabajo. Si no necesita un flujo de trabajo de aprobación, continúe con el siguiente paso.

8. Haga clic en **Siguiente**. Aparece la página **Asignación de grupos de entrega**.
9. Junto a **Elegir grupos de entrega**, escriba para buscar un grupo de entrega o seleccione uno o varios grupos. Los grupos que seleccione aparecerán en la lista **Grupos de entrega para recibir la asignación de la aplicación**.
10. Expanda **Programación de implementación** y, a continuación, configure los siguientes ajustes:

    - **Implementar:** Elija si desea implementar la aplicación en los dispositivos. El valor predeterminado es **Activado**.
    - **Programación de implementación:** Elija si desea implementar la aplicación **Ahora** o **Más tarde**. Si selecciona **Más tarde**, configure una fecha y hora para implementar la aplicación. El valor predeterminado es **Ahora**.
    - **Condición de implementación:** Elija **En cada conexión** para implementar la aplicación cada vez que el dispositivo se conecte. Elija **Solo cuando la implementación anterior haya fallado** para implementar la aplicación cuando el dispositivo no la haya recibido anteriormente. El valor predeterminado es **En cada conexión**.

    La opción **Implementar para conexión siempre activa** se aplica cuando ha configurado la clave de implementación en segundo plano de programación en **Parámetros > Propiedades del servidor**.

    La opción siempre activa:

    - No está disponible para dispositivos iOS

- No está disponible para clientes de Android y Android Enterprise que comenzaron a usar Citrix Endpoint Management con la versión 10.18.19 o posterior
- No se recomienda para clientes de Android y Android Enterprise que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19

El programa de implementación que configure es el mismo para todas las plataformas. Cualquier cambio que realice se aplica a todas las plataformas, excepto a **Implementar para conexión siempre activa**.

11. Haga clic en **Guardar**.

Agregar una aplicación empresarial

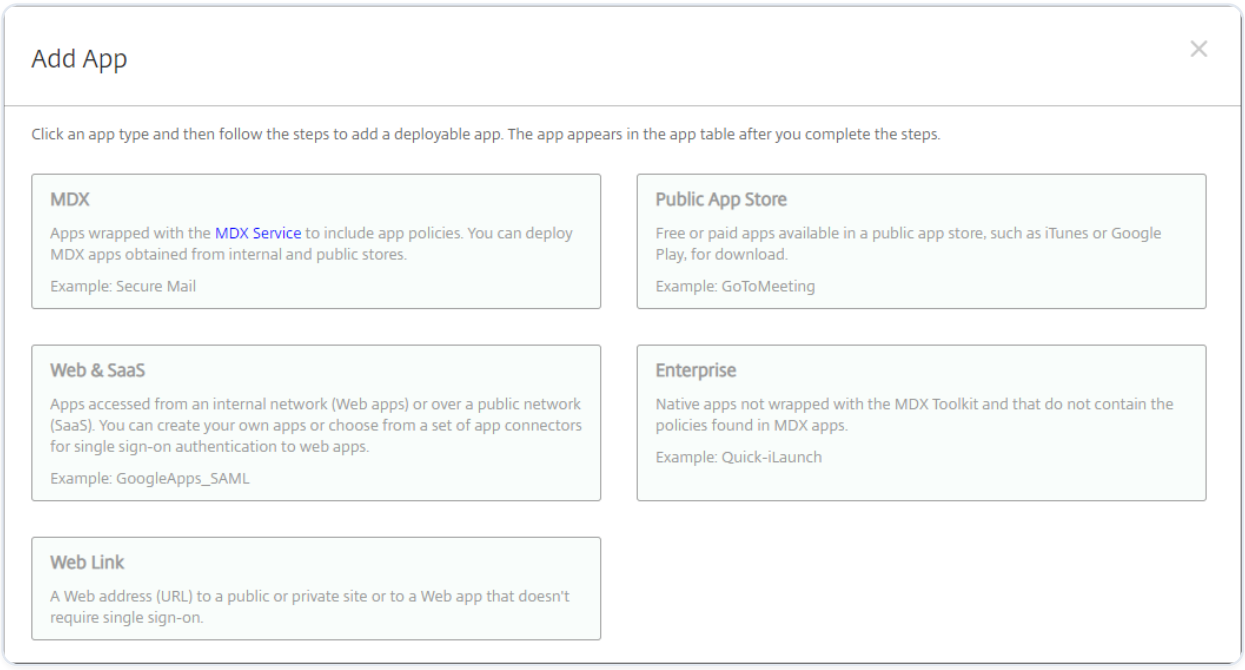
Las aplicaciones empresariales en Citrix Endpoint Management son aplicaciones privadas que usted desarrolla u obtiene de otra fuente. Excepto las aplicaciones privadas de Android Enterprise entregadas como aplicaciones habilitadas para MDX, las aplicaciones empresariales no se preparan con el SDK de MAM ni con MDX Toolkit. Puede cargar una aplicación empresarial en la ficha **Aplicaciones** de la consola de Citrix Endpoint Management. Las aplicaciones empresariales admiten las siguientes plataformas (y los tipos de archivo correspondientes):

- iOS (archivo .ipa)
- macOS (archivo .pkg)

  Citrix Endpoint Management no limita el tamaño de los archivos PKG que carga, pero sí los tiempos de carga de archivos. De forma predeterminada, debe completar la carga en 100 s. Para obtener más información, consulte Propiedades del servidor.
- Android (archivo .apk)
- Android Enterprise (archivo .apk)
- Consulte también: Agregar aplicaciones Win32 como aplicaciones empresariales
- Consulte también: Aplicaciones privadas habilitadas para MDX

No se admite agregar aplicaciones descargadas de Google Play Store como aplicaciones empresariales. En su lugar, agregue las aplicaciones de Google Play Store como aplicaciones de tienda de aplicaciones públicas. Consulte Agregar una aplicación de tienda de aplicaciones pública.

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones > Agregar**. Aparece el cuadro de diálogo **Agregar aplicación**.



2. Haga clic en **Empresarial**. Aparece la página **Información de la aplicación**.
3. En el panel **Información de la aplicación**, escriba la siguiente información:

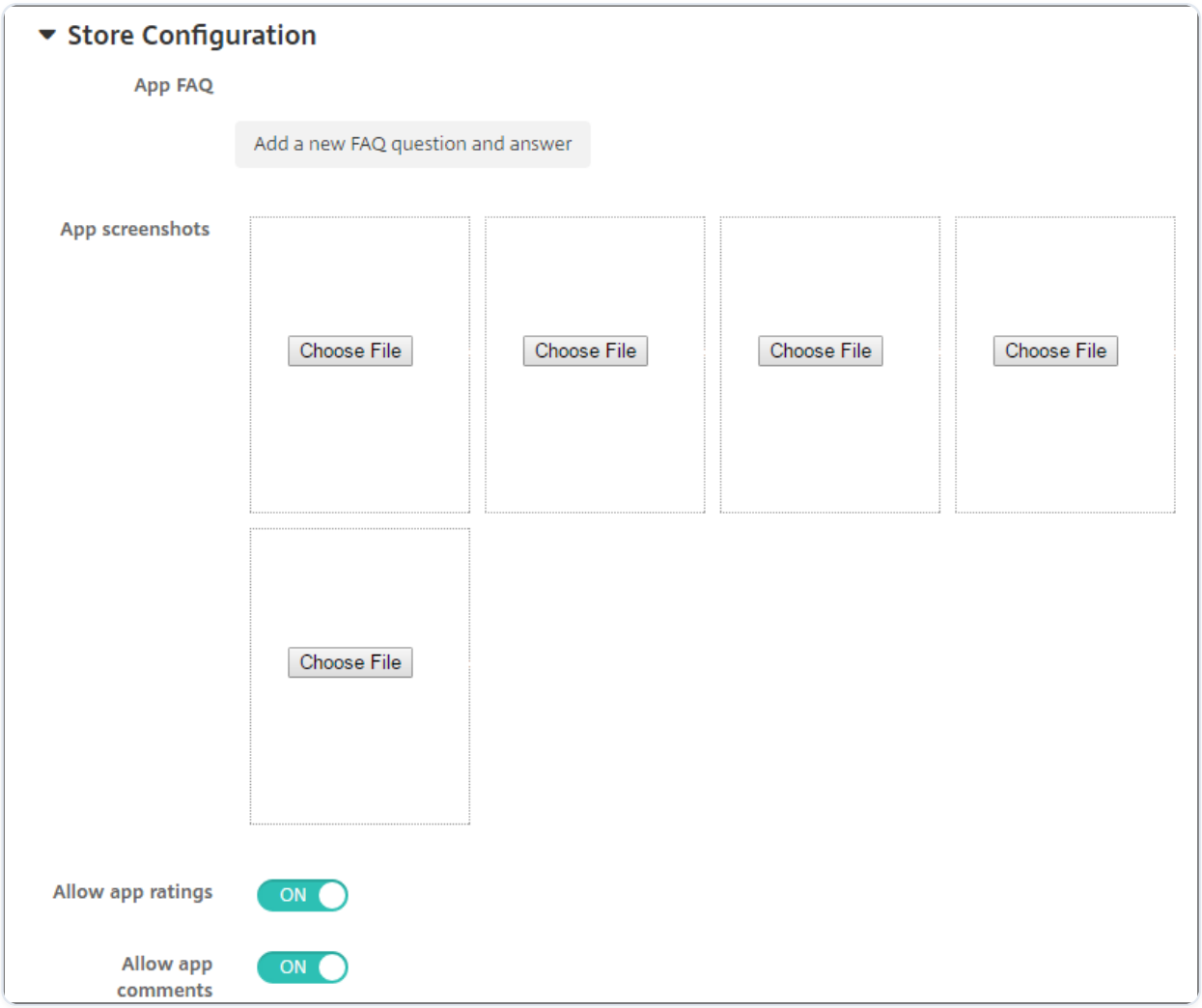
    - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre aparece en Nombre de la aplicación en la tabla Aplicaciones.
    - **Descripción:** Escriba una descripción opcional de la aplicación.
    - **Categoría de la aplicación:** Opcionalmente, en la lista, haga clic en la categoría a la que quiere añadir la aplicación. Para obtener más información sobre las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.

4. Haga clic en **Siguiente**. Aparece la página **Plataformas de aplicaciones**.
5. En **Plataformas**, seleccione las plataformas que quiere añadir. Si solo va a configurar una plataforma, desactive las demás.
6. Para cada plataforma que haya elegido, seleccione el archivo que quiere cargar haciendo clic en **Cargar** y navegando hasta la ubicación del archivo.
7. Haga clic en **Siguiente**. Aparece la página de información de la aplicación para la plataforma.
8. Configure los ajustes para el tipo de plataforma, como:

    - **Nombre de archivo:** Opcionalmente, escriba un nuevo nombre para la aplicación.
    - **Descripción de la aplicación:** Opcionalmente, escriba una nueva descripción para la aplicación.
    - **Versión de la aplicación:** No puede cambiar este campo.

- **Versión mínima del SO:** Opcionalmente, escriba la versión más antigua del sistema operativo que el dispositivo puede ejecutar para usar la aplicación.
- **Versión máxima del SO:** Opcionalmente, escriba la versión más reciente del sistema operativo que el dispositivo debe ejecutar para usar la aplicación.
- **Dispositivos excluidos:** Opcionalmente, escriba el fabricante o los modelos de dispositivos que no pueden ejecutar la aplicación.
- **ID de paquete:** Identificador único de su aplicación.
- **Eliminar aplicación si se elimina el perfil MDM:** Seleccione si desea eliminar la aplicación de un dispositivo cuando se elimine el perfil MDM. El valor predeterminado es **Activado**. Esta configuración no se aplica a macOS.
- **Impedir la copia de seguridad de datos de la aplicación:** Seleccione si desea impedir que la aplicación haga una copia de seguridad de los datos. El valor predeterminado es **Activado**. Esta configuración no se aplica a macOS.
- **Forzar la administración de la aplicación:** Seleccione si desea instalar una aplicación como aplicación administrada en dispositivos no supervisados. El tipo de dispositivo determina cómo Citrix Endpoint Management procesa esta configuración cuando está habilitada. Si habilita esta configuración, la aplicación se actualiza sin pedir confirmación al usuario. La actualización se produce tanto si la aplicación es obligatoria como opcional. El valor predeterminado es **Desactivado**.
    - En el caso de los dispositivos iOS, si la aplicación ya estaba instalada, los usuarios reciben un mensaje para permitir que la aplicación se administre. Si implementa una aplicación en dispositivos donde la aplicación no existe, la aplicación se instala como una aplicación administrada, independientemente del estado de esta configuración. Disponible en iOS 9.0 y versiones posteriores. Para los dispositivos iOS inscritos mediante la inscripción de usuarios, Citrix Endpoint Management no aplica esta configuración y no solicita a los usuarios que permitan la administración de aplicaciones.
    - Para dispositivos macOS, habilite la configuración y, a continuación, implemente la aplicación en los dispositivos. La aplicación se instala automáticamente como una aplicación administrada. Los usuarios no reciben ninguna solicitud. Si implementa una aplicación en dispositivos donde la aplicación no existe, la aplicación se instala como una aplicación administrada, independientemente del estado de esta configuración. Disponible en macOS 11.0 y versiones posteriores.

9. Configure las reglas de implementación. Para obtener más información, consulte Configurar reglas de implementación.
10. Expanda **Configuración de la tienda**.



Opcionalmente, puede configurar lo siguiente:

- **Preguntas frecuentes de la aplicación:** Haga clic en **Agregar una nueva pregunta y respuesta de preguntas frecuentes** para crear una sección de preguntas frecuentes para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agregue capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir valoraciones de la aplicación:** Permita a los usuarios valorar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de la aplicación:** Permita a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

11. Haga clic en **Siguiente**. Aparece la página **Aprobaciones**.

Para usar flujos de trabajo que requieran aprobación antes de permitir a los usuarios acceder a la aplicación, consulte Aplicar flujos de trabajo. Si no necesita un flujo de trabajo de aprobación, continúe con el siguiente paso.

12. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.
13. Junto a **Elegir grupos de entrega**, escriba para buscar un grupo de entrega o seleccione uno o varios grupos de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega para recibir la asignación de aplicaciones**.
14. Expanda **Programación de implementación** y, a continuación, configure los siguientes ajustes:

    - **Implementar:** Elija si desea implementar la aplicación en los dispositivos. El valor predeterminado es **Activado**.
    - **Programación de implementación:** Elija si desea implementar la aplicación **Ahora** o **Más tarde**. Si selecciona **Más tarde**, configure una fecha y hora para implementar la aplicación. El valor predeterminado es **Ahora**.
    - **Condición de implementación:** Elija **En cada conexión** para implementar la aplicación cada vez que el dispositivo se conecte. Elija **Solo cuando la implementación anterior haya fallado** para implementar la aplicación cuando el dispositivo no la haya recibido anteriormente. El valor predeterminado es **En cada conexión**.

    La opción **Implementar para conexión siempre activa** se aplica cuando ha configurado la clave de programación de implementación en segundo plano en **Configuración > Propiedades del servidor**.

    La opción siempre activa:

    - No está disponible para dispositivos iOS
    - No está disponible para clientes de Android y Android Enterprise que comenzaron a usar Citrix Endpoint Management con la versión 10.18.19 o posterior
    - No se recomienda para clientes de Android y Android Enterprise que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19

    La programación de implementación que configure es la misma para todas las plataformas. Cualquier cambio que realice se aplica a todas las plataformas, excepto a **Implementar para conexión siempre activa**.
15. Haga clic en **Guardar**.

Agregar aplicaciones Win32 como aplicaciones empresariales

Puede cargar archivos MSI, APPX, AppxBundle, PS1 o EXE para aplicaciones Win32 en Citrix Endpoint Management para su implementación en dispositivos de escritorio y tabletas Windows 10 y Windows 11 administrados. Después de usar Citrix Endpoint Management para implementar los archivos, el dispositivo Windows instala la aplicación de la siguiente manera:

- Si la aplicación actualizada elimina la versión anterior durante la instalación, el dispositivo incluye solo la aplicación actualizada.
- Si la aplicación actualizada no puede eliminar la versión anterior, pero la nueva versión se puede instalar, el dispositivo incluye ambas versiones de la aplicación. Citrix Endpoint Management ya no tiene la información de la versión anterior.
- Si la aplicación actualizada no se puede instalar cuando existe una versión anterior, la nueva aplicación no se instala. En ese caso, primero implemente la directiva de dispositivo de desinstalación de aplicaciones para eliminar la versión anterior. Luego, implemente la nueva versión.

Requisitos

- Windows 10 (versión 1607 o posterior) o Windows 11
- Windows 10 Professional o Windows 11 Professional
- Windows 10 Enterprise o Windows 11 Enterprise
- Aplicaciones MSI Win32 independientes instaladas con la opción /quiet. Para este caso de uso de implementación, Microsoft no admite MSI con más de una aplicación, MSI anidados o instalación interactiva.

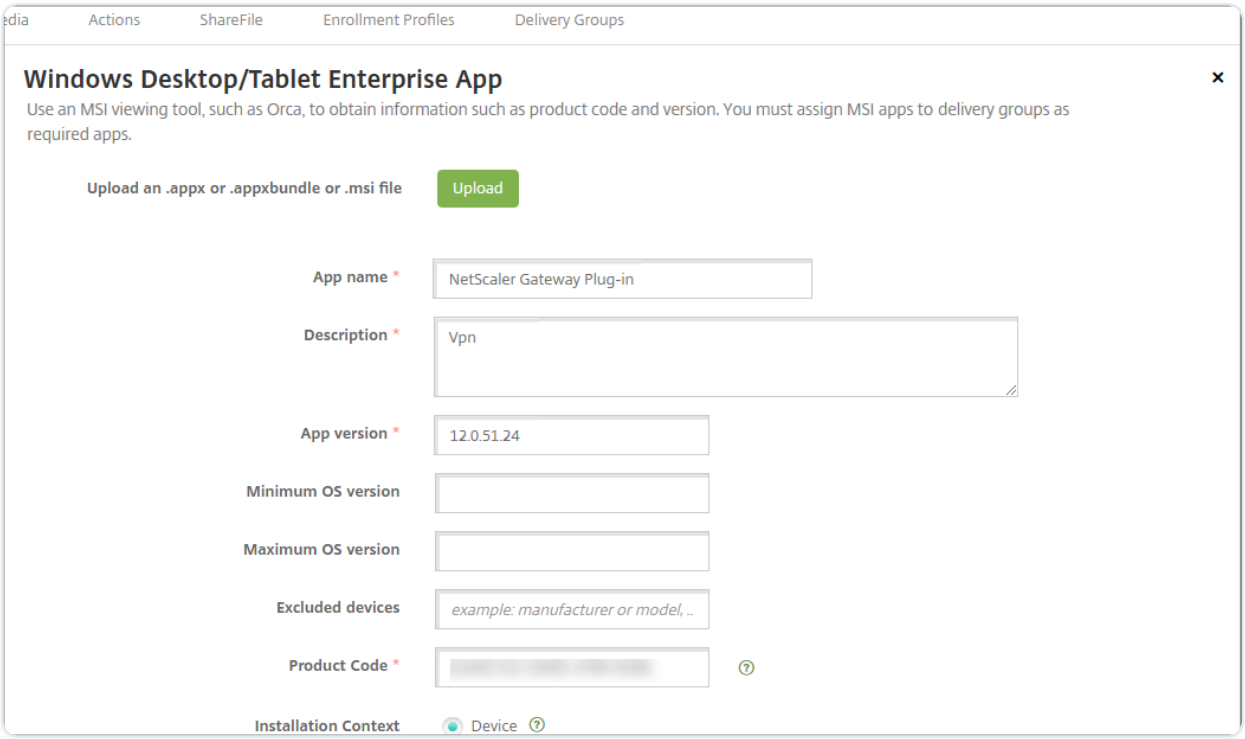
Buscar metadatos

Cuando agregue una aplicación Win32 a Citrix Endpoint Management, especifique los metadatos de la aplicación. Para buscar los metadatos, use la aplicación Orca en un equipo Windows y anote la siguiente información:

- Código de producto
- Nombre del producto
- Versión del producto
- Tipo de instalación del paquete, ya sea por usuario o por máquina

Añadir una aplicación Win32 a Citrix Endpoint Management

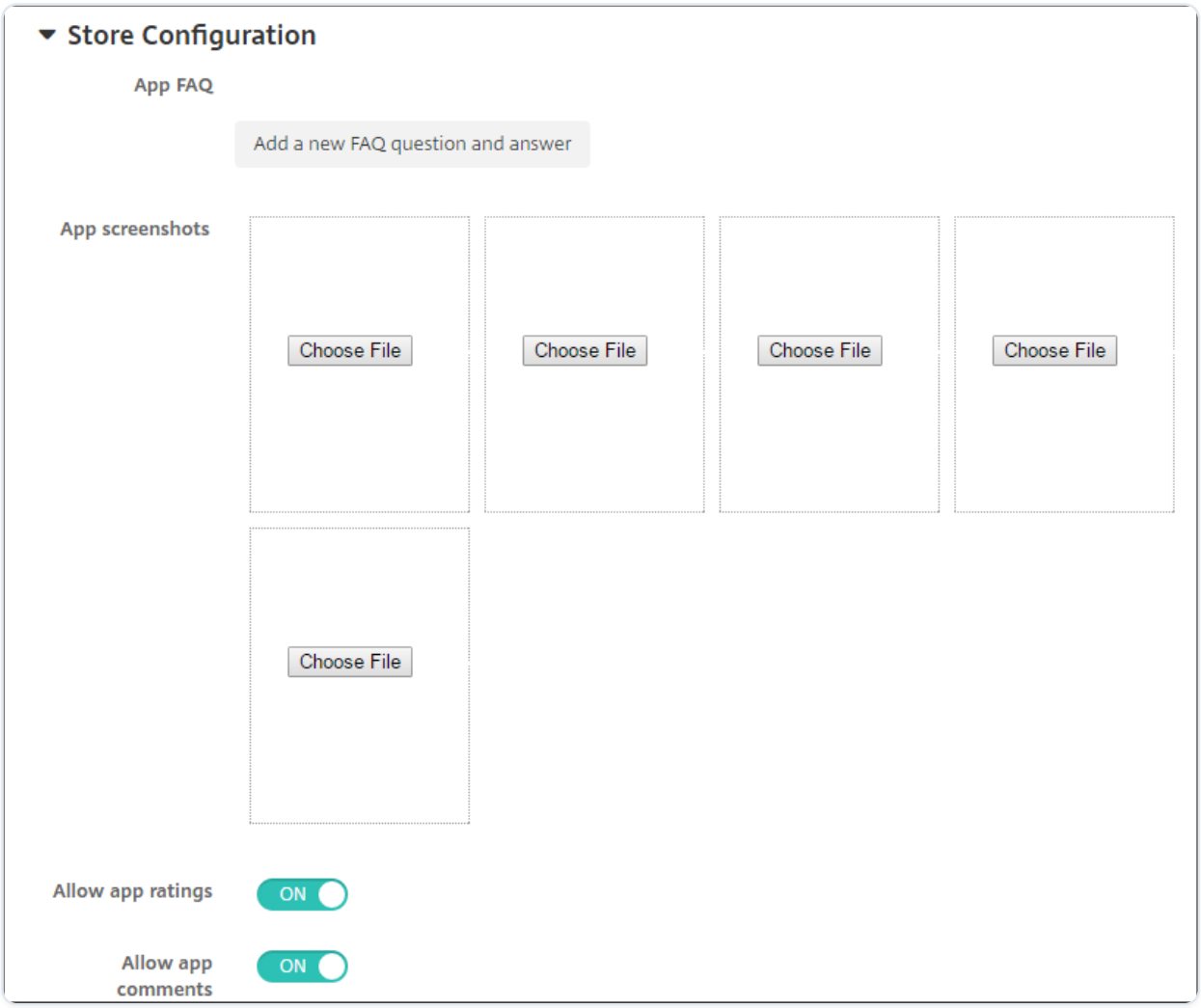
1. Vaya a **Configurar > Aplicaciones**, haga clic en **Empresa** y escriba un nombre para la aplicación en la página **Información de la aplicación**.
2. Desactive todas las casillas de verificación de Plataforma, excepto **Escritorio/Tableta Windows**.
3. En la página **Aplicación empresarial de escritorio/tableta Windows**, haga clic en **Cargar** y navegue hasta el archivo.
4. Configure estos ajustes:



- **Nombre de la aplicación:** El nombre de la aplicación, de los metadatos de la aplicación.
- **Descripción:** Una descripción para la aplicación.
- **Versión de la aplicación:** El número de versión de la aplicación, de los metadatos de la aplicación.
- **Versión mínima del SO:** Opcional. La versión más antigua del sistema operativo que el dispositivo puede ejecutar para usar la aplicación.
- **Versión máxima del SO:** Opcional. El sistema operativo más reciente que el dispositivo debe ejecutar para usar la aplicación.
- **Dispositivos excluidos:** Opcional. El fabricante o los modelos de dispositivos que no pueden ejecutar la aplicación.

- **Código de producto:** El código de producto de la aplicación MSI, en formato UUID, de los metadatos de la aplicación.
- **Contexto de instalación:** Según los metadatos de la aplicación, seleccione si la aplicación se instalará para el dispositivo o para el usuario. Esta configuración no está disponible para archivos EXE.
- **Línea de comandos:** Las opciones de línea de comandos que se usarán al llamar a MSIEXEC.exe
- **Línea de comandos de instalación:** Añada argumentos de línea de comandos para instalar archivos EXE de forma silenciosa.
- **Línea de comandos de desinstalación:** Añada argumentos de línea de comandos para desinstalar archivos EXE de forma silenciosa.
- **Número de reintentos:** El número de veces que puede reintentar una operación de descarga e instalación antes de marcar la instalación como fallida.
- **Tiempo de espera:** El número de minutos que se ejecuta el proceso de instalación antes de que el instalador interprete la instalación como fallida y deje de supervisar el proceso.
- **Intervalo de reintentos:** El número de minutos entre operaciones de reintento.

5. Configure las reglas de implementación. Para obtener más información, consulte Configurar reglas de implementación.
6. Expanda **Configuración de la tienda**.



Opcionalmente, puede configurar lo siguiente:

- **Preguntas frecuentes de la aplicación:** Haga clic en **Agregar una nueva pregunta y respuesta de preguntas frecuentes** para crear unas preguntas frecuentes para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agregue capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir valoraciones de la aplicación:** Permita a los usuarios valorar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de la aplicación:** Permita a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

7. Haga clic en **Siguiente** hasta llegar a la página **Resumen** y, a continuación, haga clic en **Guardar**.
8. Vaya a **Configurar > Grupos de entrega** y agregue la aplicación Win32 como una aplicación obligatoria.
9. Después de implementar la aplicación, informe a los usuarios que la aplicación está disponible.

Actualizar una aplicación Win32

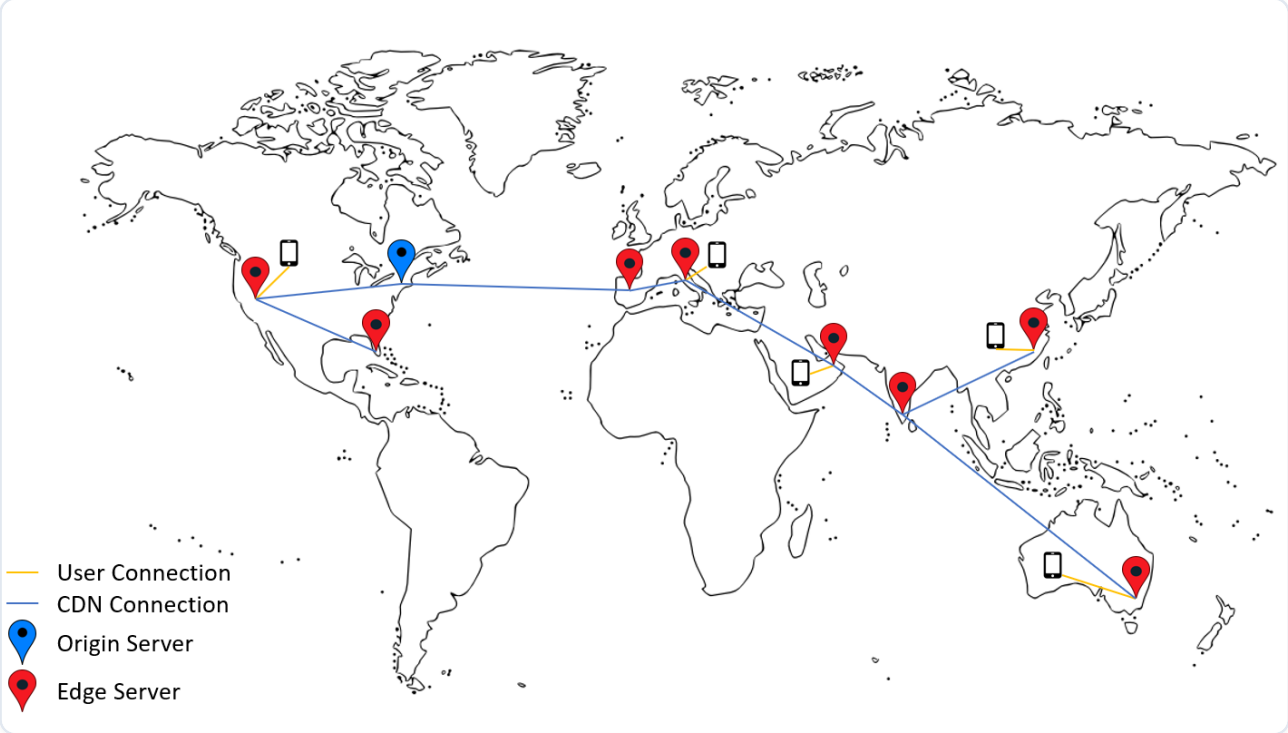
1. Busque los metadatos de la aplicación, como se describió anteriormente en "Buscar metadatos".
2. Vaya a **Configurar > Aplicaciones** para cargar la nueva versión de la aplicación. Actualice la **Versión de la aplicación**. Si la nueva versión de la aplicación tiene un **Código de producto** diferente, actualice esa configuración.
3. Envíe los cambios e implemente la aplicación.

Distribuir aplicaciones empresariales y MDX desde la CDN de Citrix

Puede distribuir aplicaciones empresariales y MDX desde la red de entrega de contenido (CDN) de Citrix. Una CDN se refiere a un grupo de servidores distribuidos geográficamente que trabajan juntos para proporcionar de forma segura una entrega rápida del contenido de la aplicación. Un servidor local entrega las aplicaciones a los dispositivos móviles.

Una CDN mejora los tiempos de descarga de aplicaciones al distribuir el contenido geográficamente más cerca de los dispositivos móviles a través de un punto de distribución de CDN cercano. La CDN entrega las aplicaciones desde la ubicación de punto de presencia (POP) más cercana a un usuario.

El siguiente diagrama muestra un ejemplo de cómo la CDN distribuye las aplicaciones al servidor perimetral más cercano a los usuarios de dispositivos móviles. Un servidor perimetral almacena en caché el contenido del servidor de origen cuando los dispositivos móviles solicitan aplicaciones.



Los usuarios pueden conectarse a las aplicaciones mediante Citrix Secure Hub. Al agregar una aplicación, Citrix Endpoint Management crea el conector de la aplicación para ella.

La compatibilidad de la CDN de Citrix con aplicaciones empresariales está disponible para las siguientes plataformas:

- iOS (inscripción MDM o MAM)
- Android (inscripción MDM o MAM)
- Escritorio o tableta Windows (inscripción MDM)
- macOS (inscripción MDM)

La compatibilidad de Citrix CDN con las aplicaciones MDX está disponible para las siguientes plataformas:

- iOS (inscripción MDM o MAM)
- Android (inscripción MDM o MAM)

Cómo funciona CDN

En el núcleo del servicio CDN, los servidores están vinculados entre sí con el objetivo de entregar las aplicaciones más rápido. Ese objetivo se logra colocando las aplicaciones de forma segura en diferentes puntos de distribución en todo el mundo. El servidor DNS de los dispositivos móviles utilizado durante la conexión inicial al servidor de Citrix Endpoint Management es lo que determina el punto de distribución.

Por ejemplo: Supongamos que la IP del servidor DNS del dispositivo móvil se origina en Fort Lauderdale, Florida. La CDN utiliza un punto de distribución local más cercano a esa ubicación para entregar la aplicación al dispositivo móvil. Ese uso de la CDN se traduce en una mejora del tiempo de descarga de la aplicación.

Cuando un dispositivo móvil solicita o envía por primera vez una aplicación empresarial, Citrix Endpoint Management copia la aplicación al punto de distribución local y la mantiene allí durante 24 horas para otras descargas de dispositivos locales.

Entregar aplicaciones empresariales desde Citrix CDN

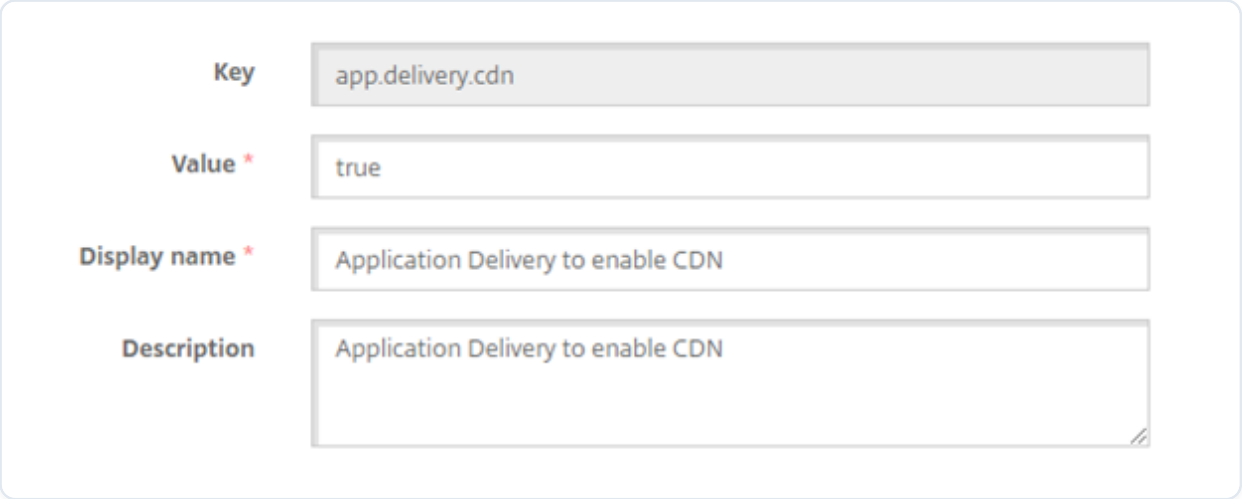
Con la versión 19.4.1 de Citrix Endpoint Management, la entrega de aplicaciones empresariales se establece de forma predeterminada en la entrega por CDN para todos los nuevos clientes de multitenencia. Para los clientes existentes antes de esta versión, siga las instrucciones de esta sección.

Para las aplicaciones empresariales que ya están en el servidor de Citrix Endpoint Management, Citrix Endpoint Management sigue entregando esas aplicaciones desde el servidor hasta que esas aplicaciones se vuelvan a cargar después de completar los siguientes pasos.

> **Importante:**

> Solo los administradores de Citrix Cloud pueden habilitar CDN para una cuenta. La propiedad de servidor `app.delivery.cdn` solo es visible en Citrix Endpoint Management cuando inicia sesión como administrador de Citrix Cloud. Para obtener información sobre los administradores de Citrix Cloud, consulte Administrar administradores de Citrix Cloud.

1. Habilite CDN para su cuenta: En la consola de Citrix Endpoint Management: Vaya a **Parámetros > Propiedades del servidor**.
2. Busque `app.delivery.cdn` y, a continuación, haga clic en **Modificar**.
3. Cambie el valor a **true**.



4. En la consola de Citrix Endpoint Management, vuelva a cargar sus aplicaciones empresariales:

   a. Vaya a **Configurar > Aplicaciones** y filtre la lista de aplicaciones por **Tipo** (**Empresarial**) y **Plataforma**.

   b. Seleccione una aplicación, haga clic en **Modificar**, haga clic en **Siguiente** y haga clic en **Cargar**.

   c. Repita el paso anterior para cada aplicación empresarial.

Entregar aplicaciones MDX desde la CDN de Citrix

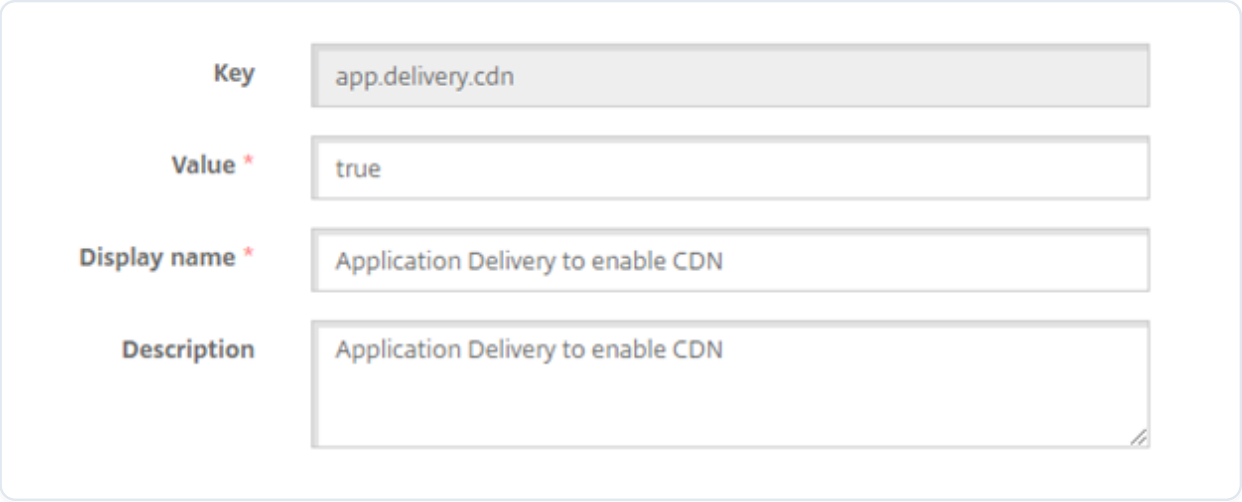
Con la versión 20.12.0 de Citrix Endpoint Management, la entrega de aplicaciones MDX se establece de forma predeterminada en la entrega de CDN para todos los nuevos clientes de multitenencia. Para los clientes existentes antes de esta versión, siga las instrucciones de esta sección.

Para las aplicaciones MDX que ya están en el servidor de Citrix Endpoint Management, Citrix Endpoint Management sigue entregando esas aplicaciones desde el servidor hasta que esas aplicaciones se vuelvan a cargar después de completar los siguientes pasos.

> **Importante:**
>
> Solo los administradores de Citrix Cloud pueden habilitar la CDN para una cuenta. La propiedad de servidor `app.delivery.cdn` es visible en Citrix Endpoint Management solo cuando inicia sesión como administrador de Citrix Cloud. Para obtener información sobre los administradores de Citrix Cloud, consulte Administrar administradores de Citrix Cloud.

1. Habilite la CDN para su cuenta: En la consola de Citrix Endpoint Management: Vaya a **Parámetros > Propiedades del servidor**.

2. Busque `app.delivery.cdn` y, a continuación, haga clic en **Modificar**.
3. Cambie el valor a **true**.



4. En la consola de Citrix Endpoint Management, cargue sus aplicaciones MDX de nuevo:
   a. Vaya a **Configurar > Aplicaciones** y filtre la lista de aplicaciones por **Tipo** (**MDX**) y **Plataforma**.
   b. Seleccione una aplicación, haga clic en **Editar**, haga clic en **Siguiente** y haga clic en **Cargar**.
   c. Repita el paso anterior para cada aplicación MDX.

Agregar un enlace web

Un enlace web es una dirección web a un sitio de Internet o intranet. Un enlace web también puede apuntar a una aplicación web que no requiere SSO. Una vez que termine de configurar un enlace web, este aparecerá como un icono en la tienda de aplicaciones. Cuando los usuarios inician sesión con Citrix Secure Hub, el enlace aparece con la lista de aplicaciones y escritorios disponibles.

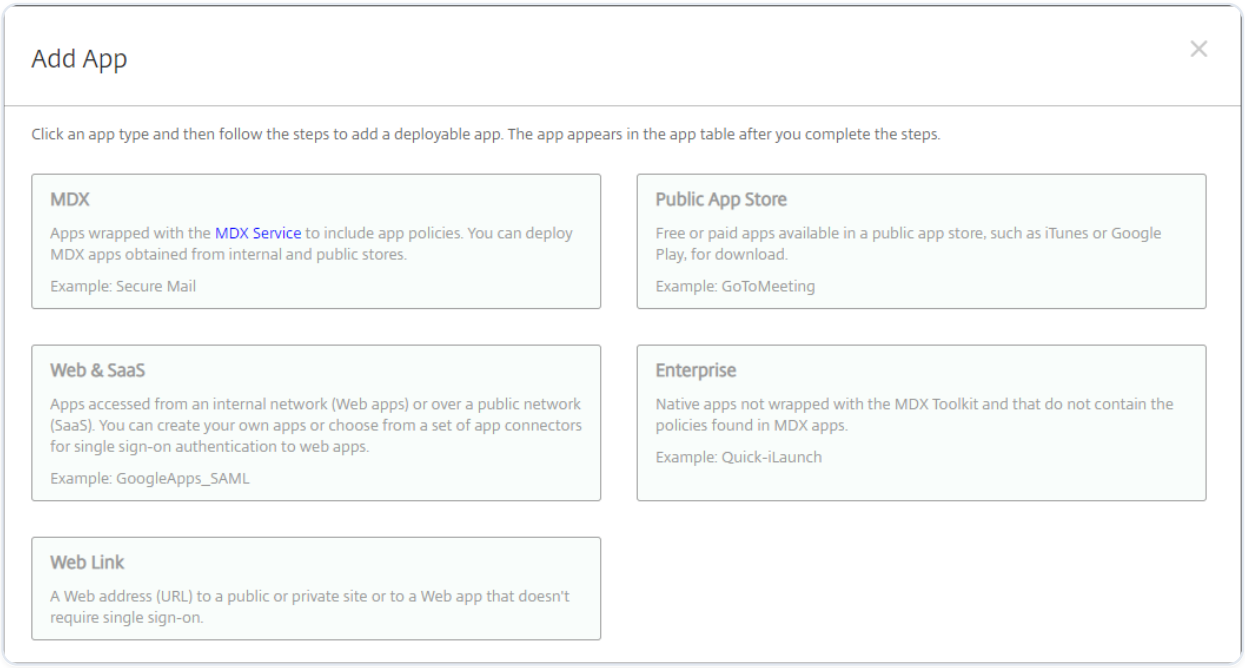
Puede configurar enlaces web desde la ficha **Aplicaciones** de la consola de Citrix Endpoint Management. Cuando termine de configurar el enlace web, este aparecerá como un icono de enlace en la lista de la tabla **Aplicaciones**. Cuando los usuarios inician sesión con Citrix Secure Hub, el enlace aparece con la lista de aplicaciones y escritorios disponibles.

Vea este vídeo para obtener más información:

Para agregar el enlace, proporcione la siguiente información:

- Nombre del enlace
- Descripción del enlace
- Dirección web (URL)
- Categoría
- Rol
- Imagen en formato .png (opcional)

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones > Agregar**. Aparece el cuadro de diálogo **Agregar aplicación**.

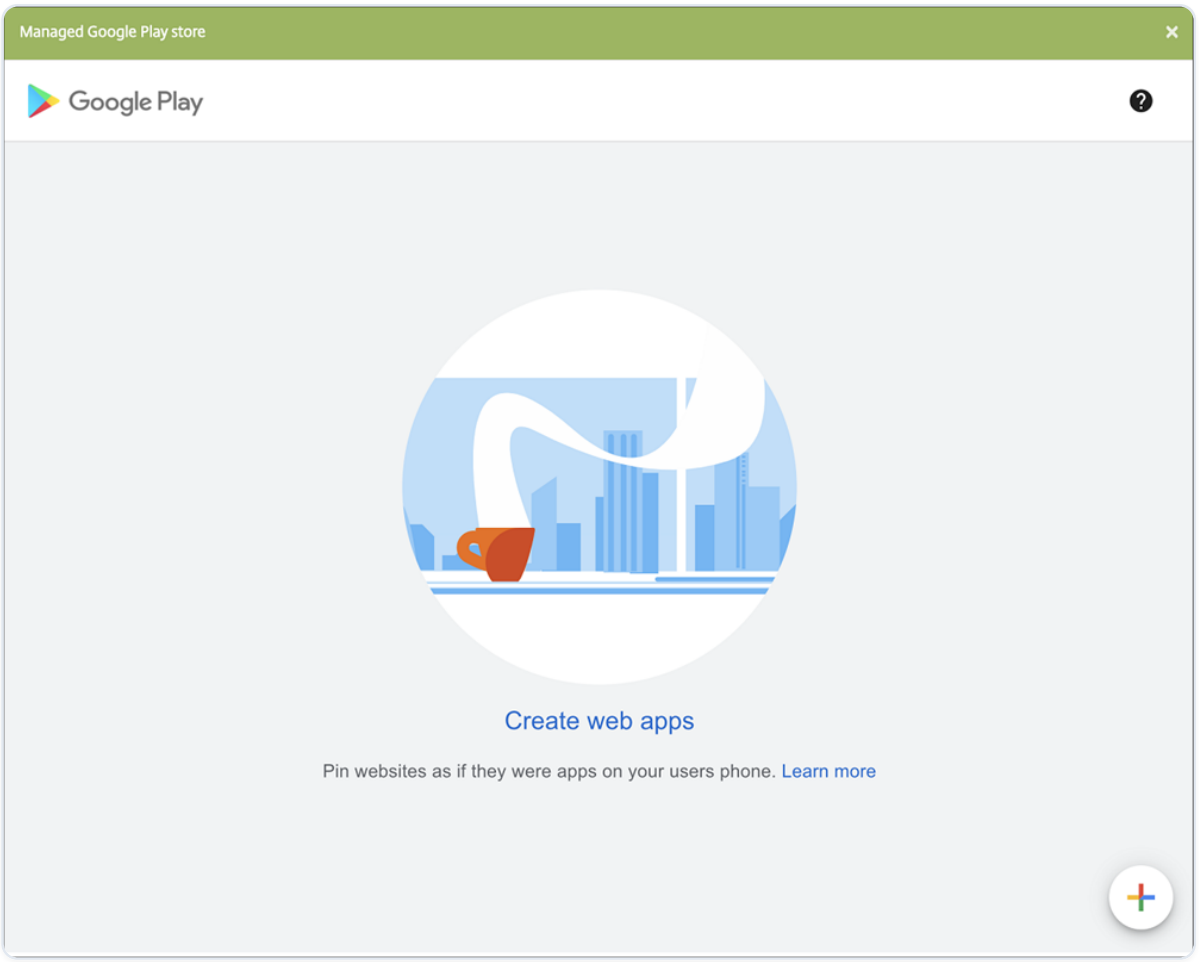


2. Haga clic en **Enlace web**. Aparece la página **Información de la aplicación**.
3. En el panel **Información de la aplicación**, escriba la siguiente información:

    - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre aparece en la tabla Aplicaciones, en Nombre de la aplicación.
    - **Descripción:** Escriba una descripción opcional de la aplicación.
    - **Categoría de aplicación:** Opcionalmente, en la lista, haga clic en la categoría a la que quiere agregar la aplicación. Para obtener más información sobre las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.

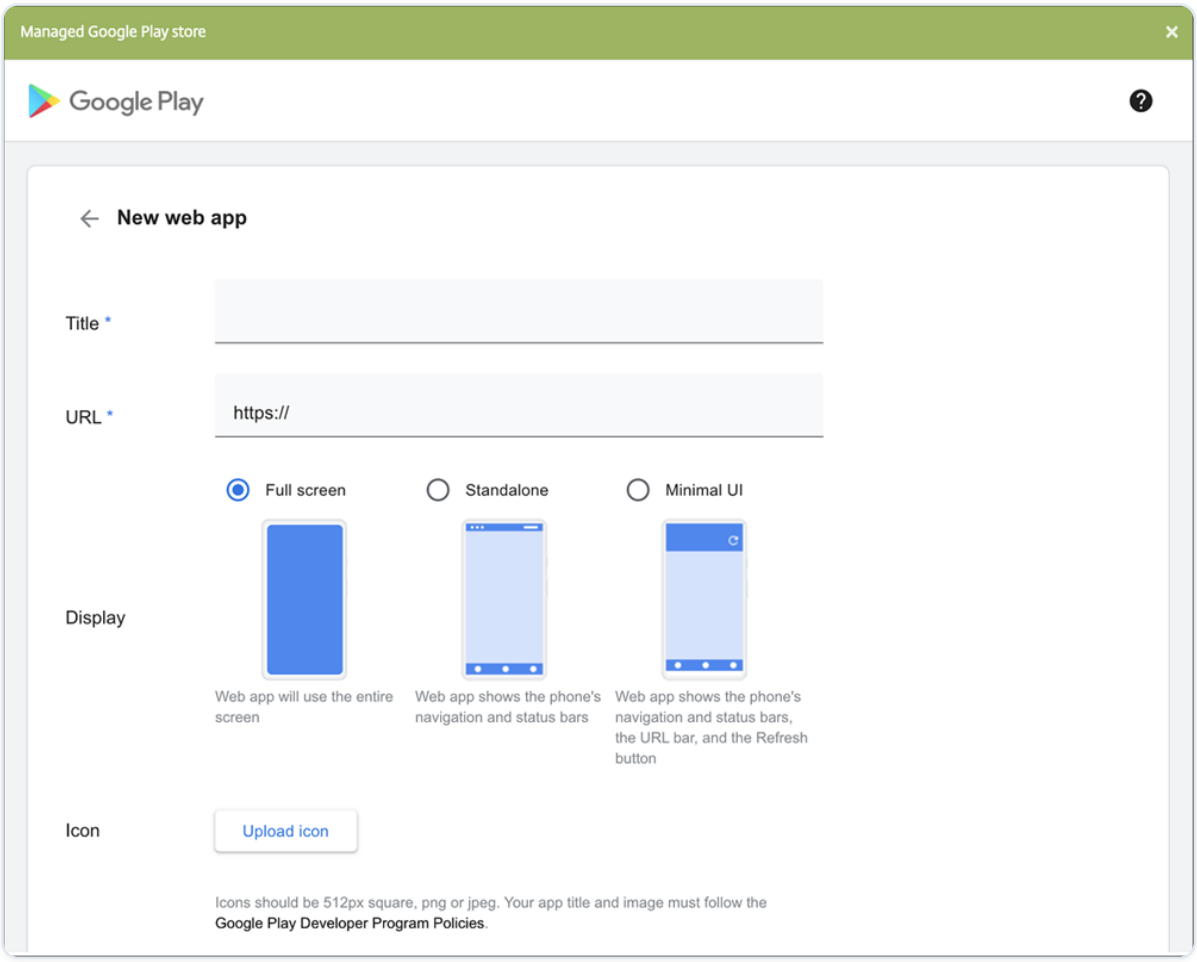
4. Haga clic en **Siguiente**. Aparece la página **Plataformas de aplicaciones**.
5. En **Plataformas**, seleccione **Otras plataformas** para agregar una aplicación web para iOS, Android (DA heredado) y Windows 8, o seleccione **Android Enterprise**. Desactive la casilla de verificación de las plataformas que no quiera incluir.

- Si selecciona **Otras plataformas**, continúe con el siguiente paso para configurar los ajustes.
- Si selecciona **Android Enterprise**, haga clic en el botón **Cargar** para abrir la tienda administrada de Google Play. No es necesario registrarse para obtener una cuenta de desarrollador para publicar una aplicación web. Haga clic en el icono **Más** en la esquina inferior derecha para continuar.



Configure estos ajustes:

  - **Título:** Escriba el nombre de la aplicación web.
  - **URL:** Escriba la dirección web de la aplicación.
  - **Visualización:** Elija cómo mostrar la aplicación web en los dispositivos de los usuarios. Las opciones disponibles son **Pantalla completa**, **Independiente** y **Interfaz de usuario mínima**.
  - **Icono:** Cargue su propia imagen para la aplicación web.



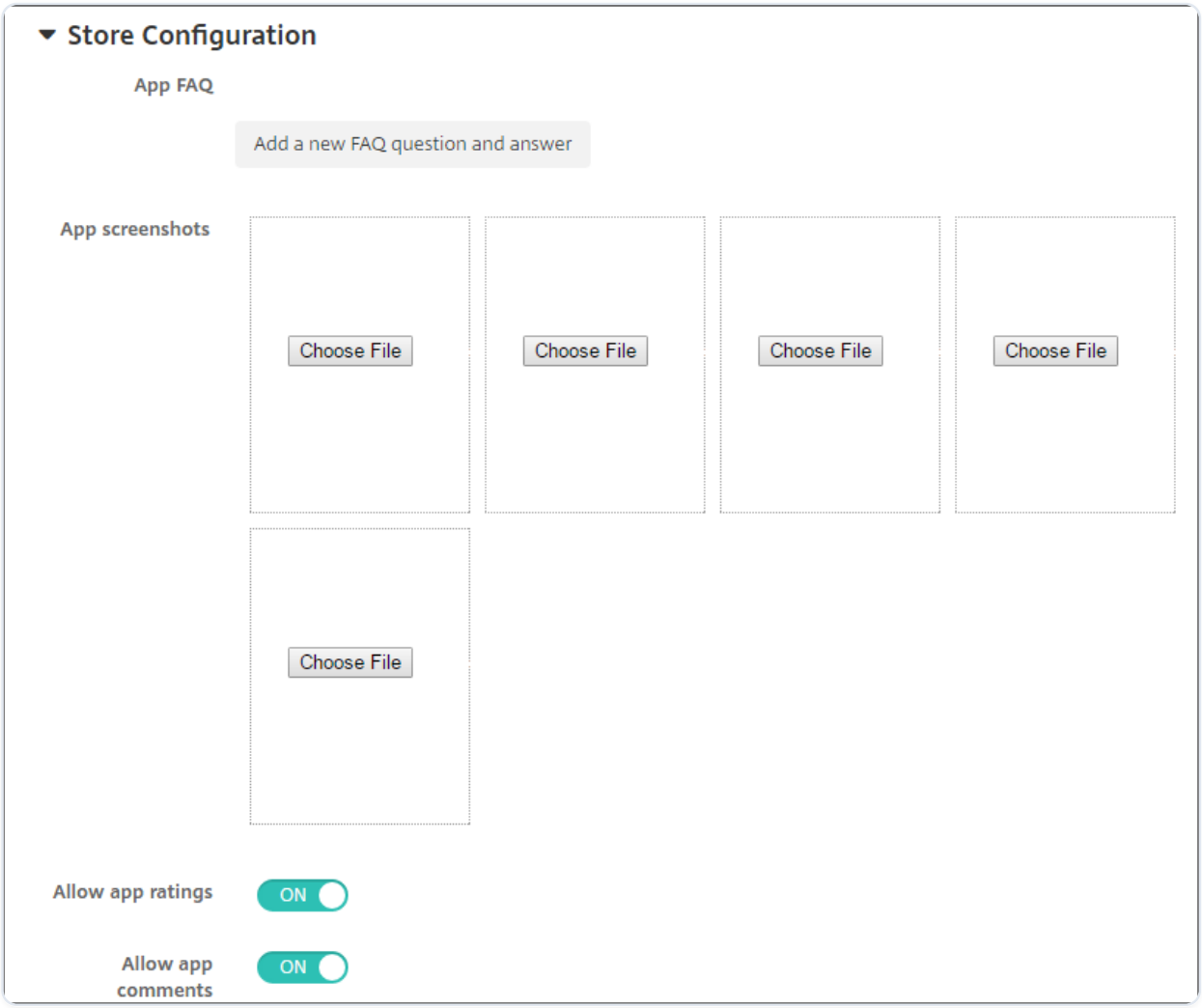
Cuando termine, haga clic en **Crear**. La publicación de la aplicación web puede tardar hasta 10 minutos.

6. Para plataformas que no sean Android Enterprise, configure estos ajustes:

   - **Nombre de la aplicación:** Acepte el nombre rellenado previamente o escriba uno nuevo.
   - **Descripción de la aplicación:** Acepte la descripción rellenada previamente o escriba una propia.
   - **URL:** Acepte la URL rellenada previamente o escriba la dirección web de la aplicación. Dependiendo del conector que elija, este campo puede tener un marcador de posición que debe reemplazar antes de poder pasar a la página siguiente.
   - **La aplicación está alojada en la red interna:** Seleccione si la aplicación se ejecuta en un servidor de su red interna. Si los usuarios se conectan desde una ubicación remota a la aplicación interna, deben conectarse a través de NetScaler Gateway. Al establecer esta opción en **Activado**, se añade la palabra clave VPN a la aplicación y se permite a los usuarios conectarse a través de NetScaler Gateway. El valor predeterminado es **Desactivado**.
   - **Categoría de la aplicación:** Haga clic en una categoría opcional de la lista desplegable para aplicarla a la aplicación.

- **Imagen:** Seleccione si desea usar la imagen predeterminada de Citrix o cargar su propia imagen de aplicación. El valor predeterminado es Usar predeterminada.
  - Para cargar su propia imagen, haga clic en **Examinar** y vaya a la ubicación del archivo. El archivo debe ser un archivo .PNG. No puede cargar un archivo JPEG o GIF. Cuando añade un gráfico personalizado, no puede cambiarlo más tarde.

7. Configure las reglas de implementación. Para obtener más información, consulte Configurar reglas de implementación.
8. Expanda **Configuración de la tienda**.



Opcionalmente, puede configurar lo siguiente:

- **Preguntas frecuentes de la aplicación:** Haga clic en **Agregar una nueva pregunta y respuesta de preguntas frecuentes** para crear preguntas frecuentes para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agregue capturas de pantalla que aparecen en la tienda de aplicaciones.

- **Permitir valoraciones de la aplicación:** Permitir que los usuarios valoren la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de la aplicación:** Permitir que los usuarios dejen comentarios sobre la aplicación en la tienda de aplicaciones.

9. Haga clic en **Siguiente**. Aparece la página **Asignación de grupos de entrega**.
10. Junto a **Elegir grupos de entrega**, escriba para buscar un grupo de entrega o seleccione uno o varios grupos de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega para recibir la asignación de aplicaciones**.
11. Expanda **Programación de implementación** y, a continuación, configure los siguientes parámetros:

    - **Implementar:** Elija si quiere implementar la aplicación en los dispositivos. El valor predeterminado es **Activado**.
    - **Programación de implementación:** Elija si quiere implementar la aplicación **Ahora** o **Más tarde**. Si selecciona **Más tarde**, configure una fecha y hora para implementar la aplicación. El valor predeterminado es **Ahora**.
    - **Condición de implementación:** Elija **En cada conexión** para implementar la aplicación cada vez que el dispositivo se conecte. Elija **Solo cuando la implementación anterior haya fallado** para implementar la aplicación cuando el dispositivo no haya podido recibirla anteriormente. El valor predeterminado es **En cada conexión**.

    La opción **Implementar para conexión siempre activa** se aplica cuando ha configurado la clave de implementación en segundo plano de programación en **Parámetros > Propiedades del servidor**.

    La opción siempre activa:

    - No está disponible para dispositivos iOS
    - No está disponible para clientes de Android y Android Enterprise que comenzaron a usar Citrix Endpoint Management con la versión 10.18.19 o posterior.
    - No se recomienda para clientes de Android y Android Enterprise que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19.

    El programa de implementación que configure es el mismo para todas las plataformas. Cualquier cambio que realice se aplica a todas las plataformas, excepto a **Implementar para conexión siempre activa**.
12. Haga clic en **Guardar**.

Habilitar aplicaciones de Microsoft 365

Puede abrir el contenedor MDX para permitir que Citrix Secure Mail, Citrix Secure Web y Citrix Files transfieran documentos y datos a las aplicaciones de Microsoft Office 365. Para obtener más información, consulte Permitir la interacción segura con las aplicaciones de Office 365.

Aplicar flujos de trabajo

Configure estos parámetros para asignar o crear un flujo de trabajo:

- **Flujo de trabajo a usar:** Haga clic en un flujo de trabajo existente en la lista desplegable o haga clic en **Crear un nuevo flujo de trabajo**. El valor predeterminado es **Ninguno**.

  Si selecciona **Crear un nuevo flujo de trabajo**, configure estos parámetros.

  - **Nombre:** Escriba un nombre único para el flujo de trabajo.
  - **Descripción:** Opcionalmente, escriba una descripción para el flujo de trabajo.
  - **Plantillas de aprobación de correo electrónico:** En la lista, seleccione la plantilla de aprobación de correo electrónico que se asignará. Al hacer clic en el icono del ojo a la derecha de este campo, aparece un cuadro de diálogo donde puede previsualizar la plantilla.
  - **Niveles de aprobación del administrador:** En la lista, seleccione el número de niveles de aprobación del administrador necesarios para este flujo de trabajo. El valor predeterminado es 1 nivel. Las opciones posibles son:
    - No es necesario
    - 1 nivel
    - 2 niveles
    - 3 niveles
  - **Seleccionar dominio de Active Directory:** En la lista, seleccione el dominio de Active Directory adecuado para el flujo de trabajo.
  - **Buscar aprobadores adicionales obligatorios:** Escriba el nombre de la persona adicional obligatoria en el campo de búsqueda y, a continuación, haga clic en **Buscar**. Los nombres provienen de Active Directory.
  - Cuando el nombre aparezca en el campo, marque la casilla junto al nombre. El nombre y la dirección de correo electrónico aparecen en la lista de **Aprobadores adicionales obligatorios seleccionados**.

Para eliminar a una persona de la lista de **Aprobadores adicionales obligatorios seleccionados**, realice una de las siguientes acciones:

- Haga clic en **Buscar** para ver una lista de todas las personas del dominio seleccionado.
- Escriba un nombre completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Buscar** para limitar los resultados de la búsqueda.
- Las personas de la lista de **Aprobadores adicionales obligatorios seleccionados** tienen marcas de verificación junto a su nombre en la lista de resultados de búsqueda. Desplácese por la lista y desmarque la casilla junto a cada nombre que desee eliminar.

Marca de la tienda de aplicaciones y de Citrix Secure Hub

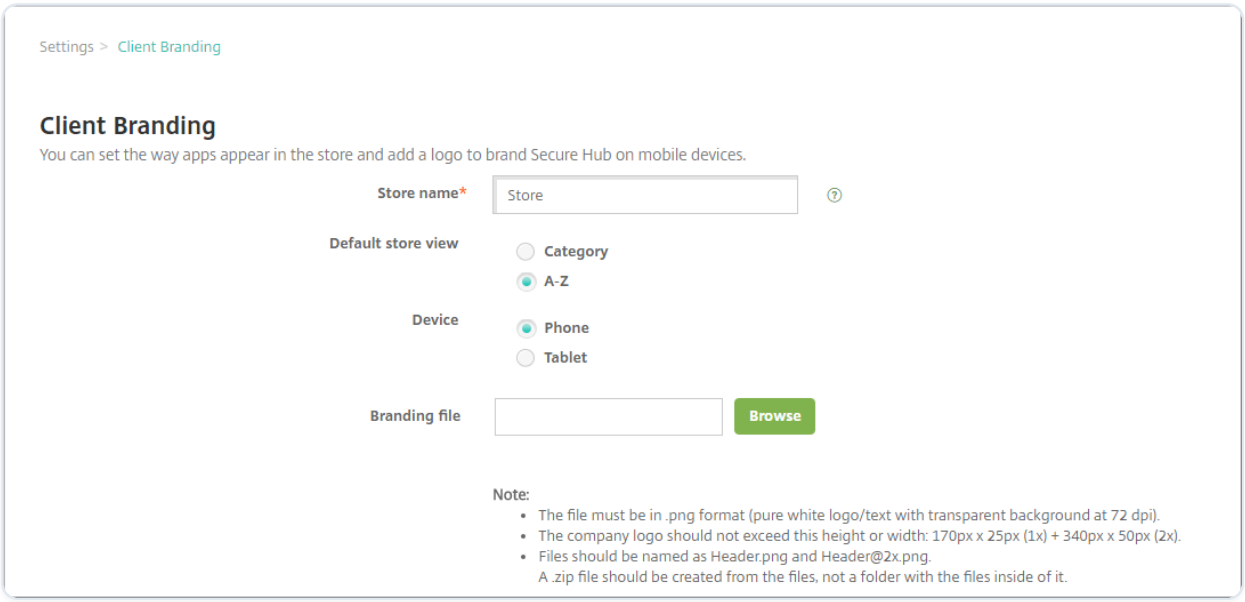
Puede configurar cómo aparecen las aplicaciones en la tienda y añadir su logotipo a Citrix Secure Hub y a la tienda de aplicaciones. Estas funciones de marca están disponibles para dispositivos iOS y Android.

Antes de empezar, asegúrese de tener su imagen personalizada lista y accesible.

La imagen personalizada debe cumplir estos requisitos:

- El archivo debe estar en formato .png
- Utilice un logotipo o texto blanco puro con un fondo transparente a 72 ppp.
- El logotipo de la empresa no puede superar esta altura o anchura: 170 px x 25 px (1x) y 340 px x 50 px (2x).
- Asigne los nombres `Header.png` y `Header@2x.png` a los archivos.
- Cree un archivo .zip con los archivos, no una carpeta que los contenga.

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje de la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En **Cliente**, haga clic en **Personalización de cliente**. Aparecerá la página **Personalización de cliente**.



Configure los siguientes parámetros:

- **Nombre de la tienda:** El nombre de la tienda aparece en la información de la cuenta del usuario. Cambiar el nombre también cambia la URL utilizada para acceder a los servicios de la tienda. Normalmente, no es necesario cambiar el nombre predeterminado.

  > **Importante:**
  >
  > El nombre de la tienda solo puede contener caracteres alfanuméricos.

- **Vista predeterminada de la tienda:** Seleccione **Categoría** o **A-Z**. El valor predeterminado es **A-Z**.
- **Opción de dispositivo:** Seleccione **Teléfono** o **Tableta**. El valor predeterminado es **Teléfono**.
- **Archivo de personalización:** Para seleccionar una imagen de personalización o un archivo .zip de imágenes, haga clic en **Examinar** y vaya a la ubicación del archivo.

3. Haga clic en **Guardar**.

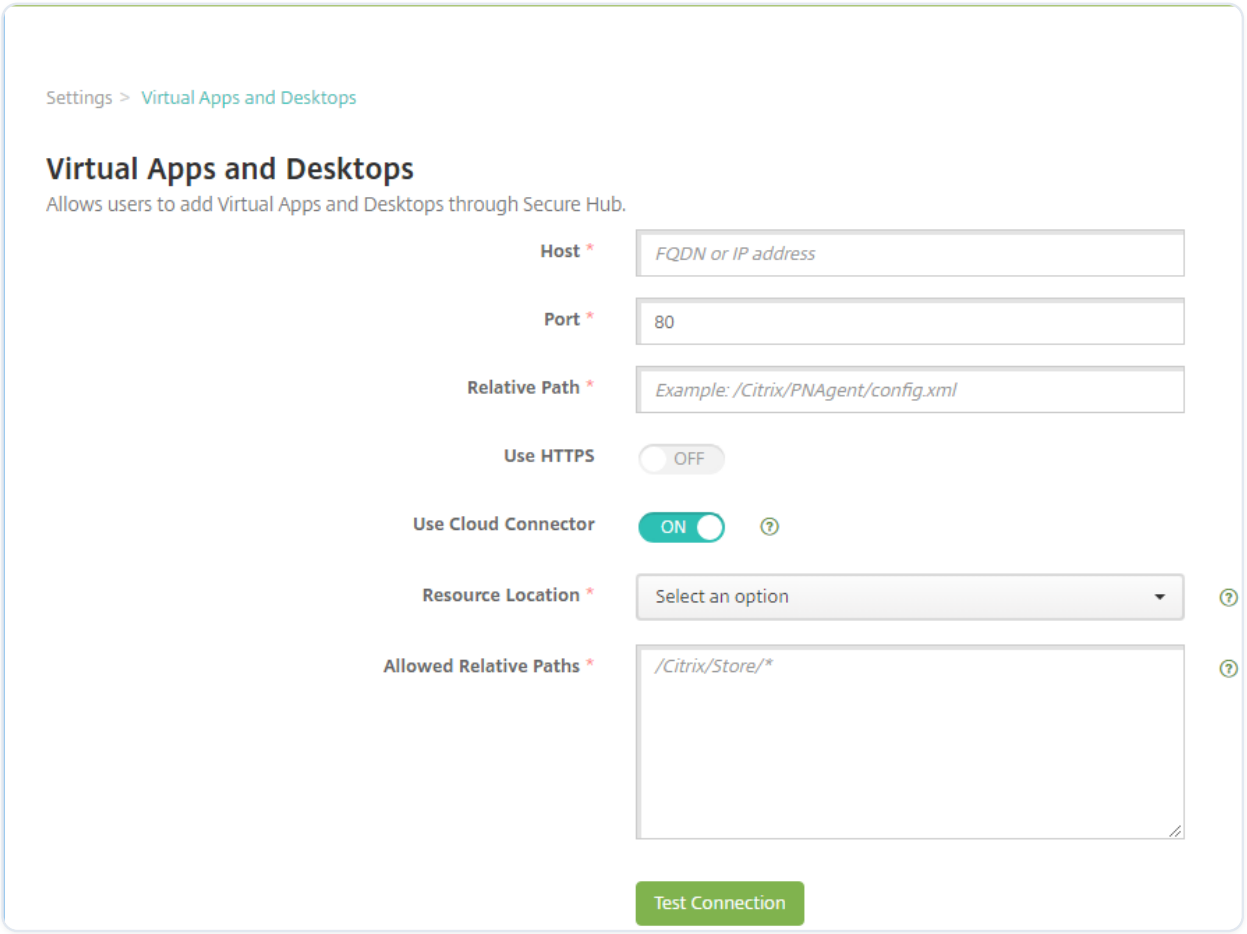
Para implementar este paquete en los dispositivos de usuario, cree un paquete de implementación y, a continuación, impleméntelo.

Citrix Virtual Apps and Desktops a través de la tienda de aplicaciones

Citrix Endpoint Management puede recopilar aplicaciones de Citrix Virtual Apps and Desktops y ponerlas a disposición de los usuarios de dispositivos móviles en la tienda de aplicaciones. Los usuarios se suscriben a las aplicaciones directamente dentro de la tienda de aplicaciones y las inician desde Citrix Workspace. La aplicación Citrix Workspace debe estar instalada en los dispositivos de usuario para iniciar las aplicaciones.

Para configurar esta opción, necesita el nombre de dominio completo (FQDN) o la dirección IP y el número de puerto de un StoreFront local.

1. En la consola web de Citrix Endpoint Management, haga clic en el icono de engranaje de la esquina superior derecha. Aparecerá la página **Parámetros**.
2. Haga clic en **Virtual Apps and Desktops**. Aparecerá la página **Virtual Apps and Desktops**.



3. Configure estos parámetros:

   - **Host:** Escriba el nombre de dominio completo (FQDN) o la dirección IP de StoreFront.
   - **Puerto:** Escriba el número de puerto de StoreFront. El valor predeterminado es 80.

- **Ruta relativa:** Escriba la ruta. Por ejemplo, /Citrix/PNAgent/config.xml
- **Usar HTTPS:** Seleccione si desea habilitar la autenticación segura entre StoreFront y el dispositivo cliente. El valor predeterminado es **Desactivado**.
- **Usar Cloud Connector:** Elija **Activado** para usar Cloud Connector para las conexiones al servidor StoreFront. A continuación, especifique una **Ubicación de recursos** y **Rutas relativas permitidas** para la conexión.
  - **Ubicación de recursos:** Elija entre las ubicaciones de recursos definidas en Citrix Cloud Connector.
  - **Rutas relativas permitidas:** Las rutas relativas permitidas para la ubicación de recursos especificada. Especifique una ruta por línea. Puede usar el comodín de asterisco (*).

  Suponga que la ubicación del recurso es `https://StoreFront.company.com` y quiere proporcionar acceso a las siguientes URL:

  - `https://StoreFront.company.com/Citrix/PNAgent/Config.xml`
  - `https://StoreFront.company.com/Citrix/PNAgent/enum.aspx`
  - `https://StoreFront.company.com/Citrix/PNAgent/launch.aspx`

  Para permitir todas las solicitudes con la URL `https://StoreFront.company.com/Citrix/PNAgent/*`, introduzca esta ruta: `/Citrix/PNAgent/*`

  Citrix Endpoint Management bloquea todas las demás rutas.

4. Haga clic en **Probar conexión** para verificar que Citrix Endpoint Management puede conectarse al servidor StoreFront especificado.
5. Haga clic en **Guardar**.

Tipos de conectores de aplicaciones

La siguiente tabla enumera los conectores y los tipos de conectores disponibles en Citrix Endpoint Management al agregar una aplicación web o SaaS. También puede agregar un conector a Citrix Endpoint Management al agregar una aplicación web o SaaS.

La tabla indica si el conector admite la administración de cuentas de usuario, lo que le permite crear cuentas automáticamente o mediante un flujo de trabajo.

NOMBRE DEL CONECTOR	SSO SAML	ADMITE LA ADMINISTRACIÓN DE CUENTAS DE USUARIO
EchoSign_SAML	Sí	Sí
Globoforce_SAML		**Nota:** Al usar este conector, debe habilitar la Administración de usuarios para el aprovisionamiento para garantizar una integración SSO sin problemas.
GoogleApps_SAML	Sí	Sí
GoogleApps_SAML_IDP	Sí	Sí
Lynda_SAML	Sí	Sí
Office365_SAML	Sí	Sí
Salesforce_SAML	Sí	Sí
Salesforce_SAML_SP	Sí	Sí
SandBox_SAML	Sí	
SuccessFactors_SAML	Sí	
ShareFile_SAML	Sí	
ShareFile_SAML_SP	Sí	
WebEx_SAML_SP	Sí	Sí

Citrix Launcher

Citrix Launcher le permite personalizar la experiencia de usuario para dispositivos Android Enterprise y dispositivos Android heredados implementados por Citrix Endpoint Management. Con Citrix Launcher, puede evitar que los usuarios accedan a ciertas configuraciones del dispositivo y restringir los dispositivos a una sola aplicación o a un pequeño conjunto de aplicaciones.

La versión mínima de Android compatible con la administración de Citrix Launcher por parte de Citrix Secure Hub es Android 6.0.

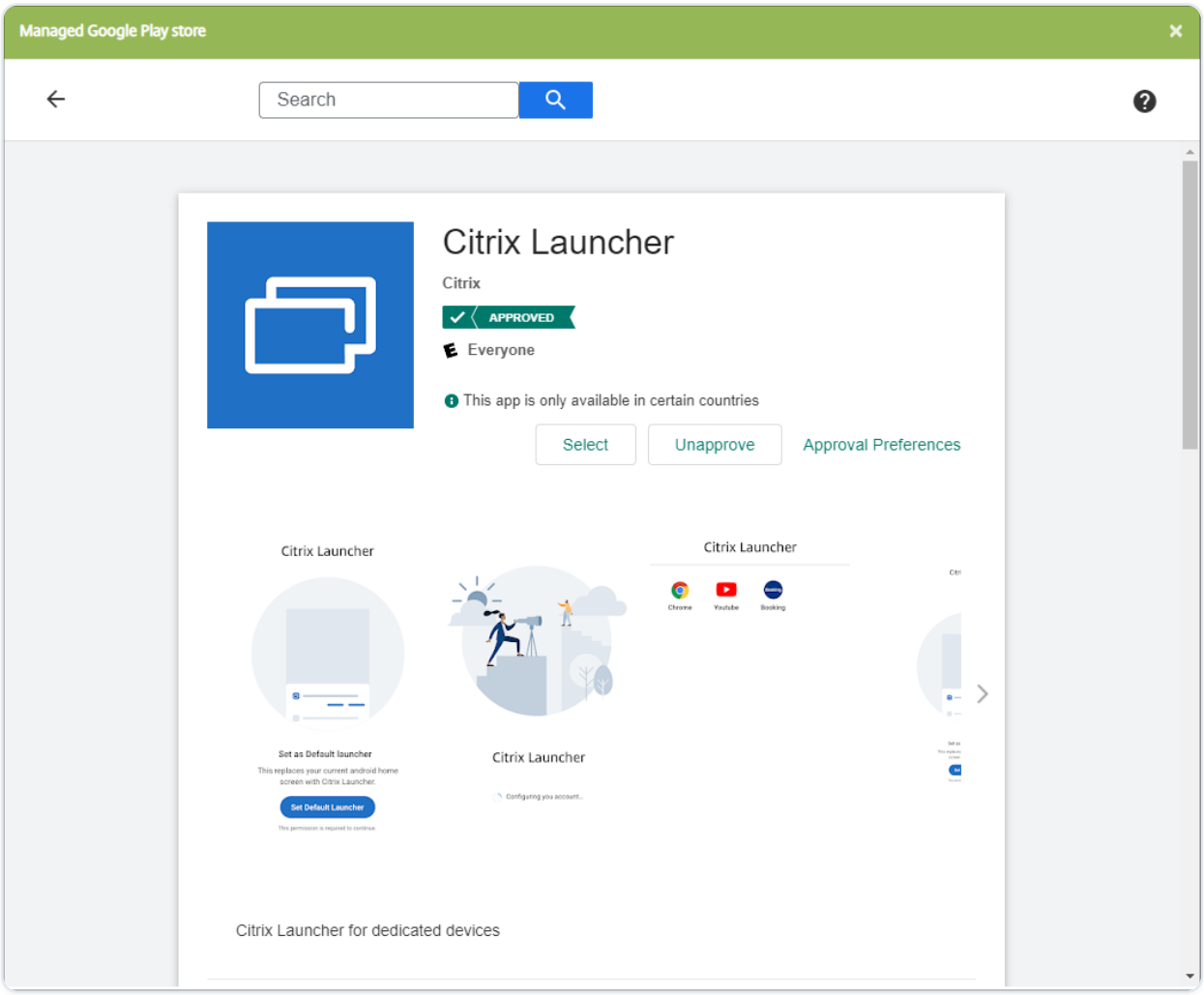
Utilice una **directiva de configuración de Launcher** para controlar estas funciones de Citrix Launcher:

- Administre dispositivos Android Enterprise y dispositivos Android heredados para que los usuarios puedan acceder solo a las aplicaciones que usted especifique.
- Opcionalmente, especifique una imagen de logotipo personalizada para el icono de Citrix Launcher y una imagen de fondo personalizada para Citrix Launcher.
- Especifique una contraseña que los usuarios deben escribir para salir del iniciador.

Citrix Launcher no está diseñado para ser una capa de seguridad adicional sobre lo que ya proporciona la plataforma del dispositivo.

Configurar Citrix Launcher para dispositivos Android Enterprise

1. Agregue la aplicación Citrix Launcher (com.citrix.launcher.droid) a Citrix Endpoint Management como una aplicación de tienda pública. En **Configurar > Aplicaciones**, haga clic en **Agregar** y, a continuación, haga clic en **Tienda de aplicaciones pública**. Para obtener más información, consulte Agregar una aplicación de tienda de aplicaciones pública.



2. En la directiva de dispositivos Kiosk, especifique qué aplicaciones deben estar disponibles en los dispositivos propiedad de la empresa para uso dedicado (también conocidos como dispositivos Android corporativos de un solo uso (COSU)). Vaya a **Configurar > Directivas de dispositivos**, haga clic en **Agregar** y seleccione **Kiosk**. Luego, seleccione la aplicación Citrix Launcher y cualquier aplicación adicional en la lista de permitidos. Si ya agregó aplicaciones a la lista, no necesita volver a cargarlas. Para obtener más información, consulte Configuración de Android Enterprise.
3. Agregue la directiva de dispositivos de configuración de Launcher. Vaya a **Configurar > Directivas de dispositivos**, haga clic en **Agregar** y seleccione **Configuración de Launcher**. En la directiva de configuración de Launcher, agregue cualquiera de las aplicaciones que especificó en la directiva Kiosk. No es necesario que agregue todas las aplicaciones que especificó en la directiva Kiosk. Debe agregar la aplicación Citrix Launcher solo en la directiva Kiosk. Para obtener más información, consulte Directiva de configuración de Launcher.
4. Cree un grupo de entrega e implemente recursos. Para obtener más información, consulte la sección Agregar un grupo de entrega e implementar recursos de este artículo.

Después de implementar Citrix Launcher en dispositivos Android Enterprise propiedad de la empresa para uso dedicado, Citrix Endpoint Management instala la aplicación y reemplaza el iniciador predeterminado de Citrix Secure Hub. Si sale de la aplicación Citrix Launcher, Citrix Secure Hub vuelve a ser el iniciador predeterminado.

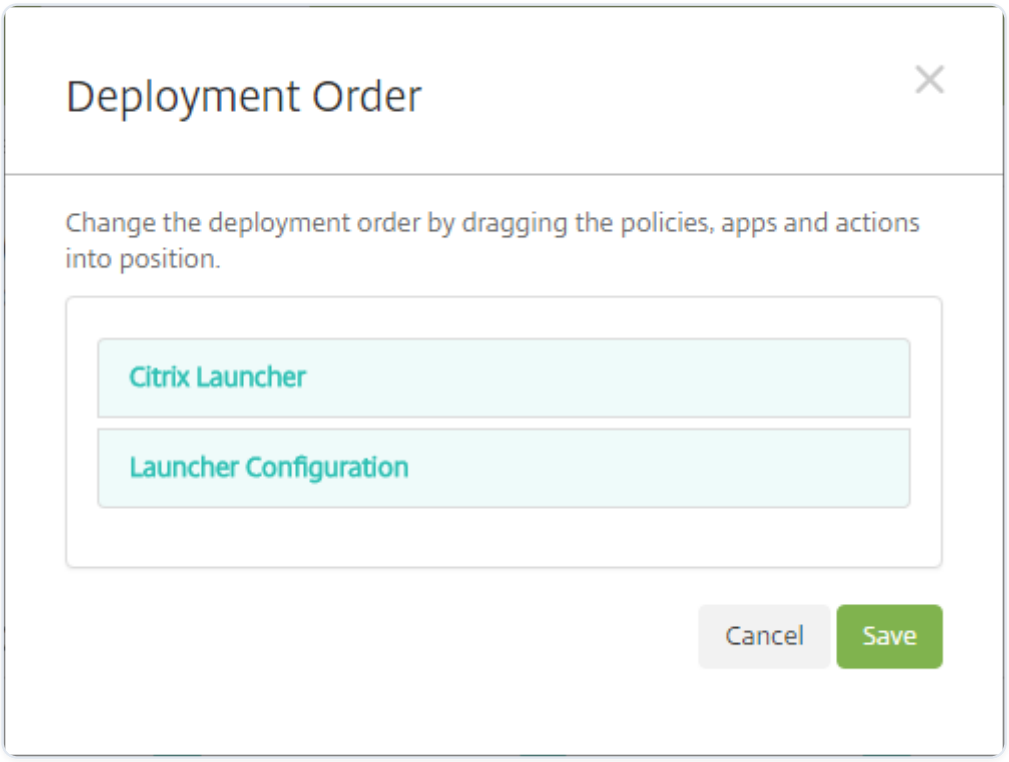
Configurar Citrix Launcher para dispositivos Android heredados

> **Nota:**
>
> En agosto de 2020, Citrix dejó de dar soporte a CitrixLauncher.apk para dispositivos Android heredados. Puede seguir utilizando la aplicación heredada Citrix Launcher (com.citrix.launcher) para dispositivos Android sin recibir las nuevas actualizaciones de funciones.

1. Para localizar la aplicación Citrix Launcher, vaya a la página de descarga de Citrix Endpoint Management y busque **Citrix Launcher**. Descargue el archivo más reciente. El archivo está listo para cargarse en Citrix Endpoint Management y no requiere encapsulado.
2. Agregue la directiva de dispositivo de Configuración de Launcher. Vaya a **Configurar > Directivas de dispositivo**, haga clic en **Agregar** y seleccione **Configuración de Launcher**. Para obtener más información, consulte Directiva de configuración de Launcher.
3. Agregue la aplicación Citrix Launcher a Citrix Endpoint Management como una aplicación empresarial. En **Configurar > Aplicaciones**, haga clic en **Agregar** y, a continuación, en **Empresarial**. Para obtener más información, consulte Agregar una aplicación empresarial.
4. Cree un grupo de entrega e implemente recursos. Para obtener más información, consulte la sección Agregar un grupo de entrega e implementar recursos de este artículo.

Agregar un grupo de entrega e implementar recursos

1. Cree un grupo de entrega para Citrix Launcher con la siguiente configuración en **Configurar > Grupos de entrega**.
    - En la página **Directivas**, agregue una **Directiva de configuración de Launcher**.
    - En la página **Aplicaciones**, arrastre **Citrix Launcher** a **Aplicaciones obligatorias**.
    - En la página **Resumen**, haga clic en **Orden de implementación** y asegúrese de que la aplicación **Citrix Launcher** precede a la directiva de **Configuración de Launcher**.



2. Implemente recursos en un grupo de entrega enviando una notificación push a todos los usuarios del grupo de entrega. Para obtener más información sobre cómo agregar recursos a un grupo de entrega, consulte Implementar recursos.

Administrar dispositivos sin Citrix Launcher

En lugar de usar Citrix Launcher, puede usar las funciones que ya están disponibles.

Para aprovisionar dispositivos dedicados:

1. Cree un perfil de inscripción estableciendo el **Modo de propietario del dispositivo** en **Dispositivo dedicado**. Consulte Aprovisionar dispositivos Android Enterprise dedicados y Perfiles de inscripción.
2. Cree una directiva de dispositivo de quiosco para agregar aplicaciones a la lista de permitidos y establecer el modo de tarea bloqueada. Si ya agregó aplicaciones a la lista, no necesita volver a cargarlas. Para obtener más información, consulte Configuración de Android Enterprise.
3. Inscriba cada dispositivo en el perfil de inscripción que creó.

Añadir aplicaciones mediante Apple Volume Purchase

Apple Business Manager (ABM) y Apple School Manager (ASM) le permiten comprar licencias de aplicaciones y libros al por mayor y sincronizar la información de Volume Purchase con Citrix Endpoint Management. A continuación, puede usar Citrix Endpoint Management para implementar

estas aplicaciones y libros en dispositivos iOS y macOS. La compra de contenido al por mayor simplifica el proceso de búsqueda, compra y distribución de aplicaciones y libros para una organización.

Para obtener más información sobre la compra de contenido mediante ABM o ASM, consulte la Guía del usuario de Apple Business Manager o la Guía del usuario de Apple School Manager. Este artículo describe cómo sincronizar las licencias compradas por volumen de ABM y ASM con Citrix Endpoint Management y cómo administrar las licencias.

> **Nota:**
>
> El programa Apple Volume Purchase Program (VPP) ya no está disponible a partir de January 14, 2021. La función Volume Purchase se integró en ABM y ASM. Si actualmente utiliza el Device Enrollment Program (DEP) o VPP, puede actualizar a ABM o ASM. Para obtener más información, consulte la documentación de Apple Upgrade from Apple Deployment Programs.

Acerca de Apple Volume Purchase

Cuando compre contenido al por mayor mediante ABM o ASM, tenga en cuenta lo siguiente:

- Puede comprar licencias para el siguiente contenido:
  - Aplicaciones y libros públicos
  - Aplicaciones personalizadas desarrolladas específicamente para su organización
- Puede implementar aplicaciones y libros comprados por volumen en dispositivos propiedad de la organización y dispositivos BYO. Los dispositivos propiedad de la organización inscritos a través de ABM o ASM admiten la inscripción MDM o MDM+MAM, pero no la inscripción MAM.
- Para obtener más información sobre la distribución de aplicaciones, consulte Distribuir aplicaciones de Apple.
- Para obtener una lista de problemas conocidos, consulte el artículo de Knowledge Center CTX222633.

Añadir una cuenta de Volume Purchase

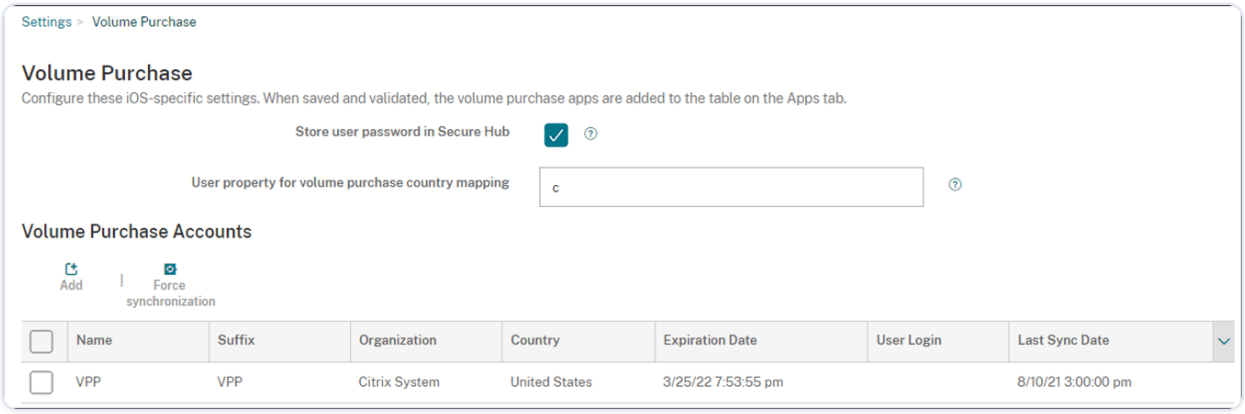
Después de comprar contenido en el portal de ABM o ASM, descargue el token de contenido asociado con Citrix Endpoint Management desde el portal. A continuación, en Citrix Endpoint Management, cree una cuenta de Volume Purchase basada en este código de contenido. Este

código permite a Citrix Endpoint Management sincronizar las licencias de contenido de ABM o ASM.

Con la Compra por volumen, puede adquirir contenido e implementarlo en dispositivos mediante licencias gestionadas. Si actualmente utiliza códigos de canje y desea cambiar a licencias gestionadas, consulte el documento de soporte de Apple.

Para agregar una cuenta de Compra por volumen en Citrix Endpoint Management

1. En el portal de ABM o ASM, compre el contenido según sea necesario y, a continuación, descargue el archivo de código de contenido en una ubicación segura.
2. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje de la esquina superior derecha. Aparecerá la página de **Configuración**.
3. Haga clic en **Compra por volumen**. Aparecerá la página de configuración de **Compra por volumen**.

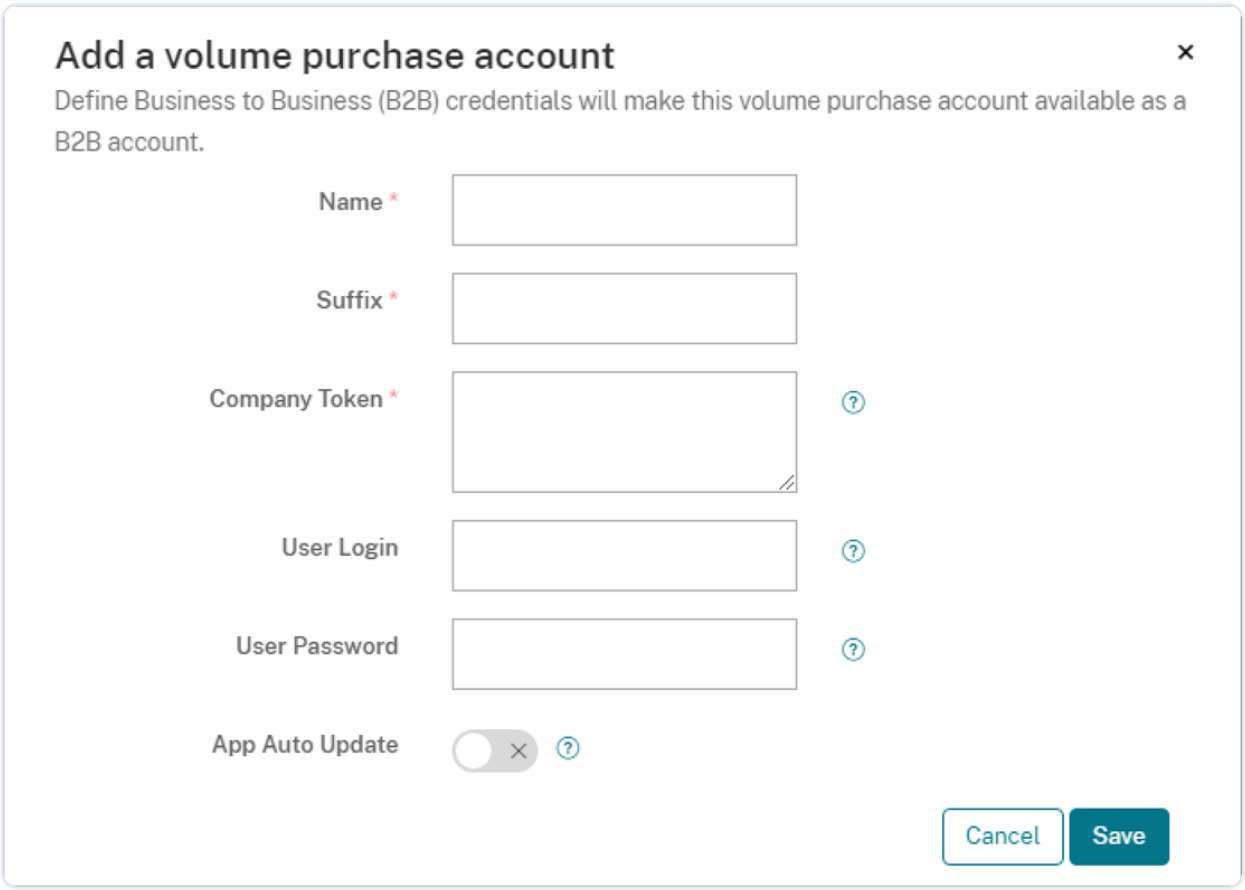


4. Configure los siguientes ajustes:

   - **Almacenar contraseña de usuario en Citrix Secure Hub:** Seleccione si desea almacenar un nombre de usuario y una contraseña en Citrix Secure Hub para la autenticación de Citrix Endpoint Management. El valor predeterminado es **Activado**.
   - **Propiedad de usuario para la asignación de país de Compra por volumen:** Escriba un código de asignación de país para permitir a los usuarios descargar aplicaciones de la tienda de aplicaciones específica del país. Póngase en contacto con su gestor de contenido para obtener este código.

     Citrix Endpoint Management utiliza el código de asignación de país para elegir el grupo de propiedades de la Compra por volumen. Por ejemplo, si la propiedad del usuario es Estados Unidos, el usuario no puede descargar aplicaciones si el código de asignación es para el Reino Unido.

5. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar una cuenta de Compra por volumen**.



6. Configure los siguientes ajustes de cuenta:

> **Nota:**
>
> Si utiliza Apple Configurator 1, cargue un archivo de licencia de la siguiente manera: Haga clic en **Configurar > Aplicaciones**, vaya a la página de plataforma de una aplicación y, a continuación, expanda **Compra por volumen**.

- **Nombre:** Escriba un nombre descriptivo para la cuenta.
- **Sufijo:** Escriba el sufijo que aparecerá con los nombres de las aplicaciones heredadas de las tiendas de Apple. Por ejemplo, si introduce **VP**, la aplicación **Citrix Secure Mail** aparecerá en la lista de aplicaciones como **Citrix Secure Mail - VP**.
- **Token de empresa:** Copie y pegue el token de contenido que descargó en el paso 1.
- **Inicio de sesión de usuario:** (Opcional) Escriba un nombre de usuario para el administrador de esta cuenta de compra por volumen. Si está configurado, el nombre de

usuario y la contraseña son necesarios para sincronizar las aplicaciones personalizadas compradas por volumen en Citrix Endpoint Management.

- **Contraseña de usuario:** (Opcional) Escriba una contraseña para el nombre de usuario que ha introducido.
- **Actualización automática de aplicaciones:** Si está **activada**, las aplicaciones compradas por volumen y las aplicaciones opcionales de la consola de Citrix Endpoint Management se actualizan automáticamente cuando hay una nueva versión disponible. Debe seguir actualizando manualmente las aplicaciones empresariales y las aplicaciones de la tienda de aplicaciones pública en la consola de Citrix Endpoint Management. Si esta opción está configurada como **Desactivada**, puede seguir actualizando manualmente las aplicaciones compradas por volumen en la consola de Citrix Endpoint Management. Una vez que una aplicación se actualiza en la consola, los dispositivos con la aplicación instalada también reciben esa actualización. El valor predeterminado es **Desactivada**.

Una vez que la cuenta de volumen se haya agregado correctamente, aparecerá un mensaje que le notificará lo siguiente:

- En la página **Configurar > Aplicaciones**, las aplicaciones compradas por volumen aparecen en la lista de aplicaciones. Los nombres de las aplicaciones aparecen con el sufijo que configuró.
- En la página **Configurar > Contenido multimedia**, los libros comprados por volumen aparecen en la lista de contenido multimedia. Los nombres de los libros aparecen con el sufijo que configuró.

Configurar aplicaciones compradas por volumen

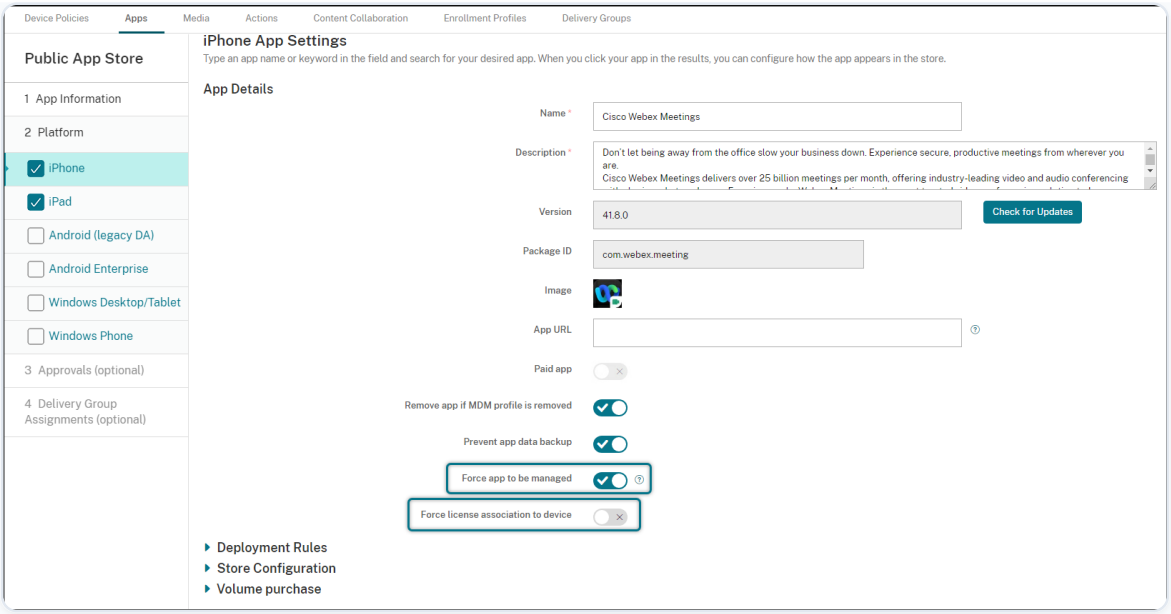
Después de agregar una cuenta de compra por volumen, la información de la aplicación se sincroniza con Citrix Endpoint Management y aparece en la página **Configurar > Aplicaciones**. Ahora puede configurar estas aplicaciones, ajustar su grupo de entrega y modificar la configuración de la directiva de dispositivos para dispositivos iOS y macOS. Una vez completada la configuración, los usuarios pueden inscribir sus dispositivos.

Al configurar una aplicación comprada por volumen, tenga en cuenta la siguiente configuración:

- En la página **Configurar > Aplicaciones**:
  - Para permitir que Citrix Endpoint Management implemente una aplicación en un dispositivo en lugar de en un usuario, active **Forzar asociación de licencias al dispositivo**. Cuando esta opción está activada, los usuarios no tienen que usar su ID de Apple y pueden descargar las aplicaciones sin iniciar sesión en su cuenta de App Store.

- Le recomendamos que active **Forzar que la aplicación sea administrada** para una aplicación, de modo que se instale automáticamente como una aplicación administrada.

> **Nota:**
>
> Para que la configuración **Forzar la administración de la aplicación** surta efecto, debe configurar la propiedad de servidor `apple.app.force.managed` en **True** en la página **Parámetros > Propiedades del servidor**. Para obtener más información, consulte Propiedades del servidor



- En la página **Configurar > Grupo de entrega**:

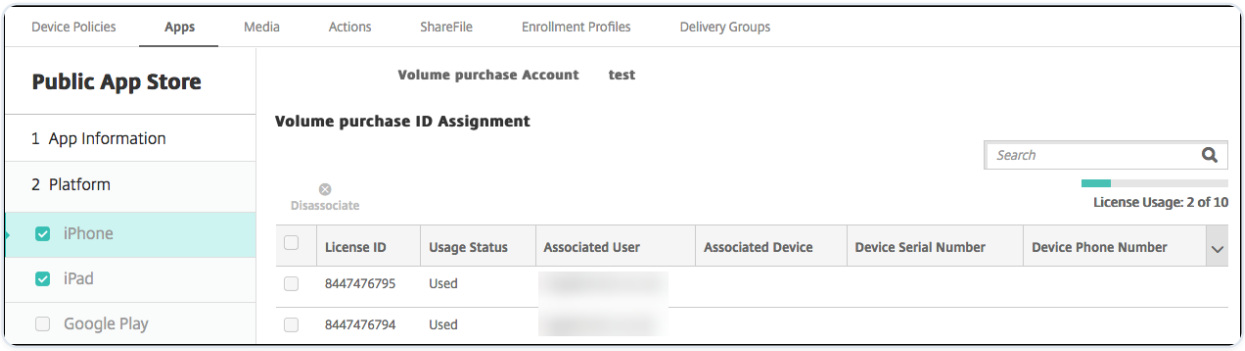
  Para que la aplicación se instale de forma silenciosa en los dispositivos de los usuarios con una interacción mínima por parte de estos, vaya a la página **Aplicaciones** y arrastre la aplicación a la lista **Aplicaciones obligatorias**. De forma predeterminada, las aplicaciones, excepto Citrix Secure Hub, son **Aplicaciones opcionales**, lo que significa que los usuarios deben iniciar la instalación de la aplicación manualmente a través de Citrix Secure Hub.

Rastrear y administrar el uso de licencias de aplicaciones

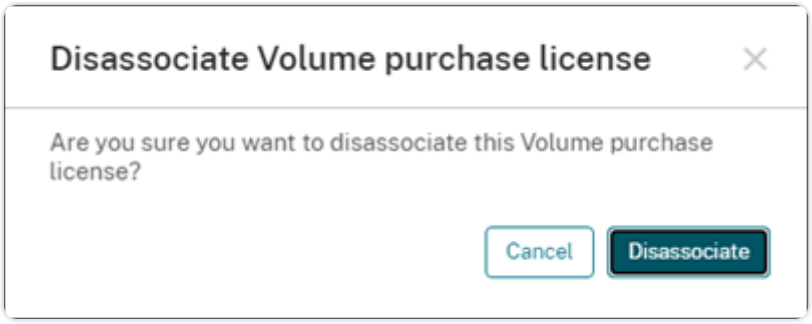
Puede rastrear el uso de licencias de una aplicación. Si es necesario, puede recuperar una licencia utilizada, poniéndola a disposición de otro usuario o dispositivo.

1. Haga clic en **Configurar > Aplicaciones**.
2. Seleccione una aplicación y haga clic en **Modificar**.

3. Vaya a la página **Plataforma** y, a continuación, expanda **Compra por volumen**. En la tabla **Asignación de ID de compra por volumen**, puede rastrear cuántas licencias se utilizan y por qué usuario o dispositivo.



4. Para recuperar una licencia, seleccione la licencia y, a continuación, haga clic en **Desasociar**.



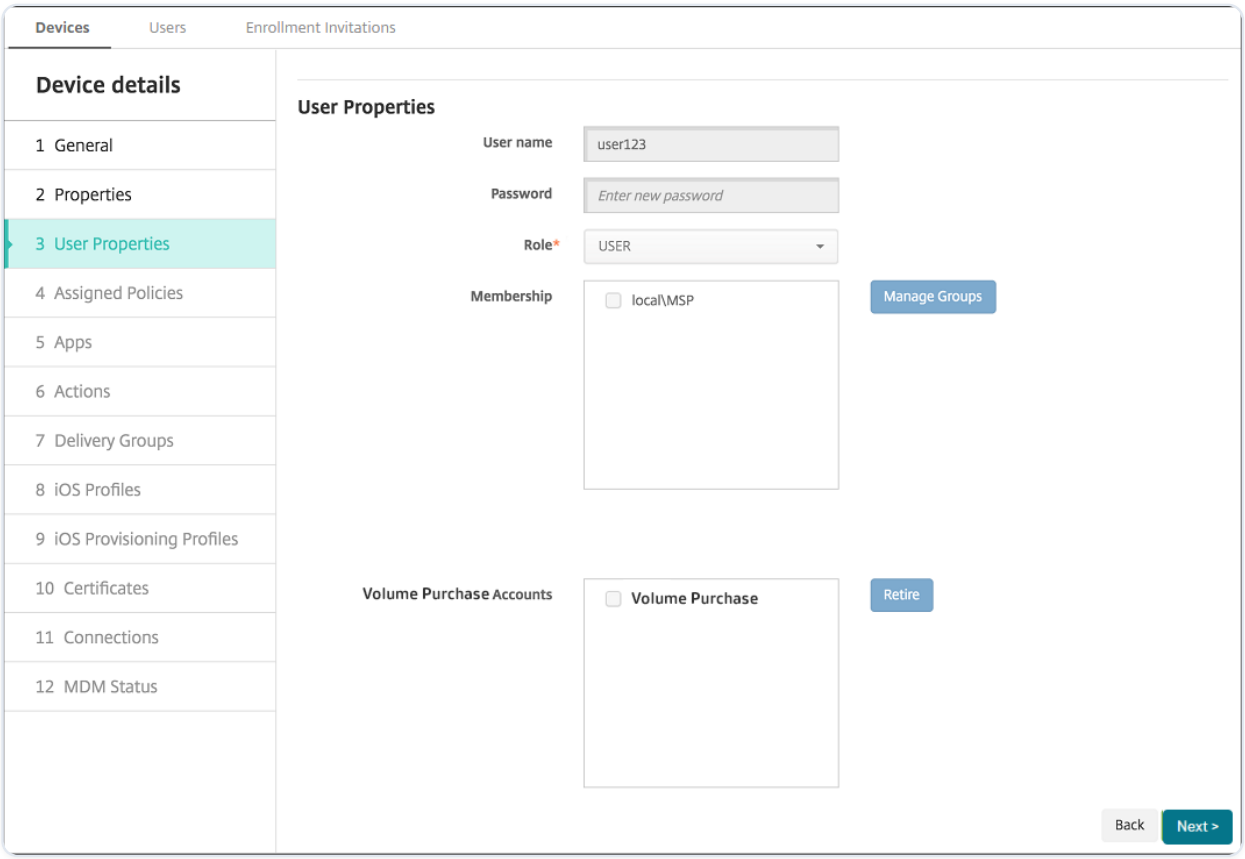
5. Haga clic en **Desasociar** para confirmar la acción.

Retirar a un usuario de la cuenta de compra por volumen

Si asocia licencias de aplicaciones a los usuarios, puede retirar usuarios de las cuentas de compra por volumen para recuperar todas las licencias asignadas a esos usuarios. Un caso de uso es cuando un usuario abandona su organización.

1. Haga clic en **Administrar > Dispositivos**
2. Seleccione el dispositivo que pertenece al usuario de destino y, a continuación, haga clic en **Modificar**.
3. Vaya a la página **Propiedades de usuario** y seleccione las cuentas de compra por volumen según sea necesario.

4. Haga clic en **Retirar**.



Citrix Endpoint Management revoca las licencias de aplicaciones de las cuentas de compra por volumen seleccionadas del usuario.

Sincronizar la información de la aplicación

Citrix Endpoint Management sincroniza periódicamente la información de la aplicación con ABM o ASM. Si es necesario, puede sincronizar manualmente la información de la aplicación. La sincronización garantiza que las licencias de aplicaciones y otra información de la aplicación reflejen todos los cambios. Estos cambios incluyen la eliminación manual de una aplicación de la cuenta de compra por volumen.

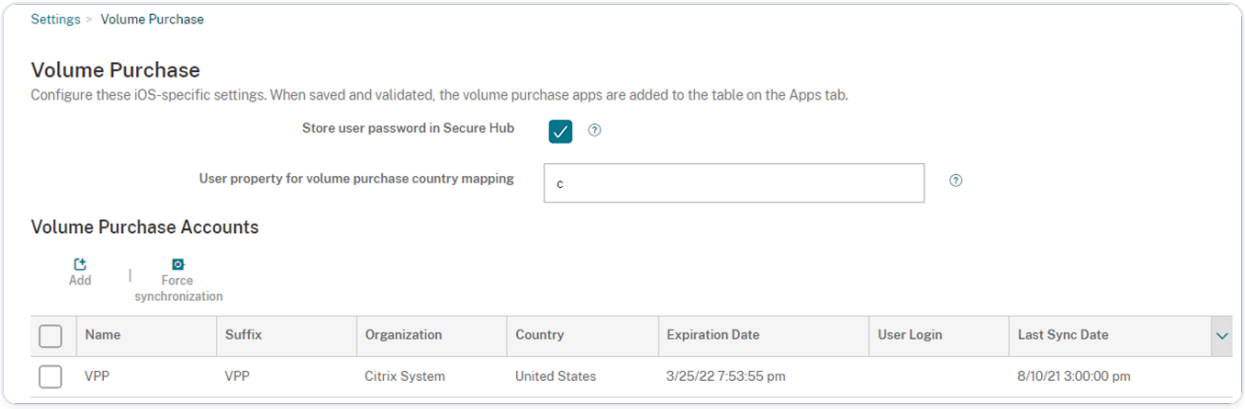
Cambiar el intervalo de sincronización predeterminado

De forma predeterminada, Citrix Endpoint Management actualiza la línea base de licencias de compra por volumen al menos cada 1440 minutos (24 horas). Un administrador de Citrix Cloud puede cambiar el intervalo predeterminado a través de la propiedad del servidor, `vpp.baseline`. Para obtener más información, consulte Propiedades del servidor.

Sincronizar manualmente la información de la aplicación

Puede forzar una sincronización con ABM o ASM para obtener la información más reciente de la aplicación de inmediato.

1. Haga clic en **Parámetros > Compra por volumen**
2. Seleccione una cuenta de compra por volumen y, a continuación, haga clic en **Forzar sincronización**. O haga clic en **Forzar sincronización** sin seleccionar una cuenta de compra por volumen para sincronizar todas las cuentas.



3. Confirme la acción de sincronización. La sincronización se inicia.

   La sincronización puede tardar varios minutos, según el número de licencias de compra por volumen. Una vez completada la sincronización, Citrix Endpoint Management actualiza la página **Compra por volumen** y actualiza la fecha y la hora de sincronización en la nueva columna **Fecha de última sincronización**.

Comprobar actualizaciones de la aplicación

Si activa la configuración de **Actualización automática de aplicaciones** al añadir una cuenta de compra por volumen, Citrix Endpoint Management comprueba periódicamente si hay nuevas versiones de las aplicaciones compradas por volumen y las aplicaciones opcionales, y realiza las actualizaciones. Si es necesario, puede buscar manualmente la nueva versión de cualquier aplicación y aplicar las actualizaciones de la aplicación a Citrix Endpoint Management.

Una vez que Citrix Endpoint Management recibe una nueva versión de una aplicación requerida, la envía al dispositivo para su instalación silenciosa sin pedir confirmación a los usuarios.

Para comprobar y aplicar la nueva versión de una aplicación

1. Haga clic en **Configurar > Aplicaciones**. Aparecerá la página **Aplicaciones**.
2. Seleccione una aplicación y haga clic en **Modificar**.
3. Vaya a la página **Plataforma** y, a continuación, haga clic en **Buscar actualizaciones** junto a **Versión**.
4. En el cuadro de diálogo **Actualizar** que aparece, aplique la actualización si hay una nueva versión disponible.

Renovar el token de contenido de su cuenta de compra por volumen

Un token de contenido caduca anualmente. Cuando el token está a punto de caducar, Citrix Endpoint Management muestra una advertencia de caducidad de la licencia. Renueve el token de contenido a tiempo para evitar interrupciones a sus usuarios.

1. Desde el portal de ABM o ASM, descargue un token actualizado.
2. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje de la esquina superior derecha. Aparecerá la página **Configuración**.
3. Haga clic en **Compra por volumen**. Aparecerá la página de configuración de Compra por volumen.
4. Edite su cuenta de Compra por volumen con la información del token actualizado.

Usar ShareFile con Citrix Endpoint Management

> **Descargo de responsabilidad:**

> Esta función quedará obsoleta si ShareFile (ahora Progress) deja de ofrecer soporte.

> Citrix Endpoint Management tiene dos opciones para integrarse con ShareFile. Son Citrix Files y los conectores de zona de almacenamiento.

Citrix Files

Puede configurar Citrix Endpoint Management para proporcionar acceso a su cuenta de ShareFile. Esa configuración:

- Ofrece a los usuarios móviles acceso a todas las funciones de ShareFile, como el uso compartido de archivos, la sincronización de archivos y los conectores de zona de almacenamiento.
- Puede proporcionar a Citrix Files autenticación de inicio de sesión único para usuarios de aplicaciones de productividad móvil y directivas de control de acceso exhaustivas.
- Proporciona la configuración de ShareFile, la supervisión del nivel de servicio y la supervisión del uso de licencias a través de la consola de Citrix Endpoint Management.

Para obtener más información sobre cómo configurar Citrix Endpoint Management para cuentas de empresa, consulte SAML para el inicio de sesión único con Citrix Files.

Conectores de zona de almacenamiento

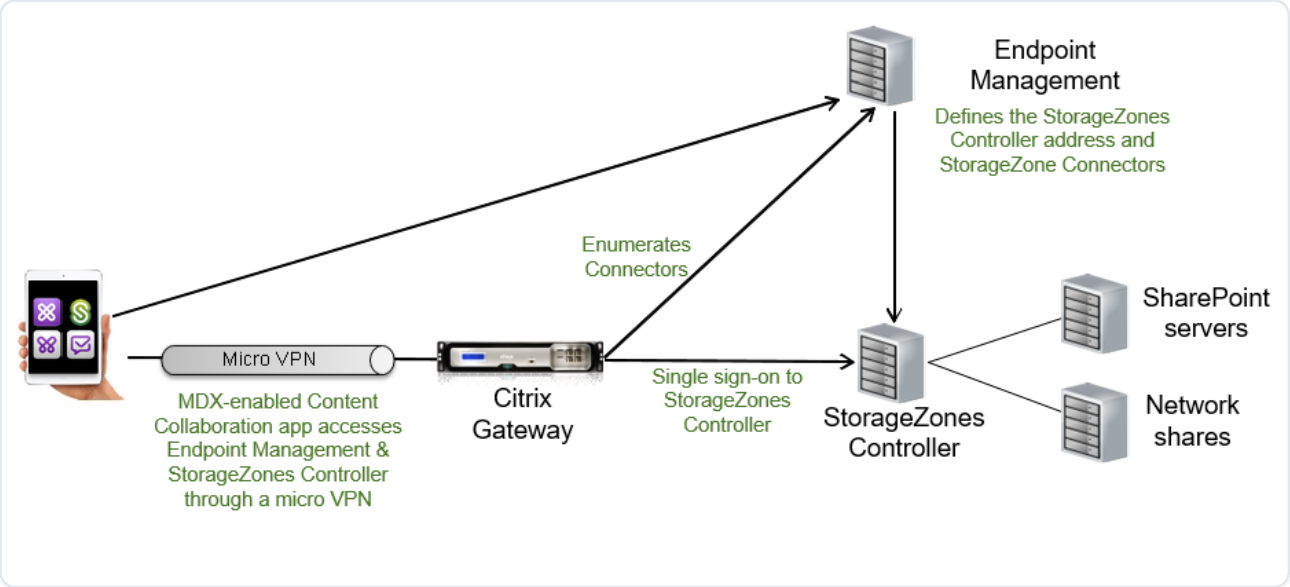
Puede configurar Citrix Endpoint Management para proporcionar acceso solo a los conectores de zona de almacenamiento que cree a través de la consola de Citrix Endpoint Management. Esa configuración:

- Proporciona acceso móvil seguro a los repositorios de almacenamiento locales existentes, como sitios de SharePoint y recursos compartidos de archivos de red.
- No requiere que configure un subdominio de ShareFile ni que aloje datos de Citrix Files.
- Proporciona a los usuarios acceso móvil a los datos a través de las aplicaciones de productividad móvil de Citrix para Citrix Files para iOS y Android. Los usuarios pueden editar documentos de Microsoft Office. Los usuarios también pueden previsualizar y anotar archivos Adobe PDF desde dispositivos móviles.
- Cumple con las restricciones de seguridad contra la fuga de información del usuario fuera de la red corporativa.
- Proporciona una configuración sencilla de los conectores de zona de almacenamiento a través de la consola de Citrix Endpoint Management. Si más adelante decide utilizar la funcionalidad completa de Citrix Files con Citrix Endpoint Management, puede cambiar la configuración en la consola de Citrix Endpoint Management.

Para una integración de Citrix Endpoint Management solo con conectores de zona de almacenamiento:

- ShareFile utiliza su configuración de inicio de sesión único en NetScaler Gateway para autenticarse con el controlador de zonas de almacenamiento.
- Citrix Endpoint Management no se autentica a través de SAML porque no se utiliza el plano de control de Citrix Files.

El siguiente diagrama muestra la arquitectura de alto nivel para el uso de Citrix Endpoint Management con conectores de zona de almacenamiento.



Requisitos

- Versiones mínimas de los componentes:
  - ShareFile para iOS (MDX) 5.3
  - ShareFile para Android (MDX) 5.3
  - Controlador de zonas de almacenamiento 5.11.20 Este artículo contiene instrucciones sobre cómo configurar el controlador de zonas de almacenamiento 5.0
- Asegúrese de que el servidor para ejecutar el controlador de zonas de almacenamiento cumpla los requisitos del sistema. Para conocer los requisitos, consulte Requisitos del sistema.

Los requisitos para las zonas de almacenamiento de datos de Citrix Files y para las zonas de almacenamiento restringidas no se aplican a una integración de Citrix Endpoint Management solo con conectores de zona de almacenamiento.

Citrix Endpoint Management no admite conectores de Documentum.

- Para ejecutar scripts de PowerShell:
  - Ejecute los scripts en la versión de 32 bits (x86) de PowerShell.

Tareas de instalación

Complete las siguientes tareas, en el orden presentado, para instalar y configurar el controlador de zonas de almacenamiento. Estos pasos son específicos solo para la integración de Citrix Endpoint Management con los conectores de zonas de almacenamiento. Algunos de estos artículos se encuentran en la documentación del controlador de zonas de almacenamiento.

1. Configurar NetScaler para el controlador de zonas de almacenamiento

   Puede usar NetScaler Gateway como proxy DMZ para el controlador de zonas de almacenamiento.

2. Instalar un certificado SSL

   Un controlador de zonas de almacenamiento que aloja zonas estándar requiere un certificado SSL. Un controlador de zonas de almacenamiento que aloja zonas restringidas y utiliza una dirección interna no requiere un certificado SSL.

3. Preparar el servidor

   Se requiere la configuración de IIS y ASP.NET para los conectores de zonas de almacenamiento.

4. Instalar el controlador de zonas de almacenamiento
5. Preparar el controlador de zonas de almacenamiento para su uso solo con conectores de zonas de almacenamiento
6. Especificar un servidor proxy para las zonas de almacenamiento

   La consola del controlador de zonas de almacenamiento le permite especificar un servidor proxy para el controlador de zonas de almacenamiento. También puede especificar un servidor proxy utilizando otros métodos.

7. Configurar el controlador de dominio para que confíe en el controlador de zonas de almacenamiento para la delegación

   Configure el controlador de dominio para admitir la autenticación NTLM o Kerberos en recursos compartidos de red o sitios de SharePoint.

8. Unir un controlador de zonas de almacenamiento secundario a una zona de almacenamiento

   Para configurar una zona de almacenamiento para alta disponibilidad, conéctele al menos dos controladores de zonas de almacenamiento.

Instalar el controlador de zonas de almacenamiento

1. Descargue e instale el software del controlador de zonas de almacenamiento:

   a. Desde Descargas de herramientas/aplicaciones de ShareFile, inicie sesión y descargue el instalador más reciente del controlador de zonas de almacenamiento.

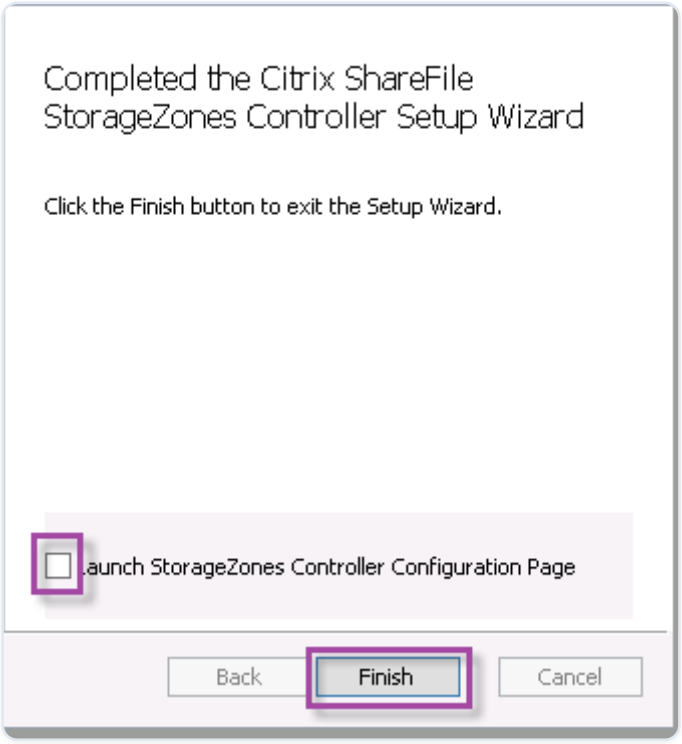
b. La instalación del controlador de zonas de almacenamiento cambia el sitio web predeterminado del servidor a la ruta de instalación del controlador. Habilite la **autenticación anónima** en el sitio web predeterminado.

2. En el servidor donde quiera instalar el controlador de zonas de almacenamiento, ejecute StorageCenter.msi.

   Se inicia el asistente de configuración del controlador de zonas de almacenamiento.

3. Responda a las indicaciones:

   - En la página **Carpeta de destino**, si Internet Information Services (IIS) está instalado en la ubicación predeterminada, deje los valores predeterminados. Si no, busque la ubicación de instalación de IIS.
   - Cuando la instalación se complete, desactive la casilla de verificación **Iniciar página de configuración del controlador de zonas de almacenamiento** y, a continuación, haga clic en **Finalizar**.



4. Cuando se le solicite, reinicie el controlador de zonas de almacenamiento.
5. Para comprobar que la instalación se realizó correctamente, vaya a `https://localhost/`. (Si recibe un error de certificado, considere la posibilidad de conectarse con HTTP en su lugar). Si la instalación se realiza correctamente, aparecerá el logotipo de Citrix Files.

   Si el logotipo de Citrix Files no aparece, borre la caché del navegador y vuelva a intentarlo.

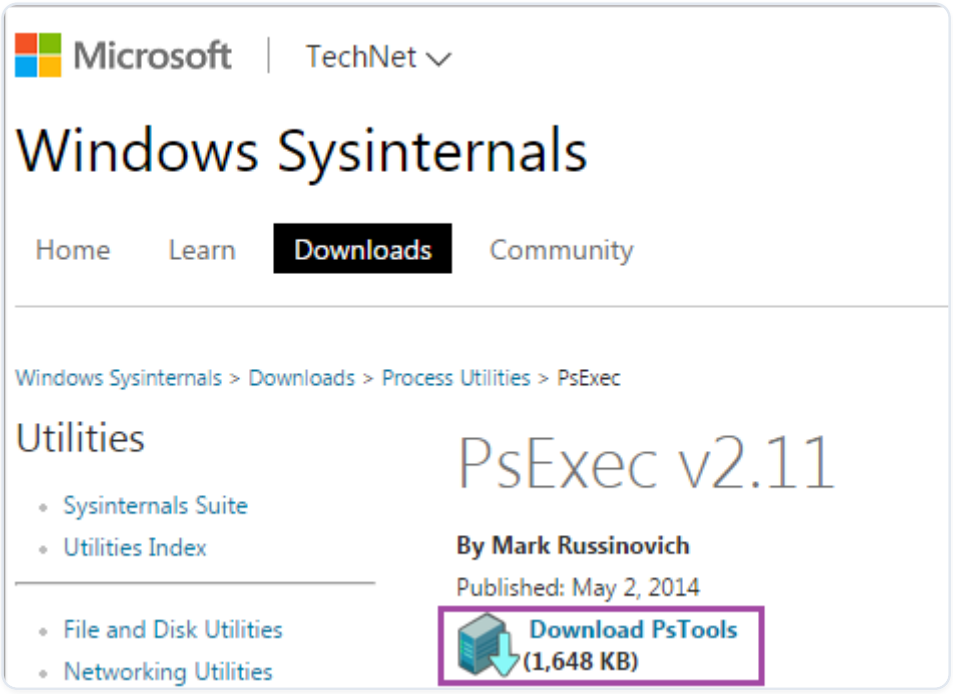
> **Importante:**
>
> Si tiene previsto clonar el controlador de zonas de almacenamiento, capture la imagen del disco antes de continuar con la configuración del controlador de zonas de almacenamiento.

Preparar el controlador de zonas de almacenamiento para usarlo solo con conectores de zonas de almacenamiento

Para una integración solo con conectores de zonas de almacenamiento, no se utiliza la consola administrativa del controlador de zonas de almacenamiento. Esa interfaz requiere una cuenta de administrador de Citrix Files, que no es necesaria para esta solución. Como resultado, se ejecuta un script de PowerShell para preparar el controlador de zonas de almacenamiento para su uso sin el plano de control de Citrix Files. El script hace lo siguiente:

- Registra el controlador de zonas de almacenamiento actual como controlador de zonas de almacenamiento principal. Más tarde, puede unir un controlador de zonas de almacenamiento secundario al controlador principal.
- Crea una zona y establece la frase de contraseña para ella.

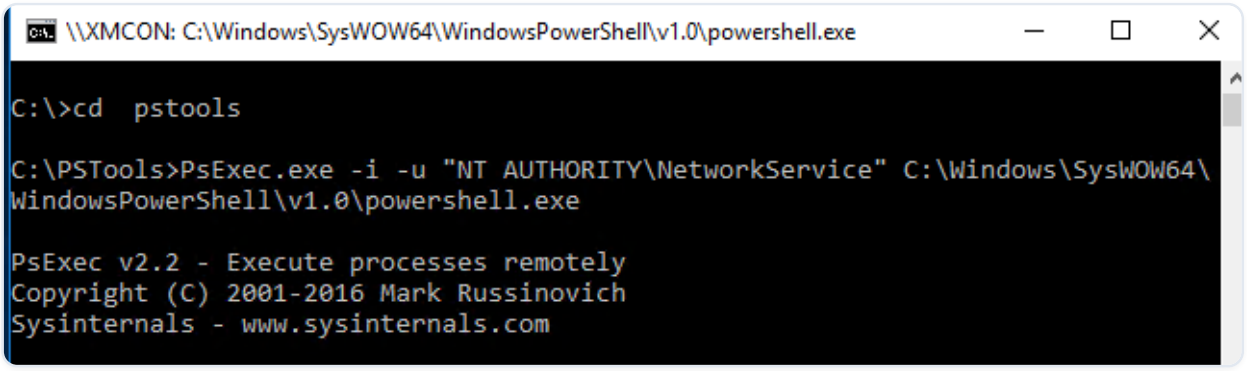
1. Desde el servidor del controlador de zonas de almacenamiento, descargue la herramienta PsExec: Vaya a Microsoft Windows Sysinternals y, a continuación, haga clic en **Download PsTools**. Extraiga la herramienta a la raíz de la unidad C.



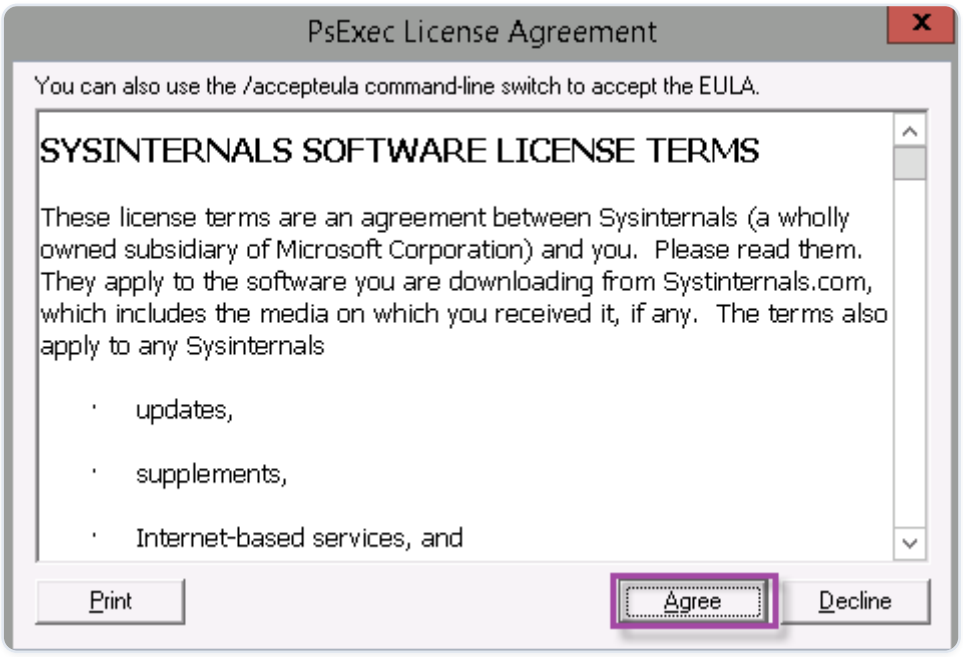
2. Ejecute la herramienta PsExec: Abra el Símbolo del sistema como usuario administrador y, a continuación, escriba lo siguiente:

```
cd c:\pstools

PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:
\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```



3. Cuando se le solicite, haga clic en **Agree** para ejecutar la herramienta Sysinternals.



Se abre una ventana de PowerShell.

4. En la ventana de PowerShell, escriba lo siguiente:

```
```

Import-Module "C:
\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"

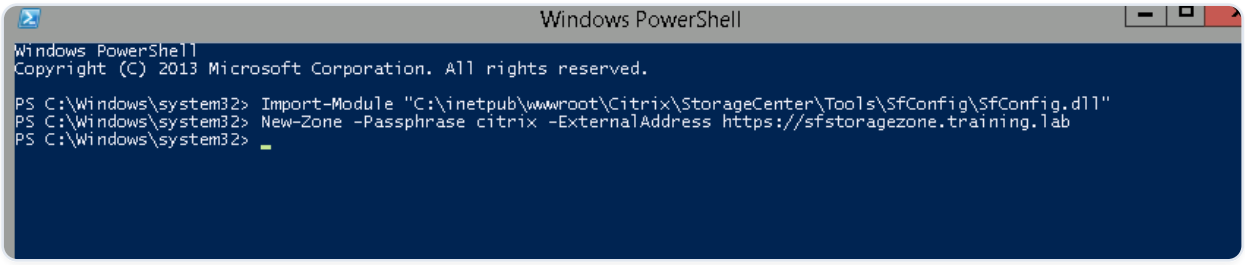
New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com

```
```

Donde:

Frase de contraseña: Es la frase de contraseña que quiere asignar al sitio. Anótela. No puede recuperar la frase de contraseña del controlador. Si pierde la frase de contraseña, no podrá reinstalar las zonas de almacenamiento, unir más controladores de zonas de almacenamiento a la zona de almacenamiento ni recuperar la zona de almacenamiento si el servidor falla.

ExternalAddress: Es el nombre de dominio completo externo del servidor del controlador de zonas de almacenamiento.



Su controlador principal de zonas de almacenamiento ya está listo.

Antes de iniciar sesión en Citrix Endpoint Management para crear conectores de zonas de almacenamiento: Complete la siguiente configuración, si corresponde:

Especificar un servidor proxy para las zonas de almacenamiento

Configurar el controlador de dominio para que confíe en el controlador de zonas de almacenamiento para la delegación

Unir un controlador secundario de zonas de almacenamiento a una zona de almacenamiento

Para crear conectores de zonas de almacenamiento, consulte Definir conexiones de controladores de zonas de almacenamiento en Citrix Endpoint Management.

Unir un controlador secundario de zonas de almacenamiento a una zona de almacenamiento

Para configurar una zona de almacenamiento para alta disponibilidad, conecte al menos dos controladores de zonas de almacenamiento a ella. Para unir un controlador secundario de zonas de almacenamiento a una zona, instale un controlador de zonas de almacenamiento en un segundo servidor. Luego, una ese controlador a la zona del controlador principal.

1. Abra una ventana de PowerShell en el servidor del controlador de zonas de almacenamiento que desea unir al servidor principal.
2. En la ventana de PowerShell, escriba lo siguiente:

   ```
   Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
   ```

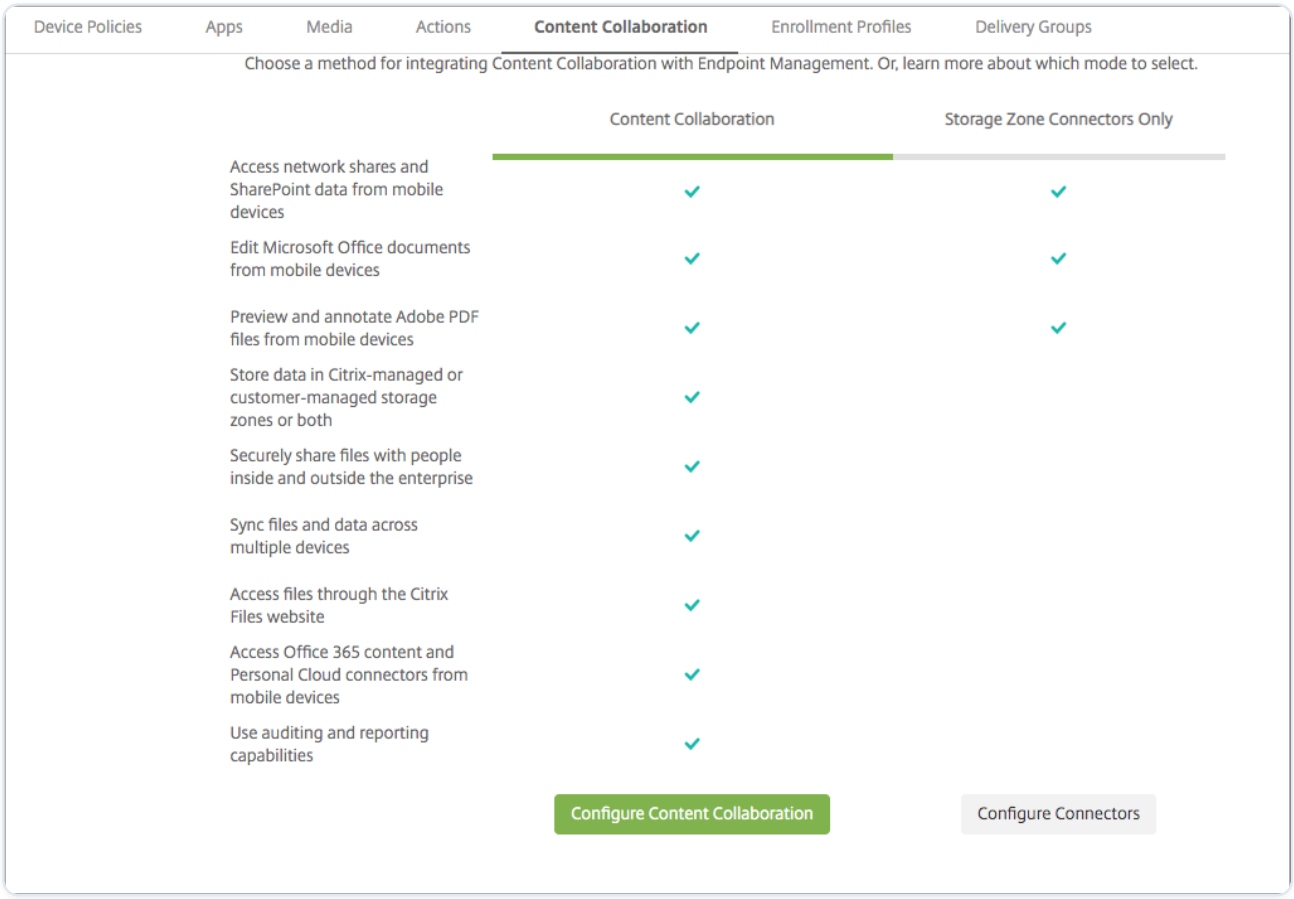
   Por ejemplo:

   ```
   Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
   ```

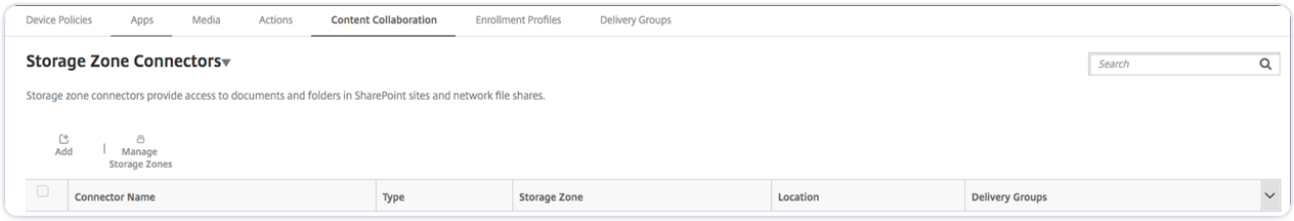
Definir conexiones del controlador de zonas de almacenamiento en Citrix Endpoint Management

Antes de añadir conectores de zona de almacenamiento, configure la información de conexión para cada controlador de zonas de almacenamiento habilitado para conectores de zona de almacenamiento. Puede definir los controladores de zonas de almacenamiento como se describe en esta sección, o al añadir un conector.

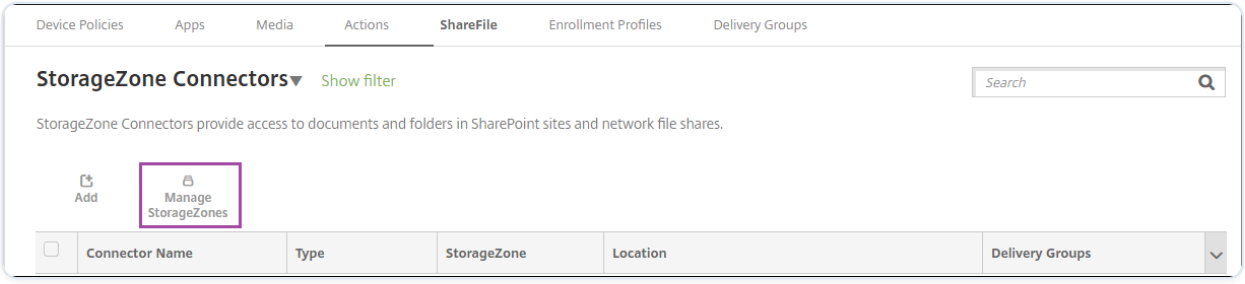
En su primera visita a la página **Configurar > ShareFile**, la página resume las diferencias entre el uso de Citrix Endpoint Management para cuentas de empresa y los conectores de zona de almacenamiento.



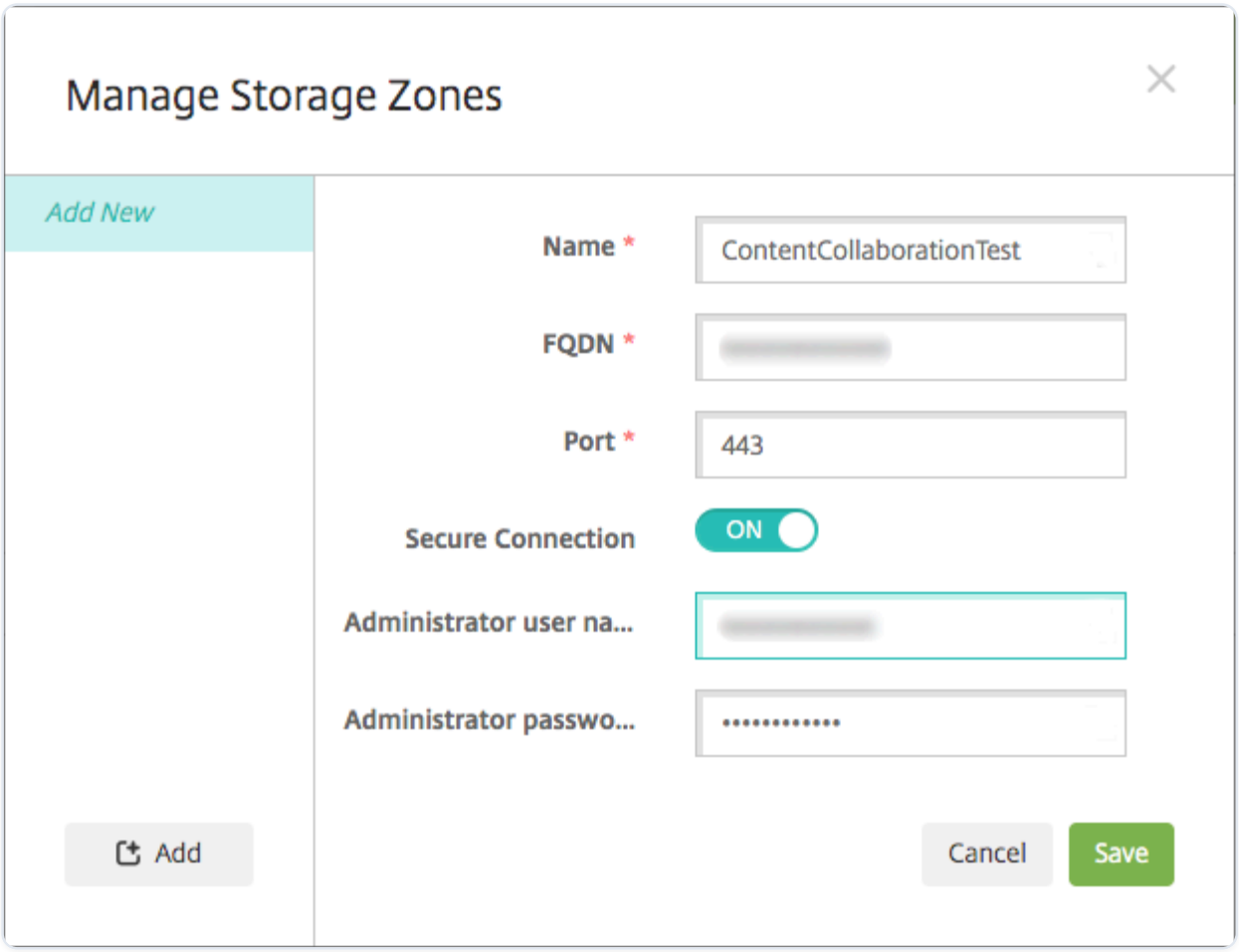
Haga clic en **Configurar conectores** para continuar con los pasos de configuración de este artículo.



1. En **Configurar > ShareFile**, haga clic en **Administrar zonas de almacenamiento**.



2. En **Administrar zonas de almacenamiento**, agregue la información de conexión.



- **Nombre:** Un nombre descriptivo para la zona de almacenamiento, utilizado para identificar la zona de almacenamiento en Citrix Endpoint Management. No incluya espacios ni caracteres especiales en el nombre.
- **FQDN y puerto:** El nombre de dominio completo y el número de puerto de un controlador de zonas de almacenamiento al que se pueda acceder desde el servidor de Citrix Endpoint Management.
- **Conexión segura:** Si utiliza SSL para las conexiones al controlador de zonas de almacenamiento, use la configuración predeterminada, Activado. Si no utiliza SSL para las conexiones, cambie esta configuración a Desactivado.
- **Nombre de usuario del administrador** y **Contraseña del administrador:** Un nombre de usuario de cuenta de servicio de administrador (con el formato domain\\admin) y una contraseña. O bien, una cuenta de usuario con permisos de lectura y escritura en los controladores de zonas de almacenamiento.

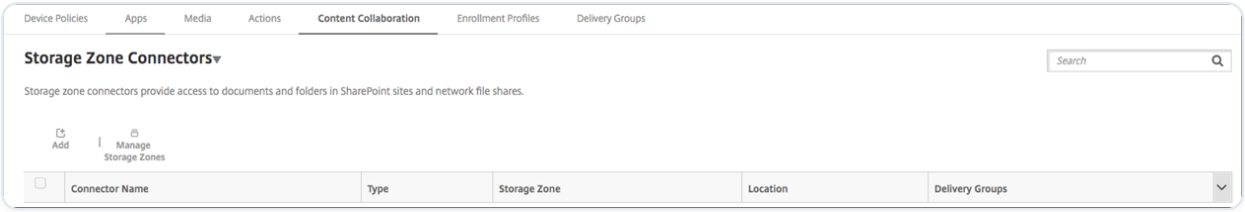
3. Haga clic en **Guardar**.
4. Para probar la conexión, verificar que el servidor de Citrix Endpoint Management pueda acceder al nombre de dominio completo del controlador de zonas de almacenamiento en el puerto 443.

5. Para definir otra conexión de controlador de zonas de almacenamiento, haga clic en el botón **Agregar** en **Administrar zonas de almacenamiento**.

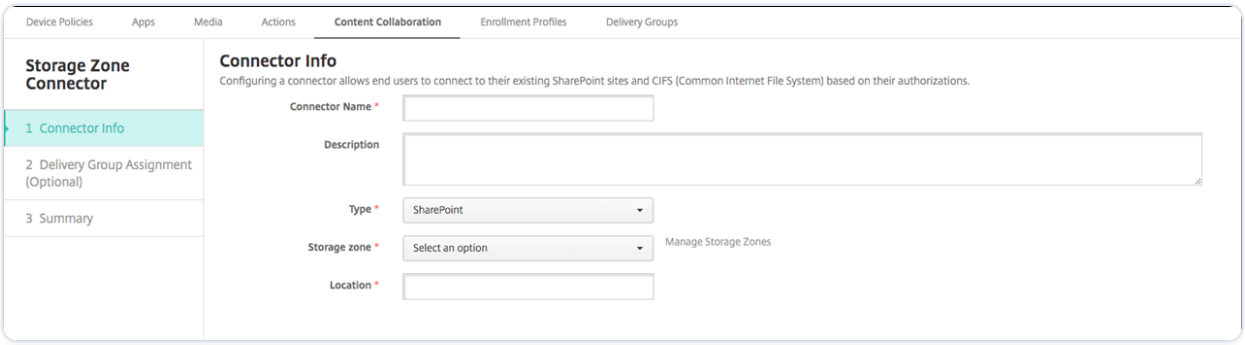
   Para modificar o eliminar la información de una conexión de controlador de zonas de almacenamiento, seleccione el nombre de la conexión en **Administrar zonas de almacenamiento**. A continuación, haga clic en **Modificar** o **Eliminar**.

Agregar un conector de zona de almacenamiento en Citrix Endpoint Management

1. Vaya a **Configurar > ShareFile** y, a continuación, haga clic en **Agregar**.

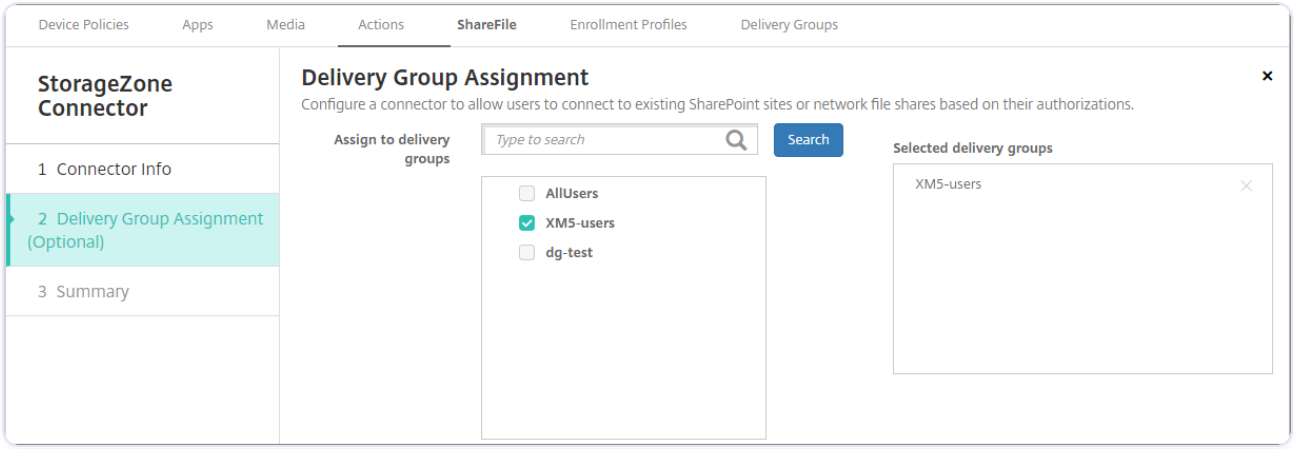


2. En la página **Información del conector**, configure estos parámetros:



   - **Nombre del conector:** Un nombre que identifica el conector de zona de almacenamiento en Citrix Endpoint Management.
   - **Descripción:** Notas opcionales sobre este conector.
   - **Tipo:** Elija **SharePoint** o **Red**.
   - **Zona de almacenamiento:** Elija la zona de almacenamiento asociada al conector. Si la zona de almacenamiento no aparece en la lista, haga clic en **Administrar zonas de almacenamiento** para definir el controlador de zonas de almacenamiento.
   - **Ubicación:** Para SharePoint, especifique la URL del sitio de nivel raíz de SharePoint, la colección de sitios o la biblioteca de documentos, con el formato `https://sharepoint.company.com`. Para un recurso compartido de red, especifique el nombre de dominio completo de la ruta de Convención de Nomenclatura Uniforme (UNC), con el formato \\\\server\\share.

3. En la página **Asignación de grupos de entrega**, asigne opcionalmente el Conector a los grupos de entrega. De lo contrario, puede asociar conectores a grupos de entrega mediante **Configurar > Grupos de entrega**.



1. En la página **Resumen**, puede revisar las opciones que configuró. Para ajustar la configuración, haga clic en **Atrás**.
2. Haga clic en **Guardar** para guardar el conector.
3. Pruebe el conector:

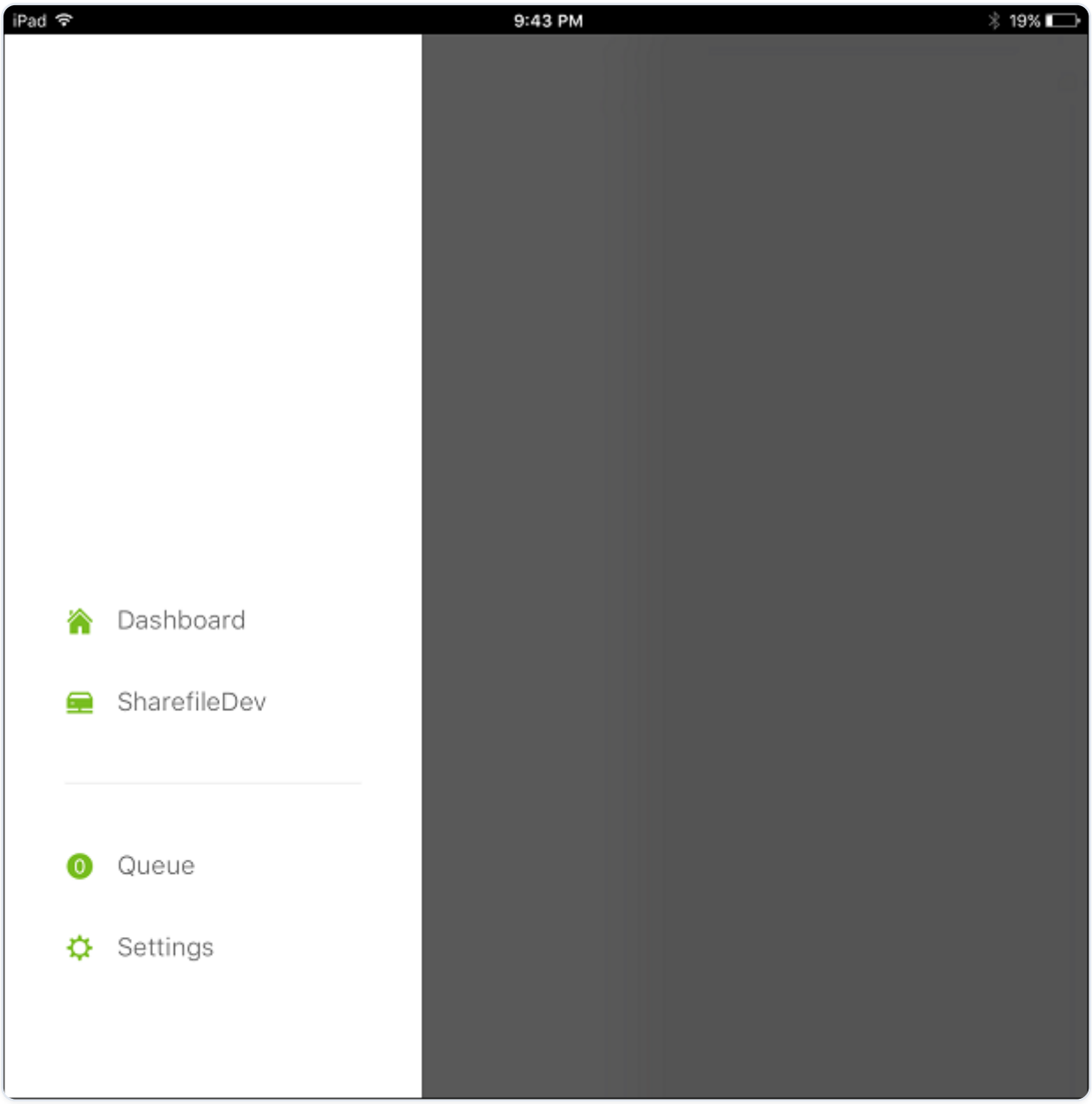
    a. Cuando encapsule los clientes de Citrix Files, establezca la directiva de acceso a la red en **Tunelizado - SSO web**.

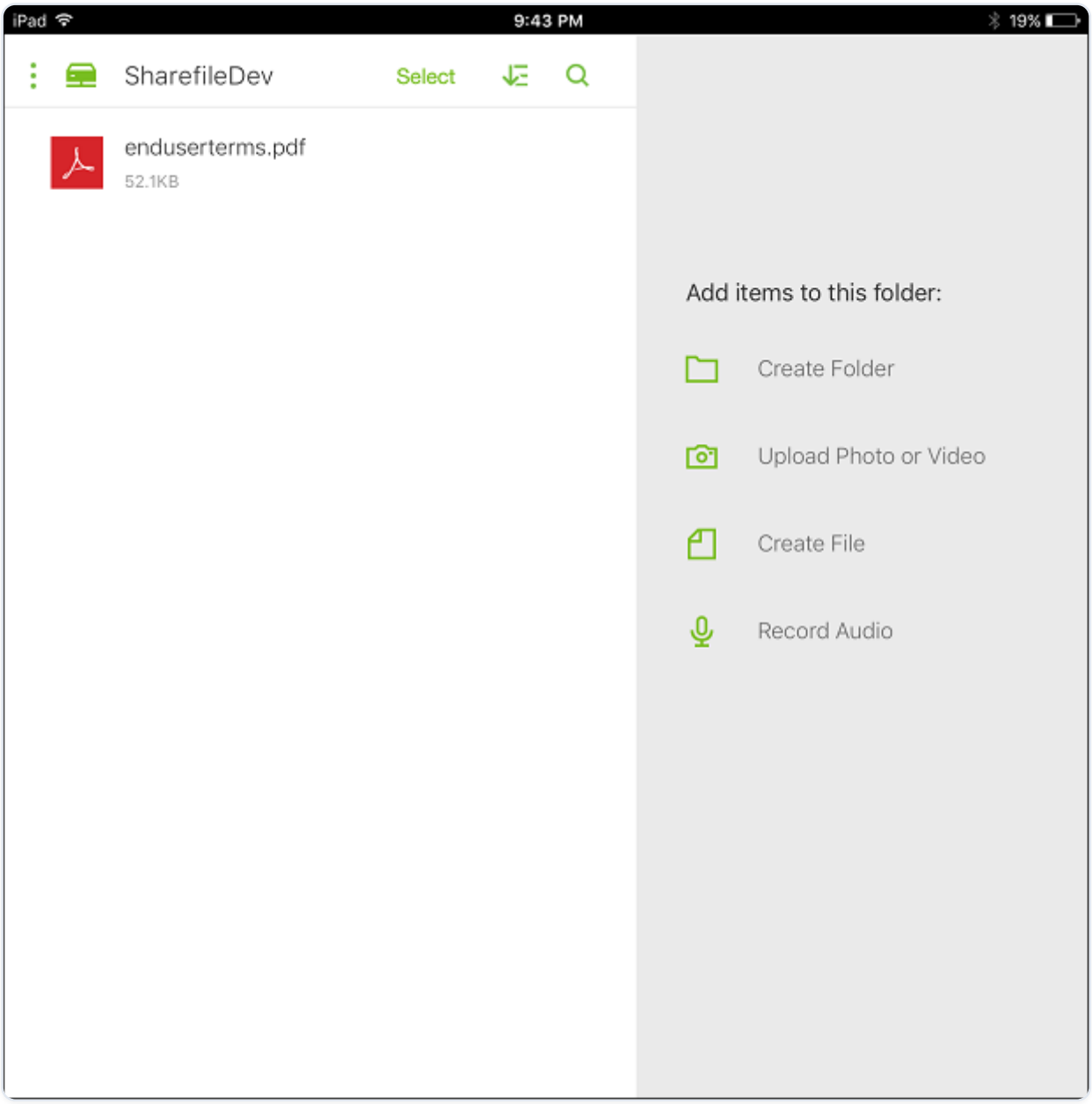
    En este modo de tunelización, el marco MDX finaliza el tráfico SSL/HTTP de una aplicación MDX. A continuación, MDX inicia nuevas conexiones a las conexiones internas para el usuario. Esta configuración de directiva permite que el marco MDX detecte y responda a los desafíos de autenticación emitidos por los servidores web.

    b. Agregue los clientes de Citrix Files a Citrix Endpoint Management. Para obtener más información, consulte Para agregar clientes de Citrix Files a Citrix Endpoint Management.

    c. Desde un dispositivo compatible, verificar el inicio de sesión único en Citrix Files y los conectores.

En los siguientes ejemplos, SharefileDev es el nombre de un conector.

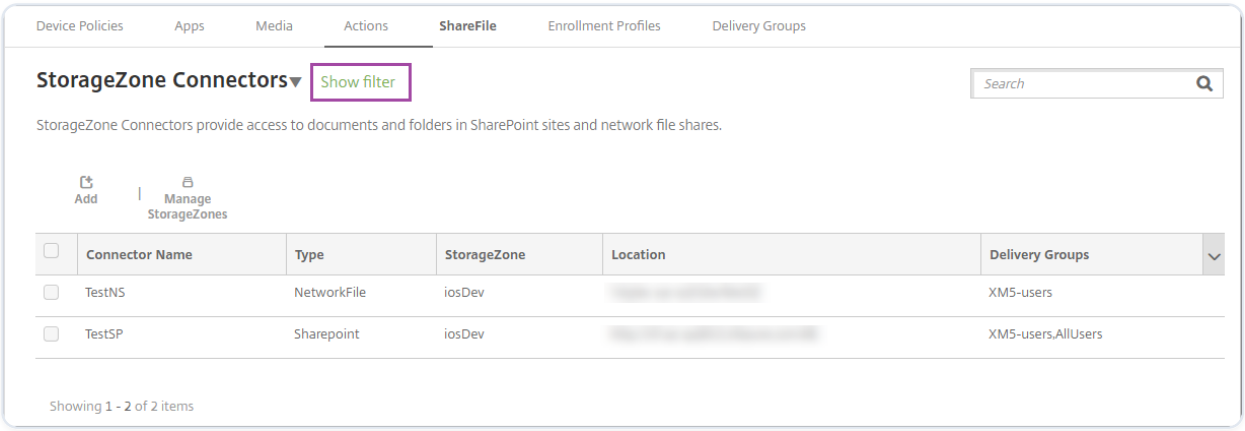

iPad
9:43 PM
19%
Dashboard
SharefileDev
Queue
0
Settings



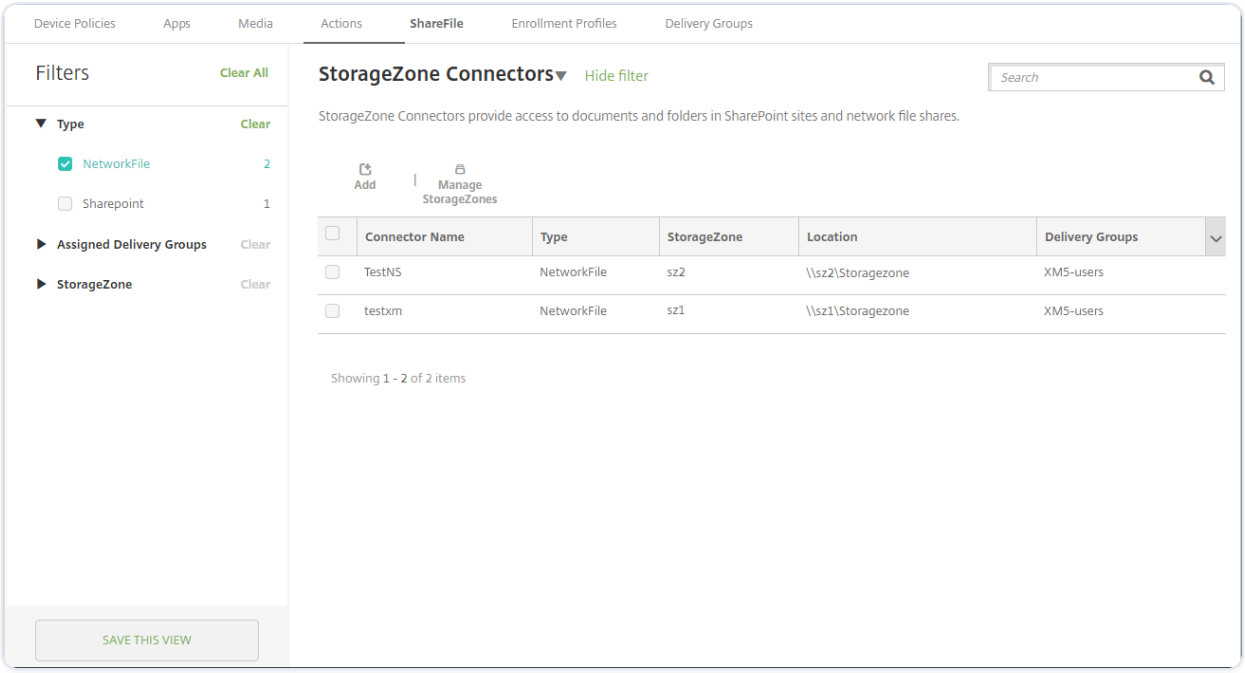
Filtrar la lista de conectores de zona de almacenamiento

Puede filtrar la lista de conectores de zona de almacenamiento por tipo de conector, grupos de entrega asignados y zona de almacenamiento.

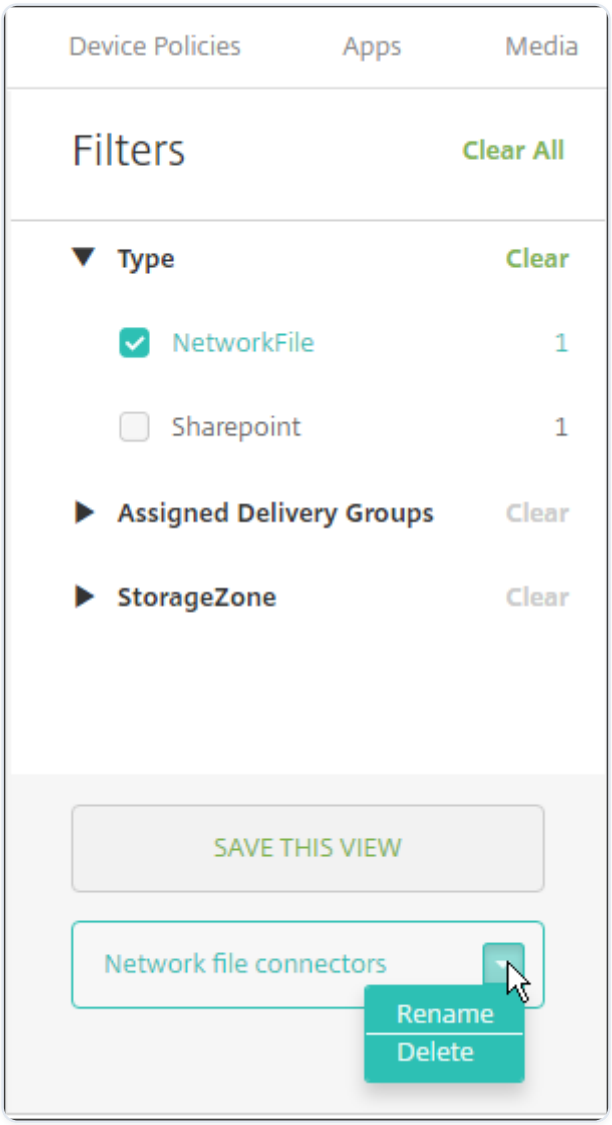
1. Vaya a **Configurar > ShareFile** y, a continuación, haga clic en **Mostrar filtro**.



2. Expanda los encabezados de filtro para hacer selecciones. Para guardar un filtro, haga clic en **Guardar esta vista**, escriba el nombre del filtro y haga clic en **Guardar**.



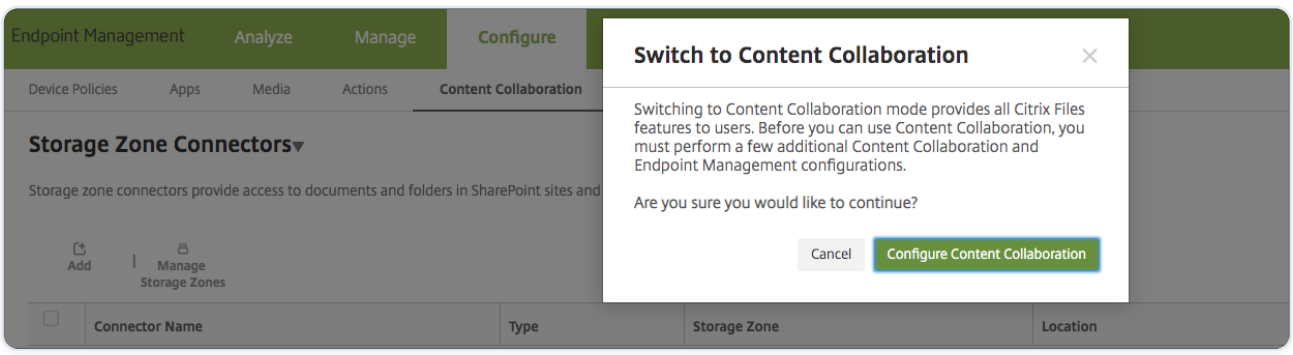
3. Para cambiar el nombre o eliminar un filtro, haga clic en el icono de flecha junto al nombre del filtro.



Cambiar a cuenta Enterprise

Después de integrar los conectores de zona de almacenamiento con Citrix Endpoint Management, puede cambiar más tarde al conjunto completo de funciones de Enterprise. Citrix Endpoint Management mantiene la configuración de integración de los conectores de zona de almacenamiento existentes.

Vaya a **Configurar > ShareFile**, haga clic en el menú desplegable **Conectores de zona de almacenamiento** y, a continuación, haga clic en **Configurar ShareFile**.



Para obtener información sobre cómo configurar cuentas Enterprise, consulte SAML para el inicio de sesión único con Citrix Files.

SmartAccess para aplicaciones HDX™

Esta función le permite controlar el acceso a las aplicaciones HDX en función de las propiedades del dispositivo, las propiedades de usuario de un dispositivo o las aplicaciones instaladas en un dispositivo. Utiliza esta función configurando acciones automatizadas para marcar el dispositivo como no conforme y denegarle el acceso. Las aplicaciones HDX utilizadas con esta función se configuran en Citrix Virtual Apps and Desktops mediante una directiva de SmartAccess que deniega el acceso a los dispositivos no conformes. Citrix Endpoint Management comunica el estado del dispositivo a StoreFront mediante una etiqueta firmada y cifrada. StoreFront permite o deniega el acceso en función de la directiva de control de acceso de la aplicación.

Para usar esta función, su implementación requiere:

- Citrix Aplicaciones y Escritorios Virtuales™
- Citrix Endpoint Management
- Citrix Endpoint Management configurado con un certificado SAML para firmar y cifrar etiquetas. El mismo certificado sin clave privada se carga en el servidor de StoreFront.

Para empezar a usar esta función:

- Configure el certificado del servidor de Citrix Endpoint Management en el almacén de StoreFront
- Configure al menos un grupo de entrega de Citrix Virtual Apps and Desktops con la directiva de SmartAccess requerida
- Establezca la acción automatizada en Citrix Endpoint Management

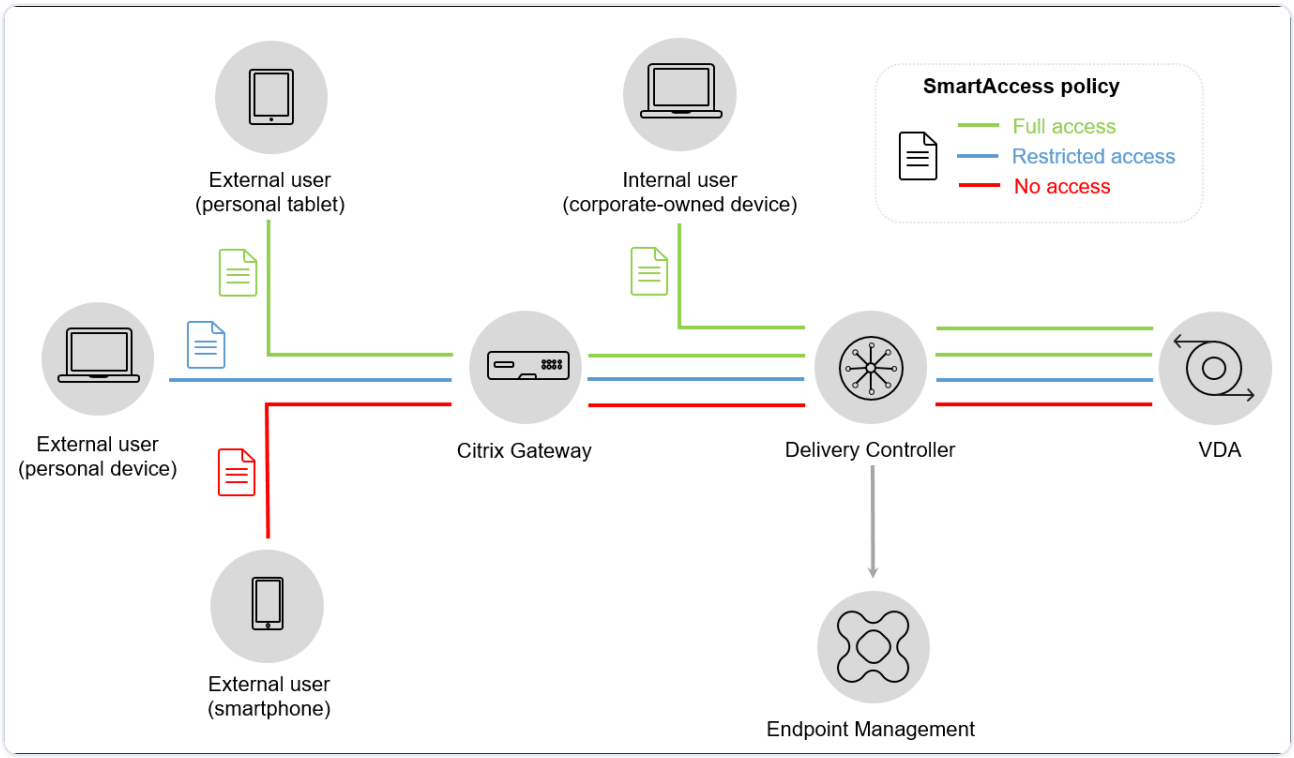
SmartAccess a aplicaciones HDX para puntos finales

Con esta función, puede aplicar un control de acceso basado en directivas para restringir el acceso de los dispositivos a las aplicaciones HDX. Puede aplicar estos niveles de acceso a las aplicaciones HDX:

- **Acceso total**. Un dispositivo puede acceder a todas las aplicaciones HDX que proporciona el almacén de Citrix Secure Hub.
- **Acceso restringido**. Un dispositivo puede acceder a una o varias aplicaciones HDX, pero no a todas.

- **Sin acceso**. Un dispositivo no puede acceder a ninguna aplicación HDX.

El siguiente gráfico ilustra cómo funciona el control de acceso. Un intento de iniciar una aplicación HDX en Citrix Secure Hub activa una solicitud a un Delivery Controller. El Delivery Controller reenvía la solicitud al servidor de Citrix Endpoint Management para su validación. El resultado de la validación determina el nivel de acceso que tiene el dispositivo. Por ejemplo, se deniega el acceso a una aplicación HDX si el dispositivo tiene jailbreak.



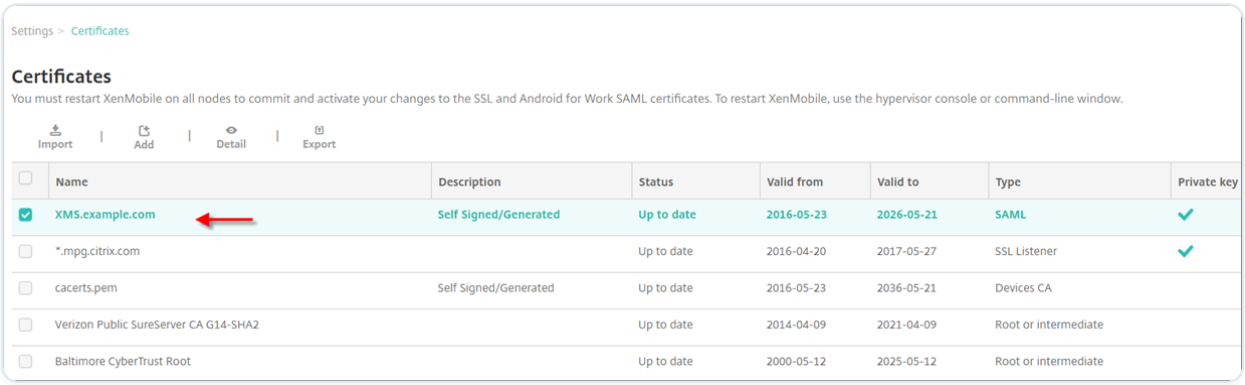
Exporte y configure el certificado del servidor de Citrix Endpoint Management y cárguelo en el almacén de StoreFront

SmartAccess utiliza etiquetas firmadas y cifradas para comunicarse entre los servidores de Citrix Endpoint Management y StoreFront. Para habilitar esa comunicación, debe agregar el certificado del servidor de Citrix Endpoint Management al almacén de StoreFront.

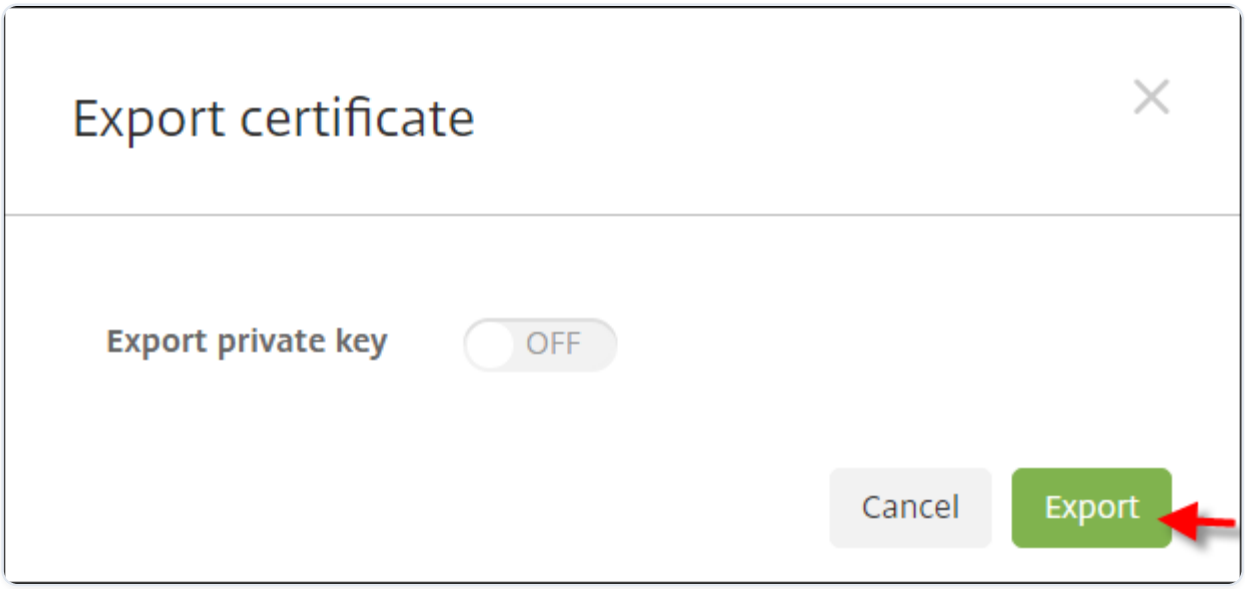
Para obtener más información sobre la integración de StoreFront y Citrix Endpoint Management cuando Citrix Endpoint Management está habilitado con autenticación basada en dominio y certificado, consulte el Centro de conocimientos de soporte.

Exportar el certificado SAML de Citrix Endpoint Management

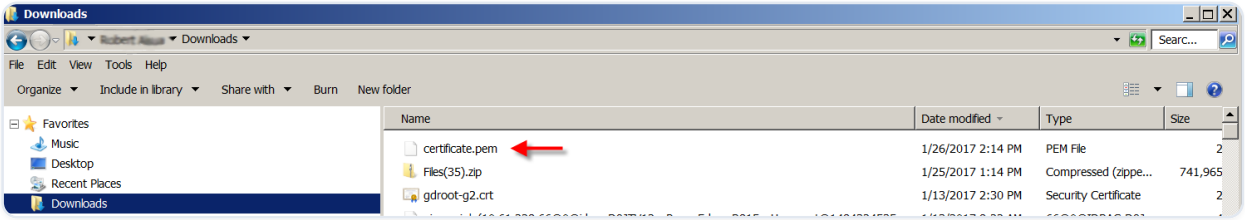
1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha. Aparece la página **Configuración**. Haga clic en **Certificados**.
2. Busque el certificado SAML del servidor de Citrix Endpoint Management.



3. Asegúrese de que **Exportar clave privada** esté establecido en **Desactivado**. Haga clic en **Exportar** para exportar el certificado a su directorio de descargas.

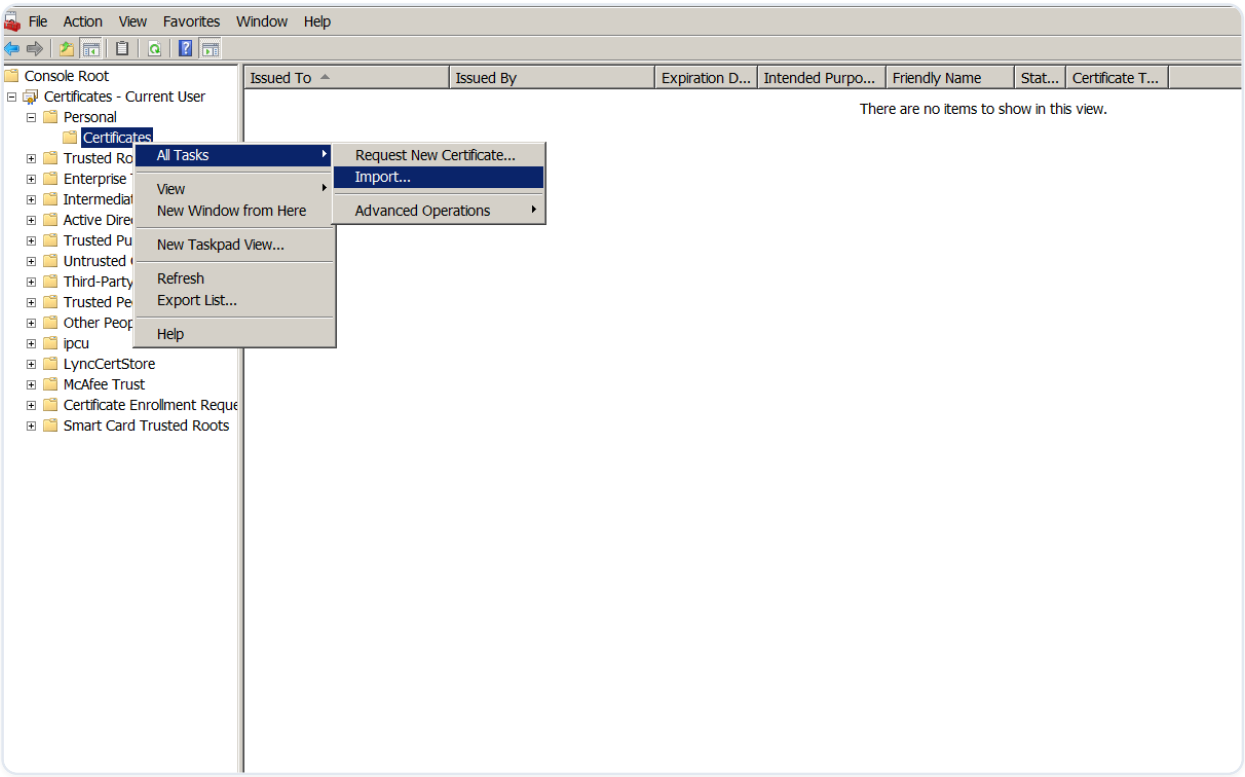


4. Busque el certificado en su directorio de descargas. El certificado está en formato PEM.

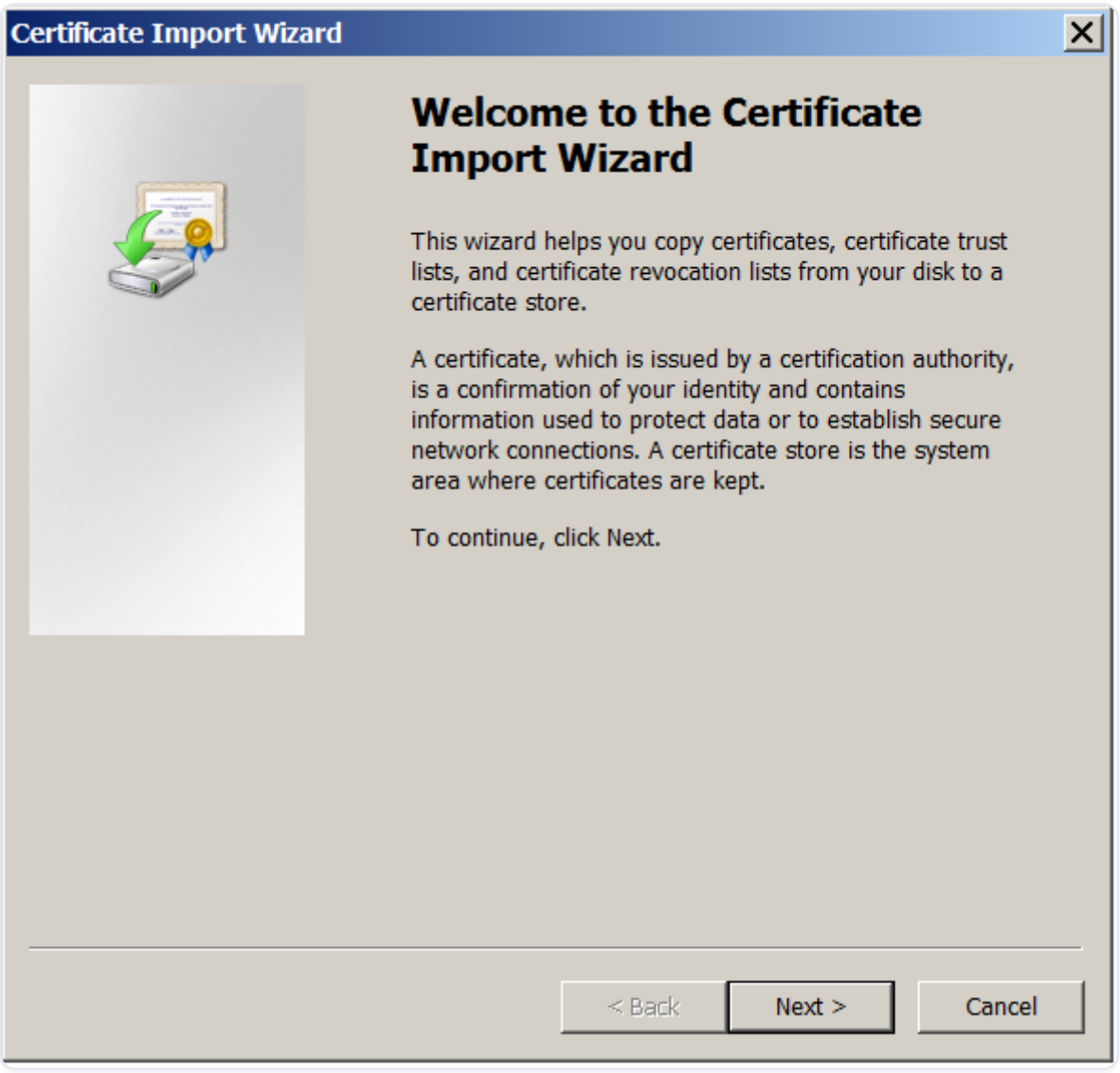


Convertir el certificado de PEM a CER

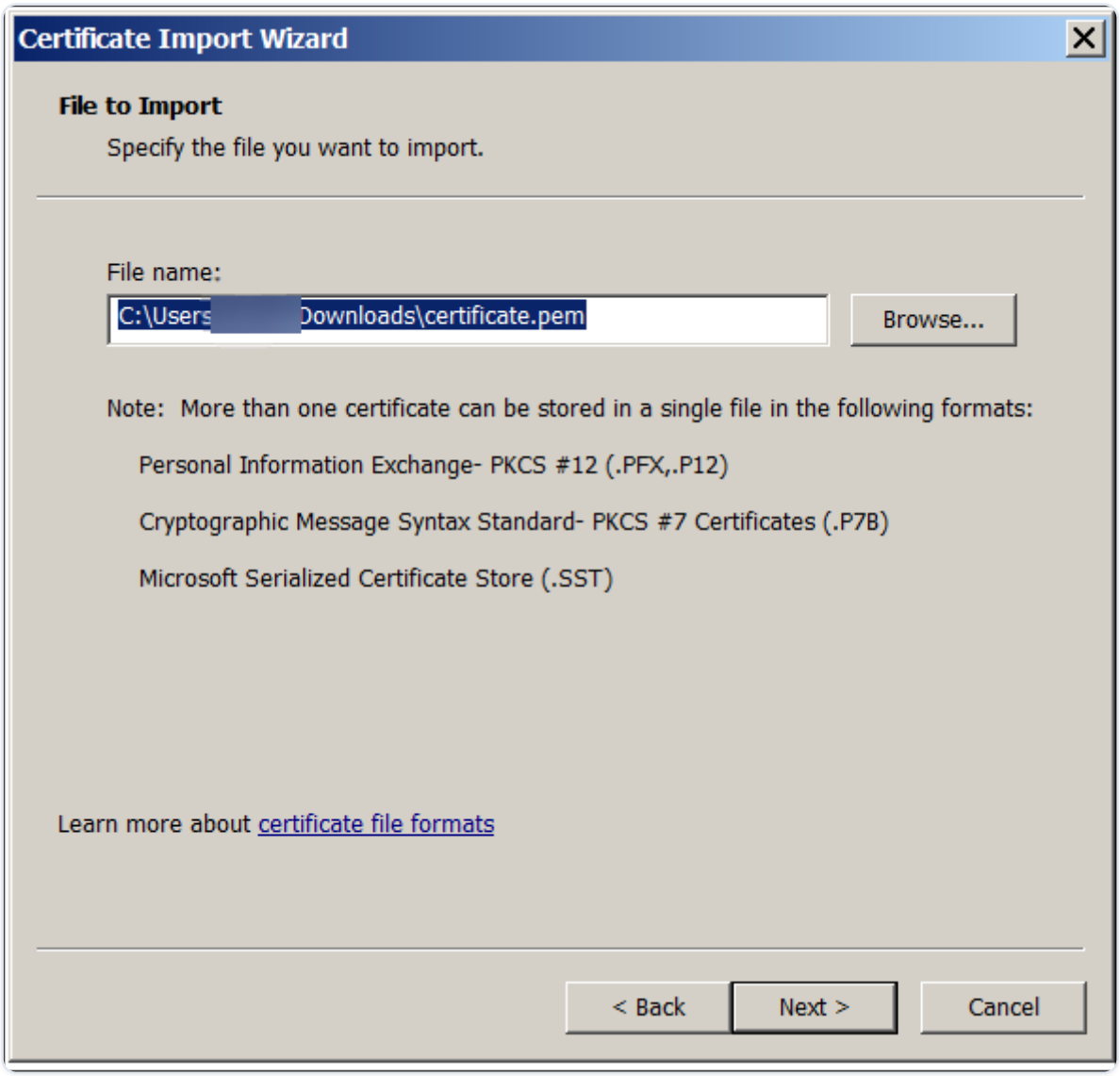
1. Abra la Consola de administración de Microsoft (MMC) y haga clic con el botón derecho en **Certificados > Todas las tareas > Importar**.



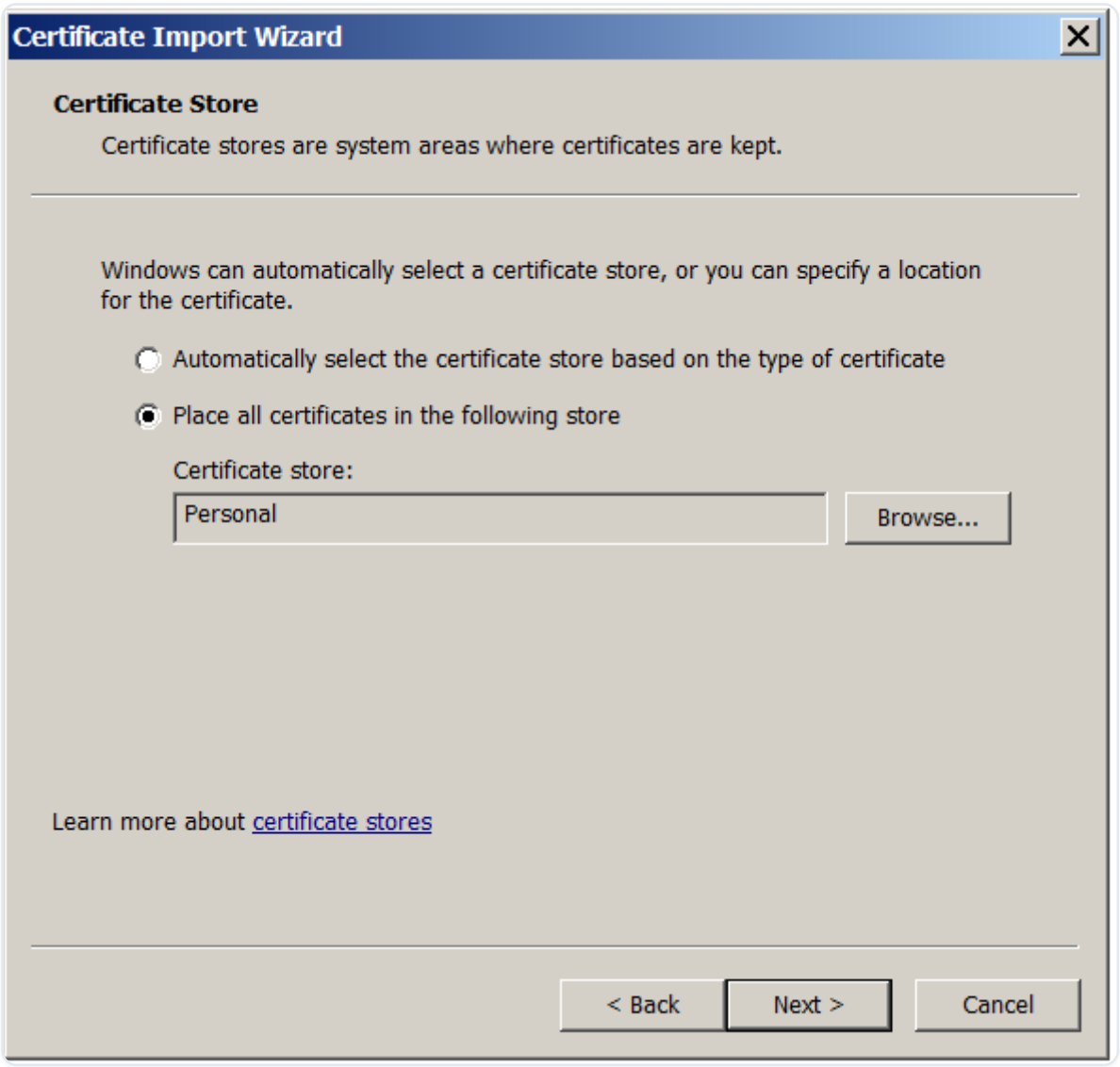
2. Cuando aparezca el asistente para la importación de certificados, haga clic en **Siguiente**.



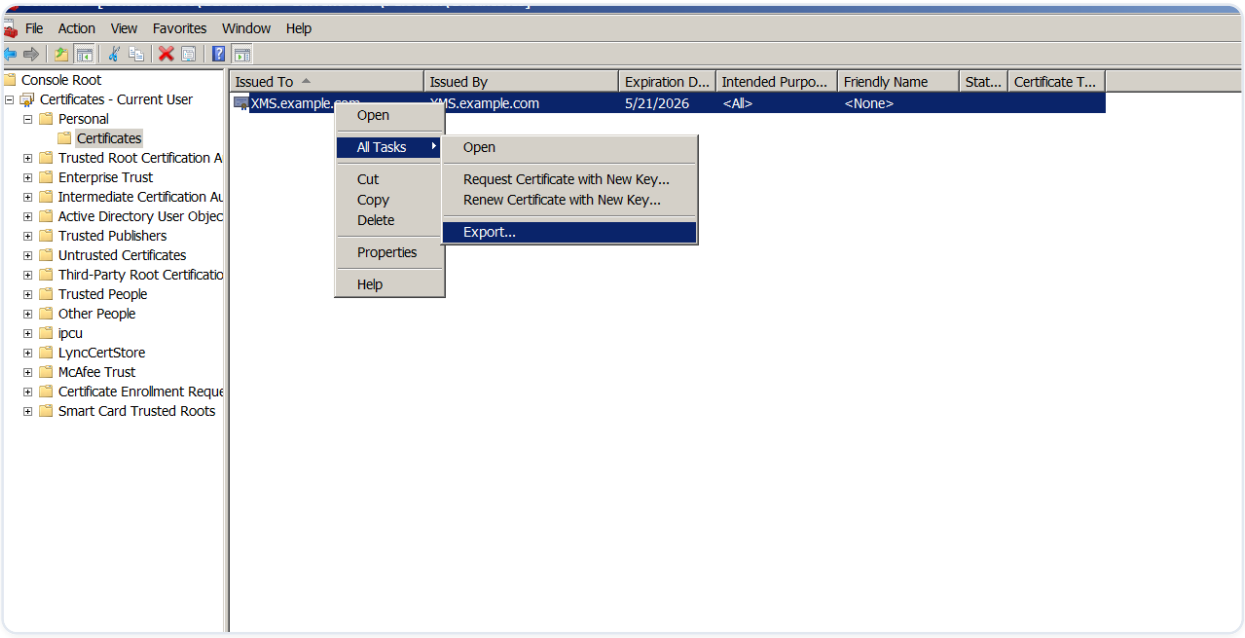
3. Busque el certificado en el directorio de descargas.



4. Seleccione **Colocar todos los certificados en el siguiente almacén** y seleccione **Personal** como almacén de certificados. Haga clic en **Siguiente**.



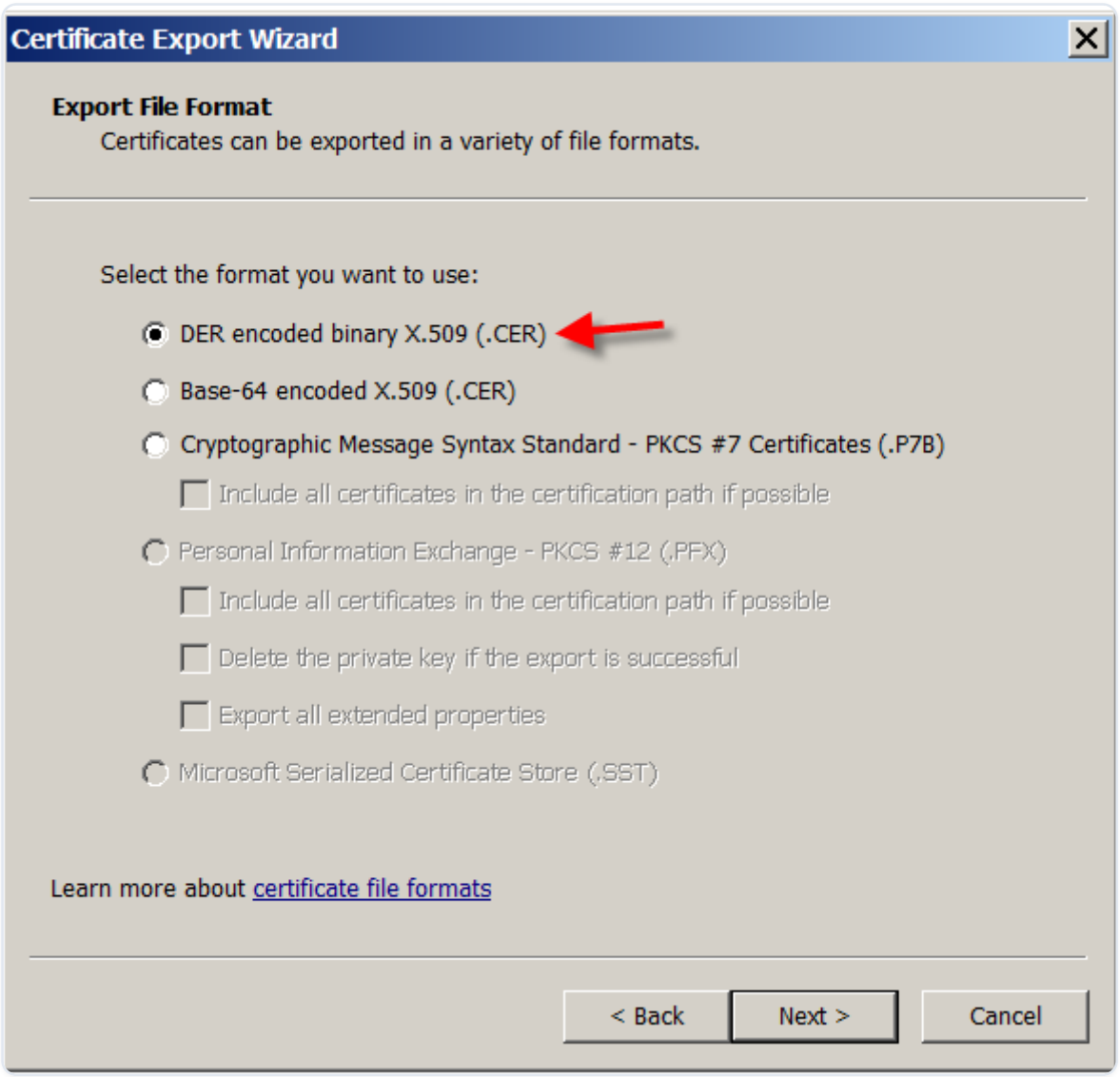
5. Revise sus selecciones y haga clic en **Finalizar**. Haga clic en **Aceptar** para cerrar la ventana de confirmación.
6. En la MMC, haga clic con el botón derecho en el certificado y, a continuación, elija **Todas las tareas > Exportar**.



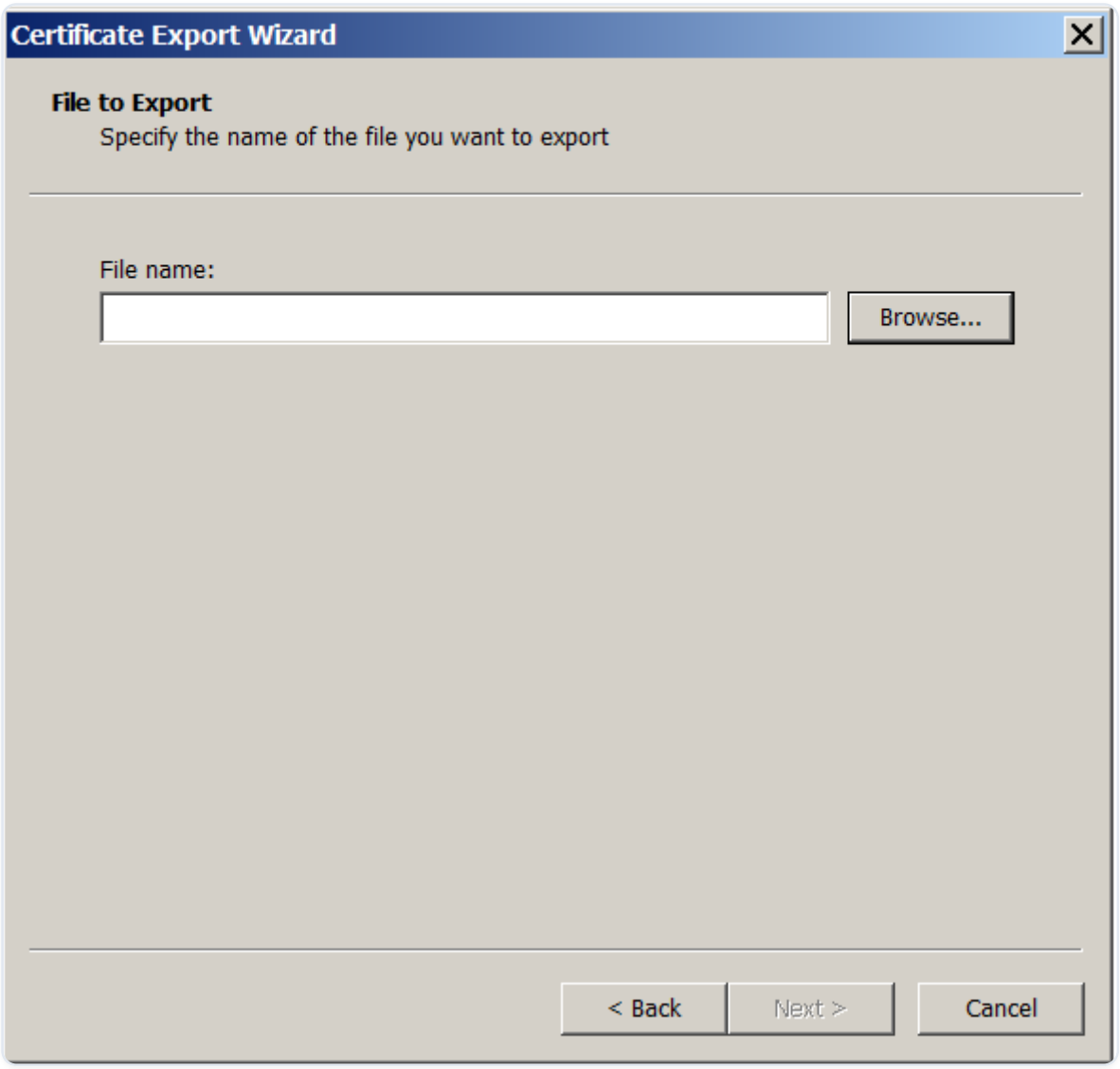
7. Cuando aparezca el asistente para la exportación de certificados, haga clic en **Siguiente**.



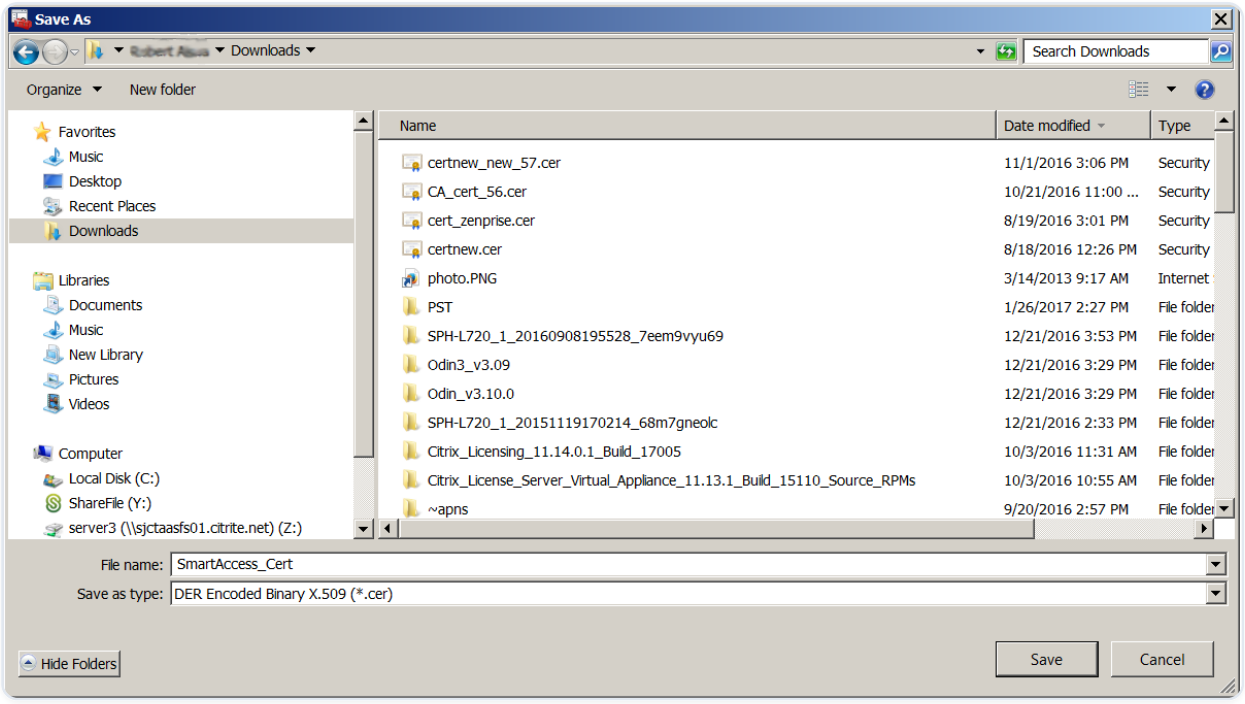
8. Elija el formato **X.509 binario codificado en DER (.CER)**. Haga clic en **Siguiente**.



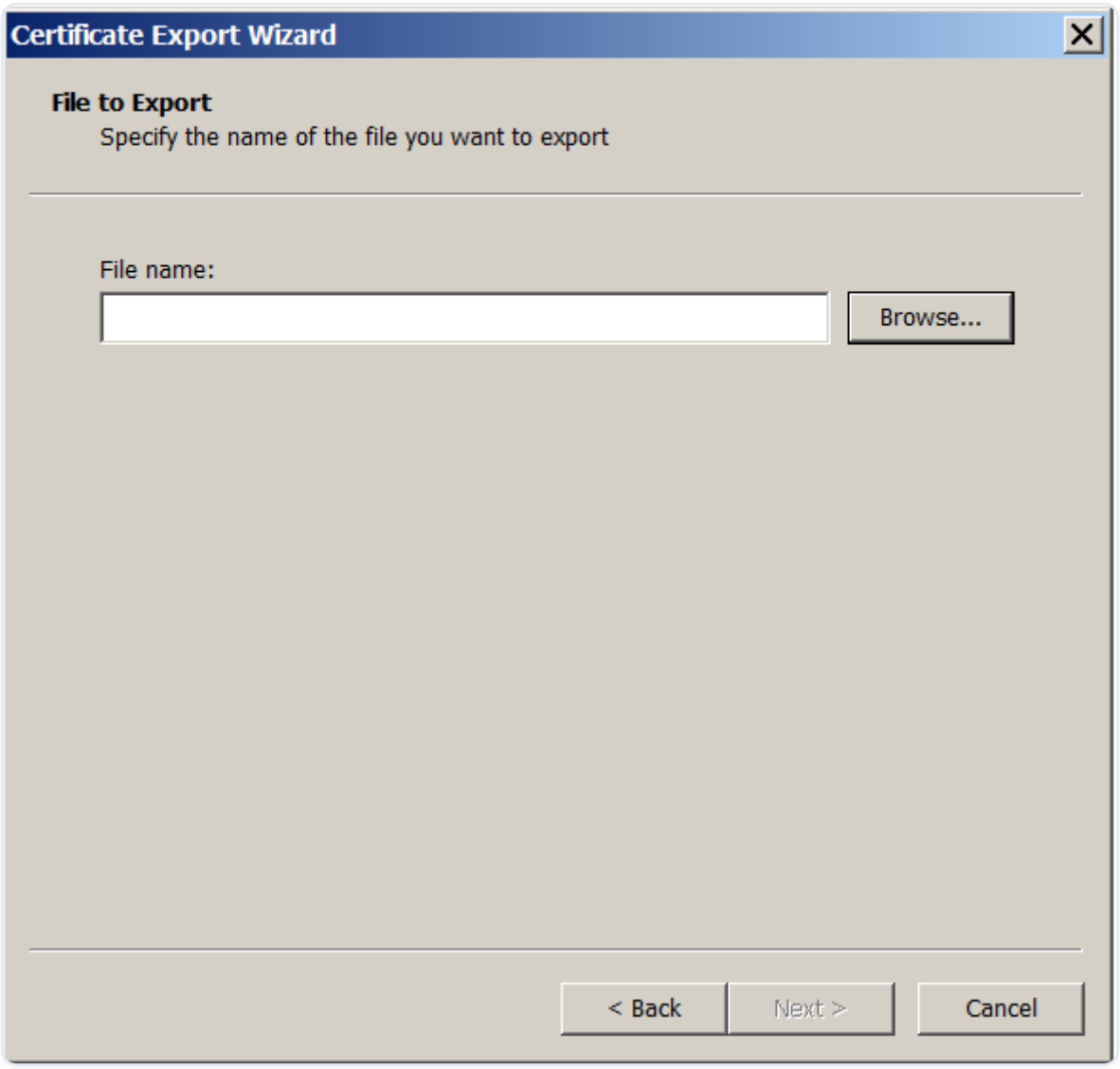
9. Busque el certificado. Escriba un nombre para el certificado y, a continuación, haga clic en **Siguiente**.



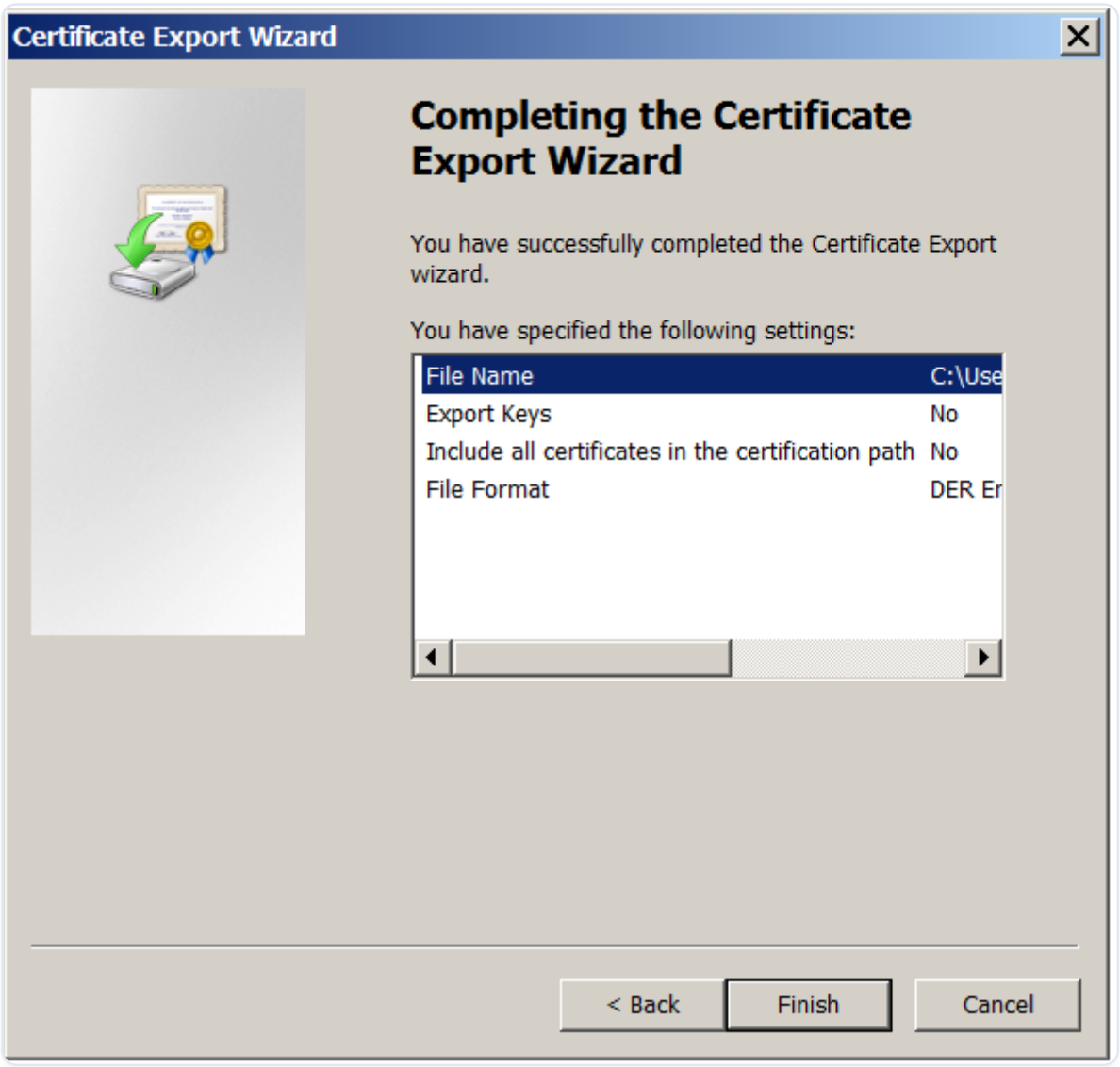
10. Guarde el certificado.



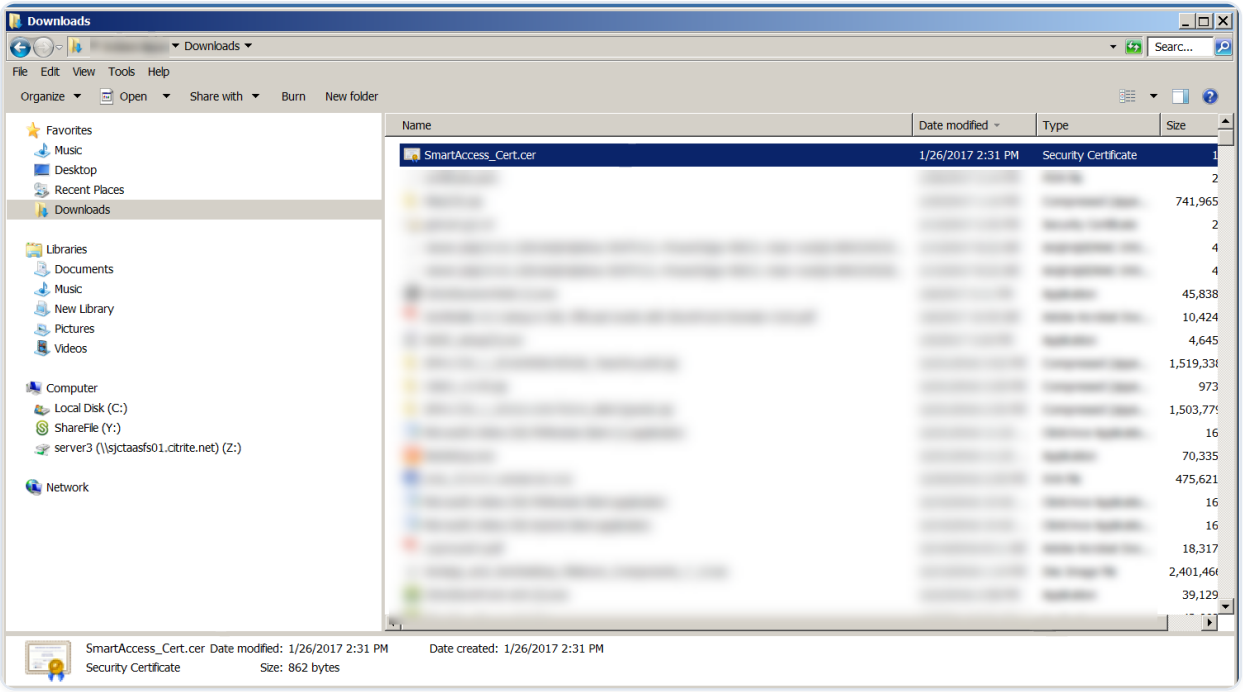
11. Busque el certificado y haga clic en **Siguiente**.



12. Revise sus selecciones y haga clic en **Finalizar**. Haga clic en **Aceptar** para cerrar la ventana de confirmación.

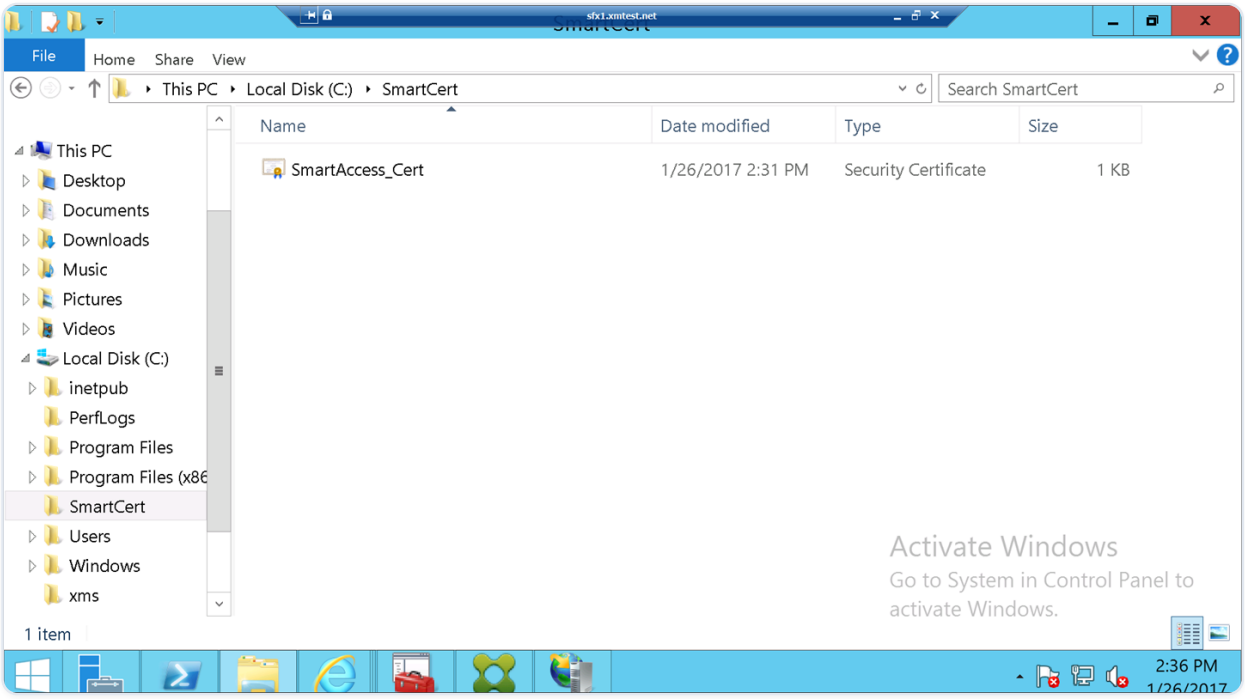


13. Localice el certificado en su directorio de descargas. El certificado está en formato CER.



Copiar el certificado al servidor de StoreFront

1. En el servidor de StoreFront, cree una carpeta llamada **SmartCert**.
2. Copie el certificado a la carpeta **SmartCert**.



Configurar el certificado en el almacén de StoreFront

En el servidor de StoreFront, ejecute este comando de PowerShell para configurar el certificado del servidor de Citrix Endpoint Management convertido en el almacén:

```
Grant-STFStorePnaSmartAccess –StoreService $store –CertificatePath  “C:\xms\xms.cer” –ServerName “XMS server”
```

Configuración de SmartAccess(/en-us/citrix-endpoint-management/media/upload-cert-storefront.png)

Si hay certificados existentes en el almacén de StoreFront, ejecute este comando de PowerShell para revocarlos:

```
Revoke-STFStorePnaSmartAccess –StoreService $store –All
```

Configuración de SmartAccess(/en-us/citrix-endpoint-management/media/revoke-certs-storefront.png)

De lo contrario, puede ejecutar cualquiera de estos comandos de PowerShell en el servidor de StoreFront para revocar los certificados existentes en el almacén de StoreFront:

- Revocar por nombre:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    Revoke-STFStorePnaSmartAccess –StoreService $store –ServerName “My XM Server"
```

- Revocar por huella digital:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    Revoke-STFStorePnaSmartAccess –StoreService $store –CertificateThumbprint "[Thumbprint]
```

- Revocar por objeto de servidor:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    $access = Get-STFStorePnaSmartAccess –StoreService $store



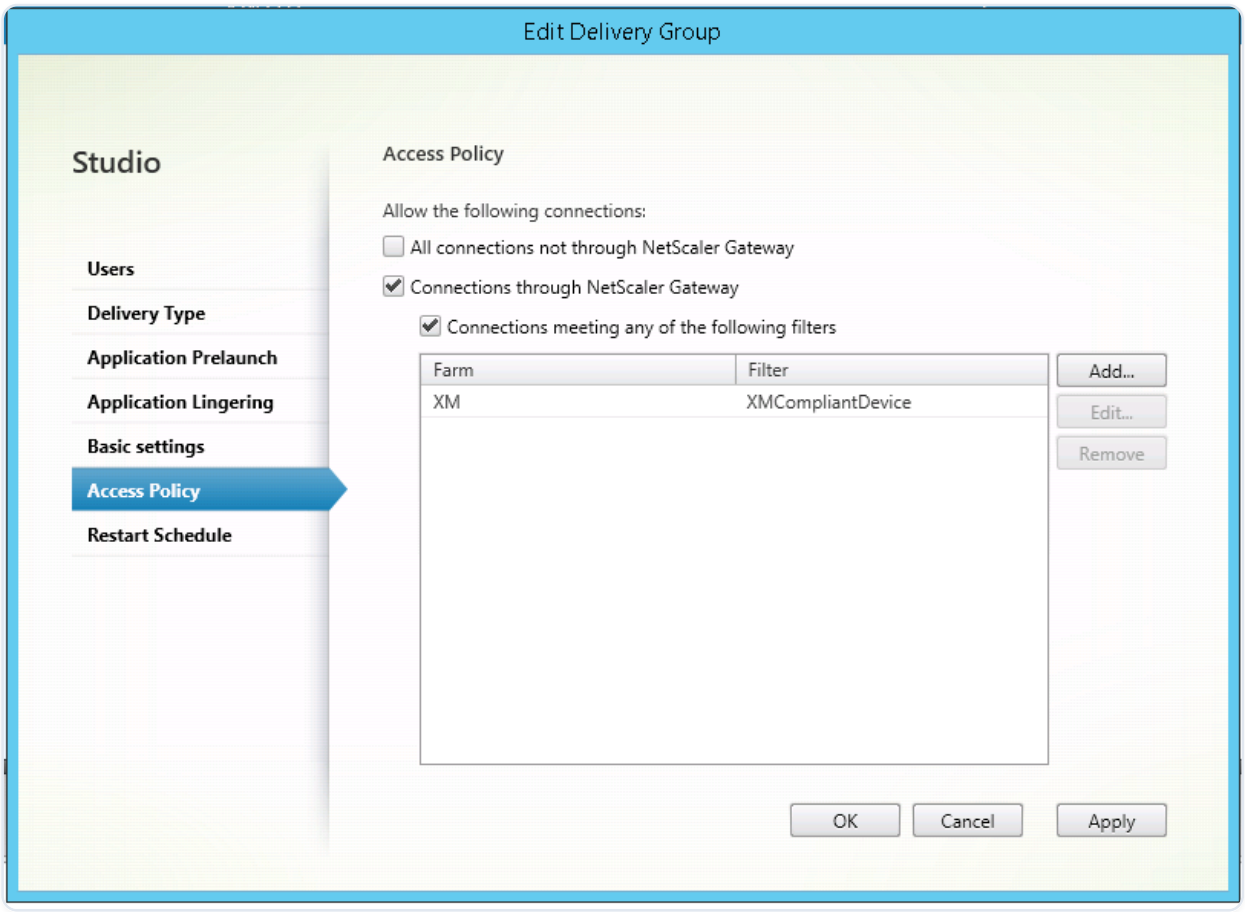
    Revoke-STFStorePnaSmartAccess –StoreService $store –SmartAccess $access.AccessConditionsTrusts[0]
```

Configurar la directiva SmartAccess para Citrix Virtual Apps and Desktops

Para agregar la directiva SmartAccess necesaria al grupo de entrega que distribuye la aplicación HDX:

1. Abra Citrix Studio desde la consola de Citrix Cloud.
2. Seleccione **Grupos de entrega** en el panel de navegación de Studio.

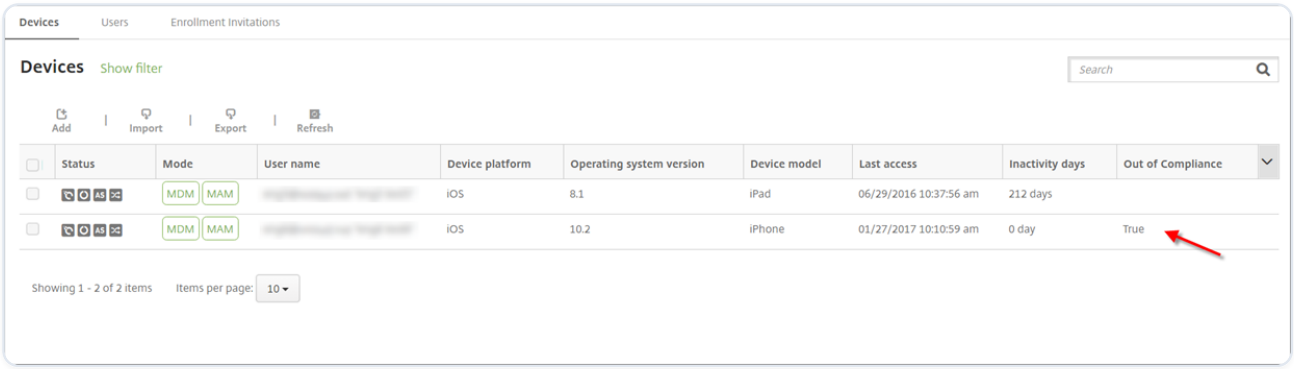
3. Seleccione un grupo que entregue las aplicaciones a las que desea controlar el acceso. A continuación, seleccione **Editar grupo de entrega** en el panel **Acciones**.
4. En la página **Directiva de acceso**, seleccione **Conexiones a través de NetScaler Gateway** y **Conexión que cumpla cualquiera de los siguientes requisitos**.
5. Haga clic en **Agregar**.
6. Agregue una directiva de acceso donde **Granja** sea **XM** y **Filtro** sea **XMCompliantDevice**.



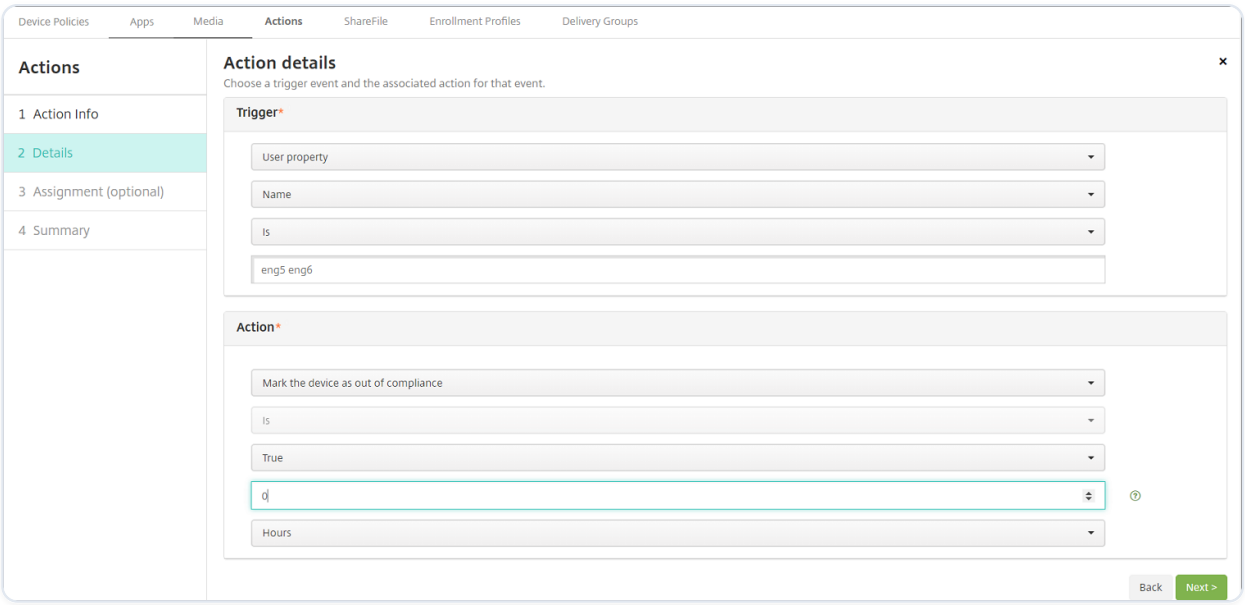
7. Haga clic en **Aplicar** para aplicar los cambios realizados y mantener la ventana abierta, o haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Establecer acciones automatizadas en Citrix Endpoint Management

La directiva de SmartAccess que estableció en el grupo de entrega para una aplicación HDX deniega el acceso a un dispositivo cuando este no cumple con la normativa. Utilice acciones automatizadas para marcar el dispositivo como no conforme.



1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Acciones**. Aparece la página **Acciones**.
2. Haga clic en **Agregar** para añadir una acción. Aparece la página **Información de la acción**.
3. En la página **Información de la acción**, escriba un nombre y una descripción para la acción.
4. Haga clic en **Siguiente**. Aparece la página **Detalles de la acción**. En el siguiente ejemplo, se crea un desencadenador que marca inmediatamente los dispositivos como no conformes si tienen el nombre de propiedad de usuario **eng5** o **eng6**.



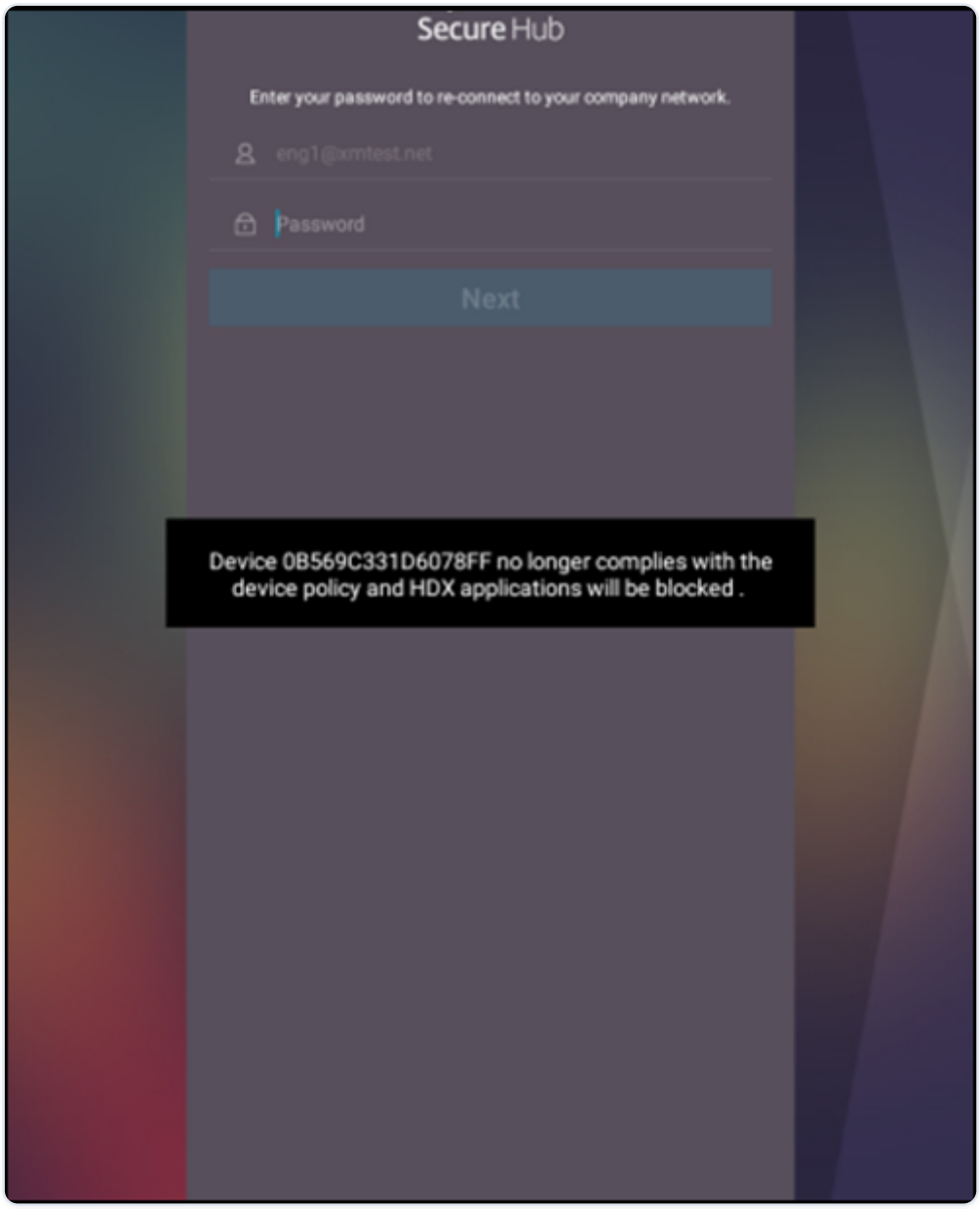
5. En la lista **Desencadenador**, elija **Propiedad del dispositivo**, **Propiedad del usuario** o **Nombre de la aplicación instalada**. SmartAccess no admite desencadenadores de eventos.
6. En la lista **Acción**:
   - Elija **Marcar el dispositivo como no conforme**.
   - Elija **Es**.
   - Elija **Verdadero**.
   - Para establecer la acción de marcar el dispositivo como no conforme inmediatamente cuando se cumpla la condición de activación, establezca el plazo en **0**.

7. Elija el grupo o los grupos de entrega de Citrix Endpoint Management a los que aplicar esta acción.
8. Revise el resumen de la acción.
9. Haga clic en **Siguiente** y, a continuación, en **Guardar**.

Cuando el dispositivo se marca como no conforme, las aplicaciones HDX ya no aparecen en la tienda de Citrix Secure Hub. El usuario ya no está suscrito a la aplicación. No se envía ninguna notificación al dispositivo y nada en la tienda de Citrix Secure Hub indica que las aplicaciones HDX estaban disponibles anteriormente.

Si quiere que se notifique a los usuarios cuando un dispositivo se marca como no conforme, cree una notificación y, a continuación, cree una acción automatizada para enviar esa notificación.

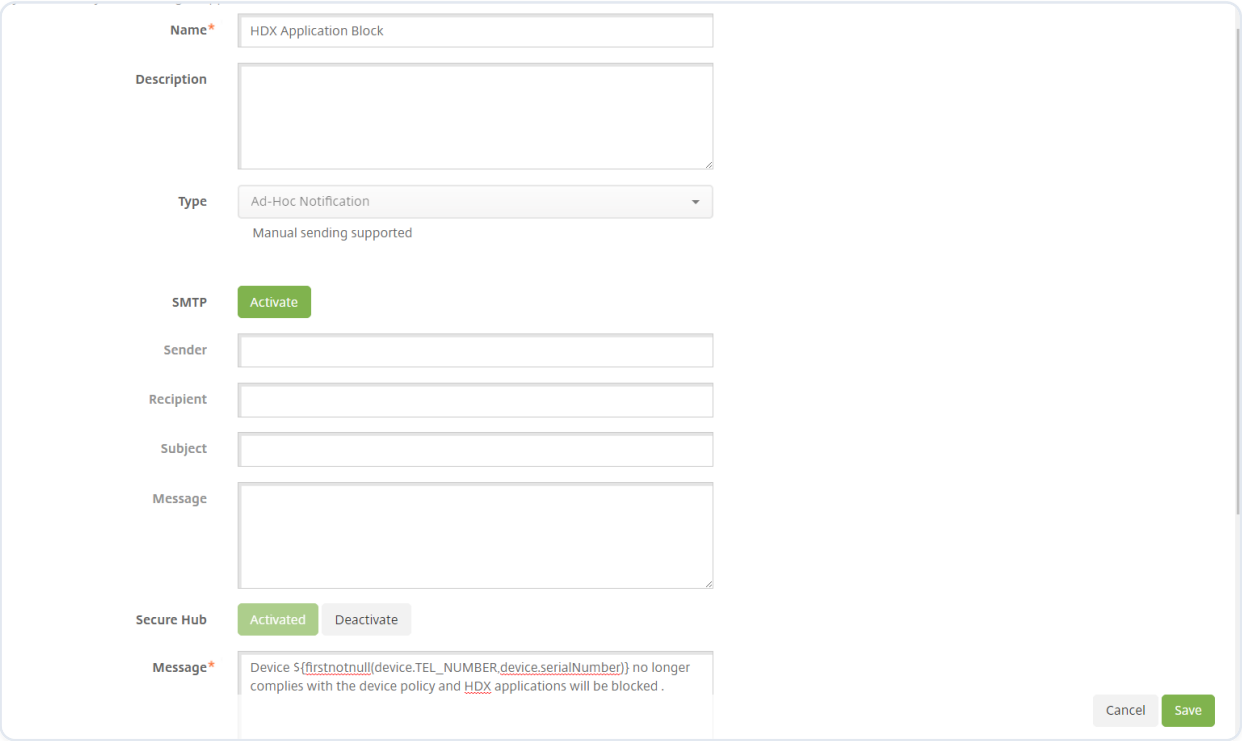
Este ejemplo crea y envía esta notificación cuando un dispositivo se marca como no conforme: "El número de serie o el número de teléfono del dispositivo ya no cumple la directiva del dispositivo y las aplicaciones HDX están bloqueadas".



Crear la notificación que ven los usuarios cuando un dispositivo se marca como no conforme

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje de la esquina superior derecha de la consola. Aparece la página **Parámetros**.
2. Haga clic en **Plantillas de notificación**. Aparece la página **Plantillas de notificación**.
3. Haga clic en **Agregar** en la página **Plantillas de notificación**.
4. Configure estos parámetros:
    - **Nombre:** Bloqueo de aplicaciones HDX
    - **Descripción:** Notificación del agente cuando un dispositivo no es conforme
    - **Tipo:** Notificación ad hoc

- **Citrix Secure Hub:** Activado
- **Mensaje:** El dispositivo `$ {firstnotnull(device.TEL_NUMBER,device.serialNumber)}` ya no cumple la directiva de dispositivos y las aplicaciones HDX están bloqueadas.

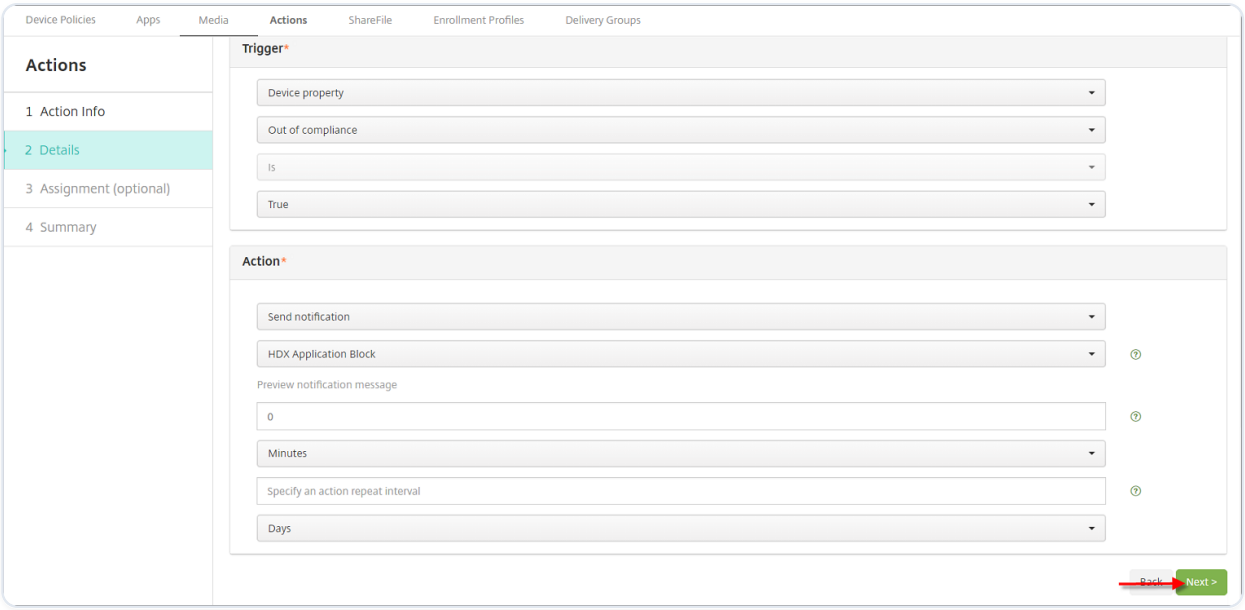


5. Haga clic en **Guardar**.

Crear la acción que envía la notificación cuando un dispositivo se marca como no conforme

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Acciones**. Aparecerá la página **Acciones**.
2. Haga clic en **Agregar** para añadir una acción. Aparecerá la página **Información de la acción**.
3. En la página **Información de la acción**, introduzca un nombre y una descripción para la acción:
   - Nombre: Notificación de HDX bloqueado
   - **Descripción:** Notificación de HDX bloqueado porque el dispositivo no cumple la normativa
4. Haga clic en **Siguiente**. Aparecerá la página **Detalles de la acción**.
5. En la lista **Desencadenador**:
   - Elija **Propiedad del dispositivo**.
   - Elija **No conforme**.

- Elija **Es**.
- Elija **Verdadero**.



6. En la lista **Acción**, especifique las acciones que se producen cuando se cumple el desencadenador:
   - Elija **Enviar notificación**
   - Elija **Bloqueo de aplicación HDX, la notificación que creó**.
   - Elija **0**. Establecer este valor en 0 hace que la notificación se envíe cuando se cumpla la condición del desencadenador.
7. Seleccione el grupo o grupos de entrega de Citrix Endpoint Management a los que aplicar esta acción. En este ejemplo, elija **Todos los usuarios**.
8. Revise el resumen de la acción.
9. Haga clic en **Siguiente** y, a continuación, haga clic en **Guardar**.

Para obtener más información sobre cómo configurar acciones automatizadas, consulte Acciones automatizadas.

Cómo los usuarios recuperan el acceso a las aplicaciones HDX

Los usuarios pueden volver a acceder a las aplicaciones HDX una vez que el dispositivo vuelve a cumplir las normativas:

1. En el dispositivo, vaya a la tienda de Citrix Secure Hub para actualizar las aplicaciones de la tienda.
2. Vaya a la aplicación y toque **Agregar** a la aplicación.

Después de añadir la aplicación, aparece en Mis aplicaciones con un punto azul al lado, porque es una aplicación recién instalada.

Configuración de SmartAccess(/en-us/citrix-endpoint-management/media/secure-hub-app-added.png)

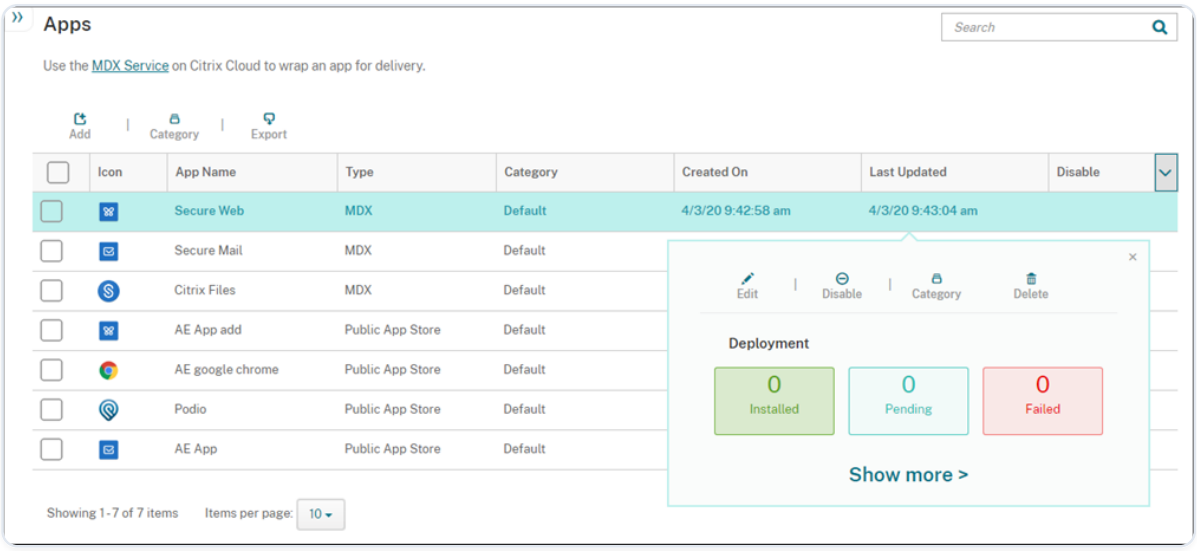
Actualizar aplicaciones MDX o empresariales

Para actualizar una aplicación MDX o empresarial en Citrix Endpoint Management, deshabilite la aplicación en la consola de Citrix Endpoint Management y, a continuación, cargue la nueva versión de la aplicación.

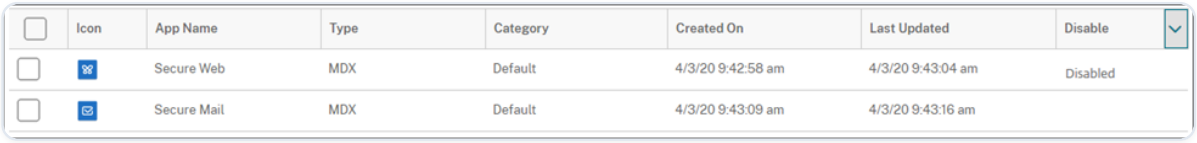
1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones**. Aparece la página **Aplicaciones**.
2. Para dispositivos administrados (dispositivos inscritos en Citrix Endpoint Management para la Administración de dispositivos móviles), vaya al Paso 3. Para dispositivos no administrados (dispositivos inscritos en Citrix Endpoint Management solo para fines de administración de aplicaciones empresariales), haga lo siguiente:

    a. En la tabla **Aplicaciones**, marque la casilla de verificación junto a la aplicación o haga clic en la línea que contiene la aplicación que desea actualizar.

    b. Haga clic en **Deshabilitar** en el menú que aparece.



    c. Haga clic en **Deshabilitar** en el cuadro de diálogo de confirmación. *Deshabilitada* aparece en la columna **Deshabilitar** de la aplicación.



> **Nota:**
>
> Mientras la aplicación está deshabilitada, los usuarios no pueden volver a conectarse a ella después de cerrar sesión. Deshabilitar una aplicación es opcional, pero recomendamos deshabilitarla para evitar problemas de funcionalidad de la aplicación. Por ejemplo, los usuarios que soliciten descargar la aplicación al mismo tiempo que usted carga la nueva versión podrían generar un problema.

3. En la tabla **Aplicaciones**, marque la casilla de verificación junto a la aplicación o haga clic en la línea que contiene la aplicación que desea actualizar.
4. Haga clic en **Modificar** en el menú que aparece. Aparece la página **Información de la aplicación** con las plataformas que eligió originalmente para la aplicación seleccionadas.
5. Configure estos ajustes:
   - **Nombre:** Opcionalmente, cambie el nombre de la aplicación.
   - **Descripción:** Opcionalmente, cambie la descripción de la aplicación.
   - **Categoría de la aplicación:** Opcionalmente, cambie la categoría de la aplicación.
6. Haga clic en **Siguiente**. Aparece la primera página de la plataforma seleccionada. Haga lo siguiente para cada plataforma seleccionada:
   a. Elija el archivo de reemplazo que desea cargar haciendo clic en **Cargar** y navegando a la ubicación del archivo. La aplicación se carga en Citrix Endpoint Management.

      Si va a cargar una aplicación para Android Enterprise, aparece una ventana de Google Play administrado. Cargue aquí la nueva versión de la aplicación. Para obtener más información, consulte Distribuir aplicaciones de Android Enterprise.
   b. Opcionalmente, cambie los detalles de la aplicación y la configuración de directivas para la plataforma.
   c. Opcionalmente, configure las reglas de implementación y la tienda de aplicaciones. Para obtener información, consulte Agregar una aplicación MDX.
7. Haga clic en **Guardar**. Aparece la página **Aplicaciones**.
8. Si inhabilitó la aplicación en el Paso 2, haga lo siguiente:
   a. En la tabla **Aplicaciones**, haga clic para seleccionar la aplicación que actualizó y, a continuación, en el menú que aparece, haga clic en **Habilitar**.

b. En el cuadro de diálogo de confirmación que aparece, haga clic en **Habilitar**. Ahora los usuarios pueden acceder a la aplicación y recibir una notificación que les pide que actualicen la aplicación.

Añadir multimedia

Agregue contenido multimedia a Citrix Endpoint Management para poder implementarlo en los dispositivos de los usuarios. Puede usar Citrix Endpoint Management para implementar libros de Apple que obtenga a través de la Compra por volumen de Apple.

Después de configurar una cuenta de Compra por volumen en Citrix Endpoint Management, los libros comprados y gratuitos aparecen en **Configurar** > **Contenido multimedia**. Desde las páginas de **Contenido multimedia**, puede configurar libros para su implementación en dispositivos iOS eligiendo grupos de entrega y especificando reglas de implementación.

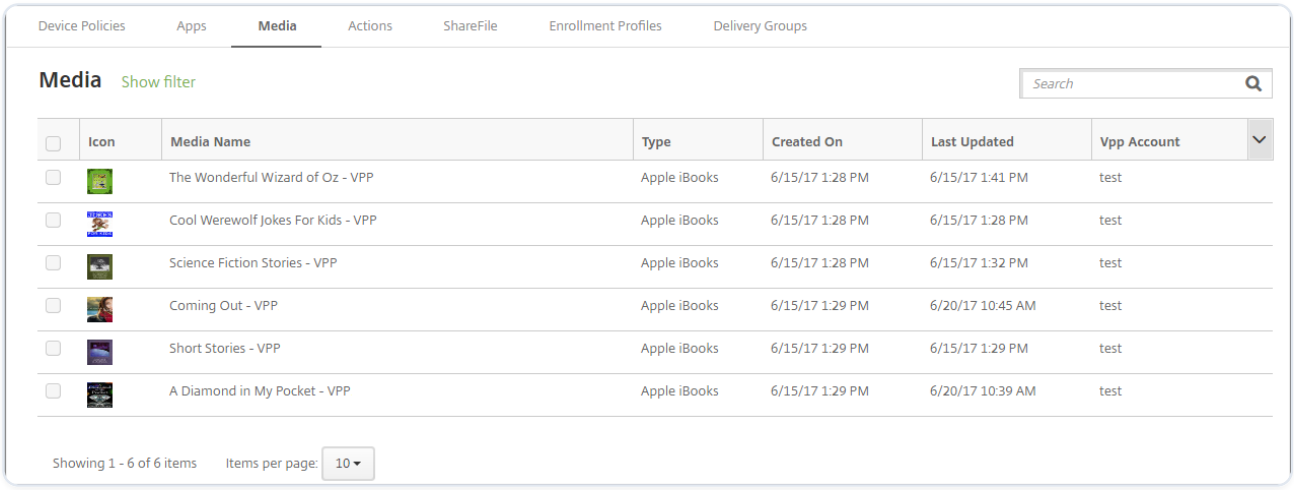
La primera vez que un usuario recibe un libro y acepta la licencia de Compra por volumen, los libros implementados se instalan en el dispositivo. Los libros aparecen en la aplicación Libros de Apple. No puede desasociar la licencia del libro del usuario ni eliminar el libro del dispositivo. Citrix Endpoint Management instala los libros como contenido multimedia obligatorio. Si un usuario elimina un libro instalado de su dispositivo, el libro permanece en la aplicación Libros de Apple, listo para descargar.

Requisitos previos

- Dispositivos iOS
- Configure la Compra por volumen de Apple en Citrix Endpoint Management, tal como se describe en Compra por volumen de Apple.

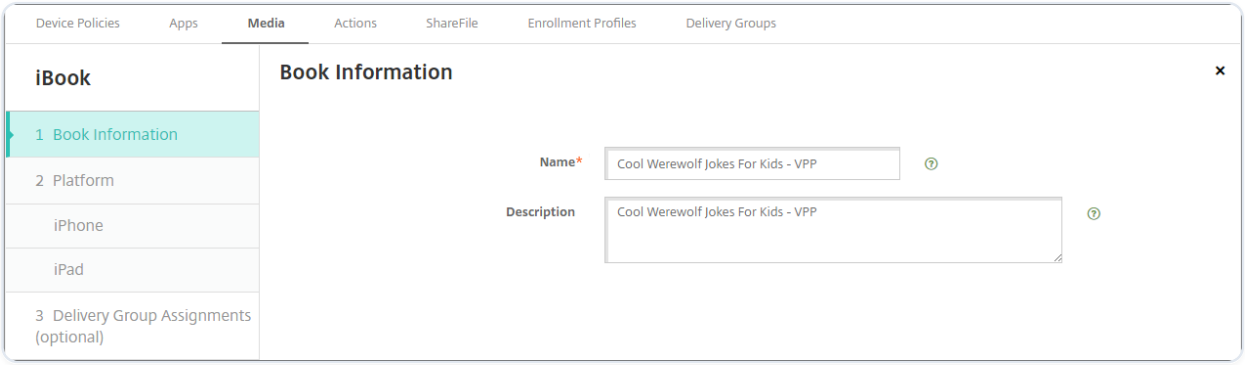
Configurar libros

Los libros de Apple obtenidos a través de la Compra por volumen aparecen en la página **Configurar** > **Contenido multimedia**.



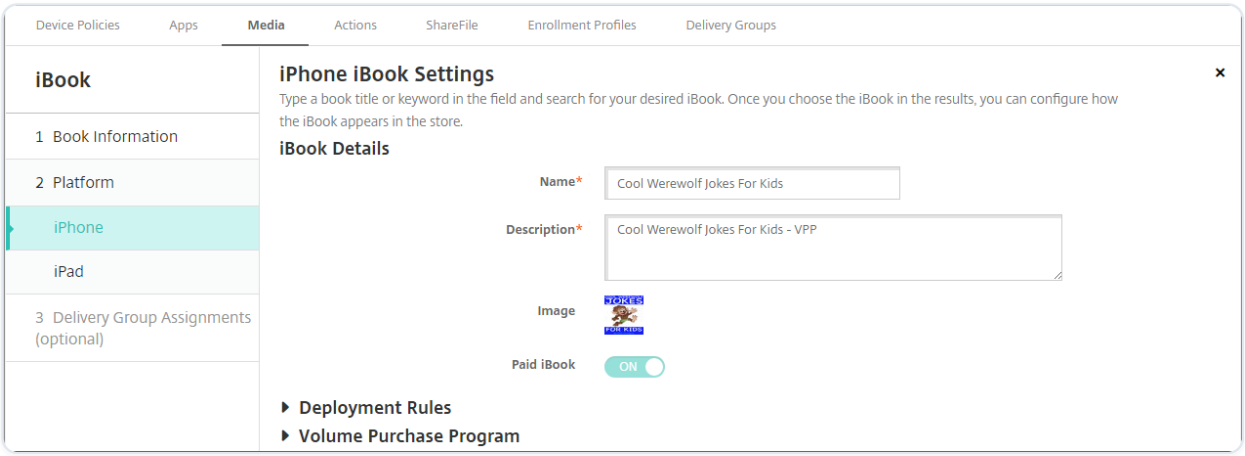
Para configurar un libro de Apple para su implementación

1. En **Configurar > Contenido multimedia**, seleccione un libro y haga clic en **Editar**. Aparecerá la página **Información del libro**.

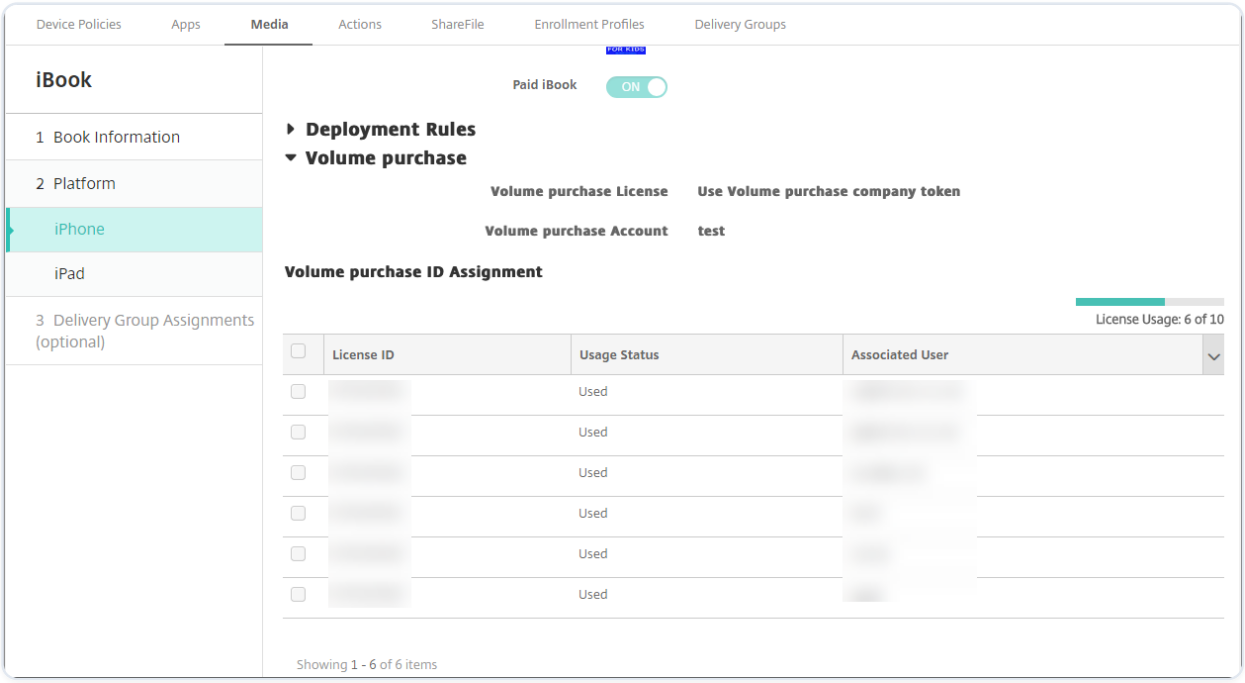


   El **Nombre** y la **Descripción** aparecen solo en la consola y los registros de Citrix Endpoint Management.

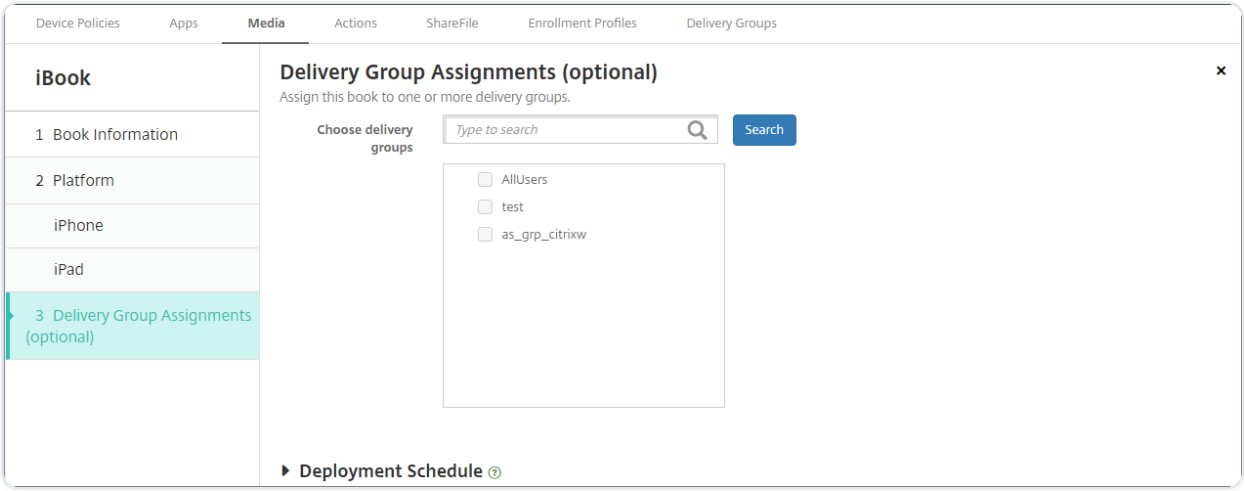
2. En las páginas **Configuración de iBooks para iPhone** y **Configuración de iBooks para iPad**: aunque puede cambiar opcionalmente el nombre y la descripción del libro, Citrix® recomienda no cambiar esta configuración. La imagen es solo para su información y no es editable. **iBook de pago** indica que un libro se ha comprado a través de la Compra por volumen de Apple.



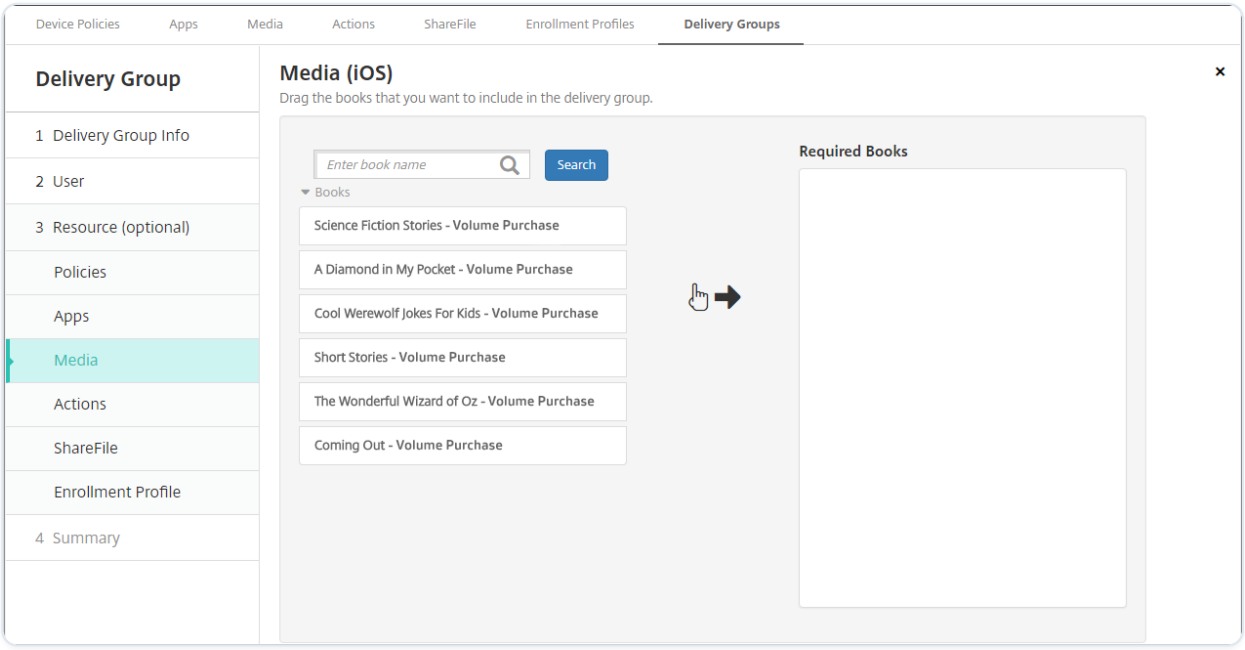
También puede especificar reglas de implementación o ver la información de Compra por Volumen.



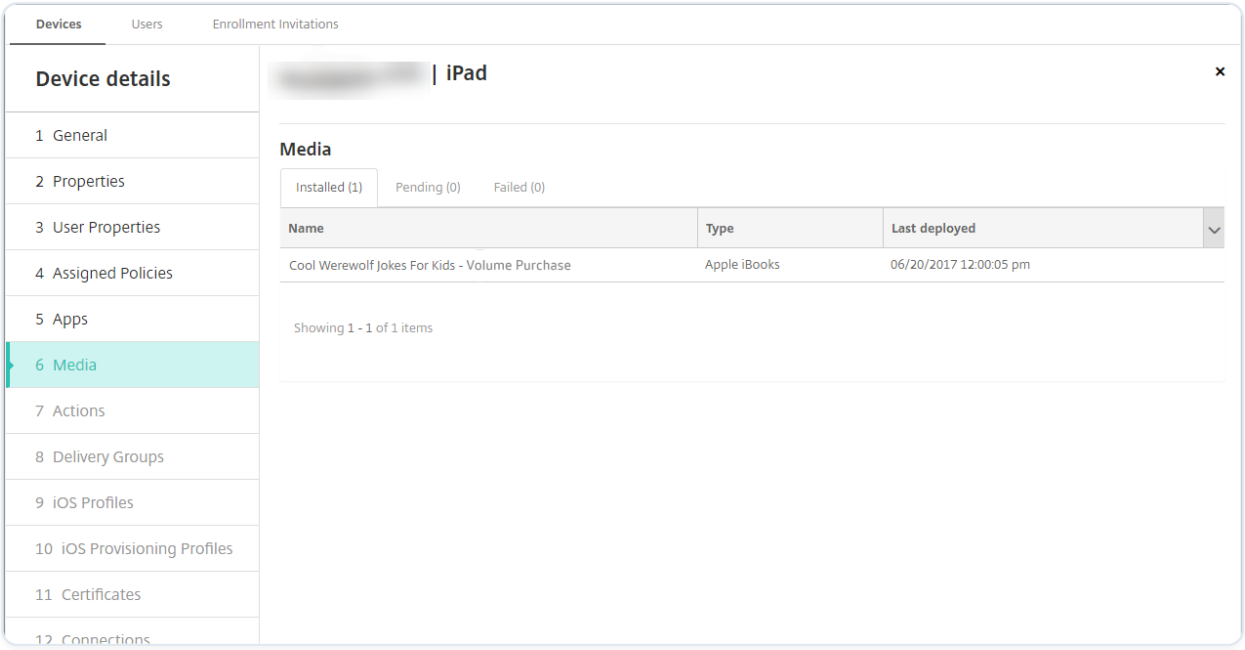
3. Opcionalmente, asigne el libro a grupos de entrega y establezca un programa de implementación.



También puede asignar libros a grupos de entrega desde la pestaña **Medios** en **Configurar > Grupos de entrega**. Citrix Endpoint Management solo admite la implementación obligatoria de libros.



4. Utilice la pestaña **Medios** en **Administrar > Dispositivos** para ver el estado de la implementación.

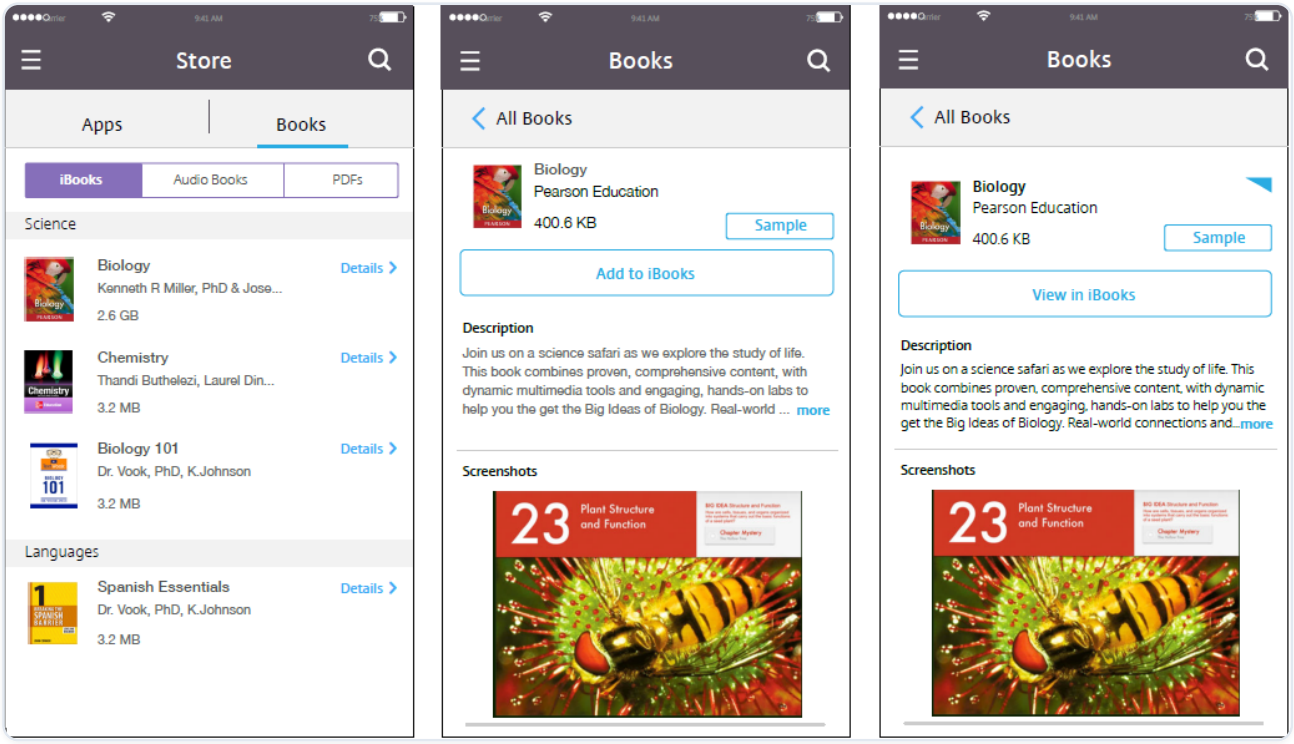


Nota:

En la página **Configurar** > **Medios**, si selecciona un libro y hace clic en **Eliminar**, Citrix Endpoint Management elimina el libro de la lista. Sin embargo, la próxima vez que Citrix

> Endpoint Management se sincronice con Apple Volume Purchase, el libro reaparecerá en la lista a menos que se haya eliminado de Apple Volume Purchase. Eliminar un libro de la lista no lo elimina del dispositivo.

Los libros aparecen en los dispositivos de los usuarios como se muestra en el siguiente ejemplo.



Implementar recursos

La configuración y administración de dispositivos suelen implicar la creación de recursos (directivas, aplicaciones y medios) y acciones en la consola de Citrix Endpoint Management, para luego empaquetarlos mediante grupos de entrega. Los grupos de entrega definen categorías de usuarios para que pueda implementar directivas, aplicaciones, medios y acciones específicos en sus dispositivos. Con la consola de Citrix Endpoint Management, puede:

- Agregar, administrar e implementar grupos de entrega.
- Cambiar el orden en que Citrix Endpoint Management envía recursos y acciones de un grupo de entrega a los dispositivos. Este orden se denomina *orden de implementación*.

  Puede especificar el orden de implementación en la consola de Citrix Endpoint Management. Sin embargo, cuando un usuario está en varios grupos de entrega que tienen directivas duplicadas o en conflicto, Citrix Endpoint Management determina el orden de implementación. Consulte Pasos de cálculo.

Acerca de los grupos de entrega

La inclusión en un grupo de entrega suele basarse en las características del usuario, como la empresa, el país, el departamento, la dirección de la oficina y el cargo. Los grupos de entrega le dan un mayor control sobre quién recibe qué recursos y cuándo los recibe. Puede implementar un grupo de entrega para todos los usuarios o para un grupo de usuarios definido.

Al instalar y configurar Citrix Endpoint Management, se crea el grupo de entrega predeterminado, AllUsers. Este grupo incluye a todos los usuarios locales y de Active Directory. No se puede eliminar el grupo AllUsers, pero se puede inhabilitar cuando no se desea enviar recursos a todos los usuarios. Para obtener más información, consulte Habilitar e inhabilitar el grupo de entrega AllUsers.

Cuando implementa un recurso en un grupo de entrega, envía una notificación push a todos los usuarios de ese grupo. Para dispositivos Apple, utilice el servicio de notificaciones push de Apple (APNs) para enviar notificaciones. Para obtener más información, consulte Certificados APNs). Para dispositivos Android, utilice Firebase Cloud Messaging (FCM). Para obtener más

información, consulte Firebase Cloud Messaging. Para dispositivos Windows, utilice el Servicio de notificaciones push de Windows (WNS).

Acerca de la implementación de recursos

Cuando trabaje en el envío de recursos a los dispositivos, tenga en cuenta lo siguiente:

- Orden de implementación: El orden de implementación es la secuencia en la que Citrix Endpoint Management envía recursos (directivas, aplicaciones y medios) y acciones a un dispositivo. El orden de implementación se aplica a los dispositivos de un grupo de entrega con un perfil de inscripción configurado para la administración de dispositivos (MDM) o para una combinación de administración de aplicaciones (MAM) y MDM.
- Reglas de implementación: Citrix Endpoint Management utiliza las reglas de implementación que usted especifica para las propiedades de usuario y dispositivo para filtrar directivas, aplicaciones, medios, acciones y grupos de entrega. Por ejemplo, una regla de implementación podría especificar que se envíe el paquete de implementación cuando un nombre de dominio coincida con un valor determinado.

  Dentro de un grupo de entrega, puede especificar un subconjunto de usuarios y dispositivos que reciben los recursos en función de sus propiedades de usuario y dispositivo. El filtrado de propiedades de usuario y dispositivo dentro de un grupo de entrega tiene prioridad sobre las reglas de implementación establecidas en el recurso.
- **Programación de la implementación:** Citrix Endpoint Management utiliza la programación de la implementación que usted especifica para las directivas, aplicaciones, medios y acciones para controlar la implementación de esos elementos. Puede especificar que una implementación se realice ahora, en una fecha y hora establecidas, o cuando se cumplan las condiciones de implementación. La programación se especifica al crear la regla. Consulte Configurar reglas de implementación.

Antes de añadir grupos de entrega, considere cómo el orden de implementación, las reglas y la programación se relacionan con sus objetivos de implementación.

Orden de implementación

El orden de implementación es la secuencia en la que Citrix Endpoint Management envía los recursos a los dispositivos. El orden de implementación es importante cuando existen requisitos previos para los recursos y dependencias entre ellos. Los recursos incluyen directivas, aplicaciones, acciones y grupos de entrega.

Por ejemplo, si está implementando una directiva de Wi-Fi que tiene autenticación basada en certificados, debe implementar la directiva de certificación antes que la directiva de Wi-Fi. De lo contrario, se producirán errores. Por el contrario, para algunas directivas (como Términos y condiciones, inventario de software y acciones), el orden de implementación no importa.

Al añadir un grupo de entrega, puede especificar el orden en que se implementan los recursos en los dispositivos. Sin embargo, Citrix Endpoint Management siempre identifica cada situación en la que un usuario se encuentra en varios grupos de entrega que tienen directivas duplicadas o en conflicto. En estos casos, Citrix Endpoint Management calcula un orden de implementación tanto para los objetos que entrega a un dispositivo como para las acciones que realiza.

Al determinar el orden de implementación, Citrix Endpoint Management aplica filtros y criterios de control, como reglas de implementación y programación de implementación, a los recursos. La siguiente tabla muestra cuáles de estos criterios puede aplicar a cada tipo de recurso.

RECURSO	PLATAFORMA DEL DISPOSITIVO	REGLAS DE IMPLEMENTACIÓN	PROGRAMACIÓN DE IMPLEMENTACIÓN	USUARIO/ GRUPOS
Directiva de dispositivo	Sí	Sí	Sí	-
Aplicación	Sí	Sí	Sí	-
Medios	Sí	Sí	Sí	-
Acción	-	Sí	Sí	-
Grupo de entrega	-	Sí	-	Sí

Pasos de cálculo

Cuando Citrix Endpoint Management necesita calcular el orden de implementación, sigue estos pasos.

> **Nota:**
>
> La plataforma del dispositivo no afecta a los pasos de cálculo.

1. Determinar todos los grupos de entrega para un usuario específico, basándose en los filtros de usuarios, grupos y reglas de implementación.
2. Crear una lista ordenada de todos los recursos (directivas, aplicaciones, medios y acciones) en los grupos de entrega seleccionados. La lista se basa en los filtros de plataforma de dispositivo, reglas de implementación y programación de implementación. El algoritmo de ordenación es el siguiente:

    a. Colocar los recursos de los grupos de entrega que tienen un orden de implementación definido por el administrador antes que los recursos de los grupos de entrega que no lo tienen. Para obtener más información, consulte Ejemplo de cálculo con orden definido por el usuario.

    b. Como desempate entre grupos de entrega, ordenar los recursos de los grupos de entrega en orden alfabético inverso por nombre de grupo de entrega. Por ejemplo, Citrix Endpoint Management coloca los recursos del grupo de entrega B antes que los recursos del grupo de entrega A.

    c. Durante la ordenación, si se especifica un orden de implementación definido por el administrador para los recursos de un grupo de entrega, mantener ese orden. De lo contrario, ordenar los recursos dentro de ese grupo de entrega alfabéticamente por nombre de recurso.

    d. Si el mismo recurso aparece más de una vez, elimine el recurso duplicado. Entregue solo el primero de estos recursos.

Los recursos asociados a un orden definido por el administrador se implementan antes que los recursos sin un orden definido por el administrador.

Ejemplo de cálculo con orden definido por el administrador

Supongamos que tiene dos grupos de entrega:

- Grupo de entrega Gestores de cuentas 1: Con orden *no especificado* para los recursos. Tiene las directivas **Red** y **Contraseña**.
- Grupo de entrega Gestores de cuentas 2: Con orden *especificado* para los recursos. Tiene las directivas **Programación de conexiones**, **Restricciones**, **Contraseña** y **Red**, en orden.

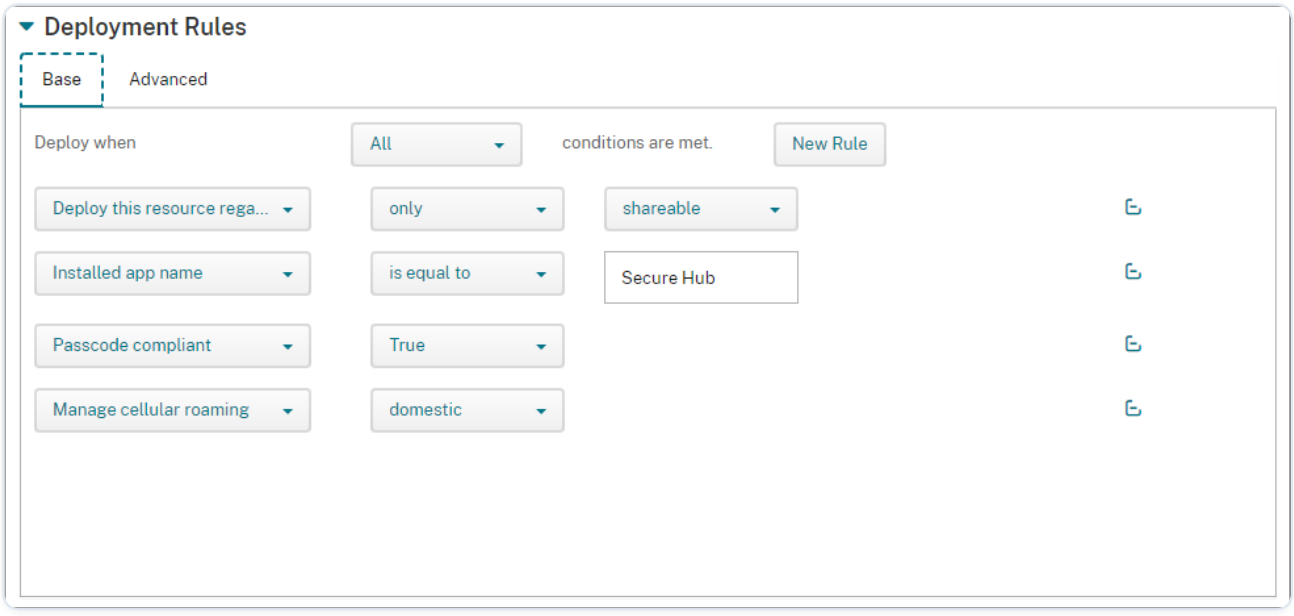
Si el algoritmo de cálculo ordenara los grupos de implementación solo por nombre, Citrix Endpoint Management podría implementarlos en este orden, comenzando por el grupo de entrega Gestores de cuentas 1: **Red**, **Contraseña**, **Programación de conexiones** y **Restricciones**. Citrix Endpoint

Management podría ignorar **Contraseña** y **Red**, ambos duplicados, del grupo de entrega Gestores de cuentas 2.

Sin embargo, el grupo Gestores de cuentas 2 tiene un orden de implementación especificado por el administrador. Por lo tanto, el algoritmo de cálculo coloca los recursos del grupo de entrega Gestores de cuentas 2 más arriba en la lista que los recursos del grupo de entrega Gestores de cuentas 1. Como resultado, Citrix Endpoint Management implementa las directivas en este orden: **Programación de conexiones**, **Restricciones**, **Contraseña** y **Red**. Citrix Endpoint Management ignora las directivas **Red** y **Contraseña** del grupo de entrega Gestores de cuentas 1, porque son duplicados. El algoritmo respeta el orden especificado por el administrador de Citrix Endpoint Management.

Configurar reglas de implementación

Configure reglas de implementación para entregar recursos cuando se cumplan condiciones específicas. Puede configurar reglas de implementación básicas o avanzadas.



Al agregar una regla de implementación mediante el editor básico, primero seleccione cuándo implementar el recurso.

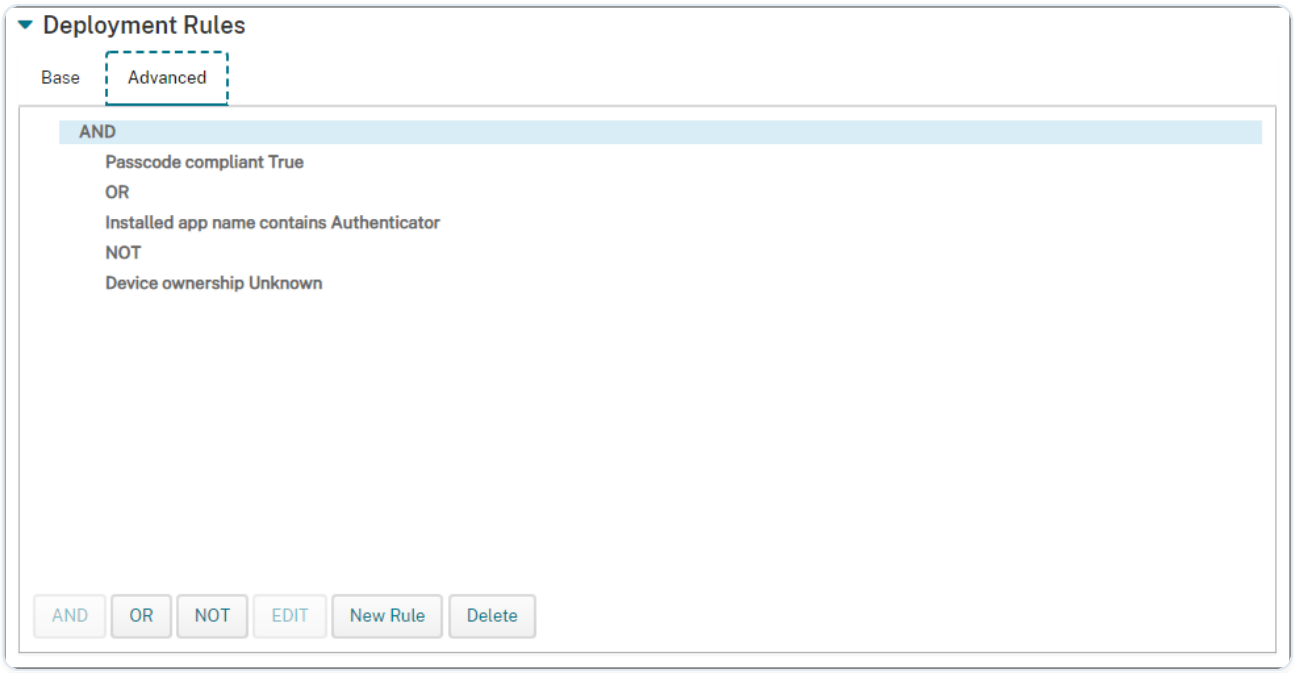
- **Todo:** Entregue el recurso cuando el usuario o el dispositivo cumpla todas las condiciones que configure.
- **Cualquiera:** Entregue el recurso cuando el usuario o el dispositivo cumpla al menos una de las condiciones que configure.

Haga clic en **Nueva regla** para elegir una regla de una lista de reglas disponibles para agregar. Las reglas disponibles varían según el recurso que se implementa y la plataforma para la que se configura el recurso. Dentro de cada regla hay condiciones.

Puede especificar que el recurso se implemente:

- Solo cuando la propiedad seleccionada exista o excepto cuando la propiedad seleccionada exista.
- Cuando la propiedad coincida exactamente con el texto que escribe, la propiedad tenga el texto que escribe o la propiedad no coincida con el texto que escribe.
- Cuando el dispositivo o el usuario cumplan con la propiedad que seleccione o no cumplan con la propiedad que seleccione.
- Cuando las propiedades del dispositivo o del usuario coincidan con una condición que seleccione de una lista predefinida.

Utilice el editor avanzado para crear reglas de implementación más complejas. Puede elegir entre más reglas y combinar diferentes operadores lógicos booleanos al crear una regla avanzada.



Trabajar con grupos de entrega

Puede trabajar con grupos de entrega de las siguientes maneras:

- Agregar un grupo de entrega
- Implementar en grupos de entrega
- Eliminar un grupo de entrega

- Modificar un grupo de entrega
- Habilitar y deshabilitar el grupo de entrega AllUsers.

Agregar un grupo de entrega

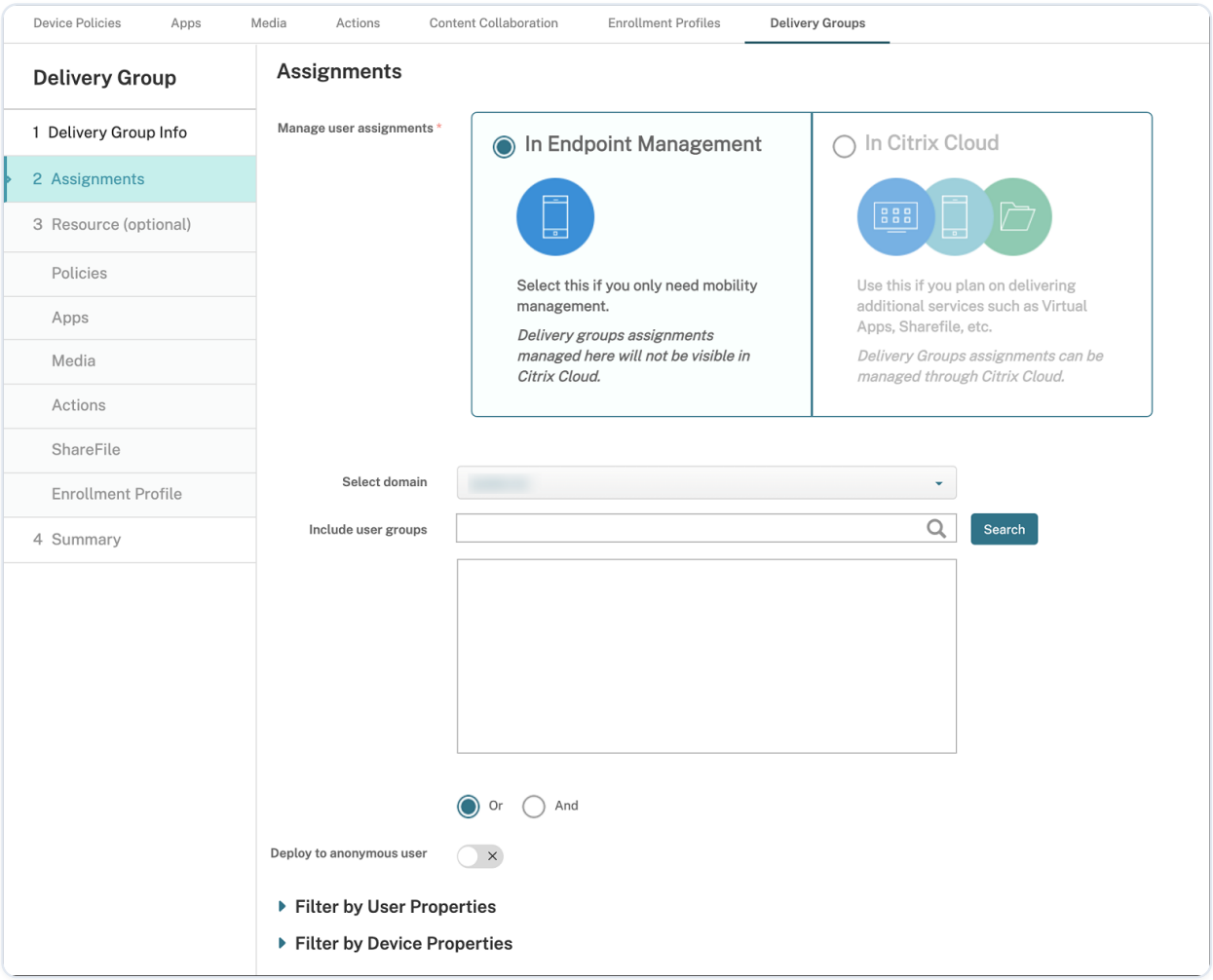
Al crear un grupo de entrega, se especifica si las asignaciones de usuario se administran en Citrix Endpoint Management o en Citrix Cloud. No se puede cambiar esta especificación después de crear el grupo de entrega.

Si tiene previsto utilizar el grupo de entrega para ofrecer otros servicios de Citrix Cloud, especifique que las asignaciones de usuario se administren en Citrix Cloud. Otros servicios de Citrix Cloud incluyen Citrix Virtual Apps and Desktops, ShareFile o Secure Browser Service. Solo puede agregar usuarios de Active Directory a los grupos de entrega administrados en Citrix Cloud.

Si solo necesita la administración de la movilidad para un grupo de entrega de usuarios y aplicaciones, establezca **Administrar asignaciones de usuario** en **En Citrix Endpoint Management**. No puede ver los grupos de entrega con usuarios administrados en Citrix Endpoint Management en Citrix Cloud. Por lo tanto, no puede utilizar los grupos de entrega administrados en Citrix Endpoint Management para ofrecer otros servicios.

> **Nota:**
>
> Recomendamos agregar grupos de entrega antes de crear directivas de dispositivo y perfiles de inscripción. Para obtener información sobre cómo crearlos, consulte Directivas de dispositivo y Perfiles de inscripción.

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Grupos de entrega**.
2. En la página **Grupos de entrega**, haga clic en **Agregar**.
3. En la página **Información del grupo de entrega**, escriba un nombre y una descripción para el grupo de entrega y, a continuación, haga clic en **Siguiente**.
4. En la página **Asignaciones**, especifique cómo administrar las asignaciones del grupo de entrega.



- **Administrar asignaciones de usuario:**
  - **En Citrix Endpoint Management:** Seleccione esta opción si tiene previsto crear un grupo de entrega para usuarios y aplicaciones que solo necesitan administración de la movilidad. No puede ver los grupos de entrega cuyas asignaciones de usuario se administran en Citrix Endpoint Management en Citrix Cloud y no puede utilizarlos para ofrecer otros servicios.
  - **En Citrix Cloud:** Seleccione esta opción si tiene previsto utilizar el grupo de entrega para ofrecer otros servicios. Esos servicios pueden incluir Citrix Virtual Apps and Desktops o ShareFile.

5. Agregue usuarios al grupo de entrega.

> **Importante:**
>
> No puede cambiar la configuración de **Administrar asignaciones de usuario** después de crear el grupo de entrega.

- **Seleccionar dominio:** En la lista, seleccione el dominio del que desea elegir usuarios.
- **Incluir grupos de usuarios:** Realice una de las siguientes acciones:
  - En la lista de grupos de usuarios, haga clic en los grupos que desea agregar. Los grupos seleccionados aparecen en la lista **Grupos de usuarios seleccionados**.
  - Haga clic en **Buscar** para ver una lista de todos los grupos de usuarios en el dominio seleccionado. También puede escribir un nombre de grupo completo o parcial en el cuadro de búsqueda y, a continuación, hacer clic en **Buscar** para acotar la búsqueda.

  Para quitar un grupo de usuarios de la lista **Grupos de usuarios seleccionados**, realice una de las siguientes acciones:
  - En la lista **Grupos de usuarios seleccionados**, haga clic en la **X** junto a cada grupo que desee quitar.
  - Haga clic en **Buscar** para ver una lista de todos los grupos de usuarios en el dominio seleccionado. O bien, escriba un nombre de grupo completo o parcial antes de hacer clic en **Buscar** para acotar la búsqueda. Desactive la casilla de cada grupo que desee quitar.
- **O/Y:** Seleccione si los usuarios están en cualquier grupo (O) o si deben estar en todos los grupos (Y) para que el recurso se les implemente.
- **Implementar en usuario anónimo:** Seleccione si desea implementar en usuarios no autenticados en el grupo de entrega. Los usuarios no autenticados son usuarios que no puede autenticar, pero a los que permitió que sus dispositivos se conectaran a Citrix Endpoint Management de todos modos.

6. Expanda **Filtrar por propiedades de usuario** o **Filtrar por propiedades de dispositivo** para especificar cómo el grupo de entrega administra los recursos.
   - Si elige **Filtrar por propiedades de dispositivo**, expanda la plataforma del dispositivo para configurar las reglas de implementación:
     - **Propiedades del dispositivo - Android** (consulte Crear una regla para implementar recursos en dispositivos Android)
     - **Propiedades del dispositivo - iOS**
     - **Propiedades del dispositivo - Solo escritorio/tableta Windows**
   - La pestaña **Base** aparece de forma predeterminada. En la pestaña **Base**, especifique cuándo implementar la directiva. Puede elegir implementar la directiva cuando se cumplan

Todas las condiciones o cuando se cumpla **Cualquiera** de ellas. La opción predeterminada está establecida en **Todas**.

- Haga clic en **Nueva regla** para definir las condiciones.
- En las listas, elija las condiciones. Por ejemplo, seleccione Propiedad del dispositivo y BYOD.
- Haga clic en **Nueva regla** para cada condición que quiera añadir.

- Haga clic en la pestaña **Avanzado** para combinar las reglas con opciones booleanas. Aparecen las condiciones que eligió en la pestaña **Base**.
  - Haga clic en **Y**, **O** o **NO** y, a continuación, haga clic en **Nueva regla**.
  - En las listas, elija las condiciones que quiera añadir a la regla y, a continuación, haga clic en el signo más (+) del lado derecho.

    En cualquier momento, puede hacer clic para seleccionar una condición y, a continuación, hacer clic en **Editar** para cambiar la condición o en **Eliminar** para quitarla.

7. Haga clic en **Siguiente** para ir a la página **Directivas**. Aquí puede añadir opcionalmente directivas, aplicaciones, medios o acciones para el grupo de entrega. Para obtener más información, consulte:
   - Añadir directivas a un grupo de entrega
   - Añadir aplicaciones a un grupo de entrega
   - Añadir medios a un grupo de entrega
   - Añadir acciones a un grupo de entrega
8. Cuando esté satisfecho con su grupo de entrega, haga clic en **Resumen** para ver un resumen de la configuración.
9. Haga clic en **Guardar**. El nuevo grupo de entrega aparece en la página **Grupos de entrega**.

Añadir directivas a un grupo de entrega

1. En la lista **Recursos (opcional)**, haga clic en **Directivas**.
2. Para cada directiva que quiera añadir, haga lo siguiente:
   - Desplácese por la lista de directivas disponibles para encontrar la que quiera añadir. O bien, escriba un nombre de directiva completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Buscar**.

- Arrastre la directiva que quiera añadir al cuadro de la derecha.

Para quitar una directiva del cuadro, haga clic en la **X** que hay junto al nombre de la directiva.

3. Haga clic en **Siguiente** para ir a la página **Aplicaciones**.

Añadir aplicaciones a un grupo de entrega

1. Para cada aplicación que quiera añadir, haga lo siguiente:

   - Desplácese por la lista de aplicaciones disponibles para encontrar la que quiera añadir. O bien, escriba un nombre de aplicación completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Buscar**.
   - Arrastre la aplicación al cuadro **Aplicaciones obligatorias** o al cuadro **Aplicaciones opcionales**.

   Para las aplicaciones marcadas como obligatorias, los usuarios pueden recibir actualizaciones rápidamente en situaciones como las siguientes:

   - Carga una nueva aplicación y la marca como obligatoria.
   - Marca una aplicación existente como obligatoria.
   - Un usuario elimina una aplicación obligatoria.
   - Hay una actualización disponible de Citrix Secure Hub.

   Para obtener información sobre la implementación forzada de aplicaciones obligatorias, incluida la forma de habilitar la función, consulte Acerca de las aplicaciones obligatorias y opcionales.

   Para quitar una aplicación del cuadro, haga clic en la **X** junto al nombre de la aplicación.

2. Haga clic en **Siguiente** para ir a la página **Medios**.

Agregar medios a un grupo de entrega

1. Para cada libro que quiera agregar, haga lo siguiente:

   - Desplácese por la lista de libros disponibles para encontrar el libro que quiere agregar. O bien, escriba el nombre completo o parcial de un libro en el cuadro de búsqueda y, a continuación, haga clic en **Buscar**.
   - Arrastre el libro que quiere agregar al cuadro **Libros obligatorios**.

   Para los libros marcados como obligatorios, los usuarios reciben actualizaciones rápidamente en situaciones como las siguientes:

- Carga un libro nuevo y lo marca como obligatorio.
- Marca un libro existente como obligatorio.
- Un usuario elimina un libro obligatorio.
- Hay una actualización disponible de Citrix Secure Hub.

Para quitar un libro del cuadro, haga clic en la **X** junto al nombre del libro.

2. Haga clic en **Siguiente** para ir a la página **Acciones**.

Añadir acciones a un grupo de entrega

1. Para cada acción que desee añadir, haga lo siguiente:
   - Desplácese por la lista de acciones disponibles para encontrar la acción que desea añadir. O bien, escriba un nombre de acción completo o parcial en el cuadro de búsqueda y, a continuación, haga clic en **Buscar**.
   - Arrastre la acción que desea añadir al cuadro de la derecha.

   Para eliminar una acción del cuadro, haga clic en la **X** que aparece junto al nombre de la acción.
2. Haga clic en **Siguiente** para ir a la página de **ShareFile**.

Aplicar la configuración de ShareFile

La página de ShareFile difiere según si configuró Citrix Endpoint Management (**Configurar > ShareFile**) para cuentas de empresa o para conectores de zona de almacenamiento.

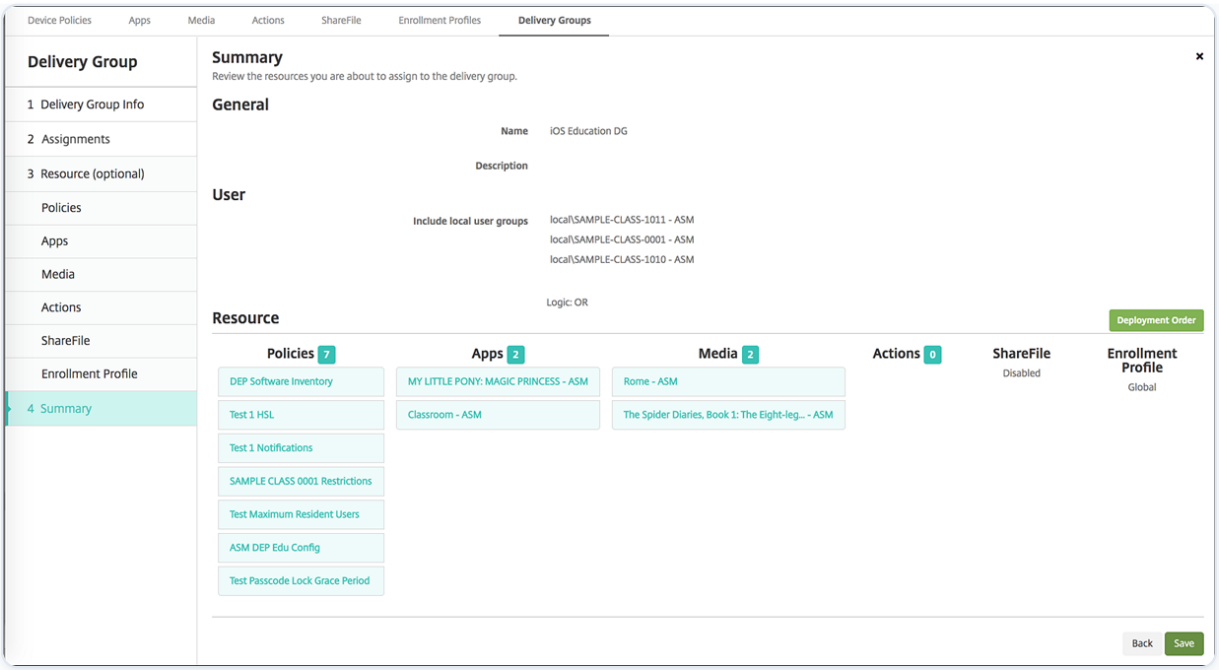
- Si configuró cuentas de empresa para su uso con Citrix Endpoint Management, establezca **Habilitar ShareFile** en **Activado**. Esta configuración proporciona al grupo de entrega acceso de inicio de sesión único al contenido y los datos de ShareFile.
- Si configuró conectores de zona de almacenamiento para su uso con Citrix Endpoint Management, arrastre los conectores de zona de almacenamiento que desee incluir en el grupo de entrega al cuadro de la derecha.

Revisar las opciones configuradas y cambiar el orden de implementación

En la página Resumen, puede revisar las opciones que ha configurado para el grupo de entrega y cambiar el orden de implementación de los recursos. La página Resumen muestra los recursos por categoría. La página Resumen no muestra el orden de implementación.

> **Nota:**

> Haga clic en **Atrás** para volver a las páginas anteriores y cambiar la configuración.



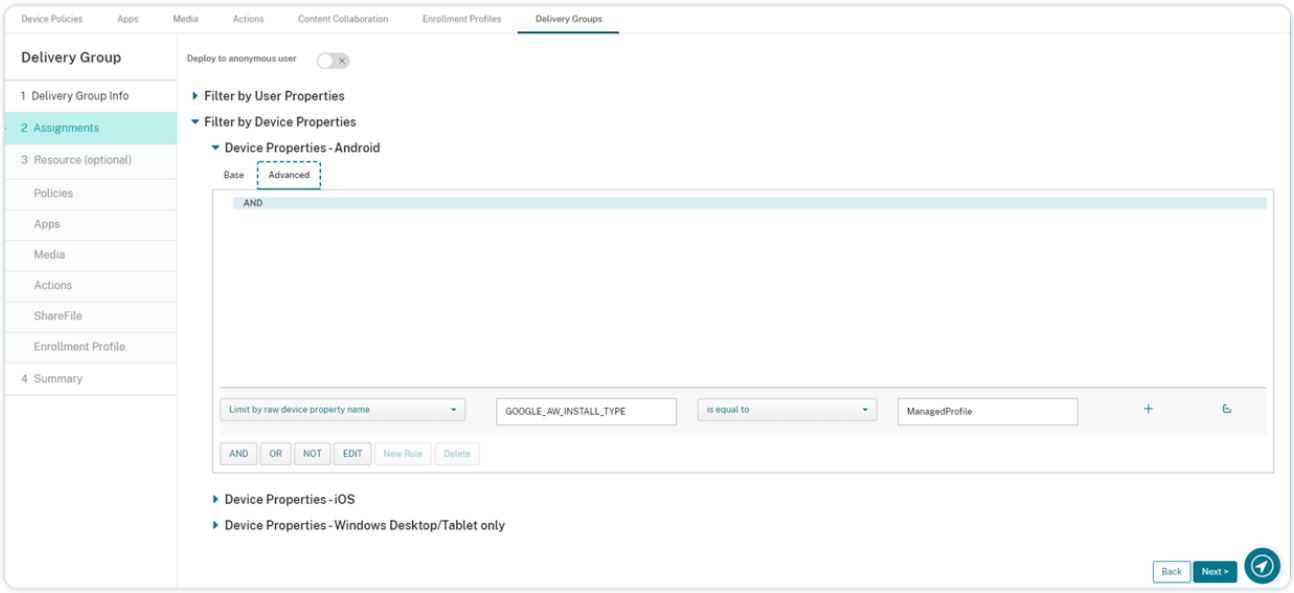
Para ver o cambiar el orden de implementación:

1. Haga clic en **Orden de implementación**.
2. En el cuadro de diálogo Orden de implementación, arrastre un recurso al lugar del orden donde quiera implementarlo. Los recursos se implementan de arriba abajo.
3. Haga clic en **Guardar** para guardar el orden de implementación.

Cuando haya terminado de configurar el grupo de entrega, en la página Resumen, haga clic en **Guardar**.

Crear una regla para implementar recursos en Android Enterprise

Puede administrar la implementación de un grupo de entrega en dispositivos Android Enterprise mediante las reglas de propiedades de dispositivos Android. Si inscribe varios dispositivos para el mismo usuario, puede crear filtros avanzados para Android Enterprise basados en el modo de inscripción del dispositivo o en el ID del paquete de la aplicación del dispositivo.



Para implementar un grupo de entrega en dispositivos Android Enterprise mediante el modo de inscripción de dispositivos:

1. Cree un grupo de entrega.
2. En la página **Asignaciones**, expanda **Filtrar por propiedades del dispositivo**.
3. En **Propiedades del dispositivo – Android**, abra la **ficha Avanzado** y haga clic en **Nueva regla**.
4. En la lista, elija la condición que desea agregar a la regla:
    - Para los nuevos dispositivos Android Enterprise, elija **Limitar por nombre de propiedad de dispositivo sin procesar** y escriba **GOOGLE_AW_INSTALL_TYPE** en el primer campo de valor. A continuación, debe establecer la condición para que sea igual a uno de los modos de inscripción.
    - Para los dispositivos Android Enterprise existentes, elija **Limitar por nombre de propiedad de dispositivo conocido** y seleccione **Tipo de instalación de Android Enterprise** en el primer campo de valor. A continuación, debe establecer la condición para que sea igual a uno de los modos de inscripción.
5. En el segundo campo, escriba un modo de inscripción para sus dispositivos Android Enterprise:
    - **DeviceAdministrator:** Especifica dispositivos propiedad de la empresa destinados únicamente al uso laboral (también conocido como modo de propietario del dispositivo)
    - **ManagedProfile:** Especifica BYOD (dispositivos personales inscritos con la administración de perfiles de trabajo, también conocido como modo de propietario de perfil)

- **CorporateOwnedSingleUse:** Especifica dispositivos dedicados (anteriormente conocidos como dispositivos de un solo uso propiedad de la empresa)
- **CorporateOwnedPersonallyEnabled:** Especifica dispositivos totalmente administrados con un perfil de trabajo (anteriormente conocidos como dispositivos propiedad de la empresa habilitados personalmente)

6. Termine de configurar el grupo de entrega como se describe en Agregar un grupo de entrega.

   Para obtener más información, consulte Escenarios y perfiles de implementación de dispositivos.

Para implementar un grupo de entrega en dispositivos Android Enterprise mediante el ID del paquete de la aplicación del dispositivo:

1. En **Propiedades del dispositivo – Android**, abra la **ficha Avanzado** y haga clic en **Nueva regla**.
2. En la lista, elija **Nombre de la aplicación instalada** e introduzca el ID del paquete de la aplicación.

Editar un grupo de entrega

No puede cambiar el nombre de un grupo de entrega existente. Para actualizar otras configuraciones, vaya a **Configurar > Grupos de entrega**, seleccione el grupo que desea editar y, a continuación, haga clic en **Editar**.

Habilitar y deshabilitar el grupo de entrega AllUsers

AllUsers es el único grupo de entrega que puede habilitar o deshabilitar. No puede eliminar AllUsers como puede hacer con otros grupos de entrega.

En la página **Grupos de entrega**, elija el grupo de entrega AllUsers seleccionando la casilla de verificación junto a **AllUsers** o haciendo clic en la línea que contiene **AllUsers**. A continuación, realice una de las siguientes acciones:

- Haga clic en **Deshabilitar** para deshabilitar el grupo de entrega AllUsers. Este comando solo está disponible si el grupo AllUsers está habilitado (el valor predeterminado). **Deshabilitado** aparece bajo el encabezado **Deshabilitado** en la tabla de grupos de entrega.
- Haga clic en **Habilitar** para habilitar el grupo de entrega AllUsers. Este comando solo está disponible si el grupo AllUsers está deshabilitado. **Deshabilitado** ya no aparece bajo el encabezado **Deshabilitado** en la tabla de grupos de entrega.

Implementar en grupos de entrega

Implementar en un grupo de entrega significa enviar una notificación push a todos los usuarios con dispositivos tablet Apple, Android y Windows.

Para los usuarios con dispositivos de otras plataformas, si esos dispositivos ya están conectados a Citrix Endpoint Management, reciben los recursos inmediatamente. De lo contrario, según su política de programación, reciben los recursos la próxima vez que se conecten.

Para que las aplicaciones actualizadas aparezcan en la lista de Actualizaciones disponibles en la tienda de aplicaciones de los dispositivos Android, primero implemente una política de inventario de aplicaciones en los dispositivos de usuario.

1. En la página **Grupos de entrega**, realice una de las siguientes acciones:

   - Para implementar en más de un grupo de entrega a la vez, seleccione las casillas de verificación junto a los grupos en los que desea implementar.
   - Para implementar en un solo grupo de entrega, seleccione la casilla de verificación junto a su nombre o haga clic en la línea que contiene su nombre.

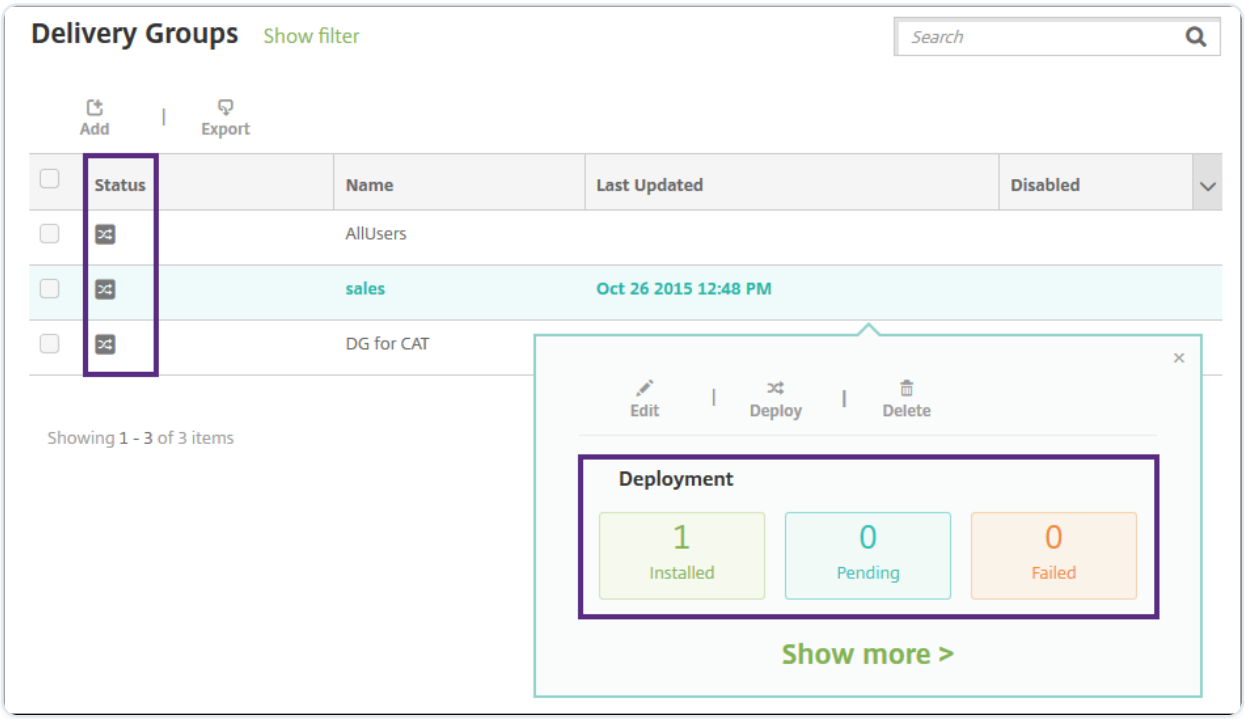
2. Haga clic en **Implementar**.

   Según cómo seleccione un solo grupo de entrega, el comando **Implementar** aparece encima o a la derecha del grupo de entrega.

   verificar que los grupos en los que desea implementar aplicaciones, directivas y acciones están listados. Luego haga clic en **Implementar**. Las aplicaciones, directivas y acciones se implementan en los grupos seleccionados según la plataforma del dispositivo y la política de programación.

   Puede comprobar el estado de la implementación en la página **Grupos de entrega** de una de estas maneras:

   - Consulte el icono de implementación bajo el encabezado **Estado** del grupo de entrega, que indica cualquier fallo de implementación.
   - Haga clic en la línea que contiene el grupo de entrega para mostrar una superposición que muestra las implementaciones **Instaladas**, **Pendientes** y **Fallidas**.



Clonar un grupo de entrega

Clone un grupo de entrega cuando quiera crear un grupo de entrega similar a uno existente. Utilice el clon como punto de partida para su nuevo grupo de entrega. Luego, realice los cambios en el clon, como agregar perfiles de inscripción o nuevos conjuntos de usuarios de AD.

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar** y, a continuación, seleccione la ficha **Grupos de entrega**.
2. En la lista de grupos de entrega, seleccione el que quiera usar como base para el nuevo grupo.
3. Seleccione **Clonar**.
4. En el cuadro de diálogo Clonar un grupo de entrega, introduzca el nombre del nuevo grupo y, opcionalmente, una descripción.
5. Seleccione **Clonar**.

Eliminar grupos de entrega

No puede eliminar el grupo de entrega AllUsers, pero puede deshabilitarlo cuando no quiera enviar recursos a todos los usuarios. Consulte Habilitar y deshabilitar el grupo de entrega AllUsers.

> **Importante:**
>
> No se puede deshacer una eliminación.

1. En la página **Grupos de entrega**, realice una de las siguientes acciones:
   - Para eliminar más de un grupo de entrega a la vez, seleccione las casillas de verificación junto a los grupos que quiera eliminar.
   - Para eliminar un solo grupo de entrega, seleccione la casilla de verificación junto a su nombre o haga clic en la línea que contiene su nombre.
2. Haga clic en **Eliminar**.

   Según cómo seleccione un único grupo de entrega, el comando **Eliminar** aparece encima o a la derecha del grupo de entrega.
3. En el cuadro de diálogo **Eliminar**, haga clic en **Eliminar**.

Exportar la tabla de grupos de entrega

1. Haga clic en **Exportar** encima de la tabla **Grupos de entrega**. Citrix Endpoint Management extrae la información de la tabla **Grupos de entrega** y la convierte en un archivo .csv.
2. Abra o guarde el archivo .csv siguiendo los pasos habituales de su explorador.

Macros

Citrix Endpoint Management proporciona macros como una forma de rellenar datos de propiedades de usuario o dispositivo dentro del campo de texto de los siguientes elementos:

- Directivas
- Notificaciones
- Plantillas de inscripción
- Archivo XML de configuración de dispositivos
- Acciones automatizadas
- Solicitudes de firma de certificados del proveedor de credenciales

Citrix Endpoint Management reemplaza una macro con los valores de usuario o sistema correspondientes. Por ejemplo, puede rellenar previamente el valor del buzón de correo de un usuario en un único perfil de Exchange para miles de usuarios.

Sintaxis de las macros

Una macro puede tener la siguiente forma:

- `${type.PROPERTYNAME}`
- `${type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)]}`

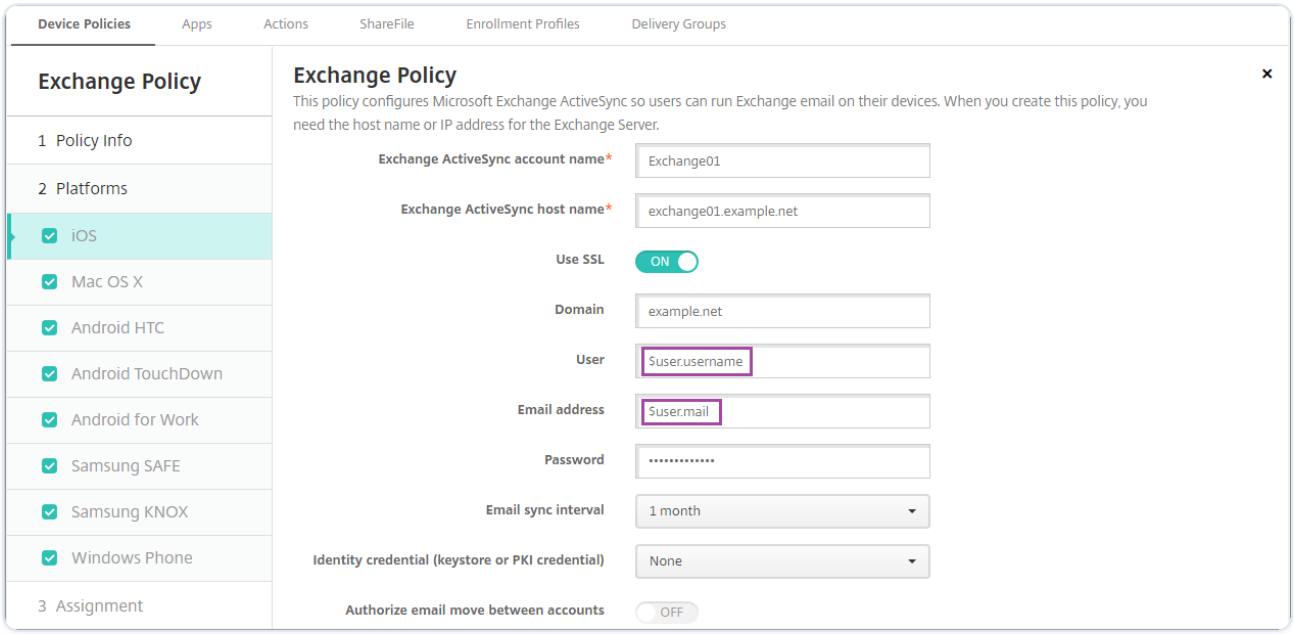
Encierre toda la sintaxis que sigue al signo de dólar ($) entre llaves ({ }).

- Los nombres de propiedades cualificados hacen referencia a una propiedad de usuario, una propiedad de dispositivo o una propiedad personalizada.
- Los nombres de propiedades cualificados constan de un prefijo, seguido del nombre de propiedad real.
- Las propiedades de usuario tienen el formato `${user.[PROPERTYNAME] (prefix="user.")}`.
- Las propiedades de dispositivo tienen el formato `${device.[PROPERTYNAME] (prefix="device.")}`.
- Los nombres de propiedades distinguen entre mayúsculas y minúsculas.
- Una función puede ser una lista limitada o un enlace a una referencia de terceros que define funciones. Esta macro para un mensaje de notificación incluye la función `firstnotnull`:

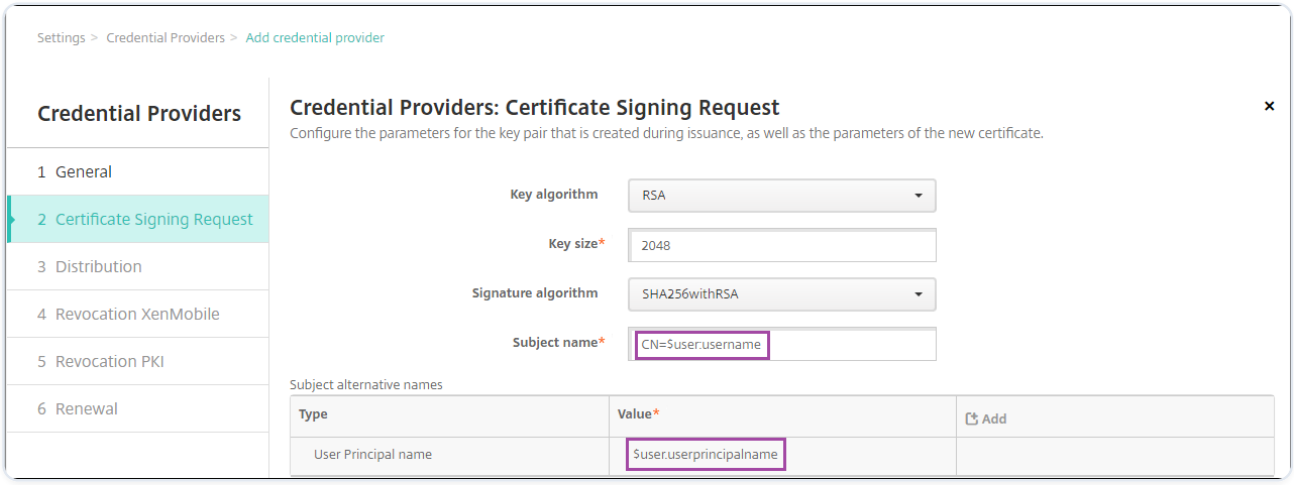
El dispositivo `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` se ha bloqueado…

- Para las macros personalizadas (propiedades que usted define), el prefijo es `${custom}`. Puede omitir el prefijo.

Aquí tiene un ejemplo de una macro de uso común, `${user.username}`, que rellena el valor del nombre de usuario en el campo de texto de una directiva. Esta macro es útil para configurar perfiles de Exchange ActiveSync y otros perfiles utilizados por muchos usuarios. El siguiente ejemplo muestra cómo usar macros en una directiva de Exchange. La macro para **Usuario** es `${user.username}`. La macro para **Dirección de correo electrónico** es `${user.mail}`.

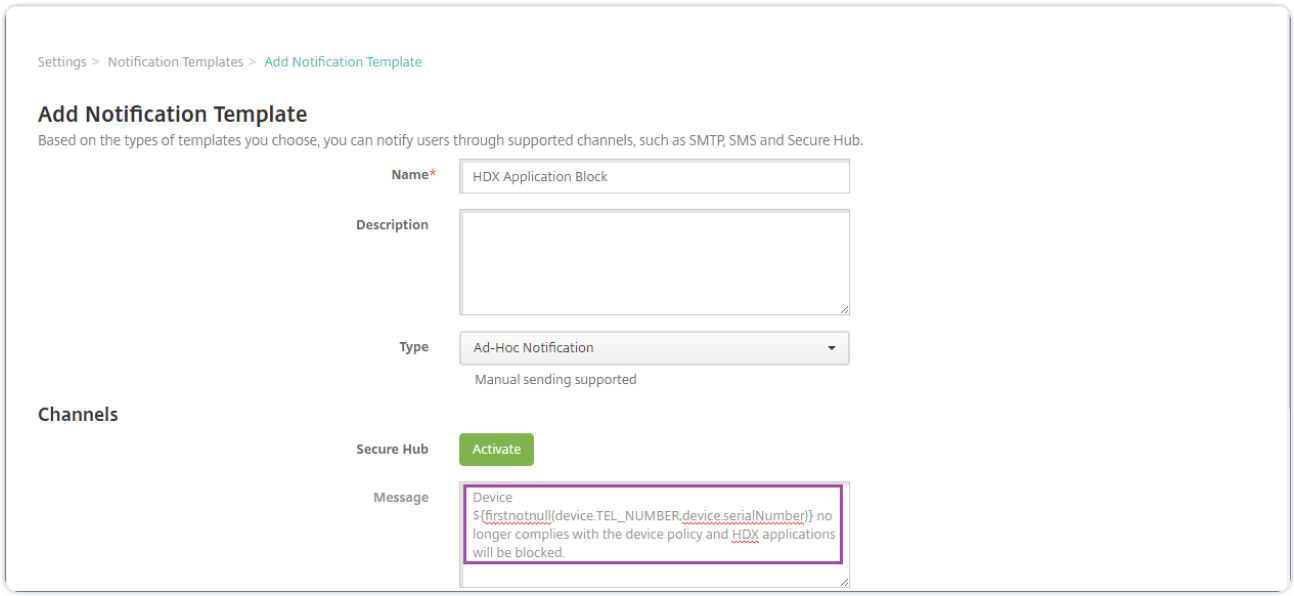


El siguiente ejemplo muestra cómo usar macros para una solicitud de firma de certificado. La macro para **Nombre del asunto** es **CN=$user.username**. La macro para el **Valor** de un **Nombre alternativo del asunto** es **$user.userprincipalname**.



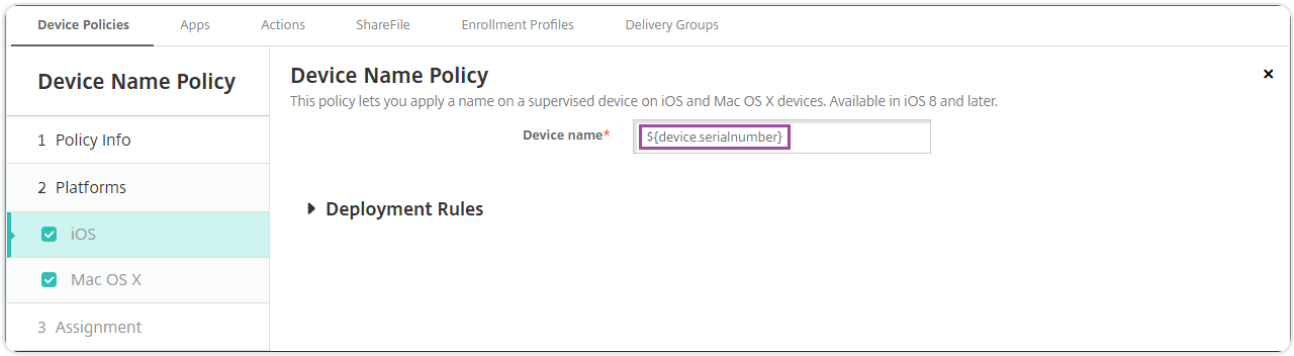
El siguiente ejemplo muestra cómo usar macros en una plantilla de notificación. La plantilla de ejemplo define el mensaje enviado a un usuario cuando las aplicaciones HDX™ se bloquean debido a un dispositivo no compatible. La macro para el **Mensaje** es:

El dispositivo `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` ya no cumple la directiva de dispositivo y las aplicaciones HDX están bloqueadas.



Para ver más ejemplos de macros utilizadas en notificaciones, vaya a **Parámetros > Plantillas de notificación**, seleccione una plantilla predefinida y haga clic en **Modificar**.

El siguiente ejemplo muestra una macro en la directiva de dispositivo Nombre de dispositivo. Puede escribir una macro, una combinación de macros o una combinación de macros y texto para asignar un nombre único a cada dispositivo. Por ejemplo, use `${device.serialnumber}` para establecer los nombres de los dispositivos como el número de serie de cada dispositivo. Use `${device.serialnumber} ${ user.username }` para incluir el nombre de usuario en el nombre del dispositivo. La directiva de dispositivo Nombre de dispositivo funciona en dispositivos iOS y macOS supervisados.



Macros para plantillas de notificación predeterminadas

Puede usar las siguientes macros en las plantillas de notificación predeterminadas:

- `${account.SUPPORT_EMAIL}`
- `${applicationName}`
- `${enrollment.andriod.agent.download.url}`
- `${enrollment.ios.agent.download.url}`

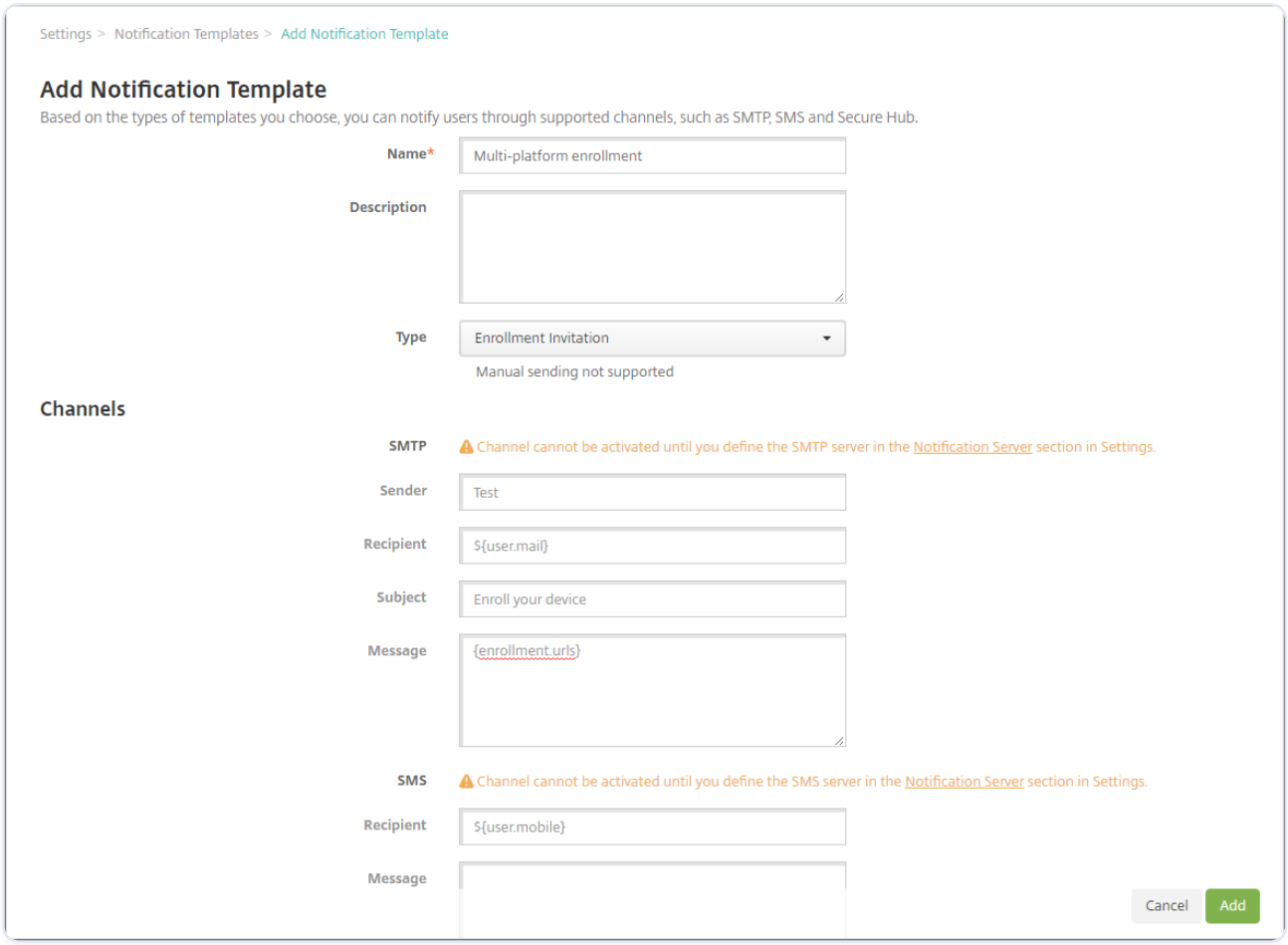
- `${enrollment.pin}`
- `${enrollment.url}`
- `${enrollment.urls}`
- `${enrollment.ios.url}`
- `${enrollment.macos.url}`
- `${enrollment.android.url}`
- `${enrollment.ios.platform}`
- `${enrollment.macos.platform}`
- `${enrollment.android.platform}`
- `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}`
- `${firstnotnull(device.TEL_NUMBER,user.mobile)}`
- `${outofcompliance.reason(smg_block)}`
- `${outofcompliance.reason(whitelist_blacklist_apps_name)}`
- `${vpp.account}`
- `${vpp.appname}`
- `${vpp.url}`
- `${zdmserver.hostPath}/enroll`

Nota:

La consola de Citrix Endpoint Management incluye los términos "lista negra" y "lista blanca". Estamos cambiando esos términos en una próxima versión a "lista de bloqueo" y "lista de permitidos".

Este ejemplo muestra cómo crear una notificación que incluye URL de inscripción para muchas plataformas de dispositivos. La macro para el **Mensaje** es:

${enrollment.urls}



Estos ejemplos muestran cómo crear mensajes para notificaciones que solicitan a los usuarios que hagan clic en la URL de inscripción para las plataformas de sus dispositivos:

Ejemplo 1:

```
To enroll, click the link below that applies to your device platform:


${enrollment.ios.platform} - ${enrollment.ios.url}


${enrollment.macos.platform} - ${enrollment.macos.url}


${enrollment.android.platform} - ${enrollment.android.url}
```

Ejemplo 2:

```
To enroll an iOS device, click the link ${enrollment.ios.url}.


To enroll a macOS device, click the link ${enrollment.macos.url}.


To enroll an Android device, click the link ${enrollment.android.url}.
```

Macros para directivas específicas

Para la directiva de dispositivo Nombre de dispositivo (para iOS y macOS), puede usar estas macros para el **Nombre de dispositivo:**

- `${device.serialnumber}`
- `${user.username}@example.com`
- `${device.serialnumber}`
- `${device.serialnumber}`
- `${user.username}`
- `${enrollment.pin}`
- `${user.dnsroot}`

Para la directiva de dispositivo Datos móviles (para iOS), puede usar macros para los valores de campos que no son de cadena, como el puerto del servidor proxy. Por ejemplo, ahora puede usar una macro como `${device.xyz}` o `${setting.xyz}`, que se expande en un número entero.

Para un archivo XML de configuración de dispositivo que importe a Citrix Endpoint Management mediante la directiva de dispositivo **Importar perfil de iOS y macOS**, puede usar macros para los valores de campos que no son de cadena.

Para la directiva de dispositivo Clave de licencia de Samsung MDM, puede usar esta macro para la **Clave de licencia de ELM:**

- `${elm.license.key}`

Para la directiva de dispositivo de clip web, puede usar esta macro para la **URL:**

- `${webeas-url}`

Macros para obtener propiedades de dispositivo integradas

NOMBRE PARA MOSTRAR	MACROS
ID de dispositivo	`$device.id`
GUID de dispositivo	`$device.uniqueid`
IMEI de dispositivo	`$device.imei`
Familia de SO	`$device.OSFamily`
Número de serie	`$device.serialNumber`

Macros para todas las propiedades del dispositivo

Nombre para mostrar: ¿Cuenta suspendida?

- **Elemento web:** `GOOGLE_AW_DIRECTORY_SUSPENDED`
- **Macros:** `${device.GOOGLE_AW_DIRECTORY_SUSPENDED}`

Nombre para mostrar: Código de omisión del bloqueo de activación

- **Elemento web:** `ACTIVATION_LOCK_BYPASS_CODE`
- **Macros:** `${device.ACTIVATION_LOCK_BYPASS_CODE}`

Nombre para mostrar: Bloqueo de activación habilitado

- **Elemento web:** `ACTIVATION_LOCK_ENABLED`
- **Macros:** `${device.ACTIVATION_LOCK_ENABLED}`

Nombre para mostrar: Cuenta activa de Apple App Store

- **Elemento web:** `ACTIVE_ITUNES`
- **Macros:** `${device.ACTIVE_ITUNES}`

Nombre para mostrar: Administrador deshabilitado

- **Elemento web:** `ADMIN_DISABLED`
- **Macros:** `${device.ADMIN_DISABLED}`

Nombre para mostrar: ¿AIK presente?

- **Elemento web:** `WINDOWS_HAS_AIK_PRESENT`
- **Macros:** `${device.WINDOWS_HAS_AIK_PRESENT}`

Nombre para mostrar: API de MDM de Amazon disponible

- **Elemento web:** `AMAZON_MDM`
- **Macros:** `${device.AMAZON_MDM}`

Nombre para mostrar: ID de dispositivo de Android Enterprise

- **Elemento web:** `GOOGLE_AW_DEVICE_ID`
- **Macros:** `${device.GOOGLE_AW_DEVICE_ID}`

Nombre para mostrar: ¿Dispositivo con Android Enterprise habilitado?

- **Elemento web:** `GOOGLE_AW_ENABLED_DEVICE`
- **Macros:** `${device.GOOGLE_AW_ENABLED_DEVICE}`

Nombre para mostrar: Tipo de instalación de Android Enterprise

- **Elemento web:** `GOOGLE_AW_INSTALL_TYPE`
- **Macros:** `${device.GOOGLE_AW_INSTALL_TYPE}`

Nombre para mostrar: Estado de la firma antispyware

- **Elemento web:** `ANTI_SPYWARE_SIGNATURE_STATUS`
- **Macros:** `${device.ANTI_SPYWARE_SIGNATURE_STATUS}`

Nombre para mostrar: Estado del antispyware

- **Elemento web:** `ANTI_SPYWARE_STATUS`
- **Macros:** `${device.ANTI_SPYWARE_STATUS}`

Nombre para mostrar: Estado de la firma del antivirus

- **Elemento web:** `ANTI_VIRUS_SIGNATURE_STATUS`
- **Macros:** `${device.ANTI_VIRUS_SIGNATURE_STATUS}`

Nombre para mostrar: Estado del antivirus

- **Elemento web:** `ANTI_VIRUS_STATUS`
- **Macros:** `${device.ANTI_VIRUS_STATUS}`

Nombre para mostrar: Código de omisión del bloqueo de activación del programa de implementación de ASM

- **Elemento web:** `DEP_ACTIVATION_LOCK_BYPASS_CODE`
- **Macros:** `${device.DEP_ACTIVATION_LOCK_BYPASS_CODE}`

Nombre para mostrar: Clave de depósito del programa de implementación de ASM

- **Elemento web:** `DEP_ESCROW_KEY`
- **Macros:** `${device.DEP_ESCROW_KEY}`

Nombre para mostrar: Etiqueta de activo

- **Elemento web:** `ASSET_TAG`
- **Macros:** `${device.ASSET_TAG}`

Nombre para mostrar: Comprobar automáticamente las actualizaciones de software

- **Elemento web:** `AutoCheckEnabled`
- **Macros:** `${device.AutoCheckEnabled}`

Nombre para mostrar: Descargar automáticamente las actualizaciones de software en segundo plano

- **Elemento web:** `BackgroundDownloadEnabled`
- **Macros:** `${device.BackgroundDownloadEnabled}`

Nombre para mostrar: Instalar automáticamente las actualizaciones de aplicaciones

- **Elemento web:** `AutomaticAppInstallationEnabled`
- **Macros:** `${device.AutomaticAppInstallationEnabled}`

Nombre para mostrar: Instalar automáticamente las actualizaciones del SO

- **Elemento web:** `AutomaticOSInstallationEnabled`
- **Macros:** `${device.AutomaticOSInstallationEnabled}`

Nombre para mostrar: Instalar automáticamente las actualizaciones de seguridad

- **Elemento web:** `AutomaticSecurityUpdatesEnabled`
- **Macros:** `${device.AutomaticSecurityUpdatesEnabled}`

Nombre para mostrar: Estado de actualización automática

- **Elemento web:** `AUTOUPDATE_STATUS`
- **Macros:** `${device.AUTOUPDATE_STATUS}`

Nombre para mostrar: RAM disponible

- **Elemento web:** `MEMORY_AVAILABLE`
- **Macros:** `${device.MEMORY_AVAILABLE}`

Nombre para mostrar: Actualizaciones de software disponibles

- **Elemento web:** `AVAILABLE_OS_UPDATE_HUMAN_READABLE`
- **Macros:** `${device.AVAILABLE_OS_UPDATE_HUMAN_READABLE}`

Nombre para mostrar: Espacio de almacenamiento disponible

- **Elemento web:** `FREEDISK`
- **Macros:** `${device.FREEDISK}`

Nombre para mostrar: Batería de reserva

- **Elemento web:** `BACKUP_BATTERY_PERCENT`
- **Macros:** `${device.BACKUP_BATTERY_PERCENT}`

Nombre para mostrar: Versión del firmware de banda base

- **Elemento web:** `MODEM_FIRMWARE_VERSION`
- **Macros:** `${device.MODEM_FIRMWARE_VERSION}

Nombre para mostrar: Carga de la batería

- **Elemento web:** `BATTERY_CHARGING_STATUS`
- **Macros:** `${device.BATTERY_CHARGING_STATUS}`

Nombre para mostrar: Carga de la batería

- **Elemento web:** `BATTERY_CHARGING`
- **Macros:** `${device.BATTERY_CHARGING}`

Nombre para mostrar: Batería restante

- **Elemento web:** `BATTERY_ESTIMATED_CHARGE_REMAINING`

- **Macros:** `${device.BATTERY_ESTIMATED_CHARGE_REMAINING}`

Nombre para mostrar: Tiempo de ejecución de la batería

- **Elemento web:** `BATTERY_RUNTIME`
- **Macros:** `${device.BATTERY_RUNTIME}`

Nombre para mostrar: Estado de la batería

- **Elemento web:** `BATTERY_STATUS`
- **Macros:** `${device.BATTERY_STATUS}`

Nombre para mostrar: BES PIN

- **Elemento web:** `BES_PIN`
- **Macros:** `${device.BES_PIN}`

Nombre para mostrar: ID de agente de servidor BES

- **Elemento web:** `AGENT_ID`
- **Macros:** `${device.AGENT_ID}`

Nombre para mostrar: Nombre del servidor BES

- **Elemento web:** `BES_SERVER`
- **Macros:** `${device.BES_SERVER}`

Nombre para mostrar: Versión del servidor BES

- **Elemento web:** `BES_VERSION`
- **Macros:** `${device.BES_VERSION}`

Nombre para mostrar: Información de la BIOS

- **Elemento web:** `BIOS_INFO`
- **Macros:** `${device.BIOS_INFO}`

Nombre para mostrar: Estado de BitLocker

- **Elemento web:** `WINDOWS_HAS_BIT_LOCKER_STATUS`
- **Macros:** `${device.WINDOWS_HAS_BIT_LOCKER_STATUS}`

Nombre para mostrar: Dirección MAC de Bluetooth

- **Elemento web:** `BLUETOOTH_MAC`
- **Macros:** `${device.BLUETOOTH_MAC}`

Nombre para mostrar: ¿Depuración de arranque habilitada?

- **Elemento web:** `WINDOWS_HAS_BOOT_DEBUGGING_ENABLED`
- **Macros:** `${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED}`

Nombre para mostrar: Versión de la lista de revisión del administrador de arranque

- **Elemento web:** `WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION`
- **Macros:** `${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION}`

Nombre para mostrar: Código de operador

- **Elemento web:** `CARRIER_CODE`
- **Macros:** `${device.CARRIER_CODE}`

Nombre para mostrar: Versión de la configuración del operador

- **Elemento web:** `CARRIER_SETTINGS_VERSION`
- **Macros:** `${device.CARRIER_SETTINGS_VERSION}`

Nombre para mostrar: URL del catálogo

- **Elemento web:** `CatalogURL`
- **Macros:** `${device.CatalogURL}`

Nombre para mostrar: Altitud celular

- **Elemento web:** `GPS_ALTITUDE_FROM_CELLULAR`
- **Macros:** `${device.GPS_ALTITUDE_FROM_CELLULAR}`

Nombre para mostrar: Rumbo celular

- **Elemento web:** `GPS_COURSE_FROM_CELLULAR`
- **Macros:** `${device.GPS_COURSE_FROM_CELLULAR}`

Nombre para mostrar: Precisión horizontal celular

- **Elemento web:** `GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR`
- **Macros:** `${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR}`

Nombre para mostrar: Latitud celular

- **Elemento web:** `GPS_LATITUDE_FROM_CELLULAR`
- **Macros:** `${device.GPS_LATITUDE_FROM_CELLULAR}`

Nombre para mostrar: Longitud celular

- **Elemento web:** `GPS_LONGITUDE_FROM_CELLULAR`
- **Macros:** `${device.GPS_LONGITUDE_FROM_CELLULAR}`

Nombre para mostrar: Velocidad de datos móviles

- **Elemento web:** `GPS_SPEED_FROM_CELLULAR`
- **Macros:** `${device.GPS_SPEED_FROM_CELLULAR}`

Nombre para mostrar: Tecnología de datos móviles

- **Elemento web:** `CELLULAR_TECHNOLOGY`
- **Macros:** `${device.CELLULAR_TECHNOLOGY}`

Nombre para mostrar: Marca de tiempo de datos móviles

- **Elemento web:** `GPS_TIMESTAMP_FROM_CELLULAR`
- **Macros:** `${device.GPS_TIMESTAMP_FROM_CELLULAR}`

Nombre para mostrar: Precisión vertical de datos móviles

- **Elemento web:** `GPS_VERTICAL_ACCURACY_FROM_CELLULAR`
- **Macros:** `${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}`

Nombre para mostrar: ¿Cambiar contraseña en el próximo inicio de sesión?

- **Elemento web:** `GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN`
- **Macros:** `${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}

Nombre para mostrar: ID de dispositivo cliente

- **Elemento web:** `CLIENT_DEVICE_ID`
- **Macros:** `${device.CLIENT_DEVICE_ID}`

Nombre para mostrar: Copia de seguridad en la nube habilitada

- **Elemento web:** `CLOUD_BACKUP_ENABLED`

- **Macros:** `${device.CLOUD_BACKUP_ENABLED}`

Nombre para mostrar: ¿Integridad del código habilitada?

- **Elemento web:** `WINDOWS_HAS_CODE_INTEGRITY_ENABLED`
- **Macros:** `${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED}`

Nombre para mostrar: Versión de la lista de revocación de integridad del código

- **Elemento web:** `WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION`
- **Macros:** `${device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION}`

Nombre para mostrar: Color

- **Elemento web:** `COLOR`
- **Macros:** `${device.COLOR}`

Nombre para mostrar: Velocidad de reloj de la CPU

- **Elemento web:** `CPU_CLOCK_SPEED`
- **Macros:** `${device.CPU_CLOCK_SPEED}`

Nombre para mostrar: Tipo de CPU

- **Elemento web:** `CPU_TYPE`
- **Macros:** `${device.CPU_TYPE}`

Nombre para mostrar: Hora de creación

- **Elemento web:** `GOOGLE_AW_DIRECTORY_CREATION_TIME`
- **Macros:** `${device.GOOGLE_AW_DIRECTORY_CREATION_TIME}`

Nombre para mostrar: Actualizaciones de software críticas

- **Elemento web:** `AVAILABLE_OS_UPDATE_IS_CRITICAL`
- **Macros:** `${device.AVAILABLE_OS_UPDATE_IS_CRITICAL}`

Nombre para mostrar: Red de operador actual

- **Elemento web:** `CARRIER`
- **Macros:** `${device.CARRIER}`

Nombre para mostrar: Código de país móvil actual

- **Elemento web:** `CURRENT_MCC`
- **Macros:** `${device.CURRENT_MCC}`

Nombre para mostrar: Código de red móvil actual

- **Elemento web:** `CURRENT_MNC`
- **Macros:** `${device.CURRENT_MNC}`

Nombre para mostrar: Itinerancia de datos permitida

- **Elemento web:** `DATA_ROAMING_ENABLED`
- **Macros:** `${device.DATA_ROAMING_ENABLED}`

Nombre para mostrar: Fecha de la última copia de seguridad de iCloud

- **Elemento web:** `LAST_CLOUD_BACKUP_DATE`
- **Macros:** `${device.LAST_CLOUD_BACKUP_DATE}`

Nombre para mostrar: Catálogo predeterminado

- **Elemento web:** `IsDefaultCatalog`
- **Macros:** `${device.IsDefaultCatalog}`

Nombre para mostrar: Nombre de la cuenta del Programa de implementación de Apple

- **Elemento web:** `BULK_ENROLLMENT_DEP_ACCOUNT_NAME`
- **Macros:** `${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME}`

Nombre para mostrar: Directiva del Programa de implementación de Apple

- **Elemento web:** `WINDOWS_HAS_DEP_POLICY`
- **Macros:** `${device.WINDOWS_HAS_DEP_POLICY}`

Nombre para mostrar: Perfil del Programa de implementación de Apple asignado

- **Elemento web:** `PROFILE_ASSIGN_TIME`
- **Macros:** `${device.PROFILE_ASSIGN_TIME}`

Nombre para mostrar: Perfil del Programa de implementación de Apple enviado

- **Elemento web:** `PROFILE_PUSH_TIME`
- **Macros:** `${device.PROFILE_PUSH_TIME}`

Nombre para mostrar: Perfil del Programa de implementación de Apple eliminado

- **Elemento web:** `PROFILE_REMOVE_TIME`
- **Macros:** `${device.PROFILE_REMOVE_TIME}`

Nombre para mostrar: Registro del programa de implementación de Apple por

- **Elemento web:** `DEVICE_ASSIGNED_BY`
- **Macros:** `${device.DEVICE_ASSIGNED_BY}`

Nombre para mostrar: Fecha de registro del programa de implementación de Apple

- **Elemento web:** `DEVICE_ASSIGNED_DATE`
- **Macros:** `${device.DEVICE_ASSIGNED_DATE}`

Nombre para mostrar: Descripción

- **Elemento web:** `DESCRIPTION`
- **Macros:** `${device.DESCRIPTION}`

Nombre para mostrar: Modelo de dispositivo

- **Elemento web:** `SYSTEM_OEM`
- **Macros:** `${device.SYSTEM_OEM}`

Nombre para mostrar: Nombre del dispositivo

- **Elemento web:** `DEVICE_NAME`
- **Macros:** `${device.DEVICE_NAME}`

Nombre para mostrar: Tipo de dispositivo

- **Elemento web:** `DEVICE_TYPE`
- **Macros:** `${device.DEVICE_TYPE}`

Nombre para mostrar: No molestar activado

- **Elemento web:** `DO_NOT_DISTURB`
- **Macros:** `${device.DO_NOT_DISTURB}`

Nombre para mostrar: ¿Controlador ELAM cargado?

- **Elemento web:** `WINDOWS_HAS_ELAM_DRIVER_LOADED`

- **Macros:** `${device.WINDOWS_HAS_ELAM_DRIVER_LOADED}`

Nombre para mostrar: Cumplimiento de cifrado

- **Elemento web:** `ENCRYPTION_COMPLIANCE`
- **Macros:** `${device.ENCRYPTION_COMPLIANCE}`

Nombre para mostrar: ENROLLMENT_KEY_GENERATION_DATE

- **Elemento web:** `ENROLLMENT_KEY_GENERATION_DATE`
- **Macros:** `${device.ENROLLMENT_KEY_GENERATION_DATE}`

Nombre para mostrar: ID de empresa

- **Elemento web:** `ENTERPRISEID`
- **Macros:** `${device.ENTERPRISEID}`

Nombre para mostrar: Almacenamiento externo 1: espacio disponible

- **Elemento web:** `EXTERNAL_STORAGE1_FREE_SPACE`
- **Macros:** `${device.EXTERNAL_STORAGE1_FREE_SPACE}`

Nombre para mostrar: Almacenamiento externo 1: espacio disponible

- **Elemento web:** `EXTERNAL_STORAGE1_FREE_SPACE`
- **Macros:** `${device.EXTERNAL_STORAGE1_FREE_SPACE}`

Nombre para mostrar: Almacenamiento externo 1: nombre

- **Elemento web:** `EXTERNAL_STORAGE1_NAME`
- **Macros:** `${device.EXTERNAL_STORAGE1_NAME}`

Nombre para mostrar: Almacenamiento externo 1: espacio total

- **Elemento web:** `EXTERNAL_STORAGE1_TOTAL_SPACE`
- **Macros:** `${device.EXTERNAL_STORAGE1_TOTAL_SPACE}`

Nombre para mostrar: Almacenamiento externo 2: espacio disponible

- **Elemento web:** `EXTERNAL_STORAGE2_FREE_SPACE`
- **Macros:** `${device.EXTERNAL_STORAGE2_FREE_SPACE}`

Nombre para mostrar: Almacenamiento externo 2: nombre

- **Elemento web:** `EXTERNAL_STORAGE2_NAME`
- **Macros:** `${device.EXTERNAL_STORAGE2_NAME}`

Nombre para mostrar: Almacenamiento externo 2: espacio total

- **Elemento web:** `EXTERNAL_STORAGE2_TOTAL_SPACE`
- **Macros:** `${device.EXTERNAL_STORAGE2_TOTAL_SPACE}`

Nombre para mostrar: Almacenamiento externo cifrado

- **Elemento web:** `EXTERNAL_ENCRYPTION`
- **Macros:** `${device.EXTERNAL_ENCRYPTION}`

Nombre para mostrar: FileVault habilitado

- **Elemento web:** `IS_FILEVAULT_ENABLED`
- **Macros:** `${device.IS_FILEVAULT_ENABLED}`

Nombre para mostrar: Estado del firewall

- **Elemento web:** `DEVICE_FIREWALL_STATUS`
- **Macros:** `${device.DEVICE_FIREWALL_STATUS}`

Nombre para mostrar: Estado del firewall

- **Elemento web:** `DEVICE_FIREWALL_STATUS`
- **Macros:** `${device.DEVICE_FIREWALL_STATUS}`

Nombre para mostrar: Estado del firewall

- **Elemento web:** `FIREWALL_STATUS`
- **Macros:** `${device.FIREWALL_STATUS}`

Nombre para mostrar: Versión del firmware

- **Elemento web:** `FIRMWARE_VERSION`
- **Macros:** `${device.FIRMWARE_VERSION}`

Nombre para mostrar: Primera sincronización

- **Elemento web:** `ZMSP_FIRST_SYNC`
- **Macros:** `${device.ZMSP_FIRST_SYNC}`

Nombre para mostrar: Alias de directorio de Google

- **Elemento web:** `GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS`
- **Macros:** `${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS}`

Nombre para mostrar: Apellido de directorio de Google

- **Elemento web:** `GOOGLE_AW_DIRECTORY_FAMILY_NAME`
- **Macros:** `${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME}`

Nombre para mostrar: Nombre de directorio de Google

- **Elemento web:** `GOOGLE_AW_DIRECTORY_NAME`
- **Macros:** `${device.GOOGLE_AW_DIRECTORY_NAME}`

Nombre para mostrar: Correo electrónico principal de directorio de Google

- **Elemento web:** `GOOGLE_AW_DIRECTORY_PRIMARY`
- **Macros:** `${device.GOOGLE_AW_DIRECTORY_PRIMARY}`

Nombre para mostrar: ID de usuario de directorio de Google

- **Elemento web:** `GOOGLE_AW_DIRECTORY_USER_ID`
- **Macros:** `${device.GOOGLE_AW_DIRECTORY_USER_ID}`

Nombre para mostrar: Altitud GPS

- **Elemento web:** `GPS_ALTITUDE_FROM_GPS`
- **Macros:** `${device.GPS_ALTITUDE_FROM_GPS}`

Nombre para mostrar: Rumbo GPS

- **Elemento web:** `GPS_COURSE_FROM_GPS`
- **Macros:** `${device.GPS_COURSE_FROM_GPS}`

Nombre para mostrar: Precisión horizontal del GPS

- **Elemento web:** `GPS_HORIZONTAL_ACCURACY_FROM_GPS`
- **Macros:** `${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS}`

Nombre para mostrar: Latitud GPS

- **Elemento web:** `GPS_LATITUDE_FROM_GPS`

- **Macros:** `${device.GPS_LATITUDE_FROM_GPS}`

Nombre para mostrar: Longitud GPS

- **Elemento web:** `GPS_LONGITUDE_FROM_GPS`
- **Macros:** `${device.GPS_LONGITUDE_FROM_GPS}`

Nombre para mostrar: Velocidad GPS

- **Elemento web:** `GPS_SPEED_FROM_GPS`
- **Macros:** `${device.GPS_SPEED_FROM_GPS}`

Nombre para mostrar: Marca de tiempo GPS

- **Elemento web:** `GPS_TIMESTAMP_FROM_GPS`
- **Macros:** `${device.GPS_TIMESTAMP_FROM_GPS}`

Nombre para mostrar: Precisión vertical GPS

- **Elemento web:** `GPS_VERTICAL_ACCURACY_FROM_GPS`
- **Macros:** `${device.GPS_VERTICAL_ACCURACY_FROM_GPS}`

Nombre para mostrar: ID de dispositivo de hardware

- **Elemento web:** `HW_DEVICE_ID`
- **Macros:** `${device.HW_DEVICE_ID}`

Nombre para mostrar: Capacidades de cifrado de hardware

- **Elemento web:** `HARDWARE_ENCRYPTION_CAPS`
- **Macros:** `${device.HARDWARE_ENCRYPTION_CAPS}`

Nombre para mostrar: HAS_CONTAINER

- **Elemento web:** `HAS_CONTAINER`
- **Macros:** `${device.HAS_CONTAINER}`

Nombre para mostrar: Hash de la cuenta de Apple App Store con la sesión iniciada actualmente

- **Elemento web:** `ITUNES_STORE_ACCOUNT_HASH`
- **Macros:** `${device.ITUNES_STORE_ACCOUNT_HASH}`

Nombre para mostrar: Red del operador de origen

- **Elemento web:** `SIM_CARRIER_NETWORK`
- **Macros:** `${device.SIM_CARRIER_NETWORK}`

Nombre para mostrar: Código de país móvil de origen

- **Elemento web:** `SIM_MCC`
- **Macros:** `${device.SIM_MCC}`

Nombre para mostrar: Código de red móvil de origen

- **Elemento web:** `SIM_MNC`
- **Macros:** `${device.SIM_MNC}`

Nombre para mostrar: ICCID

- **Elemento web:** `ICCID`
- **Macros:** `${device.ICCID}`

Nombre para mostrar: Identidad

- **Elemento web:** `AS_DEVICE_IDENTITY`
- **Macros:** `${device.AS_DEVICE_IDENTITY}`

Nombre para mostrar: Número IMEI/MEID

- **Elemento web:** `IMEI`
- **Macros:** `${device.IMEI}`

Nombre para mostrar: IMSI

- **Elemento web:** `SIM_ID`
- **Macros:** `${device.SIM_ID}`

Nombre para mostrar: Almacenamiento interno cifrado

- **Elemento web:** `LOCAL_ENCRYPTION`
- **Macros:** `${device.LOCAL_ENCRYPTION}`

Nombre para mostrar: Ubicación IP

- **Elemento web:** `IP_LOCATION`
- **Macros:** `${device.IP_LOCATION}`

Nombre para mostrar: Dirección IPV4

- **Elemento web:** `IP_ADDRESSV4`
- **Macros:** `${device.IP_ADDRESSV4}`

Nombre para mostrar: Dirección IPV6

- **Elemento web:** `IP_ADDRESSV6`
- **Macros:** `${device.IP_ADDRESSV6}`

Nombre para mostrar: Emitido el

- **Elemento web:** `WINDOWS_HAS_ISSUED_AT`
- **Macros:** `${device.WINDOWS_HAS_ISSUED_AT}`

Nombre para mostrar: Con jailbreak/rooteado

- **Elemento web:** `ROOT_ACCESS`
- **Macros:** `${device.ROOT_ACCESS}`

Nombre para mostrar: ¿Depuración del kernel habilitada?

- **Elemento web:** `WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED`
- **Macros:** `${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED}`

Nombre para mostrar: Modo quiosco

- **Elemento web:** `IS_KIOSK`
- **Macros:** `${device.IS_KIOSK}`

Nombre para mostrar: Última dirección IP conocida

- **Elemento web:** `LAST_IP_ADDR`
- **Macros:** `${device.LAST_IP_ADDR}`

Nombre para mostrar: Hora de la última actualización de la directiva

- **Elemento web:** `LAST_POLICY_UPDATE_TIME`
- **Macros:** `${device.LAST_POLICY_UPDATE_TIME}`

Nombre para mostrar: Fecha del último análisis

- **Elemento web:** `PreviousScanDate`

- **Macros:** `${device.PreviousScanDate}`

Nombre para mostrar: Último resultado de análisis

- **Elemento web:** `PreviousScanResult`
- **Macros:** `${device.PreviousScanResult}`

Nombre para mostrar: Últimas actualizaciones de software programadas

- **Elemento web:** `AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME`
- **Macros:** `${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME}`

Nombre para mostrar: Mensaje de error de las últimas actualizaciones de software programadas

- **Elemento web:** `AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG`
- **Macros:** `${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG}`

Nombre para mostrar: Estado de las últimas actualizaciones de software programadas

- **Elemento web:** `AVAILABLE_OS_UPDATE_INSTALL_STATUS`
- **Macros:** `${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS}`

Nombre para mostrar: Última sincronización

- **Elemento web:** `ZMSP_LAST_SYNC`
- **Macros:** `${device.ZMSP_LAST_SYNC}`

Nombre para mostrar: Servicio de localización habilitado

- **Elemento web:** `DEVICE_LOCATOR`
- **Macros:** `${device.DEVICE_LOCATOR}`

Nombre para mostrar: Dirección MAC

- **Elemento web:** `MAC_ADDRESS`
- **Macros:** `${device.MAC_ADDRESS}`

Nombre para mostrar: Conexión de red de dirección MAC

- **Elemento web:** `MAC_NETWORK_CONNECTION`
- **Macros:** `${device.MAC_NETWORK_CONNECTION}`

Nombre para mostrar: Tipo de dirección MAC

- **Elemento web:** `MAC_ADDRESS_TYPE`
- **Macros:** `${device.MAC_ADDRESS_TYPE}`

Nombre para mostrar: Configuración de buzón

- **Elemento web:** `GOOGLE_AW_DIRECTORY_MAILBOX_SETUP`
- **Macros:** `${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP}`

Nombre para mostrar: Batería principal

- **Elemento web:** `MAIN_BATTERY_PERCENT`
- **Macros:** `${device.MAIN_BATTERY_PERCENT}`

Nombre para mostrar: Modo perdido de MDM habilitado

- **Elemento web:** `IS_MDM_LOST_MODE_ENABLED`
- **Macros:** `${device.IS_MDM_LOST_MODE_ENABLED}`

Nombre para mostrar: MDX_SHARED_ENCRYPTION_KEY

- **Elemento web:** `MDX_SHARED_ENCRYPTION_KEY`
- **Macros:** `${device.MDX_SHARED_ENCRYPTION_KEY}`

Nombre para mostrar: MEID

- **Elemento web:** `MEID`
- **Macros:** `${device.MEID}`

Nombre para mostrar: Número de teléfono móvil

- **Elemento web:** `TEL_NUMBER`
- **Macros:** `${device.TEL_NUMBER}`

Nombre para mostrar: ID de modelo

- **Elemento web:** `MODEL_ID`
- **Macros:** `${device.MODEL_ID}`

Nombre para mostrar: Número de modelo

- **Elemento web:** `MODEL_NUMBER`
- **Macros:** `${device.MODEL_NUMBER}`

Nombre para mostrar: Tipo de adaptador de red

- **Elemento web:** `NETWORK_ADAPTER_TYPE`
- **Macros:** `${device.NETWORK_ADAPTER_TYPE}`

Nombre para mostrar: Compilación del sistema operativo

- **Elemento web:** `SYSTEM_OS_BUILD`
- **Macros:** `${device.SYSTEM_OS_BUILD}`

Nombre para mostrar: Edición del sistema operativo

- **Elemento web:** `OS_EDITION`
- **Macros:** `${device.OS_EDITION}`

Nombre para mostrar: Idioma del sistema operativo (configuración regional)

- **Elemento web:** `SYSTEM_LANGUAGE`
- **Macros:** `${device.SYSTEM_LANGUAGE}`

Nombre para mostrar: Versión del sistema operativo

- **Elemento web:** `SYSTEM_OS_VERSION`
- **Macros:** `${device.SYSTEM_OS_VERSION}`

Nombre para mostrar: Dirección de la organización

- **Elemento web:** `ORGANIZATION_ADDRESS`
- **Macros:** `${device.ORGANIZATION_ADDRESS}`

Nombre para mostrar: Correo electrónico de la organización

- **Elemento web:** `ORGANIZATION_EMAIL`
- **Macros:** `${device.ORGANIZATION_EMAIL}`

Nombre para mostrar: Magia de la organización

- **Elemento web:** `ORGANIZATION_MAGIC`
- **Macros:** `${device.ORGANIZATION_MAGIC}`

Nombre para mostrar: Nombre de la organización

- **Elemento web:** `ORGANIZATION_NAME`

- **Macros:** `${device.ORGANIZATION_NAME}`

Nombre para mostrar: Número de teléfono de la organización

- **Elemento web:** `ORGANIZATION_PHONE`
- **Macros:** `${device.ORGANIZATION_PHONE}`

'**Nombre para mostrar:** No conforme

- **Elemento web:** `OUT_OF_COMPLIANCE`
- **Macros:** `${device.OUT_OF_COMPLIANCE}`

Nombre para mostrar: Propiedad de

- **Elemento web:** `CORPORATE_OWNED`
- **Macros:** `${device.CORPORATE_OWNED}`

Nombre para mostrar: Conforme con código de acceso

- **Elemento web:** `PASSCODE_IS_COMPLIANT`
- **Macros:** `${device.PASSCODE_IS_COMPLIANT}`

Nombre para mostrar: Código de acceso compatible con la configuración

- **Elemento web:** `PASSCODE_IS_COMPLIANT_WITH_CFG`
- **Macros:** `${device.PASSCODE_IS_COMPLIANT_WITH_CFG}`

Nombre para mostrar: Código de acceso presente

- **Elemento web:** `PASSCODE_PRESENT`
- **Macros:** `${device.PASSCODE_PRESENT}`

Nombre para mostrar: PCR0

- **Elemento web:** `WINDOWS_HAS_PCR0`
- **Macros:** `${device.WINDOWS_HAS_PCR0}`

Nombre para mostrar: Violación del perímetro

- **Elemento web:** `GPS_PERIMETER_BREACH`
- **Macros:** `${device.GPS_PERIMETER_BREACH}`

Nombre para mostrar: Comprobación periódica

- **Elemento web:** `PerformPeriodicCheck`
- **Macros:** `${device.PerformPeriodicCheck}`

Nombre para mostrar: Punto de acceso personal activado

- **Elemento web:** `PERSONAL_HOTSPOT_ENABLED`
- **Macros:** `${device.PERSONAL_HOTSPOT_ENABLED}`

Nombre para mostrar: Código PIN para geocerca

- **Elemento web:** `PIN_CODE_FOR_GEO_FENCE`
- **Macros:** `${device.PIN_CODE_FOR_GEO_FENCE}`

Nombre para mostrar: Plataforma

- **Elemento web:** `SYSTEM_PLATFORM`
- **Macros:** `${device.SYSTEM_PLATFORM}`

Nombre para mostrar: Nivel de API de la plataforma

- **Elemento web:** `API_LEVEL`
- **Macros:** `${device.API_LEVEL}`

Nombre para mostrar: Nombre de la directiva

- **Elemento web:** `POLICY_NAME`
- **Macros:** `${device.POLICY_NAME}`

Nombre para mostrar: Número de teléfono principal

- **Elemento web:** `IDENTITY1_PHONENUMBER`
- **Macros:** `${device.IDENTITY1_PHONENUMBER}`

Nombre para mostrar: Operador de la tarjeta SIM principal

- **Elemento web:** `IDENTITY1_CARRIER_NETWORK_OPERATOR`
- **Macros:** `${device.IDENTITY1_CARRIER_NETWORK_OPERATOR}`

Nombre para mostrar: ICCID de la tarjeta SIM principal

- **Elemento web:** `IDENTITY1_ICCID`
- **Macros:** `${device.IDENTITY1_ICCID}`

Nombre para mostrar: IMEI de la tarjeta SIM principal

- **Elemento web:** `IDENTITY1_IMEI`
- **Macros:** `${device.IDENTITY1_IMEI}`

Nombre para mostrar: IMSI de la tarjeta SIM principal

- **Elemento web:** `IDENTITY1_IMSI`
- **Macros:** `${device.IDENTITY1_IMSI}`

Nombre para mostrar: Roaming de SIM principal

- **Elemento web:** `IDENTITY1_ROAMING`
- **Macros:** `${device.IDENTITY1_ROAMING}`

Nombre para mostrar: Roaming de SIM principal

- **Elemento web:** `IDENTITY1_ROAMING_COMPLIANCE`
- **Macros:** `${device.IDENTITY1_ROAMING_COMPLIANCE}`

Nombre para mostrar: Nombre del producto

- **Elemento web:** `PRODUCT_NAME`
- **Macros:** `${device.PRODUCT_NAME}`

Nombre para mostrar: ID de dispositivo del editor

- **Elemento web:** `PUBLISHER_DEVICE_ID`
- **Macros:** `${device.PUBLISHER_DEVICE_ID}`

Nombre para mostrar: Recuento de restablecimientos

- **Elemento web:** `WINDOWS_HAS_RESET_COUNT`
- **Macros:** `${device.WINDOWS_HAS_RESET_COUNT}`

Nombre para mostrar: Recuento de reinicios

- **Elemento web:** `WINDOWS_HAS_RESTART_COUNT`
- **Macros:** `${device.WINDOWS_HAS_RESTART_COUNT}`

Nombre para mostrar: ¿Modo seguro habilitado?

- **Elemento web:** `WINDOWS_HAS_SAFE_MODE`

- **Macros:** `${device.WINDOWS_HAS_SAFE_MODE}`

Nombre para mostrar: SBCP Hash

- **Elemento web:** `WINDOWS_HAS_SBCP_HASH`
- **Macros:** `${device.WINDOWS_HAS_SBCP_HASH}`

Nombre para mostrar: Pantalla: altura

- **Elemento web:** `SCREEN_HEIGHT`
- **Macros:** `${device.SCREEN_HEIGHT}`

Nombre para mostrar: Pantalla: número de colores

- **Elemento web:** `SCREEN_NB_COLORS`
- **Macros:** `${device.SCREEN_NB_COLORS}`

Nombre para mostrar: Pantalla: tamaño

- **Elemento web:** `SCREEN_SIZE`
- **Macros:** `${device.SCREEN_SIZE}`

Nombre para mostrar: Pantalla: ancho

- **Elemento web:** `SCREEN_WIDTH`
- **Macros:** `${device.SCREEN_WIDTH}`

Nombre para mostrar: Pantalla: resolución del eje X

- **Elemento web:** `SCREEN_XDPI`
- **Macros:** `${device.SCREEN_XDPI}`

Nombre para mostrar: Pantalla: resolución del eje Y

- **Elemento web:** `SCREEN_YDPI`
- **Macros:** `${device.SCREEN_YDPI}`

Nombre para mostrar: Número de teléfono secundario

- **Elemento web:** `IDENTITY2_PHONENUMBER`
- **Macros:** `${device.IDENTITY2_PHONENUMBER}`

Nombre para mostrar: Operador de la tarjeta SIM secundaria

- **Elemento web:** `IDENTITY2_CARRIER_NETWORK_OPERATOR`
- **Macros:** `${device.IDENTITY2_CARRIER_NETWORK_OPERATOR}`

Nombre para mostrar: ICCID de la tarjeta SIM secundaria

- **Elemento web:** `IDENTITY2_ICCID`
- **Macros:** `${device.IDENTITY2_ICCID}`

Nombre para mostrar: IMEI de la tarjeta SIM secundaria

- **Elemento web:** `IDENTITY2_IMEI`
- **Macros:** `${device.IDENTITY2_IMEI}`

Nombre para mostrar: IMSI de la tarjeta SIM secundaria

- **Elemento web:** `IDENTITY2_IMSI`
- **Macros:** `${device.IDENTITY2_IMSI}`

Nombre para mostrar: Itinerancia de la tarjeta SIM secundaria

- **Elemento web:** `IDENTITY2_ROAMING`
- **Macros:** `${device.IDENTITY2_ROAMING}`

Nombre para mostrar: Cumplimiento de itinerancia de SIM secundaria

- **Elemento web:** `IDENTITY2_ROAMING_COMPLIANCE`
- **Macros:** `${device.IDENTITY2_ROAMING_COMPLIANCE}`

Nombre para mostrar: ¿Arranque seguro habilitado?

- **Elemento web:** `WINDOWS_HAS_SECURE_BOOT_ENABLED`
- **Macros:** `${device.WINDOWS_HAS_SECURE_BOOT_ENABLED}`

Nombre para mostrar: Estado del arranque seguro

- **Elemento web:** `SECURE_BOOT_STATE`
- **Macros:** `${device.SECURE_BOOT_STATE}`

Nombre para mostrar: SecureContainer habilitado

- **Elemento web:** `DLP_ACTIVE`
- **Macros:** `${device.DLP_ACTIVE}`

Nombre para mostrar: Nivel de parche de seguridad

- **Elemento web:** `SYSTEM_SECURITY_PATCH_LEVEL`
- **Macros:** `${device.SYSTEM_SECURITY_PATCH_LEVEL}`

Nombre para mostrar: Número de serie

- **Elemento web:** `SERIAL_NUMBER`
- **Macros:** `${device.SERIAL_NUMBER}`

Nombre para mostrar: Compatible con SMS

- **Elemento web:** `IS_SMS_CAPABLE`
- **Macros:** `${device.IS_SMS_CAPABLE}`

Nombre para mostrar: Supervisado

- **Elemento web:** `SUPERVISED`
- **Macros:** `${device.SUPERVISED}`

Nombre para mostrar: Motivo de suspensión

- **Elemento web:** `GOOGLE_AW_DIRECTORY_SUSPENTION_REASON`
- **Macros:** `${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON}`

Nombre para mostrar: Estado de manipulación

- **Elemento web:** `TAMPERED_STATUS`
- **Macros:** `${device.TAMPERED_STATUS}`

Nombre para mostrar: Términos y condiciones

- **Elemento web:** `TERMS_AND_CONDITIONS`
- **Macros:** `${device.TERMS_AND_CONDITIONS}`

Nombre para mostrar: ¿Términos y acuerdo aceptados?

- **Elemento web:** `GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS`
- **Macros:** `${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS}`

Nombre para mostrar: ¿Firma de prueba habilitada?

- **Elemento web:** `WINDOWS_HAS_TEST_SIGNING_ENABLED`

- **Macros:** `${device.WINDOWS_HAS_TEST_SIGNING_ENABLED}`

Nombre para mostrar: RAM total

- **Elemento web:** `MEMORY`
- **Macros:** `${device.MEMORY}`

Nombre para mostrar: Espacio de almacenamiento total

- **Elemento web:** `TOTAL_DISK_SPACE`
- **Macros:** `${device.TOTAL_DISK_SPACE}`

Nombre para mostrar: Versión de TPM

- **Elemento web:** `TPM_VERSION`
- **Macros:** `${device.TPM_VERSION}`

Nombre para mostrar: UDID

- **Elemento web:** `UDID`
- **Macros:** `${device.UDID}`

Nombre para mostrar: Estado del Control de cuentas de usuario

- **Elemento web:** `UAC_STATUS`
- **Macros:** `${device.UAC_STATUS}`

Nombre para mostrar: Agente de usuario

- **Elemento web:** `USER_AGENT`
- **Macros:** `${device.USER_AGENT}`

Nombre para mostrar: Definido por el usuario #1

- **Elemento web:** `USER_DEFINED_1`
- **Macros:** `${device.USER_DEFINED_1}`

Nombre para mostrar: Definido por el usuario #2

- **Elemento web:** `USER_DEFINED_2`
- **Macros:** `${device.USER_DEFINED_2}`

Nombre para mostrar: Definido por el usuario #3

- **Elemento web:** `USER_DEFINED_3`
- **Macros:** `${device.USER_DEFINED_3}`

Nombre para mostrar: Idioma del usuario (configuración regional)

- **Elemento web:** `USER_LANGUAGE`
- **Macros:** `${device.USER_LANGUAGE}`

Nombre para mostrar: Proveedor

- **Elemento web:** `VENDOR`
- **Macros:** `${device.VENDOR}`

Nombre para mostrar: Compatible con voz

- **Elemento web:** `IS_VOICE_CAPABLE`
- **Macros:** `${device.IS_VOICE_CAPABLE}`

Nombre para mostrar: Roaming de voz permitido

- **Elemento web:** `VOICE_ROAMING_ENABLED`
- **Macros:** `${device.VOICE_ROAMING_ENABLED}`

Nombre para mostrar: ¿VSM habilitado?

- **Elemento web:** `WINDOWS_HAS_VSM_ENABLED`
- **Macros:** `${device.WINDOWS_HAS_VSM_ENABLED}`

Nombre para mostrar: Dirección MAC de Wi-Fi

- **Elemento web:** `WIFI_MAC`
- **Macros:** `${device.WIFI_MAC}`

Nombre para mostrar: WINDOWS_ENROLLMENT_KEY

- **Elemento web:** `WINDOWS_ENROLLMENT_KEY`
- **Macros:** `${device.WINDOWS_ENROLLMENT_KEY}`

Nombre para mostrar: ¿WinPE habilitado?

- **Elemento web:** `WINDOWS_HAS_WINPE`
- **Macros:** `${device.WINDOWS_HAS_WINPE}`

Nombre para mostrar: Estado de notificación WNS

- **Elemento web:** `PROPERTY_WNS_PUSH_STATUS`
- **Macros:** `${device.PROPERTY_WNS_PUSH_STATUS}`

Nombre para mostrar: URL de notificación WNS

- **Elemento web:** `PROPERTY_WNS_PUSH_URL`
- **Macros:** `${device.PROPERTY_WNS_PUSH_URL}`

Nombre para mostrar: Fecha de caducidad de la URL de notificación WNS

- **Elemento web:** `PROPERTY_WNS_PUSH_URL_EXPIRY`
- **Macros:** `${device.PROPERTY_WNS_PUSH_URL_EXPIRY}`

Nombre para mostrar: ID de agente de Citrix Endpoint Management

- **Elemento web:** `ENROLLMENT_AGENT_ID`
- **Macros:** {device.ENROLLMENT_AGENT_ID}`

Nombre para mostrar: Revisión del agente de Citrix Endpoint Management

- **Elemento web:** `EW_REVISION`
- **Macros:** `${device.EW_REVISION}`

Nombre para mostrar: Versión del agente de Citrix Endpoint Management

- **Elemento web:** `EW_VERSION`
- **Macros:** `${device.EW_VERSION}`

Nombre para mostrar: API de Zebra disponible

- **Elemento web:** `ZEBRA_MDM`
- **Macros:** `${device.ZEBRA_MDM}`

Nombre para mostrar: Versión de Zebra MXMF

- **Elemento web:** `ZEBRA_MDM_VERSION`
- **Macros:** `${device.ZEBRA_MDM_VERSION}`

Nombre para mostrar: Versión del parche de Zebra

- **Elemento web:** `ZEBRA_PATCH_VERSION`

- **Macros:** `${device.ZEBRA_PATCH_VERSION}`

Macros para obtener propiedades de usuario integradas

NOMBRE PARA MOSTRAR	MACROS
`domainname` (nombre de dominio; dominio predeterminado)	`${user.domainname}`
`loginname` (nombre de usuario más nombre de dominio)	`${user.loginname}`
`username` (nombre de inicio de sesión sin el dominio, si lo hubiera)	`${user.username}`

Macros para todas las propiedades de usuario

NOMBRE PARA MOSTRAR	ELEMENTO WEB	MACROS
Intentos de inicio de sesión fallidos de Active Directory	`badpwdcount`	`${user.badpwdcount}`
Correo electrónico de usuario de ActiveSync	`asuseremail`	`${user.asuseremail}`
Origen de datos de ASM	`aspersonsource`	`${user.aspersonsource}`
Nombre de cuenta del programa de implementación de ASM	`asmdepaccount`	`${user.asmdepaccount}`
ID de Apple administrado por ASM	`aspersonmanagedappleid`	`${user.aspersonmanagedappleid}`
Tipo de código de acceso de ASM	`aspersonpasscodetype`	`${user.aspersonpasscodetype}`
ID de persona de ASM	`aspersonid`	`${user.aspersonid}`
Estado de persona de ASM	`aspersonstatus`	`${user.aspersonstatus}`

NOMBRE PARA MOSTRAR	ELEMENTO WEB	MACROS
Título de persona de ASM	`aspersontitle`	`${user.aspersontitle}`
ID único de persona de ASM	`aspersonuniqueid`	`${user.aspersonuniqueid}`
ID de sistema de origen de ASM	`aspersonsourcesystemid`	`${user.aspersonsourcesystemid}`
Calificación de estudiante de ASM	`aspersongrade`	`${user.aspersongrade}`
Email de usuario BES	`besuseremail`	`${user.besuseremail}`
Empresa	`company`	`${user.company}`
Nombre de la empresa	`companyname`	`${user.companyname}`
País	`c`	`${user.c}`
Departamento	`department`	`${user.department}`
Descripción	`description`	`${user.description}`
Usuario deshabilitado	`disableduser`	`${user.disableduser}`
Nombre para mostrar	`displayname`	`${user.displayname}`
Nombre distintivo	`distinguishedname`	`${user.distinguishedname}`
Nombre de dominio	`domainname`	`${user.domainname}`
Correo electrónico	`mail`	`${user.mail}`
Nombre	`givenname`	`${user.givenname}`
Dirección particular	`homestreetaddress`	`${user.homestreetaddress}`
Ciudad de residencia	`homecity`	`${user.homecity}`

NOMBRE PARA MOSTRAR	ELEMENTO WEB	MACROS
País de origen	`homecountry`	`${user.homecountry}`
Fax particular	`homefax`	`${user.homefax}`
Teléfono particular	`homephone`	`${user.homephone}`
Estado/región de origen	`homestate`	`${user.homestate}`
Código postal de origen	`homezip`	`${user.homezip}`
Teléfono IP	`ipphone`	`${user.ipphone}`
Inicial del segundo nombre	`middleinitial`	`${user.middleinitial}`
Segundo nombre	`middlename`	`${user.middlename}`
Móvil	`mobile`	`${user.mobile}`
Nombre	`cn`	`${user.cn}`
Dirección de la oficina	`physicaldeliveryofficename`	`${user.physicaldeliveryofficename}`
Ciudad de la oficina	`l`	`${user.l}`
Número de fax de la oficina	`facsimiletelephonenumber`	`${user.facsimiletelephonenumber}`
Estado/provincia de la oficina	`st`	`${user.st}`
Dirección de la calle de la oficina	`officestreetaddress`	`${user.officestreetaddress}`
Número de teléfono de la oficina	`telephonenumber`	`${user.telephonenumber}`
Código postal de la oficina	`postalcode`	`${user.postalcode}`

NOMBRE PARA MOSTRAR	ELEMENTO WEB	MACROS
Apartado de correos	`postofficebox`	`${user.postofficebox}`
Localizador	`pager`	`${user.pager}`
ID de grupo principal	`primarygroupid`	`${user.primarygroupid}`
Cuenta SAM	`samaccountname`	`${user.samaccountname}`
Dirección postal	`streetaddress`	`${user.streetaddress}`
Apellido	`sn`	`${user.sn}`
Título	`title`	`${user.title}`
Nombre de usuario	`userprincipalname`	`${user.userprincipalname}`

Acciones automatizadas

Puede crear acciones automatizadas en Citrix Endpoint Management para programar una reacción a:

- Eventos
- Propiedades de usuario o dispositivo
- La existencia de aplicaciones en los dispositivos de usuario

Cuando se crea una acción automatizada, los desencadenadores definidos para la acción determinan lo que sucede en el dispositivo del usuario cuando se conecta a Citrix Endpoint Management. Cuando se activa un evento, puede enviar una notificación al usuario para corregir un problema antes de que se tome una medida más grave.

Los efectos que se configuran para que ocurran automáticamente van desde los siguientes:

- Borrar el dispositivo por completo o de forma selectiva.
- Marcar el dispositivo como no conforme.
- Revocar el dispositivo.
- Enviar una notificación al usuario para corregir un problema antes de que se tome una medida más grave.

Puede configurar acciones de bloqueo y borrado de aplicaciones para el modo solo MAM.

Puede usar acciones automatizadas para marcar los dispositivos Windows 10 y Windows 11 unidos a Azure Active Directory (AD) como no conformes en Azure AD.

> **Nota:**

> Antes de poder notificar a los usuarios, debe configurar los servidores de notificaciones en la configuración de Citrix Endpoint Management para SMTP, de modo que Citrix Endpoint Management pueda enviar los mensajes. Para obtener más información, consulte Notificaciones. Configure las plantillas de notificación que planea usar antes de continuar.

> Para obtener más información, consulte Notificaciones. Para configurar, consulte Crear y actualizar plantillas de notificación.

Acciones de ejemplo

Estos son algunos ejemplos de uso de acciones automatizadas:

Ejemplo uno

- Quiere detectar una aplicación que bloqueó anteriormente (por ejemplo, “Words with Friends”). Puede especificar un desencadenador que establezca el dispositivo del usuario como no conforme después de detectar la aplicación “Words with Friends”. La acción notifica a los usuarios que deben eliminar la aplicación para que su dispositivo vuelva a cumplir las normas. También puede establecer un límite de tiempo para esperar a que los usuarios cumplan. Después de ese límite de tiempo, se produce una acción definida, como el borrado selectivo del dispositivo.

Ejemplo dos

- Quiere verificar si los clientes utilizan el firmware más reciente y bloquear el acceso a los recursos si los usuarios tienen que actualizar sus dispositivos. Puede especificar un desencadenador que establezca el dispositivo del usuario como no conforme cuando un dispositivo de usuario no tenga la versión más reciente. Utiliza acciones automatizadas para bloquear recursos y notificar a los clientes.

Ejemplo tres

- Un dispositivo de usuario se pone en un estado de no conformidad y el usuario lo repara. Puede configurar una directiva para implementar un paquete que restablezca el dispositivo a un estado conforme.

Ejemplo cuatro

- Quiere marcar los dispositivos de usuario que han estado inactivos durante un cierto período de tiempo como no conformes. Puede crear una acción automatizada para dispositivos inactivos de la siguiente manera:

  a. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Control de acceso a la red** y, a continuación, seleccione **Dispositivos inactivos**. Para obtener más información sobre el ajuste **Dispositivos inactivos**, consulte Control de acceso a la red.

b. Siga los pasos para agregar una acción, como se describe en Agregar y administrar acciones. La única diferencia es que debe configurar los parámetros de la siguiente manera en la página **Detalles de la acción**:

   - **Desencadenador**. Seleccione **Propiedad del dispositivo**, **No conforme** y **Verdadero**.
   - **Acción**. Seleccione **Enviar notificación** y elija una plantilla que haya creado mediante **Plantilla de notificación** en **Parámetros**. A continuación, establezca el retraso en días, horas o minutos antes de realizar la acción. Establezca el intervalo en el que se repite la acción hasta que el usuario resuelva el problema que la desencadena.

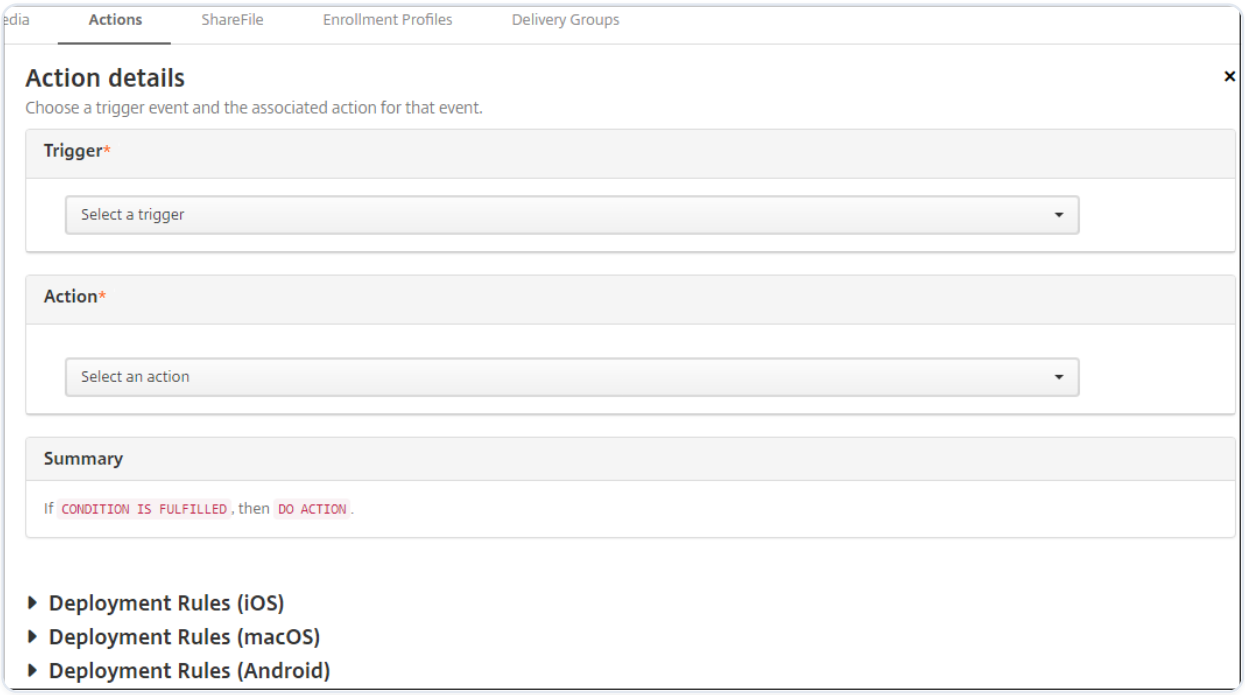
> **Sugerencia:**
>
> Para eliminar dispositivos inactivos de forma masiva, utilice la API REST pública de Citrix Endpoint Management. Primero, obtenga manualmente los ID de los dispositivos inactivos que desea eliminar y, a continuación, ejecute la API de eliminación para eliminarlos de forma masiva.

Agregar y administrar acciones

Para agregar, editar y filtrar acciones automatizadas:

1. Desde la consola de Citrix Endpoint Management, haga clic en **Configurar > Acciones**. Aparece la página **Acciones**.
2. En la página **Acciones**, realice una de las siguientes acciones:
   - Haga clic en **Agregar** para agregar una acción.
   - Seleccione una acción existente para editarla o eliminarla. Haga clic en la opción que desee utilizar.
3. Aparece la página **Información de la acción**.
4. En la página **Información de la acción**, introduzca o modifique la siguiente información:
   - **Nombre:** Escriba un nombre para identificar la acción. Este campo es obligatorio.
   - **Descripción:** Describa lo que se supone que debe hacer la acción.
5. Haga clic en **Siguiente**. Aparece la página **Detalles de la acción**.

El siguiente ejemplo muestra cómo configurar un desencadenador de **Evento**. Si selecciona un desencadenador diferente, las opciones resultantes difieren de las que se muestran aquí.



6. En la página **Detalles de la acción**, introduzca o modifique la siguiente información:

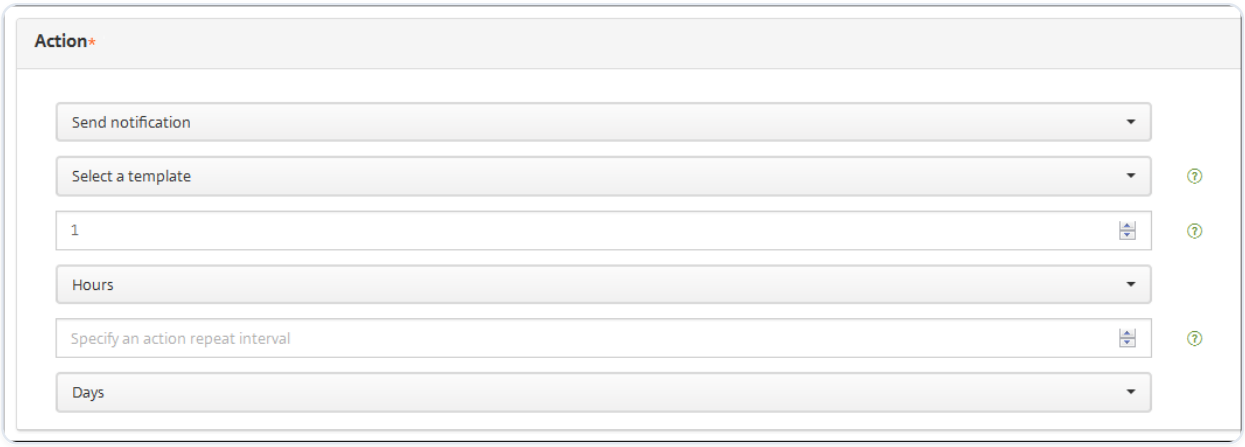
   En la lista **Trigger**, haga clic en el tipo de desencadenador de eventos para esta acción. Seleccione uno de los siguientes desencadenadores:

   - **Event:** Comprueba si el estado del dispositivo coincide con el evento de incumplimiento que elija y, a continuación, reacciona a él.
   - **Device property:** Comprueba un valor específico para un atributo de dispositivo en un dispositivo administrado por MDM y, a continuación, reacciona a él. Para obtener más información, consulte el PDF Nombres y valores de propiedades de dispositivos.
   - **User property:** Reacciona a un valor específico para un atributo de usuario, normalmente de Active Directory.
   - **Installed app name:** Reacciona a la instalación de una aplicación. No se aplica al modo solo MAM. Requiere que la directiva de inventario de aplicaciones esté habilitada en el dispositivo. La directiva de inventario de aplicaciones está habilitada en todas las plataformas de forma predeterminada. Para obtener más información, consulte Directiva de dispositivo de inventario de aplicaciones.
   - **Policy returned value:** Comprueba si el valor devuelto por los scripts de PowerShell cumple ciertos criterios lógicos. La directiva del agente de Windows debe estar habilitada y configurada. Para obtener más información sobre la directiva del agente de Windows, consulte Directiva de dispositivo del agente de Windows.

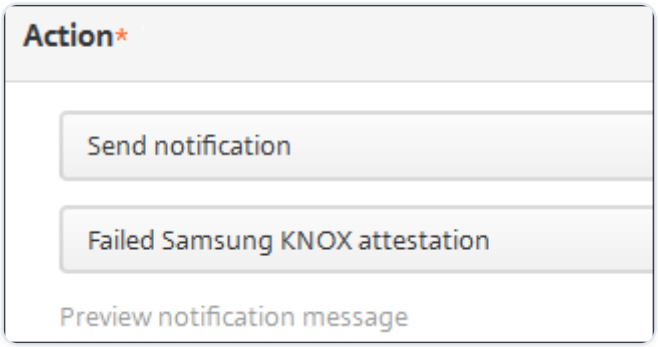
7. En la siguiente lista, haga clic en la respuesta al desencadenador.
8. En la lista **Action**, haga clic en la acción que se realizará cuando se cumpla el criterio de desencadenamiento. Excepto para la acción **Send notification**, usted elige un plazo en el que los usuarios pueden resolver el problema que causó el desencadenador. Si el problema no se resuelve dentro de ese plazo, se realiza la acción seleccionada. Para obtener una definición de las acciones, consulte Acciones de seguridad.

   Si elige **Send notification**, siga estos pasos para enviar una acción de notificación.
9. En la siguiente lista, seleccione la plantilla que se utilizará para la notificación. Aparecen las plantillas de notificación relevantes para el evento seleccionado. Si no hay ninguna plantilla para el tipo de notificación, se le pedirá que configure una plantilla con el mensaje: No hay plantilla para este tipo de evento. Cree una plantilla mediante **Notification Template** en **Settings**.

   Para notificar a los usuarios, utilice **Settings > Notification Server** para configurar los ajustes de SMTP de modo que Citrix Endpoint Management pueda enviar los mensajes. Consulte Notificaciones. Además, antes de continuar, utilice **Settings > Notification Template** para configurar las plantillas de notificación que planea usar. Consulte Crear y actualizar plantillas de notificación.



Después de seleccionar la plantilla, haga clic en **Preview notification message**.



10. En los siguientes campos, establezca el retraso en días, horas o minutos antes de realizar la acción. Establezca el intervalo en el que se repite la acción hasta que el usuario resuelva el problema que la desencadenó.



11. En **Resumen**, verificar que ha creado la acción automatizada según lo previsto.



12. Después de configurar los detalles de la acción, puede configurar las reglas de implementación para cada plataforma individualmente. Para ello, complete el paso 13 para cada plataforma que elija.
13. Configure las reglas de implementación. Para obtener información general sobre cómo configurar las reglas de implementación, consulte Implementar recursos.

    Para este ejemplo:

    - La propiedad del dispositivo debe ser **BYOD**.
    - El dispositivo debe cumplir con el código de acceso.
    - El código de país móvil del dispositivo no puede ser solo Andorra.

14. Cuando haya terminado de configurar las reglas de implementación de la plataforma para la acción, haga clic en **Siguiente**. Aparecerá la página **Asignación de acciones**, donde asignará la acción a uno o varios grupos de entrega. Este paso es opcional.
15. Junto a **Elegir grupos de entrega**, escriba para buscar un grupo de entrega o seleccione grupos de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega para recibir la asignación de aplicaciones**.
16. Expanda **Programación de implementación** y, a continuación, configure los siguientes ajustes:

- Junto a **Implementar**, haga clic en **Activado** para programar la implementación o en **Desactivado** para evitarla. La opción predeterminada es **Activado**. Si elige **Desactivado**, no se requieren otras opciones.
- Junto a **Programación de implementación**, haga clic en **Ahora** o en **Más tarde**. La opción predeterminada es **Ahora**.
- Si hace clic en **Más tarde**, haga clic en el icono del calendario y, a continuación, seleccione la fecha y la hora de implementación.
- Junto a **Condición de implementación**, haga clic en **En cada conexión** o **Solo cuando la implementación anterior haya fallado**. La opción predeterminada está establecida como **En cada conexión**.
- Junto a **Implementar para conexión siempre activa**, haga clic en **Activado** o **Desactivado**. La opción predeterminada está establecida como **Desactivado**.

  Esta opción se aplica cuando ha configurado la clave de implementación en segundo plano de programación en **Parámetros > Propiedades del servidor**.

  > **Nota:**
  >
  > Esta opción se aplica cuando ha configurado la clave de implementación en segundo plano de programación en **Parámetros > Propiedades del servidor**.
  >
  > La opción siempre activa:
  >
  > - No está disponible para dispositivos iOS
  > - No está disponible para clientes de Android y Android Enterprise que comenzaron a usar Citrix Endpoint Management con la versión 10.18.19 o posterior
  > - No se recomienda para clientes de Android y Android Enterprise que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19

> El programa de implementación que configure es el mismo para todas las plataformas. Cualquier cambio que realice se aplica a todas las plataformas, excepto a **Implementar para conexión siempre activa**.

17. Haga clic en **Siguiente**. Aparece la página **Resumen**, donde puede verificar la configuración de la acción.
18. Haga clic en **Guardar** para guardar la acción.

Acciones de bloqueo y borrado de aplicaciones para el modo solo MAM

Puede borrar o bloquear aplicaciones en un dispositivo para las cuatro categorías de desencadenantes que se enumeran en la consola de Citrix Endpoint Management: evento, propiedad del dispositivo, propiedad del usuario y nombre de la aplicación instalada.

Para configurar un borrado o bloqueo automático de aplicaciones

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Acciones**.
2. En la página **Acciones**, haga clic en **Agregar**.
3. En la página **Información de la acción**, introduzca un nombre para la acción y una descripción opcional.
4. En la página **Detalles de la acción**, seleccione el desencadenador que desee.
5. En **Acción**, seleccione una acción.

   Para este paso, tenga en cuenta las siguientes condiciones:

   Cuando el tipo de desencadenador se establece como **Evento** y el valor no es **Usuario de Active Directory inhabilitado**, las acciones de **Borrado de aplicaciones** y **Bloqueo de aplicaciones** no aparecen.

   Cuando el tipo de desencadenador se establece como **Propiedad del dispositivo** y el valor es **Modo perdido de MDM habilitado**, las siguientes acciones no aparecen:

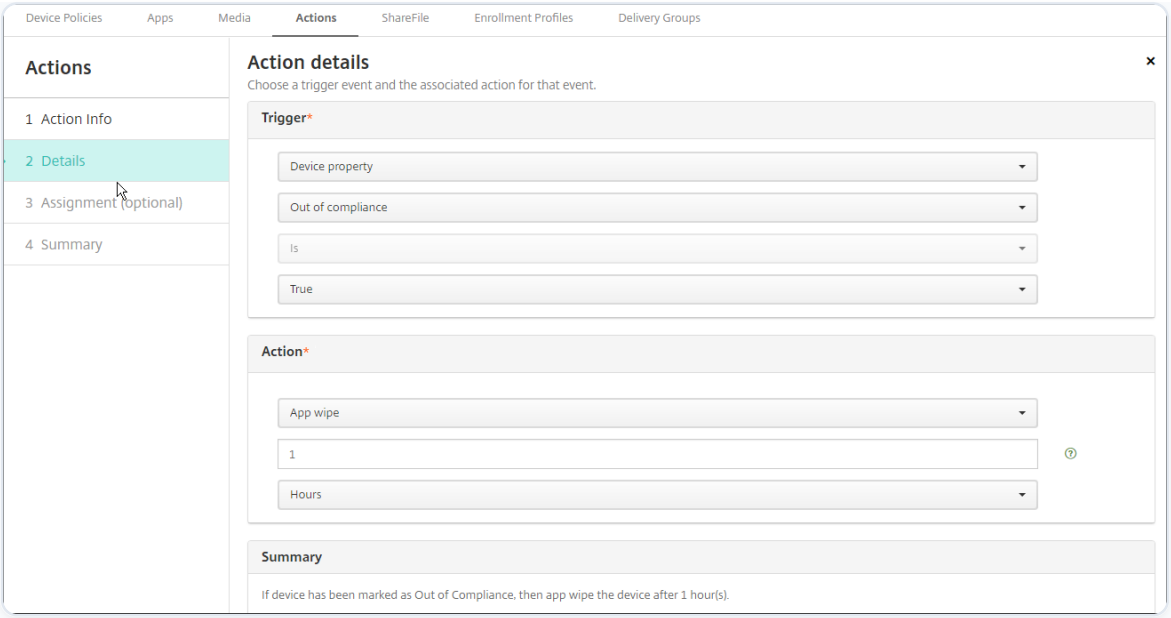
   - Borrar el dispositivo de forma selectiva
   - Borrar el dispositivo por completo
   - Revocar el dispositivo

   Para cada opción, se establece automáticamente un retraso de 1 hora, pero puede seleccionar el período de retraso en minutos, horas o días. La intención del retraso es dar tiempo a los usuarios para solucionar un problema antes de que se produzca la acción. Para obtener más información sobre las acciones de borrado de aplicaciones y bloqueo de aplicaciones, consulte Acciones de seguridad.

Nota:

Si establece el desencadenador en **evento**, el intervalo de repetición es automáticamente de un mínimo de 1 hora. El dispositivo debe actualizar las directivas para sincronizarse con el servidor y recibir la notificación. Normalmente, un dispositivo se sincroniza con el servidor cuando los usuarios inician sesión o actualizan manualmente sus directivas a través de Citrix Secure Hub.

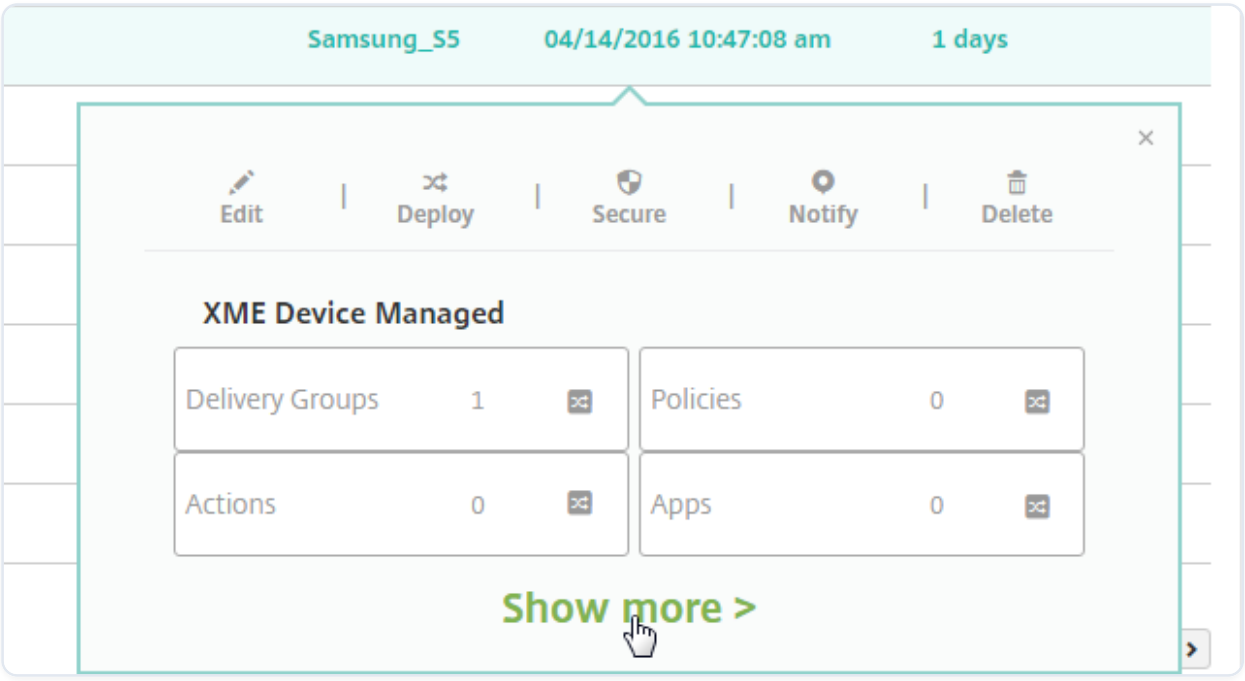
Puede producirse un retraso adicional de aproximadamente 1 hora antes de que se realice cualquier acción, para permitir que la base de datos de Active Directory se sincronice con Citrix Endpoint Management.



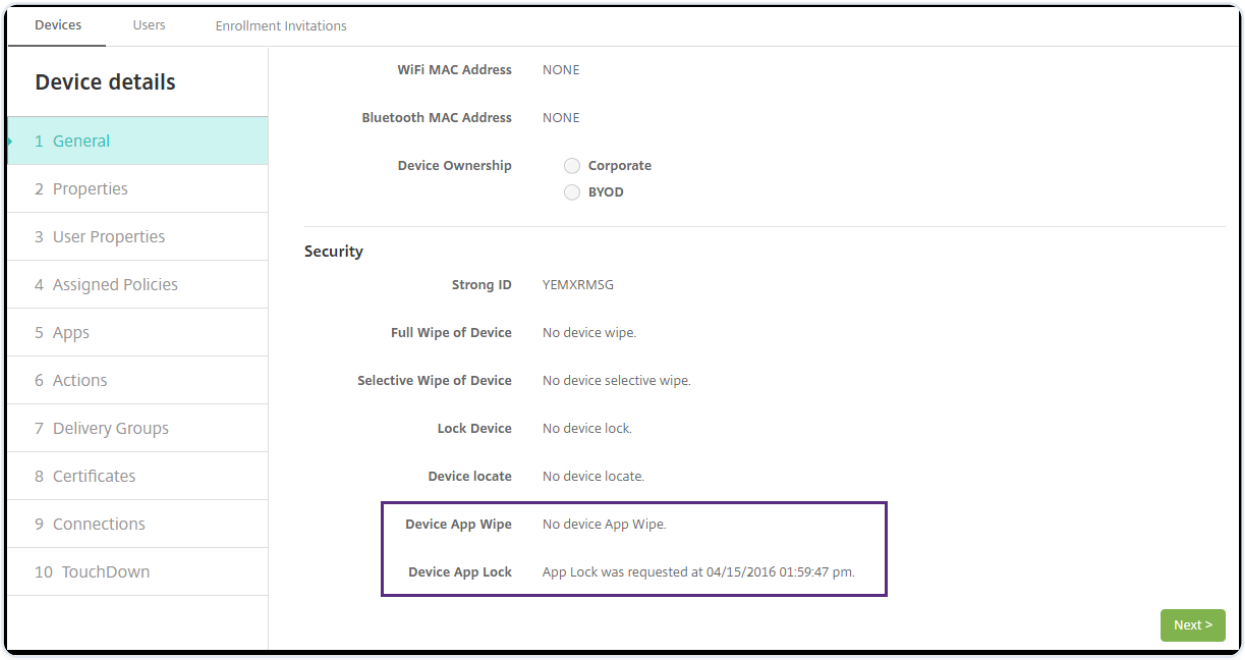
6. Configure las reglas de implementación y, a continuación, haga clic en **Siguiente**.
7. Configure las asignaciones de grupos de entrega y una programación de implementación y, a continuación, haga clic en **Siguiente**.
8. Haga clic en **Guardar**.

Para comprobar el estado de bloqueo o borrado de aplicaciones

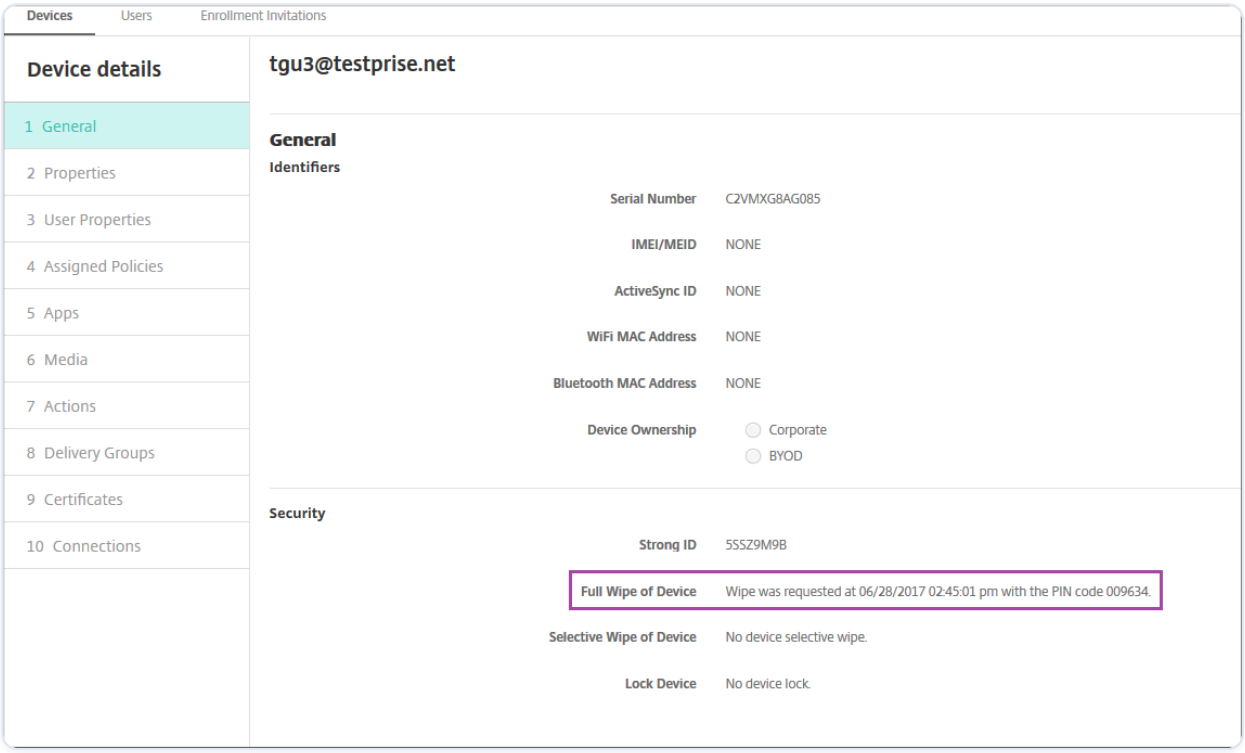
1. Vaya a **Administrar > Dispositivos**, haga clic en un dispositivo y, a continuación, haga clic en **Mostrar más**.



2. Desplácese hasta **Borrado de aplicaciones del dispositivo** y **Bloqueo de aplicaciones del dispositivo**.



Después de borrar un dispositivo, se le pide al usuario que introduzca un código PIN. Si el usuario olvida el código, puede buscarlo en los Detalles del dispositivo.



Marcar dispositivos Windows 10 y Windows 11 como no conformes en Azure AD

Cuando los dispositivos Windows 10 y Windows 11 unidos a Azure AD son marcados como no conformes por Citrix Endpoint Management, también pueden marcarse como no conformes en Azure AD. Para habilitar esta funcionalidad, agregue permisos a la aplicación MDM local para acceder a la API de Microsoft Graph en el portal de Azure AD.

1. Inicie sesión en el portal de Azure AD con sus credenciales de administrador de Azure AD.
2. En el portal de Azure AD, vaya a **Azure Active Directory > Movilidad (MDM y MAM)**. Elija **Aplicación MDM local**.
3. Haga clic en **Configuración de aplicaciones locales > Permisos requeridos > Agregar > Seleccionar una API > Microsoft Graph**. Haga clic en **Seleccionar** y guarde.
4. En **Permisos requeridos**, seleccione **Microsoft Graph**. En **Habilitar acceso**, seleccione **Leer y escribir datos de directorio**.
5. En **Permisos requeridos**, seleccione **Microsoft Graph**. A continuación, haga clic en **Conceder permisos**.
6. Haga clic en **Sí** para conceder el permiso.

Cuando un dispositivo inscrito en Azure AD que ejecuta Windows 10 o Windows 11 no cumple con las directivas, Citrix Endpoint Management también marca el dispositivo como no conforme en Azure AD.

Crear una acción automatizada basada en el resultado de una directiva de dispositivo de Windows Agent

Utilice la directiva de dispositivo de Windows Agent para implementar scripts que supervisan los valores del registro en escritorios y tabletas Windows administrados. Según los valores devueltos por un script, puede configurar una acción automatizada para que se ejecute.

1. Configure una directiva de dispositivo de Windows Agent y compruebe los valores devueltos por el script. Para obtener información sobre la directiva de dispositivo de Windows Agent, consulte Directiva de dispositivo de Windows Agent.

   Ese artículo y esta sección incluyen un ejemplo basado en un script llamado `EntApp_2019_checkFirewall`. La directiva de dispositivo de Windows Agent relacionada define una configuración llamada `cName_checkFirewall`. Esa configuración ejecuta el script de ejemplo.

   Después de que el script se ejecute en un dispositivo, obtendrá la información necesaria para crear una acción, como se describe en la Directiva de dispositivo de Windows Agent.
2. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Acciones**.
3. En la página **Acciones**, haga clic en **Agregar**.
4. En la página **Información de la acción**, introduzca un nombre para la acción y una descripción opcional.
5. En la página **Detalles de la acción**, seleccione el desencadenador **Valor devuelto por la directiva**.

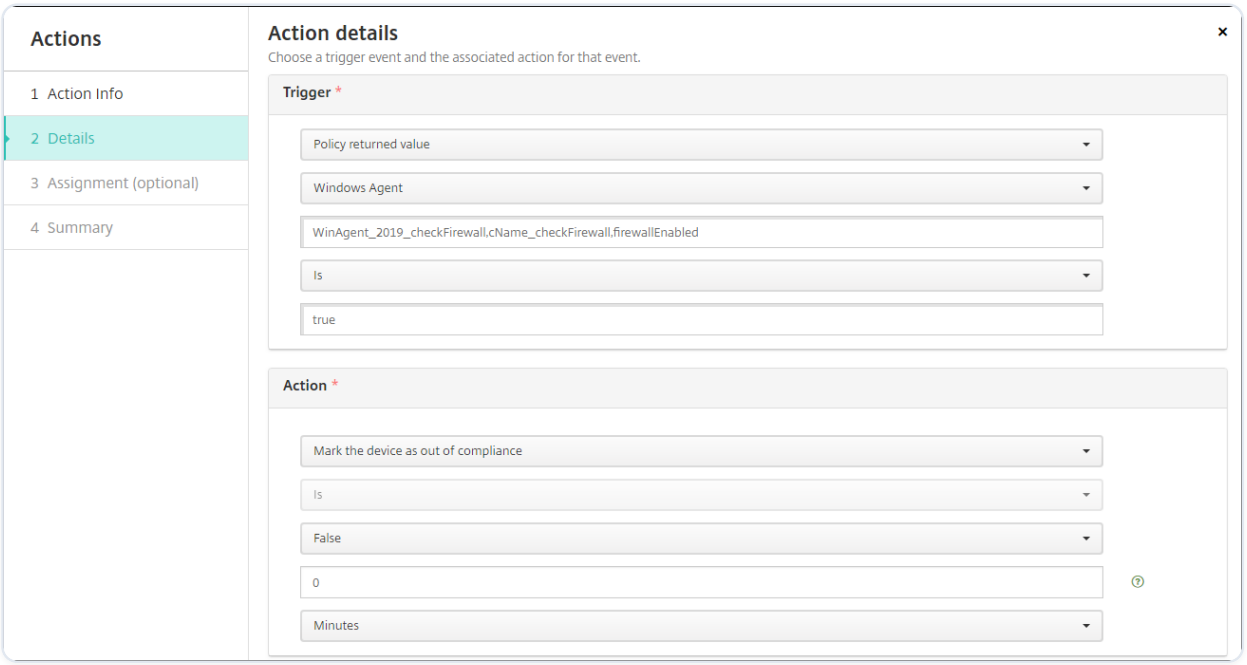


6. En los campos que aparecen, defina el desencadenante y la acción:

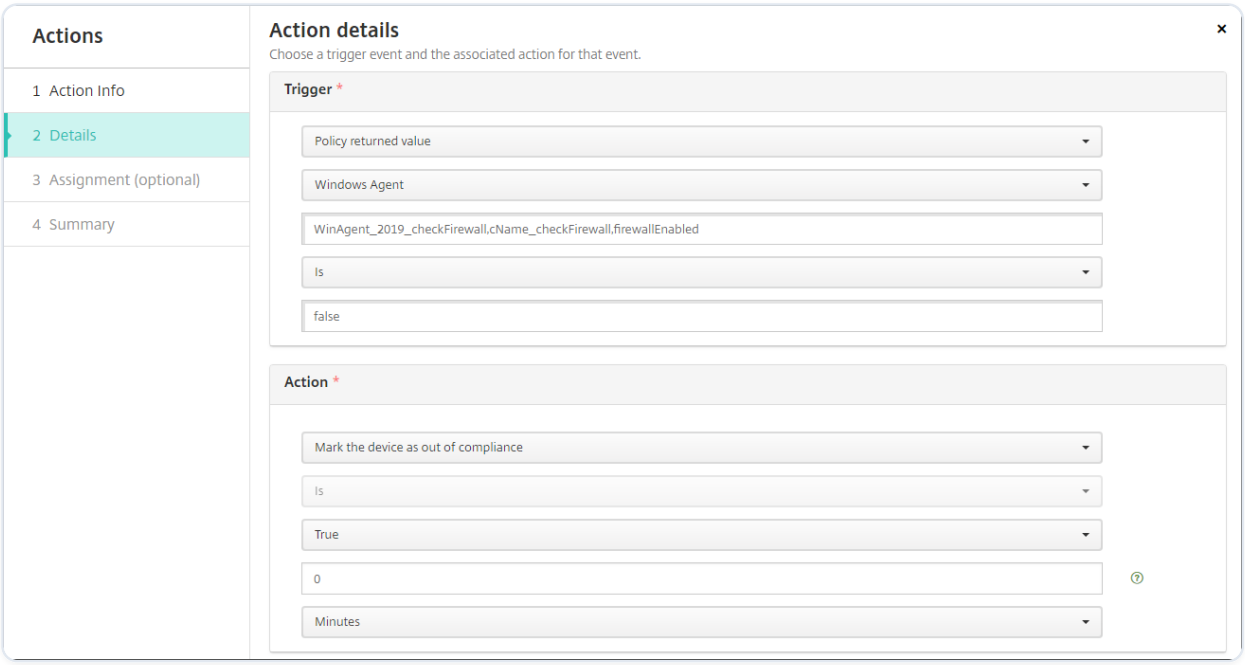
   - **Configuración del agente de Windows:** Escriba el nombre de la directiva, el nombre de la configuración y el nombre de la clave para la directiva del agente de Windows que creó.

- **Menú desplegable:** Seleccione la lógica **Es**, **No es**, **Contiene** o **No contiene**. Esta lógica se aplica al siguiente campo y hace que la acción se active si la lógica se aplica.
- **Introducir una cadena:** Introduzca la cadena resultante de la ejecución del script de PowerShell cargado en su directiva. Para obtener información sobre cómo encontrar esa cadena, consulte Directiva de dispositivo del agente de Windows.
- **Acción:** Seleccione una acción, un valor para la acción y elija un período de tiempo para resolver la acción.

En nuestro ejemplo: Si el nombre de la clave `firewallEnabled` devuelve el valor `true`, la siguiente acción marca el dispositivo como conforme.



Si el nombre de la clave `firewallEnabled` devuelve el valor `false`, la siguiente acción marca el dispositivo como no conforme.



7. Si es necesario, establezca una programación de implementación y elija grupos de entrega.

Supervisar y dar soporte

Puede usar el panel de control de Citrix Endpoint Management y la página de soporte de Citrix Endpoint Management para supervisar y solucionar problemas de su servidor de Citrix Endpoint Management. Utilice la página de soporte de Citrix Endpoint Management para acceder a información y herramientas relacionadas con el soporte.

En la consola de Citrix Endpoint Management, haga clic en el icono de la llave inglesa en la esquina superior derecha.

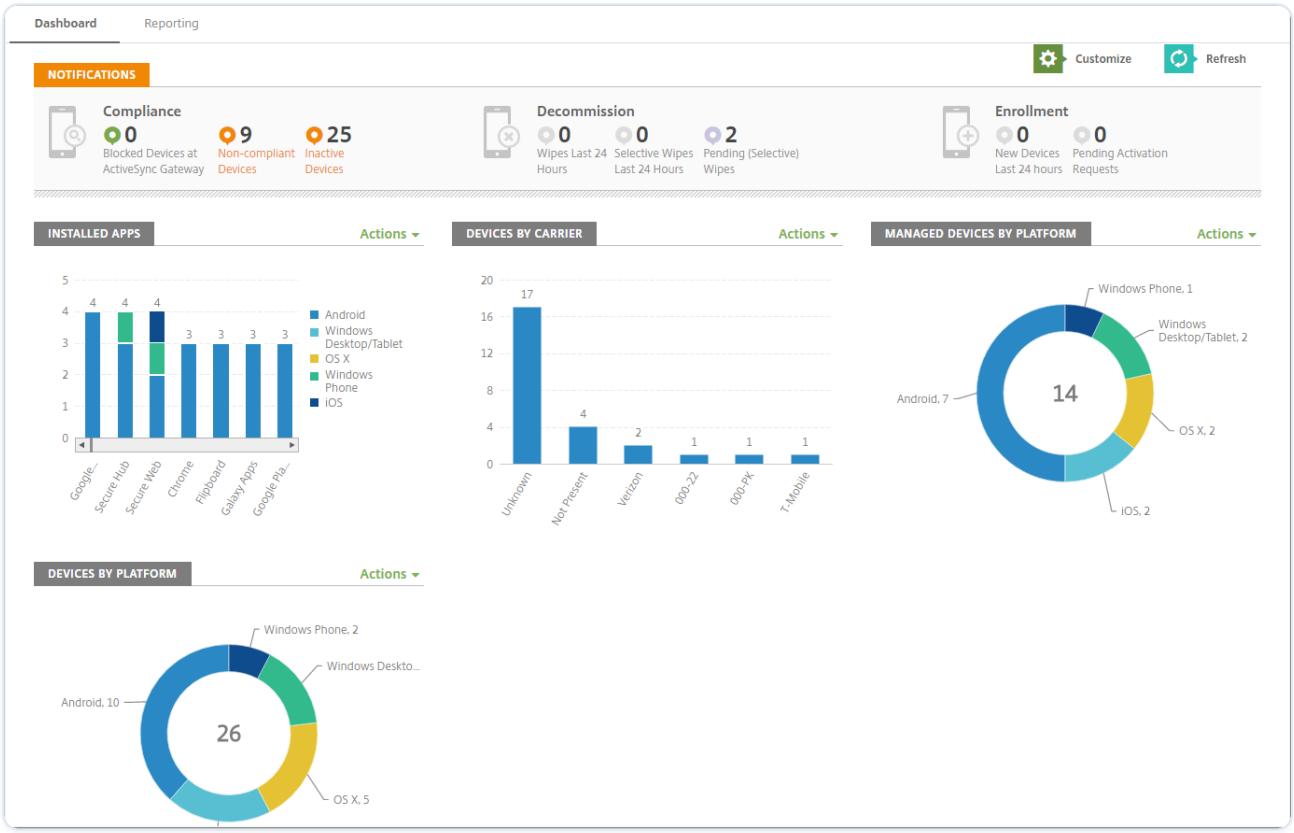


Aparece la página **Solución de problemas y soporte**.

Utilice la página **Solución de problemas y soporte** de Citrix Endpoint Management para:

- Acceder a diagnósticos.
- Acceder a enlaces a la documentación de productos de Citrix y al Knowledge Center.
- Acceder a operaciones de registro.
- Utilizar opciones de configuración avanzadas.
- Acceder a un conjunto de herramientas y utilidades.

También puede ver información de un vistazo accediendo al panel de control de su consola de Citrix Endpoint Management. Con esta información, puede ver rápidamente los problemas y los éxitos mediante widgets.

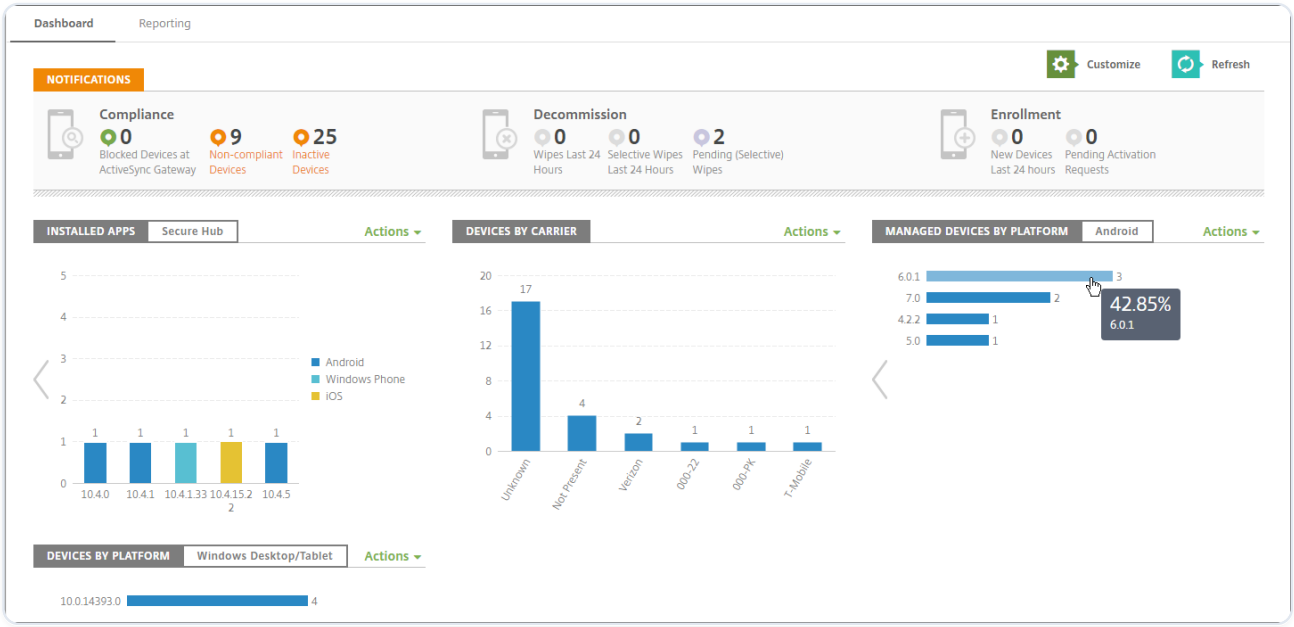


El panel de control suele ser la primera página que aparece al iniciar sesión en la consola de Citrix Endpoint Management. Para acceder al panel de control desde cualquier otra parte de la consola, haga clic en **Analizar**. Haga clic en **Personalizar** en el panel de control para editar el diseño de la página y los widgets que aparecen.

- **Mis paneles de control:** Puede guardar hasta cuatro paneles de control. Puede editar estos paneles de control por separado y ver cada uno seleccionando el panel de control guardado.
- **Estilo de diseño:** En esta fila, puede seleccionar cuántos widgets aparecen en su panel y cómo están dispuestos los widgets.
- **Selección de widgets:** Puede elegir qué información aparece en su panel.
    - **Notificaciones:** Marque la casilla de verificación encima de los números de la izquierda para añadir una barra de notificaciones encima de sus widgets. Esta barra muestra el número de dispositivos conformes, dispositivos inactivos y dispositivos borrados o inscritos en las últimas 24 horas.
    - **Dispositivos por plataforma:** Muestra el número de dispositivos administrados y no administrados por plataforma.
    - **Dispositivos por operador:** Muestra el número de dispositivos administrados y no administrados por operador. Haga clic en cada barra para ver un desglose por plataforma.
    - **Dispositivos administrados por plataforma:** Muestra el número de dispositivos administrados por plataforma.

- **Dispositivos no administrados por plataforma:** Muestra el número de dispositivos no administrados por plataforma. Los dispositivos que aparecen en este gráfico pueden tener un agente instalado, pero sus privilegios están revocados o los dispositivos están borrados.
- **Dispositivos por estado de ActiveSync Gateway:** Muestra el número de dispositivos agrupados por estado de ActiveSync Gateway. La información muestra el estado Bloqueado, Permitido o Desconocido. Puede hacer clic en cada barra para desglosar los datos por plataforma.
- **Dispositivos por propiedad:** Muestra el número de dispositivos agrupados por estado de propiedad. La información muestra el estado de propiedad corporativa, propiedad del empleado o desconocido.
- **Implementaciones fallidas de grupos de entrega:** Muestra el número total de implementaciones fallidas por paquete. Solo aparecen los paquetes que tienen implementaciones fallidas.
- **Dispositivos por motivo de bloqueo:** Muestra el número de dispositivos bloqueados por ActiveSync
- **Aplicaciones instaladas:** Escriba el nombre de una aplicación para ver un gráfico con su información.
- **Uso de licencias de aplicaciones de compra por volumen:** Muestra estadísticas de uso de licencias para las aplicaciones de compra por volumen de Apple.

Con cada widget, puede hacer clic en las partes individuales para profundizar y obtener más información.



También puede exportar la información como un archivo .csv haciendo clic en el menú **Acción**.

Menú del panel de análisis(/en-us/citrix-endpoint-management/media/analyze-dashboard-actions-menu.png)

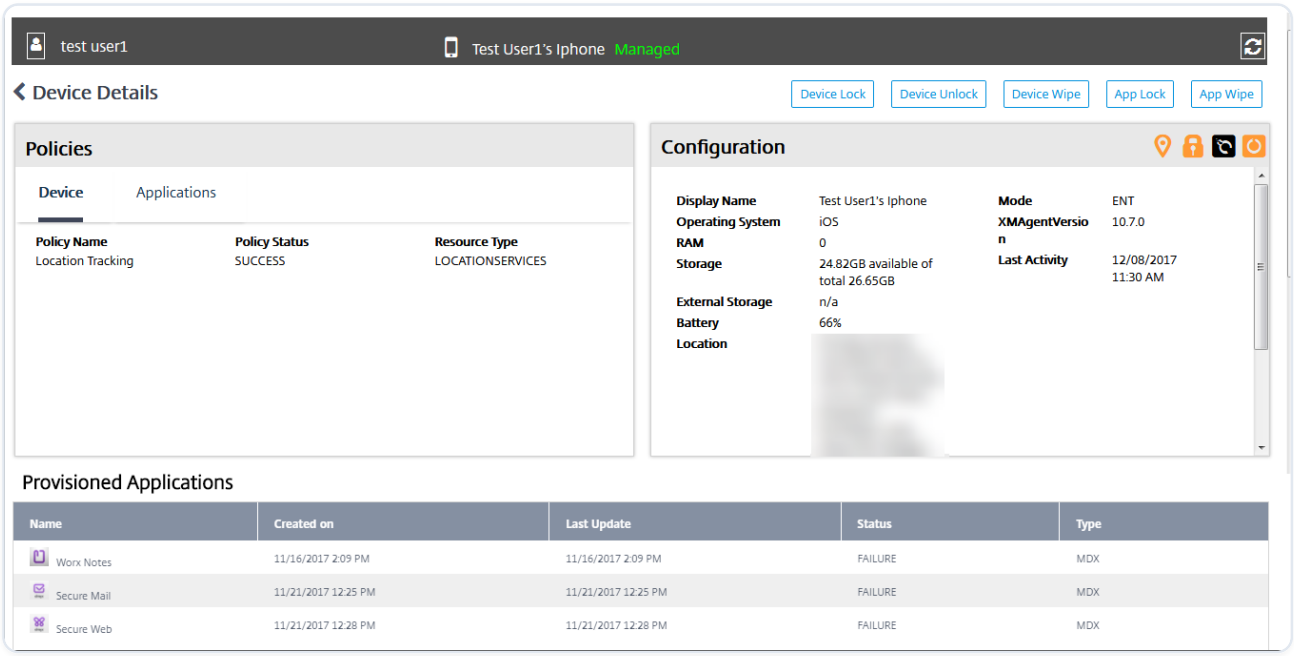
Página de supervisión para administradores de soporte técnico

Puede supervisar y solucionar problemas de Citrix Endpoint Management en la página de **Supervisión**. Esta interfaz está personalizada para que los administradores de soporte técnico realicen la solución de problemas basada en el usuario de forma eficiente.

Los administradores de soporte técnico deben tener los siguientes permisos para acceder a la página de **Supervisión** y a todos los flujos de trabajo disponibles:

- Acceso autorizado
    - Acceso a la consola de administración
    - Acceso a la API pública
- Funciones de la consola
    - Supervisión
    - Dispositivos
    - Borrar dispositivo por completo
    - Ver ubicaciones
        - Localizar dispositivo
        - Rastrear dispositivo
    - Bloquear dispositivo
    - Desbloquear dispositivo
    - Bloqueo
    - Borrado
    - Aplicación

La página **Monitor** le ofrece una vista combinada de las directivas y la configuración del dispositivo. La vista incluye acciones de solución de problemas como el bloqueo/desbloqueo de aplicaciones, el borrado de aplicaciones, el bloqueo/desbloqueo de dispositivos y el borrado de dispositivos.



Utilice la página **Monitor** para:

- Busque un usuario y un dispositivo de Active Directory (AD) que desee solucionar.
- Analice la página **Detalles del dispositivo** que contiene lo siguiente:
  - **Directivas:** Muestra las directivas de dispositivo y aplicación para el dispositivo y la aplicación seleccionados. Para obtener información sobre cómo modificar las directivas, consulte Directivas de dispositivo y Agregar aplicaciones.
  - **Configuración:** Muestra la configuración del dispositivo. Este panel incluye iconos que indican si el dispositivo tiene los servicios de ubicación habilitados, si tiene jailbreak y si está administrado por MDM o MAM. El panel también muestra el estado del cifrado de almacenamiento.
  - **Tabla de aplicaciones en ejecución:** Muestra los detalles de las aplicaciones que se están ejecutando actualmente en el dispositivo.
- Solucione problemas del dispositivo. Las acciones de seguridad disponibles en esta página se basan en la inscripción del dispositivo y en los permisos disponibles para el administrador que ha iniciado sesión:
  - Bloqueo/desbloqueo del dispositivo
  - Borrado de dispositivo
  - Bloqueo/desbloqueo de aplicaciones (disponible si el dispositivo está inscrito en MAM)
  - Borrado de aplicaciones (disponible si el dispositivo está inscrito en MAM)

Para obtener más información sobre las acciones que puede realizar, consulte Acciones de seguridad.

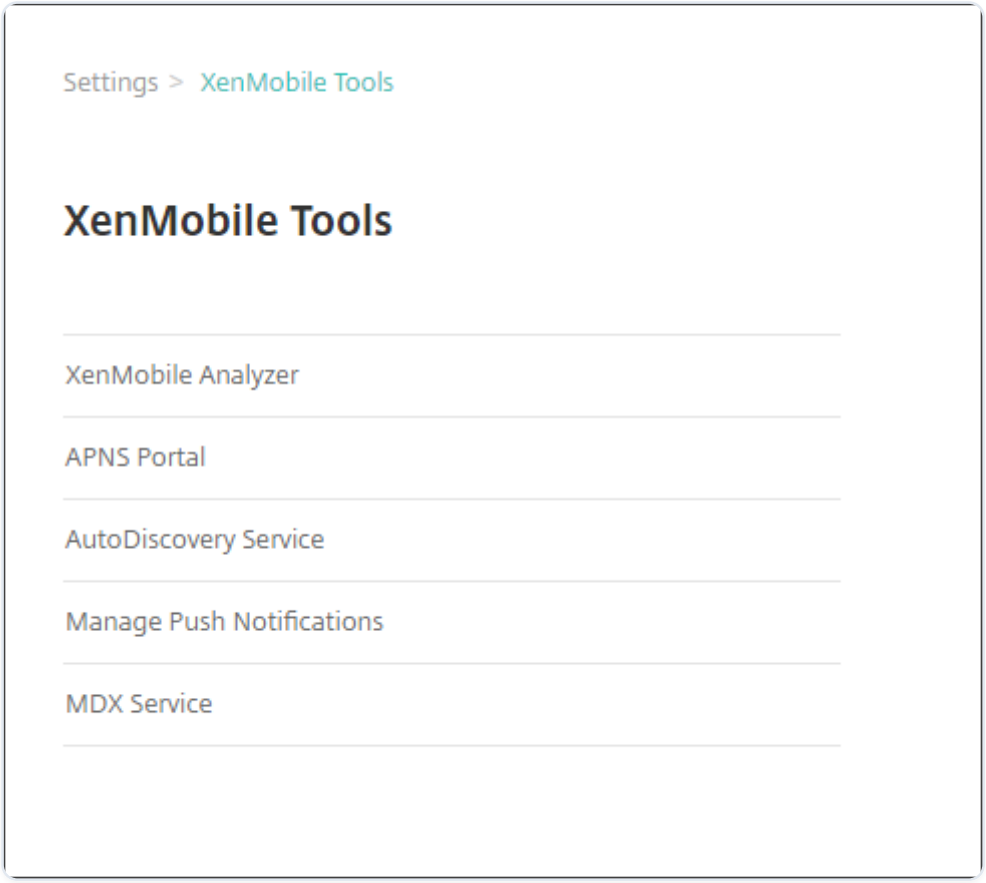
Es posible que la página Monitor no funcione como se espera 60 minutos después de su última carga, ya que no gestiona las actualizaciones del token de inicio de sesión. Como solución alternativa, actualice el token recargando la página: Haga clic en el enlace **Citrix Cloud** en la consola de su servicio y, a continuación, haga clic en **Citrix Endpoint Management > Administrar > Monitorizar**.

Acceso a las herramientas de Citrix Endpoint Management desde la consola

Puede acceder a estas herramientas de Citrix Endpoint Management desde la consola de Citrix Endpoint Management:

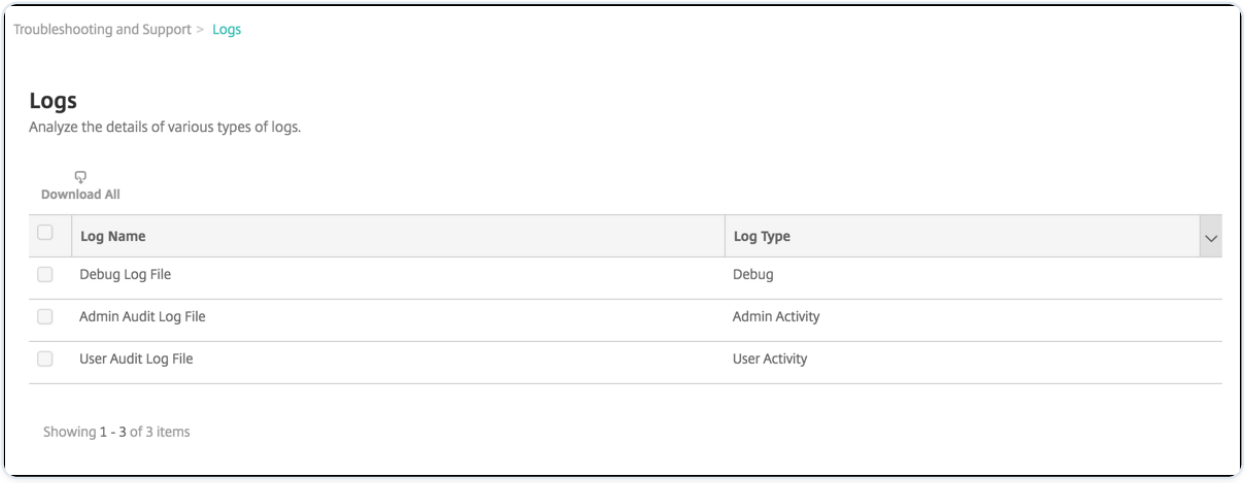
- **Portal APNs** – Envíe una solicitud a Citrix para firmar un certificado APNs, que luego enviará a Apple.
- **Servicio de detección automática** – Solicite y configure la detección automática para Citrix Endpoint Management en su dominio.
- **Administrar notificaciones push** – Administre las notificaciones push para aplicaciones móviles iOS y Windows.

Para acceder a estas herramientas, vaya a **Configuración > Herramientas de Citrix Endpoint Management**. Esta página está disponible para los usuarios con el rol de Administrador de la nube o Administrador de clientes.



Ver y analizar archivos de registro en Citrix Endpoint Management

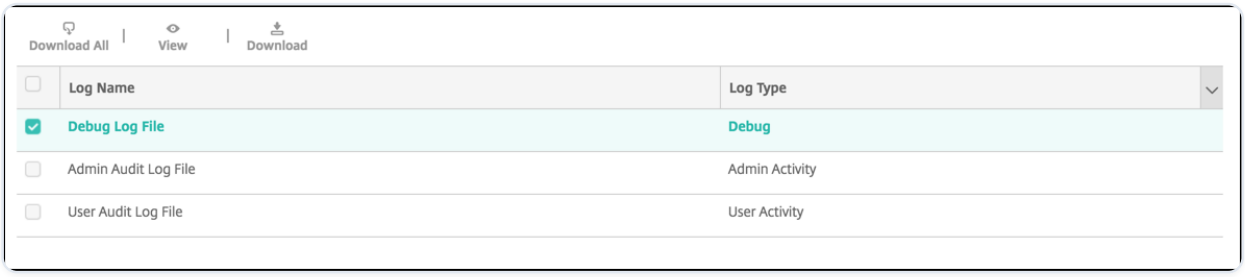
1. En la consola de Citrix Endpoint Management, haga clic en el icono de la llave inglesa en la esquina superior derecha de la consola. Se abrirá la página **Solución de problemas y soporte**.
2. En **Operaciones de registro**, haga clic en **Registros**. Aparecerá la página **Registros**. Los registros individuales aparecen en una tabla.



3. Seleccione el registro que desea ver:

- Los archivos de registro de depuración contienen información útil para el soporte de Citrix, como mensajes de error y acciones relacionadas con el servidor.
- Los archivos de registro de auditoría de administrador contienen información de auditoría sobre la actividad en la consola de Citrix Endpoint Management.
- Los archivos de registro de auditoría de usuario contienen información relacionada con los usuarios configurados.

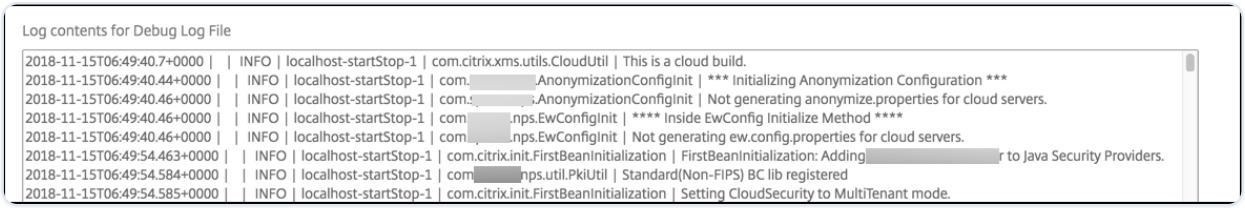
4. Utilice las acciones en la parte superior de la tabla para descargar todos, ver o descargar un solo registro.



> **Nota:**
>
> Si selecciona varios archivos de registro, solo estará disponible **Descargar todo**.

5. Realice una de las siguientes acciones:

- **Descargar todo:** La consola descarga todos los registros presentes en el sistema (incluidos los de depuración, auditoría de administrador, auditoría de usuario, registros del servidor, etc.).
- **Ver:** Muestra el contenido del registro seleccionado debajo de la tabla.
- **Descargar:** La consola descarga solo el tipo de archivo de registro único seleccionado. La consola también descarga cualquier registro archivado de ese mismo tipo.



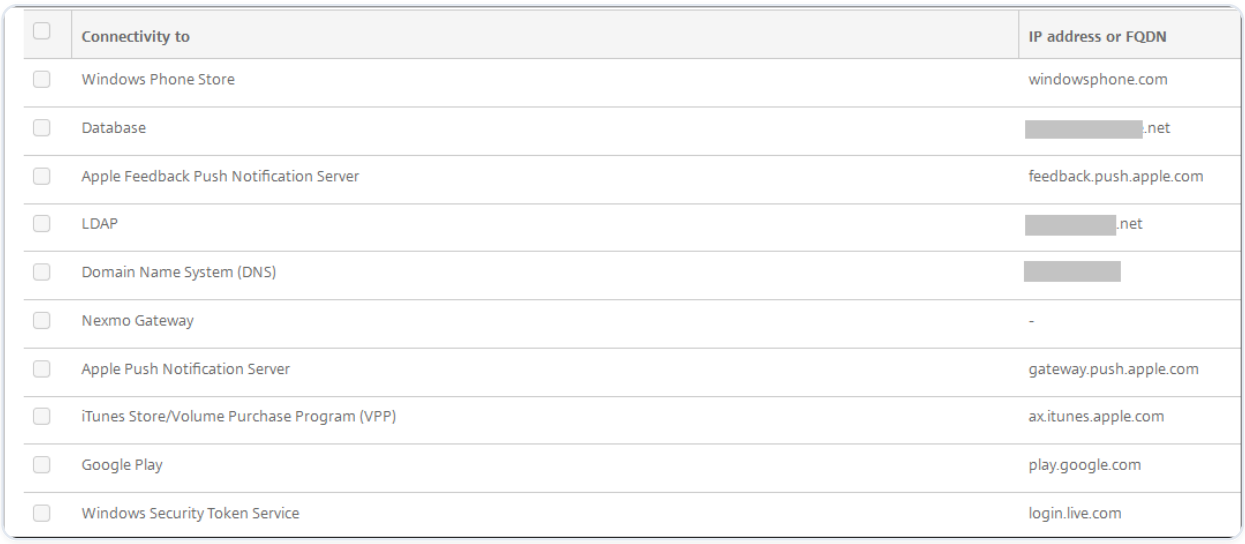
Citrix Endpoint Management utiliza el anexador de syslog log4j para enviar mensajes de syslog con formato RFC5424. Los datos del mensaje de syslog son texto sin formato sin un formato específico.

Comprobaciones de conectividad

Desde la página **Solución de problemas y soporte** de Citrix Endpoint Management, puede comprobar la conexión de Citrix Endpoint Management a NetScaler Gateway y a otros servidores y ubicaciones. Para ejecutar las comprobaciones de conectividad de Citrix Endpoint Management, necesita el rol de Soporte o de Administrador. Establezca este rol mediante el Control de acceso basado en roles (RBAC). Para obtener más información sobre la asignación de roles, consulte Configurar roles con RBAC.

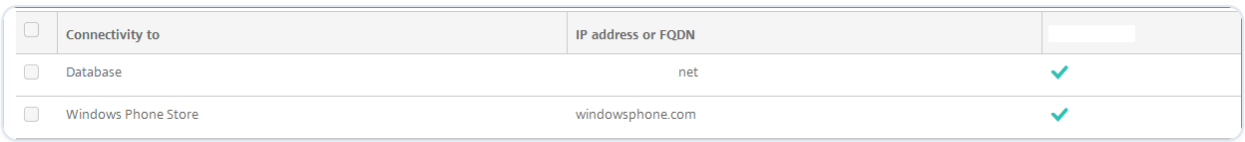
Ejecutar comprobaciones de conectividad de Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, haga clic en el icono de la llave inglesa en la esquina superior derecha de la consola. Aparece la página **Solución de problemas y soporte**.
2. En **Diagnóstico**, haga clic en **Comprobaciones de conectividad de Citrix Endpoint Management**. Aparece la página **Comprobaciones de conectividad de Citrix Endpoint Management**. Si su entorno de Citrix Endpoint Management tiene nodos agrupados, se muestran todos los nodos.



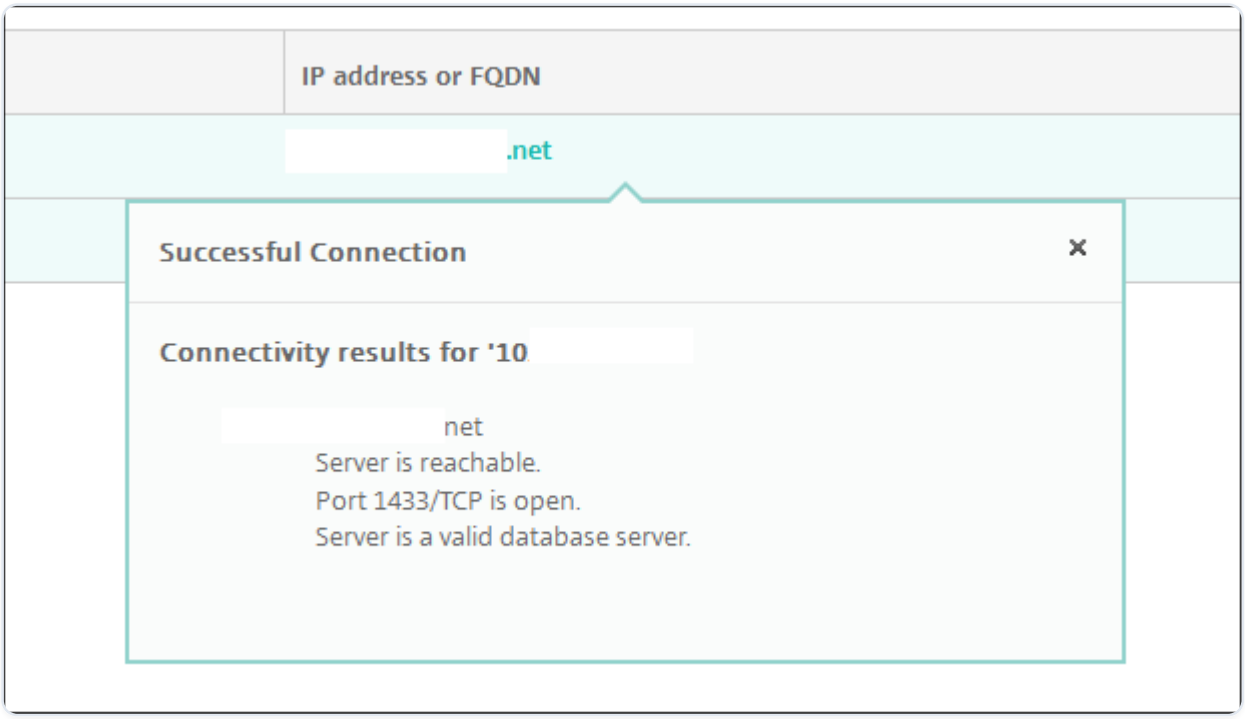
Connectivity to	IP address or FQDN
Windows Phone Store	windowsphone.com
Database	[redacted].net
Apple Feedback Push Notification Server	feedback.push.apple.com
LDAP	[redacted].net
Domain Name System (DNS)	[redacted]
Nexmo Gateway	-
Apple Push Notification Server	gateway.push.apple.com
iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
Google Play	play.google.com
Windows Security Token Service	login.live.com

3. Seleccione los servidores que desea incluir en la prueba de conectividad y, a continuación, haga clic en **Probar conectividad**. Aparece la página de resultados de la prueba.



Connectivity to	IP address or FQDN	
Database	net	✓
Windows Phone Store	windowsphone.com	✓

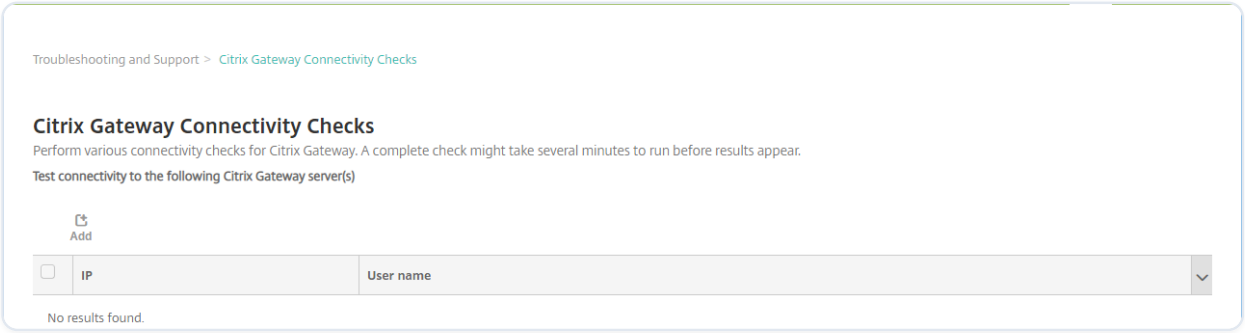
4. Seleccione un servidor en la tabla de resultados de la prueba para ver los resultados detallados de ese servidor.



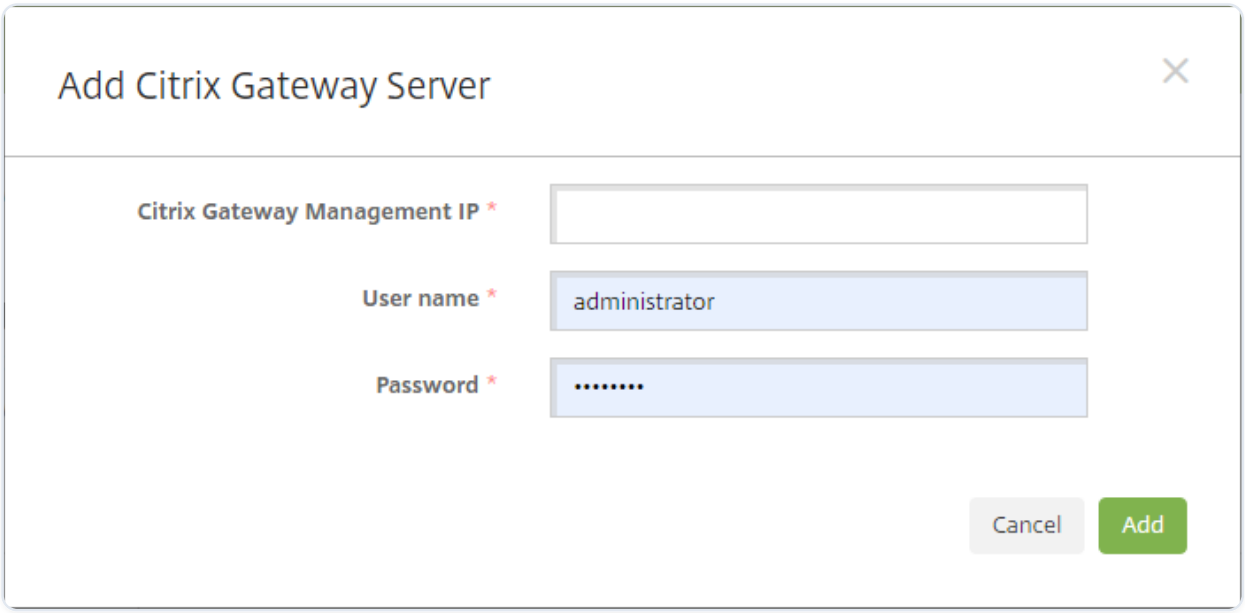
Para obtener más información sobre las comprobaciones de conectividad que puede realizar Citrix Endpoint Management y sus detalles, consulte Detalles de la comprobación de conectividad.

Realizar comprobaciones de conectividad de NetScaler Gateway

1. En la página **Solución de problemas y soporte**, en **Diagnóstico**, haga clic en **Comprobaciones de conectividad de NetScaler Gateway**. Aparece la página **Comprobaciones de conectividad de NetScaler Gateway**. La tabla está vacía si no hay conexión entre Citrix Endpoint Management y NetScaler Gateway.



2. Haga clic en **Agregar**. Aparece el cuadro de diálogo **Agregar servidor NetScaler Gateway**.



3. En **NetScaler Gateway Management IP**, escriba la dirección IP de administración del servidor que ejecuta NetScaler Gateway que desea probar.

   Si está realizando una comprobación de conectividad para un servidor NetScaler Gateway que ya se ha agregado anteriormente, se proporciona la dirección IP.

4. Escriba sus credenciales de administrador para este NetScaler Gateway.

   Si está realizando una comprobación de conectividad para un servidor NetScaler Gateway que ya se ha agregado anteriormente, se proporciona el nombre de usuario.

5. Haga clic en **Agregar**. El NetScaler Gateway se agrega a la tabla de la página **Comprobaciones de conectividad de NetScaler Gateway**.

6. Seleccione el servidor NetScaler Gateway y, a continuación, haga clic en **Probar conectividad**. Los resultados aparecen en una tabla de resultados de prueba.

7. Seleccione un servidor en la tabla de resultados de prueba para ver los resultados detallados de ese servidor.

Detalles de la comprobación de conectividad

La siguiente tabla enumera varias comprobaciones de conectividad que Citrix Endpoint Management puede realizar e incluye detalles sobre cada comprobación.

CONECTIVIDAD CON	DIRECCIÓN IP O FQDN	DETALLES
Servidor de notificaciones push de Apple	api.push.apple.com	Comprueba la conectividad entre el servidor de notificaciones push de Apple y el nodo de Citrix Endpoint

CONECTIVIDAD CON	DIRECCIÓN IP O FQDN	DETALLES
		Management. El servidor de notificaciones push de Apple es necesario para enviar mensajes a dispositivos iOS y macOS.
Servidor de notificaciones push de comentarios de Apple	feedback.push.apple.com	Comprueba la conectividad entre el servidor de comentarios de Apple y el nodo de Citrix Endpoint Management. El servidor de notificaciones push de comentarios de Apple le proporciona información sobre las notificaciones remotas fallidas enviadas a dispositivos iOS y macOS.
Servidor de licencias de Citrix	Dirección IP del servidor de licencias	Comprueba la conectividad entre el servidor de licencias de Citrix y el nodo de Citrix Endpoint Management. Los servidores que ejecutan productos Citrix se ponen en contacto con el servidor de licencias de Citrix para obtener licencias.
NetScaler Gateway	FQDN de NetScaler Gateway configurado en Citrix Endpoint Management	Comprueba la conectividad entre NetScaler Gateway y el nodo de Citrix Endpoint Management. Las aplicaciones cliente de Citrix Endpoint Management (como Citrix Secure Mail y Citrix Secure Web) utilizan NetScaler Gateway para conectarse a través de un servidor VPN para acceder a redes internas.

CONECTIVIDAD CON	DIRECCIÓN IP O FQDN	DETALLES
Base de datos	Dirección IP o FQDN del servidor de bases de datos	Comprueba la conectividad entre la base de datos de Citrix Endpoint Management y el nodo de Citrix Endpoint Management.
Sistema de nombres de dominio (DNS)	Dirección IP configurada en Citrix Endpoint Management	Comprueba la conectividad entre el servidor DNS y el nodo de Citrix Endpoint Management.
Servicio de Secure Ticket Authority	host local	Comprueba la conexión del nodo de Citrix Endpoint Management a los servicios de autenticación, los servicios STA (Secure Ticket Authority) y los servicios de clúster.
Servidor de Firebase Cloud Messaging (FCM)		Comprueba la conectividad entre el servidor FCM y el nodo de Citrix Endpoint Management. Con FCM, puede notificar a una aplicación cliente que hay un nuevo correo electrónico u otros datos disponibles para sincronizar. Puede enviar mensajes de notificación para fomentar la participación y retención de los usuarios. FCM es un reemplazo de Google Cloud Messaging (GCM).
Google Play	play.google.com	Comprueba la conectividad entre el servidor de Google Store y el nodo de Citrix Endpoint Management. Google Play se utiliza para ofrecer servicios que incluyen

CONECTIVIDAD CON	DIRECCIÓN IP O FQDN	DETALLES
		una tienda de entrega de aplicaciones empresariales privada y administrada.
iTunes Store/Compra por volumen	vpp.itunes.apple.com	Comprueba la conectividad entre el servidor de Apple Store y el nodo de Citrix Endpoint Management. Apple Store se utiliza para ofrecer servicios que incluyen una tienda de entrega de aplicaciones empresariales privada y administrada.
LDAP	Dirección IP o FQDN de LDAP configurado en Citrix Endpoint Management	Comprueba la conectividad entre el servidor LDAP y el nodo de Citrix Endpoint Management.
Servidor de notificaciones push de Microsoft	sin.notifiy.windows.com	Comprueba la conectividad entre el servidor de notificaciones de Windows y el nodo de Citrix Endpoint Management. El servidor de notificaciones de Windows se utiliza para enviar mensajes a los dispositivos Windows.
Servicio ShareFile	Dirección IP o FQDN del servicio ShareFile configurado en Citrix Endpoint Management	Comprueba la conectividad entre el servicio ShareFile y Citrix Endpoint Management. El servicio ShareFile es una plataforma segura basada en la nube para que las empresas almacenen y compartan archivos grandes.
Tienda de escritorio/tableta de Windows	windows.microsoft.com	Comprueba la conectividad entre la Tienda de escritorio/ tableta de Windows y el nodo de Citrix Endpoint Management. La Tienda de

CONECTIVIDAD CON	DIRECCIÓN IP O FQDN	DETALLES
		escritorio/tableta de Windows se utiliza para ofrecer servicios que incluyen una tienda de entrega de aplicaciones empresariales privada y administrada.
Servicio de tokens de seguridad de Windows	login.live.com	Comprueba la conectividad entre el servidor de tokens de seguridad de Windows y el nodo de Citrix Endpoint Management. El servicio de tokens de seguridad de Windows admite la autenticación de dos factores (dominio más token de seguridad) para dispositivos Windows.

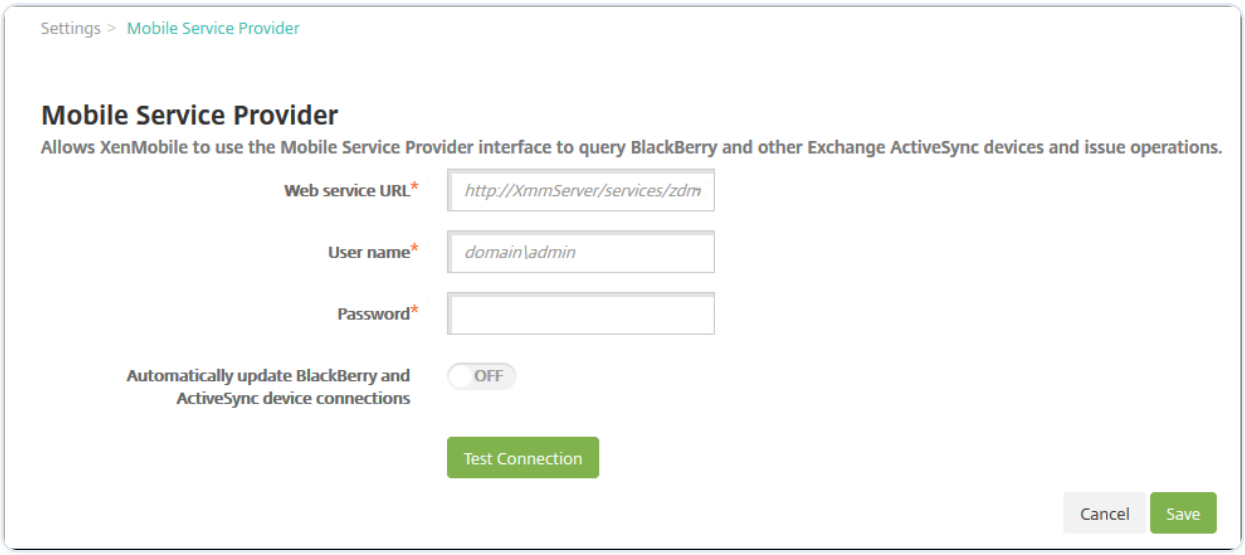
Proveedor de servicios móviles

Puede habilitar Citrix Endpoint Management para usar la interfaz del Proveedor de servicios móviles para consultar dispositivos BlackBerry y Exchange ActiveSync y emitir operaciones.

Por ejemplo, suponga que su organización tiene 1000 usuarios y cada usuario utiliza uno o más dispositivos. Después de indicar a todos los usuarios que inscriban sus dispositivos en Citrix Endpoint Management, la consola de Citrix Endpoint Management indica el número de dispositivos que los usuarios inscriben. Al configurar este ajuste, puede determinar cuántos dispositivos se conectan al servidor de Exchange. De esta manera, puede hacer lo siguiente:

- Determinar si algún usuario todavía tiene que inscribir sus dispositivos.
- Emitir comandos a los dispositivos de los usuarios que se conectan al servidor de Exchange, como borrados de datos.

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha. Aparece la página **Configuración**.
2. En **Servidor**, haga clic en **Proveedor de servicios móviles**. Aparece la página **Proveedor de servicios móviles**.



3. Configure estos ajustes:

   - **URL del servicio web:** Escriba la URL del servicio web; por ejemplo, `https://XmmServer/services/xdmservice`.
   - **Nombre de usuario:** Escriba el nombre de usuario en el formato `domain\\admin`.
   - **Contraseña:** Escriba la contraseña.
   - **Actualizar automáticamente las conexiones de dispositivos BlackBerry y ActiveSync:** Seleccione si desea actualizar automáticamente las conexiones de dispositivos. El valor predeterminado es **Desactivado**
   - Haga clic en **Probar conexión** para verificar la conectividad.

4. Haga clic en **Guardar**.

Informes

Citrix Endpoint Management proporciona los siguientes informes predefinidos que le permiten analizar las implementaciones de sus aplicaciones y dispositivos. Cada informe aparece como una tabla y un gráfico. Puede ordenar y filtrar las tablas por columna. Puede seleccionar elementos en el gráfico para obtener información más detallada.

- **Intentos de implementación total de aplicaciones:** Enumera las aplicaciones implementadas que los usuarios intentaron instalar en sus dispositivos.
- **Aplicaciones por plataforma:** Enumera las aplicaciones y las versiones de las aplicaciones por plataforma y versión del dispositivo.
- **Aplicaciones por tipo:** Enumera las aplicaciones por versión, tipo y categoría.
- **Inscripción de dispositivos:** Enumera todos los dispositivos inscritos.

- **Dispositivos y aplicaciones:** Enumera los dispositivos que ejecutan aplicaciones administradas.
- **Dispositivos inactivos:** Una lista de dispositivos que no han tenido actividad durante el número de días especificado por la propiedad del servidor de Citrix Endpoint Management `device.inactivity.days.threshold`.
- **Dispositivos con jailbreak/rooteados:** Enumera los dispositivos iOS con jailbreak y los dispositivos Android rooteados.
- **Términos y condiciones:** Enumera los usuarios que han aceptado y rechazado los acuerdos de Términos y condiciones. Puede seleccionar áreas del gráfico para ver más detalles.
- **Las 10 implementaciones fallidas principales:** Enumera hasta 10 aplicaciones que no se han podido implementar.
- **Aplicaciones bloqueadas por dispositivo y usuario**: Enumera las aplicaciones de la lista de bloqueo que los usuarios tienen en sus dispositivos.
- **Dispositivos no conformes:** Enumera los dispositivos que no cumplen los criterios de conformidad. Los criterios incluyen si el dispositivo tiene jailbreak, la versión del sistema operativo que se ejecuta y si el dispositivo tiene un código de acceso. El informe también muestra el nombre de usuario asociado al dispositivo y si el dispositivo está cifrado. Para los dispositivos iOS, la columna de cifrado muestra N/A.

Puede exportar los datos de cada tabla en formato .csv, que se abre en programas como Microsoft Excel. Los gráficos de cada informe se pueden exportar en formato PDF.

La ficha **Informes** incluye detalles del dispositivo, como el número de serie, IMEI/MEID, aplicaciones y conexiones. Para obtener informes más completos sobre un dispositivo específico, vaya a **Administrar > Dispositivos**, haga clic en ese dispositivo, haga clic en **Mostrar más** y, a continuación, vea la página **Detalles del dispositivo**. La página **Detalles del dispositivo** enumera las propiedades de seguridad del dispositivo, las propiedades del dispositivo, las directivas asignadas, las aplicaciones, las acciones, los certificados y mucho más. Para obtener información sobre la página **Detalles del dispositivo**, consulte Obtener información sobre los dispositivos.

Los siguientes aspectos determinan cómo Citrix Endpoint Management recopila información sobre las aplicaciones implementadas o instaladas en los dispositivos administrados:

- Tipo de dispositivo
- Método de inscripción
- Si la (/es-es/citrix-endpoint-management/policies/app-inventory-policy.html) está implementada

Para los dispositivos Android, el comportamiento es diferente según el tipo de dispositivo y el método de inscripción. La siguiente tabla indica dónde se enumeran las aplicaciones para **Android Enterprise** (página **Detalles del dispositivo**, informes o no disponible). Las listas de aplicaciones incluyen todas las aplicaciones, a menos que se indique lo contrario.

	MDM+MAM (TODAS LAS APLICACIONES)	MDM (TODAS LAS APLICACIONES)
Aplicaciones obligatorias (la directiva de inventario de aplicaciones no está implementada)	Página **Detalles del dispositivo** e informes	Aplicaciones públicas; página **Detalles del dispositivo** e informes
Aplicaciones opcionales (la directiva de inventario de aplicaciones no está implementada)	No disponible	No disponible
Aplicaciones obligatorias (la directiva de inventario de aplicaciones está implementada)	Página **Detalles del dispositivo** e informes	Página de **detalles del dispositivo** e informes
Aplicaciones opcionales (la política de inventario de aplicaciones está implementada)	Aplicaciones empresariales, MDX, públicas y de enlace web; informes	Página de **detalles del dispositivo** e informes

La siguiente tabla indica dónde se enumeran las aplicaciones para **Android (DA heredado)** (página de **detalles del dispositivo**, informes o no disponible). Las listas de aplicaciones incluyen todas las aplicaciones a menos que se indique lo contrario.

	MDM+MAM (TODAS LAS APLICACIONES)	MDM (APLICACIONES PÚBLICAS Y EMPRESARIALES)	MAM
Aplicaciones obligatorias (la política de inventario de aplicaciones no está implementada)	Página de **detalles del dispositivo** e informes	Página de **detalles del dispositivo** e informes	N/D

	MDM+MAM (TODAS LAS APLICACIONES)	MDM (APLICACIONES PÚBLICAS Y EMPRESARIALES)	MAM
Aplicaciones opcionales (la política de inventario de aplicaciones no está implementada)	Página de **detalles del dispositivo** e informes	Página de **detalles del dispositivo** e informes	No disponible
Aplicaciones obligatorias (la directiva de inventario de aplicaciones está implementada)	Página de **detalles del dispositivo** e informes	Página de **detalles del dispositivo** e informes	N/D
Aplicaciones opcionales (la directiva de inventario de aplicaciones está implementada)	Página de **detalles del dispositivo** e informes	Página de **detalles del dispositivo** e informes	No disponible

Para los dispositivos iOS, el comportamiento es diferente según el método de inscripción. La siguiente tabla indica dónde se enumeran las aplicaciones (página de **detalles del dispositivo** o informes). Las listas de aplicaciones incluyen todas las aplicaciones, a menos que se indique lo contrario.

	MDM+MAM (TODAS LAS APLICACIONES)	MDM (APLICACIONES PÚBLICAS Y EMPRESARIALES)	MAM (TODAS LAS APLICACIONES)
Aplicaciones obligatorias (la directiva de inventario de aplicaciones no está implementada)	Página de **detalles del dispositivo** e informes	Página de **detalles del dispositivo** e informes	Página de **detalles del dispositivo** e informes. Esas aplicaciones se muestran en estado pendiente (incluso si no están instaladas) o permanecen en

	MDM+MAM (TODAS LAS APLICACIONES)	MDM (APLICACIONES PÚBLICAS Y EMPRESARIALES)	MAM (TODAS LAS APLICACIONES)
			estado pendiente después de instalarlas manualmente.
Aplicaciones opcionales (la política de inventario de aplicaciones no está implementada)	Página de **detalles del dispositivo** e informes	Página de **detalles del dispositivo** e informes	Las aplicaciones web, SaaS y de enlace web se muestran en la página de **detalles del dispositivo** como aplicaciones instaladas. No se muestran en los informes. Las aplicaciones empresariales, MDX y públicas no se muestran en la página de **detalles del dispositivo** después de instalarlas manualmente. Las aplicaciones no se muestran en los informes después de instalarlas manualmente.
Aplicaciones obligatorias (la política de inventario de aplicaciones está implementada)	Página de **detalles del dispositivo** e informes	Página de **detalles del dispositivo** e informes	La política de inventario de aplicaciones no se puede implementar en los dispositivos. Las aplicaciones se muestran en la página de **detalles del dispositivo** y en

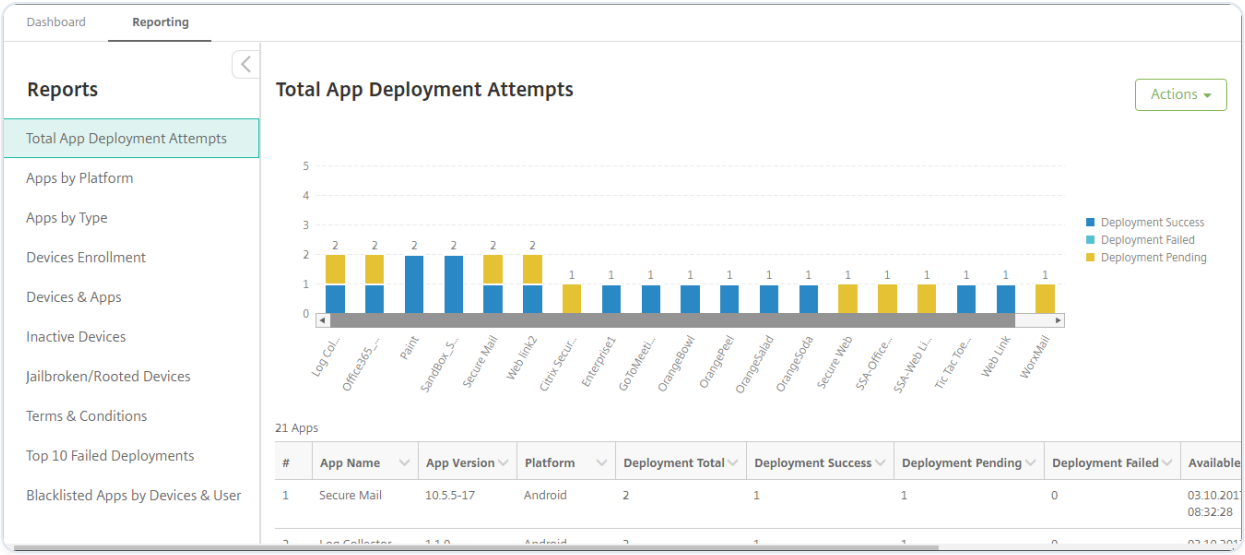
	MDM+MAM (TODAS LAS APLICACIONES)	MDM (APLICACIONES PÚBLICAS Y EMPRESARIALES)	MAM (TODAS LAS APLICACIONES)
			los informes. Esas aplicaciones se muestran en estado pendiente (incluso si no están instaladas) o permanecen en estado pendiente después de instalarlas manualmente.
Aplicaciones opcionales (la política de inventario de aplicaciones está implementada)	Página de **detalles del dispositivo** e informes	Página de **detalles del dispositivo** e informes	La política de inventario de aplicaciones no se puede implementar en los dispositivos. Las aplicaciones web, SaaS y de enlace web se muestran en la página de **detalles del dispositivo** como aplicaciones instaladas. No se muestran en los informes. Las aplicaciones empresariales, MDX y públicas no se muestran en la página de **detalles del dispositivo** después de instalarlas manualmente. Las aplicaciones no se muestran en los informes después de

	MDM+MAM (TODAS LAS APLICACIONES)	MDM (APLICACIONES PÚBLICAS Y EMPRESARIALES)	MAM (TODAS LAS APLICACIONES)
			instalarlas manualmente.

Para dispositivos macOS y Windows, Citrix Endpoint Management recopila un inventario de aplicaciones *solo* cuando se implementa la política de inventario de aplicaciones.

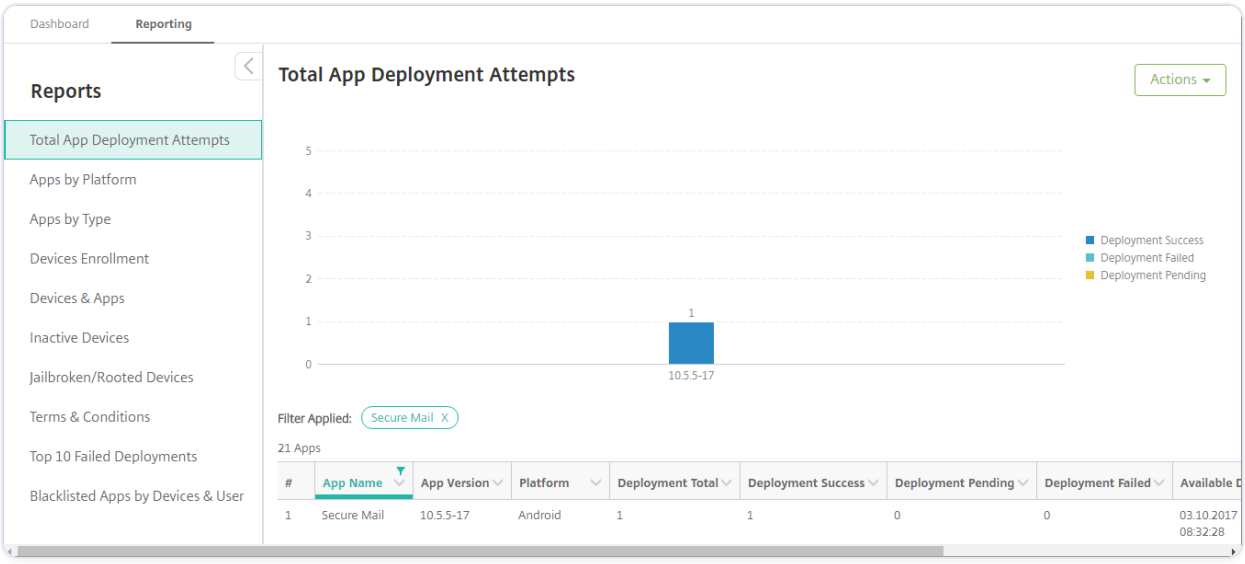
Para generar un informe

1. En la consola de Citrix Endpoint Management, haga clic en **Analizar > Informes**. Aparecerá la página **Informes**.
2. Haga clic en el informe que quiera generar.

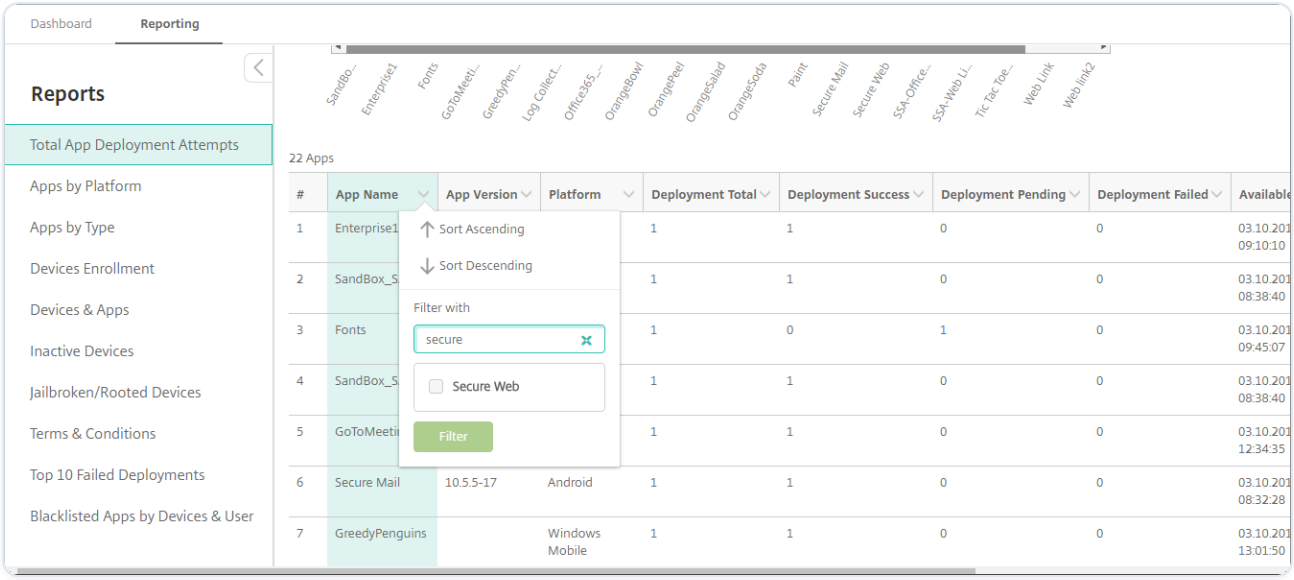


Para ver más detalles de un informe

1. Haga clic en las áreas del gráfico para desglosar y ver información más detallada.

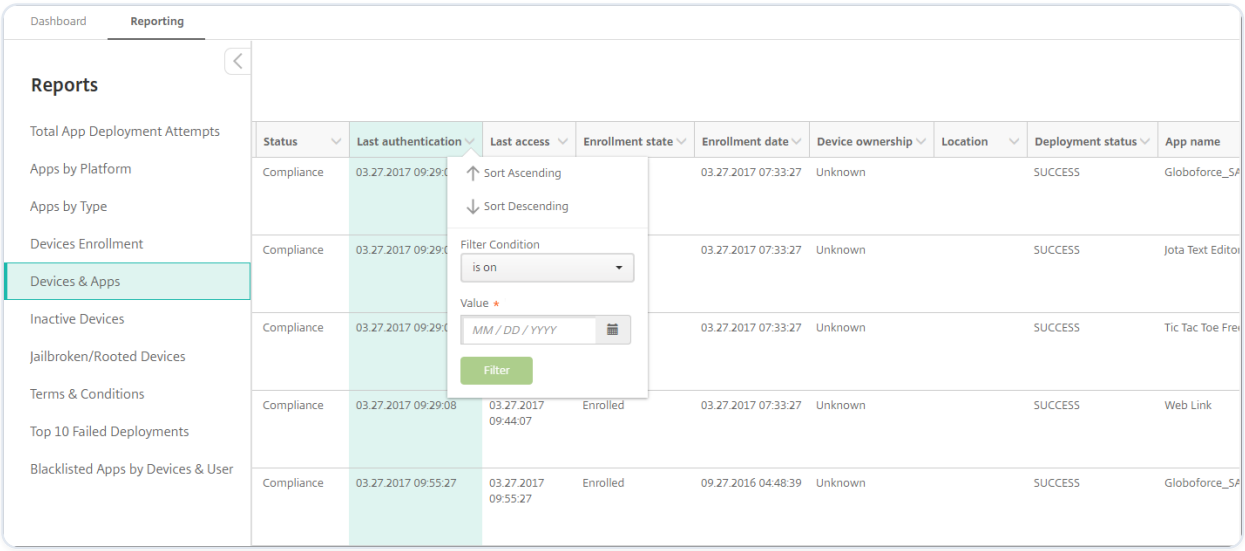


Para ordenar, filtrar o buscar en una columna de tabla, haga clic en el encabezado de la columna

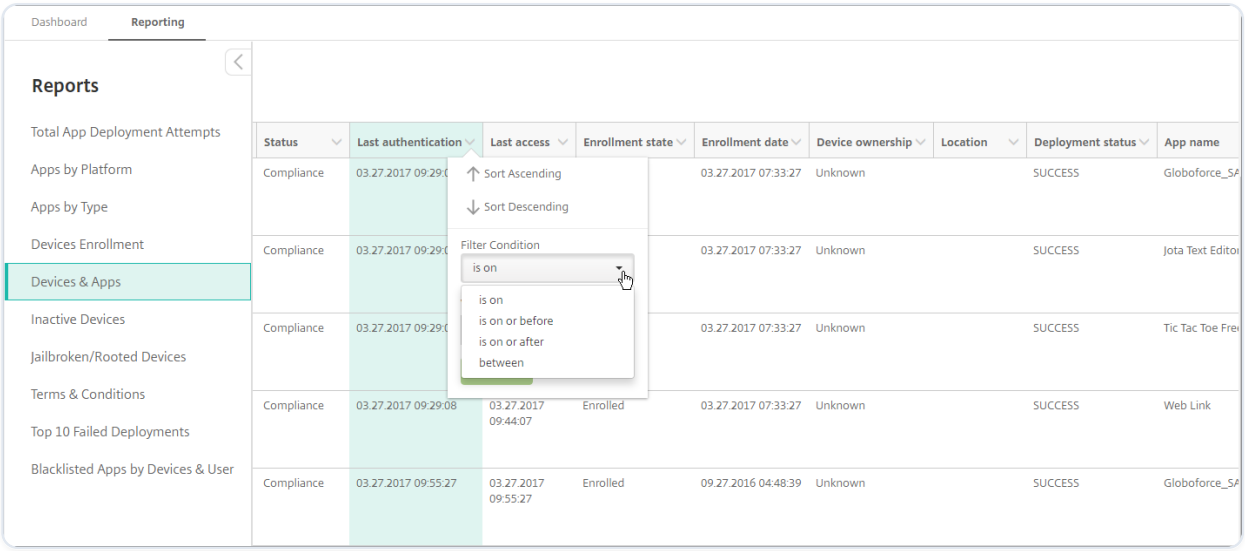


Para filtrar el informe por fecha

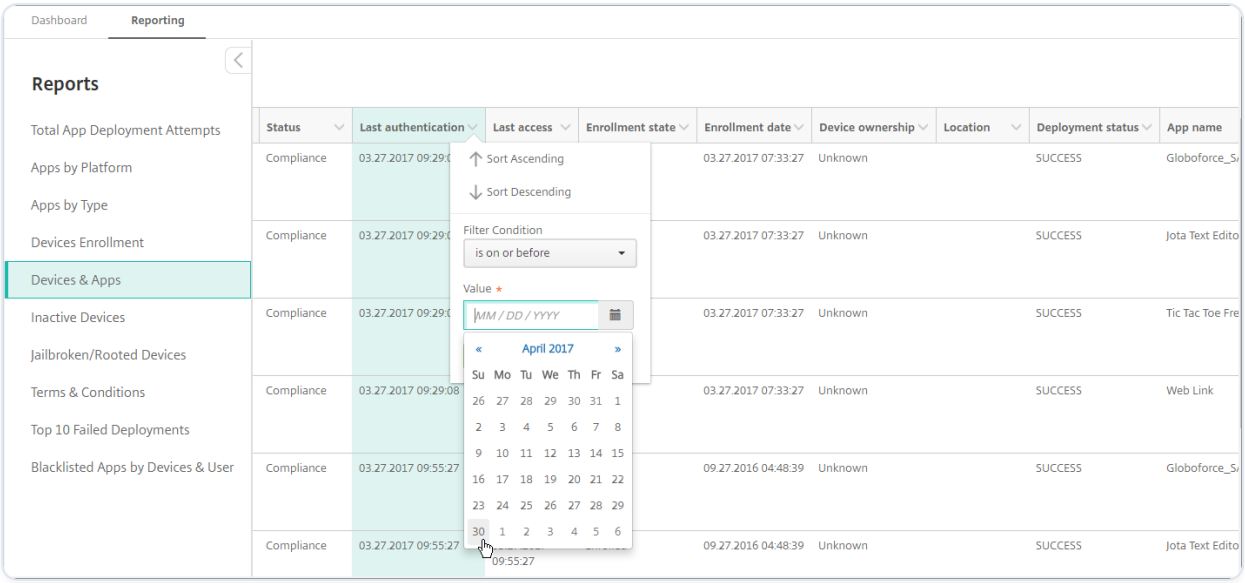
1. Haga clic en el encabezado de una columna para ver la configuración del filtro.



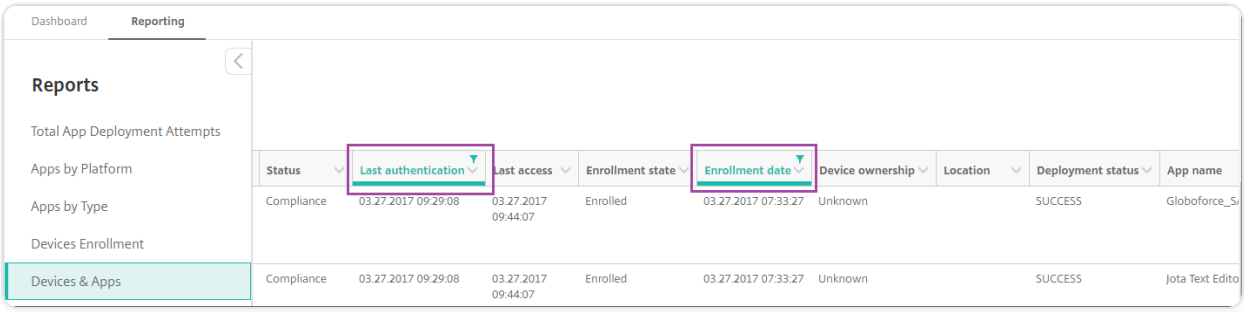
2. En **Condición de filtro**, elija cómo quiere restringir las fechas de los informes.



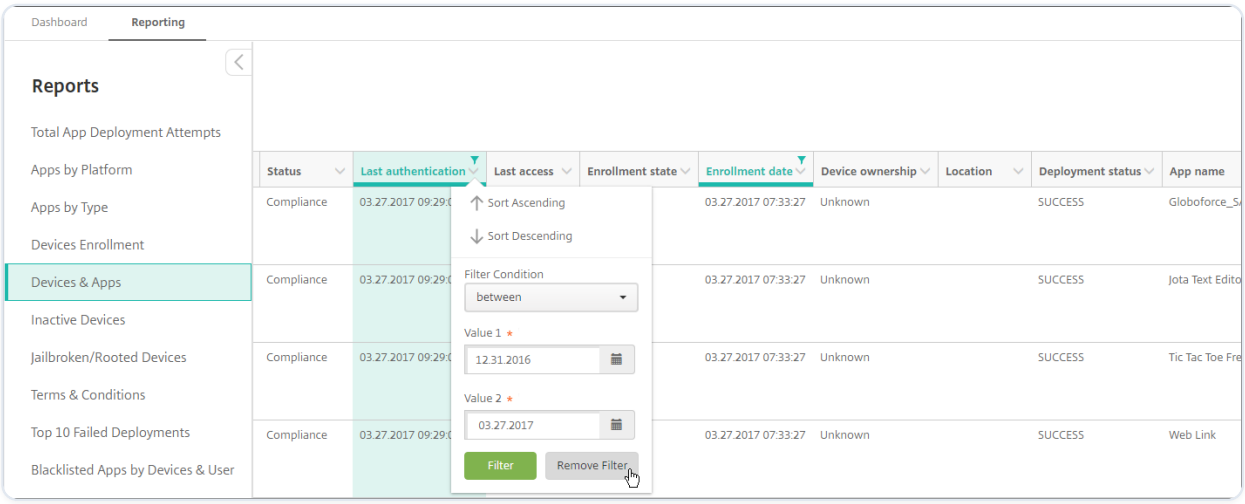
3. Utilice el selector de fechas para especificar las fechas.



4. Una columna con un filtro de fecha se muestra como en el siguiente ejemplo.

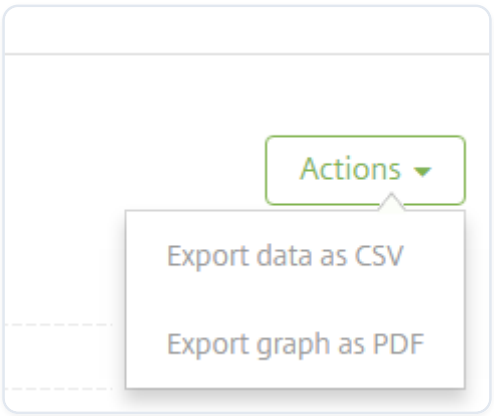


5. Para quitar un filtro, haga clic en el encabezado de la columna y, a continuación, en **Quitar filtro**



Para exportar un gráfico o una tabla

- Para exportar el gráfico en formato PDF, haga clic en **Acciones** y, a continuación, en **Exportar gráfico como PDF**.
- Para exportar los datos de la tabla en formato CSV, haga clic en **Acciones** y, a continuación, en **Exportar datos como CSV**.



API REST

Con la API REST de Citrix Endpoint Management, puede:

- Llamar a servicios que se muestran en la consola de Citrix Endpoint Management
- Llamar a servicios REST mediante cualquier cliente REST

La API no requiere que inicie sesión en la consola de Citrix Endpoint Management para llamar a los servicios.

Para obtener el conjunto completo actual de API disponibles, descargue el PDF Public API for REST Services.

Hay API disponibles para administrar sus dispositivos de punto final móviles y de escritorio y configurar los ajustes de sus aplicaciones Workspace. Vaya a `<https://developer.cloud.com/citrixworkspace>` y navegue hasta **Citrix Endpoint Management > Mobile Application Integration**.

Permisos necesarios para acceder a la API REST

El acceso a la API REST requiere uno de los siguientes permisos:

- Administrador de Citrix Cloud
- Permiso de acceso a la API pública establecido como parte de la configuración de acceso basado en roles. Para obtener más información, consulte Configuring roles with RBAC.
- Permiso de superusuario

Para acceder a la API REST con su cuenta de Citrix Cloud, genere las claves de **API**:

1. En el menú de Citrix Cloud, seleccione **Identity and Access Management**.
2. Seleccione **API Access > Secure Clients**.
3. Escriba un nombre para su cliente seguro y haga clic en **Crear cliente**.

Citrix Cloud crea el ID de cliente seguro y el secreto de cliente. Descargue una copia de esta información y guárdela de forma segura sin conexión para su referencia. Citrix Cloud no almacena los identificadores únicos después de cerrar el cuadro de diálogo.

Para invocar los servicios de la API de REST

Puede llamar a los servicios de la API de REST mediante el cliente de REST o los comandos cURL. Los siguientes ejemplos utilizan el cliente de REST avanzado para Chrome.

> **Nota:**
>
> En los siguientes ejemplos, cambie el nombre de host y el número de puerto para que coincidan con su entorno.

Iniciar sesión

El ejemplo que se muestra aquí cubre el inicio de sesión mediante un token recuperado a través de la API de Citrix Cloud.

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login/cloud`

Tipo de método: POST

Tipo de contenido: application/json

Ejemplo de solicitud:

```
{

 "bearerToken":
"eyJ0eOiJSUzJiibGcI1AiONiJ9.eyJkIjoMDExN1c2VIXiMzNDc1OTk4...qf0iQ"

}
```

Debe recuperar el token de portador mediante la API de Citrix Cloud `https://trust.citrixworkspacesapi.net/Help/Api/POST-customer-tokens-clients`. Para obtener más información, consulte la documentación para desarrolladores.

Ejemplo de respuesta:

```
{

 "auth_token": "q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"
```

```
}
```

Información relacionada

- API REST de Citrix Endpoint Management

Restringir el acceso al correo electrónico

Puerta de enlace de ActiveSync

ActiveSync es un protocolo de sincronización de datos móviles desarrollado por Microsoft. ActiveSync sincroniza datos con dispositivos portátiles y equipos de escritorio (o portátiles).

Puede configurar las reglas de la puerta de enlace de ActiveSync en Citrix Endpoint Management. La puerta de enlace de ActiveSync mantiene una lista de ID de ActiveSync para todos los dispositivos configurados en Citrix Endpoint Management. Según las reglas que configure, puede permitir o denegar el acceso de los dispositivos a los datos de ActiveSync, basándose en esos ID de ActiveSync. Por ejemplo, si activa la regla **Aplicaciones obligatorias ausentes**, Citrix Endpoint Management comprueba la Directiva de acceso a aplicaciones para las aplicaciones obligatorias. Si faltan las aplicaciones obligatorias, la directiva deniega el acceso a los datos de ActiveSync. Para cada regla, puede elegir **Permitir** o **Denegar**. La configuración predeterminada es **Permitir**.

Para obtener más información sobre la directiva de dispositivos de acceso a aplicaciones, consulte Directiva de dispositivos de acceso a aplicaciones.

Citrix Endpoint Management admite las siguientes reglas:

Dispositivos anónimos: Comprueba si un dispositivo está en modo anónimo. Esta comprobación está disponible si Citrix Endpoint Management no puede volver a autenticar al usuario cuando un dispositivo intenta volver a conectarse.

Aplicaciones prohibidas: Comprueba si un dispositivo tiene aplicaciones prohibidas, tal como se define en una directiva de acceso a aplicaciones.

Permitir y denegar implícitamente: Esta acción es la predeterminada para la puerta de enlace de ActiveSync. La puerta de enlace crea una lista de dispositivos de todos los dispositivos que no cumplen ninguno de los demás criterios de las reglas de filtro. La puerta de enlace permite o deniega las conexiones basándose en esa lista. Si ninguna regla coincide, el valor predeterminado se establece como **Permitir implícitamente**.

Dispositivos inactivos: Comprueba si un dispositivo está inactivo según lo definido por la configuración **Umbral de días de inactividad del dispositivo** en **Propiedades del servidor**.

Aplicaciones obligatorias ausentes: Comprueba si a un dispositivo le faltan las aplicaciones obligatorias, tal como se define en una directiva de acceso a aplicaciones.

Aplicaciones no sugeridas: Comprueba si un dispositivo tiene aplicaciones no sugeridas, tal como se define en una directiva de acceso a aplicaciones.

Contraseña no conforme: Comprueba si la contraseña del usuario es conforme. En dispositivos iOS y Android, Citrix Endpoint Management puede determinar si la contraseña actual del dispositivo cumple con la directiva de código de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para establecer una contraseña si Citrix Endpoint Management envía una directiva de código de acceso al dispositivo. Antes de que el usuario establezca la contraseña, el código de acceso podría no ser conforme.

Dispositivos no conformes: Comprueba si un dispositivo no cumple las normas, basándose en la propiedad de dispositivo No conforme. Las acciones automatizadas o terceros que utilizan las API de Citrix Endpoint Management suelen cambiar esa propiedad.

Estado revocado: Comprueba si el certificado del dispositivo ha sido revocado. Un dispositivo revocado no puede volver a inscribirse hasta que se autorice de nuevo.

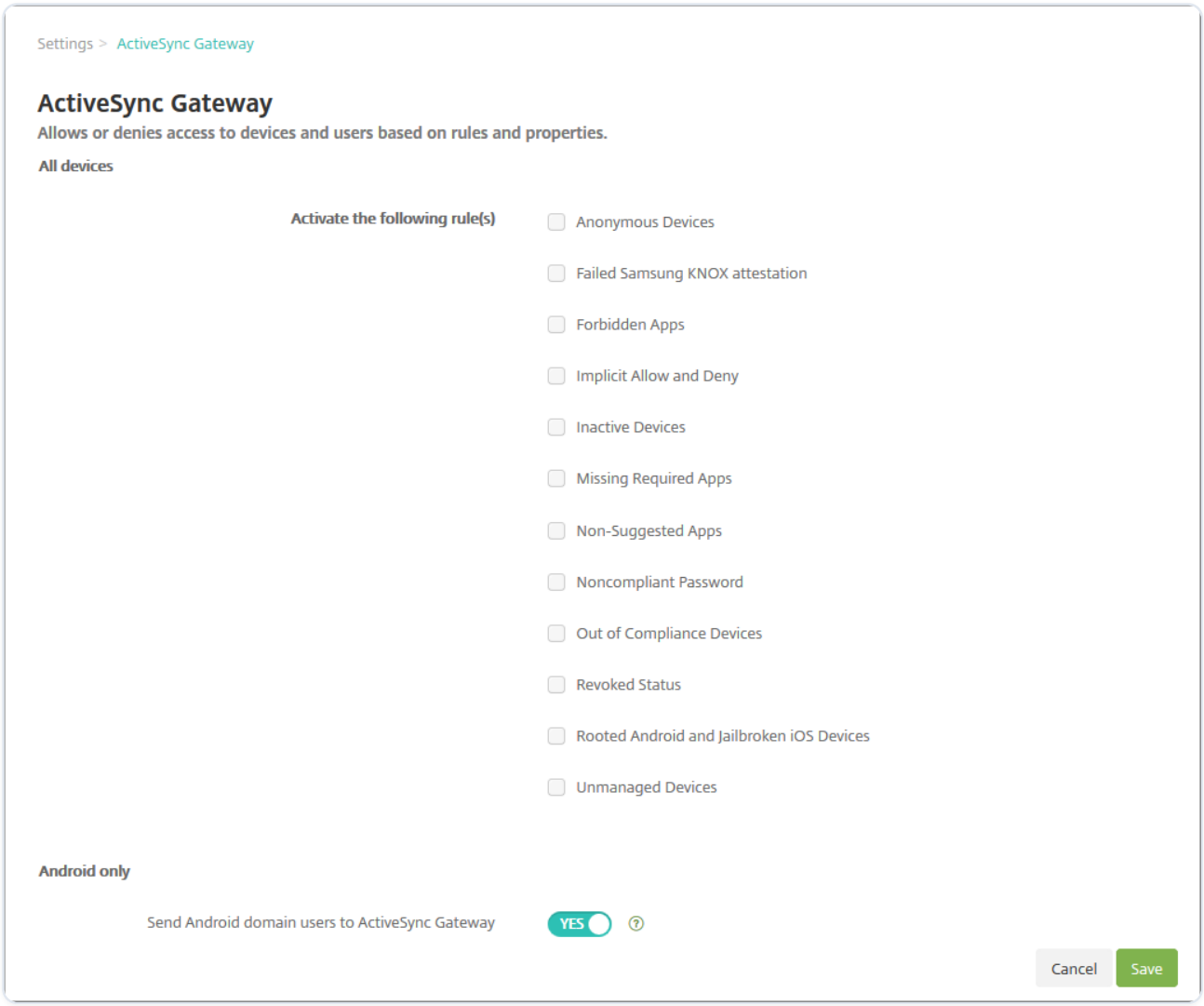
Dispositivos Android rooteados y iOS con jailbreak: Comprueba si un dispositivo Android o iOS tiene jailbreak.

Dispositivos no administrados: Compruebe si un dispositivo sigue en estado administrado, controlado por Citrix Endpoint Management. Por ejemplo, un dispositivo inscrito en MAM o un dispositivo no inscrito no está administrado.

Enviar usuarios de dominio de Android a ActiveSync Gateway: Haga clic en **YES** para que Citrix Endpoint Management envíe el nombre de usuario y el ID de ActiveSync de los propietarios de dispositivos Android a ActiveSync Gateway. Desactive esta función a menos que esté ejecutando una configuración heredada. En configuraciones más recientes, esta función permite que cualquier dispositivo acceda a los datos de ActiveSync siempre que el nombre de usuario asociado al dispositivo exista en la puerta de enlace.

Para configurar los parámetros de ActiveSync Gateway

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje de la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En **Servidor**, haga clic en **ActiveSync Gateway**. Aparecerá la página **ActiveSync Gateway**.



1. En **Activar las siguientes reglas**, seleccione una o varias reglas que quiera activar.
2. En **Solo Android**, en **Enviar usuarios de dominio de Android a ActiveSync Gateway**, haga clic en **YES** para asegurarse de que Citrix Endpoint Management envía la información del dispositivo Android a ActiveSync Gateway.
3. Haga clic en **Guardar**.

Conector de Citrix Endpoint Management para Exchange ActiveSync

XenMobile Mail Manager es ahora un conector de Citrix Endpoint Management para Exchange ActiveSync. Para obtener más información sobre el portfolio unificado de Citrix, consulte la guía de productos de Citrix.

El conector amplía las capacidades de Citrix Endpoint Management de las siguientes maneras:

- Control de acceso dinámico para dispositivos Exchange ActiveSync (EAS). Se puede permitir o bloquear automáticamente el acceso de los dispositivos EAS a los servicios de Exchange.

- La capacidad de Citrix Endpoint Management para acceder a la información de asociación de dispositivos EAS proporcionada por Exchange.
- La capacidad de Citrix Endpoint Management para borrar un dispositivo móvil según el estado de EAS.
- La capacidad de Citrix Endpoint Management para acceder a la información sobre dispositivos Blackberry y para realizar operaciones de control como Borrar y Restablecer contraseña.

Para borrar un dispositivo según el estado de EAS, configure una acción automatizada con un desencadenador de ActiveSync. Consulte Acciones automatizadas.

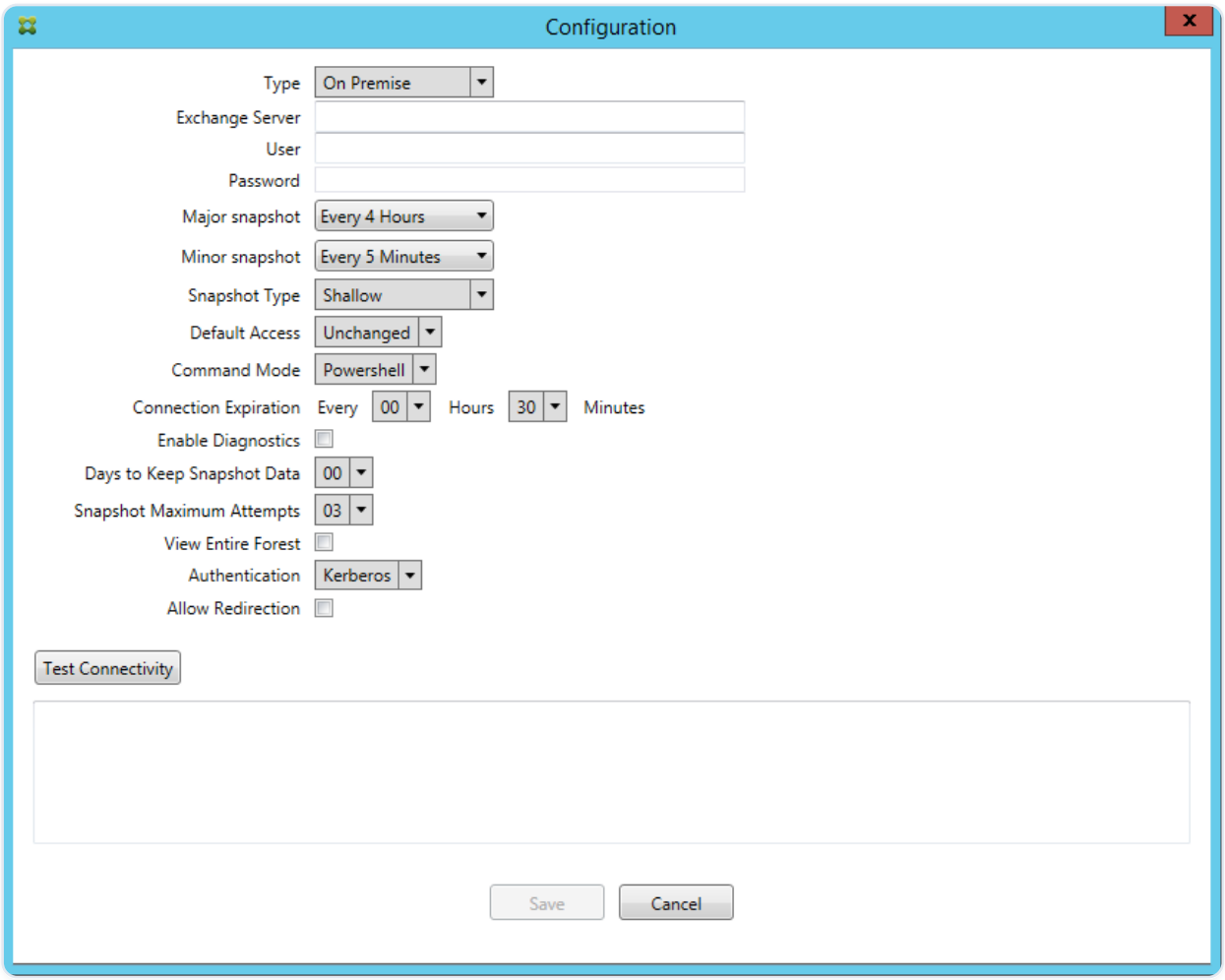
> **Importante:**
>
> A partir de octubre de 2022, los conectores de Citrix Endpoint Management y NetScaler Gateway para Exchange ActiveSync ya no son compatibles con Exchange Online, dados los cambios de autenticación anunciados por Microsoft aquí. El conector de Citrix Endpoint Management para Exchange sigue funcionando con Microsoft Exchange Server (local).

Novedades de la versión 10.1.10

Los siguientes problemas se han corregido en la versión 10.1.10:

- Es posible que los clientes que experimentan problemas de red frecuentes no puedan completar una instantánea en los tres intentos proporcionados anteriormente. Con esta versión, un administrador puede configurar el número máximo de intentos (1-10). Esta corrección permite que una instantánea incurra en múltiples interrupciones de comunicación

sin abandonar el proceso de instantánea por completo.

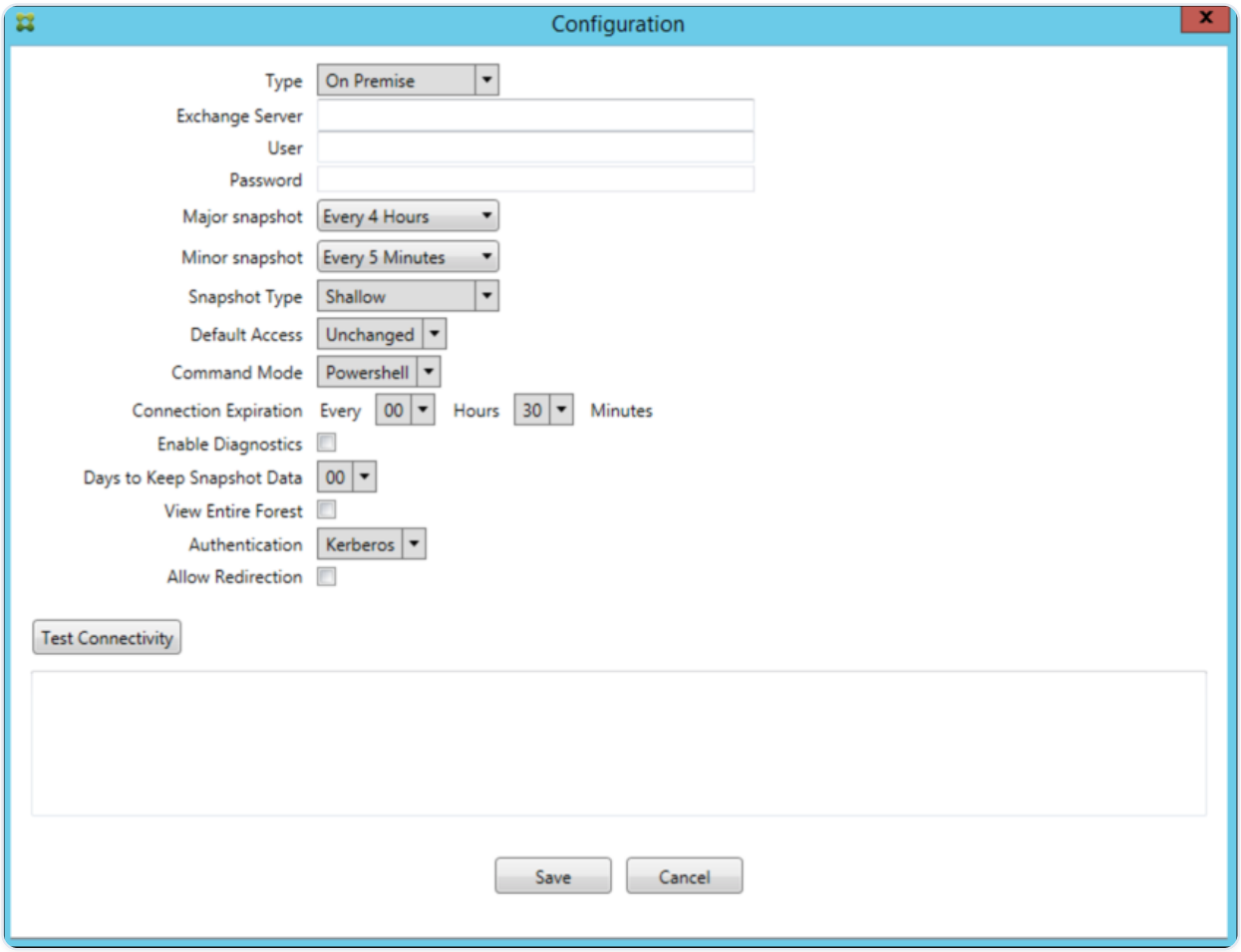


- En versiones anteriores, el tipo de instantánea no aparecía en la lista de configuraciones de Exchange. Ahora, el tipo de instantánea aparece.
- La excepción PSRemotingTransport notificada por PowerShell indica que la sesión a Exchange ya no es viable. El estado se agrega a la lista de errores críticos en el archivo de configuración de forma predeterminada. Al hacerlo, cuando se detecta la PSRemotingTransportException, la conexión se marca como en Error para su posterior eliminación. La siguiente comunicación utiliza una conexión válida o crea una conexión.
- Cuando se guarda un cambio de configuración, es posible que no todos los componentes internos configurados previamente se hayan eliminado correctamente antes de cargar la nueva configuración. Este problema podría provocar un comportamiento impredecible. El comportamiento depende del cambio específico y de si el cambio entraba en conflicto con la configuración anterior. En esta versión, todos los componentes internos se eliminan antes de cargar la nueva configuración.

¿Novedades de la versión 10.1.9?

Los siguientes problemas se han corregido en la versión 10.1.9:

- Los cambios de configuración ahora se gestionan de forma más coherente. Cuando el servicio detecta un cambio en la configuración, cada subsistema interno se detiene, lo que significa que cualquier procesamiento activo o programado se interrumpe. A continuación, se carga la nueva configuración y los subsistemas se inician de nuevo, lo que significa que todos los programas y otras infraestructuras internas se restablecen con la nueva configuración. Este problema corrige un problema conocido en la versión 10.1.8.
- Durante una actualización, la configuración de la base de datos existente no se fusionaba con el nuevo archivo de configuración. La configuración de la base de datos ahora se fusiona con el archivo de configuración actualizado.
- En los archivos de diagnóstico relacionados con las instantáneas, faltaban los encabezados de columna. Los encabezados se han restaurado.
- Al actualizar desde una versión anterior, la sección de valores predeterminados del archivo de configuración se sobrescribía con la sección análoga del archivo de configuración en uso. Este problema impedía que el servicio cargara adiciones o mejoras en la sección de valores predeterminados después de la actualización. A partir de esta versión, la sección de valores predeterminados siempre refleja la configuración más reciente.
- Los administradores ya no pueden acceder a ciertas opciones pulsando Mayús al ejecutar la aplicación. Estas opciones estaban disponibles anteriormente con el permiso de Citrix®. Algunas opciones ahora están totalmente disponibles, como Permitir redirección, y otras, como Detección de bloqueo y Corrección de recuento, están obsoletas.



¿Novedades de versiones anteriores?

La siguiente sección enumera las nuevas funciones y los problemas corregidos en versiones anteriores del conector de Citrix Endpoint Management para Exchange ActiveSync.

¿Novedades de la versión 10.1.8?

- Es posible que Exchange limite el conector de Citrix Endpoint Management para el servicio Exchange ActiveSync para que no emita comandos con demasiada frecuencia. Este problema es común en las conexiones a Office 365. El efecto de la limitación requiere que el servicio se detenga durante un período especificado antes de enviar el siguiente comando. La consola de configuración ahora muestra la cantidad de tiempo restante en la pausa.
- Cuando se realizan modificaciones en las secciones "Watchdog" y/o "SpecialistsDefaults" del archivo de configuración (config.xml), los cambios no se reflejan en el archivo de configuración después de una actualización. Con esta versión, las modificaciones se fusionan correctamente en el nuevo archivo de configuración.
- Se han añadido más detalles a los análisis enviados a Google Analytics, especialmente en lo que respecta a las instantáneas.

- La función de prueba de conectividad de Exchange intentaría inicializar la conexión solo una vez. Dado que las conexiones de Office 365 pueden ser limitadas, era posible que una prueba de conectividad pareciera fallar cuando se limitaba. El conector de Citrix Endpoint Management para Exchange ActiveSync ahora intenta iniciar una conexión hasta tres veces.
- Para aplicar políticas en Exchange, el conector de Citrix Endpoint Management para Exchange ActiveSync debe compilar un comando **Set-CASMailbox** que incluya todos los dispositivos pertinentes para cada buzón, en dos listas: permitir y bloquear. Si un dispositivo no está incluido en ninguna de las listas, Exchange recurre a su estado de acceso predeterminado. Si ese estado de acceso predeterminado es diferente del estado deseado para un dispositivo, ese dispositivo deja de cumplir las normas. Por lo tanto, un usuario podría perder el acceso a su correo electrónico si el estado de acceso predeterminado de Exchange está bloqueado y debería estar permitido. O bien, a un usuario cuyo acceso al correo electrónico debería estar bloqueado se le podría conceder acceso. El conector de Citrix Endpoint Management para Exchange ActiveSync ahora se asegura de que todos los dispositivos con un estado deseado válido estén incluidos en cada comando **Set-CasMailbox**.

Se conoce el siguiente problema en la versión 10.1.8:

Si un administrador realiza un cambio en la aplicación Configurar que modifica los datos de configuración, mientras el servicio realiza operaciones de larga duración, como una instantánea o una evaluación de políticas, el servicio puede entrar en un estado indeterminado. Un posible síntoma puede ser que los cambios de política no se procesen o que las instantáneas no se inicien. Para que el servicio vuelva a un estado de funcionamiento, debe reiniciarse. Es posible que deba usar el administrador de servicios de Windows para finalizar el proceso del servicio antes de iniciarlo.

Novedades de la versión 10.1.7

- XenMobile Mail Manager ahora es un conector de Citrix Endpoint Management para Exchange ActiveSync.
- Hemos dejado de usar la opción **Disable Pipelining** en el cuadro de diálogo de configuración de Exchange. Puede lograr la misma funcionalidad configurando varios pasos para cada comando en el archivo config.xml.

Los siguientes problemas se han corregido en la versión 10.1.7:

- En la ventana Historial de instantáneas, los mensajes de error podrían mostrarse con poco contexto. Ahora, los mensajes de error se anteponen con el contexto de dónde ocurrieron.

- El archivo XmmGoogleAnalytics .dll no tenía la versión de archivo correspondiente para la versión.
- Para mejorar el diagnóstico, recientemente cambiamos el formato de cadena para una lista de ID de dispositivo utilizados para establecer un estado de buzón Permitido/Bloqueado. Sin embargo, una especificación de demasiados dispositivos excedía el tamaño máximo de la cadena. Ahora, usamos una estructura de datos de matriz interna. Esta estructura no tiene un límite de tamaño y también formatea los datos de manera adecuada para fines de diagnóstico.
- Cuando se detectan políticas de dispositivos que no están sincronizadas con Exchange, sus comandos pueden incluir dispositivos que no pertenecen al buzón relevante. El conector de Citrix Endpoint Management para Exchange ActiveSync ahora se asegura de que los comandos a Exchange representen solo los dispositivos que pertenecen a sus respectivos buzones.
- En algunos entornos, un ensamblado de Microsoft no está disponible. El ensamblado requerido ahora se instala explícitamente con la aplicación.
- Si los Nombres Distinguidos para dispositivos o buzones tienen espacios entre el nombre del atributo y el signo igual, o espacios después del signo igual y antes del valor, el conector de Citrix Endpoint Management para Exchange ActiveSync podría no emparejar correctamente un dispositivo con su buzón y viceversa. El resultado podría ser que algunos dispositivos y/o buzones sean rechazados durante la conciliación de instantáneas.

Nota:

Las siguientes secciones de Novedades se refieren al conector de Citrix Endpoint Management para Exchange ActiveSync por su antiguo nombre de XenMobile Mail Manager. El nombre cambió a partir de la versión 10.1.7.

Actualización en la versión 10.1.6.20

Una actualización a la versión 10.1.6 incluye la siguiente corrección en la versión 10.1.6.20:

- Cuando se detectan directivas de dispositivos que no están sincronizadas con Exchange, sus comandos pueden incluir dispositivos que no pertenecen al buzón correspondiente. XenMobile® Mail Manager ahora garantiza que los comandos a Exchange representen solo los dispositivos que pertenecen a sus buzones respectivos.

Novedades de la versión 10.1.6

XenMobile Mail Manager versión 10.1.6 incluye las siguientes mejoras y problemas solucionados:

- La ventana del historial de instantáneas, a veces, entra en un estado en el que ya no se actualiza. Se ha mejorado el mecanismo de actualización de las ventanas para que se actualicen de forma más fiable.
- Se utilizaban dos modos y rutas de código distintos para las instantáneas particionadas y no particionadas. Dado que las instantáneas no particionadas son equivalentes a las instantáneas particionadas con una configuración que utiliza una única partición "*", se elimina el modo de instantánea no particionada. El modo de instantánea predeterminado ahora es instantáneas particionadas con 36 particiones (0–9, A–Z).
- En la ventana Historial de instantáneas, los mensajes de estado sobrescriben los mensajes de error. Ahora, XenMobile Mail Manager proporciona dos campos separados para que los usuarios puedan ver el estado y los errores simultáneamente.
- Al conectarse a Exchange Online (Office 365), las consultas relacionadas con instantáneas pueden dar como resultado un conjunto de datos truncado. Este problema puede ocurrir cuando XenMobile Mail Manager ejecuta un script canalizado de múltiples comandos. El comando ascendente no puede pasar los datos lo suficientemente rápido al comando descendente, que luego completa el trabajo prematuramente. Como resultado, se producen datos incompletos. XenMobile Mail Manager ahora puede imitar la canalización y esperar hasta que el comando ascendente termine antes de invocar el comando descendente. Este cambio debería dar como resultado que todos los datos se procesen y capturen.
- Si se produce un error no resoluble en un comando de actualización de directivas a Exchange, el mismo comando se devuelve a la cola de trabajo repetidamente durante un largo período. Esta situación provocó que el comando se enviara a Exchange muchas veces. En esta versión de XenMobile Mail Manager, un comando que da como resultado un error solo se devuelve a la cola de trabajo un número discreto de veces.
- Si una actualización de directiva para un buzón específico implicaba permitir o bloquear todos los dispositivos: El comando **Set-CASMailbox** emitido fallaría porque la lista vacía se convertía en una cadena vacía en lugar de un valor **NULL**. Ahora se envían los datos correctos.
- Al procesar un nuevo dispositivo, Exchange puede devolver el estado como "DeviceDiscovery" durante algún tiempo (normalmente 15 minutos). XenMobile Mail Manager no estaba gestionando específicamente este estado. XenMobile Mail Manager ahora gestiona el estado. En la pestaña Monitor de la interfaz de usuario, los usuarios pueden filtrar los dispositivos en este estado.

- XenMobile Mail Manager no comprobaba la capacidad de escribir en la base de datos de XenMobile Mail Manager. Por lo tanto, si los permisos estaban restringidos, el comportamiento podría no ser predecible. XenMobile Mail Manager ahora captura y valida los permisos necesarios de la base de datos. XenMobile Mail Manager indica permisos reducidos al probar la conexión (mensaje mostrado) o en el indicador de base de datos (pasar el ratón para ver el mensaje) en la parte inferior de la ventana principal de Configuración.
- Dependiendo de la carga de trabajo actual, cuando se le indica, el servicio XenMobile Mail Manager puede no detenerse rápidamente. Por lo tanto, el servicio parece estar en un estado que no responde. Las mejoras permiten interrumpir las tareas en curso, lo que resulta en un apagado más elegante.

Novedades de la versión 10.1.5

XenMobile Mail Manager versión 10.1.5 tiene los siguientes problemas resueltos:

- Cuando Exchange aplica la limitación de velocidad a la actividad de XenMobile Mail Manager, no hay ninguna indicación (fuera de los registros) de que la limitación se esté produciendo. Con esta versión, el usuario puede pasar el ratón por encima de la instantánea activa y aparecerá un estado de "limitación de velocidad". Además, mientras XenMobile Mail Manager está siendo limitado, el inicio de una instantánea principal está prohibido hasta que Exchange levante el embargo de limitación.
- Si Exchange limita la velocidad de XenMobile Mail Manager durante una instantánea principal: Es posible que no se permita que transcurra el tiempo suficiente antes de ejecutar el siguiente intento de instantánea. Este problema provoca una mayor limitación y un error en la instantánea. XenMobile Mail Manager ahora espera un mínimo del tiempo que Exchange especifica que se debe esperar entre los intentos de instantánea.
- Cuando los diagnósticos están habilitados, el archivo de comandos muestra comandos **Set-CasMailbox** a los que les faltan guiones antes de cada nombre de propiedad. Este problema solo ocurre en el formato del archivo de diagnóstico y no en el comando real a Exchange. El guion que falta impide que un usuario corte el comando y lo pegue directamente en un símbolo del sistema de PowerShell para realizar pruebas o validaciones. Se han añadido los guiones.
- Si una identidad de buzón tiene el formato `lastname, firstname`, Exchange añade una barra invertida antes de la coma al devolver datos de una consulta. Esta barra invertida debe eliminarse cuando XenMobile Mail Manager utiliza la identidad para consultar más datos.

Limitaciones conocidas

> **Nota:**

> La siguiente limitación se resuelve en la versión 10.1.6.

> XenMobile Mail Manager tiene una limitación conocida que puede provocar que los comandos a Exchange fallen. Para aplicar cambios de directiva a Exchange, XenMobile Mail Manager emite un comando **Set_CASMailbox**. Este comando puede tomar dos listas de dispositivos: una para Permitir y otra para Bloquear. El comando se aplica a los dispositivos asociados con un buzón.

Estas listas están limitadas a 256 caracteres cada una por la API de Microsoft. Si una de esas listas excede la limitación, el comando falla por completo, impidiendo que se establezcan las directivas para esos dispositivos del buzón. El error notificado, que aparece en los registros de XenMobile Mail Manager, se vería como el siguiente. El ejemplo es para la lista bloqueada.

“Mensaje:'No se puede enlazar el parámetro 'ActiveSyncBlockedDeviceIDs' al destino. Excepción al establecer "ActiveSyncBlockedDeviceIDs": "La longitud de la propiedad es demasiado larga. La longitud máxima es 256 y la longitud del valor proporcionado es …"

La longitud de los ID de dispositivo puede variar, pero una buena pauta es que unos 10 dispositivos o más permitidos o bloqueados simultáneamente podrían exceder el límite. Aunque tener tantos dispositivos asociados a un buzón específico es raro, es una posibilidad. Hasta que Mail Manager se mejore para manejar tal escenario, le recomendamos que limite el número de dispositivos asociados a un usuario y buzón a 10 o menos.

Novedades de la versión 10.1.4

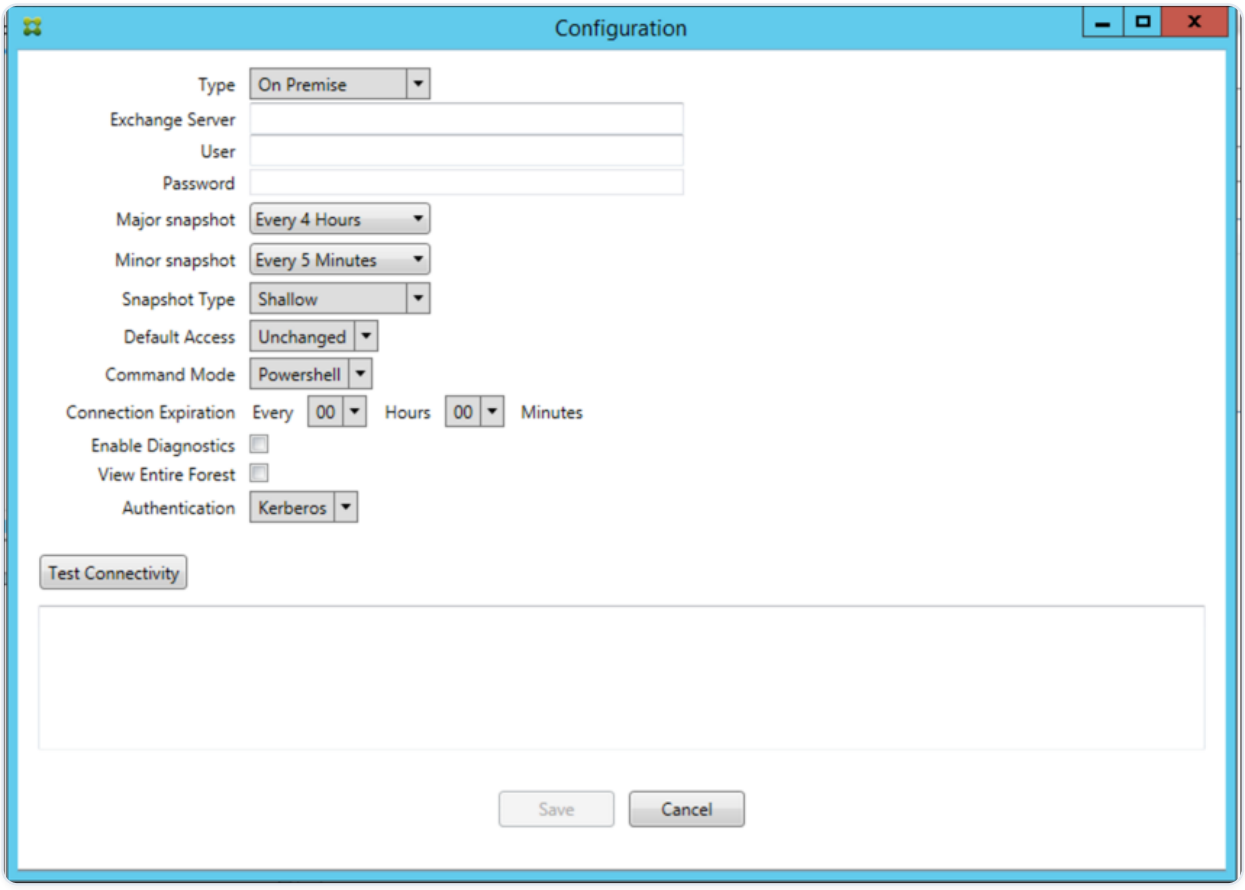
XenMobile Mail Manager versión 10.1.4 tiene los siguientes problemas resueltos:

- Debido a su seguridad debilitada, el Consejo PCI está desaprobando TLS 1.0 y TLS 1.1. Se añade compatibilidad con 1.2 a XenMobile Mail Manager.
- XenMobile Mail Manager incluye un nuevo archivo de diagnóstico. Cuando se selecciona **Habilitar diagnósticos** en la especificación de Exchange, se genera un nuevo archivo de historial de instantáneas. Con cada intento de instantánea, se añade una línea al archivo con los resultados de la instantánea.
- En el archivo de diagnóstico de comandos, la lista de dispositivos permitidos o bloqueados no aparecía para el comando **Set-CASMailbox**. En su lugar, se mostraba el nombre de la clase interna en el archivo para los argumentos relacionados. XenMobile Mail Manager ahora muestra la lista de ID de dispositivo como una lista separada por comas.

- Cuando un intento de adquirir una conexión a Exchange falla debido a una especificación incorrecta: Un mensaje incorrecto anula el mensaje de error: "Todas las conexiones en uso". Ahora aparecen mensajes más descriptivos, como "Todas las conexiones están inoperables", "El grupo de conexiones está vacío", "Todas las conexiones están limitadas" y "No hay conexiones disponibles".
- A veces, los comandos de permitir/bloquear/borrar se ponen en cola en la caché interna de XenMobile Mail Manager varias veces. Este problema provoca un retraso en el envío del comando a Exchange. XenMobile Mail Manager ahora solo pone en cola una instancia de cada comando.

Novedades de la versión 10.1.3

- **Compatibilidad con Google Analytics:** Queremos saber cómo utiliza XenMobile Mail Manager para poder centrarnos en cómo mejorar el producto.
- **Configuración para habilitar diagnósticos:** Una casilla de verificación **Habilitar diagnóstico** aparece en la consola de configuración, en el cuadro de diálogo **Configuración**.



Problemas resueltos en la versión 10.1.3

- En la ventana **Historial de instantáneas**, las informaciones sobre herramientas que muestran el estado actual de la instantánea no reflejan el estado real. Ocasionalmente, XenMobile Mail

Manager no puede escribir en el archivo de diagnóstico de comandos. Cuando esto ocurre, el historial de comandos no se registra en su totalidad.

- Cuando se produce un error en una conexión, es posible que la conexión no se marque como "con error". Como resultado, un comando posterior puede intentar usar la conexión y causar otro error.
- Cuando se produce una limitación por parte del servidor de Exchange, se puede generar una excepción en la rutina de comprobación de estado. Como resultado, las conexiones que han experimentado un error o han caducado podrían no purgarse. Además, XenMobile Mail Manager podría no crear conexiones hasta que expire el tiempo de limitación. .
- Cuando se supera el número máximo de sesiones para Exchange, XenMobile Mail Manager informa del error "Error al capturar el dispositivo", lo cual no es un mensaje preciso. En su lugar, el mensaje debería indicar que las dos sesiones que XenMobile Mail Manager utiliza normalmente para la comunicación con Exchange están en uso.

Novedades de la versión 10.1.2

- **Conexión mejorada a Exchange:** XenMobile Mail Manager utiliza sesiones de PowerShell para comunicarse con Exchange. Una sesión de PowerShell, especialmente al tratar con Office 365, puede volverse inestable después de un tiempo, impidiendo que los comandos posteriores se ejecuten correctamente. XenMobile Mail Manager ahora puede establecer un período de caducidad para las conexiones. Cuando la conexión alcanza su tiempo de caducidad, XenMobile Mail Manager cierra la sesión de PowerShell de forma controlada y crea una sesión. Al hacerlo, es menos probable que la sesión de PowerShell se vuelva inestable, lo que reduce significativamente la posibilidad de un error de instantánea.
- **Flujo de trabajo de instantáneas mejorado:** Las instantáneas principales son una operación que consume mucho tiempo y recursos. Si se produce un error durante una instantánea, XenMobile Mail Manager ahora intenta varias veces (hasta tres) completar una instantánea. Los intentos posteriores no comienzan desde el principio. XenMobile Mail Manager continúa desde donde lo dejó. Esta mejora aumenta la tasa de éxito de las instantáneas en general al permitir que los errores transitorios pasen mientras una instantánea aún está en curso.
- **Diagnóstico mejorado:** La resolución de problemas de las operaciones de instantáneas es ahora más fácil con tres nuevos archivos de diagnóstico que se generan opcionalmente durante una instantánea. Estos archivos ayudan a identificar problemas de comandos de PowerShell, buzones con información faltante y dispositivos que no se pueden relacionar con un buzón. Un administrador puede usar estos archivos para identificar datos que pueden no ser correctos en Exchange.

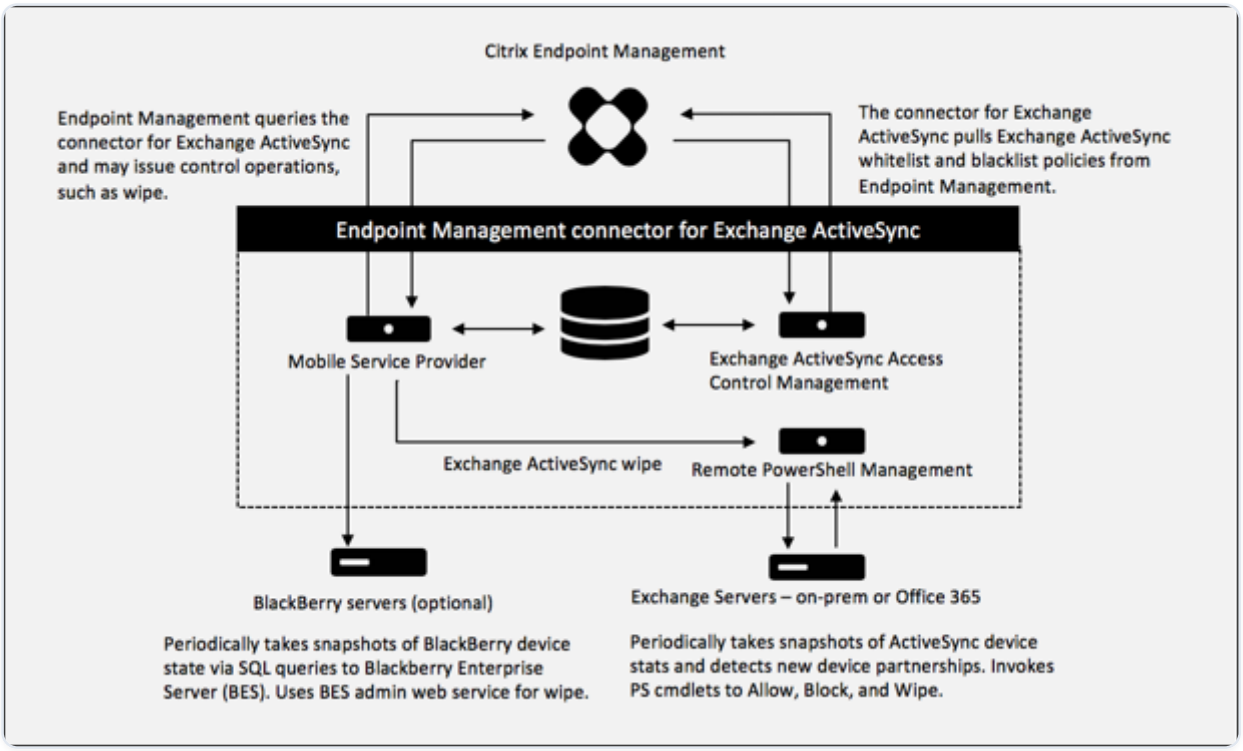
- **Uso de memoria mejorado:** XenMobile Mail Manager ahora es más eficiente en el uso de la memoria. Los administradores pueden programar XenMobile Mail Manager para que se reinicie automáticamente y así proporcionar un estado limpio al sistema.
- **Requisito previo de Microsoft .NET Framework 4.6:** La versión de requisito previo de Microsoft .NET Framework es ahora la versión 4.6.

Problemas resueltos

- Error de solicitud de credenciales: La inestabilidad de la sesión de Office 365 a menudo causaba este error. La mejora de la conexión a Exchange aborda el problema. (XMHELP-293, XMHELP-311, XMHELP-801)
- Imprecisiones en el recuento de buzones y dispositivos: XenMobile Mail Manager tiene un algoritmo mejorado de asociación de buzones a dispositivos. La función de diagnóstico mejorado ayuda a identificar buzones y dispositivos que XenMobile Mail Manager considera que no están dentro de su ámbito de responsabilidad. (XMHELP-623)
- Comandos de permitir/bloquear/borrar no reconocidos: Se corrigió un error por el cual, a veces, los comandos de permitir/bloquear/borrar de XenMobile Mail Manager no se reconocían. (XMHELP-489)
- Administración de memoria: Mejor administración y mitigación de la memoria. (XMHELP-419)

Arquitectura

El siguiente diagrama muestra los componentes principales del conector de Citrix Endpoint Management para Exchange ActiveSync. Para un diagrama de arquitectura de referencia detallado, consulte Arquitectura.



Los dos componentes principales son:

- **Administración de control de acceso de Exchange ActiveSync:** Se comunica con Citrix Endpoint Management para recuperar una política de Exchange ActiveSync de Citrix Endpoint Management y fusiona esta política con cualquier política definida localmente para determinar los dispositivos de Exchange ActiveSync a los que se debe permitir o denegar el acceso a Exchange. La política local permite ampliar las reglas de la política para permitir el control de acceso por grupo de Active Directory, usuario, tipo de dispositivo o agente de usuario del dispositivo (generalmente la versión de la plataforma móvil).
- **Administración remota de PowerShell:** Responsable de programar e invocar comandos remotos de PowerShell para aplicar la directiva compilada por la Administración de control de acceso de Exchange ActiveSync. Periódicamente, toma una instantánea de la base de datos de Exchange ActiveSync para detectar dispositivos Exchange ActiveSync nuevos o modificados.

Requisitos del sistema y requisitos previos

Se requieren los siguientes requisitos mínimos del sistema para usar el conector de Citrix Endpoint Management para Exchange ActiveSync:

- Windows Server 2016, Windows Server 2012 R2 o Windows Server 2008 R2 Service Pack 1. Debe ser un servidor basado en inglés. La compatibilidad con Windows Server 2008 R2 Service Pack 1 finaliza el January 14, 2020 y la compatibilidad con Windows Server 2012 R2 finaliza el October 10, 2023.

- Microsoft SQL Server 2016 Service Pack 2, SQL Server 2014 Service Pack 3 o SQL Server 2012 Service Pack 4.
- Microsoft .NET Framework 4.6.
- Blackberry Enterprise Service, versión 5 (opcional).

Versiones mínimas compatibles de Microsoft Exchange Server:

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013 (la compatibilidad finaliza el April 11, 2023)
- Exchange Server 2010 Service Pack 3 (la compatibilidad finaliza el January 14, 2020)

Requisitos previos

- Debe instalarse Windows Management Framework.
    - PowerShell V5, V4 y V3
- La política de ejecución de PowerShell debe establecerse en RemoteSigned mediante Set-ExecutionPolicy RemoteSigned.
- El puerto TCP 80 debe estar abierto entre el equipo que ejecuta el conector para Exchange ActiveSync y el servidor remoto de Exchange.

Clientes de correo electrónico de dispositivos: No todos los clientes de correo electrónico devuelven de forma coherente el mismo ID de ActiveSync para un dispositivo. Dado que el conector para Exchange ActiveSync espera un ID de ActiveSync único para cada dispositivo, solo se admiten los clientes de correo electrónico que generan de forma coherente el mismo ID de ActiveSync único para cada dispositivo. Citrix ha probado estos clientes de correo electrónico y no se han producido errores:

- Cliente de correo electrónico nativo de Samsung
- Cliente de correo electrónico nativo de iOS

Exchange: Los requisitos para el equipo local que ejecuta Exchange son los siguientes:

Las credenciales especificadas en la interfaz de usuario de configuración de Exchange deben poder conectarse al servidor de Exchange y tener acceso completo para ejecutar los siguientes cmdlets de PowerShell específicos de Exchange.

- **Para Exchange Server 2010 SP2:**

  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-ActiveSyncDevice`
  - `Get-ActiveSyncDeviceStatistics`
  - `Clear-ActiveSyncDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`

- **Para Exchange Server 2013 y Exchange Server 2016:**
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`

- Si el conector para Exchange ActiveSync está configurado para ver todo el bosque, se debe haber concedido permiso para ejecutar: **Set-AdServerSettings -ViewEntireForest $true**
- Las credenciales proporcionadas deben tener el derecho de conectarse a Exchange Server a través de la Shell remota. De forma predeterminada, el usuario que instaló Exchange tiene este derecho.
- Para establecer una conexión remota y ejecutar comandos remotos, las credenciales deben corresponder a un usuario que sea administrador en la máquina remota. Puede utilizar Set-PSSessionConfiguration para eliminar el requisito administrativo, pero la discusión de ese comando está fuera del alcance de este documento. Para obtener más información, consulte el artículo de Microsoft Acerca de las configuraciones de sesión.

- El servidor de Exchange debe configurarse para admitir solicitudes remotas de PowerShell a través de HTTP. Normalmente, lo único que se requiere es que un administrador ejecute el siguiente comando de PowerShell en el servidor de Exchange: WinRM QuickConfig.
- Exchange tiene muchas directivas de limitación. Una de las directivas controla cuántas conexiones simultáneas de PowerShell se permiten por usuario. El número predeterminado de conexiones simultáneas permitidas para un usuario es 18 en Exchange 2010. Cuando se alcanza el límite de conexiones, el conector para Exchange ActiveSync no puede conectarse al servidor de Exchange. Hay formas de cambiar el número máximo de conexiones simultáneas permitidas a través de PowerShell que están fuera del alcance de esta documentación. Si le interesa, investigue las directivas de limitación de Exchange relacionadas con la administración remota con PowerShell.

Requisitos para Office 365 Exchange

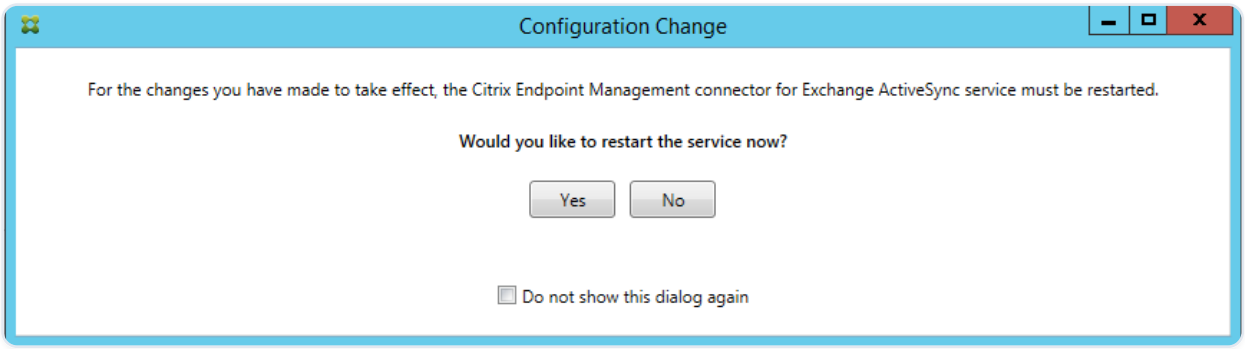
- **Permisos:** Las credenciales especificadas en la interfaz de usuario de configuración de Exchange deben poder conectarse a Office 365 y tener acceso completo para ejecutar los siguientes cmdlets de PowerShell específicos de Exchange:
  - `Get-CASMailbox`
  - `Set-CASMailbox`
  - `Get-Mailbox`
  - `Get-MobileDevice`
  - `Get-MobileDeviceStatistics`
  - `Clear-MobileDevice`
  - `Get-ExchangeServer`
  - `Get-ManagementRole`
  - `Get-ManagementRoleAssignment`
- **Privilegios:** Las credenciales proporcionadas deben haber recibido el derecho de conectarse al servidor de Office 365 a través de la Shell remota. De forma predeterminada, el administrador en línea de Office 365 tiene los privilegios necesarios.
- **Directivas de limitación:** Exchange tiene muchas directivas de limitación. Una de las directivas controla cuántas conexiones simultáneas de PowerShell se permiten por usuario. El número predeterminado de conexiones simultáneas permitidas para un usuario es de tres en Office 365. Cuando se alcanza el límite de conexiones, el conector para Exchange ActiveSync no puede conectarse al servidor de Exchange. Hay formas de cambiar el número máximo de

conexiones simultáneas permitidas a través de PowerShell que están fuera del alcance de esta documentación. Si le interesa, investigue las directivas de limitación de Exchange relacionadas con la administración remota con PowerShell.

Instalar y configurar

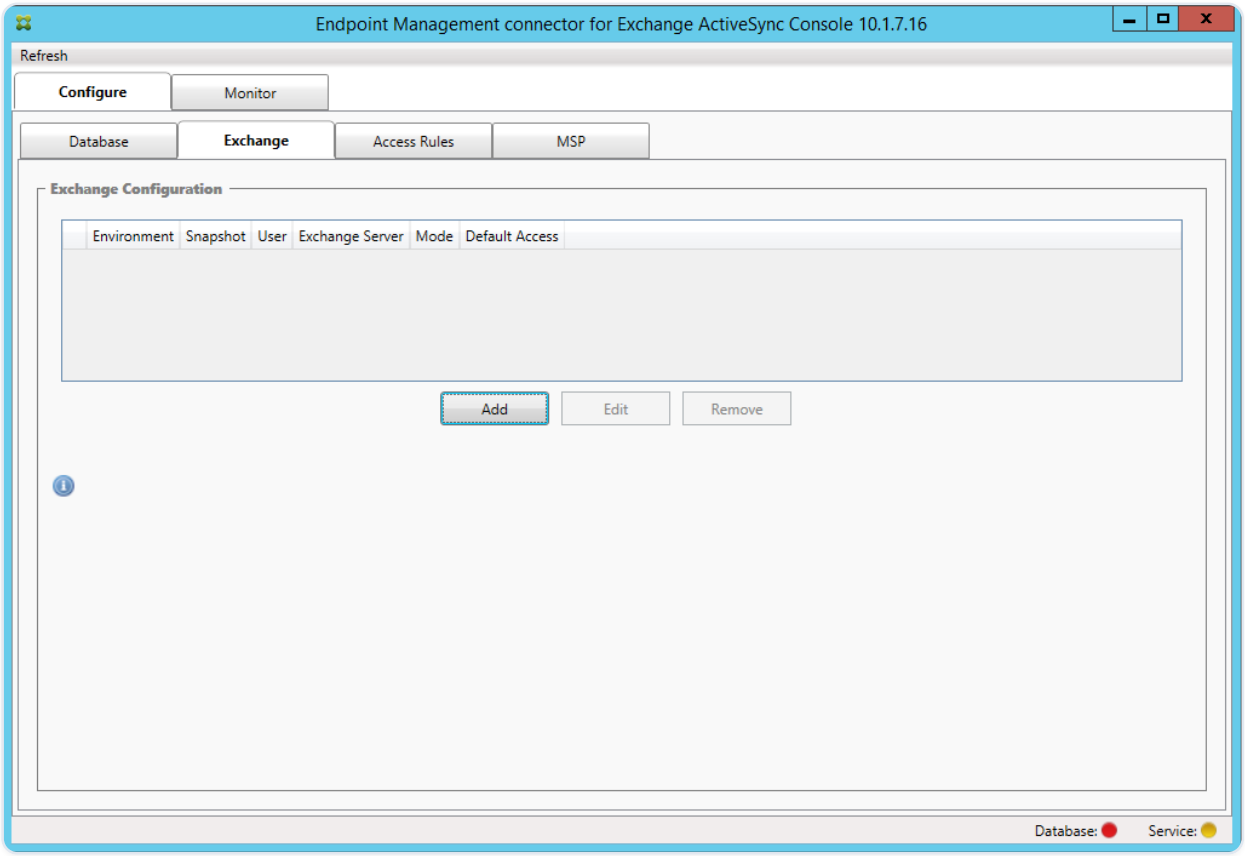
1. Haga clic en el archivo XmmSetup.msi y siga las indicaciones del instalador para instalar el conector de Citrix Endpoint Management para Exchange ActiveSync.
2. Deje seleccionada la opción **Iniciar la utilidad de configuración** en la última pantalla del asistente de configuración. O, desde el menú **Inicio**, abra el conector para Exchange ActiveSync.
3. Configure las siguientes propiedades de la base de datos:
   - Seleccione la ficha **Configurar > Base de datos**.
   - Introduzca el nombre del servidor SQL (el valor predeterminado es localhost).
   - Mantenga la base de datos como la predeterminada **CitrixXmm**.
4. Seleccione uno de los siguientes modos de autenticación utilizados para SQL:
   - **SQL:** Introduzca el nombre de usuario y la contraseña de un usuario SQL válido.
   - **Windows Integrated:** Si selecciona esta opción, las credenciales de inicio de sesión del servicio XenMobile Mail Manager deben cambiarse a una cuenta de Windows que tenga permisos para acceder al servidor SQL. Para ello, abra **Panel de control > Herramientas administrativas > Servicios**, haga clic con el botón secundario en la entrada del servicio XenMobile Mail Manager y, a continuación, haga clic en la ficha **Iniciar sesión**.

   Si también se elige Windows Integrated para la conexión a la base de datos de BlackBerry, la cuenta de Windows especificada aquí también debe tener acceso a la base de datos de BlackBerry.
5. Haga clic en **Probar conectividad** para comprobar que se puede establecer una conexión con el servidor SQL y, a continuación, haga clic en **Guardar**.
6. Un mensaje le pide que reinicie el servicio. Haga clic en **Sí**.



7. Configure uno o varios servidores Exchange:

   - Si gestiona un único entorno de Exchange, especifique un solo servidor. Si gestiona varios entornos de Exchange, especifique un único servidor de Exchange para cada entorno de Exchange.
   - Haga clic en la pestaña **Configure > Exchange** y, a continuación, haga clic en **Add**.

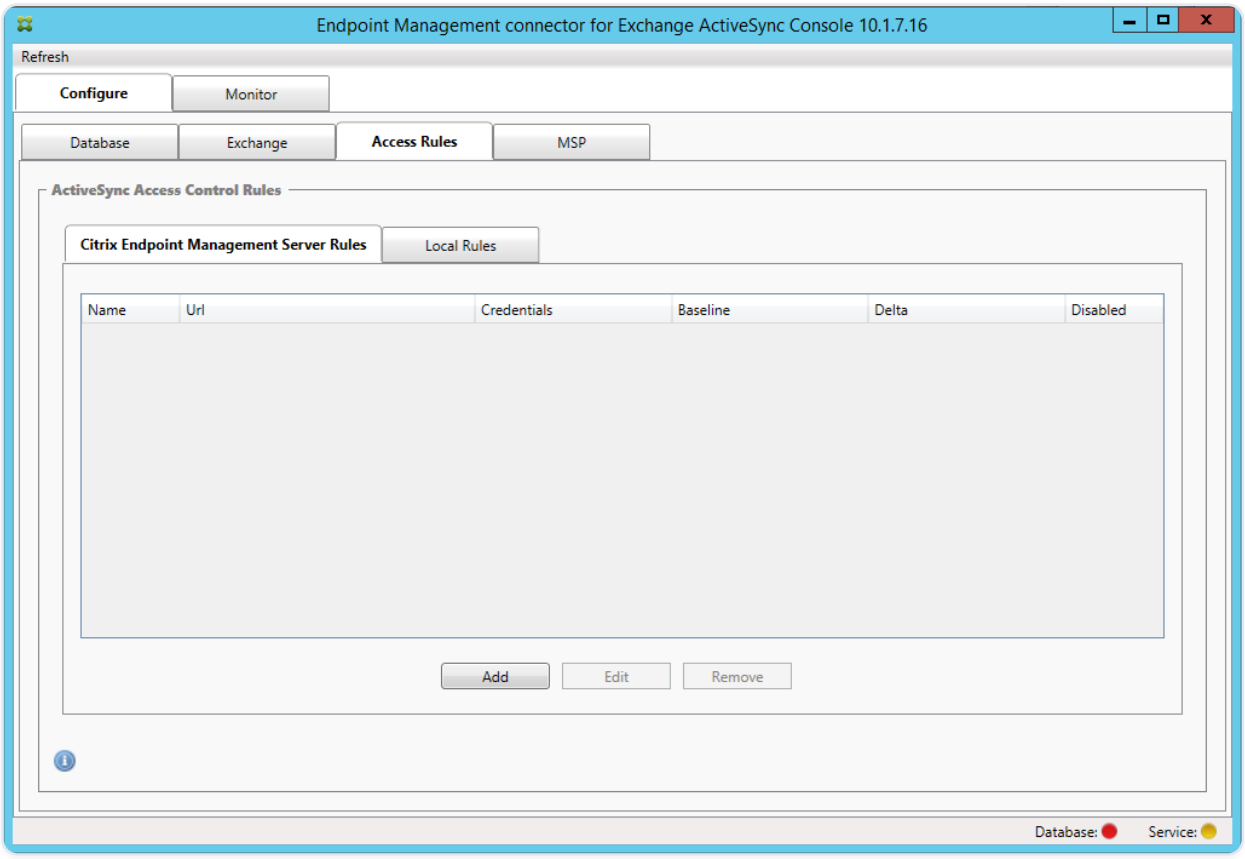


8. Seleccione el tipo de entorno de Exchange Server: **On Premise** u **Office 365**.

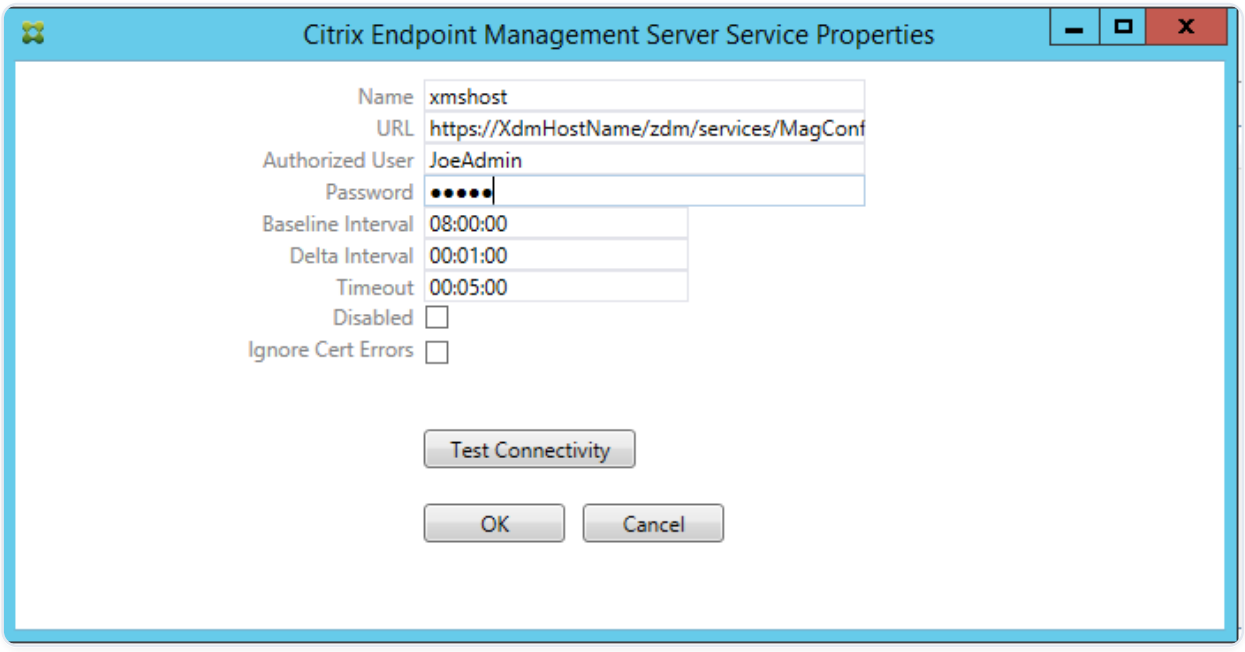
   - Si selecciona **On Premise**, introduzca el nombre del servidor de Exchange que se utilizará para los comandos de PowerShell remoto.
   - Introduzca el **nombre de usuario** de una identidad de Windows que tenga los derechos adecuados en el servidor de Exchange, tal como se especifica en la sección Requisitos, y, a continuación, introduzca la **contraseña** del usuario.

- Seleccione la programación para ejecutar instantáneas principales. Una instantánea principal detecta cada asociación de Exchange ActiveSync.
- Seleccione la programación para ejecutar instantáneas secundarias. Una instantánea secundaria detecta las asociaciones de Exchange ActiveSync recién creadas.
- Seleccione el tipo de instantánea: **Deep** o **Shallow**. Las instantáneas superficiales suelen ser mucho más rápidas y son suficientes para realizar todas las funciones de control de acceso de Exchange ActiveSync del conector para Exchange ActiveSync.
- Seleccione el acceso predeterminado: **Allow**, **Block** o **Unchanged**. Esta configuración controla cómo se tratan todos los dispositivos que no sean los identificados por reglas explícitas de Citrix Endpoint Management o locales. Si selecciona **Allow**, se permite el acceso de ActiveSync a todos esos dispositivos. Si selecciona **Block**, se deniega el acceso. Si selecciona **Unchanged**, no se realiza ningún cambio.
- Seleccione el modo de comando de ActiveSync: **PowerShell** o **Simulation**.
- En el modo **PowerShell**, el conector para Exchange ActiveSync emite comandos de PowerShell para aplicar el control de acceso deseado. En el modo de simulación, el conector para Exchange ActiveSync no emite comandos de PowerShell, sino que registra el comando previsto y los resultados previstos en la base de datos. En el modo de simulación, el usuario puede utilizar la pestaña **Monitor** para ver qué habría ocurrido si el modo PowerShell estuviera habilitado.
- En **Connection Expiration**, establezca las horas y los minutos de la duración de una conexión. Cuando una conexión alcanza la edad especificada, se marca como caducada, de modo que la conexión nunca se vuelve a utilizar. Cuando la conexión caducada ya no se utiliza, el conector para Exchange ActiveSync cierra la conexión de forma segura. Cuando se necesita una conexión de nuevo, se inicializa una nueva conexión si no hay ninguna disponible. Si no se especifica ninguna, se utiliza el valor predeterminado de 30 minutos.
- Seleccione **View Entire Forest** para configurar el conector para Exchange ActiveSync para que vea todo el bosque de Active Directory en el entorno de Exchange.
- Seleccione el protocolo de autenticación: **Kerberos** o **Basic**. El conector para Exchange ActiveSync admite la autenticación básica para implementaciones locales. Esto permite utilizar el conector cuando el servidor del conector no es miembro del dominio en el que reside el servidor de Exchange.
- Haga clic en **Probar conectividad** para comprobar que se puede establecer una conexión con el servidor de Exchange y, a continuación, haga clic en **Guardar**.
- Un mensaje le pide que reinicie el servicio. Haga clic en **Sí**.

9. Configure las reglas de acceso: Seleccione la ficha **Configurar > Reglas de acceso**, haga clic en la ficha **Reglas de Citrix Endpoint Management** y, a continuación, haga clic en **Agregar**.



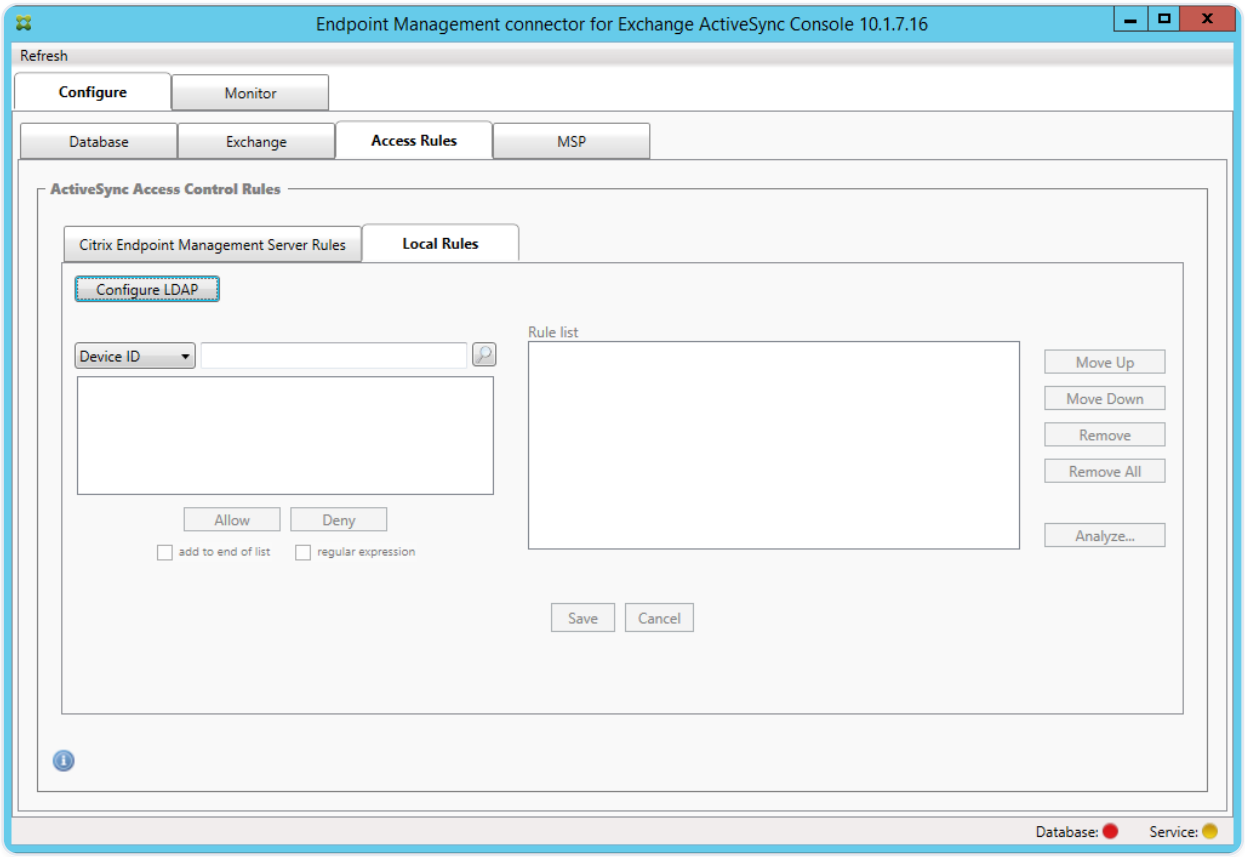
10. En la página **Propiedades del servicio del servidor de Citrix Endpoint Management**, modifique la cadena de URL para que apunte al servidor de Citrix Endpoint Management. Por ejemplo, si el nombre de la instancia es `zdm`, introduzca `https://<XdmHostName>/zdm/services/MagConfigService`. En el ejemplo, reemplace `XdmHostName` por la dirección IP o DNS del servidor de Citrix Endpoint Management.



- Introduzca un usuario autorizado del servidor.
- Introduzca la contraseña del usuario.
- Mantenga los valores predeterminados para **Intervalo de línea base**, **Intervalo delta** y **Tiempo de espera**.
- Haga clic en **Probar conectividad** para comprobar la conexión con el servidor y, a continuación, haga clic en **Aceptar**.

Si la casilla de verificación **Inhabilitado** está seleccionada, el servicio de correo de Citrix Endpoint Management no recopila directivas de Citrix Endpoint Management.

11. Haga clic en la ficha **Reglas locales**.

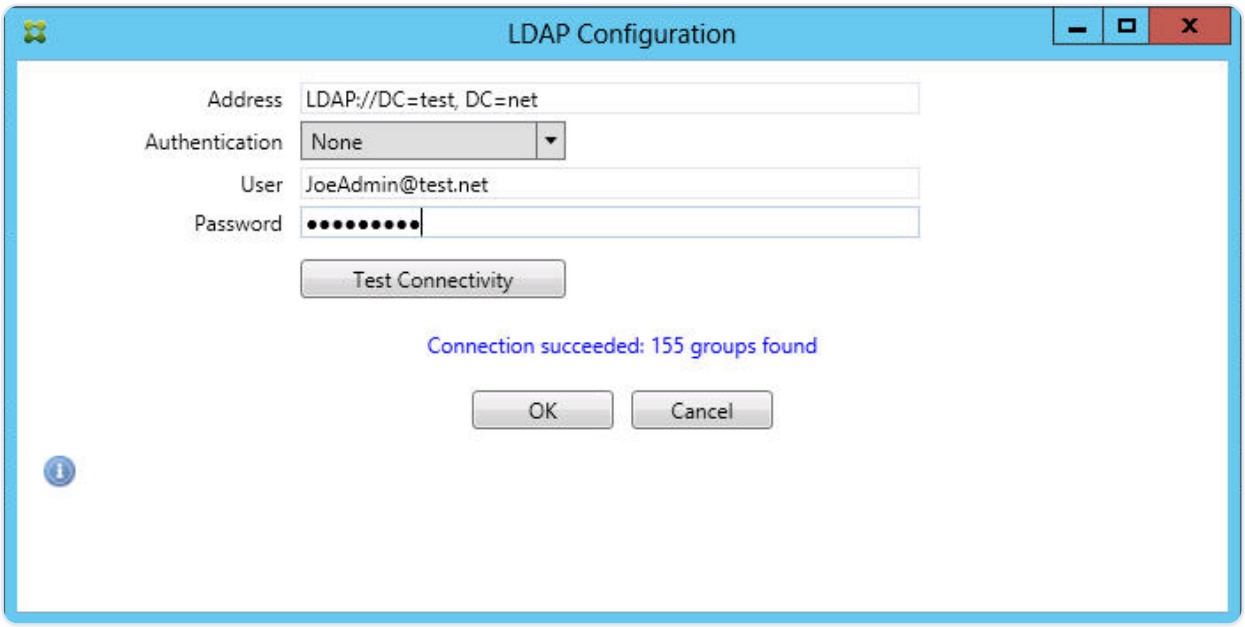


- Puede agregar reglas locales basadas en ActiveSync Device ID, Device Type, AD Group, User o UserAgent del dispositivo. En la lista, seleccione el tipo adecuado.
- Introduzca texto o fragmentos de texto en el cuadro de texto. Opcionalmente, haga clic en el botón de consulta para ver las entidades que coinciden con el fragmento.

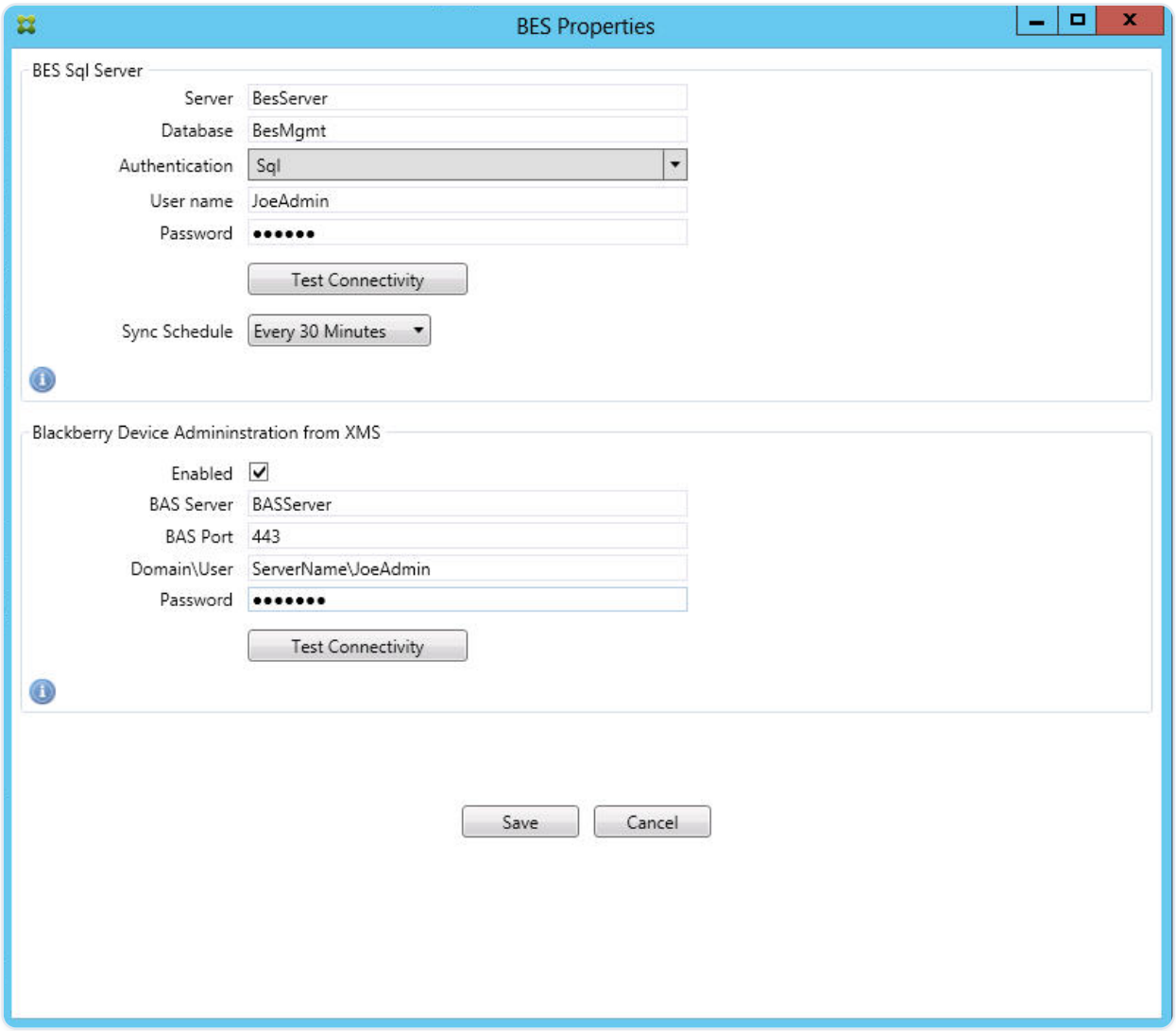
Para todos los tipos excepto Grupo, el sistema se basa en los dispositivos que se han encontrado en una instantánea. Por lo tanto, si está empezando y no ha completado una instantánea, no hay entidades disponibles.

- Seleccione un valor de texto y, a continuación, haga clic en **Permitir** o **Denegar** para agregarlo al panel **Lista de reglas** de la derecha. Puede cambiar el orden de las reglas o eliminarlas mediante los botones situados a la derecha del panel **Lista de reglas**. El orden es importante porque, para un usuario y un dispositivo determinados, las reglas se evalúan en el orden mostrado y una coincidencia con una regla superior (más cercana a la parte superior) hace que las reglas posteriores no tengan efecto. Por ejemplo, si tiene una regla que permite todos los dispositivos iPad y una regla posterior que bloquea al usuario Matt, el iPad de Matt seguirá estando permitido porque la regla del iPad tiene una prioridad efectiva más alta que la regla de Matt.
- Para realizar un análisis de las reglas dentro de la lista de reglas y encontrar posibles anulaciones, conflictos o construcciones suplementarias, haga clic en **Analizar** y, a continuación, en **Guardar**.

12. Si quiere construir reglas locales que operen en grupos de Active Directory, haga clic en **Configurar LDAP** y, a continuación, configure las propiedades de conexión LDAP.



13. Opcionalmente, configure una o varias instancias de BlackBerry Enterprise Server (BES): Haga clic en **Agregar** y, a continuación, introduzca el nombre del servidor SQL de BES.



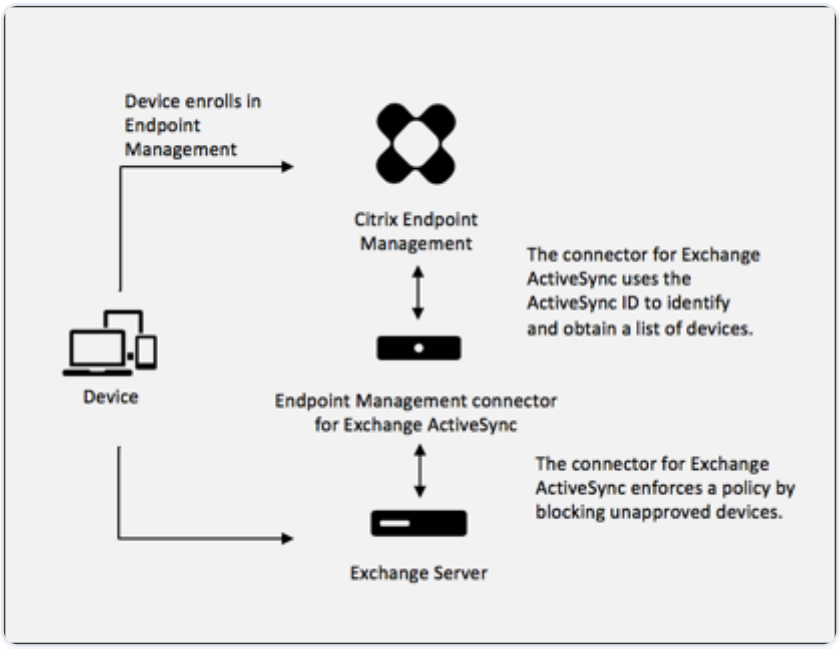
- Introduzca el nombre de la base de datos de administración de BES.
- Seleccione el modo de **autenticación**. Si selecciona la autenticación integrada de Windows, la cuenta de usuario del conector para el servicio Exchange ActiveSync es la cuenta que se utiliza para conectarse al servidor SQL de BES. Si también elige Windows Integrated para la conexión de la base de datos del conector, la cuenta de Windows especificada aquí también debe tener acceso a la base de datos del conector.
- Si selecciona la **autenticación SQL**, introduzca el nombre de usuario y la contraseña.
- Establezca la **programación de sincronización**. Esta es la programación utilizada para conectarse al servidor SQL de BES y comprobar si hay actualizaciones de dispositivos.
- Haga clic en **Probar conectividad** para comprobar la conectividad con el servidor SQL. Si selecciona Windows Integrated, esta prueba utiliza el usuario actualmente conectado y no el usuario del servicio del conector, por lo que no prueba con precisión la autenticación SQL.

- Para admitir el borrado remoto y el restablecimiento de contraseña de dispositivos BlackBerry desde Citrix Endpoint Management, seleccione la casilla de verificación **Habilitado**.
- Introduzca el nombre de dominio completo (FQDN) de BES.
- Introduzca el puerto de BES utilizado para el servicio web de administración.
- Introduzca el usuario completo y la contraseña requeridos por el servicio BES.
- Haga clic en **Probar conectividad** para probar la conexión a BES y, a continuación, haga clic en **Guardar**.

Aplicar directivas de correo electrónico con ID de ActiveSync

La directiva de correo electrónico de su empresa puede dictar que ciertos dispositivos no están aprobados para el uso del correo electrónico corporativo. Para seguir esta directiva, debe asegurarse de que los empleados no puedan acceder al correo electrónico corporativo desde dichos dispositivos. El conector de Citrix Endpoint Management para Exchange ActiveSync y Citrix Endpoint Management trabajan juntos para aplicar dicha directiva de correo electrónico. Citrix Endpoint Management establece la directiva para el acceso al correo electrónico corporativo. Cuando un dispositivo no aprobado se inscribe en Citrix Endpoint Management, el conector para Exchange ActiveSync aplica la directiva.

El cliente de correo electrónico de un dispositivo se anuncia a Exchange Server (u Office 365) utilizando el ID del dispositivo, también conocido como ID de ActiveSync, que se utiliza para identificar el dispositivo. Citrix Secure Hub obtiene un identificador similar y lo envía a Citrix Endpoint Management cuando el dispositivo se inscribe. Al comparar los dos ID de dispositivo, el conector para Exchange ActiveSync puede determinar si un dispositivo específico debe tener acceso al correo electrónico corporativo. La siguiente figura ilustra este concepto:



Si Citrix Endpoint Management envía al conector para Exchange ActiveSync un ID de ActiveSync diferente del ID que el dispositivo publica en Exchange, el conector no puede indicar a Exchange qué hacer con el dispositivo.

La coincidencia de ID de ActiveSync funciona de forma fiable en la mayoría de las plataformas. Sin embargo, Citrix ha descubierto que en algunas implementaciones de Android, el ID de ActiveSync del dispositivo es diferente del ID que el cliente de correo anuncia a Exchange. Para mitigar este problema, puede hacer lo siguiente:

- En las plataformas Android, Citrix recomienda utilizar Citrix Secure Mail.

Para garantizar que la directiva de acceso al correo electrónico corporativo se aplique correctamente, puede adoptar una postura de seguridad defensiva. Configure el conector de Citrix Endpoint Management para Exchange ActiveSync para bloquear correos electrónicos estableciendo la directiva estática en **Denegar** de forma predeterminada. Esto significa que si un empleado configura otro cliente de correo electrónico en un dispositivo Android y la detección de ID de ActiveSync no funciona, el correo electrónico corporativo deniega el acceso al empleado.

Reglas de control de acceso

El conector de Citrix Endpoint Management para Exchange ActiveSync proporciona un enfoque basado en reglas para configurar dinámicamente el control de acceso para dispositivos Exchange ActiveSync. Una regla de control de acceso del conector consta de dos partes: una expresión de coincidencia y un estado de acceso deseado (Permitir o Bloquear). Una regla se puede evaluar contra un dispositivo Exchange ActiveSync dado para determinar si la regla se aplica o coincide con el dispositivo. Existen varios tipos de expresiones de coincidencia; por ejemplo, una regla puede coincidir con todos los dispositivos de un tipo de dispositivo determinado, o con un ID de

dispositivo Exchange ActiveSync específico, o con todos los dispositivos de un usuario específico, y así sucesivamente.

En cualquier momento durante la adición, eliminación y reorganización de las reglas en la lista de reglas, al hacer clic en el botón **Cancelar** se revierte la lista de reglas al estado en que se encontraba cuando se abrió por primera vez. A menos que haga clic en **Guardar**, cualquier cambio realizado en esta ventana se perderá si cierra la herramienta Configurar.

El conector de Citrix Endpoint Management para Exchange ActiveSync tiene tres tipos de reglas: reglas locales, reglas del servidor de Citrix Endpoint Management (también conocidas como reglas XDM) y la regla de acceso predeterminada.

Reglas locales: Las reglas locales tienen la máxima prioridad: si un dispositivo coincide con una regla local, la evaluación de la regla se detiene. No se consultarán ni las reglas del servidor de Citrix Endpoint Management ni la regla de acceso predeterminada. Las reglas locales se configuran localmente en el conector para Exchange ActiveSync a través de la ficha **Configurar > Reglas de acceso > Reglas locales**. La coincidencia de soporte se basa en la pertenencia de un usuario a un grupo de Active Directory determinado. La coincidencia de soporte se basa en expresiones regulares para los siguientes campos:

- ID de dispositivo de ActiveSync
- Tipo de dispositivo de ActiveSync
- Nombre principal de usuario (UPN)
- Agente de usuario de ActiveSync (normalmente la plataforma del dispositivo o el cliente de correo electrónico)

Siempre que se haya completado una instantánea principal y se hayan encontrado dispositivos, puede agregar una regla normal o una regla de expresión regular. Si no se ha completado una instantánea principal, solo puede agregar reglas de expresión regular.

Reglas del servidor de Citrix Endpoint Management: Las reglas del servidor de Citrix Endpoint Management son referencias a un servidor externo de Citrix Endpoint Management que proporciona reglas sobre los dispositivos administrados. El servidor de Citrix Endpoint Management se puede configurar con sus propias reglas de alto nivel que identifican los dispositivos que se permitirán o bloquearán en función de las propiedades conocidas por Citrix Endpoint Management, como si el dispositivo tiene jailbreak o si tiene aplicaciones prohibidas. Citrix Endpoint Management evalúa las reglas de alto nivel y produce un conjunto de ID de dispositivo de ActiveSync permitidos o bloqueados, que luego se entregan al XenMobile Mail Manager.

Regla de acceso predeterminada: La regla de acceso predeterminada es única porque puede coincidir potencialmente con todos los dispositivos y siempre se evalúa en último lugar. Esta regla es la regla general, lo que significa que si un dispositivo determinado no coincide con una regla local o del servidor de Citrix Endpoint Management, el estado de acceso deseado del dispositivo se determina por el estado de acceso deseado de la regla de acceso predeterminada.

- **Acceso predeterminado – Permitir:** Se permitirá cualquier dispositivo que no coincida con una regla local o del servidor de Citrix Endpoint Management.
- **Acceso predeterminado – Bloquear:** Se bloqueará cualquier dispositivo que no coincida con una regla local o del servidor de Citrix Endpoint Management.
- **Acceso predeterminado - Sin cambios:** El conector para Exchange ActiveSync no modificará de ninguna manera el estado de acceso de ningún dispositivo que no coincida con una regla local o del servidor de Citrix Endpoint Management. Si Exchange ha puesto un dispositivo en modo de cuarentena, no se realiza ninguna acción. Por ejemplo, la única forma de sacar un dispositivo del modo de cuarentena es que una regla explícita local o de XDM anule la cuarentena.

Acerca de las evaluaciones de reglas

Para cada dispositivo que Exchange notifica al conector para Exchange ActiveSync, las reglas se evalúan en secuencia, de mayor a menor prioridad, de la siguiente manera:

- Reglas locales
- Reglas del servidor de Citrix Endpoint Management
- Regla de acceso predeterminada

Cuando se encuentra una coincidencia, la evaluación se detiene. Por ejemplo, si una regla local coincide con un dispositivo determinado, el dispositivo no se evaluará con ninguna de las reglas del servidor de Citrix Endpoint Management ni con la regla de acceso predeterminada. Esto también es válido dentro de un tipo de regla determinado. Por ejemplo, si hay más de una coincidencia para un dispositivo determinado en la lista de reglas locales, cuando se cumple la primera coincidencia, la evaluación se detiene.

El conector para Exchange ActiveSync reevalúa el conjunto de reglas actualmente definido cuando cambian las propiedades del dispositivo, cuando se agregan o eliminan dispositivos, o cuando las propias reglas cambian. Las instantáneas principales recogen los cambios y eliminaciones de propiedades del dispositivo a intervalos configurables. Las instantáneas secundarias recogen los nuevos dispositivos a intervalos configurables.

Exchange ActiveSync también tiene reglas que rigen el acceso. Es importante comprender cómo funcionan estas reglas en el contexto del conector para Exchange ActiveSync. Exchange se puede configurar con tres niveles de reglas: exenciones personales, reglas de dispositivo y configuraciones de la organización. El conector para Exchange ActiveSync automatiza el control de acceso emitiendo solicitudes de PowerShell remoto de forma programática para afectar las listas de exenciones personales. Estas son listas de ID de dispositivos de Exchange ActiveSync permitidos o bloqueados asociados a un buzón determinado. Cuando se implementa, el conector para Exchange ActiveSync asume eficazmente la administración de la capacidad de listas de exenciones dentro de Exchange. Consulte el artículo de Microsoft, Administración de dispositivos con Exchange y Configuration Manager.

El análisis es útil en situaciones en las que se han definido varias reglas para el mismo campo. Puede solucionar los problemas de las relaciones entre las reglas. El análisis se realiza desde la perspectiva de los campos de las reglas. Por ejemplo, las reglas se analizan en grupos según el campo que se está comparando, como el ID del dispositivo ActiveSync, el tipo de dispositivo ActiveSync, el usuario o el agente de usuario.

Terminología de las reglas

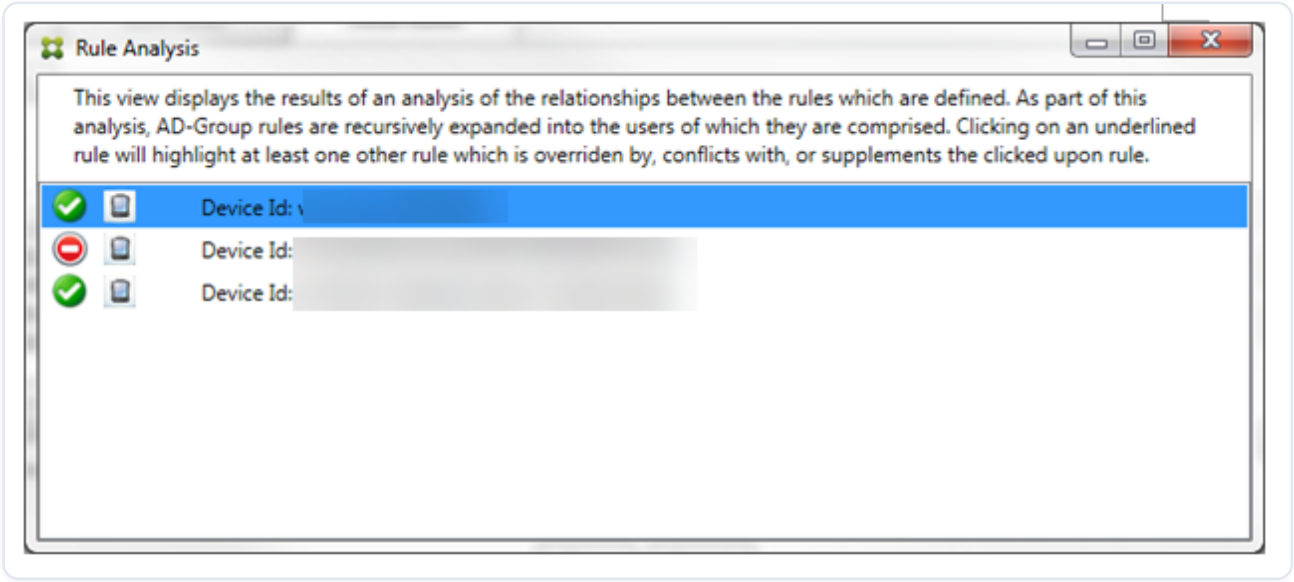
- **Regla de anulación:** Una anulación ocurre cuando más de una regla puede aplicarse al mismo dispositivo. Dado que las reglas se evalúan por prioridad en la lista, las instancias de reglas posteriores que podrían aplicarse podrían no evaluarse nunca.
- **Regla en conflicto:** Un conflicto ocurre cuando más de una regla puede aplicarse al mismo dispositivo, pero el acceso (Permitir/Bloquear) no coincide. Si las reglas en conflicto no son reglas de expresión regular, un conflicto siempre connota implícitamente una anulación.
- **Regla suplementaria:** Un suplemento ocurre cuando más de una regla es una regla de expresión regular y, por lo tanto, puede ser necesario asegurarse de que las dos (o más) expresiones regulares se puedan combinar en una única regla de expresión regular o que no dupliquen la funcionalidad. Una regla suplementaria también puede entrar en conflicto en su acceso (Permitir/Bloquear).
- **Regla principal:** La regla principal es la regla en la que se ha hecho clic dentro del cuadro de diálogo. La regla se indica visualmente mediante una línea de borde sólida que la rodea. La regla también tendrá una o dos flechas verdes que apuntan hacia arriba o hacia abajo. Si una flecha apunta hacia arriba, indica que hay reglas auxiliares que preceden a la regla principal. Si una flecha apunta hacia abajo, indica que hay reglas auxiliares que vienen después de la regla principal. Solo una regla principal puede estar activa en un momento dado.
- **Regla auxiliar:** Una regla auxiliar está relacionada de alguna manera con la regla principal, ya sea por anulación, conflicto o una relación suplementaria. Las reglas se indican visualmente

mediante un borde discontinuo que las rodea. Para cada regla principal, puede haber entre una y muchas reglas auxiliares. Al hacer clic en cualquier entrada subrayada, la regla o reglas auxiliares que se resaltan siempre son desde la perspectiva de la regla principal. Por ejemplo, la regla auxiliar es anulada por la regla principal, o la regla auxiliar entra en conflicto en su acceso con la regla principal, o la regla auxiliar complementa la regla principal.

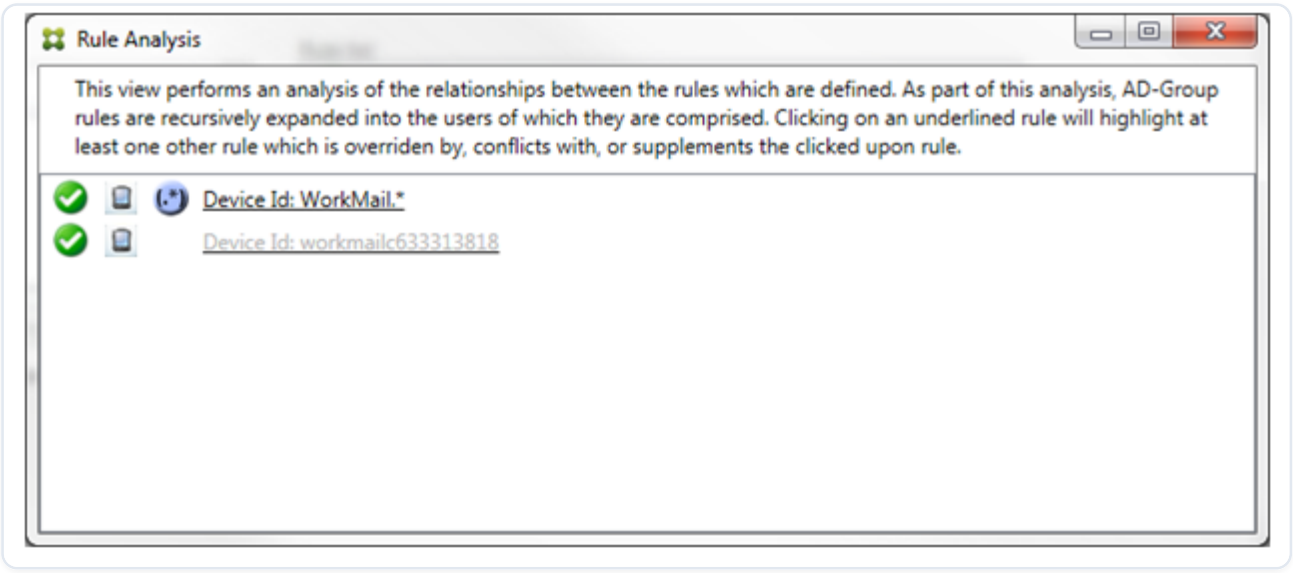
Cómo aparecen los tipos de reglas en el cuadro de diálogo Análisis de reglas

Cuando no hay conflictos, anulaciones o suplementos, el cuadro de diálogo **Análisis de reglas** no tiene entradas subrayadas. Hacer clic en cualquiera de los elementos no tiene ningún impacto; por ejemplo, se producen los efectos visuales normales de los elementos seleccionados.

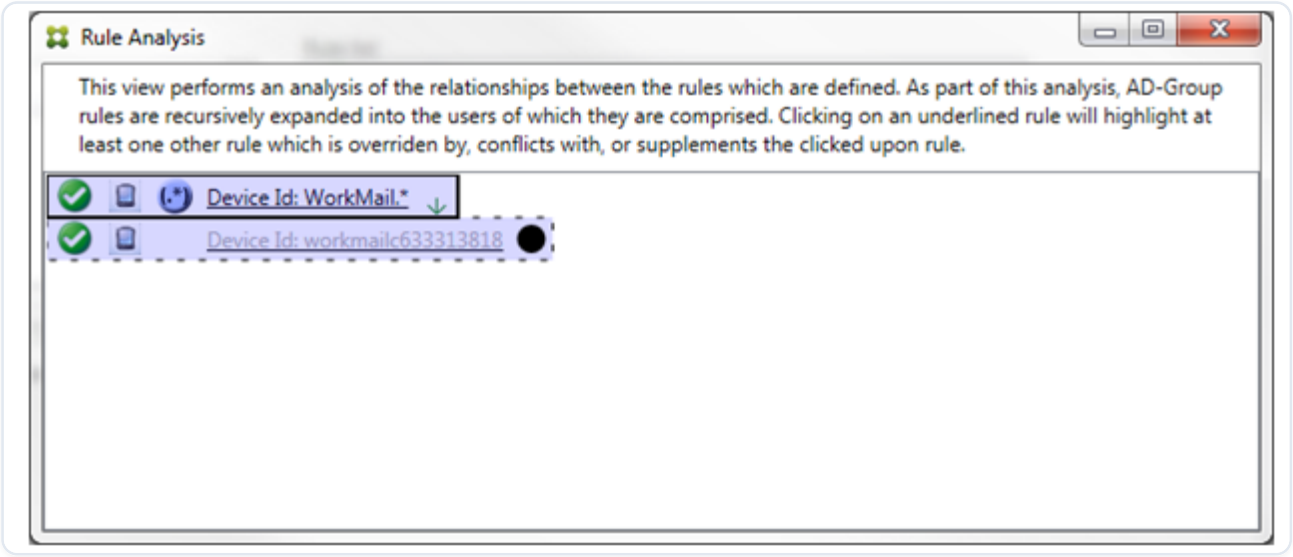
La ventana **Análisis de reglas** tiene una casilla de verificación que, cuando se selecciona, muestra solo aquellas reglas que son conflictos, anulaciones, redundancias o suplementos.



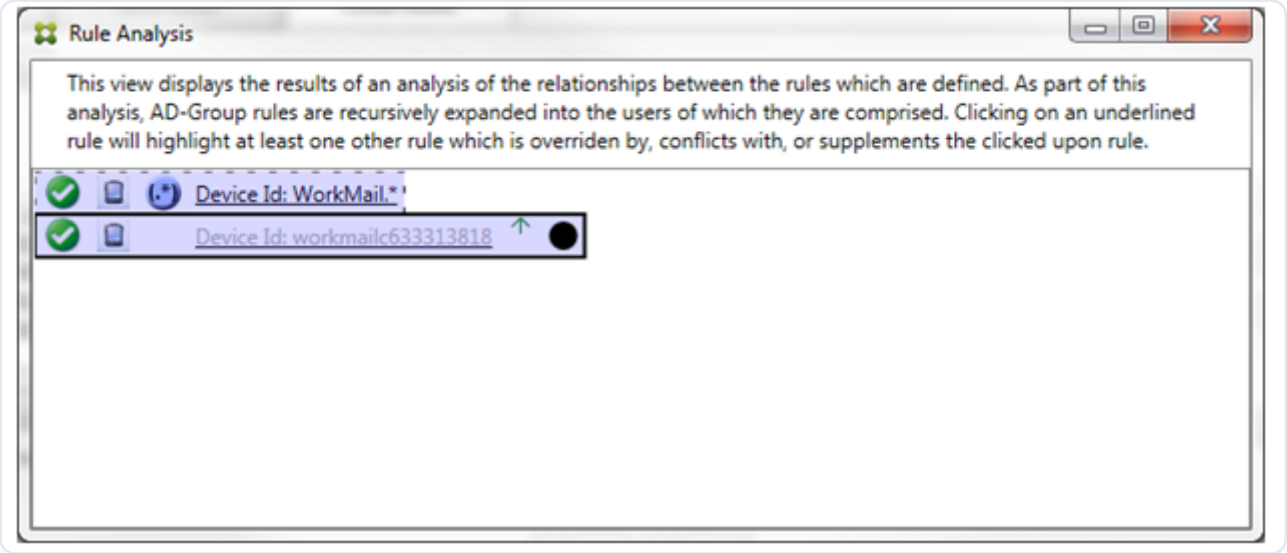
Cuando se produce una anulación, al menos dos reglas estarán subrayadas: la regla principal y la regla o reglas auxiliares. Al menos una regla auxiliar aparece con una fuente más clara para indicar que la regla ha sido anulada por una regla de mayor prioridad. Puede hacer clic en la regla anulada para averiguar qué regla o reglas la han anulado. Cada vez que se resalta una regla anulada, ya sea porque la regla es la principal o la auxiliar, aparece un círculo negro junto a ella como una indicación visual adicional de que la regla está inactiva. Por ejemplo, antes de hacer clic en la regla, el cuadro de diálogo aparece de la siguiente manera:



Al hacer clic en la regla de mayor prioridad, el cuadro de diálogo aparece de la siguiente manera:

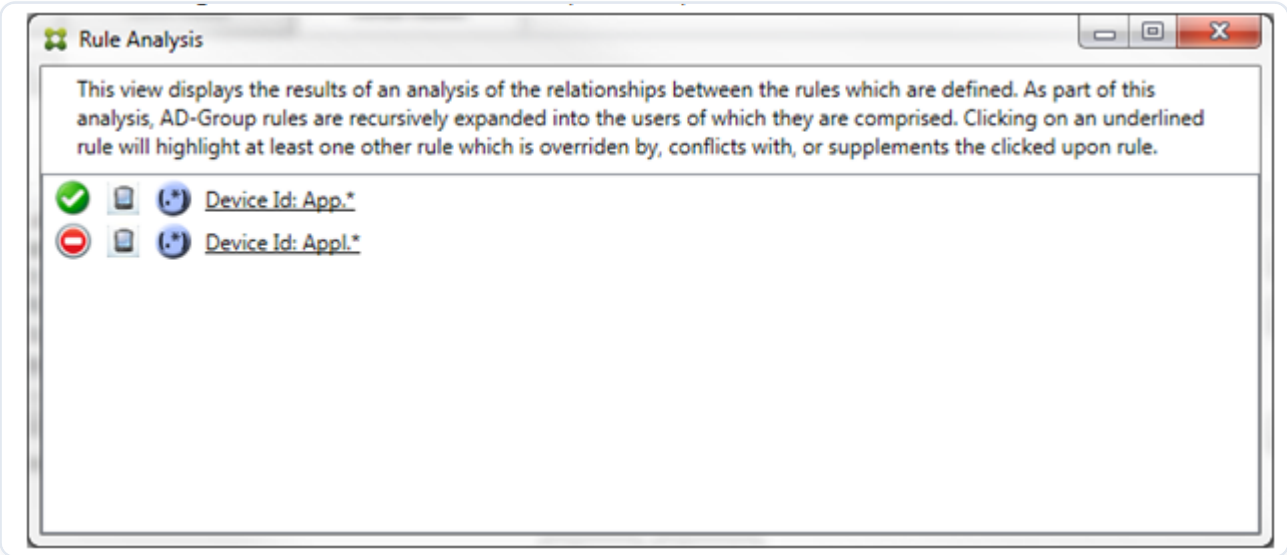


En este ejemplo, la regla de expresión regular `WorkMail.*` es la regla principal (indicada por el borde sólido) y la regla normal `workmailc633313818` es una regla auxiliar (indicada por el borde discontinuo). El punto negro junto a la regla auxiliar es una señal visual que indica además que la regla está inactiva (nunca se evaluará) debido a la regla de expresión regular de mayor prioridad que la precede. Después de hacer clic en la regla anulada, el cuadro de diálogo aparece de la siguiente manera:



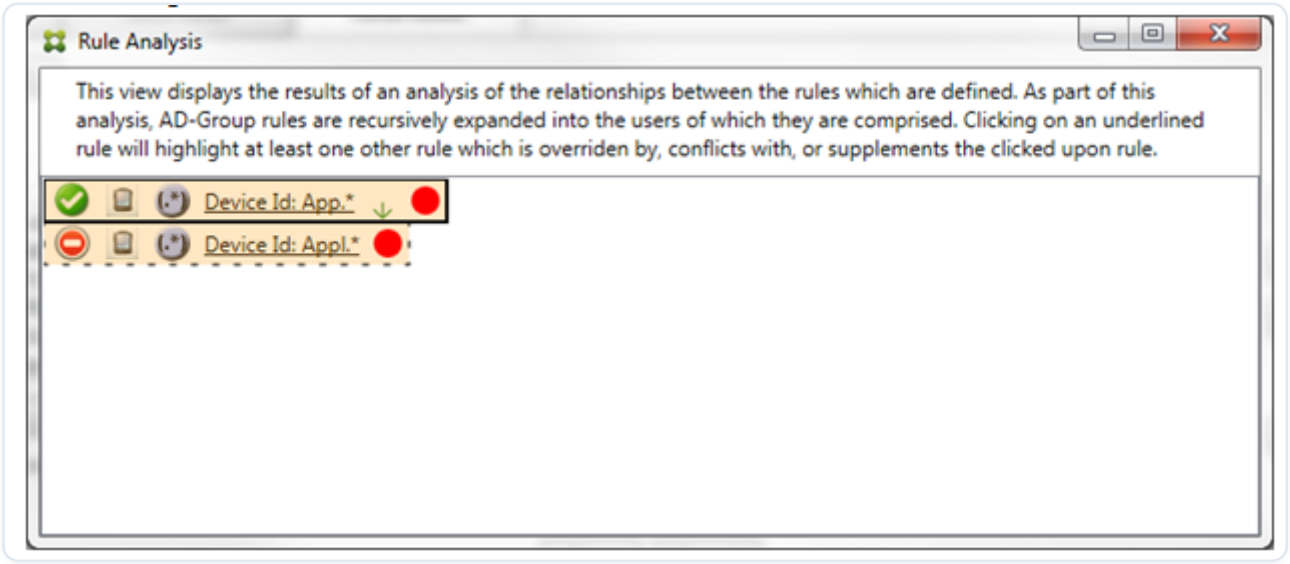
En el ejemplo anterior, la regla de expresión regular `WorkMail.*` es la regla auxiliar (indicada por el borde discontinuo) y la regla normal `workmailc633313818` es una regla principal (indicada por el borde sólido). Para este ejemplo sencillo, no hay mucha diferencia. Para un ejemplo más complicado, consulte el ejemplo de expresión compleja más adelante en este tema. En un escenario con muchas reglas definidas, al hacer clic en la regla anulada se identificaría rápidamente qué regla o reglas la habían anulado.

Cuando se produce un conflicto, al menos dos reglas se subrayarán: la regla principal y la regla o reglas auxiliares. Las reglas en conflicto se indican con un punto rojo. Las reglas que solo entran en conflicto entre sí solo son posibles con dos o más reglas de expresión regular definidas. En todos los demás escenarios de conflicto, no solo habrá un conflicto, sino también una anulación en juego. Antes de hacer clic en cualquiera de las reglas en un ejemplo sencillo, el cuadro de diálogo aparece de la siguiente manera:



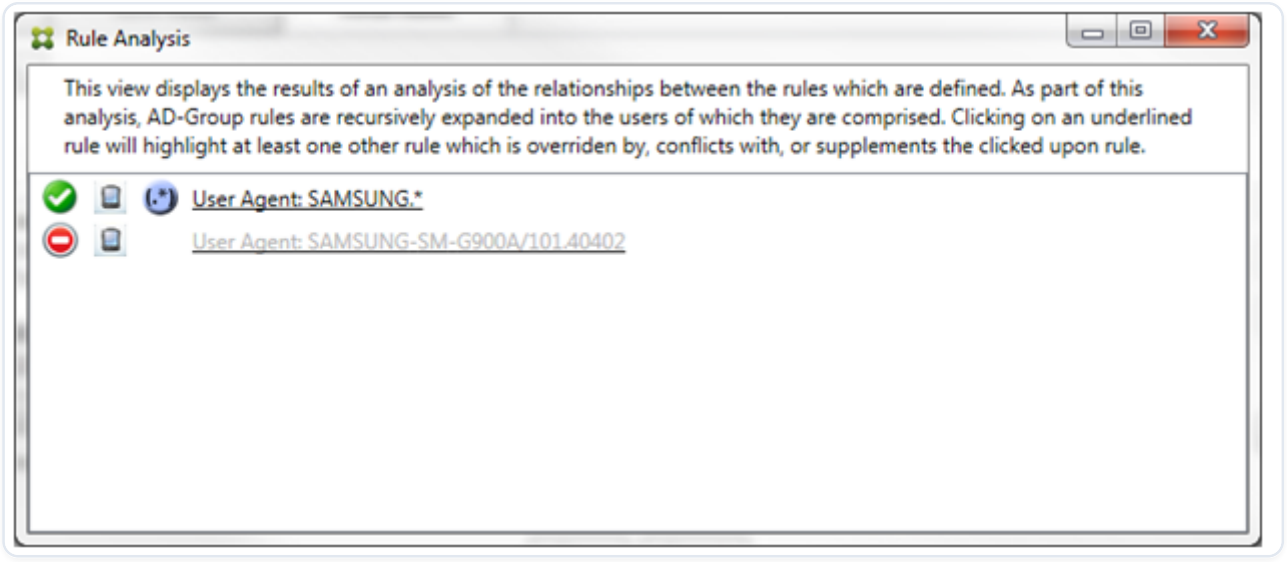
Al inspeccionar las dos reglas de expresión regular, es evidente que la primera regla permite todos los dispositivos con un ID de dispositivo que tiene "App" y que la segunda regla deniega todos los

dispositivos con un ID de dispositivo que tiene `Appl`. Además, aunque la segunda regla deniega todos los dispositivos con un ID de dispositivo que tiene `Appl`, ningún dispositivo con esos criterios de coincidencia será denegado debido a la mayor precedencia de la regla de permiso. Después de hacer clic en la primera regla, el cuadro de diálogo aparece de la siguiente manera:



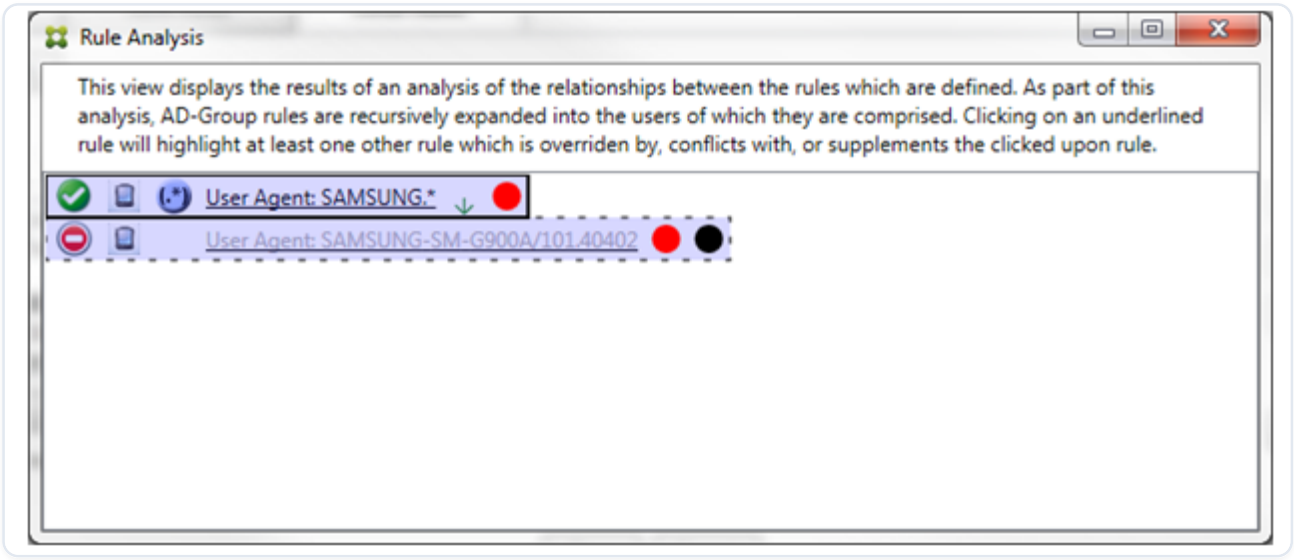
En el escenario anterior, tanto la regla principal (regla de expresión regular `App.*`) como la regla auxiliar (regla de expresión regular `Appl.*`) están resaltadas en amarillo. Esto es simplemente una advertencia visual para alertarle sobre el hecho de que ha aplicado más de una regla de expresión regular a un único campo coincidente, lo que puede significar un problema de redundancia o algo más grave.

En un escenario con conflicto y anulación, tanto la regla principal (regla de expresión regular `App.*`) como la regla auxiliar (regla de expresión regular `Appl.*`) están resaltadas en amarillo. Esto es simplemente una advertencia visual para alertarle sobre el hecho de que ha aplicado más de una regla de expresión regular a un único campo coincidente, lo que puede significar un problema de redundancia o algo más grave.



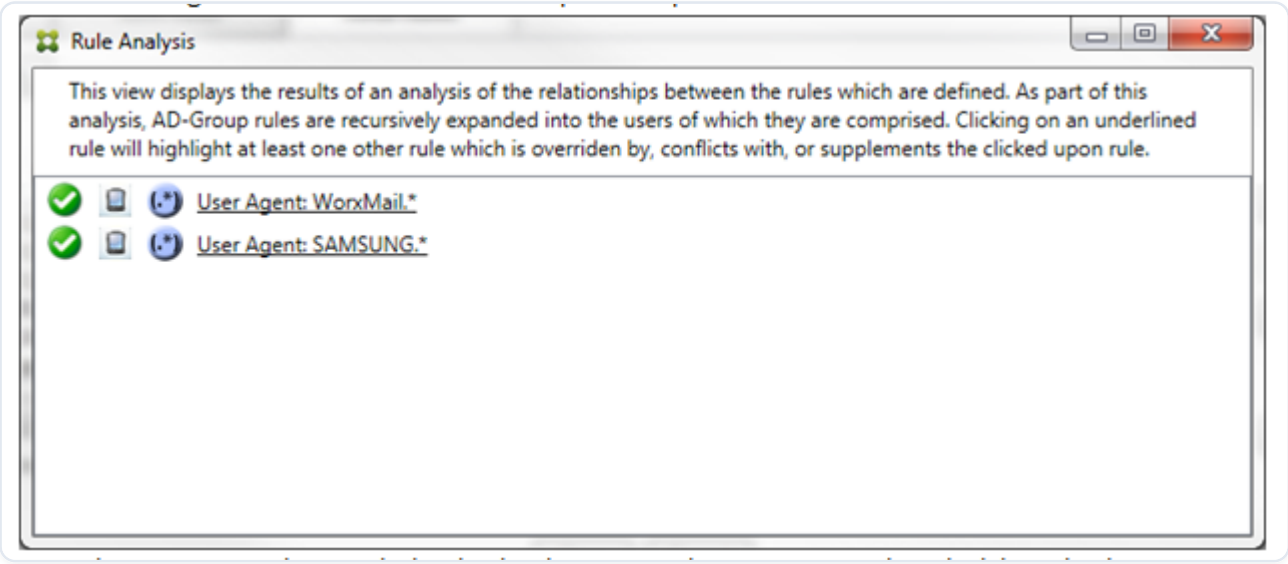
Es fácil ver en el ejemplo anterior que la primera regla (regla de expresión regular `SAMSUNG.*`) no solo anula la siguiente regla (regla normal `SAMSUNG-SM-G900A/101.40402`), sino que las dos reglas difieren en su acceso (la principal especifica Permitir, la auxiliar especifica Bloquear). La segunda regla (regla normal `SAMSUNG-SM-G900A/101.40402`) se muestra en texto más claro para indicar que ha sido anulada y, por lo tanto, está inactiva.

Después de hacer clic en la regla de expresión regular, el cuadro de diálogo aparece de la siguiente manera:

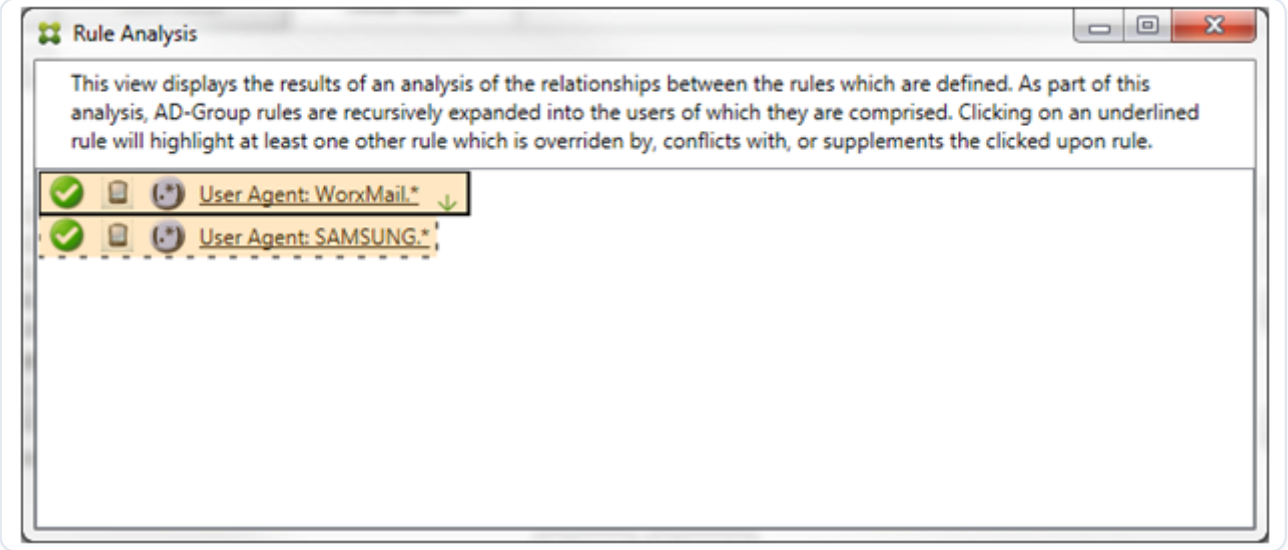


La regla principal (regla de expresión regular `SAMSUNG.*`) va seguida de un punto rojo para indicar que su estado de acceso entra en conflicto con una o varias reglas auxiliares. La regla auxiliar (regla normal `SAMSUNG-SM-G900A/101.40402`) va seguida de un punto rojo para indicar que su estado de acceso entra en conflicto con la regla principal. Esa regla también va seguida de un punto negro para indicar que está anulada y, por lo tanto, inactiva.

Al menos dos reglas estarán subrayadas: la regla principal y la regla o reglas auxiliares. Las reglas que solo se complementan entre sí solo implicarán reglas de expresión regular. Cuando las reglas se complementan entre sí, se indican con una superposición amarilla. Antes de hacer clic en cualquiera de las reglas, en un ejemplo sencillo, el cuadro de diálogo aparece de la siguiente manera:



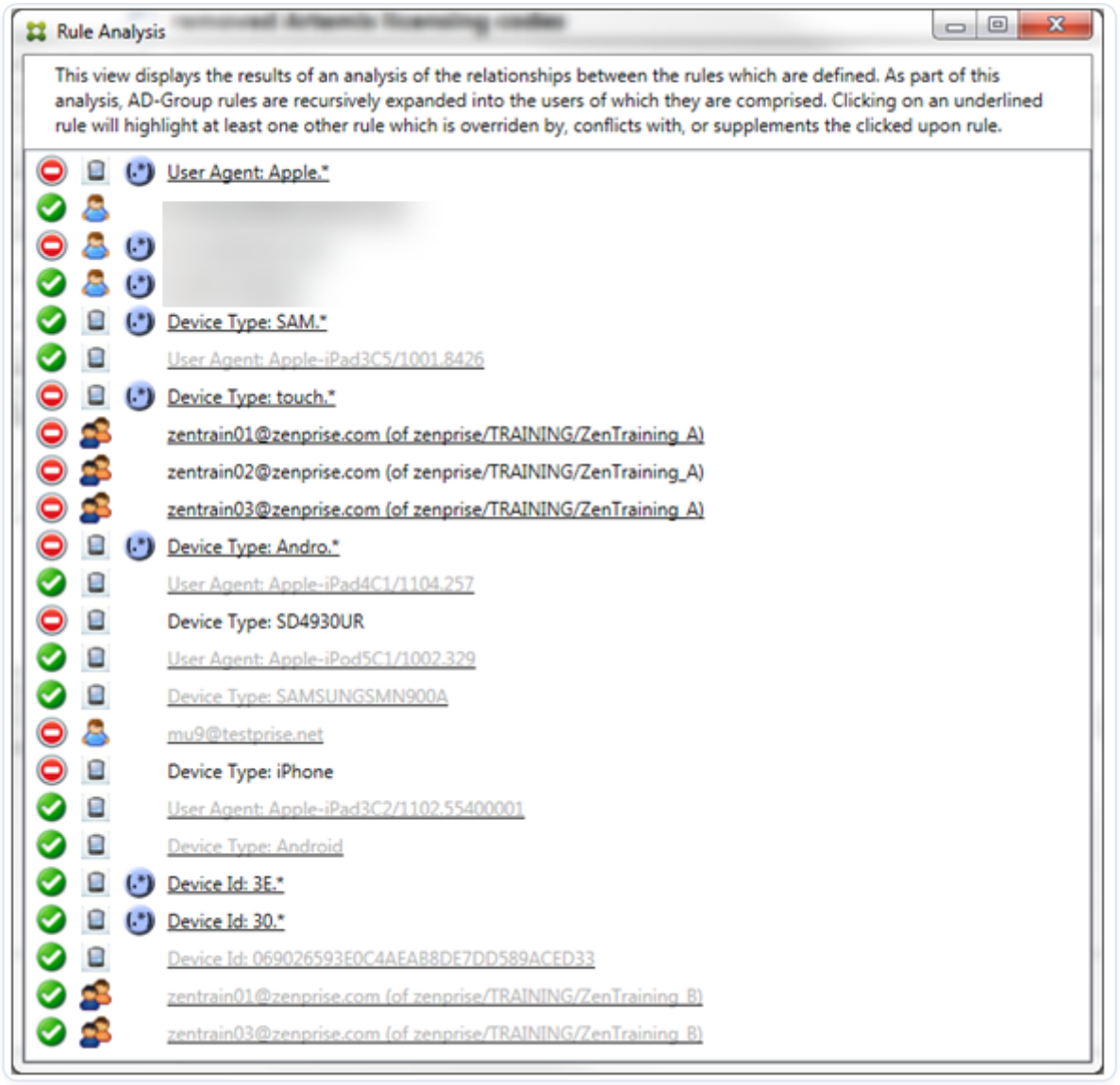
La inspección visual revela fácilmente que ambas son reglas de expresión regular que se han aplicado al campo ID de dispositivo de ActiveSync en el conector de Citrix Endpoint Management para Exchange ActiveSync. Después de hacer clic en la primera regla, el cuadro de diálogo tiene el siguiente aspecto:



La regla principal (regla de expresión regular `WorkMail.*`) se resalta con una superposición amarilla para indicar que existe al menos una regla auxiliar más que es una expresión regular. La regla auxiliar (regla de expresión regular `SAMSUNG.*`) se resalta con una superposición amarilla para indicar que tanto esta como la regla principal son reglas de expresión regular que se aplican al mismo campo dentro del conector para Exchange ActiveSync. En este caso, ese campo es el ID de dispositivo de ActiveSync. Las expresiones regulares pueden o no superponerse. Depende de usted decidir si sus expresiones regulares están correctamente elaboradas.

Ejemplo de una expresión compleja

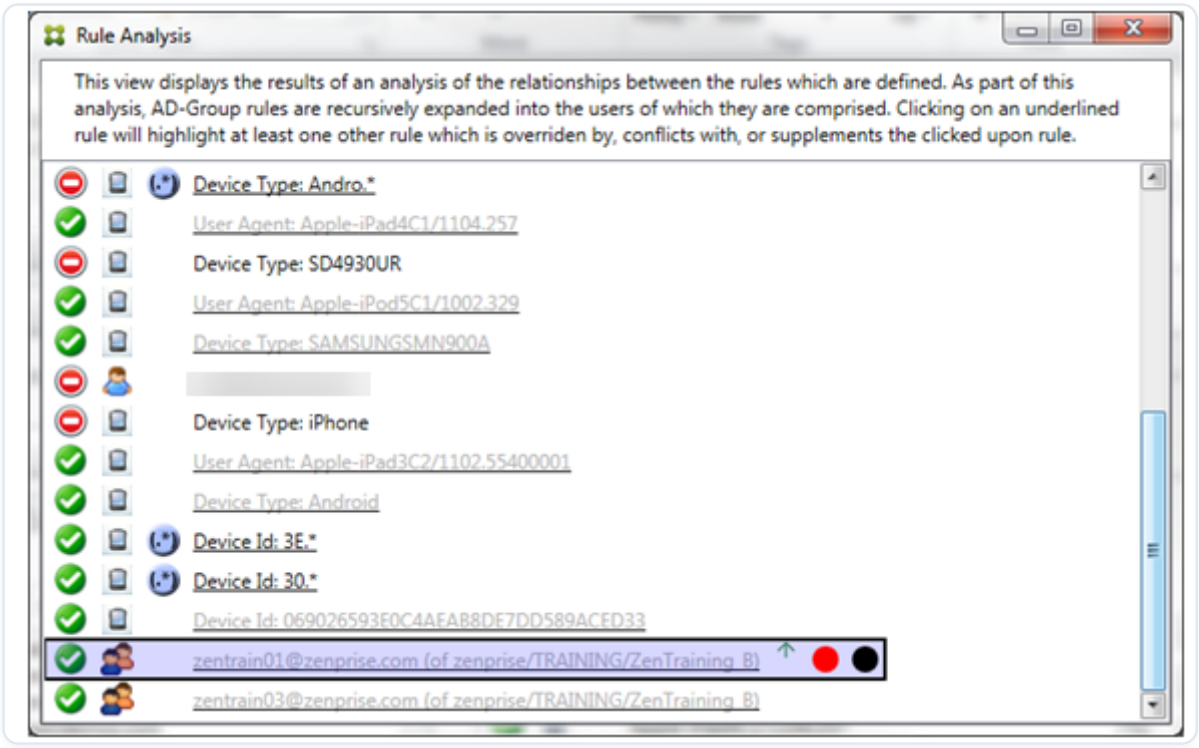
Pueden producirse muchas posibles anulaciones, conflictos o complementos, lo que hace imposible dar un ejemplo de todos los escenarios posibles. El siguiente ejemplo analiza qué no hacer, al mismo tiempo que sirve para ilustrar todo el poder del constructo visual de análisis de reglas. La mayoría de los elementos están subrayados en la siguiente figura. Muchos de los elementos se muestran con una fuente más clara, lo que indica que la regla en cuestión ha sido anulada de alguna manera por una regla de mayor prioridad. También se incluyen varias reglas de expresión regular en la lista, como indica el icono (.*).



Cómo analizar una anulación

Para ver qué regla o reglas han anulado una regla en particular, haga clic en la regla.

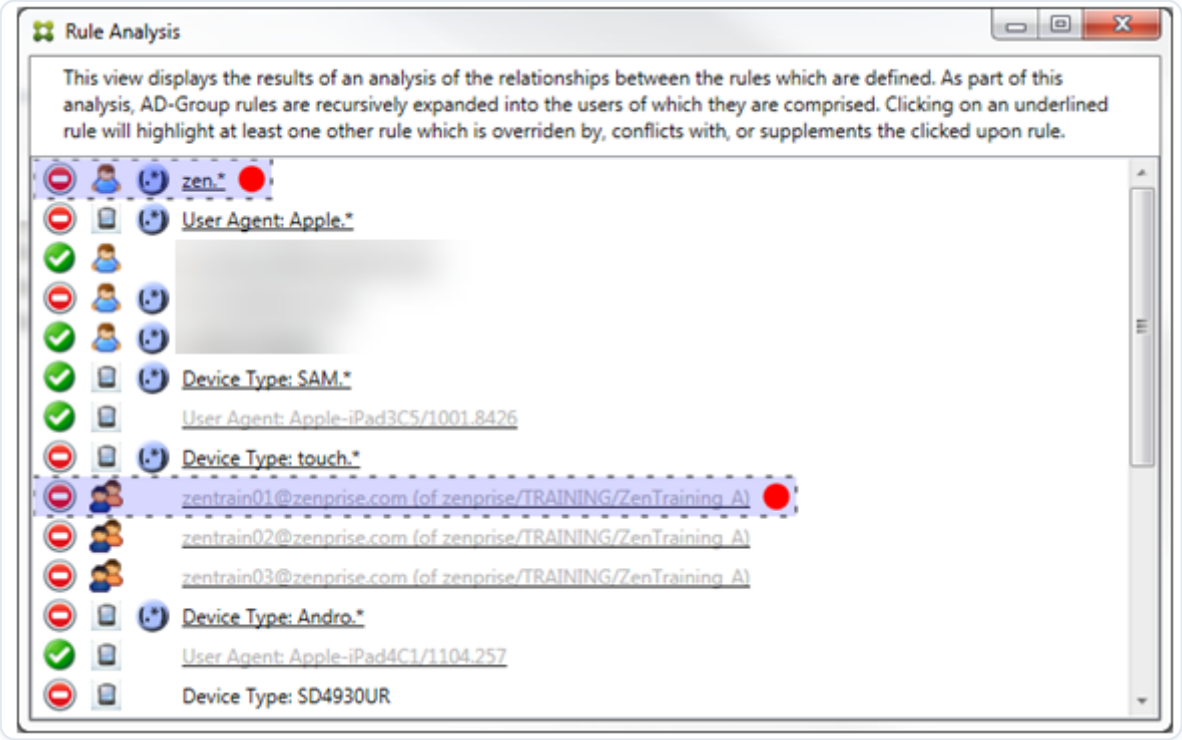
Ejemplo 1: Este ejemplo examina por qué se ha anulado `zentrain01@zenprise.com`.



La regla principal (regla de grupo de AD `zenprise/TRAINING/ZenTraining B`, de la que `zentrain01@zenprise.com` es miembro) tiene las siguientes características:

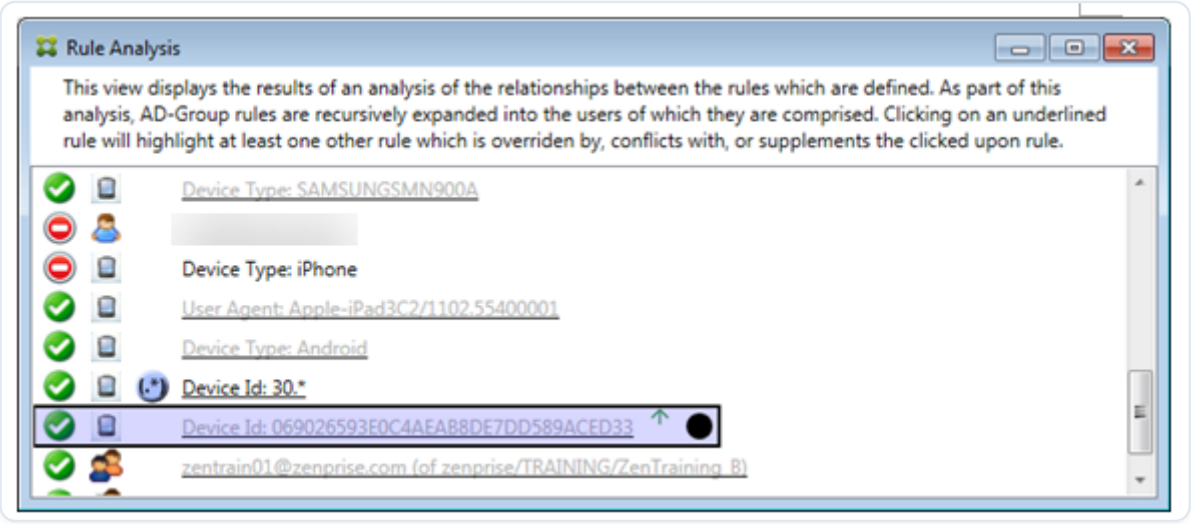
- Está resaltado en azul y tiene un borde sólido.
- Tiene una flecha verde que apunta hacia arriba (para indicar que todas las reglas auxiliares se encuentran encima).
- Le sigue un círculo rojo y un círculo negro para indicar, respectivamente, que una o más reglas auxiliares entran en conflicto con su acceso y que la regla principal ha sido anulada y, por lo tanto, está inactiva.

Al desplazarse hacia arriba, verá lo siguiente:



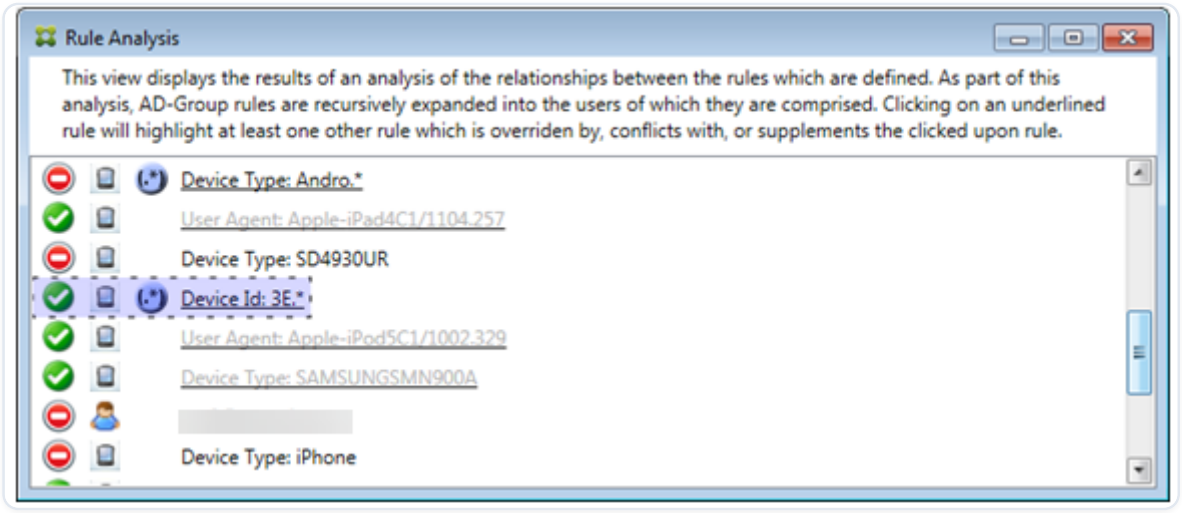
En este caso, hay dos reglas auxiliares que anulan la regla principal: la regla de expresión regular `zen.*` y la regla normal `zentrain01@zenprise.com` (de `zenprise/TRAINING/ZenTraining A`). En el caso de esta última regla auxiliar, lo que ha ocurrido es que la regla de grupo de Active Directory `ZenTraining A` tiene al usuario `zentrain01@zenprise.com`, y la regla de grupo de Active Directory `ZenTraining B` también tiene al usuario `zentrain01@zenprise.com`. Sin embargo, debido a que la regla auxiliar tiene una precedencia mayor que la regla principal, la regla principal ha sido anulada. El acceso de la regla principal es Permitir, y como el acceso de ambas reglas auxiliares es Bloquear, todas van seguidas de un círculo rojo para indicar además un conflicto de acceso.

Ejemplo 2: Este ejemplo muestra por qué se ha anulado el dispositivo con un ID de dispositivo de ActiveSync de `069026593E0C4AEAB8DE7DD589ACED33`:



La regla principal (regla de ID de dispositivo normal `069026593E0C4AEAB8DE7DD589ACED33`) tiene las siguientes características:

- Está resaltado en azul y tiene un borde sólido.
- Tiene una flecha verde que apunta hacia arriba (para indicar que la regla auxiliar se encuentra encima).
- Le sigue un círculo negro para indicar que una regla auxiliar ha anulado la regla principal y, por lo tanto, está inactiva.



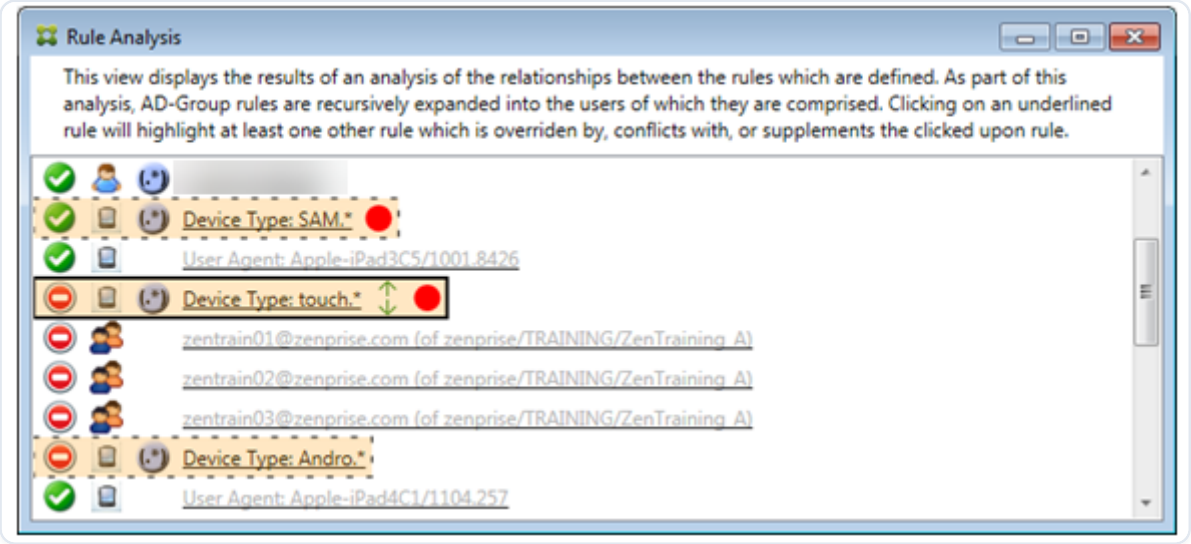
En este caso, una única regla auxiliar anula la regla principal: La regla de ID de dispositivo de ActiveSync de expresión regular es `3E.*`. Dado que la expresión regular `3E.*` coincidiría con `069026593E0C4AEAB8DE7DD589ACED33`, la regla principal nunca se evaluará.

Cómo analizar un suplemento y un conflicto

En este caso, la regla principal es la regla de tipo de dispositivo ActiveSync de expresión regular `touch.*` Las características son las siguientes:

- Se indica con un borde sólido con una superposición amarilla como advertencia de que hay más de una regla de expresión regular que opera contra un campo de regla particular, en este caso el tipo de dispositivo ActiveSync.
- Dos flechas apuntan hacia arriba y hacia abajo respectivamente, lo que indica que hay al menos una regla auxiliar con mayor prioridad y al menos una regla auxiliar con menor prioridad.
- El círculo rojo junto a ella indica que al menos una regla auxiliar tiene su acceso configurado en **Permitir**, lo que entra en conflicto con el acceso de la regla principal de **Bloquear**.
- Hay dos reglas auxiliares: la regla de tipo de dispositivo ActiveSync de expresión regular `SAM.*` y la regla de tipo de dispositivo ActiveSync de expresión regular `Andro.*`.

- Ambas reglas auxiliares están bordeadas con guiones para indicar que son auxiliares.
- Ambas reglas auxiliares están superpuestas con amarillo para indicar que también se aplican al campo de regla del tipo de dispositivo ActiveSync.
- Debe asegurarse en tales escenarios de que sus reglas de expresión regular no sean redundantes.



Cómo analizar más a fondo las reglas

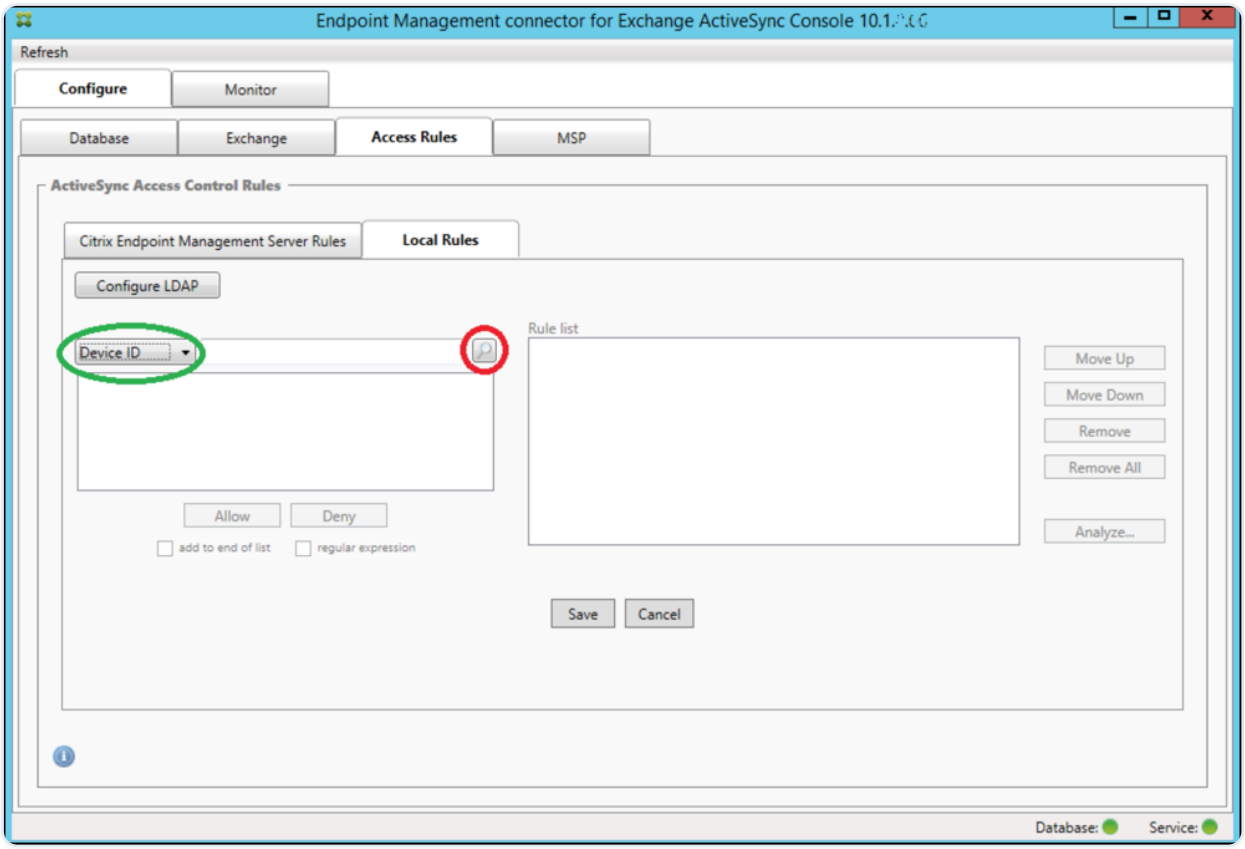
Este ejemplo explora cómo las relaciones de reglas siempre se ven desde la perspectiva de la regla principal. El ejemplo anterior mostró cómo al hacer clic en la regla de expresión regular aplicada al campo de regla de tipo de dispositivo con un valor de `touch.*`. Al hacer clic en la regla auxiliar `Andro.*`, se muestra un conjunto diferente de reglas auxiliares resaltadas.



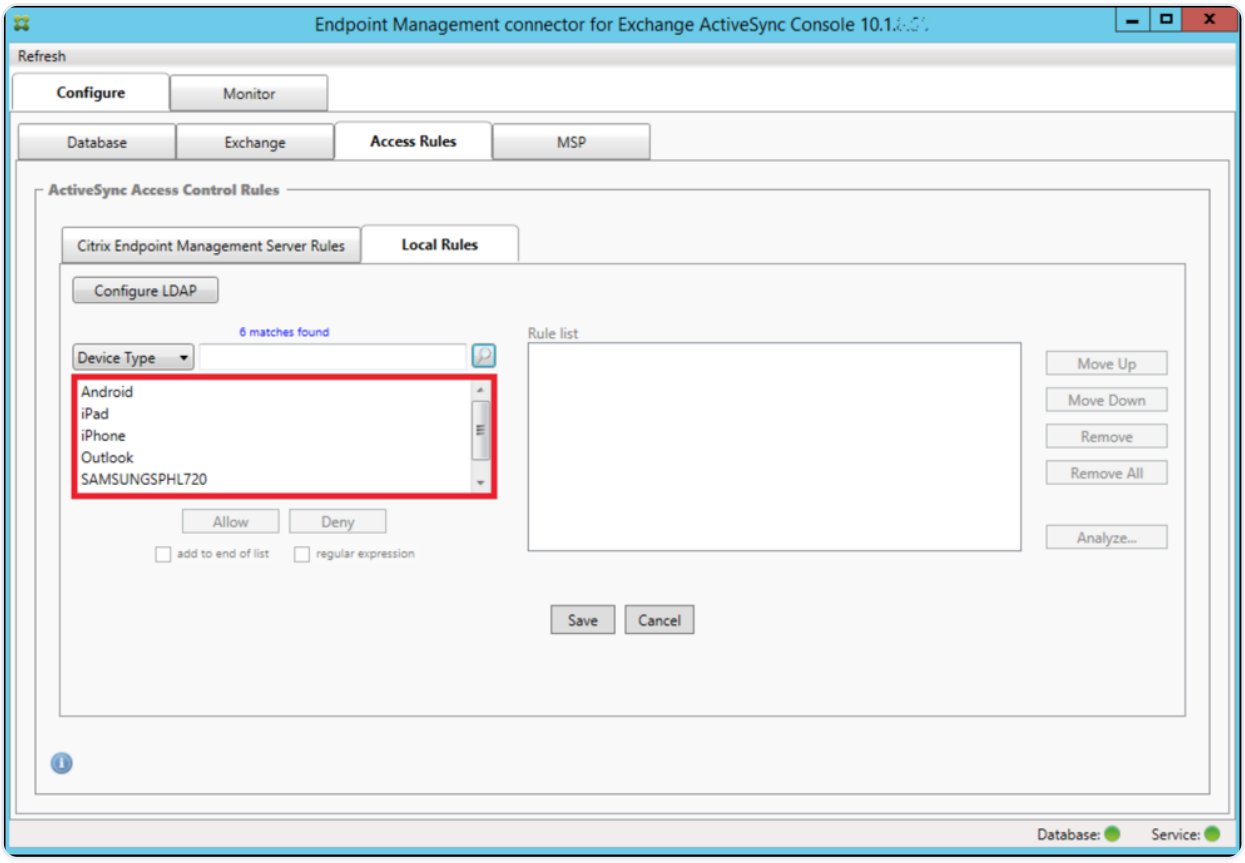
El ejemplo muestra una regla anulada que se incluye en la relación de reglas. Esta regla es la regla normal de tipo de dispositivo ActiveSync `Android`, que está anulada (indicado por la fuente más clara y el círculo negro junto a ella) y también entra en conflicto en su acceso con la regla principal de tipo de dispositivo ActiveSync de expresión regular `Andro.*`. Esa regla era anteriormente una regla auxiliar antes de hacer clic en ella. En el ejemplo anterior, la regla normal de tipo de dispositivo ActiveSync `Android` no se mostraba como una regla auxiliar porque, desde la perspectiva de la regla principal de entonces (la regla de tipo de dispositivo ActiveSync de expresión regular `touch.*`), no estaba relacionada con ella.

Para configurar una regla local de expresión normal

1. Haga clic en la pestaña **Reglas de acceso**.



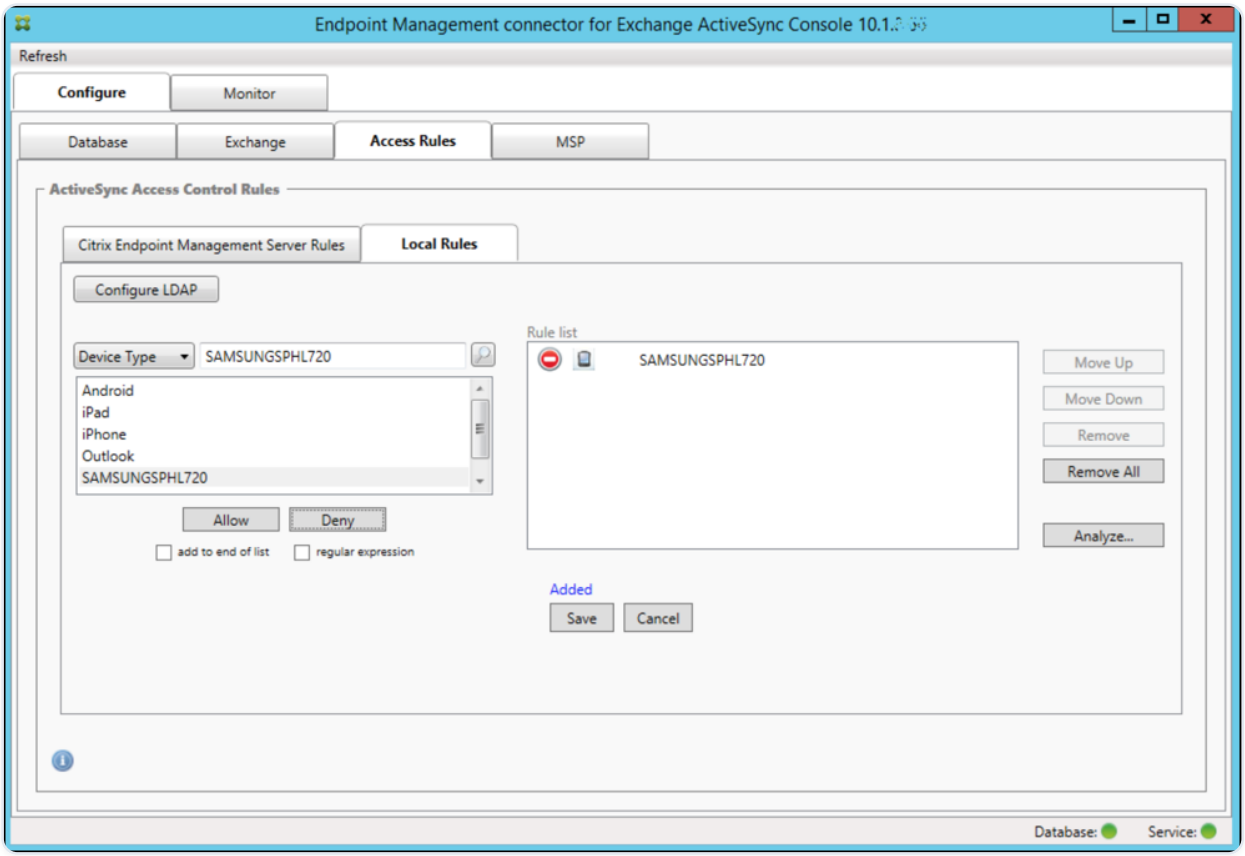
2. En la lista **ID de dispositivo**, seleccione el campo para el que desea crear una regla local.
3. Haga clic en el icono de la lupa para mostrar todas las coincidencias únicas para el campo elegido. En este ejemplo, se ha elegido el campo **Tipo de dispositivo** y las opciones se muestran en el siguiente cuadro de lista:



4. Haga clic en uno de los elementos del cuadro de lista de resultados y, a continuación, haga clic en una de las siguientes opciones:

   - **Permitir** significa que Exchange se configurará para permitir el tráfico de ActiveSync para todos los dispositivos coincidentes.
   - **Denegar** significa que Exchange se configurará para denegar el tráfico de ActiveSync para todos los dispositivos coincidentes.

   En este ejemplo, se deniega el acceso a todos los dispositivos que tienen un tipo de dispositivo SamsungSPhl720.

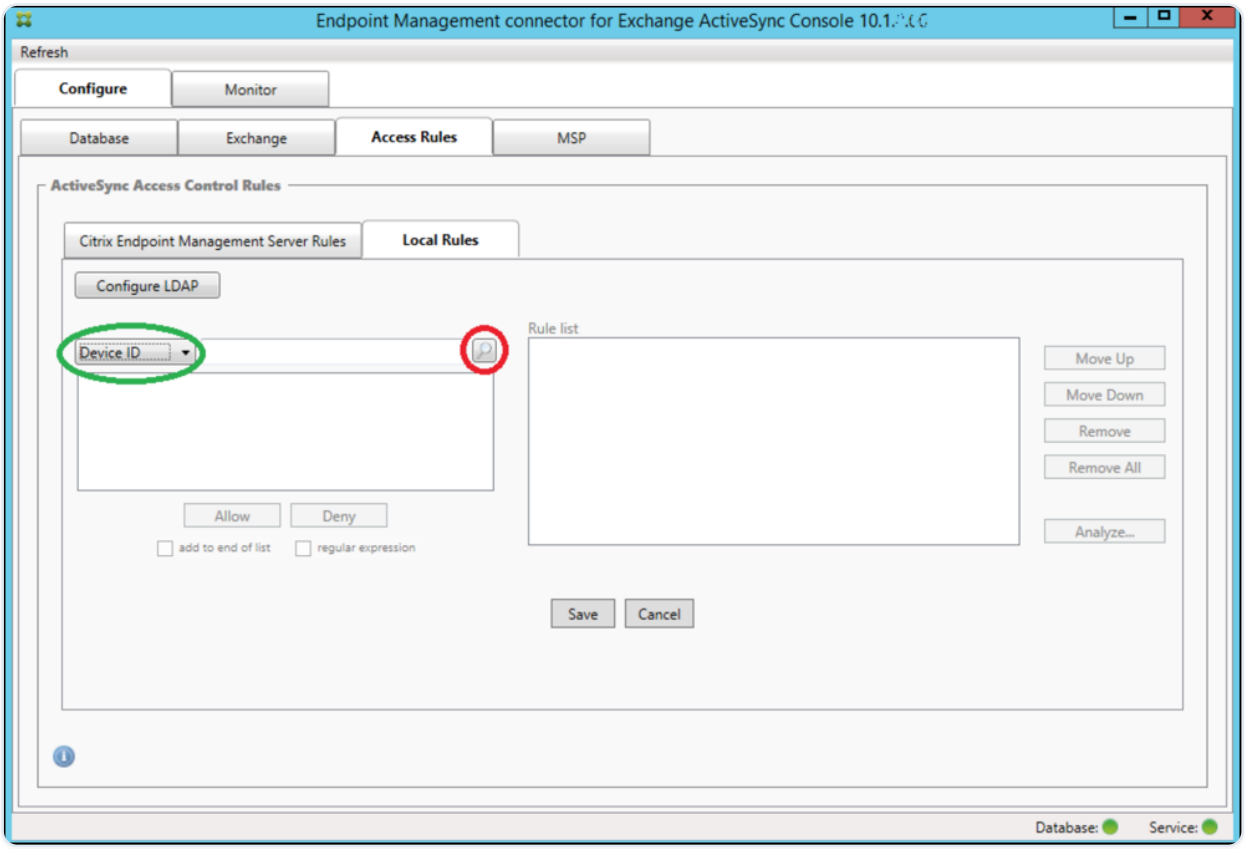


Para agregar una expresión regular

Las reglas locales de expresiones regulares se pueden distinguir por el icono que aparece junto a ellas -  . Para agregar una regla de expresión regular, puede crear una regla de expresión regular a partir de un valor existente de la lista de resultados para un campo determinado (siempre que se haya completado una instantánea principal), o simplemente puede escribir la expresión regular que desee.

Para crear una expresión regular a partir de un valor de campo existente

1. Haga clic en la pestaña **Reglas de acceso**.



2. En la lista **ID de dispositivo**, seleccione el campo para el que desea crear una regla local de expresión regular.
3. Haga clic en el icono de la lupa para mostrar todas las coincidencias únicas del campo elegido. En este ejemplo, se ha elegido el campo **Tipo de dispositivo** y las opciones se muestran en el siguiente cuadro de lista:

   Opciones de tipo de dispositivo(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-magnifier.png)
4. Haga clic en uno de los elementos de la lista de resultados. En este ejemplo, se ha seleccionado **SAMSUNGSPHL720** y aparece en el cuadro de texto junto a **Tipo de dispositivo**.

   Análisis de reglas(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-localrules-samsung-regex.png)
5. Para permitir todos los tipos de dispositivos que contengan "Samsung" en el valor de su tipo de dispositivo, agregue una regla de expresión regular siguiendo estos pasos:

   a. Haga clic dentro del cuadro de texto del elemento seleccionado.
   b. Cambie el texto de **SAMSUNGSPHL720** a **SAMSUNG.***.
   c. Asegúrese de que la casilla de verificación de expresión regular esté seleccionada.

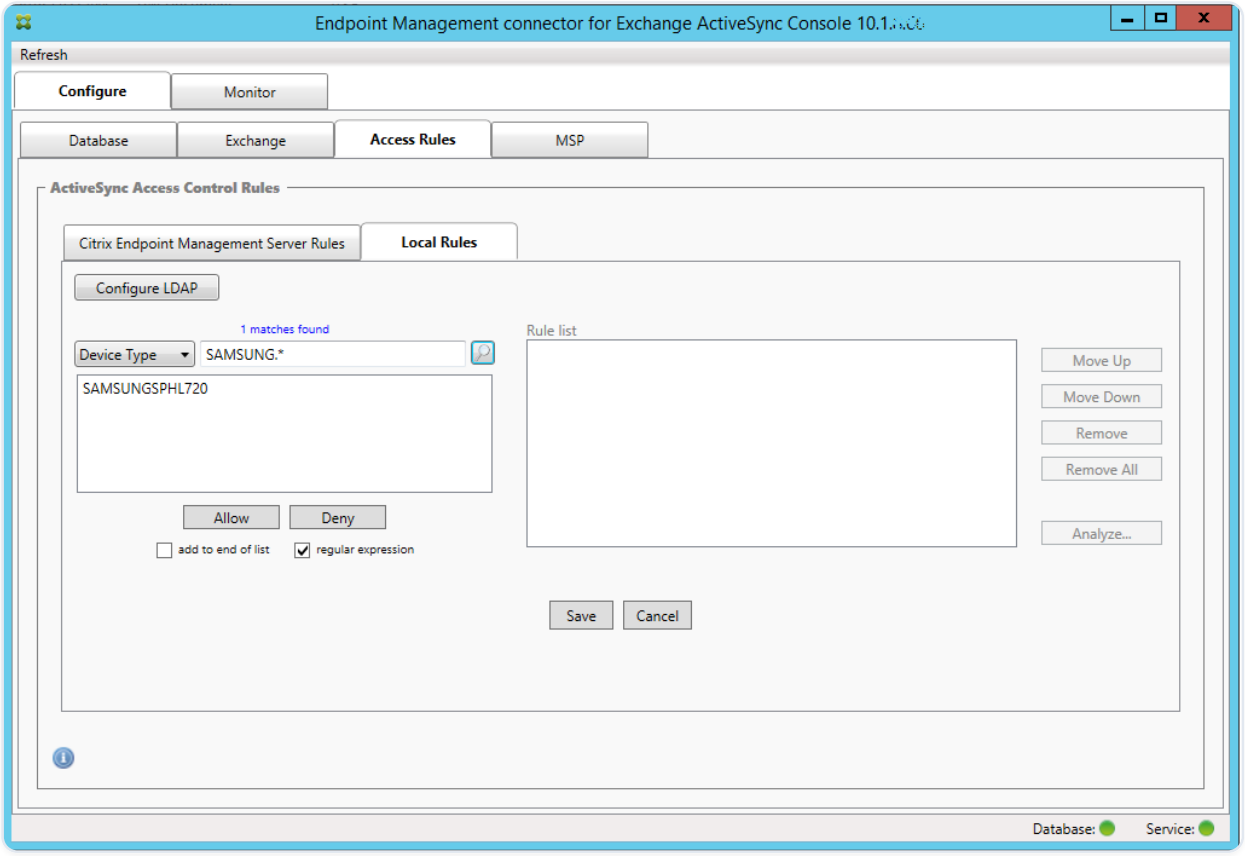
d. Haga clic en **Permitir**.

Mensaje de permitir(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-accessrules-allow-samsung.png)

Para crear una regla de acceso

1. Haga clic en la ficha **Reglas locales**.
2. Para introducir la expresión regular, debe utilizar tanto la lista de ID de dispositivo como el cuadro de texto del elemento seleccionado.

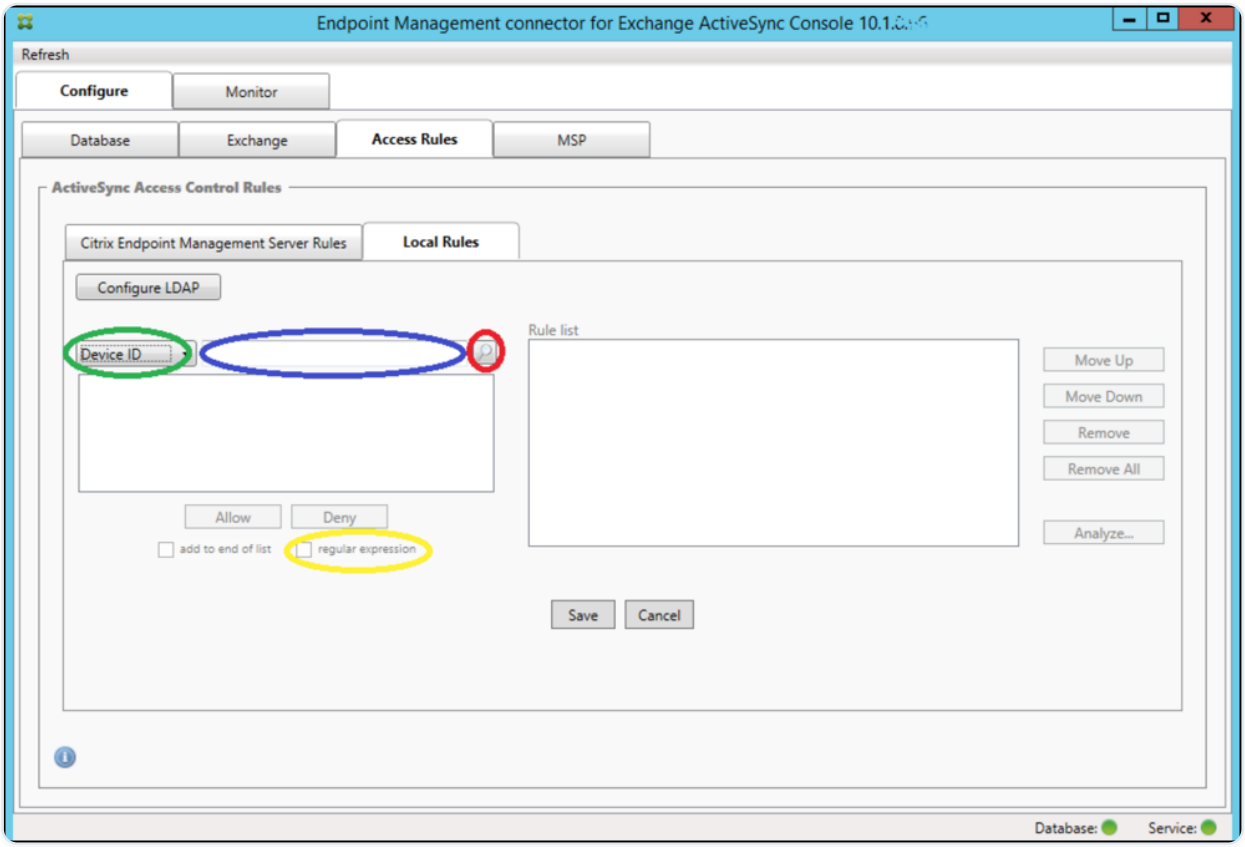
   Regla de acceso(/en-us/citrix-endpoint-management/media/connector-exchangeactivesync-local-rule.png)
3. Seleccione el campo con el que desea establecer la coincidencia. En este ejemplo, se utiliza **Tipo de dispositivo**.
4. Escriba la expresión regular. Este ejemplo utiliza `samsung.*`.
5. Asegúrese de que la casilla de verificación de expresión regular esté seleccionada y, a continuación, haga clic en **Permitir** o **Denegar**. En este ejemplo, la opción se establece como **Permitir**. El resultado final es el siguiente:



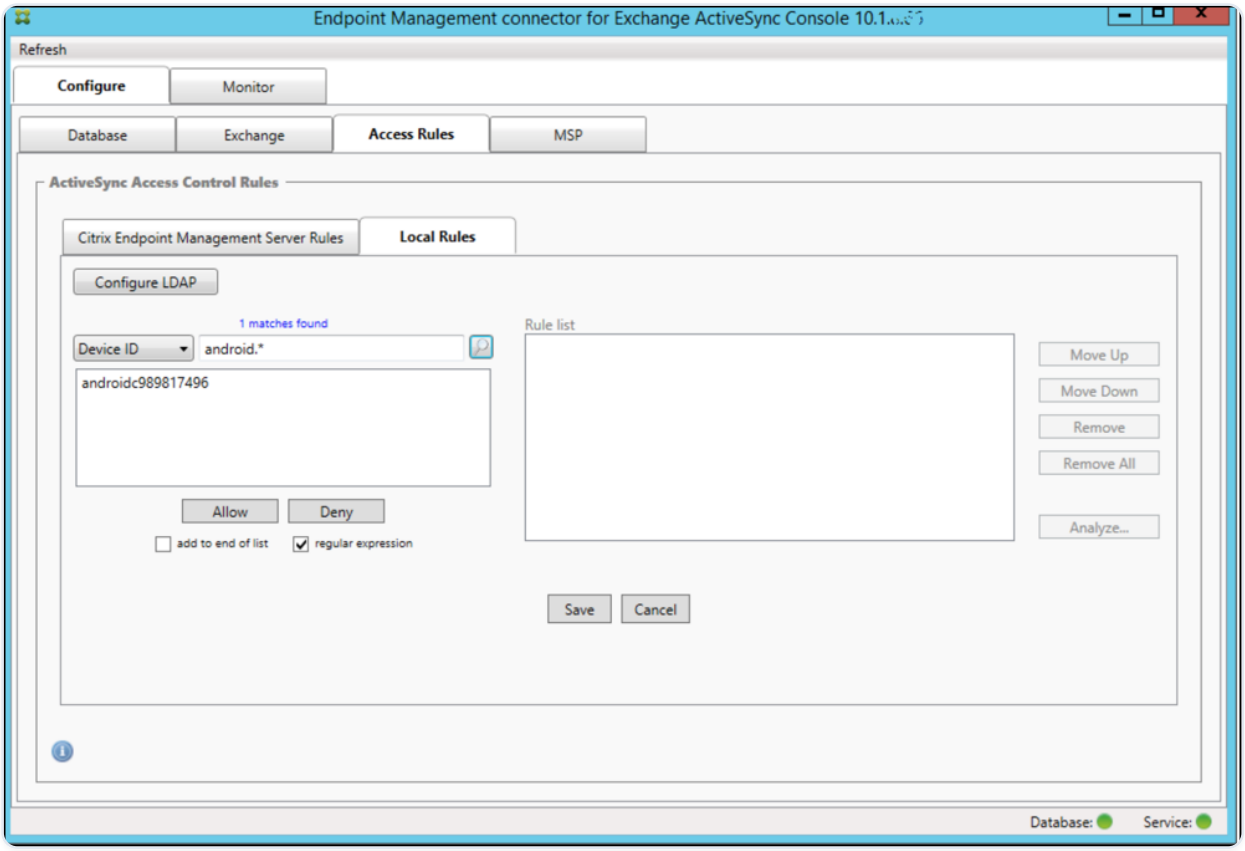
Para buscar dispositivos

Al seleccionar la casilla de verificación de expresión regular, puede realizar búsquedas de dispositivos específicos que coincidan con la expresión dada. Esta función solo está disponible si se ha completado correctamente una instantánea principal. Puede usar esta función incluso si no hay planes de usar reglas de expresión regular. Por ejemplo, suponga que desea encontrar todos los dispositivos que tienen el texto `workmail` en su ID de dispositivo de ActiveSync. Para ello, siga este procedimiento.

1. Haga clic en la ficha **Reglas de acceso**.
2. Asegúrese de que el selector de campo de coincidencia de dispositivo esté establecido en ID de dispositivo (el valor predeterminado).



3. Haga clic dentro del cuadro de texto del elemento seleccionado (como se muestra en azul en la figura anterior) y, a continuación, escriba `workmail.*`.
4. Asegúrese de que la casilla de verificación de expresión regular esté seleccionada y, a continuación, haga clic en el icono de la lupa para mostrar las coincidencias como se muestra en la siguiente figura.

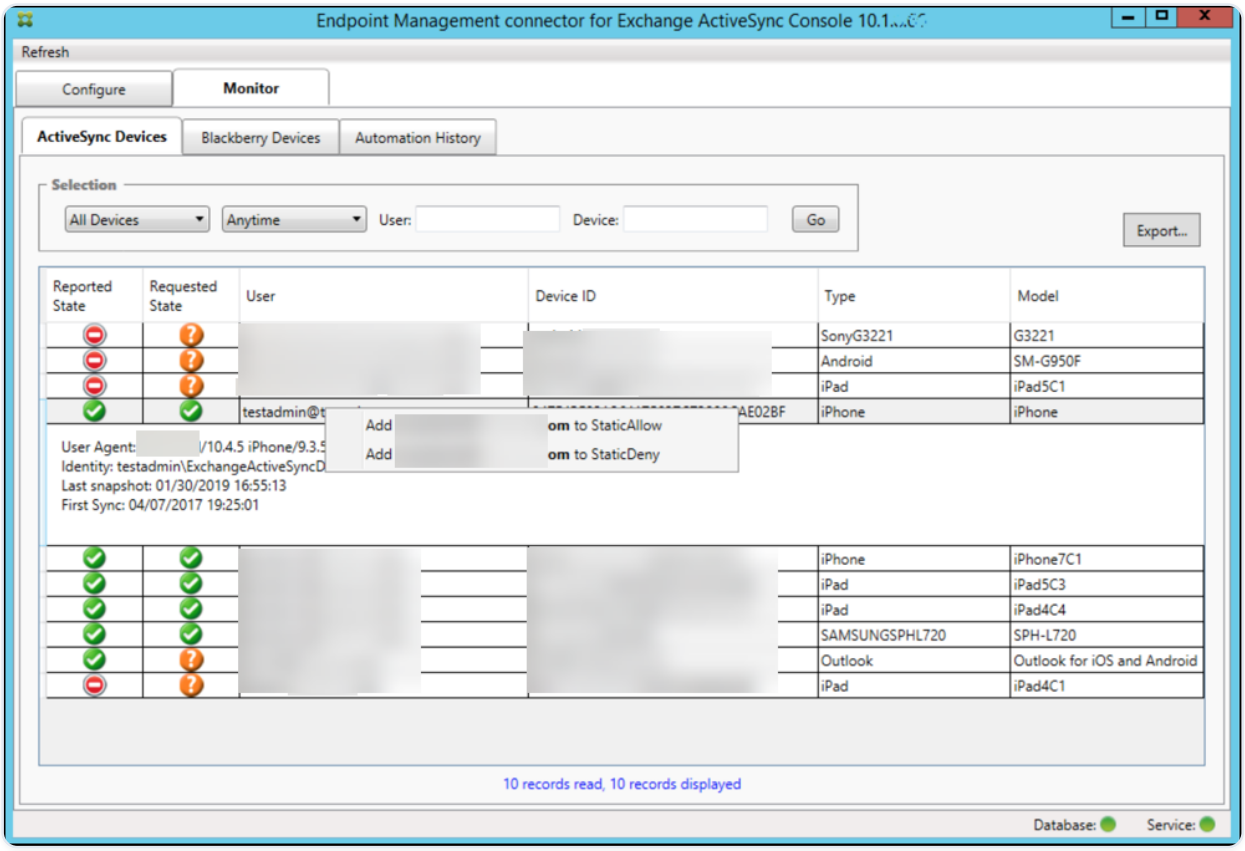


Para agregar un usuario individual, dispositivo o tipo de dispositivo a una regla estática

Puede agregar reglas estáticas basadas en el usuario, el ID del dispositivo o el tipo de dispositivo en la ficha **Dispositivos ActiveSync**.

1. Haga clic en la ficha **Dispositivos ActiveSync**.
2. En la lista, haga clic con el botón derecho en un usuario, dispositivo o tipo de dispositivo y seleccione si desea permitir o denegar su selección.

   La siguiente imagen muestra la opción Permitir/Denegar cuando se selecciona user1.



Supervisión de dispositivos

La pestaña **Monitor** del conector de Citrix Endpoint Management para Exchange ActiveSync le permite examinar los dispositivos Exchange ActiveSync y BlackBerry que se han detectado y el historial de comandos automatizados de PowerShell que se han emitido. La pestaña **Monitor** tiene las tres pestañas siguientes:

- **Dispositivos ActiveSync:**
  - Puede exportar las asociaciones de dispositivos ActiveSync mostradas haciendo clic en el botón **Exportar**.
  - Puede agregar reglas locales (estáticas) haciendo clic con el botón derecho en las columnas **Usuario**, **ID de dispositivo** o **Tipo** y seleccionando el tipo de regla de permitir o bloquear adecuado.
  - Para contraer una fila expandida, haga Ctrl+clic en la fila expandida.
- **Dispositivos BlackBerry**
- **Historial de automatización**

La pestaña **Configurar** muestra el historial de todas las instantáneas. El historial de instantáneas muestra cuándo se realizó la instantánea, cuánto tiempo tardó, cuántos dispositivos se detectaron y los errores que se produjeron:

- En la pestaña **Exchange**, haga clic en el icono de información del servidor Exchange deseado.

Solución de problemas y diagnósticos

El conector de Citrix Endpoint Management para Exchange ActiveSync registra errores y otra información operativa en su archivo de registro: *Carpeta de instalación*\log\XmmWindowsService.log. El conector para Exchange ActiveSync también registra eventos importantes en el registro de eventos de Windows.

Para cambiar el nivel de registro

El conector de Citrix Endpoint Management para Exchange ActiveSync incluye los siguientes niveles de registro: Error, Info, Warn, Debug y Trace.

> **Nota:**
>
> Cada nivel sucesivo genera más detalles (más datos). Por ejemplo, el nivel Error proporciona el menor detalle, pero el nivel Trace proporciona el mayor detalle.

Para cambiar el nivel de registro, haga lo siguiente:

1. En el conector de Citrix Endpoint Management `C:\Program Files\Citrix\Citrix`, abra el archivo nlog.config.
2. En la sección `<rules>`, cambie el parámetro *minilevel* al nivel de registro que prefiera. Por ejemplo:

```
<rules >


<logger name="*" writeTo="file" minlevel="Debug" />


</rules>
```

3. Guarde el archivo.

   Los cambios surten efecto inmediatamente. No es necesario reiniciar el conector para Exchange ActiveSync.

Errores comunes

La siguiente lista incluye errores comunes:

- El conector para el servicio Exchange ActiveSync no se inicia

  Compruebe el archivo de registro y el registro de eventos de Windows para ver si hay errores. Las causas típicas son las siguientes:

  - El conector para el servicio Exchange ActiveSync no puede acceder a SQL Server. Esto puede deberse a los siguientes problemas:
    - El servicio SQL Server no se está ejecutando.
    - Error de autenticación.

    Si la autenticación integrada de Windows está configurada, la cuenta de usuario del conector para el servicio Exchange ActiveSync debe ser un inicio de sesión SQL permitido. La cuenta del conector para el servicio Exchange ActiveSync tiene como valor predeterminado Sistema local, pero se puede cambiar a cualquier cuenta que tenga privilegios de administrador local. Si la autenticación SQL está configurada, el inicio de sesión SQL debe configurarse correctamente en SQL.

Herramientas de solución de problemas

Hay un conjunto de utilidades de PowerShell para la solución de problemas disponible en la carpeta **Support\PowerShell**.

Una herramienta de solución de problemas realiza un análisis en profundidad de los buzones de correo y los dispositivos de los usuarios, detectando condiciones de error y posibles áreas de fallo, y un análisis RBAC en profundidad de los usuarios. Puede guardar una salida sin procesar de todos los cmdlets en un archivo de texto.

Conector de NetScaler Gateway para Exchange ActiveSync

XenMobile NetScaler Connector es ahora el conector de NetScaler Gateway para Exchange ActiveSync. Para obtener más detalles sobre la cartera unificada de Citrix, consulte la guía de productos de Citrix.

El conector para Exchange ActiveSync proporciona un servicio de autorización a nivel de dispositivo de los clientes de ActiveSync a NetScaler Gateway, que actúa como proxy inverso para el protocolo Exchange ActiveSync. Usted controla la autorización mediante una combinación de:

- Directivas que defina en Citrix Endpoint Management
- Reglas definidas localmente por el conector de NetScaler Gateway para Exchange ActiveSync

Para obtener más información, consulte ActiveSync Gateway.

Para ver un diagrama de arquitectura de referencia detallado, consulte Arquitectura.

La versión actual del conector de NetScaler Gateway para Exchange ActiveSync es la versión 8.5.3.

Para descargar el conector:

1. Vaya a `<https://www.citrix.com/downloads>`.
2. Vaya a **Citrix Endpoint Management (y Citrix XenMobile Server) > XenMobile Server (local) > Product Software > XenMobile Server 10 > Server Components**.
3. En el mosaico **NetScaler Gateway Connector**, haga clic en **Download File**.

Para instalar el conector, consulte Instalación del conector de NetScaler Gateway para Exchange ActiveSync).

> **Importante:**

> A partir de octubre de 2022, los conectores de Citrix Endpoint Management y NetScaler Gateway para Exchange ActiveSync dejarán de ser compatibles con Exchange Online, dados los cambios de autenticación anunciados por Microsoft aquí. El conector de Citrix Endpoint Management para Exchange sigue funcionando con Microsoft Exchange Server (local).

Novedades de la versión 8.5.3

- Esta versión añade compatibilidad con los protocolos ActiveSync 16.0 y 16.1.
- Se han añadido más detalles a los análisis enviados a Google Analytics, especialmente en lo que respecta a las instantáneas.

Novedades de versiones anteriores

> **Nota:**

> La siguiente sección de Novedades se refiere al conector de NetScaler Gateway para Exchange ActiveSync por su antiguo nombre, XenMobile NetScaler Connector. El nombre cambió a partir de la versión 8.5.2.

Novedades de la versión 8.5.2

- XenMobile NetScaler Connector ahora es el conector de NetScaler Gateway para Exchange ActiveSync.

Los siguientes problemas se han corregido en esta versión:

- Si se utiliza más de un criterio para definir una regla de directiva y si un criterio implica el ID de usuario, puede ocurrir el siguiente problema: Si un usuario tiene más alias, los alias tampoco se comprueban al aplicar la regla.

Novedades de la versión 8.5.1.11

- **Cambio en los requisitos del sistema:** La versión actual de NetScaler Connector requiere Microsoft .NET Framework 4.5.
- **Compatibilidad con Google Analytics:** Queremos saber cómo utiliza el conector para poder centrarnos en cómo mejorar el producto.
- **Compatibilidad con TLS 1.1 y 1.2:** Debido al debilitamiento de su seguridad, el Consejo PCI está desaprobando TLS 1.0 y TLS 1.1. Se ha añadido compatibilidad con TLS 1.2 al XenMobile NetScaler Connector.

Supervisión del conector de NetScaler Gateway para Exchange ActiveSync

La utilidad de configuración del conector de NetScaler Gateway para Exchange ActiveSync proporciona un registro detallado. Utilice los registros para ver todo el tráfico que pasa por su servidor Exchange que Secure Mobile Gateway permite o bloquea.

Utilice la pestaña **Registro** para ver el historial de las solicitudes de ActiveSync reenviadas al conector para Exchange ActiveSync para su autorización.

Además, para asegurarse de que el servicio web del conector para Exchange ActiveSync se está ejecutando, cargue la siguiente URL en un explorador en el servidor del conector `https://<host:port>/services/ActiveSync/Version`. Si la URL devuelve la versión del producto como una cadena, el servicio web responde.

Para simular el tráfico de ActiveSync con el conector para Exchange ActiveSync

Puede usar el conector de NetScaler Gateway para Exchange ActiveSync para simular el tráfico de ActiveSync con sus directivas. En la utilidad de configuración del conector, haga clic en la pestaña **Simulador**. Los resultados muestran cómo se aplican sus directivas según las reglas que haya configurado.

Elegir filtros para el conector para Exchange ActiveSync

Los filtros del conector de NetScaler Gateway para Exchange ActiveSync funcionan analizando un dispositivo en busca de una infracción de directiva o una configuración de propiedad determinadas. Si el dispositivo cumple los criterios, se coloca en una Lista de dispositivos. Esta Lista de dispositivos no es una lista de permitidos ni una lista de bloqueados. Es una lista de dispositivos que cumplen los criterios definidos. Los siguientes filtros están disponibles para el conector para Exchange ActiveSync en Citrix Endpoint Management. Las dos opciones para cada filtro son **Permitir** o **Denegar**.

- **Dispositivos anónimos:** Permite o deniega dispositivos inscritos en Citrix Endpoint Management, pero cuya identidad de usuario es desconocida. Por ejemplo, un usuario inscrito tiene una identidad desconocida si tiene una contraseña de Active Directory caducada o credenciales desconocidas.
- **Aplicaciones prohibidas:** Permite o deniega dispositivos en función de la Lista de dispositivos definida por las listas de bloqueados en las directivas y la presencia de aplicaciones en una lista de bloqueados.
- **Permitir/Denegar implícito:** Crea una Lista de dispositivos de todos los dispositivos que no cumplen ninguno de los demás criterios de reglas de filtro y permite o deniega en función de esa lista. La opción Permitir/Denegar implícito garantiza que el estado del conector para Exchange ActiveSync en la pestaña Dispositivos esté habilitado y muestre el estado del conector para sus dispositivos. La opción Permitir/Denegar implícito también controla todos los demás filtros del conector que no están seleccionados. Por ejemplo, el conector deniega las aplicaciones de la lista de bloqueados. Sin embargo, el conector permite todos los demás filtros porque la opción Permitir/Denegar implícito está establecida en **Permitir**.
- **Dispositivos inactivos:** Crea una Lista de dispositivos de los dispositivos que no se han comunicado con Citrix Endpoint Management en un tiempo especificado. Estos dispositivos se consideran inactivos. El filtro permite o deniega los dispositivos en consecuencia.
- **Aplicaciones obligatorias que faltan:** Cuando un usuario se inscribe, recibe una lista de aplicaciones obligatorias que deben instalarse. El filtro de aplicaciones obligatorias que faltan

indica que una o varias de las aplicaciones ya no están presentes; por ejemplo, el usuario eliminó una o varias aplicaciones.

- **Aplicaciones no sugeridas:** Cuando un usuario se inscribe, recibe una lista de las aplicaciones que debe instalar. El filtro de aplicaciones no sugeridas comprueba el dispositivo en busca de aplicaciones que no estén en esa lista.
- **Contraseña no conforme:** Crea una Lista de dispositivos de todos los dispositivos que no tienen un código de acceso en el dispositivo.
- **Dispositivos no conformes:** Le permite denegar o permitir dispositivos que cumplen sus propios criterios internos de cumplimiento de TI. El cumplimiento es una configuración arbitraria definida por la propiedad del dispositivo denominada No conforme, que es un indicador booleano que puede ser **Verdadero** o **Falso**. (Puede crear esta propiedad manualmente y establecer el valor. O puede usar acciones automatizadas para crear esta propiedad en un dispositivo, según si el dispositivo cumple criterios específicos.)
  - **Fuera de cumplimiento = Verdadero:** Si un dispositivo no cumple con los estándares de cumplimiento y las definiciones de directivas establecidas por su departamento de TI, el dispositivo está fuera de cumplimiento.
  - **Fuera de cumplimiento = Falso:** Si un dispositivo cumple con los estándares de cumplimiento y las definiciones de directivas establecidas por su departamento de TI, el dispositivo cumple.
- **Estado revocado:** Crea una lista de dispositivos de todos los dispositivos revocados y permite o deniega según el estado revocado.
- **Dispositivos Android rooteados/iOS con jailbreak:** Crea una lista de dispositivos de todos los dispositivos marcados como rooteados y permite o deniega según el estado de rooteo.
- **Dispositivos no administrados:** Crea una lista de dispositivos de todos los dispositivos en la base de datos de Citrix Endpoint Management. Implemente Mobile Application Gateway en modo de bloqueo.

Para configurar una conexión al conector de NetScaler Gateway para Exchange ActiveSync

El conector de NetScaler Gateway para Exchange ActiveSync se comunica con Citrix Endpoint Management y otros proveedores de configuración remota a través de los servicios web seguros de Citrix.

1. En la utilidad de configuración del conector para Exchange ActiveSync, haga clic en la ficha **Proveedores de configuración** y, a continuación, haga clic en **Agregar**.

2. En el cuadro de diálogo **Proveedores de configuración**, en **Nombre**, introduzca un nombre de usuario que tenga privilegios administrativos y que se utilice para la autorización HTTP básica con el servidor de Citrix Endpoint Management.
3. En **URL**, introduzca la dirección web del GCS de Citrix Endpoint Management, normalmente en el formato `https://<FQDN>/<instanceName>/services/<MagConfigService>`. El nombre *MagConfigService* distingue entre mayúsculas y minúsculas.
4. En **Contraseña**, introduzca la contraseña que se utilizará para la autorización HTTP básica con el servidor de Citrix Endpoint Management.
5. En **Host de administración**, introduzca el nombre del servidor del conector para Exchange ActiveSync.
6. En **Intervalo de línea base**, especifique un período de tiempo para cuándo extraer un nuevo conjunto de reglas dinámicas actualizado de Citrix Endpoint Management.
7. En **Intervalo delta**, especifique un período de tiempo para cuándo extraer una actualización de las reglas dinámicas.
8. En **Tiempo de espera de solicitud**, especifique el intervalo de tiempo de espera de la solicitud del servidor.
9. En **Config Provider**, seleccione si la instancia del servidor del proveedor de configuración está proporcionando la configuración de la directiva.
10. En **Events Enabled**, habilite esta opción si desea que el conector para Exchange ActiveSync notifique a Citrix Endpoint Management cuando se bloquee un dispositivo. Esta opción es necesaria si utiliza las reglas del conector en cualquiera de sus acciones automatizadas de Citrix Endpoint Management.
11. Haga clic en **Save** y, a continuación, en **Test Connectivity** para probar la conectividad entre la puerta de enlace y el proveedor de configuración. Si la conexión falla, compruebe que la configuración del firewall local permite la conexión o póngase en contacto con su administrador.
12. Cuando la conexión se realice correctamente, desactive la casilla de verificación **Disabled** y, a continuación, haga clic en **Save**.

Al agregar un proveedor de configuración, el conector para Exchange ActiveSync crea automáticamente una o varias directivas asociadas al proveedor. Una definición de plantilla contenida en `config\policyTemplates.xml` en la sección `NewPolicyTemplate` define las directivas. Por cada elemento de directiva definido en esta sección, se crea una nueva directiva.

El operador puede agregar, eliminar o modificar elementos de directiva si se cumple lo siguiente: El elemento de directiva se ajusta a la definición del esquema y las cadenas de sustitución

estándar (entre llaves) no se modifican. A continuación, agregue nuevos grupos para el proveedor y actualice la directiva para incluir los nuevos grupos.

Para importar una directiva de Citrix Endpoint Management

1. En la utilidad de configuración del conector para Exchange ActiveSync, haga clic en la ficha **Config Providers** y, a continuación, en **Add**.
2. En el cuadro de diálogo **Config Providers**, en **Name**, introduzca un nombre de usuario para la autorización HTTP básica con Citrix Endpoint Management. El usuario debe tener privilegios administrativos.
3. En **Url**, introduzca la dirección web del Servicio de configuración de puerta de enlace (GCS) de Citrix Endpoint Management, normalmente en el formato `https://<xdmHost>/xdm/services/<MagConfigService>`. El nombre MagConfigService distingue entre mayúsculas y minúsculas.
4. En **Password**, introduzca la contraseña que se utiliza para la autorización HTTP básica con el servidor de Citrix Endpoint Management.
5. Haga clic en **Test Connectivity** para probar la conectividad entre la puerta de enlace y el proveedor de configuración. Si la conexión falla, compruebe que la configuración del firewall local permite la conexión o consulte con su administrador.
6. Cuando la conexión se realice correctamente, desactive la casilla de verificación **Disabled** y, a continuación, haga clic en **Save**.
7. En **Managing Host**, deje el nombre DNS predeterminado del equipo host local. Esta configuración se utiliza para coordinar la comunicación con Citrix Endpoint Management cuando se configuran varios servidores Forefront Threat Management Gateway (TMG) en una matriz.

   Después de guardar la configuración, abra el GCS.

Configuración del conector de NetScaler Gateway para el modo de directiva de Exchange ActiveSync

El conector de NetScaler Gateway para Exchange ActiveSync puede ejecutarse en los seis modos siguientes:

- **Permitir todo:** Este modo de directiva concede acceso a todo el tráfico que pasa por el conector para Exchange ActiveSync. No se utilizan otras reglas de filtrado.
- **Denegar todo:** Este modo de directiva bloquea el acceso a todo el tráfico que pasa por el conector para Exchange ActiveSync. No se utilizan otras reglas de filtrado.

- **Reglas estáticas: Modo de bloqueo:** Este modo de directiva ejecuta reglas estáticas con una instrucción implícita de denegación o bloqueo al final. El conector para Exchange ActiveSync bloquea los dispositivos que no están permitidos a través de otras reglas de filtro.
- **Reglas estáticas: Modo de permiso:** Este modo de directiva ejecuta reglas estáticas con una instrucción implícita de permiso al final. Los dispositivos que no están bloqueados o denegados a través de otras reglas de filtro se permiten a través del conector para Exchange ActiveSync.
- **Reglas estáticas + ZDM:** Modo de bloqueo. Este modo de directiva ejecuta primero reglas estáticas, seguidas de reglas dinámicas de Citrix Endpoint Management con una instrucción implícita de denegación o bloqueo al final. Los dispositivos se permiten o deniegan en función de los filtros definidos y las reglas de Citrix Endpoint Management. Cualquier dispositivo que no coincida con los filtros y reglas definidos se bloquea.
- **Reglas estáticas + ZDM:** Modo de permiso. Este modo de directiva ejecuta primero reglas estáticas, seguidas de reglas dinámicas de Citrix Endpoint Management con una instrucción implícita de permiso al final. Los dispositivos se permiten o deniegan en función de los filtros definidos y las reglas de Citrix Endpoint Management. Cualquier dispositivo que no coincida con los filtros y reglas definidos se permite.

El conector para el proceso de Exchange ActiveSync permite o bloquea las reglas dinámicas basándose en los ID de ActiveSync únicos para dispositivos móviles iOS y basados en Windows recibidos de Citrix Endpoint Management. Los dispositivos Android difieren en su comportamiento según el fabricante y algunos no exponen fácilmente un ID de ActiveSync único. Para compensar, Citrix Endpoint Management envía información de ID de usuario para dispositivos Android para tomar una decisión de permiso o bloqueo. Como resultado, si un usuario tiene solo un dispositivo Android, los permisos y bloqueos funcionan normalmente. Si el usuario tiene varios dispositivos Android, todos los dispositivos se permiten porque los dispositivos Android no se pueden diferenciar. Puede configurar la puerta de enlace para bloquear estáticamente estos dispositivos por ActiveSyncID, si se conocen. También puede configurar la puerta de enlace para bloquear según el tipo de dispositivo o el agente de usuario.

Para especificar el modo de directiva, en la utilidad de configuración del controlador SMG, haga lo siguiente:

1. Haga clic en la ficha **Path Filters** y, a continuación, en **Add**.
2. En el cuadro de diálogo **Path Properties**, seleccione un modo de directiva en la lista **Policy** y, a continuación, haga clic en **Save**.

Puede revisar las reglas en la ficha **Policies** de la utilidad de configuración. Las reglas se procesan en el conector para Exchange ActiveSync de arriba a abajo. Las directivas de permiso se muestran con una marca de verificación verde. Las directivas de denegación se muestran como un círculo rojo con una línea que lo atraviesa. Para actualizar la pantalla y ver las reglas más recientes, haga clic en **Refresh**. También puede modificar el orden de las reglas en el archivo config.xml.

Para probar las reglas, haga clic en la ficha **Simulator**. Especifique los valores en los campos. Puede obtener los valores de los registros. Un mensaje de resultado especifica Permitir o Bloquear.

Para configurar reglas estáticas

Introduzca reglas estáticas con valores que la función de filtrado ISAPI de las solicitudes HTTP de conexión de ActiveSync lee. Las reglas estáticas permiten que el conector para Exchange ActiveSync permita o bloquee el tráfico según los siguientes criterios:

- **Usuario:** El conector para Exchange ActiveSync utiliza el valor de usuario autorizado y la estructura de nombres que se capturaron durante la inscripción del dispositivo. Esa estructura se encuentra comúnmente como `domain\username` según lo referenciado por el servidor que ejecuta Citrix Endpoint Management conectado a Active Directory a través de LDAP. La ficha **Registro** de la utilidad de configuración del conector muestra los valores que pasan por el conector. Los valores se pasan si el conector debe determinar la estructura del valor o si la estructura difiere.
- **DeviceID (ActiveSyncID):** También conocido como el ActiveSyncID del dispositivo conectado. Este valor se encuentra comúnmente en la página de propiedades del dispositivo específico en la consola de Citrix Endpoint Management. Este valor también se puede obtener de la ficha **Registro** en la utilidad de configuración del conector para Exchange ActiveSync.
- **DeviceType:** El conector para Exchange ActiveSync puede determinar si un dispositivo es un iPhone, iPad u otro tipo de dispositivo y puede permitir o bloquear según ese criterio. Al igual que con otros valores, la utilidad de configuración del conector puede revelar todos los tipos de dispositivos conectados que se están procesando para la conexión de ActiveSync.
- **UserAgent:** Contiene información sobre el cliente de ActiveSync que se utiliza. Por lo general, el valor especificado corresponde a una compilación y versión específicas del sistema operativo para la plataforma del dispositivo móvil.

El conector para la utilidad de configuración de Exchange ActiveSync que se ejecuta en el servidor siempre administra las reglas estáticas.

1. En la utilidad de configuración del controlador SMG, haga clic en la ficha **Reglas estáticas** y, a continuación, haga clic en **Agregar**.
2. En el cuadro de diálogo **Propiedades de regla estática**, especifique los valores que desea utilizar como criterios. Por ejemplo, puede introducir un usuario para permitir el acceso introduciendo el nombre de usuario (por ejemplo, AllowedUser) y, a continuación, desmarcando la casilla de verificación **Inhabilitado**.
3. Haga clic en **Guardar**.

   La regla estática ya está en vigor. Además, puede utilizar expresiones regulares para definir valores, pero debe habilitar el modo de procesamiento de reglas en el archivo config.xml.

Para configurar reglas dinámicas

Las directivas y propiedades de los dispositivos en Citrix Endpoint Management definen reglas dinámicas y pueden activar un conector dinámico para el filtro de Exchange ActiveSync. Los desencadenantes se basan en la presencia de una infracción de directiva o una configuración de propiedad. Los filtros del conector para Exchange ActiveSync funcionan analizando un dispositivo en busca de una infracción de directiva o una configuración de propiedad determinada. Si el dispositivo cumple los criterios, se coloca en una lista de dispositivos. Esta lista de dispositivos no es una lista de permitidos ni una lista de bloqueados. Es una lista de dispositivos que cumplen los criterios definidos. Las siguientes opciones de configuración le permiten definir si desea permitir o denegar los dispositivos de la lista de dispositivos mediante el conector para Exchange ActiveSync.

> **Nota:**
>
> Utilice la consola de Citrix Endpoint Management para configurar reglas dinámicas.

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha. Aparece la página **Parámetros**.
2. En **Servidor**, haga clic en **ActiveSync Gateway**. Aparece la página ActiveSync Gateway.
3. En **Activar las siguientes reglas**, seleccione una o varias reglas que desee activar.
4. Solo en Android, en **Enviar usuarios de dominio de Android a ActiveSync Gateway**, haga clic en **SÍ** para asegurarse de que Citrix Endpoint Management envíe la información del dispositivo Android a Secure Mobile Gateway.

Con esta opción habilitada, Citrix Endpoint Management envía información del dispositivo Android al conector si Citrix Endpoint Management no tiene el identificador de ActiveSync para el usuario del dispositivo.

Para configurar directivas personalizadas editando el conector para el archivo XML de Exchange ActiveSync

Puede ver las directivas básicas en la configuración predeterminada en la ficha **Directivas** de la utilidad de configuración del conector para Exchange ActiveSync. Si desea crear directivas personalizadas, puede editar el archivo de configuración XML del conector de NetScaler Gateway para Exchange ActiveSync (config\config.xml).

1. Busque la sección **PolicyList** en el archivo y, a continuación, agregue un nuevo elemento **Policy**.
2. Si también se requiere un nuevo grupo, como otro grupo estático o un grupo para admitir otro GCP, agregue el nuevo elemento **Group** a la sección **GroupList**.
3. Opcionalmente, puede cambiar el orden de los grupos dentro de una directiva existente reorganizando los elementos **GroupRef**.

Configuración del conector para el archivo XML de Exchange ActiveSync

El conector para Exchange ActiveSync utiliza un archivo de configuración XML para dictar las acciones del conector. Entre otras entradas, el archivo especifica los archivos de grupo y las acciones asociadas que el filtro realiza al evaluar las solicitudes HTTP. De forma predeterminada, el archivo se denomina config.xml y se encuentra en la siguiente ubicación: ..\Program Files\Citrix\XenMobile NetScaler Connector\config\.

Nodos GroupRef

Los nodos GroupRef definen los nombres de grupo lógicos. Los valores predeterminados son AllowGroup y DenyGroup.

> **Nota:**
>
> El orden de los nodos GroupRef tal como aparecen en el nodo GroupRefList es significativo.
>
> El valor de ID de un nodo GroupRef identifica un contenedor lógico o una colección de miembros que se utilizan para hacer coincidir cuentas de usuario o dispositivos específicos. Los atributos de acción especifican cómo el filtro trata a un miembro que coincide con una regla de la colección. Por ejemplo, una cuenta de usuario o un dispositivo que coincide con

> una regla del conjunto AllowGroup "pasa". Pasar significa que se le permite acceder al CAS de Exchange. Una cuenta de usuario o un dispositivo que coincide con una regla del conjunto DenyGroup es "rechazado". Rechazado significa que no se le permite acceder al CAS de Exchange.

Cuando una cuenta de usuario/dispositivo o una combinación particular cumple las reglas de ambos grupos, se utiliza una convención de precedencia para dirigir el resultado de la solicitud. La precedencia se materializa en el orden de los nodos GroupRef en el archivo config.xml de arriba a abajo. Los nodos GroupRef se clasifican por orden de prioridad. Las reglas para una condición dada en el grupo Permitir siempre tendrán prioridad sobre las reglas para la misma condición en el grupo Denegar.

Nodos de grupo

Además, el archivo config.xml define nodos de grupo. Estos nodos vinculan los contenedores lógicos AllowGroup y DenyGroup a archivos XML externos. Las entradas almacenadas en los archivos externos forman la base de las reglas de filtro.

> **Nota:**

> En esta versión, solo se admiten archivos XML externos.

> La instalación predeterminada implementa dos archivos XML en la configuración: allow.xml y deny.xml.

Configuración del conector de NetScaler Gateway para Exchange ActiveSync

Puede configurar el conector de NetScaler Gateway para Exchange ActiveSync para bloquear o permitir selectivamente las solicitudes de ActiveSync en función de las siguientes propiedades: **ID de servicio de Active Sync**, **Tipo de dispositivo**, **Agente de usuario** (sistema operativo del dispositivo), **Usuario autorizado** y **Comando de ActiveSync**.

La configuración predeterminada admite una combinación de grupos estáticos y dinámicos. Los grupos estáticos se mantienen mediante la utilidad de configuración del controlador SMG. Los grupos estáticos pueden consistir en categorías conocidas de dispositivos, como todos los dispositivos que utilizan un agente de usuario determinado.

Una fuente externa denominada Proveedor de configuración de Gateway mantiene los grupos dinámicos. El conector para Exchange ActiveSync conecta los grupos periódicamente. Citrix Endpoint Management puede exportar grupos de dispositivos y usuarios permitidos y bloqueados al conector para Exchange ActiveSync.

Una fuente externa denominada Proveedor de configuración de Gateway mantiene los grupos dinámicos. El conector para Exchange ActiveSync recopila grupos dinámicos periódicamente. Citrix Endpoint Management puede exportar grupos de dispositivos y usuarios permitidos y bloqueados al conector.

Una directiva es una lista ordenada de grupos en la que cada grupo tiene una acción asociada (permitir o bloquear) y una lista de miembros del grupo. Una directiva puede tener cualquier número de grupos. El orden de los grupos dentro de una directiva es importante porque cuando se encuentra una coincidencia, se realiza la acción del grupo y no se evalúan los grupos posteriores.

Un miembro define una forma de hacer coincidir las propiedades de una solicitud. Puede coincidir con una sola propiedad, como el ID del dispositivo, o con varias propiedades, como el tipo de dispositivo y el agente de usuario.

Elección de un modelo de seguridad para el conector de NetScaler Gateway para Exchange ActiveSync

Establecer un modelo de seguridad es esencial para una implementación exitosa de dispositivos móviles en organizaciones de cualquier tamaño. Es común usar un control de red protegido o en cuarentena para permitir el acceso a un usuario, equipo o dispositivo de forma predeterminada. Esta práctica no siempre es ideal. Cada organización que gestiona la seguridad de TI puede tener un enfoque ligeramente diferente o personalizado para la seguridad de los dispositivos móviles.

La misma lógica se aplica a la seguridad de los dispositivos móviles. Usar un modelo permisivo es una opción débil debido a la multitud de dispositivos y tipos de dispositivos móviles, dispositivos móviles por usuario y plataformas y aplicaciones de sistemas operativos disponibles. En la mayoría de las organizaciones, el modelo restrictivo es la opción más lógica.

Los escenarios de configuración que Citrix permite para integrar el conector para Exchange ActiveSync con Citrix Endpoint Management son los siguientes:

Modelo permisivo (modo permisivo)

El modelo de seguridad permisivo opera bajo la premisa de que todo está permitido o se le concede acceso de forma predeterminada. Solo a través de reglas y filtros se bloquea algo y se aplica una restricción. El modelo de seguridad permisivo es bueno para organizaciones que tienen

una preocupación de seguridad relativamente laxa con respecto a los dispositivos móviles. El modelo solo aplica controles restrictivos para denegar el acceso cuando sea apropiado (cuando una regla de directiva falla).

Modelo restrictivo (modo de bloqueo)

El modelo de seguridad restrictivo se basa en la premisa de que nada está permitido o se le concede acceso de forma predeterminada. Todo lo que pasa por el punto de control de seguridad se filtra e inspecciona, y se le deniega el acceso a menos que se cumplan las reglas que permiten el acceso. El modelo de seguridad restrictivo es bueno para organizaciones que tienen un criterio de seguridad relativamente estricto con respecto a los dispositivos móviles. El modo solo concede acceso para el uso y la funcionalidad con los servicios de red cuando se han cumplido todas las reglas para permitir el acceso.

Administrar el conector de NetScaler Gateway para Exchange ActiveSync

Puede usar el conector de NetScaler Gateway para Exchange ActiveSync para crear reglas de control de acceso. Las reglas permiten o bloquean el acceso a las solicitudes de conexión de ActiveSync desde dispositivos administrados. El acceso se basa en el estado del dispositivo, las listas de aplicaciones permitidas o bloqueadas y otras condiciones de cumplimiento.

Al usar el conector para la utilidad de configuración de Exchange ActiveSync, puede crear reglas dinámicas y estáticas que aplican las directivas de correo electrónico corporativas. Esas reglas y directivas le permiten bloquear a los usuarios que infringen los estándares de cumplimiento. También puede configurar el cifrado de archivos adjuntos de correo electrónico, de modo que todos los archivos adjuntos que pasan por su servidor Exchange a los dispositivos administrados estén cifrados. Solo los usuarios autorizados con dispositivos administrados pueden ver los archivos adjuntos cifrados.

Para desinstalar el XNC

1. Ejecute XncInstaller.exe con una cuenta de administrador.
2. Siga las instrucciones en pantalla para completar la desinstalación.

Para instalar, actualizar o desinstalar el conector para Exchange ActiveSync

1. Ejecute XncInstaller.exe con una cuenta de administrador para instalar el conector para Exchange ActiveSync o permitir la actualización o eliminación de un conector existente.
2. Siga las instrucciones en pantalla para completar la instalación, actualización o desinstalación.

Después de instalar el conector para Exchange ActiveSync, debe reiniciar manualmente el servicio de configuración de Citrix Endpoint Management y el servicio de notificaciones.

Instalación del conector de NetScaler Gateway para Exchange ActiveSync

Puede instalar el conector para Exchange ActiveSync en su propio servidor o en el mismo servidor donde instaló Citrix Endpoint Management.

Puede considerar instalar el conector para Exchange ActiveSync en su propio servidor (separado de Citrix Endpoint Management) por los siguientes motivos:

- Si su servidor de Citrix Endpoint Management está alojado de forma remota en la nube (ubicación física)
- Si no quiere que los reinicios del servidor de Citrix Endpoint Management afecten al conector para Exchange ActiveSync (disponibilidad)
- Si quiere dedicar los recursos del sistema de un servidor exclusivamente al conector para Exchange ActiveSync (rendimiento)

La carga de CPU que el conector para Exchange ActiveSync impone a un servidor depende de la cantidad de dispositivos administrados. Una recomendación general es aprovisionar un núcleo de CPU adicional si el conector se implementa en el mismo servidor que Citrix Endpoint Management. Para un gran número de dispositivos (más de 50 000), es posible que deba aprovisionar más núcleos si no tiene un entorno en clúster. El consumo de memoria del conector no es lo suficientemente significativo como para justificar más memoria.

Requisitos del sistema del conector de NetScaler Gateway para Exchange ActiveSync

El conector de NetScaler Gateway para Exchange ActiveSync se comunica con NetScaler Gateway a través de un puente SSL configurado en el dispositivo NetScaler Gateway. El puente permite que el dispositivo conecte todo el tráfico seguro directamente a Citrix Endpoint Management. El conector para Exchange ActiveSync tiene la siguiente configuración mínima del sistema:

COMPONENTE	REQUISITO
Equipo y procesador	Procesador Pentium III de 733 MHz o superior. Procesador Pentium III de 2,0 GHz o superior (recomendado)

COMPONENTE	REQUISITO
Citrix Gateway	Dispositivo Citrix Gateway con la versión de software 10
Memoria	1 GB
Disco duro	Partición local con formato NTFS con 150 MB de espacio disponible en disco duro
Sistema operativo	Windows Server 2016, Windows Server 2012 R2 o Windows Server 2008 R2 Service Pack 1. Debe ser un servidor basado en inglés. El soporte para Windows Server 2008 R2 Service Pack 1 finaliza el January 14, 2020 y el soporte para Windows Server 2012 R2 finaliza el October 10, 2023.
Otros dispositivos	Adaptador de red compatible con el sistema operativo host para la comunicación con la red interna
Microsoft .NET Framework	La versión 8.5.1.11 requiere Microsoft .NET Framework 4.5.
Pantalla	Monitor VGA o de mayor resolución

El equipo host para el conector de Exchange ActiveSync requiere el siguiente espacio mínimo disponible en disco duro:

- **Aplicación:** 10–15 MB (100 MB recomendados)
- **Registro:** 1 GB (20 GB recomendados)

Para obtener información sobre la compatibilidad de la plataforma con el conector para Exchange ActiveSync, consulte Sistemas operativos de dispositivos compatibles.

Clientes de correo electrónico de dispositivos

No todos los clientes de correo electrónico devuelven sistemáticamente el mismo ID de ActiveSync para un dispositivo. Dado que el conector para Exchange ActiveSync espera un ID de ActiveSync único para cada dispositivo, se cumple lo siguiente: Solo se admiten los clientes de correo electrónico que generan sistemáticamente el mismo ID de ActiveSync único para cada

dispositivo. Citrix ha probado estos clientes de correo electrónico y los clientes han funcionado sin errores:

- Cliente de correo electrónico nativo de Samsung
- Cliente de correo electrónico nativo de iOS

Implementación del conector de NetScaler Gateway para Exchange ActiveSync

El conector de NetScaler Gateway para Exchange ActiveSync le permite usar NetScaler Gateway para proxy y equilibrar la carga de la comunicación del servidor de Citrix Endpoint Management con los dispositivos administrados por Citrix Endpoint Management. El conector para Exchange ActiveSync se comunica periódicamente con Citrix Endpoint Management para sincronizar las directivas. Puede agrupar el conector para Exchange ActiveSync y Citrix Endpoint Management, juntos o de forma independiente.

Componentes del conector para Exchange ActiveSync

- **El servicio de conector para Exchange ActiveSync:** Este servicio proporciona una interfaz de servicio web REST que NetScaler Gateway puede invocar para determinar si una solicitud de ActiveSync de un dispositivo está autorizada.
- **Servicio de configuración de Citrix Endpoint Management:** Este servicio se comunica con Citrix Endpoint Management para sincronizar los cambios de directivas de Citrix Endpoint Management con el conector para Exchange ActiveSync.
- **Servicio de notificaciones de Citrix Endpoint Management:** Este servicio envía notificaciones de acceso no autorizado a dispositivos a Citrix Endpoint Management. De este modo, Citrix Endpoint Management puede tomar las medidas adecuadas, como notificar al usuario por qué se bloqueó el dispositivo.
- **La utilidad de configuración del conector para Exchange ActiveSync:** Esta aplicación permite al administrador configurar y supervisar el conector para Exchange ActiveSync.

Para configurar las direcciones de escucha del conector de NetScaler Gateway para Exchange ActiveSync

Para que el conector de NetScaler Gateway para Exchange ActiveSync reciba solicitudes de NetScaler Gateway para autorizar el tráfico de ActiveSync, haga lo siguiente. Especifique el puerto en el que el conector para Exchange ActiveSync escucha las llamadas al servicio web de NetScaler Gateway.

1. En el menú **Inicio**, seleccione el conector para la utilidad de configuración de Exchange ActiveSync.
2. Haga clic en la ficha **Servicio web** y, a continuación, escriba las direcciones de escucha para el servicio web del conector. Puede seleccionar **HTTP** o **HTTPS** o ambos. Si el conector para Exchange ActiveSync reside en el mismo servidor que Citrix Endpoint Management (instalado en el mismo servidor), seleccione valores de puerto que no entren en conflicto con Citrix Endpoint Management.
3. Una vez configurados los valores, haga clic en **Guardar** y, a continuación, en **Iniciar servicio** para iniciar el servicio web.

Para configurar las directivas de control de acceso de dispositivos en el conector de NetScaler Gateway para Exchange ActiveSync

Para configurar la directiva de control de acceso que quiere aplicar a sus dispositivos administrados, haga lo siguiente:

1. En la utilidad de configuración del conector para Exchange ActiveSync, haga clic en la ficha **Filtros de ruta**.
2. Seleccione la primera fila, **Microsoft-Server-ActiveSync es para ActiveSync** y, a continuación, haga clic en **Editar**.
3. En la lista **Directiva**, seleccione la directiva deseada. Para una directiva que incluya las directivas de Citrix Endpoint Management, seleccione **Estático + ZDM: Modo de permiso o Estático + ZDM: Modo de bloqueo**. Estas directivas combinan reglas locales (o estáticas) con las reglas de Citrix Endpoint Management. El modo de permiso significa que todos los dispositivos no identificados explícitamente por las reglas tienen permitido el acceso a ActiveSync. El modo de bloqueo significa que dichos dispositivos están bloqueados.
4. Después de establecer las directivas, haga clic en **Guardar**.

Para configurar la comunicación con Citrix Endpoint Management

Especifique el nombre y las propiedades del servidor de Citrix Endpoint Management que quiere usar con el conector de NetScaler Gateway para Exchange ActiveSync y NetScaler Gateway.

> **Nota:**

> Esta tarea asume que ya ha instalado y configurado Citrix Endpoint Management. La utilidad de configuración de Exchange ActiveSync utiliza el término Proveedor de configuración para Citrix Endpoint Management.

1. En la utilidad de configuración del conector para Exchange ActiveSync, haga clic en la ficha **Proveedores de configuración** y, a continuación, en **Agregar**.
2. Introduzca el nombre y la URL del servidor de Citrix Endpoint Management que utiliza en esta implementación. Si tiene varios servidores de Citrix Endpoint Management implementados en una implementación multiempresa, este nombre debe ser único para cada instancia de servidor.
3. En **Url**, introduzca la dirección web del proveedor de configuración global (GCP) de Citrix Endpoint Management, normalmente en el formato `https://<FQDN>/<instanceName>/services/<MagConfigService>`. El nombre *MagConfigService* distingue entre mayúsculas y minúsculas.
4. En **Password**, introduzca la contraseña que se utilizará para la autorización HTTP básica con el servidor web de Citrix Endpoint Management.
5. En **Managing Host**, introduzca el nombre del servidor donde instaló el conector para Exchange ActiveSync.
6. En **Baseline Interval**, especifique un período de tiempo para cuando se extraiga un nuevo conjunto de reglas dinámicas actualizado de Citrix Endpoint Management.
7. En **Request Timeout**, especifique el intervalo de tiempo de espera de la solicitud del servidor.
8. En **Config Provider**, seleccione si la instancia del servidor del proveedor de configuración está proporcionando la configuración de la directiva.
9. En **Events Enabled**, habilite esta opción si desea que Secure Mobile Gateway notifique a Citrix Endpoint Management cuando se bloquee un dispositivo. Esta opción es obligatoria si utiliza las reglas de Secure Mobile Gateway en cualquiera de sus acciones automatizadas de Citrix Endpoint Management.
10. Después de configurar el servidor, haga clic en **Test Connectivity** para probar la conexión a Citrix Endpoint Management.
11. Cuando se haya establecido la conectividad, haga clic en **Save**.

Implementación del conector de NetScaler Gateway para Exchange ActiveSync para redundancia y escalabilidad

Para escalar la implementación del conector de NetScaler Gateway para Exchange ActiveSync y Citrix Endpoint Management, puede instalar instancias del conector para Exchange ActiveSync en varios servidores Windows. Todas las instancias del conector apuntan a la misma instancia de Citrix Endpoint Management. A continuación, puede utilizar NetScaler Gateway para equilibrar la carga de los servidores.

Hay dos modos para la configuración del conector para Exchange ActiveSync:

- En el modo no compartido, cada conector para una instancia de Exchange ActiveSync se comunica con un servidor de Citrix Endpoint Management y mantiene su propia copia privada de la directiva resultante. Por ejemplo, para un clúster de servidores de Citrix Endpoint Management, puede ejecutar una instancia de conector en cada servidor de Citrix Endpoint Management. El conector obtiene entonces las directivas de la instancia local de Citrix Endpoint Management.
- En el modo compartido, un conector para un nodo de Exchange ActiveSync se designa como nodo principal. El conector se comunica con Citrix Endpoint Management. Los otros nodos comparten la configuración resultante a través de un recurso compartido de red de Windows o mediante la replicación de Windows (o de terceros).

La configuración completa del conector para Exchange ActiveSync se encuentra en una única carpeta (que consta de unos pocos archivos XML). El proceso del conector detecta cambios en cualquier archivo de esta carpeta y recarga automáticamente la configuración. No hay conmutación por error para el nodo principal en modo compartido. Sin embargo, el sistema puede tolerar que el servidor principal esté inactivo durante unos minutos (por ejemplo, para reiniciarse). La última configuración válida conocida se almacena en caché en el proceso del conector.

Conceptos avanzados

Los artículos de Conceptos avanzados de Citrix Endpoint Management ofrecen una inmersión más profunda en la información del producto sobre Citrix Endpoint Management. El objetivo es ayudar a reducir el tiempo de implementación mediante técnicas expertas. Los artículos pueden citar a los expertos técnicos que han redactado el contenido.

Para conocer los puntos de decisión, las recomendaciones, las preguntas frecuentes y los casos de uso de su entorno de Citrix Endpoint Management, consulte (/es-es/citrix-endpoint-management/advanced-concepts/deployment.html) en esta sección.

Para ver los foros de soporte de la comunidad sobre Citrix Endpoint Management, consulte Debates de Citrix.

Implementación de Citrix Endpoint Management

Hay mucho que considerar al planificar una implementación de Citrix Endpoint Management. ¿Qué dispositivos elige? ¿Cómo los gestiona? ¿Cómo se asegura de que su red permanezca segura mientras proporciona una buena experiencia de usuario? ¿Qué hardware necesita y cómo lo soluciona? Los artículos de esta sección tienen como objetivo ayudar a responder estas preguntas. Se incluyen casos de uso y recomendaciones sobre temas que cubren sus preocupaciones de implementación.

Tenga en cuenta que una directriz o recomendación podría no aplicarse a todos los entornos o casos de uso. Asegúrese de configurar un entorno de prueba antes de poner en marcha una implementación de Citrix Endpoint Management.

Los artículos de esta sección cubren estas áreas:

- **Evaluar:** Casos de uso comunes y preguntas a considerar al planificar su implementación.
- **Diseñar y configurar:** Recomendaciones para diseñar y configurar su entorno
- **Operar y supervisar:** Asegurar el buen funcionamiento de su entorno en ejecución.

Evaluar

Como con cualquier implementación, evaluar sus necesidades debe ser su primera prioridad. ¿Cuál es su necesidad principal de Citrix Endpoint Management? ¿Es necesario gestionar todos los dispositivos de su entorno, solo las aplicaciones, o ambos? ¿Qué nivel de seguridad se necesita para su entorno de Citrix Endpoint Management? Veamos casos de uso comunes y preguntas que debe considerar al planificar su implementación.

- Modos de administración
- Requisitos de los dispositivos
- Seguridad y experiencia del usuario
- Aplicaciones
- Comunidades de usuarios
- Estrategia de correo electrónico
- Integración de Citrix Endpoint Management

Diseñar y configurar

Una vez que haya terminado de evaluar sus necesidades de implementación, puede decidir cómo diseñar y configurar su entorno. Los elementos a planificar incluyen:

- Elegir el hardware para su servidor
- Configurar directivas para aplicaciones y dispositivos
- Inscribir a los usuarios

Esta sección incluye casos de uso y recomendaciones para cada uno de estos escenarios y más.

- Integración con NetScaler Gateway y Citrix ADC
- Consideraciones de SSO y proxy para aplicaciones MDX
- Autenticación
- Propiedades del servidor
- Directivas de dispositivos y aplicaciones
- Opciones de inscripción de usuarios

Operar y supervisar

Una vez que su entorno de Citrix Endpoint Management esté en funcionamiento, querrá supervisarlo para asegurarse de que funcione sin problemas. La sección de supervisión explica dónde puede encontrar los diversos registros y mensajes que generan Citrix Endpoint Management y sus componentes, y cómo leer esos registros. Esta sección también incluye varios pasos comunes de solución de problemas que puede seguir para reducir el tiempo de respuesta del soporte al cliente.

- Aprovisionamiento y desaprovisionamiento de aplicaciones(/es-es/citrix-endpoint-management/advanced-concepts/deployment/app-provisioning-deprovisioning.html)
- Operaciones basadas en el panel(/es-es/citrix-endpoint-management/advanced-concepts/deployment/dashboard-based-operations.html)
- Control de acceso basado en roles y soporte de Citrix Endpoint Management(/es-es/citrix-endpoint-management/advanced-concepts/deployment/role-based-access-control-support.html)
- Supervisión y soporte(/es-es/citrix-endpoint-management/monitor-support.html)
- Proceso de soporte de Citrix(/es-es/citrix-endpoint-management/advanced-concepts/deployment/citrix-support-process.html)

Modos de administración

Modos de administración es un término que incluye la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM). Puede configurar:

- Perfiles de inscripción para inscribir dispositivos Android e iOS en MDM, MAM o ambos (MDM+MAM). Si elige MDM+MAM, puede dar a los usuarios la opción de no participar en MDM.
- Perfiles de inscripción para inscribir dispositivos Windows 10 y Windows 11 en MDM.

Las opciones de inscripción se especifican en los perfiles de inscripción, que se adjuntan a los grupos de entrega. Para obtener información sobre las opciones de inscripción, consulte Perfiles de inscripción. Las siguientes secciones se centran en las consideraciones para administrar dispositivos y aplicaciones.

Administración de dispositivos móviles (MDM)

Con MDM, puede configurar, proteger y dar soporte a dispositivos móviles. MDM le permite proteger los dispositivos y los datos de los dispositivos a nivel de sistema. Puede configurar

directivas, acciones y funciones de seguridad. Por ejemplo, puede borrar un dispositivo de forma selectiva si se pierde, es robado o no cumple con las normativas.

Aunque no elija administrar aplicaciones en los dispositivos, puede entregar aplicaciones móviles, como las de tiendas de aplicaciones públicas y las aplicaciones empresariales.

Los siguientes son casos de uso comunes para MDM:

- MDM es una consideración para los dispositivos propiedad de la empresa donde se requieren directivas de administración a nivel de dispositivo o ciertas restricciones. Esas restricciones incluyen borrado completo, borrado selectivo o geolocalización.
- Cuando los clientes requieren la administración de un dispositivo real, pero no requieren directivas MDX.
- Cuando los usuarios solo necesitan que el correo electrónico se entregue a sus clientes de correo electrónico nativos en sus dispositivos móviles, y Exchange ActiveSync o Client Access Server ya son accesibles externamente. En este caso de uso, puede usar MDM para configurar la entrega de correo electrónico.
- Cuando implementa aplicaciones empresariales nativas (no MDX), aplicaciones de tiendas de aplicaciones públicas o aplicaciones MDX entregadas desde tiendas públicas. Tenga en cuenta que una solución MDM por sí sola podría no evitar la fuga de datos de información confidencial entre aplicaciones en el dispositivo. La fuga de datos podría ocurrir con operaciones de copiar y pegar o Guardar como en aplicaciones de Office 365.

Administración de aplicaciones móviles (MAM)

MAM protege los datos de las aplicaciones y le permite controlar el uso compartido de datos de las aplicaciones. MAM también permite la administración de datos y recursos corporativos, por separado de los datos personales. Con Citrix Endpoint Management configurado para MAM, puede usar aplicaciones móviles habilitadas para MDX para proporcionar contención y control por aplicación.

Mediante el uso de políticas MDX, Citrix Endpoint Management proporciona control a nivel de aplicación sobre el acceso a la red (como micro VPN), la interacción entre aplicaciones y dispositivos, y el acceso a las aplicaciones.

MAM suele ser adecuado para dispositivos de tipo «traiga su propio dispositivo» (BYO) porque, aunque el dispositivo no está administrado, los datos corporativos están protegidos. MDX tiene muchas políticas solo de MAM que no requieren un control MDM.

MAM también es compatible con las aplicaciones de productividad móvil de Citrix. Esta compatibilidad incluye:

- Entrega segura de correo electrónico a Citrix Secure Mail
- Uso compartido de datos entre las aplicaciones de productividad móvil seguras de Citrix
- Almacenamiento seguro de datos en Citrix Files.

Para obtener más información, consulte Aplicaciones de productividad móvil.

MAM suele ser adecuado para los siguientes ejemplos:

- Usted entrega aplicaciones móviles, como las aplicaciones MDX, administradas a nivel de aplicación.
- No es necesario que administre los dispositivos a nivel de sistema.

MDM+MAM

Citrix Endpoint Management le permite especificar si los usuarios pueden optar por no participar en la administración de dispositivos. Esta flexibilidad es útil para entornos que incluyen una combinación de casos de uso. Estos entornos pueden requerir la administración de un dispositivo a través de políticas MDM para acceder a sus recursos MAM.

MDM+MAM es adecuado para los siguientes ejemplos:

- Tiene un único caso de uso en el que se requieren tanto MDM como MAM. Se requiere MDM para acceder a sus recursos MAM.
- Algunos casos de uso requieren MDM, mientras que otros no.
- Algunos casos de uso requieren MAM, mientras que otros no.

Administración de dispositivos e inscripción en MDM

Un entorno de Citrix Endpoint Management Enterprise puede incluir una combinación de casos de uso, algunos de los cuales requieren la administración de dispositivos a través de directivas MDM para permitir el acceso a los recursos de MAM.

Antes de implementar las aplicaciones de productividad móvil de Citrix para los usuarios, evalúe completamente sus casos de uso y decida si requiere la inscripción en MDM. Si más tarde decide cambiar el requisito de inscripción en MDM, es posible que los usuarios deban volver a inscribir sus dispositivos. Para obtener más información, consulte Perfiles de inscripción.

Para obtener información sobre la inscripción y NetScaler Gateway, consulte Integración con NetScaler Gateway y Citrix ADC.

A continuación, se presenta un resumen de las ventajas y desventajas (junto con las mitigaciones) de requerir la inscripción en MDM.

Cuando la inscripción en MDM es opcional

Ventajas

- Los usuarios pueden acceder a los recursos de MAM sin someter sus dispositivos a la administración de MDM. Esta opción puede aumentar la adopción por parte del usuario.
- Capacidad para proteger el acceso a los recursos de MAM para proteger los datos empresariales.
- Las directivas MDX, como **Código de acceso de la aplicación**, pueden controlar el acceso a la aplicación para cada aplicación MDX.
- La configuración de NetScaler Gateway, Citrix Endpoint Management y los tiempos de espera por aplicación, junto con el PIN de Citrix, proporcionan una capa adicional de protección.
- Aunque las acciones de MDM no se aplican al dispositivo, algunas directivas MDX están disponibles para denegar el acceso a MAM. La denegación se basa en la configuración del sistema, como dispositivos con jailbreak o rooteados.
- Los usuarios pueden elegir si inscribir su dispositivo en MDM durante el primer uso.

Desventajas

- Los recursos MAM están disponibles para dispositivos no inscritos en MDM.
- Las políticas y acciones de MDM solo están disponibles para dispositivos inscritos en MDM.

Opciones de mitigación

- Haga que los usuarios acepten los términos y condiciones de la empresa que los responsabilizan si deciden incumplir las normas. Haga que los administradores supervisen los dispositivos no administrados.
- Administre el acceso y la seguridad de las aplicaciones mediante temporizadores de aplicaciones. La reducción de los valores de tiempo de espera aumenta la seguridad, pero puede afectar a la experiencia del usuario.

Cuando se requiere la inscripción en MDM

Ventajas

- Capacidad para restringir el acceso a los recursos MAM solo a dispositivos administrados por MDM.
- Las políticas y acciones de MDM se pueden aplicar a todos los dispositivos del entorno como usted desee.
- Los usuarios no pueden optar por no inscribir su dispositivo.

Desventajas

- Requiere que todos los usuarios se inscriban en MDM.
- Podría reducir la adopción para los usuarios que se oponen a la administración corporativa de sus dispositivos personales.

Opciones de mitigación

- Eduque a los usuarios sobre lo que Citrix Endpoint Management realmente administra en sus dispositivos y a qué información pueden acceder los administradores.

Requisitos del dispositivo

Un punto importante a considerar para cualquier implementación es el conjunto de dispositivos que planea implementar. En las plataformas iOS, Android y Windows, las opciones son muchas. Para obtener una lista de los dispositivos compatibles con Citrix Endpoint Management, consulte Plataformas de dispositivos compatibles.

En un entorno de traer su propio dispositivo (BYOD), es posible una mezcla de plataformas compatibles. Sin embargo, tenga en cuenta las limitaciones del artículo Plataformas de dispositivos compatibles al informar a los usuarios sobre los dispositivos que pueden inscribir. Incluso si solo permite uno o dos dispositivos en su entorno, Citrix Endpoint Management funciona de forma ligeramente diferente en los dispositivos iOS, Android y Windows. Hay diferentes conjuntos de funciones disponibles en cada plataforma.

Además, no todos los diseños de aplicaciones están dirigidos a factores de forma de tabletas y teléfonos. Antes de realizar cambios generalizados, pruebe las aplicaciones para asegurarse de que se ajustan a la pantalla del dispositivo que desea implementar.

También puede considerar los factores de inscripción. Apple y Google ofrecen programas de inscripción empresarial. A través del Programa de implementación de Apple y Google Android Enterprise, puede comprar dispositivos preconfigurados y listos para que los usen los empleados.

Para obtener más información sobre la inscripción, consulte Opciones de inscripción de usuarios.

Seguridad y experiencia de usuario

La seguridad es importante para cualquier organización, pero es necesario lograr un equilibrio entre la seguridad y la experiencia del usuario. Por ejemplo, puede tener un entorno altamente seguro que sea difícil de usar para los usuarios. O bien, su entorno podría ser tan fácil de usar que el control de acceso no sea tan estricto. Las otras secciones de este manual virtual cubren las funciones de seguridad en detalle. El propósito de este artículo es ofrecer una descripción general de las preocupaciones de seguridad comunes y las opciones de seguridad disponibles en Citrix Endpoint Management.

Estas son algunas consideraciones clave que debe tener en cuenta para cada caso de uso:

- ¿Quiere proteger ciertas aplicaciones, todo el dispositivo o ambos?
- ¿Cómo quiere que los usuarios autentiquen su identidad? ¿Quiere usar LDAP, autenticación basada en certificados o una combinación de ambos?
- ¿Cuánto tiempo quiere que dure la sesión de un usuario antes de que caduque? Tenga en cuenta que hay diferentes valores de tiempo de espera para los servicios en segundo plano, Citrix ADC y para poder acceder a las aplicaciones sin conexión.
- ¿Quiere que los usuarios configuren un código de acceso a nivel de dispositivo y un código de acceso a nivel de aplicación? ¿Cuántos intentos de inicio de sesión quiere permitir? Tenga en cuenta los requisitos adicionales de autenticación por aplicación que podrían implementarse con MAM y cómo los usuarios podrían percibirlos.
- ¿Qué otras restricciones quiere imponer a los usuarios? ¿Quiere dar a los usuarios acceso a servicios en la nube como Siri? ¿Qué pueden hacer con cada aplicación que les ponga a su disposición y qué no pueden hacer? ¿Quiere implementar directivas de red corporativa (Wi-Fi) para evitar que se utilicen planes de datos móviles desde dentro de la oficina?

Aplicación frente a dispositivo

Una de las primeras cosas a considerar es si quiere proteger:

- Solo ciertas aplicaciones (administración de aplicaciones móviles o MAM)
- Todo el dispositivo (administración de dispositivos móviles o MDM).
- MDM+MAM

Lo más común es que, si no necesita un control a nivel de dispositivo, solo tenga que administrar aplicaciones móviles, especialmente si su organización admite Bring Your Own Device (BYOD).

Los usuarios con dispositivos que Citrix Endpoint Management no administra pueden instalar aplicaciones a través de la tienda de aplicaciones. En lugar de controles a nivel de dispositivo, como el borrado selectivo o completo, usted controla el acceso a las aplicaciones a través de directivas de aplicaciones. Según los valores que establezca, las directivas requieren que el dispositivo compruebe Citrix Endpoint Management periódicamente para confirmar que las aplicaciones aún tienen permiso para ejecutarse.

MDM le permite proteger un dispositivo completo, incluida la capacidad de inventariar todo el software de un dispositivo. MDM le permite evitar la inscripción si el dispositivo tiene jailbreak, está rooteado o tiene software inseguro instalado. Sin embargo, asumir este nivel de control hace que los usuarios desconfíen de permitir tanto poder sobre sus dispositivos personales y puede reducir las tasas de inscripción.

Autenticación

La autenticación es donde tiene lugar gran parte de la experiencia del usuario. Si su organización ya utiliza Active Directory, usar Active Directory es la forma más sencilla de que sus usuarios accedan al sistema.

Otra parte importante de la experiencia de usuario de autenticación son los tiempos de espera. Un entorno de alta seguridad podría hacer que los usuarios inicien sesión cada vez que acceden al sistema. Esa opción podría no ser ideal para todas las organizaciones o casos de uso.

Entropía de usuario

Para mayor seguridad, puede habilitar una función llamada *entropía de usuario*. Citrix Secure Hub y otras aplicaciones suelen compartir datos comunes como contraseñas, PIN y certificados para asegurarse de que todo funcione correctamente. Esta información se almacena en una bóveda genérica dentro de Citrix Secure Hub. Si habilita la entropía de usuario a través de la opción **Cifrar secretos**, Citrix Endpoint Management crea una bóveda llamada UserEntropy. Citrix Endpoint Management mueve la información de la bóveda genérica a esta nueva bóveda. Para que Citrix Secure Hub u otra aplicación acceda a los datos, los usuarios deben introducir una contraseña o un PIN.

Habilitar la entropía de usuario añade otra capa de autenticación en varios lugares. Como resultado, cada vez que una aplicación requiera acceso a datos compartidos en la bóveda UserEntropy (incluidas contraseñas, PIN y certificados), los usuarios deberán autenticarse.

Puede obtener más información sobre la entropía de usuario leyendo Acerca de MDX Toolkit. Para activar la entropía de usuario, puede encontrar la configuración relacionada en las Propiedades del cliente.

Directivas

Tanto las directivas MDX como las MDM ofrecen una gran flexibilidad a las organizaciones, pero también pueden restringir a los usuarios. Es posible que desee esa restricción en algunas situaciones, pero las directivas también pueden hacer que un sistema sea inutilizable. Por ejemplo, es posible que desee bloquear el acceso a aplicaciones en la nube como Siri o iCloud que tienen el potencial de enviar datos confidenciales a ubicaciones externas. Puede configurar una directiva para bloquear el acceso a estos servicios, pero tenga en cuenta que dicha directiva puede tener consecuencias no deseadas. Por ejemplo, el micrófono del teclado de iOS depende del acceso a la nube.

Aplicaciones

Enterprise Mobility Management (EMM) se divide en Mobile Device Management (MDM) y Mobile Application Management (MAM). Mientras que MDM permite a las organizaciones proteger y controlar los dispositivos móviles, MAM facilita la entrega y la gestión de aplicaciones. Con la creciente adopción de BYOD, normalmente puede implementar una solución MAM, como Citrix Endpoint Management, para ayudar con lo siguiente:

- entrega de aplicaciones
- licencias de software
- configuración
- gestión del ciclo de vida de las aplicaciones

Con Citrix Endpoint Management, puede añadir más seguridad a estas aplicaciones configurando políticas MAM específicas y ajustes de VPN para evitar fugas de datos y otras amenazas de seguridad. Citrix Endpoint Management ofrece a las organizaciones la flexibilidad de incluir la funcionalidad MDM y MAM en el mismo entorno.

Además de la capacidad de entregar aplicaciones a dispositivos móviles, Citrix Endpoint Management ofrece la contenerización de aplicaciones a través de la tecnología MDX. MDX protege las aplicaciones mediante un cifrado independiente del cifrado a nivel de dispositivo proporcionado por la plataforma. Puede borrar o bloquear aplicaciones. Las aplicaciones están sujetas a controles granulares basados en políticas. Los proveedores de software independientes (ISV) pueden aplicar estos controles mediante el SDK de aplicaciones móviles.

En un entorno corporativo, los usuarios utilizan varias aplicaciones móviles para ayudarles en su función laboral. Las aplicaciones pueden incluir aplicaciones de la tienda de aplicaciones pública,

aplicaciones desarrolladas internamente o aplicaciones nativas. Citrix Endpoint Management clasifica estas aplicaciones de la siguiente manera:

Aplicaciones públicas: Estas aplicaciones incluyen aplicaciones gratuitas o de pago disponibles en una tienda de aplicaciones pública, como Apple App Store o Google Play. Los proveedores externos a la organización suelen poner sus aplicaciones a disposición en las tiendas de aplicaciones públicas. Esta opción permite a sus clientes descargar las aplicaciones directamente de Internet. Es posible que utilice muchas aplicaciones públicas en su organización, según las necesidades de los usuarios. Ejemplos de estas aplicaciones incluyen GoToMeeting, Salesforce y las aplicaciones de EpicCare.

Citrix® no admite la descarga de binarios de aplicaciones directamente desde las tiendas de aplicaciones públicas para luego empaquetarlos con el MDX Toolkit para su distribución empresarial. Para habilitar aplicaciones de terceros con MDX, póngase en contacto con el proveedor de la aplicación para obtener los binarios de la aplicación. Puede empaquetar los binarios utilizando el MDX Toolkit o integrar el SDK de MAM con los binarios.

Aplicaciones internas: Muchas organizaciones tienen desarrolladores internos que crean aplicaciones que proporcionan funcionalidades específicas y se desarrollan y distribuyen de forma independiente dentro de la organización. En algunos casos, algunas organizaciones también pueden tener aplicaciones proporcionadas por ISV. Puede implementar estas aplicaciones como aplicaciones nativas o puede contenerizar las aplicaciones utilizando una solución MAM, como Citrix Endpoint Management. Por ejemplo, una organización sanitaria puede crear una aplicación interna que permita a los médicos ver la información del paciente en dispositivos móviles. Una organización puede entonces habilitar la aplicación con el SDK de MAM o empaquetarla con MDM para proteger la información del paciente y habilitar el acceso VPN al servidor de la base de datos de pacientes de back-end.

Aplicaciones web y SaaS: Estas aplicaciones incluyen aplicaciones a las que se accede desde una red interna (aplicaciones web) o a través de una red pública (SaaS). Citrix Endpoint Management también le permite crear aplicaciones web y SaaS personalizadas utilizando una lista de conectores de aplicaciones. Estos conectores de aplicaciones pueden facilitar el inicio de sesión único (SSO) en las aplicaciones web existentes. Para obtener más información, consulte Tipos de conectores de aplicaciones. Por ejemplo, puede utilizar Google Apps SAML para SSO basado en Security Assertion Markup Language (SAML) para Google Apps.

Aplicaciones de productividad móvil: Las aplicaciones de productividad móvil son aplicaciones desarrolladas por Citrix que se incluyen con la licencia de Citrix Endpoint Management. Para obtener más información, consulte Acerca de las aplicaciones de productividad móvil. Citrix

también ofrece otras aplicaciones listas para empresas. Los ISV desarrollan aplicaciones listas para empresas utilizando el SDK de aplicaciones móviles.

Aplicaciones HDX: Las aplicaciones HDX son aplicaciones alojadas en Windows que se publican con StoreFront. Si tiene un entorno de Citrix Virtual Apps and Desktops, puede integrar las aplicaciones con Citrix Endpoint Management para que estén disponibles para los usuarios inscritos.

Según el tipo de aplicaciones móviles que planee implementar y administrar con Citrix Endpoint Management, la configuración y la arquitectura subyacentes difieren. Supongamos que muchos grupos de usuarios con varios niveles de permisos consumen una única aplicación. En ese caso, puede crear grupos de entrega separados para implementar dos versiones de la aplicación. Asegúrese de que la pertenencia a grupos de usuarios sea mutuamente excluyente para evitar desajustes de políticas en los dispositivos de los usuarios.

También es posible que desee administrar las licencias de aplicaciones iOS mediante Apple Volume Purchase. Esta opción requiere que se registre en el programa Apple Volume Purchase. Y debe utilizar la consola de Citrix Endpoint Management para configurar los ajustes de Volume Purchase. Esa configuración le permite distribuir las aplicaciones con las licencias de Volume Purchase. Varios de estos casos de uso hacen que sea importante evaluar y planificar su estrategia de MAM antes de implementar el entorno de Citrix Endpoint Management. Puede empezar a planificar su estrategia de MAM definiendo lo siguiente:

Tipos de aplicaciones: Enumere los diferentes tipos de aplicaciones que planea admitir. Luego, clasifique las aplicaciones, como públicas, nativas, aplicaciones de productividad móvil de Citrix, web, internas y aplicaciones de ISV. Además, clasifique las aplicaciones para diferentes plataformas de dispositivos, como iOS y Android. Esta categorización le ayuda a alinear la configuración de Citrix Endpoint Management que se requiere para cada tipo de aplicación. Por ejemplo: Ciertas aplicaciones podrían no ser aptas para el empaquetado. O bien, algunas aplicaciones podrían requerir el uso del SDK de aplicaciones móviles para habilitar API especiales para la interacción con otras aplicaciones.

Requisitos de red: Configure las aplicaciones con requisitos específicos de acceso a la red con la configuración adecuada. Por ejemplo, ciertas aplicaciones podrían necesitar acceso a su red interna a través de una VPN. Algunas aplicaciones podrían requerir acceso a Internet para enrutar el acceso a través de la DMZ. Para permitir que dichas aplicaciones se conecten a la red requerida, debe configurar varios ajustes en consecuencia. Defina los requisitos de red por aplicación para ayudar a finalizar sus decisiones arquitectónicas de antemano. Ese trabajo agiliza el proceso general de implementación.

Requisitos de seguridad: Defina los requisitos de seguridad que se aplican a aplicaciones individuales o a todas las aplicaciones. Algunos ajustes, como las políticas MDX, se aplican a aplicaciones individuales. Los ajustes de sesión y autenticación se aplican a todas las aplicaciones. Algunas aplicaciones pueden tener requisitos específicos de cifrado, contenerización, empaquetado, autenticación, geocercado, código de acceso o uso compartido de datos. Describa esos requisitos con antelación para simplificar su implementación.

Requisitos de implementación: Es posible que desee utilizar una implementación basada en políticas para permitir que solo los usuarios conformes descarguen las aplicaciones publicadas. Por ejemplo, es posible que desee que ciertas aplicaciones requieran que:

- la encriptación basada en la plataforma del dispositivo esté habilitada
- el dispositivo esté administrado
- el dispositivo cumpla con una versión mínima del sistema operativo
- ciertas aplicaciones estén disponibles solo para usuarios corporativos

Describa dichos requisitos con antelación para poder configurar las reglas o acciones de implementación adecuadas.

Requisitos de licencia: Registre los requisitos de licencia relacionados con las aplicaciones. Estas notas le ayudarán a gestionar el uso de las licencias de forma eficaz y a decidir si necesita configurar funciones específicas en Citrix Endpoint Management para facilitar la concesión de licencias. Por ejemplo, si implementa una aplicación iOS gratuita o de pago, Apple impone requisitos de licencia en la aplicación haciendo que los usuarios inicien sesión en su cuenta de Apple Store. Puede registrarse en Apple Volume Purchase para distribuir y administrar estas aplicaciones a través de Citrix Endpoint Management. Volume Purchase permite a los usuarios descargar las aplicaciones sin tener que iniciar sesión en su cuenta de Apple Store. Además, herramientas como Samsung Knox tienen requisitos de licencia especiales que debe cumplir antes de implementar esas funciones.

Requisitos de lista de permitidos y lista de bloqueados: Es probable que desee evitar que los usuarios instalen o utilicen algunas aplicaciones. Cree una lista de permitidos de aplicaciones que hacen que un dispositivo no cumpla con las normas. Luego, configure políticas para que se activen cuando un dispositivo deje de cumplir con las normas. Por otro lado, una aplicación podría ser aceptable para su uso, pero podría estar en la lista de bloqueados por alguna razón. En ese caso, puede agregar la aplicación a una lista de permitidos e indicar que la aplicación es aceptable para usar, pero no es obligatoria. Además, tenga en cuenta que las aplicaciones preinstaladas en los nuevos dispositivos pueden incluir algunas aplicaciones de uso común que no forman parte del

sistema operativo. Esas aplicaciones podrían entrar en conflicto con su estrategia de lista de bloqueados.

Caso de uso de aplicaciones

Una organización de atención médica planea implementar Citrix Endpoint Management para que sirva como solución MAM para sus aplicaciones móviles. Las aplicaciones móviles se entregan a usuarios corporativos y BYOD. TI decide entregar y administrar las siguientes aplicaciones:

- **Aplicaciones de productividad móvil:** Aplicaciones iOS y Android proporcionadas por Citrix.
- **Citrix Files:** Aplicación para acceder a datos compartidos y para compartir, sincronizar y editar archivos.

TIENDA DE APLICACIONES PÚBLICA

- **Citrix Secure Hub:** Cliente utilizado por todos los dispositivos móviles para comunicarse con Citrix Endpoint Management. TI envía configuraciones de seguridad, configuraciones y aplicaciones móviles a los dispositivos móviles a través del cliente Citrix Secure Hub. Los dispositivos Android e iOS se inscriben en Citrix Endpoint Management a través de Citrix Secure Hub.
- **Aplicación Citrix Workspace:** Aplicación móvil que permite a los usuarios abrir en dispositivos móviles aplicaciones alojadas por Citrix Virtual Apps.
- **GoToMeeting:** Cliente de reuniones en línea, uso compartido de escritorio y videoconferencias que permite a los usuarios reunirse con otros usuarios de ordenador, clientes o compañeros a través de Internet en tiempo real.
- **SalesForce1:** Salesforce1 permite a los usuarios acceder a Salesforce desde dispositivos móviles y reúne todas las aplicaciones Chatter, CRM, personalizadas y los procesos de negocio en una experiencia unificada para cualquier usuario de Salesforce.
- **RSA SecurID:** Token basado en software para autenticación de dos factores.
- **EpicCare apps:** Estas aplicaciones proporcionan a los profesionales sanitarios acceso seguro y portátil a historiales de pacientes, listas de pacientes, programaciones y mensajería.
    - **Haiku:** Aplicación móvil para iPhone y teléfonos Android.
    - **Canto:** Aplicación móvil para iPad
    - **Rover:** Aplicaciones móviles para iPhone y iPad.

HDX: Citrix Virtual Apps entrega aplicaciones HDX a Citrix Workspace.

- **Epic Hyperspace:** Aplicación cliente de Epic para la gestión de historiales médicos electrónicos.

ISV

- **Vocera:** Aplicación móvil de voz sobre IP y mensajería compatible con HIPAA que extiende los beneficios de la tecnología de voz de Vocera en cualquier momento y lugar a través de smartphones iPhone y Android.

APLICACIONES INTERNAS

- **HCMail:** Aplicación que ayuda a redactar mensajes cifrados, buscar libretas de direcciones en servidores de correo internos y enviar los mensajes cifrados a los contactos utilizando un cliente de correo electrónico.

APLICACIONES WEB INTERNAS

- **PatientRounding:** Aplicación web utilizada para registrar información de salud del paciente por diferentes departamentos.
- **Outlook Web Access:** Permite el acceso al correo electrónico a través de un navegador web.
- **SharePoint:** Se utiliza para compartir archivos y datos en toda la organización.

La siguiente tabla enumera la información básica necesaria para la configuración de MAM.

APLICACIÓN	TIPO DE APLICACIÓN	AJUSTE MDX	IOS	ANDROID
Citrix Secure Mail	Aplicación de productividad móvil	No para la versión 10.4.1 y posteriores	Sí	Sí
Citrix Secure Web	Aplicación de productividad móvil	No para la versión 10.4.1 y posteriores	Sí	Sí
Citrix Files	Aplicación de productividad móvil	No para la versión 10.4.1 y posteriores	Sí	Sí
Citrix Secure Hub	Aplicación pública	N/A	Sí	Sí
Aplicación Citrix Workspace	Aplicación pública	NA	Sí	Sí
GoToMeeting	Aplicación pública	NA	Sí	Sí

APLICACIÓN	TIPO DE APLICACIÓN	AJUSTE MDX	IOS	ANDROID
SalesForce1	Aplicación pública	NA	Sí	Sí
RSA SecurID	Aplicación pública	N/A	Sí	Sí
Epic Haiku	Aplicación pública	N/A	Sí	Sí
Epic Canto	Aplicación pública	N/A	Sí	No
Epic Rover	Aplicación pública	NA	Sí	No
Epic Hyperspace	Aplicación HDX™	NA	Sí	Sí
Vocera	Aplicación ISV	Sí	Sí	Sí
HCMail	Aplicación interna	Sí	Sí	Sí
PatientRounding	Aplicación web	N/A	Sí	Sí
Outlook Web Access	Aplicación web	N/A	Sí	Sí
SharePoint	Aplicación web	NA	Sí	Sí

Las siguientes tablas enumeran los requisitos específicos que puede consultar al configurar las directivas MAM en Citrix Endpoint Management.

NOMBRE DE LA APP	VPN REQUERIDA	INTERACCIÓN (CON APLICACIONES FUERA DEL CONTENEDOR)	INTERACCIÓN (DESDE APLICACIONES FUERA DEL CONTENEDOR)	CIFRADO BASADO EN LA PLATAFORMA DEL DISPOSITIVO
Citrix Secure Mail	Sí	Permitido selectivamente	Permitido	No requerido
Citrix Secure Web	Sí	Permitido	Permitido	No requerido
Citrix Files	Sí	Permitido	Permitido	No requerido
Citrix Secure Hub	Sí	N/A	N/A	N/A
Aplicación Citrix Workspace	Sí	N/A	N/A	N/A
GoToMeeting	No	N/A	N/A	N/A
SalesForce1	No	N/A	N/A	N/A
RSA SecurID	N	N/A	N/A	N/A
Epic Haiku	S	N/A	N/A	N/A
Epic Canto	S	N/A	N/A	N/A
Epic Rover	Sí	N/D	N/D	N/D
Epic Hyperspace	Sí	N/D	N/D	N/D
Vocera	Sí	Bloqueado	Bloqueado	No requerido
HCMail	Sí	Bloqueado	Bloqueado	Obligatorio
PatientRounding	Sí	N/A	N/A	Obligatorio

NOMBRE DE LA APP	VPN REQUERIDA	INTERACCIÓN (CON APLICACIONES FUERA DEL CONTENEDOR)	INTERACCIÓN (DESDE APLICACIONES FUERA DEL CONTENEDOR)	CIFRADO BASADO EN LA PLATAFORMA DEL DISPOSITIVO
Outlook Web Access	Sí	N/A	N/A	No obligatorio
SharePoint	Sí	N/D	N/D	No requerido

APLICACIÓN	FILTRADO DE PROXY	LICENCIAS	GEOCERCADO	SDK DE APLICACIONES MÓVILES	VERSIÓN MÍNIMA DEL SISTEMA OPERATIVO
Citrix Secure Mail	Requerido	N/D	Requerido selectivamente	N/D	Aplicado
Citrix Secure Web	Obligatorio	N/D	No obligatorio	N/D	Aplicado
Secure Notes	Obligatorio	N/D	No obligatorio	N/D	Aplicado
Citrix Files	Obligatorio	N/D	No requerido	N/D	Aplicado
Citrix Secure Hub	No requerido	Compra por volumen	No requerido	N/D	No aplicado
Aplicación Citrix Workspace	No requerido	Compra por volumen	No requerido	N/D	No aplicado
GoToMeeting	No requerido	Compra por volumen	No requerido	N/A	No aplicado
SalesForce1	No requerido	Compra por volumen	No requerido	N/A	No aplicado

APLICACIÓN	FILTRADO DE PROXY	LICENCIAS	GEOCERCADO	SDK DE APLICACIONES MÓVILES	VERSIÓN MÍNIMA DEL SISTEMA OPERATIVO
RSA SecurID	No requerido	Compra por volumen	No requerido	N/D	No aplicado
Epic Haiku	No requerido	Compra por volumen	No requerido	N/D	No aplicado
Epic Canto	No requerido	Compra por volumen	No requerido	N/D	No exigido
Epic Rover	No requerido	Compra por volumen	No requerido	N/A	No exigido
Epic Hyperspace	No requerido	N/A	No requerido	N/A	No exigido
Vocera	Requerido	N/D	Obligatorio	Obligatorio	Aplicado
HCMail	Obligatorio	N/D	Obligatorio	Obligatorio	Aplicado
PatientRound-ing	Obligatorio	N/D	No obligatorio	N/D	No aplicado
Outlook Web Access	Obligatorio	N/A	No obligatorio	N/A	No aplicado
SharePoint	Obligatorio	N/A	No obligatorio	N/A	No aplicado

Comunidades de usuarios

Cada organización está formada por diversas comunidades de usuarios que operan en diferentes roles funcionales. Estas comunidades de usuarios realizan diferentes tareas y funciones de oficina utilizando diversos recursos que usted proporciona a través de dispositivos de usuario. Los usuarios pueden trabajar desde casa o en oficinas remotas utilizando los dispositivos móviles que usted les proporciona. O bien, los usuarios pueden ser propietarios de sus propios dispositivos

móviles, lo que les permite acceder a herramientas que están sujetas a ciertas reglas de cumplimiento de seguridad.

A medida que más comunidades de usuarios empiezan a utilizar dispositivos móviles en sus funciones laborales, la gestión de la movilidad empresarial (EMM) se vuelve fundamental para evitar fugas de datos. La EMM también es crucial para aplicar las restricciones de seguridad de una organización. Para una gestión de dispositivos móviles más eficiente y sofisticada, puede categorizar sus comunidades de usuarios. Esto simplifica la asignación de usuarios a los recursos y alinea las políticas de seguridad adecuadas con los usuarios.

El siguiente ejemplo ilustra cómo se clasifican las comunidades de usuarios de una organización sanitaria para la EMM.

Caso de uso de comunidades de usuarios

Esta organización sanitaria de ejemplo proporciona recursos tecnológicos y acceso a muchos usuarios, incluidos empleados de la red y afiliados, y voluntarios. La organización ha optado por implementar la solución EMM solo para usuarios no ejecutivos.

Las funciones y roles de los usuarios de esta organización se pueden dividir en subgrupos que incluyen: clínicos, no clínicos y contratistas. Los usuarios seleccionados reciben dispositivos móviles corporativos, mientras que otros pueden acceder a recursos limitados de la empresa desde sus dispositivos personales. Para aplicar el nivel adecuado de restricciones de seguridad y evitar fugas de datos, la organización decidió que el departamento de TI corporativo gestionara cada dispositivo inscrito. Esos dispositivos pueden ser propiedad de la empresa o Bring Your Own Device (BYOD). Además, los usuarios solo pueden inscribir un único dispositivo.

La siguiente sección proporciona una descripción general de los roles y funciones de cada subgrupo:

CLÍNICO

- Enfermeros/as
- Médicos (doctores, cirujanos, etc.)
- Especialistas (dietistas, anestesiólogos, radiólogos, cardiólogos, oncólogos, etc.)
- Médicos externos (médicos no empleados y personal de oficina que trabaja desde oficinas remotas)
- Servicios de atención domiciliaria (personal de oficina y móvil que presta servicios médicos en visitas a domicilio de pacientes)

- Especialista en investigación (trabajadores del conocimiento y usuarios avanzados en seis institutos de investigación que realizan investigación clínica para encontrar respuestas a problemas en medicina)
- Educación y formación (enfermeros, médicos y especialistas en educación y formación)

NO CLÍNICO

- Servicios Compartidos (Trabajadores de oficina que realizan diversas funciones administrativas, incluyendo RRHH, Nóminas, Cuentas por Pagar y Servicio de Cadena de Suministro)
- Servicios Médicos (Trabajadores de oficina que realizan diversas funciones de gestión sanitaria, servicios administrativos y soluciones de procesos de negocio para proveedores, incluyendo: Servicios Administrativos, Análisis e Inteligencia de Negocio, Sistemas de Negocio, Servicios al Cliente, Finanzas, Administración de Atención Gestionada, Soluciones de Acceso al Paciente, Soluciones de Ciclo de Ingresos, y así sucesivamente)
- Servicios de Soporte (Trabajadores de oficina que realizan diversas funciones no clínicas, incluyendo: Administración de Beneficios, Integración Clínica, Comunicaciones, Compensación y Gestión del Rendimiento, Servicios de Instalaciones y Propiedades, Sistemas de Tecnología de RRHH, Servicios de Información, Auditoría Interna y Mejora de Procesos, y así sucesivamente)
- Programas Filantrópicos (Trabajadores de oficina y móviles que realizan diversas funciones en apoyo de programas filantrópicos)

CONTRATISTAS

- Socios fabricantes y proveedores (En el sitio y conectados remotamente a través de VPN de sitio a sitio, proporcionando diversas funciones de soporte no clínico)

Basándose en la información anterior, la organización creó las siguientes entidades. Para obtener más información sobre los grupos de entrega en Citrix Endpoint Management, consulte Implementar recursos.

UNIDADES ORGANIZATIVAS (OU) Y GRUPOS DE ACTIVE DIRECTORY

Para la OU **=** Recursos de Citrix Endpoint Management:

- OU = Clínica; Grupos =
    - XM-Nurses
    - XM-Physicians
    - XM-Specialists

    - XM-Outside Physicians
    - XM-Home Health Services
    - XM-Especialista en investigación
    - XM-Educación y formación
- OU = No clínico; Grupos =
    - XM-Servicios compartidos
    - XM-Servicios médicos
    - XM-Servicios de soporte
    - XM-Programas filantrópicos

USUARIOS Y GRUPOS LOCALES DE CITRIX ENDPOINT MANAGEMENT

Para Grupo= Contratistas, Usuarios =

- Proveedor1
- Proveedor2
- Proveedor 3
- … Proveedor 10

GRUPOS DE ENTREGA DE CITRIX ENDPOINT MANAGEMENT

- Clínico-Enfermeros
- Clínico-Médicos
- Clínico-Especialistas
- Clínico-Médicos externos
- Clínico-Servicios de salud a domicilio
- Clínico-Especialista en investigación
- Clínico-Educación y formación
- No clínico-Servicios compartidos
- No clínico-Servicios médicos
- No clínico-Servicios de soporte
- No clínico-Programas filantrópicos

ASIGNACIÓN DE GRUPOS DE ENTREGA Y GRUPOS DE USUARIOS

GRUPOS DE ACTIVE DIRECTORY	GRUPOS DE ENTREGA DE CITRIX ENDPOINT MANAGEMENT
XM-Enfermeros	Clínico-Enfermeros
XM-Médicos	Clinical-Médicos
XM-Especialistas	Clinical-Especialistas
XM-Médicos externos	Clinical-Médicos externos
XM-Servicios de salud a domicilio	Clinical-Servicios de salud a domicilio
XM-Especialista en investigación	Clinical-Especialista en investigación
XM-Educación y formación	Clinical-Educación y formación
XM-Servicios compartidos	Non-Clinical-Servicios compartidos
XM-Servicios médicos	Servicios no clínicos para médicos
XM-Servicios de soporte	Servicios de soporte no clínicos
XM-Programas filantrópicos	Programas filantrópicos no clínicos

ASIGNACIÓN DE GRUPOS DE ENTREGA Y RECURSOS

Las siguientes tablas ilustran los recursos asignados a cada grupo de entrega en este caso de uso. La primera tabla muestra las asignaciones de aplicaciones móviles. La segunda tabla muestra la aplicación pública, las aplicaciones HDX y los recursos de administración de dispositivos.

GRUPOS DE ENTREGA DE CITRIX ENDPOINT MANAGEMENT	APLICACIONES MÓVILES DE CITRIX	APLICACIONES MÓVILES PÚBLICAS	APLICACIONES MÓVILES HDX
Clínico-Enfermeros	X		
Clínico-Médicos			
Clínico-Especialistas			

GRUPOS DE ENTREGA DE CITRIX ENDPOINT MANAGEMENT	APLICACIONES MÓVILES DE CITRIX	APLICACIONES MÓVILES PÚBLICAS	APLICACIONES MÓVILES HDX
Clínico - Médicos externos	X		
Clínico - Servicios de atención domiciliaria	X		
Clínico - Especialista en investigación	X		
Clínico - Educación y formación		X	X
No clínico - Servicios compartidos		X	X
No clínico - Servicios médicos		X	X
Servicios de soporte no clínicos	X	X	X
Programas filantrópicos no clínicos	X	X	X
Contratistas	X	X	X

GRUPOS DE ENTREGA DE CITRIX ENDPOINT MANAGEMENT	APLICACIÓN PÚBLICA: RSA SECURID	APLICACIÓN PÚBLICA: EPICCARE HAIKU	APLICACIÓN HDX: EPIC HYPERSPACE	DIRECTIVA DE CÓDIGO DE ACCESO	RESTRICCIONES DE DISPOSITIVO	ACCIONES AUTOMATIZADAS	DIRECTIVA DE RED
Clínico-Enfermeras							X
Clínico-Médicos					X		
Clínico-Especialistas							
Clínico-Médicos externos							
Clínico-Servicios de salud a domicilio							
Clínico-Especialista en investigación							
Clínico-Educación y formación		X	X				

GRUPOS DE ENTREGA DE CITRIX ENDPOINT MANAGEMENT	APLICACIÓN PÚBLICA: RSA SECURID	APLICACIÓN PÚBLICA: EPICCARE HAIKU	APLICACIÓN HDX: EPIC HYPERSPACE	DIRECTIVA DE CÓDIGO DE ACCESO	RESTRICCIONES DE DISPOSITIVO	ACCIONES AUTOMATIZADAS	DIRECTIVA DE RED
Servicios compartidos no clínicos		X	X				
Servicios médicos no clínicos		X	X				
Servicios de soporte no clínicos		X	X				

NOTAS Y CONSIDERACIONES

- Citrix Endpoint Management crea un grupo de entrega predeterminado llamado Todos los usuarios durante la configuración inicial. Si no inhabilita este grupo de entrega, todos los usuarios de Active Directory tienen derecho a inscribirse en Citrix Endpoint Management.
- Citrix Endpoint Management sincroniza los usuarios y grupos de Active Directory a petición mediante una conexión dinámica al servidor LDAP.
- Si un usuario forma parte de un grupo que no está asignado en Citrix Endpoint Management, ese usuario no puede inscribirse. Del mismo modo, si un usuario es miembro de muchos grupos, Citrix Endpoint Management solo lo clasifica como parte de los grupos asignados a Citrix Endpoint Management.

Requisitos de seguridad

El alcance de las consideraciones de seguridad relacionadas con un entorno de Citrix Endpoint Management puede volverse rápidamente abrumador. Hay muchas piezas y configuraciones interconectadas. Es posible que no sepa por dónde empezar o qué elegir para asegurarse de que haya un nivel de protección aceptable disponible. Para simplificar estas elecciones, Citrix ofrece recomendaciones para seguridad Alta, Superior y Máxima, como se describe en la siguiente tabla.

Las preocupaciones de seguridad no son la única consideración para el modo en que se inscriben sus dispositivos: MAM, MDM+MAM con MDM opcional o MDM+MAM con MDM obligatorio. También es importante revisar los requisitos del caso de uso y decidir si puede mitigar los problemas de seguridad antes de elegir su modo de administración.

Alta: El uso de esta configuración proporciona una experiencia de usuario óptima a la vez que mantiene un nivel básico de seguridad aceptable para la mayoría de las organizaciones.

Superior: Esta configuración crea un equilibrio más sólido entre seguridad y facilidad de uso.

Máxima: Seguir estas recomendaciones proporciona un alto nivel de seguridad a costa de la facilidad de uso y la adopción por parte del usuario.

Consideraciones de seguridad del modo de administración

La siguiente tabla especifica los modos de administración para cada nivel de seguridad.

SEGURIDAD ALTA	SEGURIDAD SUPERIOR	SEGURIDAD MÁXIMA
MAM, MDM+MAM	MDM+MAM	MDM+MAM

Notas:

- Según el caso de uso, una implementación solo de MAM puede cumplir los requisitos de seguridad y proporcionar una buena experiencia de usuario.
- Para casos de uso como BYOD en los que todos los requisitos empresariales y de seguridad pueden satisfacerse solo con la contenedorización de aplicaciones, Citrix recomienda el modo solo MAM.
- Para entornos de alta seguridad (y dispositivos corporativos), Citrix recomienda MDM+MAM para aprovechar todas las capacidades de seguridad disponibles.

Consideraciones de seguridad de Citrix ADC y NetScaler Gateway

La siguiente tabla especifica las recomendaciones de Citrix ADC y NetScaler Gateway para cada nivel de seguridad.

SEGURIDAD ALTA	SEGURIDAD MÁS ALTA	SEGURIDAD MÁXIMA
Se recomienda Citrix ADC. NetScaler Gateway es necesario para MAM y MDM+MAM.	NetScaler estándar para la configuración del asistente de XenMobile con puente SSL si Citrix Endpoint Management está en la DMZ.	Descarga SSL con cifrado de extremo a extremo

Notas:

- Exponer el servidor de Citrix Endpoint Management a Internet a través de NAT o de proxies/ equilibradores de carga de terceros existentes podría ser una opción para MDM. Sin embargo, en ese caso, el tráfico SSL termina en un servidor de Citrix Endpoint Management, lo que supone un riesgo de seguridad potencial.
- Para entornos de alta seguridad, NetScaler Gateway con la configuración predeterminada de Citrix Endpoint Management normalmente cumple o supera los requisitos de seguridad.
- Para inscripciones de MDM con las más altas necesidades de seguridad, la terminación SSL en NetScaler Gateway le permite inspeccionar el tráfico en el perímetro, manteniendo el cifrado SSL de extremo a extremo.
- Opciones para definir cifrados SSL/TLS.
- Para obtener más información, consulte Integración con NetScaler Gateway y Citrix ADC.

Consideraciones de seguridad de la inscripción

La siguiente tabla especifica las recomendaciones de Citrix ADC y NetScaler Gateway para cada nivel de seguridad.

SEGURIDAD ALTA	SEGURIDAD MÁS ALTA	SEGURIDAD MÁXIMA
Solo pertenencia a grupos de Active Directory. Grupo de entrega de todos los usuarios inhabilitado.	Modo de seguridad de inscripción solo por invitación. Solo pertenencia a grupos de Active Directory. Grupo de entrega de todos los usuarios inhabilitado	Modo de seguridad de inscripción vinculado al ID de dispositivo. Solo pertenencia a grupos de Active Directory. Grupo de entrega de todos los usuarios inhabilitado

Notas:

- Citrix generalmente recomienda que restrinja la inscripción solo a los usuarios de grupos de Active Directory predefinidos. Esta restricción requiere inhabilitar el grupo de entrega integrado de todos los usuarios.
- Puede usar invitaciones de inscripción para restringir la inscripción a usuarios con una invitación. Las invitaciones de inscripción no están disponibles para dispositivos Windows.
- Puede usar invitaciones de inscripción con PIN de un solo uso (OTP) como solución de autenticación de dos factores y para controlar el número de dispositivos que un usuario puede inscribir. (Las invitaciones OTP no están disponibles para dispositivos Windows).

Consideraciones de seguridad del código de acceso del dispositivo

La siguiente tabla especifica las recomendaciones de código de acceso del dispositivo para cada nivel de seguridad.

SEGURIDAD ALTA	SEGURIDAD MÁS ALTA	SEGURIDAD MÁXIMA
Recomendado. Se requiere seguridad alta para el cifrado a nivel de dispositivo. Se puede aplicar con MDM. Se puede establecer como obligatorio solo para MAM mediante la directiva MDX, Comportamiento de dispositivo no conforme.	Aplicado mediante una directiva MDM, MAM o MDM+MAM.	Aplicado mediante una directiva MDM y MDX. Directiva de código de acceso complejo de MDM.

Notas:

- Citrix recomienda el uso de un código de acceso para el dispositivo.
- Puede aplicar un código de acceso para el dispositivo mediante una directiva MDM.
- Puede utilizar una directiva MDX para que un código de acceso del dispositivo sea un requisito para usar aplicaciones administradas; por ejemplo, para casos de uso de BYOD.
- Citrix recomienda combinar las opciones de directivas MDM y MDX para aumentar la seguridad en las inscripciones de MDM+MAM.

- Para entornos con los requisitos de seguridad más altos, puede configurar directivas de código de acceso complejas y aplicarlas con MDM. Puede configurar acciones automáticas para notificar a los administradores o emitir borrados selectivos/completos del dispositivo cuando un dispositivo no cumple una directiva de código de acceso.

Aplicaciones

La gestión de la movilidad empresarial (EMM) se divide en gestión de dispositivos móviles (MDM) y gestión de aplicaciones móviles (MAM). Mientras que MDM permite a las organizaciones proteger y controlar los dispositivos móviles, MAM ayuda con la entrega y gestión de aplicaciones. Con la creciente adopción de BYOD, normalmente puede implementar una solución MAM, como Citrix Endpoint Management. Citrix Endpoint Management ayuda con la entrega de aplicaciones, las licencias de software, la configuración y la gestión del ciclo de vida de las aplicaciones. Puede exigir o permitir que los usuarios también opten por la gestión MDM.

Con Citrix Endpoint Management, protege las aplicaciones configurando directivas MAM y ajustes de VPN para evitar fugas de datos y otras amenazas de seguridad. Citrix Endpoint Management ofrece a las organizaciones la flexibilidad de inscribir dispositivos solo como MAM o como MDM+MAM.

Además de la capacidad de entregar aplicaciones a dispositivos móviles, Citrix Endpoint Management ofrece la contenedorización de aplicaciones a través de la tecnología MDX. Las aplicaciones están sujetas a controles granulares basados en directivas. Los proveedores de software independientes (ISV) pueden aplicar estos controles mediante el SDK de aplicaciones móviles.

En un entorno corporativo, los usuarios utilizan varias aplicaciones móviles para ayudarles en su función laboral. Las aplicaciones pueden incluir aplicaciones de la tienda de aplicaciones pública, aplicaciones desarrolladas internamente o aplicaciones nativas. Citrix Endpoint Management clasifica estas aplicaciones de la siguiente manera:

- **Aplicaciones públicas:** Estas aplicaciones incluyen aplicaciones gratuitas o de pago disponibles en una tienda de aplicaciones pública, como Apple App Store o Google Play. Los proveedores externos a la organización suelen poner sus aplicaciones a disposición en las tiendas de aplicaciones públicas. Esta opción permite a sus clientes descargar las aplicaciones directamente desde Internet. Es posible que utilice muchas aplicaciones públicas en su organización, según las necesidades de los usuarios. Ejemplos de estas aplicaciones incluyen GoToMeeting, Salesforce y las aplicaciones EpicCare.

  - **Si utiliza el SDK de MAM:** Obtenga los binarios de la aplicación de su proveedor de aplicaciones. Luego, integre el SDK de MAM en la aplicación.
  - **Si utiliza MDX Toolkit:** Citrix® no admite la descarga de binarios de aplicaciones directamente desde tiendas de aplicaciones públicas y su posterior empaquetado con MDX Toolkit para la distribución empresarial. Para empaquetar aplicaciones de terceros, trabaje con su proveedor de aplicaciones para obtener los binarios de la aplicación. A continuación, puede empaquetar los binarios mediante MDX Toolkit.

- **Aplicaciones internas:** Muchas organizaciones tienen desarrolladores internos que crean aplicaciones que proporcionan funcionalidades específicas y se desarrollan y distribuyen de forma independiente dentro de la organización. En algunos casos, algunas organizaciones también pueden tener aplicaciones proporcionadas por ISV. Puede implementar estas aplicaciones como aplicaciones nativas o puede contenedorizar las aplicaciones mediante una solución MAM, como Citrix Endpoint Management.

  Por ejemplo, una organización sanitaria podría crear una aplicación interna que permita a los médicos ver la información del paciente en dispositivos móviles. Una organización puede entonces proteger la información del paciente y habilitar el acceso VPN a la base de datos de pacientes utilizando una de las siguientes opciones:

  - SDK de MAM
  - MDX Toolkit

- **Aplicaciones web y SaaS:** Estas aplicaciones incluyen aplicaciones a las que se accede desde una red interna (aplicaciones web) o a través de una red pública (SaaS). Citrix Endpoint Management también le permite crear aplicaciones web y SaaS personalizadas utilizando una lista de conectores de aplicaciones. Estos conectores de aplicaciones pueden facilitar el inicio de sesión único (SSO) a las aplicaciones web existentes. Para obtener más información, consulte (/es-es/citrix-endpoint-management/apps/app-connector-types.html). Por ejemplo, puede utilizar SAML de Google Apps para SSO basado en Security Assertion Markup Language (SAML) para Google Apps.
- **Aplicaciones de productividad móvil:** Las aplicaciones de productividad móvil son aplicaciones desarrolladas por Citrix que se incluyen con la licencia de Citrix Endpoint Management. Para obtener más información, consulte Acerca de las aplicaciones de productividad móvil. Citrix también ofrece otras aplicaciones listas para la empresa que los ISV desarrollan mediante el SDK de aplicaciones móviles.

- **Aplicaciones HDX:** Las aplicaciones HDX son aplicaciones alojadas en Windows que se publican con StoreFront. Si utiliza Citrix Virtual Apps and Desktops y Citrix Workspace, las aplicaciones HDX están disponibles para los usuarios inscritos.

Según el tipo de aplicaciones móviles que planee implementar y administrar con Citrix Endpoint Management, la configuración subyacente podría diferir. Por ejemplo, muchos grupos de usuarios con diferentes niveles de permisos podrían consumir una sola aplicación. En ese caso, puede crear grupos de entrega separados para implementar dos versiones distintas de la misma aplicación. Además, debe asegurarse de que la pertenencia a grupos de usuarios sea mutuamente excluyente para evitar incoherencias de directivas en los dispositivos de los usuarios.

También puede administrar las licencias de aplicaciones iOS mediante Apple Volume Purchase. Esta opción requiere que se registre en el programa Volume Purchase y que configure los ajustes de Volume Purchase en la consola de Citrix Endpoint Management. Esa configuración le permite distribuir las aplicaciones con las licencias de Volume Purchase. Varios casos de uso hacen que sea importante evaluar y planificar su estrategia de MAM antes de implementar el entorno de Citrix Endpoint Management. Puede empezar a planificar su estrategia de MAM definiendo lo siguiente:

- **Tipos de aplicaciones:** Enumere los diferentes tipos de aplicaciones que planea admitir y clasifíquelas, como aplicaciones públicas, nativas, web, internas o de ISV. Además, clasifique las aplicaciones para diferentes plataformas de dispositivos, como iOS y Android. Esta categorización ayuda a alinear las diversas configuraciones de Citrix Endpoint Management que se requieren para cada tipo de aplicación. Por ejemplo, algunas aplicaciones podrían requerir el uso del SDK de aplicaciones móviles para habilitar API especiales para la interacción con otras aplicaciones.
- **Requisitos de red:** Configure los ajustes de las aplicaciones que tienen requisitos específicos de acceso a la red. Por ejemplo, ciertas aplicaciones podrían necesitar acceso a su red interna a través de una VPN. Algunas aplicaciones podrían requerir acceso a Internet para enrutar el acceso a través de la DMZ. Para permitir que dichas aplicaciones se conecten a la red requerida, debe configurar varios ajustes en consecuencia. La definición de los requisitos de red por aplicación ayuda a completar sus decisiones arquitectónicas de forma temprana, lo que agiliza el proceso general de implementación.
- **Requisitos de seguridad:** Puede definir requisitos de seguridad para aplicar a aplicaciones individuales o a todas las aplicaciones.
    - Los ajustes, como las directivas MDX, se aplican a aplicaciones individuales
    - Los ajustes de sesión y autenticación se aplican a todas las aplicaciones

- Algunas aplicaciones podrían tener requisitos específicos de contenedorización, MDX, autenticación, geocercado, código de acceso o uso compartido de datos

Describa esos requisitos con antelación para simplificar su implementación. Para obtener más información sobre la seguridad en Citrix Endpoint Management, consulte Seguridad y experiencia del usuario.

- **Requisitos de implementación:** Es posible que desee utilizar una implementación basada en directivas para permitir que solo los usuarios conformes descarguen las aplicaciones publicadas. Por ejemplo, ciertas aplicaciones pueden requerir que el dispositivo esté administrado o que cumpla con una versión mínima del sistema operativo. También es posible que desee que ciertas aplicaciones estén disponibles solo para usuarios corporativos. Describa estos requisitos con antelación para poder configurar las reglas o acciones de implementación adecuadas.
- **Requisitos de licencias:** Mantenga un registro de los requisitos de licencias relacionados con las aplicaciones. Sus notas pueden ayudarle a administrar el uso de licencias de manera efectiva y a decidir si configurar funciones específicas en Citrix Endpoint Management para facilitar las licencias. Por ejemplo, si implementa una aplicación iOS gratuita o de pago, Apple impone requisitos de licencia en la aplicación. Como resultado, los usuarios deben iniciar sesión en su cuenta de Apple App Store.

  Sin embargo, puede registrarse en Apple Volume Purchase para distribuir y administrar estas aplicaciones mediante Citrix Endpoint Management. Volume Purchase permite a los usuarios descargar las aplicaciones sin tener que iniciar sesión en su cuenta de Apple App Store.

  Algunas plataformas tienen requisitos de licencia especiales que deben completarse antes de implementar esas funciones.
- **Requisitos de listas de permitidos y bloqueados:** Puede identificar aplicaciones que no desea que los usuarios instalen o utilicen. La creación de una lista de bloqueados define un evento de incumplimiento. Luego puede configurar directivas para que se activen cuando ocurra el evento. Por otro lado, una aplicación podría ser aceptable para su uso, pero podría caer en la lista de bloqueados por alguna razón. En ese caso, puede agregar la aplicación a una lista de permitidos e indicar que la aplicación es aceptable para usar, pero no es obligatoria. Además, tenga en cuenta que las aplicaciones preinstaladas en dispositivos nuevos pueden incluir algunas aplicaciones de uso común que no forman parte del sistema operativo. Dichas aplicaciones pueden entrar en conflicto con su estrategia de lista de bloqueados.

Caso de uso

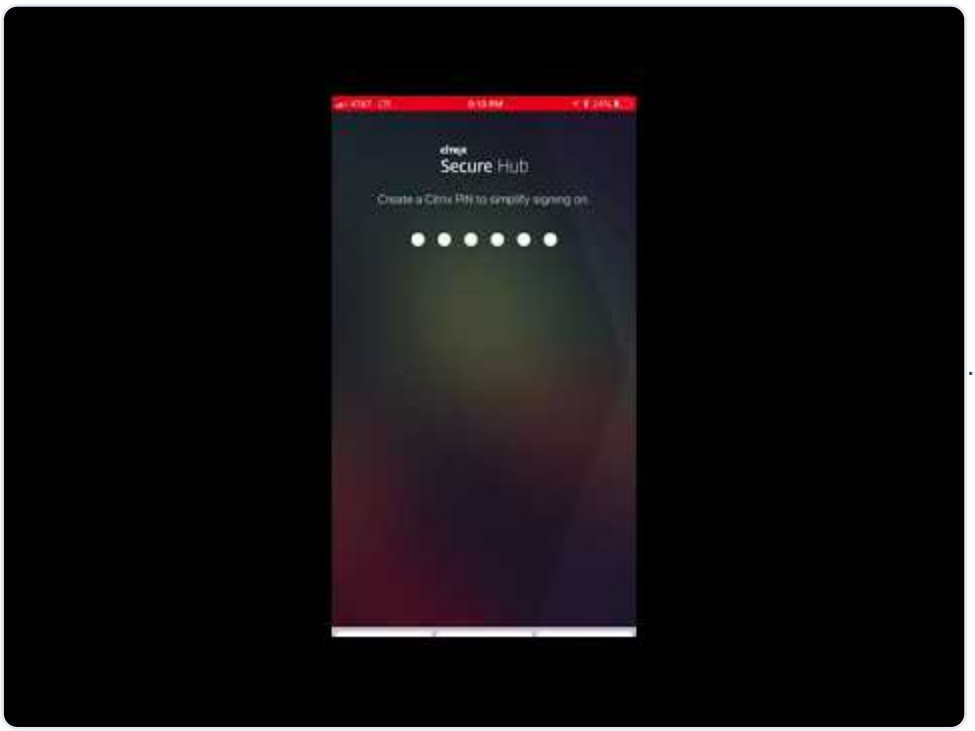
Una organización sanitaria planea implementar Citrix Endpoint Management para que sirva como solución MAM para sus aplicaciones móviles. Las aplicaciones móviles se entregan a usuarios corporativos y BYOD. TI decide entregar y administrar las siguientes aplicaciones:

Aplicaciones de productividad móvil: Aplicaciones iOS y Android proporcionadas por Citrix. Para obtener más información, consulte Aplicaciones de productividad móvil.

Citrix Secure Hub: Para clientes que se incorporaron antes de Citrix Endpoint Management 10.18.14: Puede enviar configuraciones de seguridad, configuraciones y aplicaciones móviles a dispositivos móviles mediante Citrix Secure Hub. Los dispositivos Android e iOS se inscriben en Citrix Endpoint Management a través de Citrix Secure Hub.

Para nuevos clientes a partir de Citrix Endpoint Management 10.18.14: Citrix Secure Hub admite el uso de la tienda de aplicaciones de Workspace. Al abrir Citrix Secure Hub, los usuarios ya no ven la tienda de Citrix Secure Hub. Ahora, un botón de Agregar aplicaciones lleva a los usuarios a la tienda de aplicaciones de Workspace.

A continuación, se muestra un vídeo que muestra un dispositivo iOS realizando una inscripción en Citrix Endpoint Management mediante la aplicación Citrix Workspace.



Citrix Workspace app: La aplicación Citrix Workspace incorpora la tecnología existente de Citrix Receiver, Citrix Secure Hub y otras tecnologías de cliente de Citrix Workspace. La aplicación Citrix Workspace proporciona a los usuarios finales una experiencia unificada y contextual.

GoToMeeting: Un cliente de reuniones en línea, uso compartido de escritorio y videoconferencias que permite a los usuarios reunirse con otros usuarios de equipos, clientes o colegas a través de Internet en tiempo real.

SalesForce1: Salesforce1 permite a los usuarios acceder a Salesforce desde dispositivos móviles y reúne todas las aplicaciones de Chatter, CRM, aplicaciones personalizadas y procesos de negocio en una experiencia unificada para cualquier usuario de Salesforce.

RSA SecurID: Token basado en software para autenticación de dos factores.

Aplicaciones EpicCare: Estas aplicaciones proporcionan a los profesionales de la salud acceso seguro y portátil a los historiales de pacientes, listas de pacientes, programaciones y mensajería.

Haiku: Aplicación móvil para iPhone y teléfonos Android.

Canto: Aplicación móvil para iPad

Rover: Aplicaciones móviles para iPhone y iPad.

HDX: Estas aplicaciones se entregan a través de Citrix Virtual Apps en Citrix Workspace.

- **Epic Hyperspace:** Aplicación cliente de Epic para la gestión de registros médicos electrónicos.

ISV:

- **Vocera:** Aplicación móvil de mensajería y voz sobre IP compatible con HIPAA que extiende los beneficios de la tecnología de voz de Vocera en cualquier momento y lugar a través de smartphones iPhone y Android.

Aplicaciones internas:

- **HCMail:** Aplicación que ayuda a redactar mensajes cifrados, buscar libretas de direcciones en servidores de correo internos y enviar los mensajes cifrados a los contactos utilizando un cliente de correo electrónico.

Aplicaciones web internas:

- **PatientRounding:** Aplicación web utilizada para registrar información de salud del paciente por diferentes departamentos.
- **Outlook Web Access:** Permite el acceso al correo electrónico a través de un navegador web.
- **SharePoint:** Se utiliza para compartir archivos y datos en toda la organización.

La siguiente tabla enumera la información básica necesaria para la configuración de MAM.

NOMBRE DE LA APLICACIÓN	TIPO DE APLICACIÓN	COMPATIBLE CON MDX	IOS	ANDROID
Citrix Secure Mail	Aplicación de productividad móvil	No	Sí	Sí
Citrix Secure Web	Aplicación de productividad móvil	No	Sí	Sí
Citrix Files	Aplicación de productividad móvil	No	Sí	Sí
Citrix Secure Hub	Aplicación pública	N/D	Sí	Sí
Aplicación Citrix Workspace	Aplicación pública	N/D	Sí	Sí
GoToMeeting	Aplicación pública	N/D	Sí	Sí
SalesForce1	Aplicación pública	N/D	Sí	Sí
RSA SecurID	Aplicación pública	N/D	Sí	Sí
Epic Haiku	Aplicación pública	N/D	Sí	Sí
Epic Canto	Aplicación pública	N/D	Sí	No
Epic Rover	Aplicación pública	N/D	Sí	No
Epic Hyperspace	Aplicación HDX	N/D	Sí	Sí
Vocera	Aplicación ISV	Sí	Sí	Sí

NOMBRE DE LA APLICACIÓN	TIPO DE APLICACIÓN	COMPATIBLE CON MDX	IOS	ANDROID
HCMail	Aplicación interna	Sí	Sí	Sí
PatientRounding	Aplicación web	N/D	Sí	Sí
Acceso web de Outlook	Aplicación web	N/A	Sí	Sí
SharePoint	Aplicación web	N/A	Sí	Sí

La siguiente tabla enumera los requisitos específicos que puede consultar al configurar las directivas MAM en Citrix Endpoint Management.

NOMBRE DE LA APLICACIÓN	VPN NECESARIA	INTERACCIÓN (CON APLICACIONES FUERA DEL CONTENEDOR)	INTERACCIÓN (DESDE APLICACIONES FUERA DEL CONTENEDOR)	FILTRADO DE PROXY	LICENCIAS	GEOCERCADO	SDK DE APLICACIONES MÓVILES	VERSIÓN MÍNIMA DEL SISTEMA OPERATIVO
Citrix Secure Mail	Sí	Permitido selectivamente	Permitido	Obligatorio	N/D	Obligatorio selectivamente	N/D	Aplicado
Citrix Secure Web	Sí	Permitido	Permitido	Obligatorio	N/A	No obligatorio	N/A	Aplicado

NOMBRE DE LA APLICACIÓN	VPN NECESARIA	INTERACCIÓN (CON APLICACIONES FUERA DEL CONTENEDOR)	INTERACCIÓN (DESDE APLICACIONES FUERA DEL CONTENEDOR)	FILTRADO DE PROXY	LICENCIAS	GEOCERCADO	SDK DE APLICACIONES MÓVILES	VERSIÓN MÍNIMA DEL SISTEMA OPERATIVO
Citrix Files	Sí	Permitido	Permitido	Obligatorio	N/A	No obligatorio	N/D	Aplicado
Citrix Secure Hub	Sí	N/D	N/D	No requerido	Compra por volumen	No requerido	N/D	No aplicado
Aplicación Citrix Workspace	Sí	N/D	N/D	No requerido	Compra por volumen	No requerido	N/A	No aplicado
GoTo Meeting	N	N/A	N/A	No requerido	Compra por volumen	No requerido	N/A	No aplicado
Sales Force 1	N	N/A	N/A	No necesario	Compra por volumen	No necesario	N/A	No aplicado
RSA SecurID	N	N/A	N/A	No necesario	Compra por volumen	No necesario	N/D	No aplicado

NOMBRE DE LA APLICACIÓN	VPN NECESARIA	INTERACCIÓN (CON APLICACIONES FUERA DEL CONTENEDOR)	INTERACCIÓN (DESDE APLICACIONES FUERA DEL CONTENEDOR)	FILTRADO DE PROXY	LICENCIAS	GEOCERCADO	SDK DE APLICACIONES MÓVILES	VERSIÓN MÍNIMA DEL SISTEMA OPERATIVO
Epic Haiku	Sí	N/D	N/D	No requerido	Compra por volumen	No requerido	N/D	No aplicado
Epic Canto	Sí	N/D	N/D	No requerido	Compra por volumen	No requerido	N/D	No exigido
Epic Rover	Sí	N/D	N/D	No requerido	Compra por volumen	No requerido	N/D	No exigido
Epic Hyperspace	Sí	N/A	N/A	No requerido	N/A	No requerido	N/A	No aplicado
Vocera	Sí	Bloqueado	Bloqueado	Requerido	N/A	Requerido	Obligatorio	Aplicado
HCMail	Sí	Bloqueado	Bloqueado	Obligatorio	N/D	Obligatorio	Obligatorio	Aplicado
PatientRound-ing	Sí	N/D	N/D	Obligatorio	N/D	No obligatorio	N/D	No aplicado

NOMBRE DE LA APLICACIÓN	VPN NECESARIA	INTERACCIÓN (CON APLICACIONES FUERA DEL CONTENEDOR)	INTERACCIÓN (DESDE APLICACIONES FUERA DEL CONTENEDOR)	FILTRADO DE PROXY	LICENCIAS	GEOCERCADO	SDK DE APLICACIONES MÓVILES	VERSIÓN MÍNIMA DEL SISTEMA OPERATIVO
Outlook Web Access	Sí	N/D	N/D	Obligatorio	N/D	No obligatorio	N/D	No aplicado
Share Point	Sí	N/A	N/A	Obligatorio	N/A	No obligatorio	N/A	No exigido

Comunidades de usuarios

Cada organización consta de diversas comunidades de usuarios que operan en diferentes roles funcionales. Estas comunidades de usuarios realizan diferentes tareas y funciones de oficina utilizando varios recursos que usted proporciona a través de dispositivos móviles de usuario. Los usuarios pueden trabajar desde casa o en oficinas remotas utilizando los dispositivos móviles que usted proporciona. O bien, los usuarios pueden usar dispositivos móviles personales, lo que les permite acceder a herramientas sujetas a ciertas reglas de cumplimiento de seguridad.

Con más comunidades de usuarios que utilizan dispositivos móviles, la Administración de la movilidad empresarial (EMM) se vuelve fundamental para evitar una fuga de datos y para aplicar restricciones de seguridad organizativas. Para una Administración de dispositivos móviles más eficiente y sofisticada, puede categorizar sus comunidades de usuarios. Esto simplifica la asignación de usuarios a los recursos y garantiza que las políticas de seguridad correctas se apliquen a los usuarios adecuados.

La categorización de las comunidades de usuarios puede incluir el uso de los siguientes componentes:

- Unidades organizativas (OU) y grupos de Active Directory

Los usuarios agregados a grupos de seguridad específicos de Active Directory pueden recibir directivas y recursos, como aplicaciones. Al eliminar usuarios de los grupos de seguridad de Active Directory, se elimina el acceso a los recursos de Citrix Endpoint Management permitidos anteriormente.

- Usuarios y grupos locales de Citrix Endpoint Management

  Para los usuarios que no tienen una cuenta en Active Directory, puede crearlos como usuarios locales de Citrix Endpoint Management. Puede agregar usuarios locales a grupos de entrega y aprovisionarles recursos de la misma manera que a los usuarios de Active Directory.

- Grupos de entrega de Citrix Endpoint Management

  Si muchos grupos de usuarios con diferentes niveles de permisos van a consumir una sola aplicación, es posible que desee crear grupos de entrega separados. Con grupos de entrega separados, puede implementar dos versiones distintas de la misma aplicación. Citrix® recomienda crear grupos de entrega antes de crear directivas de dispositivo.

- Asignación de grupos de entrega y grupos de usuarios

  Las asignaciones de grupos de entrega a grupos de Active Directory pueden ser uno a uno o uno a varios. Asigne directivas y aplicaciones base a una asignación de grupo de entrega de uno a varios. Asigne directivas y aplicaciones específicas de la función a asignaciones de grupo de entrega uno a uno.

- Asignación de grupos de entrega y recursos de aplicaciones

  Asigne aplicaciones específicas a cada grupo de entrega.

- Asignación de grupos de entrega y recursos de MDM

  Asigne aplicaciones y recursos específicos de administración de dispositivos a cada grupo de entrega. Por ejemplo, configure un grupo de entrega con cualquier combinación de lo siguiente: Tipos de aplicaciones (públicas, HDX™, etc.), aplicaciones específicas por tipo de aplicación y recursos como directivas de dispositivo y acciones automatizadas.

El siguiente ejemplo ilustra cómo se clasifican las comunidades de usuarios de una organización sanitaria para EMM.

Caso de uso

Esta organización sanitaria de ejemplo proporciona recursos tecnológicos y acceso a muchos usuarios, incluidos empleados de red y afiliados, y voluntarios. La organización ha optado por implementar la solución EMM solo para usuarios no ejecutivos.

Puede dividir los roles y funciones de los usuarios de esta organización en subgrupos que incluyen: personal clínico, no clínico y contratistas. Un conjunto seleccionado de usuarios recibe dispositivos móviles corporativos, mientras que otros pueden acceder a recursos limitados de la empresa desde sus dispositivos personales (BYOD). Para aplicar el nivel adecuado de restricciones de seguridad y evitar fugas de datos, la organización decidió que el departamento de TI corporativo gestiona cada dispositivo inscrito. Además, los usuarios solo pueden inscribir un único dispositivo.

Las siguientes secciones proporcionan una descripción general de los roles y funciones de cada subgrupo.

Clínico

- Enfermeros
- Médicos (doctores, cirujanos, etc.)
- Especialistas (dietistas, anestesiólogos, radiólogos, cardiólogos, oncólogos, etc.)
- Médicos externos (médicos no empleados y trabajadores de oficina que trabajan desde oficinas remotas)
- Servicios de salud a domicilio (trabajadores de oficina y móviles que prestan servicios médicos para visitas a domicilio de pacientes)
- Especialista en investigación (trabajadores del conocimiento y usuarios avanzados en seis institutos de investigación que realizan investigación clínica para encontrar respuestas a problemas en medicina)
- Educación y formación (enfermeros, médicos y especialistas en educación y formación)

No clínico

- Servicios compartidos (Trabajadores de oficina que realizan diversas funciones administrativas, incluyendo: RR. HH., Nóminas, Cuentas por pagar, Servicio de cadena de suministro, y así sucesivamente)
- Servicios para Médicos (Trabajadores de oficina que realizan diversas soluciones de gestión sanitaria, servicios administrativos y procesos de negocio para proveedores, incluyendo: Servicios Administrativos, Análisis e Inteligencia de Negocio, Sistemas de Negocio, Servicios al Cliente, Finanzas, Administración de Atención Gestionada, Soluciones de Acceso al Paciente, Soluciones de Ciclo de Ingresos, y así sucesivamente)
- Servicios de Soporte (Trabajadores de oficina que realizan diversas funciones no clínicas, incluyendo: Administración de Beneficios, Integración Clínica, Comunicaciones, Gestión de Compensaciones y Rendimiento, Servicios de Instalaciones y Propiedades, Sistemas de

Tecnología de RR. HH., Servicios de Información, Auditoría Interna y Mejora de Procesos, y así sucesivamente.)

- Programas Filantrópicos (Trabajadores de oficina y móviles que realizan diversas funciones en apoyo de programas filantrópicos)

Contratistas

- Socios fabricantes y proveedores (Conectados in situ y de forma remota a través de VPN de sitio a sitio, proporcionando diversas funciones de soporte no clínicas)

Basándose en la información anterior, la organización creó las siguientes entidades. Para obtener más información sobre los grupos de entrega en Citrix Endpoint Management, consulte Implementar recursos en la documentación del producto de Citrix Endpoint Management.

Unidades organizativas (OU) y grupos de Active Directory

Para OU = Citrix Endpoint Management Resources

- OU = Clínico; Grupos =
  - XM-Nurses
  - XM-Physicians
  - XM-Specialists
  - XM-Outside Physicians
  - XM-Home Health Services
  - XM-Especialista en investigación
  - XM-Educación y formación
- OU = No clínico; Grupos =
  - XM-Servicios compartidos
  - XM-Servicios médicos
  - XM-Servicios de soporte
  - XM-Programas filantrópicos

Usuarios y grupos locales de Citrix Endpoint Management

Para Grupo= Contratistas, Usuarios =

- Proveedor1
- Proveedor2

- Proveedor 3
- … Proveedor 10

Grupos de entrega de Citrix Endpoint Management

- Clínico-Enfermeras
- Clínico-Médicos
- Clínico-Especialistas
- Clínico-Médicos externos
- Clínico-Servicios de atención domiciliaria
- Clínico-Especialista en investigación
- Clínico-Educación y formación
- No clínico-Servicios compartidos
- No clínico-Servicios médicos
- No clínico-Servicios de soporte
- No clínico-Programas filantrópicos

Asignación de grupos de entrega y grupos de usuarios

GRUPOS DE ACTIVE DIRECTORY	GRUPOS DE ENTREGA DE CITRIX ENDPOINT MANAGEMENT
XM-Enfermeras	Clínico-Enfermeras
XM-Médicos	Clínicos-Médicos
XM-Especialistas	Clínicos-Especialistas
XM-Médicos externos	Clínicos-Médicos externos
XM-Servicios de salud a domicilio	Clínicos-Servicios de salud a domicilio
XM-Especialista en investigación	Clínico-Especialista en investigación
XM-Educación y formación	Clínica-Educación y formación
XM-Servicios compartidos	No clínicos-Servicios compartidos
XM-Servicios médicos	Servicios no clínicos - Médicos

GRUPOS DE ACTIVE DIRECTORY	GRUPOS DE ENTREGA DE CITRIX ENDPOINT MANAGEMENT
Servicios de soporte de XM	Servicios de soporte no clínicos
Programas filantrópicos de XM	Programas filantrópicos no clínicos

Asignación de aplicaciones a grupos de entrega y recursos

	SECURE MAIL	SECURE WEB	CITRIX FILES	APLICACIÓN WORKSPACE	SALESFORCE1	RSA SECURID	EPICCARE HAIKU	EPIC HYPERSPACE
Clínico - Enfermeros	X	X	X					
Clínicos- Médicos								
Clínicos- Especialistas								
Clínicos- Médicos externos	X		X					
Clínicos- Servicios de salud a	X		X					

	SECURE MAIL	SECURE WEB	CITRIX FILES	APLICACIÓN WORKSPACE	SALESFORCE1	RSA SECURID	EPICCARE HAIKU	EPIC HYPERSPACE
domicilio								
Clínicos-Especialista en investigación	X		X					
Clínicos-Educación y formación							X	X
Servicios compartidos no clínicos							X	X
Servicios médicos no clínicos							X	X
Servicios de soporte no	X		X				X	X

	SECURE MAIL	SECURE WEB	CITRIX FILES	APLICACIÓN WORKSPACE	SALESFORCE1	RSA SECURID	EPICCARE HAIKU	EPIC HYPERSPACE
clínicos								
Programas filantrópicos no clínicos	X		X				X	X
Contratistas	X		X	X	X		X	X

Asignación de recursos MDM a grupos de entrega y recursos

	MDM: DIRECTIVA DE CÓDIGO DE ACCESO	MDM: RESTRICCIONES DE DISPOSITIVO	MDM: ACCIONES AUTOMATIZADAS	MDM: DIRECTIVA DE RED
Clínico-Enfermeras				X
Clínico-Médicos		X		
Clínico-Especialistas				
Clínico-Médicos externos				
Clínico-Servicios de salud a domicilio				

	MDM: DIRECTIVA DE CÓDIGO DE ACCESO	MDM: RESTRICCIONES DE DISPOSITIVO	MDM: ACCIONES AUTOMATIZADAS	MDM: DIRECTIVA DE RED
Clínico-Especialista en investigación				
Clínico-Educación y formación				
No clínico-Servicios compartidos				
No clínico-Servicios médicos				
No clínico-Servicios de soporte				
No clínico-Programas filantrópicos				
Contratistas				X

Notas y consideraciones

- Citrix Endpoint Management crea un grupo de entrega predeterminado denominado Todos los usuarios durante la configuración inicial. Si no deshabilita este grupo de entrega, todos los usuarios de Active Directory tienen derecho a inscribirse en Citrix Endpoint Management.
- Citrix Endpoint Management sincroniza los usuarios y grupos de Active Directory a petición mediante una conexión dinámica al servidor LDAP.
- Si un usuario forma parte de un grupo que no está asignado en Citrix Endpoint Management, ese usuario no puede inscribirse. Del mismo modo, si un usuario es miembro de muchos grupos, Citrix Endpoint Management solo clasifica al usuario como perteneciente a los grupos asignados a Citrix Endpoint Management.

Estrategia de correo electrónico

El acceso seguro al correo electrónico desde dispositivos móviles es uno de los principales impulsores de la iniciativa de gestión de la movilidad de cualquier organización. Decidir la estrategia de correo electrónico adecuada suele ser un componente clave de cualquier diseño de Citrix Endpoint Management. Citrix Endpoint Management ofrece varias opciones para adaptarse a diferentes casos de uso, en función de los requisitos de seguridad, experiencia de usuario e integración. Este artículo cubre el proceso típico de decisión de diseño y las consideraciones para elegir la solución adecuada, desde la selección del cliente hasta el flujo de tráfico de correo.

Elección de los clientes de correo electrónico

La selección del cliente suele ser lo primero en el diseño general de la estrategia de correo electrónico. Puede elegir entre varios clientes: Citrix Secure Mail, el correo nativo que se incluye con el sistema operativo de una plataforma móvil en particular, u otros clientes de terceros disponibles a través de las tiendas de aplicaciones públicas. Según sus necesidades, es posible que pueda dar soporte a las comunidades de usuarios con un único cliente (estándar) o que tenga que utilizar una combinación de clientes.

La siguiente tabla describe algunas consideraciones de diseño para las diferentes opciones de cliente disponibles:

Tema	Citrix Secure Mail	Nativo (por ejemplo, iOS Mail)	Correo de terceros
Configuración	Perfiles de cuenta de Exchange configurados mediante una política MDX.	Perfiles de cuenta de Exchange configurados mediante una política MDM. La compatibilidad con Android se limita a: Android Enterprise. Todos los demás clientes se consideran clientes de terceros.	Generalmente requiere configuración manual por parte del usuario.
Seguridad	Seguro por diseño, proporcionando la máxima seguridad.	Basado en el conjunto de características del	Basado en el conjunto de características del

	Utiliza políticas MDX con niveles de cifrado de datos adicionales. Citrix Secure Mail es una aplicación totalmente administrada mediante una política MDX. Capa adicional de autenticación con PIN de Citrix.	proveedor/ aplicación. Proporciona mayor seguridad. Utiliza la configuración de cifrado del dispositivo. Se basa en la autenticación a nivel de dispositivo para acceder a la aplicación.	proveedor/ aplicación. Proporciona alta seguridad.
Integración	Permite la interacción con aplicaciones administradas (MDX) de forma predeterminada. Abre URL web con Citrix Secure Web. Guarda archivos en y adjunta archivos desde Citrix Files. Se une y marca directamente a GoToMeeting.	Solo puede interactuar con otras aplicaciones no administradas (no MDX) de forma predeterminada.	Solo puede interactuar con otras aplicaciones no administradas (no MDX) de forma predeterminada.
Implementación/ Licencias	Puede enviar Citrix Secure Mail a través de MDM, directamente desde las tiendas de aplicaciones públicas. Incluido con las licencias Citrix Endpoint Management Advanced y Enterprise.	Aplicación cliente incluida con el sistema operativo de la plataforma. No se requieren licencias adicionales.	Puede enviar a través de MDM, como una aplicación empresarial o directamente desde las tiendas de aplicaciones públicas. El modelo de licencia/costos asociado se basa en el proveedor de la aplicación.

Soporte	Soporte de un único proveedor para el cliente y la solución EMM (Citrix). Información de contacto de soporte integrada en Citrix Secure Hub/ capacidades de registro de depuración de la aplicación. Un cliente para soportar.	Soporte definido por el proveedor (Apple/ Google). Es posible que deba admitir diferentes clientes según la plataforma del dispositivo.	Soporte definido por el proveedor. Un cliente para soportar, asumiendo que el cliente de terceros es compatible con todas las plataformas de dispositivos administrados.

Consideraciones sobre el flujo y el filtrado del tráfico de correo

Esta sección analiza los tres escenarios principales y las consideraciones de diseño sobre el flujo de tráfico de correo (ActiveSync) en el contexto de Citrix Endpoint Management.

Escenario 1: Exchange expuesto

Los entornos que admiten clientes externos suelen tener los servicios de Exchange ActiveSync expuestos a Internet. Los clientes móviles de ActiveSync se conectan a través de esta ruta externa mediante un proxy inverso (por ejemplo, NetScaler Gateway) o un servidor Edge. Esta opción es necesaria para el uso de clientes de correo nativos o de terceros, lo que convierte a estos clientes en la opción popular para este escenario. Aunque no es una práctica común, también puede utilizar el cliente Citrix Secure Mail en este escenario. Al hacerlo, se beneficia de las funciones de seguridad que ofrece el uso de las directivas MDX y la administración de la aplicación.

Escenario 2: Túnel a través de NetScaler Gateway (micro VPN y STA)

Este escenario es el predeterminado cuando se utiliza el cliente Citrix Secure Mail, debido a sus capacidades de micro VPN. En este caso, el cliente Citrix Secure Mail establece una conexión segura con ActiveSync a través de NetScaler Gateway. En esencia, puede considerar que Citrix Secure Mail es el cliente que se conecta directamente a ActiveSync desde la red interna. Los clientes de Citrix a menudo estandarizan Citrix Secure Mail como el cliente móvil de ActiveSync preferido. Esa decisión forma parte de una iniciativa para evitar exponer los servicios de ActiveSync a Internet en un servidor Exchange expuesto, como se describe en el primer escenario.

Solo las aplicaciones habilitadas para MAM SDK o encapsuladas en MDX pueden usar la función de micro VPN. Este escenario no se aplica a los clientes nativos si utiliza el encapsulado MDX. Aunque podría ser posible encapsular clientes de terceros con el MDX Toolkit, esta práctica no es común. El uso de clientes VPN a nivel de dispositivo para permitir el acceso en túnel a clientes nativos o de terceros ha demostrado ser engorroso y no una solución factible.

Escenario 3: Servicios de Exchange alojados en la nube

Los servicios de Exchange alojados en la nube, como Microsoft Office 365, son cada vez más populares. En el contexto de Citrix Endpoint Management, este escenario podría tratarse de la misma manera que el primer escenario, ya que el servicio ActiveSync también está expuesto a Internet. En este caso, los requisitos del proveedor de servicios en la nube dictan las opciones de cliente. Las opciones generalmente incluyen soporte para la mayoría de los clientes de ActiveSync, como Citrix Secure Mail y otros clientes nativos o de terceros.

Citrix Endpoint Management puede añadir valor en tres áreas para este escenario:

- Clientes con directivas MDX y administración de aplicaciones con Citrix Secure Mail
- Configuración de cliente con el uso de una directiva MDM en clientes de correo electrónico nativos compatibles
- Opciones de filtrado de ActiveSync con el uso del conector de Citrix Endpoint Management para Exchange ActiveSync

Consideraciones sobre el filtrado del tráfico de correo

Como ocurre con la mayoría de los servicios expuestos a Internet, debe proteger la ruta y proporcionar filtrado para el acceso autorizado. La solución Citrix Endpoint Management incluye dos componentes diseñados específicamente para proporcionar capacidades de filtrado de ActiveSync para clientes nativos y de terceros: el conector de NetScaler Gateway para Exchange ActiveSync y el conector de Citrix Endpoint Management para Exchange ActiveSync.

Conector de NetScaler Gateway para Exchange ActiveSync

El conector de NetScaler Gateway para Exchange ActiveSync proporciona filtrado de ActiveSync en el perímetro, utilizando NetScaler Gateway como proxy para el tráfico de ActiveSync. Como resultado, el componente de filtrado se encuentra en la ruta del flujo de tráfico de correo, interceptando el correo a medida que entra o sale del entorno. El conector para Exchange ActiveSync actúa como intermediario entre NetScaler Gateway y Citrix Endpoint Management. Cuando un dispositivo se comunica con Exchange a través del servidor virtual de ActiveSync en NetScaler Gateway, NetScaler Gateway realiza una llamada HTTP al conector para el servicio de Exchange ActiveSync. Ese servicio comprueba entonces el estado del dispositivo con Citrix

Endpoint Management. Basándose en el estado del dispositivo, el conector para Exchange ActiveSync responde a NetScaler Gateway para permitir o denegar la conexión. También puede configurar reglas estáticas para filtrar el acceso según el usuario, el agente y el tipo o ID de dispositivo.

Esta configuración permite que los servicios de Exchange ActiveSync se expongan a Internet con una capa adicional de seguridad para evitar el acceso no autorizado. Las consideraciones de diseño incluyen las siguientes:

- **Windows Server:** El conector para el componente de Exchange ActiveSync requiere un servidor Windows.
- **Conjunto de reglas de filtrado:** El conector para Exchange ActiveSync está diseñado para filtrar según el estado y la información del dispositivo, en lugar de la información del usuario. Aunque puede configurar reglas estáticas para filtrar por ID de usuario, no existen opciones para filtrar según la pertenencia a grupos de Active Directory, por ejemplo. Si existe un requisito de filtrado de grupos de Active Directory, puede utilizar el conector de Citrix Endpoint Management para Exchange ActiveSync en su lugar.
- **Escalabilidad de NetScaler Gateway:** Dada la necesidad de actuar como proxy para el tráfico de ActiveSync a través de NetScaler Gateway: El dimensionamiento adecuado de la instancia de NetScaler Gateway es fundamental para soportar la carga de trabajo adicional de todas las conexiones SSL de ActiveSync.
- **Almacenamiento en caché integrado de NetScaler Gateway:** El conector para la configuración de Exchange ActiveSync en NetScaler Gateway utiliza la función de almacenamiento en caché integrado para almacenar en caché las respuestas del conector. Debido a esa configuración, NetScaler Gateway no necesita emitir una solicitud al conector para cada transacción de ActiveSync en una sesión determinada. Esa configuración también es fundamental para un rendimiento y una escala adecuados. El almacenamiento en caché integrado está disponible con NetScaler Gateway Platinum Edition.
- **Directivas de filtrado personalizadas:** Es posible que tenga que crear directivas personalizadas de NetScaler Gateway para restringir ciertos clientes de ActiveSync fuera de los clientes móviles nativos estándar. Esta configuración requiere conocimientos sobre las solicitudes HTTP de ActiveSync y la creación de directivas de respuesta de NetScaler Gateway.
- **Clientes de Citrix Secure Mail:** Citrix Secure Mail tiene capacidades de micro VPN que eliminan la necesidad de filtrado en el perímetro. El cliente de Citrix Secure Mail puede tratarse generalmente como un cliente de ActiveSync interno (de confianza) cuando se conecta a través de NetScaler Gateway. Si se requiere compatibilidad con clientes nativos y de terceros

(con el conector para Exchange ActiveSync) y clientes de Citrix Secure Mail: Citrix recomienda que el tráfico de Citrix Secure Mail no fluya a través del servidor virtual de NetScaler Gateway utilizado para el conector. Puede lograr este flujo de tráfico a través de DNS y evitar que la directiva del conector afecte a los clientes de Citrix Secure Mail.

Para ver un diagrama del conector de NetScaler Gateway para Exchange ActiveSync en una implementación de Citrix Endpoint Management, consulte Arquitectura.

Conector de Citrix Endpoint Management para Exchange ActiveSync

El conector de Citrix Endpoint Management para Exchange ActiveSync es un componente de Citrix Endpoint Management que proporciona filtrado de ActiveSync a nivel de servicio de Exchange. Como resultado, el filtrado solo se produce una vez que el correo llega al servicio de Exchange, en lugar de cuando entra en el entorno de Citrix Endpoint Management. Mail Manager utiliza PowerShell para consultar Exchange ActiveSync en busca de información de asociación de dispositivos y controlar el acceso a través de acciones de cuarentena de dispositivos. Esas acciones ponen y sacan dispositivos de la cuarentena basándose en los criterios de las reglas del conector de Citrix Endpoint Management para Exchange ActiveSync.

De forma similar al conector de NetScaler Gateway para Exchange ActiveSync, el conector para Exchange ActiveSync comprueba el estado del dispositivo con Citrix Endpoint Management para filtrar el acceso según el cumplimiento del dispositivo. También puede configurar reglas estáticas para filtrar el acceso según el tipo o ID de dispositivo, la versión del agente y la pertenencia a grupos de Active Directory.

Esta solución no requiere el uso de NetScaler Gateway. Puede implementar el conector para Exchange ActiveSync sin cambiar el enrutamiento del tráfico de ActiveSync existente. Las consideraciones de diseño incluyen:

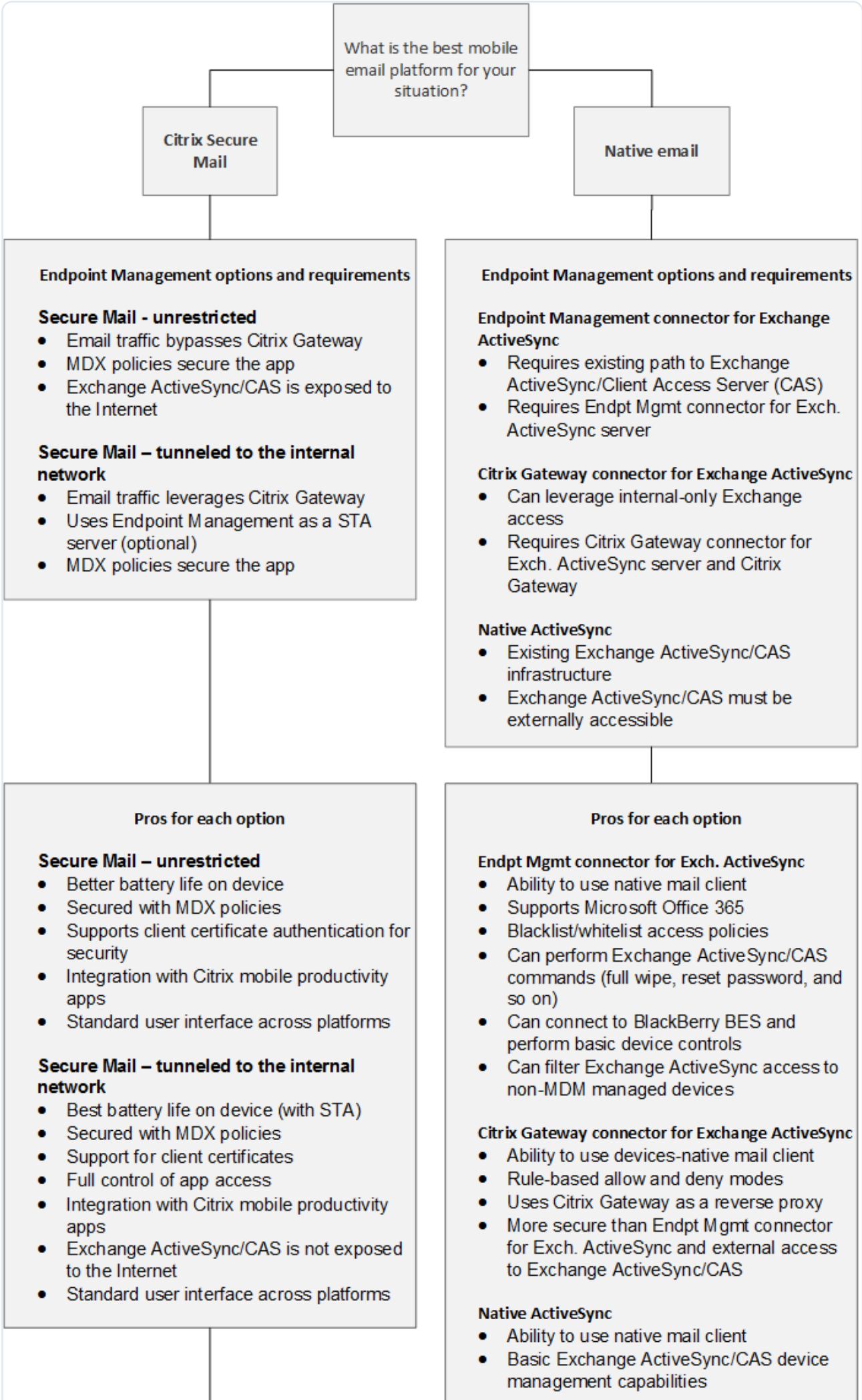
- **Windows Server:** El conector para Exchange ActiveSync requiere la implementación de Windows Server.
- **Conjunto de reglas de filtrado:** Al igual que el conector de NetScaler Gateway para Exchange ActiveSync, el conector para Exchange ActiveSync incluye reglas de filtrado para evaluar el estado del dispositivo. Además, el conector para Exchange ActiveSync también admite reglas estáticas para filtrar según la pertenencia a grupos de Active Directory.
- **Integración con Exchange:** El conector para Exchange ActiveSync requiere acceso directo al servidor de acceso de cliente (CAS) de Exchange que aloja la función de ActiveSync y control sobre las acciones de cuarentena de dispositivos. Este requisito podría suponer un desafío en función de la arquitectura del entorno y la postura de seguridad. Es fundamental que evalúe este requisito técnico de antemano.

- **Otros clientes de ActiveSync:** Dado que el conector para Exchange ActiveSync filtra a nivel de servicio de ActiveSync, tenga en cuenta otros clientes de ActiveSync fuera del entorno de Citrix Endpoint Management. Puede configurar las reglas estáticas del conector para Exchange ActiveSync para evitar un impacto no deseado en otros clientes de ActiveSync.
- **Funciones extendidas de Exchange:** Mediante la integración directa con Exchange ActiveSync, el conector para Exchange ActiveSync permite a Citrix Endpoint Management realizar un borrado de Exchange ActiveSync en un dispositivo móvil. El conector para Exchange ActiveSync también permite a Citrix Endpoint Management acceder a información sobre dispositivos Blackberry y realizar otras operaciones de control.

Para ver un diagrama del conector de Citrix Endpoint Management para Exchange ActiveSync en una implementación de Citrix Endpoint Management, consulte Arquitectura.

Árbol de decisión de la plataforma de correo electrónico

La siguiente figura le ayuda a distinguir las ventajas y desventajas de usar el correo electrónico nativo o las soluciones de Citrix Secure Mail en su implementación de Citrix Endpoint Management. Cada opción permite las opciones y requisitos asociados de Citrix Endpoint Management para habilitar el acceso al servidor, la red y la base de datos. Las ventajas y desventajas incluyen detalles sobre consideraciones de seguridad, directivas e interfaz de usuario.


What is the best mobile email platform for your situation?
Citrix Secure Mail
Native email
Endpoint Management options and requirements
Secure Mail - unrestricted
Email traffic bypasses Citrix Gateway
MDX policies secure the app
Exchange ActiveSync/CAS is exposed to the Internet
Secure Mail – tunneled to the internal network
Email traffic leverages Citrix Gateway
Uses Endpoint Management as a STA server (optional)
MDX policies secure the app
Endpoint Management options and requirements
Endpoint Management connector for Exchange ActiveSync
Requires existing path to Exchange ActiveSync/Client Access Server (CAS)
Requires Endpt Mgmt connector for Exch. ActiveSync server
Citrix Gateway connector for Exchange ActiveSync
Can leverage internal-only Exchange access
Requires Citrix Gateway connector for Exch. ActiveSync server and Citrix Gateway
Native ActiveSync
Existing Exchange ActiveSync/CAS infrastructure
Exchange ActiveSync/CAS must be externally accessible
Pros for each option
Secure Mail – unrestricted
Better battery life on device
Secured with MDX policies
Supports client certificate authentication for security
Integration with Citrix mobile productivity apps
Standard user interface across platforms
Secure Mail – tunneled to the internal network
Best battery life on device (with STA)
Secured with MDX policies
Support for client certificates
Full control of app access
Integration with Citrix mobile productivity apps
Exchange ActiveSync/CAS is not exposed to the Internet
Standard user interface across platforms
Pros for each option
Endpt Mgmt connector for Exch. ActiveSync
Ability to use native mail client
Supports Microsoft Office 365
Blacklist/whitelist access policies
Can perform Exchange ActiveSync/CAS commands (full wipe, reset password, and so on)
Can connect to BlackBerry BES and perform basic device controls
Can filter Exchange ActiveSync access to non-MDM managed devices
Citrix Gateway connector for Exchange ActiveSync
Ability to use devices-native mail client
Rule-based allow and deny modes
Uses Citrix Gateway as a reverse proxy
More secure than Endpt Mgmt connector for Exch. ActiveSync and external access to Exchange ActiveSync/CAS
Native ActiveSync
Ability to use native mail client
Basic Exchange ActiveSync/CAS device management capabilities

Integración de Citrix Endpoint Management

Este artículo trata sobre lo que debe tener en cuenta al planificar cómo Citrix Endpoint Management se integrará con su red y soluciones existentes. Por ejemplo, si ya utiliza NetScaler Gateway para Citrix Virtual Apps and Desktops:

- ¿Quiere usar la instancia de NetScaler Gateway existente o una instancia nueva y dedicada?
- ¿Quiere integrar con Citrix Endpoint Management las aplicaciones HDX publicadas con StoreFront?
- ¿Tiene previsto usar Citrix Files con Citrix Endpoint Management?
- ¿Tiene una solución de control de acceso a la red que quiera integrar en Citrix Endpoint Management?

NetScaler Gateway

NetScaler Gateway es necesario para Citrix Endpoint Management. NetScaler Gateway proporciona una ruta micro VPN para acceder a todos los recursos corporativos y ofrece un sólido soporte de autenticación multifactor.

Puede usar instancias de NetScaler Gateway existentes o configurar otras nuevas para Citrix Endpoint Management. Las siguientes secciones describen las ventajas y desventajas de usar instancias de NetScaler Gateway existentes o nuevas y dedicadas.

NetScaler Gateway MPX compartido con un VIP de NetScaler Gateway creado para Citrix Endpoint Management

Ventajas:

- Utiliza una instancia común de NetScaler Gateway para todas las conexiones remotas de Citrix: Citrix Virtual Apps, VPN completa y VPN sin cliente.
- Utiliza las configuraciones existentes de NetScaler Gateway, como la autenticación de certificados y el acceso a servicios como DNS, LDAP y NTP.
- Utiliza una única licencia de plataforma de NetScaler Gateway.

Desventajas:

- Es más difícil planificar la escalabilidad cuando se manejan dos casos de uso diferentes en el mismo NetScaler Gateway.
- A veces se necesita una versión específica de NetScaler Gateway para un caso de uso de Citrix Virtual Apps. Esa misma versión podría tener problemas conocidos para Citrix Endpoint

Management. O Citrix Endpoint Management podría tener problemas conocidos para la versión de NetScaler Gateway.

- Si ya existe un NetScaler Gateway, no puede ejecutar el asistente de NetScaler para XenMobile una segunda vez para crear la configuración de NetScaler Gateway para Citrix Endpoint Management.
- Excepto cuando se utilizan licencias Platinum para NetScaler Gateway 11.1 o posterior: Las licencias de acceso de usuario instaladas en NetScaler Gateway y necesarias para la conectividad VPN se agrupan. Dado que esas licencias están disponibles para todos los servidores virtuales de NetScaler Gateway, otros servicios distintos de Citrix Endpoint Management pueden consumirlas.

Instancia dedicada de NetScaler Gateway VPX/MPX

Ventajas:

Citrix recomienda usar una instancia dedicada de NetScaler Gateway.

- Más fácil de planificar la escalabilidad y separar el tráfico de Citrix Endpoint Management de una instancia de NetScaler Gateway que ya podría tener recursos limitados.
- Evita problemas cuando Citrix Endpoint Management y Citrix Virtual Apps necesitan diferentes versiones de software de NetScaler Gateway. La recomendación general es usar la última versión y compilación compatible de NetScaler Gateway para Citrix Endpoint Management.
- Permite la configuración de NetScaler Gateway para Citrix Endpoint Management a través del asistente integrado de NetScaler para XenMobile.
- Separación virtual y física de los servicios.

Desventajas:

- Requiere la configuración de servicios adicionales en NetScaler Gateway para admitir la configuración de Citrix Endpoint Management.
- Requiere otra licencia de plataforma de NetScaler Gateway. Licencie cada instancia de NetScaler Gateway para NetScaler Gateway.

Para obtener información sobre qué considerar al integrar NetScaler Gateway y Citrix ADC para los modos de administración de Citrix Endpoint Management, consulte Integración con NetScaler Gateway y Citrix ADC.

StoreFront

Si tiene un entorno de Citrix Virtual Apps and Desktops, puede integrar aplicaciones HDX con Citrix Endpoint Management mediante StoreFront. Al integrar aplicaciones HDX con Citrix Endpoint Management:

- Las aplicaciones están disponibles para los usuarios inscritos en Citrix Endpoint Management.
- Las aplicaciones se muestran en la tienda de aplicaciones junto con otras aplicaciones móviles.
- Citrix Endpoint Management utiliza Citrix Receiver en StoreFront.
- Cuando la aplicación Citrix Workspace está instalada en un dispositivo, las aplicaciones HDX se inician con esa aplicación.

StoreFront tiene una limitación de un sitio de servicio por instancia de StoreFront. Supongamos que tiene muchas tiendas y quiere segmentarlas de otros usos de producción. En ese caso, Citrix generalmente recomienda que considere una nueva instancia de StoreFront y un sitio de servicios para Citrix Endpoint Management.

Las consideraciones incluyen:

- ¿Existen requisitos de autenticación diferentes para StoreFront? El sitio de servicios de StoreFront requiere credenciales de Active Directory para iniciar sesión. Los clientes que solo usan autenticación basada en certificados no pueden enumerar aplicaciones a través de Citrix Endpoint Management usando el mismo NetScaler Gateway.
- ¿Usar la misma tienda o crear una tienda?
- ¿Usar el mismo servidor StoreFront o uno diferente?

Las siguientes secciones señalan las ventajas y desventajas de usar StoreFronts separados o combinados para Citrix Workspace y las aplicaciones de productividad móvil de Citrix.

Integrar su instancia de StoreFront existente con Citrix Endpoint Management

Ventajas:

- Misma tienda: No se requiere configuración adicional de StoreFront para Citrix Endpoint Management, asumiendo que utiliza el mismo VIP de NetScaler Gateway para el acceso HDX. Supongamos que elige usar la misma tienda y desea dirigir el acceso a Citrix Workspace a un nuevo VIP de NetScaler Gateway. En ese caso, agregue la configuración de NetScaler Gateway adecuada a StoreFront.
- Mismo servidor StoreFront: Utiliza la instalación y configuración de StoreFront existentes.

Desventajas:

- Misma tienda: Cualquier reconfiguración de StoreFront para admitir cargas de trabajo de Citrix Virtual Apps and Desktops podría afectar negativamente a Citrix Endpoint Management.
- Mismo servidor StoreFront: En entornos grandes, tenga en cuenta la carga adicional del uso de Citrix Receiver por parte de Citrix Endpoint Management para la enumeración e inicio de aplicaciones.

Usar una instancia de StoreFront nueva y dedicada para la integración con Citrix Endpoint Management

Ventajas:

- Nueva tienda: Cualquier cambio de configuración de la tienda StoreFront para Citrix Endpoint Management no afecta a las cargas de trabajo existentes de Virtual Apps and Desktops.
- Nuevo servidor StoreFront: Los cambios de configuración del servidor no afectan a los flujos de trabajo de Virtual Apps and Desktops. Además, la carga ajena al uso de Citrix Receiver por parte de Citrix Endpoint Management para la enumeración e inicio de aplicaciones no afecta a la escalabilidad.

Desventajas:

- Nueva tienda: Configuración de la tienda StoreFront.
- Nuevo servidor StoreFront: Requiere una nueva instalación y configuración de StoreFront.

Para obtener más información, consulte Citrix Virtual Apps and Desktops a través de la tienda de aplicaciones.

ShareFile y Citrix Files

> **Descargo de responsabilidad:**

> Esta función quedará obsoleta si ShareFile (ahora Progress) deja de ofrecer soporte.

> ShareFile le permite intercambiar documentos de forma fácil y segura, enviar documentos grandes por correo electrónico y gestionar de forma segura las transferencias de documentos a terceros. La aplicación Citrix Files permite a los usuarios acceder y sincronizar todos sus datos desde cualquier dispositivo. Con Citrix Files, los usuarios pueden compartir datos de forma segura con personas tanto dentro como fuera de la organización.

Citrix Endpoint Management proporciona a Citrix Files lo siguiente:

- Autenticación de inicio de sesión único para usuarios de aplicaciones de productividad móvil.
- Aprovisionamiento de cuentas de usuario basado en Active Directory.
- Directivas de control de acceso exhaustivas.

Los usuarios móviles pueden beneficiarse del conjunto completo de funciones de la cuenta Enterprise.

Alternativamente, puede configurar Citrix Endpoint Management para que se integre solo con los conectores de zona de almacenamiento. A través de los conectores de zona de almacenamiento, Citrix Files proporciona acceso a:

- Documentos y carpetas
- Recursos compartidos de archivos de red
- En sitios de SharePoint: Colecciones de sitios y bibliotecas de documentos.

Los recursos compartidos de archivos conectados pueden incluir las mismas unidades de inicio de red utilizadas en entornos de Citrix Virtual Apps and Desktops. Utilice la consola de Citrix Endpoint Management para configurar la integración con cuentas Enterprise o conectores de zona de almacenamiento. Para obtener más información, consulte Citrix Files para Citrix Endpoint Management.

Las siguientes secciones recogen las preguntas que debe hacerse al tomar decisiones de diseño para Citrix Files.

Integrar con Citrix Files o solo con conectores de zona de almacenamiento

Preguntas que debe hacerse:

- ¿Desea almacenar datos en zonas de almacenamiento administradas por Citrix?
- ¿Quiere proporcionar a los usuarios capacidades de sincronización y uso compartido de archivos?
- ¿Quiere permitir a los usuarios acceder a archivos en el sitio web de Citrix Files? ¿O acceder a contenido de Office 365 y conectores de nube personal desde dispositivos móviles?

Decisión de diseño:

- Si la respuesta a cualquiera de esas preguntas es "sí", integre con una cuenta Enterprise.
- Una integración solo con conectores de zona de almacenamiento proporciona a los usuarios de iOS acceso móvil seguro a los repositorios de almacenamiento locales existentes, como

sitios de SharePoint y recursos compartidos de archivos de red. En esta configuración, no se configura un subdominio de Citrix Files, no se aprovisionan usuarios en Citrix Files ni se alojan datos de Citrix Files. El uso de conectores de zona de almacenamiento con Citrix Endpoint Management sigue las restricciones de seguridad contra la fuga de información del usuario fuera de la red corporativa.

Ubicación del servidor del controlador de zonas de almacenamiento

Preguntas que debe hacerse:

- ¿Necesita almacenamiento local o funciones como los conectores de zona de almacenamiento?
- Si utiliza funciones locales de Citrix Files, ¿dónde se ubicarán los controladores de zonas de almacenamiento en la red?

Decisión de diseño:

- Determine si ubicar los servidores del controlador de zonas de almacenamiento en la nube de Citrix Files, en su sistema de almacenamiento local de un solo inquilino o en un almacenamiento en la nube de terceros compatible.
- Los controladores de zonas de almacenamiento requieren cierto acceso a Internet para comunicarse con el plano de control de Citrix Files. Puede conectarse de varias maneras, incluido el acceso directo o las configuraciones NAT/PAT.

Conectores de zona de almacenamiento

Preguntas que debe hacerse:

- ¿Cuáles son las rutas de recursos compartidos CIFS?
- ¿Cuáles son las URL de SharePoint?

Decisión de diseño:

- Determine si se requieren controladores de zonas de almacenamiento locales para acceder a esas ubicaciones.
- Debido a la comunicación del conector de zonas de almacenamiento con recursos internos como repositorios de archivos, recursos compartidos CIFS y SharePoint: Citrix recomienda que los controladores de zonas de almacenamiento estén en la red interna detrás de los firewalls de la DMZ y delante de NetScaler Gateway.

Integración de SAML con Citrix Endpoint Management

Preguntas que hacer:

- ¿Se requiere autenticación de Active Directory para Citrix Files?
- ¿El primer uso de la aplicación Citrix Files para Citrix Endpoint Management requiere SSO?
- ¿Hay un IdP estándar en su entorno actual?
- ¿Cuántos dominios se requieren para usar SAML?
- ¿Hay muchos alias de correo electrónico para los usuarios de Active Directory?
- ¿Hay alguna migración de dominio de Active Directory en curso o programada para pronto?

Decisión de diseño:

Puede optar por usar SAML como mecanismo de autenticación para Citrix Files. Las opciones de autenticación son:

- Utilice el servidor de Citrix Endpoint Management como proveedor de identidades (IdP) para SAML

  Esta opción puede proporcionar una excelente experiencia de usuario, automatizar la creación de cuentas de Citrix Files y habilitar las funciones de SSO de aplicaciones móviles.

  El servidor de Citrix Endpoint Management está mejorado para este proceso: no requiere la sincronización de Active Directory.

  Utilice la Herramienta de administración de usuarios de Citrix Files para el aprovisionamiento de usuarios.
- Utilice un proveedor de terceros compatible como IdP para SAML

  Si tiene un IdP existente y compatible y no necesita capacidades de SSO de aplicaciones móviles, esta opción podría ser la más adecuada para usted. Esta opción también requiere el uso de la Herramienta de administración de usuarios de Citrix Files para el aprovisionamiento de cuentas.

  El uso de soluciones IdP de terceros, como ADFS, también podría proporcionar capacidades de SSO en el lado del cliente de Windows. Asegúrese de evaluar los casos de uso antes de elegir su IdP SAML de Citrix Files.
- O, para satisfacer ambos casos de uso, consulte Guía de configuración de inicio de sesión único de ShareFile para proveedores de identidades duales.

Aplicaciones móviles

Preguntas que debe hacerse:

- ¿Qué aplicación móvil de Citrix Files piensa utilizar (pública, MDM, MDX)?

Decisión de diseño:

- Usted distribuye las aplicaciones de productividad móvil de Citrix desde Apple App Store y Google Play Store. Con esa distribución de la tienda de aplicaciones pública, obtiene aplicaciones encapsuladas desde la página de descargas de Citrix.
- Si sus requisitos de seguridad son bajos y no necesita la contenedorización, la aplicación pública de Citrix Files podría no ser adecuada.
- Para obtener más información, consulte Aplicaciones y Citrix Files para Citrix Endpoint Management.

Seguridad, directivas y control de acceso

Preguntas que hacer:

- ¿Qué restricciones necesita para los usuarios de escritorio, web y móviles?
- ¿Qué configuraciones estándar de control de acceso desea para los usuarios?
- ¿Qué política de retención de archivos planea usar?

Decisión de diseño:

- Citrix Files le permite gestionar los permisos de los empleados. Para obtener más información, consulte Permisos de empleados.
- Algunas configuraciones de seguridad de dispositivos de Citrix Files y políticas MDX controlan las mismas funciones. En esos casos, las políticas de Citrix Endpoint Management tienen prioridad, seguidas de las configuraciones de seguridad de dispositivos de Citrix Files. Ejemplos: Si deshabilita las aplicaciones externas en Citrix Files, pero las habilita en Citrix Endpoint Management, las aplicaciones externas se deshabilitan en Citrix Files. Puede configurar las aplicaciones para que Citrix Endpoint Management no requiera un PIN/código de acceso, pero la aplicación Citrix Files sí lo requiera.

Zonas de almacenamiento estándar frente a restringidas

Preguntas que hacer:

- ¿Necesita zonas de almacenamiento restringidas?

Decisión de diseño:

- Una zona de almacenamiento estándar está destinada a datos no confidenciales y permite a los empleados compartir datos con personas que no son empleados. Esta opción admite flujos de trabajo que implican compartir datos fuera de su dominio.

- Una zona de almacenamiento restringida protege los datos confidenciales: solo los usuarios de dominio autenticados pueden acceder a los datos almacenados en la zona.

Control de acceso

Las empresas pueden gestionar dispositivos móviles dentro y fuera de las redes. Las soluciones de gestión de movilidad empresarial, como Citrix Endpoint Management, son excelentes para proporcionar seguridad y controles para dispositivos móviles, independientemente de la ubicación. Sin embargo, cuando se combinan con una solución de control de acceso a la red (NAC), se puede añadir QoS y un control más granular a los dispositivos que son internos a su red. Esa combinación le permite extender la evaluación de seguridad de dispositivos de Citrix Endpoint Management a través de su solución NAC. Su solución NAC puede entonces utilizar la evaluación de seguridad de Citrix Endpoint Management para facilitar y gestionar las decisiones de autenticación.

Puede utilizar cualquiera de estas soluciones para aplicar políticas de NAC:

- NetScaler Gateway
- ForeScout

Citrix no garantiza la integración con otras soluciones NAC.

Las ventajas de la integración de una solución NAC con Citrix Endpoint Management incluyen las siguientes:

- Mejor seguridad, cumplimiento y control para todos los puntos finales en una red empresarial.
- Una solución NAC puede:
    - Detectar dispositivos en el instante en que intentan conectarse a su red.
    - Consultar Citrix Endpoint Management para obtener atributos de dispositivo.
    - Utilizar esa información del dispositivo para determinar si se permite, bloquea, limita o redirige esos dispositivos. Esas decisiones dependen de las políticas de seguridad que elija aplicar.
- Una solución NAC proporciona a los administradores de TI una vista de los dispositivos no administrados y no conformes.

Para obtener una descripción de los filtros de cumplimiento de NAC compatibles con Citrix Endpoint Management y una descripción general de la configuración, consulte Control de acceso a la red.

Integración con NetScaler Gateway y Citrix ADC

Cuando se integra con Citrix Endpoint Management, NetScaler Gateway proporciona un mecanismo de autenticación para el acceso remoto de dispositivos a la red interna para dispositivos MAM. La integración permite que las aplicaciones de productividad móvil de Citrix se conecten a los servidores corporativos de la intranet a través de una micro VPN. Citrix Endpoint Management crea una micro VPN desde las aplicaciones del dispositivo hasta NetScaler Gateway. NetScaler Gateway proporciona una ruta de micro VPN para acceder a todos los recursos corporativos y ofrece un sólido soporte de autenticación multifactor.

Cuando un usuario opta por no inscribirse en MDM, los dispositivos se inscriben utilizando el FQDN de NetScaler Gateway.

Citrix Cloud Operations gestiona el equilibrio de carga de Citrix ADC.

Decisiones de diseño

Las siguientes secciones resumen las muchas decisiones de diseño que deben tenerse en cuenta al planificar una integración de NetScaler Gateway con Citrix Endpoint Management.

Certificados

Detalles de la decisión:

- ¿Necesita un mayor grado de seguridad para la inscripción y el acceso al entorno de Citrix Endpoint Management?
- ¿LDAP no es una opción?

Guía de diseño:

La configuración predeterminada de Citrix Endpoint Management es la autenticación de nombre de usuario y contraseña. Para añadir otra capa de seguridad para la inscripción y el acceso al entorno de Citrix Endpoint Management, considere la posibilidad de utilizar la autenticación basada en certificados. Puede utilizar certificados con LDAP para la autenticación de dos factores, lo que proporciona un mayor grado de seguridad sin necesidad de un servidor RSA.

Si no permite LDAP y utiliza tarjetas inteligentes o métodos similares, la configuración de certificados le permite representar una tarjeta inteligente en Citrix Endpoint Management. Los usuarios se inscriben utilizando un PIN único que Citrix Endpoint Management genera para ellos. Una vez que un usuario tiene acceso, Citrix Endpoint Management crea e implementa el certificado que se utilizará posteriormente para autenticarse en el entorno de Citrix Endpoint Management.

Citrix Endpoint Management admite la lista de revocación de certificados (CRL) solo para una entidad de certificación de terceros. Si tiene una CA de Microsoft configurada, Citrix Endpoint Management utiliza NetScaler Gateway para administrar la revocación. Al configurar la autenticación basada en certificados de cliente, considere si necesita configurar el ajuste de la lista de revocación de certificados (CRL) de NetScaler Gateway **Enable CRL Auto Refresh**. Este paso garantiza que el usuario de un dispositivo inscrito solo en MAM no pueda autenticarse utilizando un certificado existente en el dispositivo. Citrix Endpoint Management vuelve a emitir un nuevo certificado, ya que no restringe a un usuario la generación de un certificado de usuario si se revoca uno. Esta configuración aumenta la seguridad de las entidades PKI cuando la CRL comprueba las entidades PKI caducadas.

VIP de NetScaler Gateway dedicadas o compartidas

Detalles de la decisión:

- ¿Utiliza actualmente NetScaler Gateway para Citrix Virtual Apps and Desktops?
- ¿Utilizará Citrix Endpoint Management el mismo NetScaler Gateway que Citrix Virtual Apps and Desktops?
- ¿Cuáles son los requisitos de autenticación para ambos flujos de tráfico?

Guía de diseño:

Cuando su entorno Citrix incluye Citrix Endpoint Management, además de Virtual Apps and Desktops, puede utilizar el mismo servidor virtual de NetScaler Gateway para ambos. Debido a los posibles conflictos de versiones y al aislamiento del entorno, se recomienda un NetScaler Gateway dedicado para cada entorno de Citrix Endpoint Management.

Si utiliza la autenticación LDAP, Citrix Secure Hub puede autenticarse en el mismo NetScaler Gateway sin problemas. Si utiliza la autenticación basada en certificados, Citrix Endpoint Management envía un certificado en el contenedor MDX y Citrix Secure Hub utiliza el certificado para autenticarse con NetScaler Gateway.

Puede considerar esta solución alternativa, que le permite utilizar el mismo FQDN para dos VIP de NetScaler Gateway. Puede crear dos VIP de NetScaler Gateway con la misma dirección IP. La de Citrix Secure Hub utiliza el puerto estándar 443 y la de Citrix Virtual Apps and Desktops (que implementa la aplicación Citrix Workspace) utiliza el puerto 444. Entonces, un FQDN se resuelve en la misma dirección IP. Para esta solución alternativa, es posible que deba configurar StoreFront para que devuelva un archivo ICA para el puerto 444, en lugar del predeterminado, el puerto 443. Esta solución alternativa no requiere que los usuarios introduzcan un número de puerto.

Tiempos de espera de NetScaler Gateway

Detalles de la decisión:

- ¿Cómo desea configurar los tiempos de espera de NetScaler Gateway para el tráfico de Citrix Endpoint Management?

Guía de diseño:

NetScaler Gateway incluye las configuraciones Tiempo de espera de sesión y Tiempo de espera forzado. Para obtener más información, consulte Configuraciones recomendadas. Tenga en cuenta que existen diferentes valores de tiempo de espera para los servicios en segundo plano, NetScaler Gateway y para acceder a las aplicaciones sin conexión.

FQDN de inscripción

> **Importante:**
>
> Para cambiar el FQDN de inscripción se requiere una nueva base de datos de SQL Server y una reconstrucción del servidor de Citrix Endpoint Management.

Tráfico de Citrix Secure Web

Detalles de la decisión:

- ¿Restringirá Citrix Secure Web solo a la navegación web interna?
- ¿Habilitará Citrix Secure Web para la navegación web tanto interna como externa?

Guía de diseño:

Si planea usar Citrix Secure Web solo para la navegación web interna, la configuración de NetScaler Gateway es sencilla. Sin embargo, si Citrix Secure Web no puede acceder a todos los sitios internos de forma predeterminada, es posible que deba configurar firewalls y servidores proxy.

Si planea usar Citrix Secure Web para la navegación interna y externa, debe habilitar el SNIP para que tenga acceso a Internet saliente. El departamento de TI generalmente considera los dispositivos inscritos (que usan el contenedor MDX) como una extensión de la red corporativa. Por lo tanto, TI normalmente quiere que las conexiones de Citrix Secure Web regresen a NetScaler Gateway, pasen por un servidor proxy y luego salgan a Internet. De forma predeterminada, el acceso a Citrix Secure Web se tuneliza a la red interna. Citrix Secure Web utiliza un túnel VPN por

aplicación de vuelta a la red interna para todo el acceso a la red y NetScaler Gateway utiliza la configuración de túnel dividido.

Para una discusión sobre las conexiones de Citrix Secure Web, consulte Configuración de conexiones de usuario.

Notificaciones push para Citrix Secure Mail

Detalles de la decisión:

- ¿Utilizará notificaciones push?

Guía de diseño para iOS:

Si la configuración de NetScaler Gateway incluye Secure Ticket Authority (STA) y el túnel dividido está desactivado: NetScaler Gateway debe permitir el tráfico de Citrix Secure Mail a las URL del servicio de escucha de Citrix. Esas URL se especifican en las notificaciones push para Citrix Secure Mail para iOS.

Guía de diseño para Android:

Utilice Firebase Cloud Messaging (FCM) para controlar cómo y cuándo los dispositivos Android necesitan conectarse a Citrix Endpoint Management. Con FCM configurado, cualquier acción de seguridad o comando de implementación activa una notificación push a Citrix Secure Hub para solicitar al usuario que se vuelva a conectar al servidor de Citrix Endpoint Management.

HDX™ STAs

Detalles de la decisión:

- ¿Qué STA usar si integra el acceso a aplicaciones HDX?

Guía de diseño:

Los STA de HDX deben coincidir con los STA de StoreFront y deben ser válidos para el sitio de Virtual Apps and Desktops.

Citrix Files y ShareFile

Detalles de la decisión:

- ¿Utilizará un controlador de zonas de almacenamiento en el entorno?
- ¿Qué URL VIP de Citrix Files utilizará?

Guía de diseño:

Si incluye un controlador de zonas de almacenamiento en su entorno, asegúrese de configurar correctamente lo siguiente:

- VIP de conmutador de contenido de Citrix Files (utilizado por el plano de control de Citrix Files para comunicarse con los servidores del controlador de zonas de almacenamiento)
- VIP de equilibrio de carga de Citrix Files
- Todas las directivas y perfiles necesarios

Para obtener más información, consulte la documentación de Storage zones controller.

IdP de SAML

Detalle de la decisión:

- Si se requiere SAML para Citrix Files, ¿quiere usar Citrix Endpoint Management como IdP de SAML?

Guía de diseño:

La mejor práctica recomendada es integrar Citrix Files con Citrix Endpoint Management, una alternativa más sencilla a la configuración de la federación basada en SAML. Citrix Endpoint Management proporciona a Citrix Files:

- Autenticación de inicio de sesión único (SSO) para usuarios de aplicaciones de productividad móvil de Citrix
- Aprovisionamiento de cuentas de usuario basado en Active Directory
- Directivas de control de acceso exhaustivas.

La consola de Citrix Endpoint Management le permite configurar Citrix Files y supervisar los niveles de servicio y el uso de licencias.

Hay dos tipos de clientes de Citrix Files: Citrix Files para Citrix Endpoint Management (también conocido como Citrix Files encapsulado) y clientes móviles de Citrix Files (también conocido como Citrix Files sin encapsular). Para comprender las diferencias, consulte Cómo se diferencian los clientes de Citrix Files para Citrix Endpoint Management de los clientes móviles de Citrix Files.

Puede configurar Citrix Endpoint Management y Citrix Files para usar SAML y proporcionar acceso SSO a:

- Aplicaciones de Citrix Files habilitadas para MAM SDK o encapsuladas mediante MDX Toolkit
- Clientes de Citrix Files sin encapsular, como el sitio web, el complemento de Outlook o los clientes de sincronización

Si quiere usar Citrix Endpoint Management como IdP de SAML para Citrix Files, asegúrese de que las configuraciones adecuadas estén implementadas. Para obtener más información, consulte SAML para SSO con Citrix Files.

Conexiones directas de ShareConnect

Detalle de la decisión:

- ¿Accederán los usuarios a un equipo host desde un equipo o dispositivo móvil que ejecute ShareConnect mediante conexiones directas?

Guía de diseño:

ShareConnect permite a los usuarios conectarse de forma segura a sus equipos a través de iPads, tabletas Android y teléfonos Android para acceder a sus archivos y aplicaciones. Para las conexiones directas, Citrix Endpoint Management utiliza NetScaler Gateway para proporcionar acceso seguro a los recursos fuera de la red local. Para obtener detalles de configuración, consulte ShareConnect.

FQDN de inscripción para cada modo de administración

MODO DE ADMINISTRACIÓN	FQDN DE INSCRIPCIÓN
MDM+MAM con inscripción MDM obligatoria	FQDN del servidor de Citrix Endpoint Management
MDM+MAM con inscripción MDM opcional	FQDN del servidor de Citrix Endpoint Management
Solo MAM	FQDN del servidor de Citrix Endpoint Management

Resumen de la implementación

Si tiene muchas instancias de Citrix Endpoint Management, como para entornos de prueba, desarrollo y producción, debe configurar NetScaler Gateway para los entornos adicionales manualmente. Cuando tenga un entorno en funcionamiento, tome nota de la configuración antes de intentar configurar NetScaler Gateway manualmente para Citrix Endpoint Management.

Una decisión clave es si usar HTTPS o HTTP para la comunicación con el servidor de Citrix Endpoint Management. HTTPS proporciona comunicación segura de back-end, ya que el tráfico entre NetScaler Gateway y Citrix Endpoint Management está cifrado. El recifrado afecta al rendimiento del servidor de Citrix Endpoint Management. HTTP proporciona un mejor rendimiento

del servidor de Citrix Endpoint Management. El tráfico entre NetScaler Gateway y Citrix Endpoint Management no está cifrado. Las siguientes tablas muestran los requisitos de puerto HTTP y HTTPS para NetScaler Gateway y Citrix Endpoint Management.

HTTPS

Citrix suele recomendar SSL Bridge para las configuraciones de servidores virtuales MDM de NetScaler Gateway. Para el uso de descarga SSL de NetScaler Gateway con servidores virtuales MDM, Citrix Endpoint Management solo admite el puerto 80 como servicio de back-end.

MODO DE ADMINISTRACIÓN	MÉTODO DE EQUILIBRIO DE CARGA DE NETSCALER GATEWAY	RECIFRADO SSL	PUERTO DEL SERVIDOR DE CITRIX ENDPOINT MANAGEMENT
MAM	Descarga SSL	Habilitado	8443
MDM+MAM	MDM: SSL Bridge	N/A	443, 8443
MDM+MAM	MAM: Descarga SSL	Habilitado	8443

HTTP

MODO DE ADMINISTRACIÓN	MÉTODO DE EQUILIBRIO DE CARGA DE NETSCALER GATEWAY	RE-CIFRADO SSL	PUERTO DEL SERVIDOR DE CITRIX ENDPOINT MANAGEMENT
MAM	Descarga SSL	Habilitado	8443
MDM+MAM	MDM: Descarga SSL	No compatible	80
MDM+MAM	MAM: Descarga SSL	Habilitado	8443

Para ver diagramas de NetScaler Gateway en implementaciones de Citrix Endpoint Management, consulte Arquitectura.

Consideraciones de SSO y proxy para aplicaciones MDX

La integración de Citrix Endpoint Management con NetScaler Gateway le permite proporcionar a los usuarios inicio de sesión único (SSO) para todos los recursos HTTP/HTTPS de back-end.

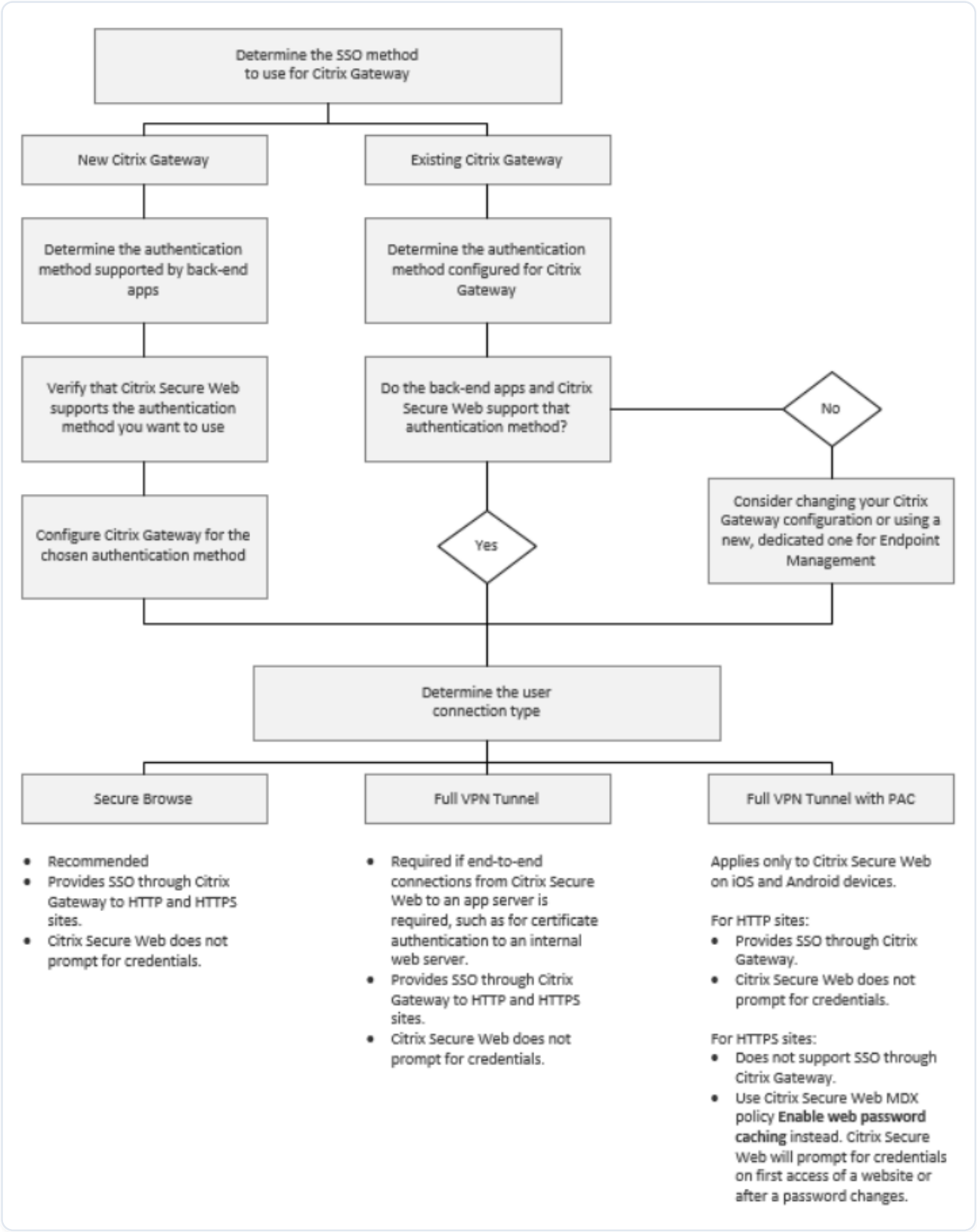
Según sus requisitos de autenticación de SSO, configure las conexiones de usuario para que una aplicación MDX utilice Secure Browse (Tunneled - Web SSO), que es un tipo de VPN sin cliente.

Importante:

Citrix dejó de admitir un túnel VPN completo y un archivo de configuración automática de proxy (PAC) con una implementación de túnel VPN completo para dispositivos iOS y Android. Para obtener más información, consulte Desuso.

Si NetScaler Gateway no es la mejor manera de proporcionar SSO en su entorno, puede configurar una aplicación MDX con almacenamiento en caché de contraseñas local basado en políticas. Este artículo explora las diversas opciones de SSO y proxy, centrándose en Citrix Secure Web. Los conceptos se aplican a otras aplicaciones MDX.

El siguiente diagrama de flujo resume el flujo de decisiones para SSO y las conexiones de usuario.



Métodos de autenticación de NetScaler Gateway

Esta sección proporciona información general sobre los métodos de autenticación compatibles con NetScaler Gateway.

Autenticación SAML

Cuando configura NetScaler Gateway para Security Assertion Markup Language (SAML), los usuarios pueden conectarse a aplicaciones web que admiten el protocolo SAML para el inicio de sesión único. NetScaler Gateway admite el inicio de sesión único del proveedor de identidades (IdP) para aplicaciones web SAML.

Configuración requerida:

- Configure el SSO de SAML en el perfil de tráfico de NetScaler Gateway.
- Configure el IdP de SAML para el servicio solicitado.

Autenticación NTLM

Si el inicio de sesión único (SSO) en las aplicaciones web está habilitado en el perfil de sesión, NetScaler Gateway realiza la autenticación NTLM automáticamente.

Configuración necesaria:

- Habilite el inicio de sesión único (SSO) en el perfil de sesión o de tráfico de NetScaler Gateway.

Suplantación de Kerberos

Citrix Endpoint Management solo admite Kerberos para Citrix Secure Web. Al configurar NetScaler Gateway para el inicio de sesión único (SSO) de Kerberos, NetScaler Gateway utiliza la suplantación cuando una contraseña de usuario está disponible para NetScaler Gateway. La suplantación significa que NetScaler Gateway utiliza las credenciales de usuario para obtener el tíquet necesario para acceder a los servicios, como Citrix Secure Web.

Configuración necesaria:

- Configure la política de sesión `Worx` de NetScaler Gateway para permitirle identificar el dominio Kerberos de su conexión.
- Configure una cuenta de delegación restringida de Kerberos (KCD) en NetScaler Gateway. Configure esa cuenta sin contraseña y vincúlela a una política de tráfico en su puerta de enlace de Citrix Endpoint Management.
- Para obtener estos y otros detalles de configuración, consulte el blog de Citrix: WorxWeb and Kerberos Impersonation SSO.

Delegación restringida de Kerberos

Citrix Endpoint Management solo admite Kerberos para Citrix Secure Web. Al configurar NetScaler Gateway para el inicio de sesión único (SSO) de Kerberos, NetScaler Gateway utiliza la delegación restringida cuando una contraseña de usuario no está disponible para NetScaler Gateway.

Con la delegación restringida, NetScaler Gateway utiliza una cuenta de administrador especificada para obtener tíquets para usuarios y servicios.

Configuración necesaria:

- Configure una cuenta KCD en Active Directory con los permisos necesarios y una cuenta KDC en NetScaler Gateway.
- Habilite el inicio de sesión único (SSO) en el perfil de tráfico de NetScaler Gateway.
- Configure el sitio web de back-end para la autenticación Kerberos.

Autenticación de relleno de formularios

Cuando configura NetScaler Gateway para el inicio de sesión único basado en formularios, los usuarios pueden iniciar sesión una vez para acceder a todas las aplicaciones protegidas de su red. Este método de autenticación se aplica a las aplicaciones que utilizan el modo Tunneled - Web SSO.

Configuración necesaria:

- Configure un SSO basado en formularios en el perfil de tráfico de NetScaler Gateway.

Autenticación HTTP Digest

Si habilita el SSO para aplicaciones web en el perfil de sesión, NetScaler Gateway realiza la autenticación HTTP Digest automáticamente. Este método de autenticación se aplica a las aplicaciones que utilizan el modo Tunneled - Web SSO.

Configuración necesaria:

- Habilite el SSO en el perfil de sesión o de tráfico de NetScaler Gateway.

Autenticación HTTP básica

Si habilita el SSO para aplicaciones web en el perfil de sesión, NetScaler Gateway realiza la autenticación HTTP básica automáticamente. Este método de autenticación se aplica a las aplicaciones que utilizan el modo Tunneled - Web SSO.

Configuración necesaria:

- Habilite el SSO en el perfil de sesión o de tráfico de NetScaler Gateway.

SSO web tunelizado seguro

Esta sección describe los tipos de conexión de usuario **Tunneled - Web SSO** para Citrix Secure Web.

Las conexiones que se tunelizan a la red interna pueden usar una variación de una VPN sin cliente, denominada Tunneled - Web SSO. Tunneled - Web SSO es la configuración predeterminada especificada para la directiva Citrix Secure Web **Preferred VPN mode**. Citrix recomienda Tunneled - Web SSO para las conexiones que requieren inicio de sesión único (SSO).

En el modo Tunneled - Web SSO, NetScaler Gateway divide la sesión HTTPS en dos partes:

- Del cliente a NetScaler Gateway
- De NetScaler Gateway al servidor de recursos de back-end.

De esta manera, NetScaler Gateway tiene visibilidad completa de todas las transacciones entre el cliente y el servidor, lo que le permite proporcionar SSO.

También puede configurar servidores proxy para Citrix Secure Web cuando se usa en modo Tunneled - Web SSO. Para obtener más información, consulte la entrada del blog Citrix Endpoint Management WorxWeb Traffic Through Proxy Server in Secure Browse Mode.

> **Nota:**
>
> Citrix anunció la desaprobación del túnel VPN completo con PAC. Consulte Deprecación.

> Citrix Endpoint Management admite la autenticación de proxy proporcionada por NetScaler Gateway. Un archivo PAC tiene reglas que definen cómo los exploradores web seleccionan un proxy para acceder a una URL determinada. Las reglas del archivo PAC pueden especificar el manejo tanto para sitios internos como externos. Citrix Secure Web analiza las reglas del archivo PAC y envía la información del servidor proxy a NetScaler Gateway. NetScaler Gateway no tiene conocimiento del archivo PAC ni del servidor proxy.

Para la autenticación en sitios web HTTPS: La directiva MDX de Citrix Secure Web **Enable web password caching** permite a Citrix Secure Web autenticarse y proporcionar SSO al servidor proxy a través de MDX.

Tunelización dividida de NetScaler Gateway

Al planificar la configuración de SSO y proxy, también debe decidir si usar la tunelización dividida de NetScaler Gateway. Citrix recomienda usar la tunelización dividida de NetScaler Gateway solo si es necesario. Esta sección ofrece una visión general de cómo funciona la tunelización dividida: NetScaler Gateway determina la ruta del tráfico en función de su tabla de enrutamiento. Cuando la tunelización dividida de NetScaler Gateway está activada, Citrix Secure Hub distingue el tráfico de red interno (protegido) del tráfico de Internet. Citrix Secure Hub realiza esa determinación basándose en el sufijo DNS y las aplicaciones de Intranet. Citrix Secure Hub solo tuneliza el tráfico de red interno a través del túnel VPN. Cuando la tunelización dividida de NetScaler Gateway está desactivada, todo el tráfico pasa por el túnel VPN.

Si prefiere supervisar todo el tráfico por motivos de seguridad, desactive la tunelización dividida de NetScaler Gateway. Como resultado, todo el tráfico pasa por el túnel VPN.

NetScaler Gateway también tiene un modo de tunelización dividida inversa de micro VPN. Esta configuración admite una lista de exclusión de direcciones IP que no se tunelizan a NetScaler Gateway. En su lugar, esas direcciones se envían mediante la conexión a Internet del dispositivo. Para obtener más información sobre la tunelización dividida inversa, consulte la documentación de NetScaler Gateway.

Citrix Endpoint Management incluye una **Reverse split tunnel exclusion list**. Para evitar que ciertos sitios web se tunelicen a través de NetScaler Gateway: Agregue una lista separada por comas de nombres de dominio completos (FQDN) o sufijos DNS que se conecten mediante la LAN en su lugar. Esta lista se aplica solo al modo Tunneled - Web SSO con NetScaler Gateway configurado para tunelización dividida inversa.

Autenticación

En una implementación de Citrix Endpoint Management, entran en juego varias consideraciones al decidir cómo configurar la autenticación. Esta sección describe los diversos factores que afectan a la autenticación:

- Las principales directivas MDX, las propiedades de cliente de Citrix Endpoint Management y la configuración de NetScaler Gateway implicadas en la autenticación.
- Las formas en que estas directivas, propiedades de cliente y configuraciones interactúan.
- Las ventajas y desventajas de cada elección.

Este artículo también incluye tres ejemplos de configuraciones recomendadas para grados crecientes de seguridad.

En términos generales, una seguridad más sólida da como resultado una experiencia de usuario menos óptima, porque los usuarios tienen que autenticarse con más frecuencia. La forma en que equilibre esas preocupaciones depende de las necesidades y prioridades de su organización. Revise las tres configuraciones recomendadas para comprender la interacción de las diversas opciones de autenticación.

Modos de autenticación

Autenticación en línea: Permite a los usuarios acceder a la red de Citrix Endpoint Management. Requiere una conexión a Internet.

Autenticación sin conexión: Se produce en el dispositivo. Los usuarios desbloquean la bóveda segura y tienen acceso sin conexión a elementos como correo descargado, sitios web almacenados en caché y notas.

Métodos de autenticación

FACTOR ÚNICO

LDAP: Puede configurar una conexión en Citrix Endpoint Management a uno o más directorios que cumplan con el Protocolo ligero de acceso a directorios (LDAP). Este método se usa comúnmente para proporcionar inicio de sesión único (SSO) para entornos empresariales. Puede optar por el PIN de Citrix con el almacenamiento en caché de contraseñas de Active Directory para mejorar la experiencia del usuario con LDAP. Al mismo tiempo, puede proporcionar la seguridad de contraseñas complejas en la inscripción, la caducidad de contraseñas y el bloqueo de cuentas.

Para obtener más detalles, consulte Autenticación de dominio o de dominio más token de seguridad.

Certificado de cliente: Citrix Endpoint Management puede integrarse con autoridades de certificación estándar de la industria para usar certificados como único método de autenticación en línea. Citrix Endpoint Management proporciona este certificado después de la inscripción del usuario, lo que requiere una contraseña de un solo uso, una URL de invitación o credenciales LDAP. Cuando se utiliza un certificado de cliente como método principal de autenticación, se requiere un PIN de Citrix en entornos de solo certificado de cliente para proteger el certificado en el dispositivo.

Citrix Endpoint Management solo admite la lista de revocación de certificados (CRL) para una entidad de certificación de terceros. Si tiene una CA de Microsoft configurada, Citrix Endpoint Management utiliza NetScaler Gateway para administrar la revocación. Al configurar la autenticación basada en certificados de cliente, considere si necesita configurar el ajuste de la

lista de revocación de certificados (CRL) de NetScaler Gateway, Habilitar actualización automática de CRL. Este paso garantiza que un dispositivo inscrito solo en MAM no pueda autenticarse utilizando un certificado existente en el dispositivo. Citrix Endpoint Management vuelve a emitir un nuevo certificado, ya que no restringe a un usuario la generación de un certificado de usuario si se revoca uno. Esta configuración aumenta la seguridad de las entidades PKI cuando la CRL comprueba las entidades PKI caducadas.

Para ver un diagrama que muestra la implementación necesaria para la autenticación basada en certificados o el uso de su entidad de certificación (CA) empresarial para emitir certificados de dispositivo, consulte Arquitectura.

AUTENTICACIÓN DE DOS FACTORES

LDAP + Certificado de cliente: Esta configuración es la mejor combinación de seguridad y experiencia de usuario para Citrix Endpoint Management. El uso de la autenticación LDAP y de certificado de cliente:

- Ofrece las mejores posibilidades de SSO junto con la seguridad proporcionada por la autenticación de dos factores en NetScaler Gateway.
- Proporciona seguridad con algo que los usuarios conocen (sus contraseñas de Active Directory) y algo que tienen (certificados de cliente en sus dispositivos).

Citrix Secure Mail puede configurar automáticamente y proporcionar una experiencia de usuario fluida por primera vez con la autenticación de certificado de cliente. Esa función requiere un entorno de servidor de acceso de cliente de Exchange configurado correctamente.

Para una usabilidad óptima, puede combinar la autenticación LDAP y de certificado de cliente con el PIN de Citrix y el almacenamiento en caché de contraseñas de Active Directory.

LDAP + Token: Esta configuración permite la configuración clásica de credenciales LDAP, además de una contraseña de un solo uso, utilizando el protocolo RADIUS. Para una usabilidad óptima, puede combinar esta opción con el PIN de Citrix y el almacenamiento en caché de contraseñas de Active Directory.

Directivas, configuraciones y propiedades de cliente importantes para la autenticación

Las siguientes directivas, configuraciones y propiedades de cliente entran en juego con las tres configuraciones recomendadas siguientes:

Directivas MDX

Contraseña de aplicación: Si está **Activado**, se requiere un PIN o una contraseña de Citrix para desbloquear la aplicación cuando se inicia o se reanuda después de un período de inactividad. El valor predeterminado es **Activado**.

Para configurar el temporizador de inactividad para todas las aplicaciones, establezca el valor INACTIVITY_TIMER en minutos en la consola de Citrix Endpoint Management en **Propiedades de cliente** en la ficha **Configuración**. El valor predeterminado es 15 minutos. Para deshabilitar el temporizador de inactividad, de modo que un PIN o una contraseña solo aparezcan cuando se inicie la aplicación, establezca el valor en cero.

Sesión micro VPN requerida: Si está **Activado**, el usuario debe tener una conexión a la red empresarial y una sesión activa para acceder a la aplicación en el dispositivo. Si está **Desactivado**, no se requiere una sesión activa para acceder a la aplicación en el dispositivo. El valor predeterminado es **Desactivado**.

Período máximo sin conexión (horas): Define el período máximo durante el cual una aplicación puede ejecutarse sin volver a confirmar el derecho de la aplicación y sin actualizar las directivas de Citrix Endpoint Management. Una aplicación iOS recupera nuevas directivas para las aplicaciones MDX de Citrix Endpoint Management sin interrupción para los usuarios después de cumplir las siguientes condiciones:

- Ha establecido el Período máximo sin conexión y
- Citrix Secure Hub para iOS tiene un token de NetScaler Gateway válido.

Si Citrix Secure Hub no tiene un token de NetScaler Gateway válido, los usuarios deben autenticarse a través de Citrix Secure Hub antes de que las directivas de la aplicación puedan actualizarse. El token de NetScaler Gateway puede dejar de ser válido debido a la inactividad de la sesión de NetScaler Gateway o a una directiva de tiempo de espera de sesión forzada. Cuando los usuarios inician sesión en Citrix Secure Hub de nuevo, pueden seguir ejecutando la aplicación.

Se recuerda a los usuarios que inicien sesión 30, 15 y 5 minutos antes de que expire el período. Después de la expiración, la aplicación se bloquea hasta que los usuarios inicien sesión. El valor predeterminado es **72 horas (3 días)**. El período mínimo es de 1 hora.

> **Nota:**

> Tenga en cuenta que, en un escenario en el que los usuarios viajan con frecuencia y utilizan la itinerancia internacional, el valor predeterminado de 72 horas (3 días) podría ser demasiado corto.

> **Caducidad del tíquet de servicios en segundo plano:** El período de tiempo durante el cual un tíquet de servicio de red en segundo plano permanece válido. Cuando Citrix Secure Mail se conecta a través de NetScaler Gateway a un servidor Exchange que ejecuta ActiveSync, Citrix Endpoint Management emite un token. Citrix Secure Mail utiliza ese token para conectarse al servidor Exchange interno. Esta configuración de propiedad determina la duración durante la cual Citrix Secure Mail puede usar el token sin requerir un nuevo token para la autenticación y la conexión al servidor Exchange. Cuando el límite de tiempo expira, los usuarios deben iniciar sesión de nuevo para generar un nuevo token. El valor predeterminado es **168 horas (7 días)**. Cuando este tiempo de espera expira, las notificaciones de correo se detienen.

Período de gracia requerido para la sesión de micro VPN: Determina cuántos minutos puede un usuario usar la aplicación sin conexión hasta que se valide la sesión en línea. El valor predeterminado es **0** (sin período de gracia).

Para obtener información sobre las directivas de autenticación, consulte:

- Si utiliza el SDK de MAM: Información general del SDK de MAM
- Si utiliza el MDX Toolkit: Directivas MDX de Citrix Endpoint Management para iOS y Directivas MDX de Citrix Endpoint Management para Android

Propiedades de cliente de Citrix Endpoint Management

> **Nota:**

> Las propiedades de cliente son configuraciones globales que se aplican a todos los dispositivos que se conectan a Citrix Endpoint Management.

> **PIN de Citrix:** Para una experiencia de inicio de sesión sencilla, puede optar por habilitar el PIN de Citrix. Con el PIN, los usuarios no tienen que introducir otras credenciales repetidamente, como sus nombres de usuario y contraseñas de Active Directory. Puede configurar el PIN de Citrix solo como autenticación sin conexión independiente, o combinar el PIN con el almacenamiento en caché de contraseñas de Active Directory para simplificar

> la autenticación y lograr una usabilidad óptima. Puede configurar el PIN de Citrix en **Configuración > Cliente > Propiedades del cliente** en la consola de Citrix Endpoint Management.

A continuación, se presenta un resumen de algunas propiedades importantes. Para obtener más información, consulte Propiedades del cliente.

ENABLE_PASSCODE_AUTH

Nombre para mostrar: Habilitar autenticación con PIN de Citrix

Esta clave le permite activar la funcionalidad del PIN de Citrix. Con el PIN o código de acceso de Citrix, se pide a los usuarios que definan un PIN para usarlo en lugar de su contraseña de Active Directory. Habilite esta configuración si **ENABLE_PASSWORD_CACHING** está habilitado o si Citrix Endpoint Management utiliza la autenticación de certificados.

Valores posibles: true o **false**

Valor predeterminado: false

ENABLE_PASSWORD_CACHING

Nombre para mostrar: Habilitar almacenamiento en caché de contraseñas de usuario

Esta clave le permite que la contraseña de Active Directory de los usuarios se almacene en caché localmente en el dispositivo móvil. Cuando establece esta clave en true, se pide a los usuarios que configuren un PIN o código de acceso de Citrix. La clave **ENABLE_PASSCODE_AUTH** debe establecerse en true cuando establece esta clave en **true**.

Valores posibles: true o **false**

Valor predeterminado: false

PASSCODE_STRENGTH

Nombre para mostrar: Requisito de fortaleza del PIN

Esta clave define la fortaleza del PIN o código de acceso de Citrix. Cuando cambia esta configuración, se pide a los usuarios que configuren un nuevo PIN o código de acceso de Citrix la próxima vez que se les solicite autenticarse.

Valores posibles: Bajo, **Medio** o **Fuerte**

Valor predeterminado: Medio

INACTIVITY_TIMER

Nombre para mostrar: Temporizador de inactividad

Esta clave define el tiempo en minutos que los usuarios pueden dejar sus dispositivos inactivos y luego acceder a una aplicación sin que se les solicite un PIN o código de acceso de Citrix. Para habilitar esta configuración para una aplicación MDX, debe establecer la configuración de **Código de acceso de la aplicación** en **Activado**. Si la configuración de **Código de acceso de la aplicación** está establecida en **Desactivado**, los usuarios son redirigidos a Citrix Secure Hub para realizar una autenticación completa. Cuando cambia esta configuración, el valor surte efecto la próxima vez que se solicite a los usuarios que se autentiquen. El valor predeterminado es 15 minutos.

ENABLE_TOUCH_ID_AUTH

Nombre para mostrar: Habilitar autenticación con Touch ID

Permite el uso del lector de huellas dactilares (solo en iOS) para la autenticación sin conexión. La autenticación en línea sigue requiriendo el método de autenticación principal.

ENCRYPT_SECRETS_USING_PASSCODE

Nombre para mostrar: Cifrar secretos con código de acceso

Esta clave permite que los datos confidenciales se almacenen en el dispositivo móvil en una bóveda secreta en lugar de en un almacén nativo basado en la plataforma, como el llavero de iOS. Esta clave de configuración permite un cifrado fuerte de los artefactos clave, pero también añade entropía de usuario (un código PIN aleatorio generado por el usuario que solo el usuario conoce).

Valores posibles: true o **false**

Valor predeterminado: false

Configuración de NetScaler Gateway

Tiempo de espera de la sesión: Si habilita esta configuración, NetScaler Gateway desconecta la sesión si NetScaler Gateway no detecta actividad de red durante el intervalo especificado. Esta configuración se aplica a los usuarios que se conectan con el complemento de NetScaler Gateway, Citrix Secure Hub o a través de un navegador web. El valor predeterminado es **1440 minutos**. Si establece este valor en cero, la configuración se deshabilita.

Tiempo de espera forzado: Si habilita esta configuración, NetScaler Gateway desconecta la sesión una vez transcurrido el intervalo de tiempo de espera, independientemente de lo que esté

haciendo el usuario. Cuando transcurre el intervalo de tiempo de espera, el usuario no puede realizar ninguna acción para evitar la desconexión. Esta configuración se aplica a los usuarios que se conectan con el plug-in de NetScaler Gateway, Citrix Secure Hub o a través de un explorador web. Si Citrix Secure Mail utiliza STA, un modo especial de NetScaler Gateway, esta configuración no se aplica a las sesiones de Citrix Secure Mail. El valor predeterminado es ningún valor, lo que significa que las sesiones se extienden para cualquier actividad.

Para obtener más información sobre la configuración de tiempo de espera para NetScaler Gateway, consulte la documentación de NetScaler Gateway.

Para obtener más información sobre los escenarios que solicitan a los usuarios que se autentiquen con Citrix Endpoint Management introduciendo credenciales en sus dispositivos, consulte Escenarios de solicitud de autenticación.

Configuración predeterminada

Esta configuración es la predeterminada proporcionada por:

- Asistente de NetScaler® para XenMobile
- SDK de MAM o MDX Toolkit
- Consola de Citrix Endpoint Management

CONFIGURACIÓN	DÓNDE ENCONTRAR LA CONFIGURACIÓN	CONFIGURACIÓN PREDETERMINADA
Tiempo de espera de la sesión	NetScaler Gateway	1440 minutos
Tiempo de espera forzado	NetScaler Gateway	Sin valor (desactivado)
Período máximo sin conexión	Directivas MDX	72 horas
Caducidad del tíquet de servicios en segundo plano	Directivas MDX	168 horas (7 días)
Sesión de micro VPN requerida	Directivas MDX	Desactivado
Período de gracia de sesión de micro VPN requerida	Directivas MDX	0
PIN de la aplicación	Directivas MDX	Activado

CONFIGURACIÓN	DÓNDE ENCONTRAR LA CONFIGURACIÓN	CONFIGURACIÓN PREDETERMINADA
Cifrar secretos con código de acceso	Propiedades del cliente de Citrix Endpoint Management	falso
Habilitar autenticación PIN de Citrix	Propiedades del cliente de Citrix Endpoint Management	falso
Requisito de fortaleza del PIN	Propiedades del cliente de Citrix Endpoint Management	Medio
Tipo de PIN	Propiedades del cliente de Citrix Endpoint Management	Numérico
Habilitar almacenamiento en caché de contraseñas de usuario	Propiedades del cliente de Citrix Endpoint Management	falso
Temporizador de inactividad	Propiedades del cliente de Citrix Endpoint Management	15
Habilitar autenticación Touch ID	Propiedades del cliente de Citrix Endpoint Management	falso

Configuraciones recomendadas

Esta sección ofrece ejemplos de tres configuraciones de Citrix Endpoint Management que van desde la seguridad más baja y la experiencia de usuario óptima hasta la seguridad más alta y una experiencia de usuario más intrusiva. Estos ejemplos le proporcionan puntos de referencia útiles para determinar en qué punto de la escala desea situar su propia configuración. La modificación de estos ajustes podría requerir que altere otros ajustes. Por ejemplo, el período máximo sin conexión no debe exceder el tiempo de espera de la sesión.

Máxima seguridad

Esta configuración ofrece el nivel más alto de seguridad, pero conlleva importantes desventajas en cuanto a la usabilidad.

Configuración	**Dónde encontrar la configuración**	**Configuración recomendada**	**Impacto en el comportamiento**

Tiempo de espera de la sesión	NetScaler Gateway	1440	Los usuarios introducen sus credenciales de Citrix Secure Hub solo cuando se requiere autenticación en línea, cada 24 horas.
Tiempo de espera forzado	NetScaler Gateway	Sin valor	Las sesiones se extienden si hay alguna actividad.
Período máximo sin conexión	Directivas MDX	23	Requiere la actualización de la directiva cada día.
Caducidad del tíquet de servicios en segundo plano	Directivas MDX	72 horas	Tiempo de espera para STA, que permite sesiones de larga duración sin un token de sesión de NetScaler Gateway. Para Citrix Secure Mail, hacer que el tiempo de espera de STA sea más largo que el tiempo de espera de la sesión evita que las notificaciones de correo se detengan. En ese caso, Citrix Secure Mail no le pide al usuario si no abre la aplicación antes de que expire la sesión.
sesión micro VPN requerida	Directivas MDX	Desactivado	Proporciona una conexión de red válida y una sesión

			de NetScaler Gateway para usar las aplicaciones.
período de gracia de sesión micro VPN requerida	Directivas MDX	0	Sin período de gracia (si habilitó la sesión micro VPN requerida).
Contraseña de la aplicación	Directivas MDX	Activado	Requiere una contraseña para una aplicación.
Cifrar secretos con contraseña	Propiedades del cliente de Citrix Endpoint Management	Sí	Una clave derivada de la entropía del usuario protege la bóveda.
Habilitar la autenticación PIN de Citrix	Propiedades del cliente de Citrix Endpoint Management	Sí	Habilitar el PIN de Citrix para una experiencia de autenticación simplificada.
Requisito de fortaleza del PIN	Propiedades del cliente de Citrix Endpoint Management	Fuerte	Requisitos de alta complejidad de contraseña.
Tipo de PIN	Propiedades del cliente de Citrix Endpoint Management	Alfanumérico	El PIN es una secuencia alfanumérica.
Habilitar el almacenamiento en caché de contraseñas	Propiedades del cliente de Citrix Endpoint Management	falso	La contraseña de Active Directory no se almacena en caché y se utiliza un PIN de Citrix para las autenticaciones sin conexión.

Temporizador de inactividad	Propiedades del cliente de Citrix Endpoint Management	15	Si un usuario no utiliza las aplicaciones MDX o Citrix Secure Hub durante este período, se le solicitará la autenticación sin conexión.
Habilitar la autenticación con Touch ID	Propiedades del cliente de Citrix Endpoint Management	falso	Deshabilita Touch ID para casos de uso de autenticación sin conexión en iOS.

Mayor seguridad

Un enfoque más intermedio, esta configuración requiere que los usuarios se autentiquen con más frecuencia (cada 3 días, como máximo, en lugar de 7) y una seguridad más sólida. El mayor número de autenticaciones bloquea el contenedor con más frecuencia, lo que proporciona seguridad de los datos cuando los dispositivos no están en uso.

Configuración	**Dónde encontrar la configuración**	**Configuración recomendada**	**Impacto en el comportamiento**
Tiempo de espera de la sesión	NetScaler Gateway	4320	Los usuarios introducen sus credenciales de Citrix Secure Hub solo cuando se requiere autenticación en línea, cada 3 días
Tiempo de espera forzado	NetScaler Gateway	Sin valor	Las sesiones se extienden si hay alguna actividad.
Período máximo sin conexión	Directivas MDX	71	Requiere la actualización de la directiva cada 3 días.

			La diferencia de una hora es para permitir la actualización antes de que expire la sesión.
Caducidad del ticket de servicios en segundo plano	Directivas MDX	168 horas	Tiempo de espera para STA, que permite sesiones de larga duración sin un token de sesión de NetScaler Gateway. Para Citrix Secure Mail, hacer que el tiempo de espera de STA sea más largo que el tiempo de espera de la sesión evita que las notificaciones de correo se detengan sin avisar al usuario.
Sesión de micro VPN requerida	Directivas MDX	Desactivado	Proporciona una conexión de red válida y una sesión de NetScaler Gateway para usar las aplicaciones.
Período de gracia de sesión de micro VPN requerida	Directivas MDX	0	Sin período de gracia (si habilitó la sesión de micro VPN requerida).
Contraseña de la aplicación	Directivas MDX	Activado	Requerir un código de acceso para una aplicación.
Cifrar secretos con código de acceso	Propiedades del cliente de Citrix	falso	No requerir entropía de usuario para cifrar la bóveda.

	Endpoint Management		
Habilitar la autenticación PIN de Citrix	Propiedades del cliente de Citrix Endpoint Management	verdadero	Habilitar el PIN de Citrix para una experiencia de autenticación simplificada.
Requisito de fortaleza del PIN	Propiedades del cliente de Citrix Endpoint Management	Medio	Aplica reglas de complejidad de contraseña media.
Tipo de PIN	Propiedades del cliente de Citrix Endpoint Management	Numérico	Un PIN es una secuencia numérica.
Habilitar el almacenamiento en caché de contraseñas	Propiedades del cliente de Citrix Endpoint Management	verdadero	El PIN del usuario almacena en caché y protege la contraseña de Active Directory.
Temporizador de inactividad	Propiedades del cliente de Citrix Endpoint Management	30	Si un usuario no utiliza las aplicaciones MDX o Citrix Secure Hub durante este período, se le solicitará la autenticación sin conexión.
Habilitar la autenticación con Touch ID	Propiedades del cliente de Citrix Endpoint Management	verdadero	Habilita Touch ID para casos de uso de autenticación sin conexión en iOS.

Alta seguridad

Esta configuración, la más conveniente para los usuarios, proporciona seguridad de nivel básico.

Configuración	Dónde encontrar la configuración	Configuración recomendada	Impacto en el comportamiento
Tiempo de espera de la sesión	NetScaler Gateway	10080	Los usuarios introducen sus credenciales de Citrix Secure Hub solo cuando se requiere autenticación en línea, cada 7 días.
Tiempo de espera forzado	NetScaler Gateway	Sin valor	Las sesiones se extienden si hay alguna actividad.
Período máximo sin conexión	Directivas MDX	167	Requiere la actualización de la directiva cada semana (cada 7 días). La diferencia horaria es para permitir la actualización antes de que caduque la sesión.
Caducidad del tíquet de servicios en segundo plano	Directivas MDX	240	Tiempo de espera para STA, lo que permite sesiones de larga duración sin un token de sesión de NetScaler Gateway. Para Citrix Secure Mail, hacer que el tiempo de espera de STA sea más largo que el tiempo de espera de la sesión evita que las notificaciones de correo se detengan.

			En ese caso, Citrix Secure Mail no solicita al usuario si no abre la aplicación antes de que caduque la sesión.
Sesión de micro VPN requerida	Directivas MDX	Desactivado	Proporciona una conexión de red válida y una sesión de NetScaler Gateway para usar las aplicaciones.
Período de gracia requerido para la sesión de micro VPN	Directivas MDX	0	Sin período de gracia (si habilitó la sesión de micro VPN requerida).
Contraseña de la aplicación	Directivas MDX	Activado	Requerir un código de acceso para una aplicación.
Cifrar secretos mediante código de acceso	Propiedades del cliente de Citrix Endpoint Management	falso	No requerir entropía de usuario para cifrar el almacén.
Habilitar la autenticación con PIN de Citrix	Propiedades del cliente de Citrix Endpoint Management	verdadero	Habilitar el PIN de Citrix para una experiencia de autenticación simplificada.
Requisito de fortaleza del PIN	Propiedades del cliente de Citrix Endpoint Management	Baja	Sin requisitos de complejidad de contraseña
Tipo de PIN	Propiedades del cliente de Citrix	Numérico	Un PIN es una secuencia numérica.

	Endpoint Management		
Habilitar el almacenamiento en caché de contraseñas	Propiedades del cliente de Citrix Endpoint Management	verdadero	El PIN de usuario almacena en caché y protege la contraseña de Active Directory.
Temporizador de inactividad	Propiedades del cliente de Citrix Endpoint Management	90	Si un usuario no utiliza las aplicaciones MDX o Citrix Secure Hub durante este período, se le solicitará la autenticación sin conexión.
Habilitar la autenticación Touch ID	Propiedades del cliente de Citrix Endpoint Management	verdadero	Habilita Touch ID para casos de uso de autenticación sin conexión en iOS.

Uso de la autenticación de paso a paso

Algunas aplicaciones pueden requerir una autenticación mejorada. Por ejemplo, un factor de autenticación secundario, como un token o tiempos de espera de sesión agresivos. Este método de autenticación se controla mediante una política MDX. El método también requiere un servidor virtual independiente para controlar los métodos de autenticación (ya sea en el mismo dispositivo NetScaler Gateway o en dispositivos separados).

CONFIGURACIÓN	DÓNDE ENCONTRAR LA CONFIGURACIÓN	CONFIGURACIÓN RECOMENDADA	IMPACTO EN EL COMPORTAMIENTO
NetScaler Gateway alternativo	Políticas MDX	Requiere el FQDN y el puerto del dispositivo NetScaler Gateway secundario.	Permite una autenticación mejorada controlada por las políticas de autenticación y sesión del dispositivo

CONFIGURACIÓN	DÓNDE ENCONTRAR LA CONFIGURACIÓN	CONFIGURACIÓN RECOMENDADA	IMPACTO EN EL COMPORTAMIENTO
			NetScaler Gateway secundario.

Si un usuario abre una aplicación que utiliza el NetScaler Gateway alternativo, todas las demás aplicaciones utilizan esa instancia de NetScaler Gateway para comunicarse con la red interna. La sesión solo vuelve a la instancia de NetScaler Gateway de menor seguridad cuando la sesión caduca en la instancia de NetScaler Gateway con seguridad mejorada.

Uso de la sesión de micro VPN requerida

Para ciertas aplicaciones, como Citrix Secure Web, puede asegurarse de que los usuarios ejecuten una aplicación solo cuando tengan una sesión autenticada. Esta política aplica esa opción y permite un período de gracia para que los usuarios puedan terminar su trabajo.

CONFIGURACIÓN	DÓNDE ENCONTRAR LA CONFIGURACIÓN	CONFIGURACIÓN RECOMENDADA	IMPACTO EN EL COMPORTAMIENTO
Sesión de micro VPN requerida	Directivas MDX	Activado	Garantiza que un dispositivo esté en línea y tenga un token de autenticación válido.
Período de gracia de sesión de micro VPN requerida	Directivas MDX	15	Permite un período de gracia de 15 minutos antes de que el usuario ya no pueda usar las aplicaciones.

Propiedades del servidor

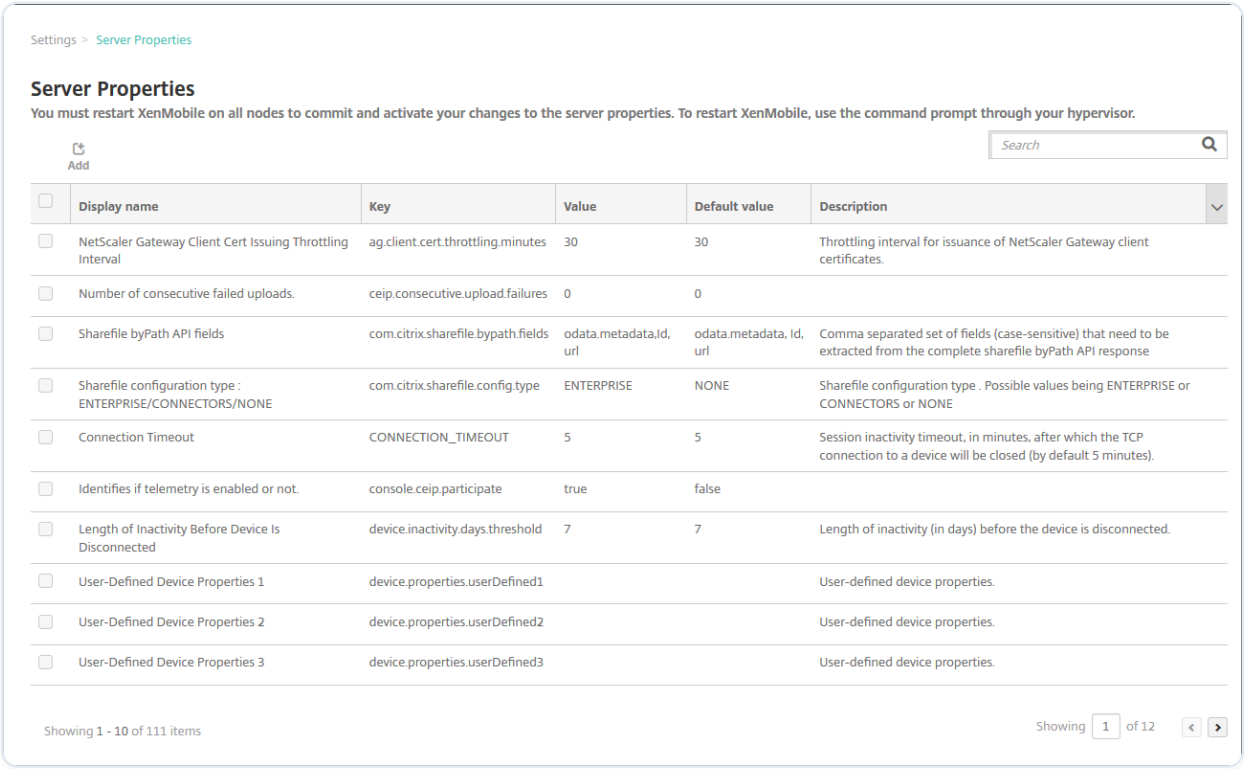
Las propiedades del servidor son propiedades globales que se aplican a las operaciones, los usuarios y los dispositivos en toda una instancia de Citrix Endpoint Management. Citrix recomienda que evalúe para su entorno las propiedades del servidor que se tratan en este artículo. Asegúrese de consultar con Citrix antes de cambiar otras propiedades del servidor.

Para actualizar las propiedades del servidor, vaya a **Parámetros > Propiedades del servidor**.

Agregar, modificar o eliminar propiedades del servidor

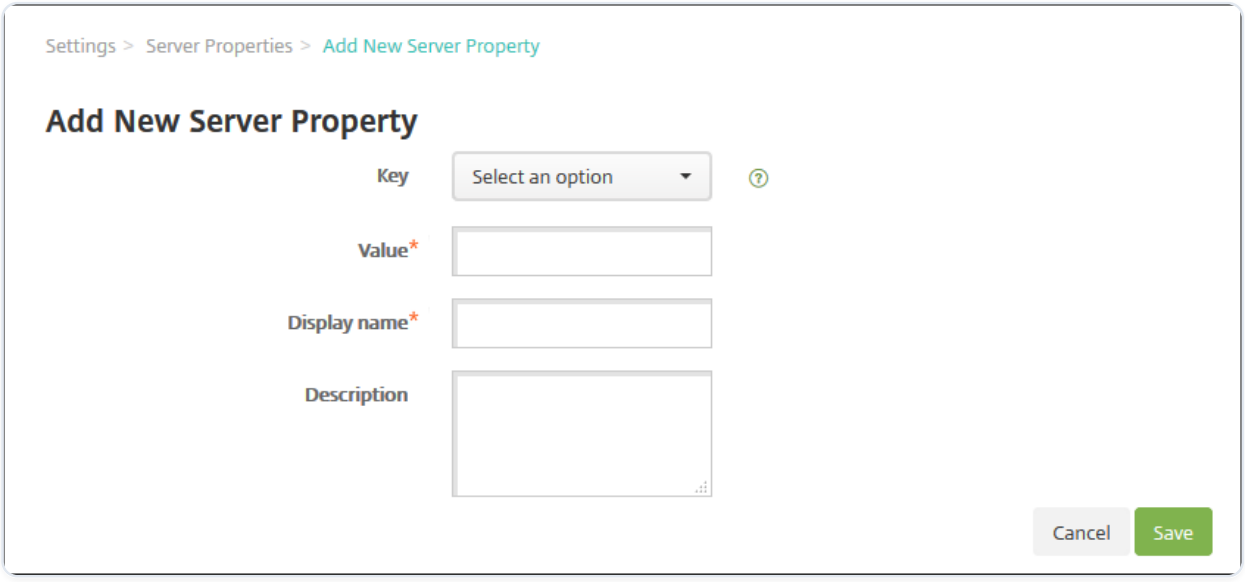
En Citrix Endpoint Management, puede aplicar propiedades al servidor.

1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje de la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En **Servidor**, haga clic en **Propiedades del servidor**. Aparecerá la página **Propiedades del servidor**. Desde esta página, puede agregar, modificar o eliminar propiedades del servidor.



Para agregar una propiedad del servidor

1. Haga clic en **Agregar**. Aparecerá la página **Agregar nueva propiedad del servidor**.



2. Configure estos parámetros:

   - Clave: En la lista, seleccione la clave adecuada. Las claves distinguen entre mayúsculas y minúsculas. Póngase en contacto con el Soporte técnico de Citrix antes de modificar los valores de las propiedades o para solicitar una clave especial.
   - Valor: Introduzca un valor en función de la clave que haya seleccionado.
   - Nombre para mostrar: Introduzca un nombre para el nuevo valor de propiedad que aparece en la tabla **Propiedades del servidor**.
   - Descripción: Opcionalmente, escriba una descripción para la nueva propiedad del servidor.

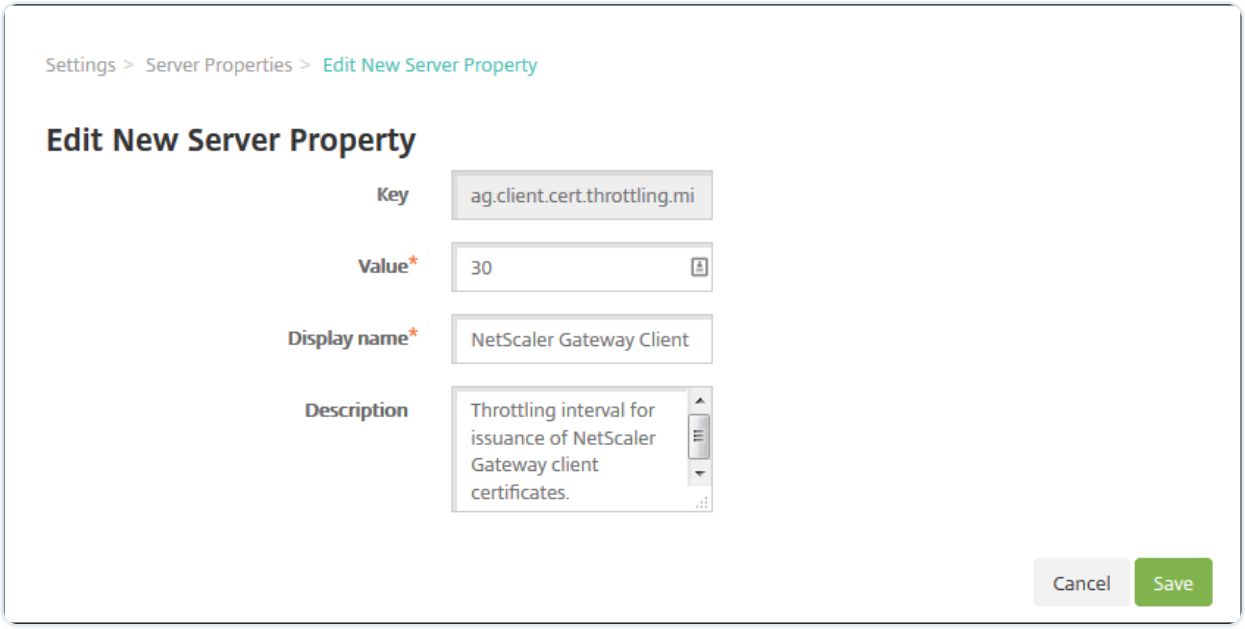
3. Haga clic en **Guardar**.

Para editar una propiedad del servidor

1. En la tabla **Propiedades del servidor**, seleccione la propiedad del servidor que desea editar.

   Cuando selecciona la casilla de verificación junto a una propiedad del servidor, el menú de opciones aparece encima de la lista de propiedades del servidor. Haga clic en cualquier otro lugar de la lista para abrir el menú de opciones en el lado derecho de la lista.

2. Haga clic en **Editar**. Aparece la página **Editar nueva propiedad del servidor**.



3. Cambie la siguiente información según corresponda:

   - Clave: No puede cambiar este campo.
   - Valor: El valor de la propiedad.
   - Nombre para mostrar: El nombre de la propiedad.

- Descripción: La descripción de la propiedad.

4. Haga clic en **Guardar** para guardar los cambios o en **Cancelar** para dejar la propiedad sin cambios.

Para eliminar una propiedad del servidor

1. En la tabla **Propiedades del servidor**, seleccione las propiedades del servidor que desea eliminar.
2. Haga clic en **Eliminar**. Aparece un cuadro de diálogo de confirmación. Vuelva a hacer clic en **Eliminar**.

Definiciones de propiedades del servidor

Acceder a todas las aplicaciones en la tienda de Google Play administrada

- Si es **true**, Citrix Endpoint Management hace que todas las aplicaciones de la tienda pública de Google Play sean accesibles desde la tienda de Google Play administrada. Puede utilizar la directiva de dispositivo Restricciones para controlar el acceso a estas aplicaciones. El valor predeterminado es **false**.

Agregar dispositivo siempre

- Si es **true**, Citrix Endpoint Management agrega un dispositivo a la consola de Citrix Endpoint Management, incluso si falla la inscripción. Como resultado, puede ver qué dispositivos intentaron inscribirse. El valor predeterminado es **false**.

Intervalo de limitación de emisión de certificados de cliente AG

- El período de gracia entre la generación de certificados. Este intervalo evita que Citrix Endpoint Management genere muchos certificados para un dispositivo en un corto período de tiempo. Citrix recomienda no cambiar este valor. El valor predeterminado es **30** minutos.

Permite la eliminación de dispositivos marcados como inactivos durante un período de tiempo especificado

- Si es **true**, los dispositivos que han estado inactivos durante un tiempo especificado (en días) se eliminan de Citrix Endpoint Management. El período de actividad se establece mediante la propiedad de servidor **Length of Time Device Can Be Inactive Before Being Automatically Removed From CEM**. El valor predeterminado es **true**. Para cambiar el valor de esta propiedad, consulte a su representante de Citrix.

Registrador de auditoría

- Si es **False**, no registra eventos de la interfaz de usuario (UI). El valor predeterminado es **False**.

Bloquear la inscripción de dispositivos Android rooteados y iOS con jailbreak

Cuando esta propiedad se establece en **true**, Citrix Endpoint Management bloquea las inscripciones de dispositivos Android rooteados y dispositivos iOS con jailbreak. La configuración recomendada es **true** para todos los niveles de seguridad. El valor predeterminado es **true**.

cdn.s3.retry.interval y cdn.s3.max.retry

Las propiedades de servidor `cdn.s3.retry.interval` y `cdn.s3.max.retry` funcionan conjuntamente para establecer el límite de tiempo máximo en cada carga de archivo PKG de macOS. De forma predeterminada, Citrix Endpoint Management limita los tiempos de carga de archivos a 100 segundos. Si una carga de archivo supera ese límite, la carga falla. Para cambiar el valor predeterminado, configure las claves `cdn.s3.retry.interval` y `cdn.s3.max.retry` de la siguiente manera:

- `cdn.s3.retry.interval`. Permite definir el intervalo, en milisegundos, en el que Citrix Endpoint Management verifica si una carga de archivo se completa correctamente. El valor predeterminado es `10000`.
- `cdn.s3.max.retry`. Permite definir el número máximo de reintentos de verificación después de los cuales la carga falla. El valor predeterminado es `10`.

Las dos claves funcionan conjuntamente para limitar los tiempos de carga de archivos. De forma predeterminada, el límite de tiempo es de 100 segundos (10000*10 milisegundos).

Renovación de certificados en segundos

- Número de segundos antes de que caduque un certificado en los que Citrix Endpoint Management comienza a renovar los certificados. Un ejemplo es cuando un certificado caduca el 30 de diciembre y esta propiedad se establece en 30 días. Si el dispositivo se conecta entre el 1 y el 30 de diciembre, Citrix Endpoint Management intenta renovar el certificado. El valor predeterminado es **2592000** segundos (30 días).

Tiempo de espera de conexión

- Tiempo de espera de inactividad de la sesión, en minutos, tras el cual Citrix Endpoint Management cierra la conexión TCP a un dispositivo. La sesión permanece abierta. Se aplica a dispositivos Android. El valor predeterminado es **5** minutos.

Canal de implementación predeterminado

- Determina cómo Citrix Endpoint Management implementa un recurso en un dispositivo: a nivel de usuario (**DEFAULT_TO_USER**) o a nivel de dispositivo. El valor predeterminado es **DEFAULT_TO_DEVICE**.

Desaprobar proveedor de servicios móviles

- Desaprueba la compatibilidad con la interfaz del proveedor de servicios móviles utilizada para consultar dispositivos Blackberry y otros dispositivos Exchange ActiveSync. Cuando está habilitada, la interfaz del **proveedor de servicios móviles** está oculta en la consola. El valor predeterminado es **true**.

Etiquetado de dispositivos

- Si establece `enable.device.tagging` en **true**, Citrix Endpoint Management etiqueta los dispositivos automáticamente por tipo de dispositivo. Puede usar las etiquetas de dispositivo para implementar directivas y aplicaciones o configurar grupos de entrega. Citrix Endpoint Management aplica etiquetas a los dispositivos para lo siguiente:
    - Etiquetas BYOD
        - Inscripción de usuario de iOS
        - Perfil de trabajo de Android Enterprise
    - Etiquetas corporativas
        - Dispositivos corporativos totalmente administrados de Android Enterprise
        - Inscripción masiva
            - Dispositivos de Apple Business Manager
            - Dispositivos de Apple School Manager
            - Dispositivos de Windows AutoPilot
            - Inscripción masiva de Android Enterprise

Deshabilitar la verificación del nombre de host

- De forma predeterminada, la verificación del nombre de host está habilitada en las conexiones salientes, excepto para el servidor PKI de Microsoft. Cuando la verificación del nombre de host falla, el registro del servidor incluye errores como: "No se puede conectar al servidor de compra por volumen: el nombre de host '192.0.2.0' no coincide con el asunto del certificado

proporcionado por el par". Si la verificación del nombre de host interrumpe su implementación, cambie esta propiedad a **true**. El valor predeterminado es **false**.

Deshabilitar la verificación del servidor SSL

- Si es **True**, deshabilita la validación del certificado del servidor SSL cuando se cumplen todas las condiciones siguientes:
  - Ha habilitado la autenticación basada en certificados en Citrix Endpoint Management
  - El servidor CA de Microsoft es el emisor del certificado
  - Una CA interna, cuya raíz Citrix Endpoint Management no confía, firmó su certificado.

  El valor predeterminado es **True**.

Habilitar informes de fallos

- Si es **true**, Citrix recopila informes de fallos y diagnósticos para ayudar a solucionar problemas con Citrix Secure Hub para iOS y Android. Si es **false**, no se recopilan datos. El valor predeterminado es **true**.

Habilitar/deshabilitar el registro de estadísticas de Hibernate para diagnósticos

- Si es **True**, habilita el registro de estadísticas de Hibernate para ayudar a solucionar problemas de rendimiento de la aplicación. Hibernate es un componente utilizado para las conexiones de Citrix Endpoint Management a un Microsoft SQL Server. De forma predeterminada, el registro está deshabilitado porque afecta al rendimiento de la aplicación. Habilite el registro solo por un corto período para evitar crear un archivo de registro enorme. Citrix Endpoint Management escribe los registros en /opt/sas/logs/hibernate_stats.log. El valor predeterminado es **False**.

Habilitar OTAE de macOS

- Si es **false**, impide el uso de un enlace de inscripción para dispositivos macOS, lo que significa que los usuarios de macOS solo pueden inscribirse mediante una invitación de inscripción. El valor predeterminado es **true**.

Habilitar activador de notificaciones

- Habilita o deshabilita las notificaciones del cliente de Citrix Secure Hub. El valor **true** habilita las notificaciones. El valor predeterminado es **true**.

Extracción completa de usuarios permitidos y denegados de ActiveSync

- El intervalo (en segundos) en el que Citrix Endpoint Management extrae una lista completa (línea base) de usuarios permitidos y denegados de ActiveSync. El valor predeterminado es **28800** segundos.

Identifica si la telemetría está habilitada o no

- Identifica si la telemetría está habilitada. La telemetría también se conoce como Programa de mejora de la experiencia del cliente (CEIP). Puede participar en CEIP al instalar o actualizar Citrix Endpoint Management. Si Citrix Endpoint Management tiene 15 cargas fallidas consecutivas, deshabilita la telemetría. El valor predeterminado es **false**.

Tiempo de espera por inactividad en minutos

- El número de minutos después de los cuales Citrix Endpoint Management cierra la sesión de un usuario inactivo. El usuario debe haber utilizado la API pública de Citrix Endpoint Management para acceder a la consola de Citrix Endpoint Management o a cualquier aplicación de terceros. Un valor de tiempo de espera de **0** significa que un usuario inactivo permanece conectado. Para las aplicaciones de terceros que acceden a la API, normalmente es necesario permanecer conectado. El valor predeterminado se establece en **5**.
- Si la propiedad de servidor **WebServices timeout type** es **INACTIVITY_TIMEOUT:** Esta propiedad define el número de minutos después de los cuales Citrix Endpoint Management cierra la sesión de un administrador inactivo que hizo lo siguiente:
  - Utilizó la API pública para servicios REST para acceder a la consola de Citrix Endpoint Management
  - Utilizó la API pública para servicios REST para acceder a cualquier aplicación de terceros. Un tiempo de espera de **0** significa que un usuario inactivo permanece conectado.

include.device.properties.during.search

- Incluye todas las propiedades del dispositivo en una búsqueda de dispositivos. El valor predeterminado es **Off**, lo que limita el ámbito de búsqueda a estas propiedades del dispositivo, para una búsqueda rápida:
  - Número de serie
  - IMEI
  - Dirección MAC de Wi-Fi
  - Dirección MAC de Bluetooth
  - ID de Active Sync

- Nombre de usuario

Cuando esta propiedad se establece en **On**, las búsquedas de dispositivos pueden tardar más.

ios.delayBeforeDeclareUnreachable; macos.delayBeforeDeclareUnreachable

- Especifica el número de días después de los cuales un dispositivo iOS o macOS sin conexión se considera inalcanzable. Cuando un dispositivo iOS o macOS alcanza el límite especificado, deja de comunicarse con Citrix Endpoint Management. Ambas propiedades tienen un valor predeterminado de **45** días.

Inscripción de gestión de dispositivos iOS: instalar CA raíz si es necesario

- La propiedad del servidor **ios.mdm.enrollment.installRootCalfRequired** está establecida en **False** para todos los entornos de Citrix Endpoint Management. Citrix Endpoint Management utiliza una cadena de certificados de confianza pública, por lo que no es necesario enviar una CA raíz a los dispositivos. (Esta propiedad se utiliza solo para entornos locales).

Inscripción de gestión de dispositivos iOS: último paso retrasado

- Durante la inscripción de dispositivos, este valor de propiedad especifica el tiempo de espera entre la instalación del perfil MDM y el inicio del Agente en el dispositivo. Citrix recomienda que edite esta propiedad solo para problemas de latencia o velocidad de red. En ese caso, no establezca el valor en más de 5000 milisegundos (5 segundos). El valor predeterminado es **1000** milisegundos (1 segundo).

Modo de entrega de identidad de gestión de dispositivos iOS

- Especifica si Citrix Endpoint Management distribuye el certificado MDM a los dispositivos mediante **SCEP** (recomendado por razones de seguridad) o **PKCS12**. En el modo PKCS12, el par de claves se genera en el servidor y no se realiza ninguna negociación. El valor predeterminado es **SCEP**.

Tamaño de clave de identidad de gestión de dispositivos iOS

- Define el tamaño de las claves privadas para las identidades MDM, el servicio de perfiles de iOS y las identidades de agente de iOS de Citrix Endpoint Management. El valor predeterminado es **2048**.

Días de renovación de identidad de gestión de dispositivos iOS

- Especifica el número de días antes de la caducidad del certificado en que Citrix Endpoint Management comienza a renovar los certificados. Por ejemplo: Si un certificado caduca en 10 días y esta propiedad es de **10** días: Cuando un dispositivo se conecta 9 días antes de la

caducidad, Citrix Endpoint Management emite un nuevo certificado. El valor predeterminado es **30** días.

Contraseña de clave privada de APNS de iOS MDM

- Esta propiedad contiene la contraseña de APNs, que es necesaria para que Citrix Endpoint Management envíe notificaciones a los servidores de Apple.

Duración de la inactividad antes de que se desconecte el dispositivo

- Especifica cuánto tiempo puede estar inactivo un dispositivo, incluida la última autenticación, antes de que Citrix Endpoint Management lo desconecte. El valor predeterminado es **7** días.

Tiempo que un dispositivo puede estar inactivo antes de ser eliminado automáticamente de CEM

- La duración (en días) que un dispositivo puede estar inactivo antes de ser eliminado automáticamente de Citrix Endpoint Management. El mínimo es de **14** días y el valor predeterminado es de **30** días. La propiedad de servidor **Allows The Removal of Devices That Have Been Marked Inactive For A Specified Period Of Time** debe establecerse en **true** para que esta propiedad surta efecto.

local.user.account.lockout.time

- Especifica el número de minutos que un usuario debe esperar después de exceder el límite de bloqueo. Los valores admitidos son 0–999. El valor predeterminado es de **30** minutos.

local.user.account.lockout.limit

- Especifica el número máximo de intentos de inicio de sesión no válidos consecutivos por usuario. Los valores admitidos son 0–999. El valor predeterminado es **6**.

mac.dep.admin.passwd.rotate

Esta propiedad de servidor le permite configurar los intervalos de rotación de contraseñas de administrador para dispositivos macOS inscritos a través del Programa de implementación de Apple. Citrix Endpoint Management comprueba diariamente si debe rotar la contraseña de la cuenta de administrador. De forma predeterminada, Citrix Endpoint Management rota la contraseña cada 10 080 minutos (7 días). Configure la clave `mac.dep.admin.passwd.rotate` de la siguiente manera:

- Valor: *definido por el administrador* El intervalo, en minutos, en el que Citrix Endpoint Management rota la contraseña. Escriba un valor igual o superior a 360 (6 horas). Citrix

Endpoint Management ignora los valores inferiores a 360 y, en su lugar, rota la contraseña cada 360 minutos (6 horas).

- Nombre para mostrar: *definido por el administrador*
- Descripción: *definida por el administrador*

Máximo de dispositivos solo MAM

- Esta clave personalizada limita el número de dispositivos solo MAM que cada usuario puede inscribir. Configure la clave de la siguiente manera. Un **Valor** de **0** permite la inscripción ilimitada de dispositivos.
- Clave = **number.of.mam.devices.per.user**
- Valor = **5**
- Nombre para mostrar = **Máximo de dispositivos solo MAM**
- Description = **Limita el número de dispositivos MAM que cada usuario puede inscribir.**

MaxNumberOfWorker

- El número de subprocesos utilizados al importar muchas licencias de compra por volumen. El valor predeterminado es **3**. Si necesita una mayor optimización, puede aumentar el número de subprocesos. Sin embargo, un mayor número de subprocesos provoca un alto uso de la CPU.

Inicio de sesión único de NetScaler Gateway (NetScaler)

- Si es **False**, inhabilita la función de devolución de llamada de Citrix Endpoint Management durante el inicio de sesión único de NetScaler Gateway a Citrix Endpoint Management. Si la configuración de NetScaler Gateway incluye una URL de devolución de llamada, Citrix Endpoint Management utiliza la función de devolución de llamada para verificar el ID de sesión de NetScaler Gateway. El valor predeterminado es **False**.

Número de cargas fallidas consecutivas

- Muestra el número de errores consecutivos durante las cargas del Programa de mejora de la experiencia del cliente (CEIP). Citrix Endpoint Management incrementa el valor cuando falla una carga. Después de 15 errores de carga, Citrix Endpoint Management inhabilita el CEIP, también llamado telemetría. Para obtener más información, consulte la propiedad del servidor **Identifies if telemetry is enabled or not**. Citrix Endpoint Management restablece el valor a **0** cuando una carga se realiza correctamente.

Número de usuarios por dispositivo

- El número máximo de usuarios que pueden inscribir el mismo dispositivo en MDM. El valor **0** significa que un número ilimitado de usuarios puede inscribir el mismo dispositivo. El valor predeterminado es **0**.

optional.user.identity.attributes

- Esta propiedad del servidor le permite personalizar los atributos de usuario opcionales de Active Directory.

  Cree la clave personalizada y, en el campo **Valores**, edite los atributos de usuario para definir a qué atributos puede acceder Citrix Endpoint Management para crear una cuenta de usuario. Para obtener más información, consulte Personalizar propiedades de usuario.

  - Clave: **Clave personalizada**
  - Clave: **optional.user.identity.attributes**
  - Valor: **commonName, firstName, lastName, displayName, streetAddress, city, state, country, workPhone, homePhone, mobilePhone, company, department, description, employeeID, faxNumber, initials, ipPhone, manager, homePostalAddress, otherMobile, pager, physicalDeliveryOfficeName, postalCode, postOfficeBox, title, organization, preferredLanguage**
  - Nombre para mostrar: **optional.user.identity.attributes**
  - Descripción: **Atributos de usuario opcionales de Active Directory**

Nombre de la organización para perfiles de inscripción de macOS y iOS/iPadOS

- El valor que escriba para `apple.mdm.enrollment.profile.organization.name` corresponde al nombre de la organización que proporciona el perfil de inscripción. El nombre se muestra cuando los usuarios inscriben su dispositivo en Citrix Endpoint Management. El nombre predeterminado que se muestra es **Citrix Workspace**.

Extracción de cambios incrementales de usuarios permitidos y denegados

- Número de segundos que Citrix Endpoint Management espera una respuesta del dominio al ejecutar un comando de PowerShell para obtener un delta de dispositivos ActiveSync. El valor predeterminado es **60** segundos.

Tiempo de espera de lectura para el servidor de certificación de Microsoft

- Número de segundos que Citrix Endpoint Management espera una respuesta del servidor de certificados al realizar una lectura. Si el servidor de certificados es lento y tiene mucho tráfico,

puede aumentar este valor a 60 segundos o más. Un servidor de certificados que no responde después de 120 segundos requiere mantenimiento. El valor predeterminado es **15000** milisegundos (15 segundos).

Servicios web REST

- Habilita el Servicio web REST. El valor predeterminado es **true**.

Recupera información de dispositivos en fragmentos de tamaño especificado

- Este valor se utiliza internamente para el multiproceso durante las exportaciones de dispositivos. Si el valor es mayor, un solo hilo analiza más dispositivos. Si el valor es menor, más hilos recuperan los dispositivos. Reducir el valor podría aumentar el rendimiento de las exportaciones y las recuperaciones de listas de dispositivos, pero podría reducir la memoria disponible. El valor predeterminado es **1000**.

shp.console.enable

- Si es **False**, impide el acceso al Portal de autoayuda. Los usuarios que navegan al portal en el puerto 4443 reciben un mensaje de "Acceso denegado". Si es **True**, proporciona acceso al Portal de autoayuda a través del puerto 443.

  El valor predeterminado es **False**.

enable.new.shp

- Si es **Falso**, impide a los usuarios habilitar sus dispositivos desde el Portal de autoayuda. Si es **Verdadero**, los usuarios pueden habilitar sus dispositivos desde el Portal de autoayuda.

  La función de clave de recuperación de BitLocker requiere que configure esta propiedad en **Falso** y la propiedad `shp.console.enable` en **Verdadero**.

  El valor predeterminado es **Falso**.

Limpieza del registro de sesión (en días)

- El número de días que Citrix Endpoint Management conserva el registro de sesión. El valor predeterminado es **7**.

Tipo de configuración de ShareFile

- Especifica el tipo de almacenamiento de Citrix Files. **ENTERPRISE** habilita el modo Citrix Files Enterprise. **CONNECTORS** proporciona acceso solo a los conectores de zona de almacenamiento que cree a través de la consola de Citrix Endpoint Management. El valor predeterminado es **NONE**, que muestra la vista inicial de la pantalla **Configurar > Citrix Files**

donde puede elegir entre Citrix Files Enterprise y Connectors. El valor predeterminado es **NONE**.

Tiempo de espera estático en minutos

- Si la propiedad de servidor **WebServices timeout type** es **STATIC_TIMEOUT:** Esta propiedad define el número de minutos después de los cuales Citrix Endpoint Management cierra la sesión de un administrador después de usar lo siguiente:
  - La API pública para servicios REST para acceder a la consola de Citrix Endpoint Management.
  - La API pública para servicios REST para acceder a cualquier aplicación de terceros.

  El valor predeterminado es **60**.

Supresión de mensajes del agente de activación

- Habilita o deshabilita la mensajería del cliente de Citrix Secure Hub. El valor **false** habilita la mensajería. El valor predeterminado es **true**.

Supresión de sonido del agente de activación

- Habilita o deshabilita los sonidos del cliente de Citrix Secure Hub. El valor **false** habilita los sonidos. El valor predeterminado es **true**.

Descarga de aplicaciones no autenticadas para dispositivos Android

- Si es **True**, puede descargar aplicaciones autohospedadas en dispositivos Android que ejecuten Android Enterprise. Citrix Endpoint Management necesita esta propiedad si la opción de Android Enterprise para proporcionar una URL de descarga estáticamente en Google Play Store está habilitada. En ese caso, las URL de descarga no pueden incluir un ticket de un solo uso (definido por la propiedad **XAM One-Time Ticket server**) que contenga el token de autenticación. El valor predeterminado es **False**.

Descarga de aplicaciones no autenticadas para dispositivos Windows

- Se utiliza solo para versiones anteriores de Citrix Secure Hub que no validan los tickets de un solo uso. Si es **False**, puede descargar aplicaciones no autenticadas desde Citrix Endpoint Management a dispositivos Windows. El valor predeterminado es **False**.

Usar el ID de ActiveSync para realizar un borrado de dispositivo ActiveSync

- Si es **true**, el conector de Citrix Endpoint Management para Exchange ActiveSync utiliza el identificador de ActiveSync como argumento para el método **asWipeDevice**. El valor predeterminado es **false**.

Solo usuarios de Exchange

- Si es **true**, deshabilita la autenticación de usuario para los usuarios de ActiveSync Exchange. El valor predeterminado es **false**.

Intervalo de referencia de Volume Purchase

- El intervalo mínimo en el que Citrix Endpoint Management reimporta las licencias de Volume Purchase de Apple. La actualización de la información de la licencia garantiza que Citrix Endpoint Management refleje todos los cambios, como cuando se elimina manualmente una aplicación importada de Volume Purchase. De forma predeterminada, Citrix Endpoint Management actualiza la línea base de licencias de Volume Purchase como mínimo cada **1440** minutos.
    - Si tiene muchas licencias de Volume Purchase instaladas (por ejemplo, más de 50 000): Citrix recomienda aumentar el intervalo de referencia para reducir la frecuencia y la sobrecarga de la importación de licencias.
    - Si espera cambios frecuentes en las licencias de Volume Purchase de Apple: Citrix recomienda reducir el valor para mantener Citrix Endpoint Management actualizado con los cambios.
    - El intervalo mínimo entre las dos líneas base es de 60 minutos. Además, Citrix Endpoint Management realiza una importación delta cada 60 minutos para capturar los cambios desde la última importación. Por lo tanto, si el intervalo de referencia de Volume Purchase es de 60 minutos, el intervalo entre las líneas base podría retrasarse hasta 119 minutos.

Tipo de tiempo de espera de WebServices

- Especifica cómo caducar un token de autenticación recuperado de la API pública.
    - Si **STATIC_TIMEOUT:** Citrix Endpoint Management considera que un token ha caducado, según el valor de la propiedad del servidor **Static Timeout in Minutes**.
    - Si **INACTIVITY_TIMEOUT:** Citrix Endpoint Management considera que un token ha caducado, según el valor de la propiedad del servidor **Inactivity Timeout in Minutes**. El valor predeterminado es **STATIC_TIMEOUT**.

Validez extendida del certificado MDM de Windows Tablet (5 años)

- El período de validez del certificado de dispositivo emitido por MDM para la tableta Windows. Los dispositivos utilizan un certificado de dispositivo para autenticarse en el servidor MDM durante la administración del dispositivo. Si es **true**, el período de validez es de cinco años. Si es **false**, el período de validez es de dos años. El valor predeterminado es **true**.

Canal WNS de Windows - Número de días antes de la renovación

- La frecuencia de renovación para ChannelURI. El valor predeterminado es **10** días.

Intervalo de latido de WNS de Windows

- Cuánto tiempo espera Citrix Endpoint Management antes de conectarse a un dispositivo después de conectarse a él cada tres minutos cinco veces. El valor predeterminado es **6** horas.

Ticket de un solo uso de XAM

- El número de milisegundos que un token de autenticación de un solo uso (OTT) es válido para descargar una aplicación. Esta propiedad y las propiedades **Unauthenticated App download for Android** y **Unauthenticated App download for Windows** funcionan juntas. Esas propiedades especifican si se permiten las descargas de aplicaciones no autenticadas. El valor predeterminado es **3600000**.

Intervalo máximo de inactividad de la consola del portal de autoayuda MDM de Citrix Endpoint Management (minutos)

- Este nombre de propiedad refleja las versiones anteriores de Citrix Endpoint Management. La propiedad controla el intervalo máximo de inactividad de la consola de Citrix Endpoint Management. Ese intervalo es el número de minutos después de los cuales Citrix Endpoint Management cierra la sesión de un usuario inactivo en la consola de Citrix Endpoint Management. Un tiempo de espera de **0** significa que un usuario inactivo permanece conectado. El valor predeterminado es **30**.

Eliminar dispositivos ABM de CEM cuando se desasignan del servidor MDM de ABM

- Si `remove.unassigned.abm.devices` es **true**, CEM elimina los dispositivos que ya no están asignados a este servidor. El valor predeterminado es **false**.

Directivas de dispositivos y aplicaciones

Las directivas de dispositivos y aplicaciones de Citrix Endpoint Management le permiten optimizar el equilibrio entre factores como:

- Seguridad empresarial
- Protección de datos y activos corporativos
- Privacidad del usuario
- Experiencias de usuario productivas y positivas

El equilibrio óptimo entre esos factores puede variar. Por ejemplo, las organizaciones altamente reguladas, como las financieras, requieren controles de seguridad más estrictos que otras industrias, como la educación y el comercio minorista, en las que la productividad del usuario es una consideración principal.

Puede controlar y configurar directivas de forma centralizada en función de la identidad, el dispositivo, la ubicación y el tipo de conectividad de los usuarios para restringir el uso malintencionado del contenido corporativo. Si un dispositivo se pierde o es robado, puede deshabilitar, bloquear o borrar de forma remota las aplicaciones y los datos empresariales. El resultado general es una solución que aumenta la satisfacción y la productividad de los empleados, al tiempo que garantiza la seguridad y el control administrativo.

El objetivo principal de este artículo son las numerosas directivas de dispositivos y aplicaciones relacionadas con la seguridad.

Directivas que abordan los riesgos de seguridad

Las directivas de dispositivos y aplicaciones de Citrix Endpoint Management abordan muchas situaciones que podrían suponer un riesgo de seguridad, como cuando:

- Los usuarios intentan acceder a aplicaciones y datos desde dispositivos no fiables y ubicaciones impredecibles
- Los usuarios transfieren datos entre dispositivos
- Un usuario no autorizado intenta acceder a los datos
- Un usuario que ha dejado la empresa utilizó su propio dispositivo (BYOD)
- Un usuario extravía un dispositivo
- Los usuarios deben acceder a la red de forma segura siempre
- Los usuarios tienen su propio dispositivo administrado y debe separar los datos de trabajo de los datos personales
- Un dispositivo está inactivo y requiere la verificación de las credenciales del usuario de nuevo
- Los usuarios copian y pegan contenido confidencial en sistemas de correo electrónico no protegidos

- Los usuarios reciben archivos adjuntos de correo electrónico o enlaces web con datos confidenciales en un dispositivo que contiene cuentas personales y de la empresa

Esas situaciones se relacionan con dos áreas principales de preocupación al proteger los datos de la empresa, que son cuando los datos están:

- En reposo
- En tránsito

Cómo Citrix Endpoint Management protege los datos en reposo

Los datos almacenados en dispositivos móviles se denominan datos en reposo. Citrix Endpoint Management utiliza el cifrado de dispositivos proporcionado por las plataformas iOS y Android. Citrix Endpoint Management complementa el cifrado basado en la plataforma con funciones como la comprobación de cumplimiento, disponible a través del SDK de Citrix MAM.

Las capacidades de administración de aplicaciones móviles (MAM) de Citrix Endpoint Management permiten una gestión, seguridad y control completos sobre las aplicaciones de productividad móvil de Citrix, las aplicaciones habilitadas para MDX y sus datos asociados.

El SDK de aplicaciones móviles permite la implementación de aplicaciones para Citrix Endpoint Management mediante el uso de la tecnología de contenedor de aplicaciones Citrix MDX. La tecnología de contenedor separa las aplicaciones y los datos corporativos de las aplicaciones y los datos personales en un dispositivo de usuario. La separación de datos le permite proteger cualquier aplicación móvil desarrollada a medida, de terceros o BYO con controles completos basados en políticas.

Citrix Endpoint Management también incluye cifrado a nivel de aplicación. Citrix Endpoint Management cifra por separado los datos almacenados dentro de cualquier aplicación habilitada para MDX sin requerir un código de acceso del dispositivo y sin requerir que administre el dispositivo para aplicar la política.

- En dispositivos iOS, Citrix Endpoint Management utiliza servicios y bibliotecas criptográficos sólidos validados por FIPS, como el llavero.
- OpenSSL proporciona módulos validados por FIPS para varias plataformas de dispositivos. OpenSSL asegura aún más los datos en movimiento y los certificados necesarios para administrar e inscribir dispositivos.
- Citrix Endpoint Management utiliza la API de bóveda compartida del SDK de MAM para compartir contenido administrado entre aplicaciones que tienen el mismo grupo de acceso al

llavero. Por ejemplo, puede compartir certificados de usuario a través de una aplicación inscrita para que las aplicaciones puedan obtener un certificado de la bóveda segura.

- Citrix Endpoint Management utiliza el cifrado de dispositivos proporcionado por las plataformas.
- Los controles MAM de Citrix Endpoint Management a nivel de aplicación realizan una comprobación de cumplimiento para validar que el cifrado del dispositivo está habilitado en cada inicio de aplicación.

¿Cómo protege Citrix Endpoint Management los datos en tránsito?

Los datos que se mueven entre los dispositivos móviles de su usuario y su red interna se denominan datos en tránsito. La tecnología de contenedores de aplicaciones MDX proporciona acceso VPN específico de la aplicación a su red interna a través de NetScaler Gateway.

Considere la situación en la que un empleado desea acceder a los siguientes recursos que se encuentran en la red empresarial segura desde un dispositivo móvil:

- El servidor de correo electrónico corporativo
- Una aplicación web habilitada para SSL alojada en la intranet corporativa
- Documentos almacenados en un servidor de archivos o Microsoft SharePoint

MDX permite el acceso a todos estos recursos empresariales desde dispositivos móviles a través de una micro VPN específica de la aplicación. Cada dispositivo tiene su propio túnel micro VPN dedicado.

La funcionalidad de micro VPN no requiere una VPN para todo el dispositivo, lo que puede comprometer la seguridad en dispositivos móviles no confiables. Como resultado, la red interna no está expuesta a malware o ataques que puedan infectar todo el sistema corporativo. Las aplicaciones móviles corporativas y las aplicaciones móviles personales pueden coexistir en un solo dispositivo.

Para ofrecer niveles de seguridad aún más sólidos, puede configurar aplicaciones habilitadas para MDX con una política de puerta de enlace NetScaler alternativa. La política se utiliza para la autenticación y para las sesiones de micro VPN con una aplicación. Puede utilizar una puerta de enlace NetScaler alternativa con la política de sesión de micro VPN requerida para forzar a las aplicaciones a volver a autenticarse en la puerta de enlace específica. Dichas puertas de enlace pueden tener requisitos de autenticación y políticas de gestión de tráfico diferentes (de mayor seguridad).

Además de las funciones de seguridad, la función de micro VPN también ofrece técnicas de optimización de datos, incluidos algoritmos de compresión. Los algoritmos de compresión aseguran que:

- Solo se transfieren datos mínimos
- La transferencia se realiza en el menor tiempo posible. La velocidad mejora la experiencia del usuario, lo cual es un factor clave de éxito en la adopción de dispositivos móviles.

Reevalúe sus directivas de dispositivo periódicamente, por ejemplo, en estas situaciones:

- Cuando una nueva versión de Citrix Endpoint Management incluya directivas nuevas o actualizadas debido al lanzamiento de actualizaciones del sistema operativo del dispositivo
- Cuando agregue un tipo de dispositivo:

  Aunque muchas directivas son comunes a todos los dispositivos, cada dispositivo tiene un conjunto de directivas específicas de su sistema operativo. Como resultado, puede encontrar diferencias entre dispositivos iOS, Android y Windows, e incluso entre dispositivos Android de diferentes fabricantes.
- Para mantener el funcionamiento de Citrix Endpoint Management sincronizado con los cambios empresariales o del sector, como nuevas directivas de seguridad corporativas o normativas de cumplimiento
- Cuando una nueva versión del SDK de MAM incluya directivas nuevas o actualizadas
- Cuando agregue o actualice una aplicación
- Para integrar nuevos flujos de trabajo para sus usuarios debido a nuevas aplicaciones o nuevos requisitos

Directivas de aplicaciones y escenarios de casos de uso

Aunque puede elegir qué aplicaciones están disponibles a través de Citrix Secure Hub, es posible que también desee definir cómo interactúan esas aplicaciones con Citrix Endpoint Management. Utilice las directivas de aplicaciones:

- Si desea que los usuarios se autentiquen después de que transcurra un cierto período de tiempo.
- Si desea proporcionar a los usuarios acceso sin conexión a su información.

Las siguientes secciones incluyen algunas de las directivas y ejemplos de uso.

- Para obtener una lista de las directivas de terceros que puede integrar en su aplicación iOS y Android mediante el SDK de MAM, consulte Información general del SDK de MAM.

- Para obtener una lista de todas las directivas MDX por plataforma, consulte Directivas MDX de un vistazo.

Directivas de autenticación

- **Contraseña del dispositivo**

  Por qué usar esta directiva: Habilite la directiva Contraseña del dispositivo para exigir que un usuario solo pueda acceder a una aplicación MDX si el dispositivo tiene una contraseña de dispositivo habilitada. Esta función garantiza el uso del cifrado de iOS a nivel del dispositivo.

  Ejemplo de usuario: Habilitar esta directiva significa que el usuario debe establecer una contraseña en su dispositivo iOS antes de poder acceder a la aplicación MDX.

- **Contraseña de la aplicación**

  Por qué usar esta directiva: Habilite la directiva Contraseña de la aplicación para que Citrix Secure Hub solicite al usuario que se autentique en la aplicación administrada antes de que pueda abrirla y acceder a los datos. El usuario puede autenticarse con su contraseña de Active Directory, PIN de Citrix o TouchID de iOS, según lo que configure en **Parámetros > Propiedades de cliente** en la consola de Citrix Endpoint Management. Puede establecer un temporizador de inactividad en Propiedades de cliente para que Citrix Secure Hub no solicite al usuario que se vuelva a autenticar en la aplicación administrada hasta que el temporizador caduque.

  La contraseña de la aplicación difiere de la contraseña del dispositivo. Con una directiva de contraseña de dispositivo enviada a un dispositivo, Citrix Secure Hub solicita al usuario que configure una contraseña o un PIN. El usuario debe desbloquear su dispositivo cuando lo enciende o cuando caduca el temporizador de inactividad. Para obtener más información, consulte Autenticación en Citrix Endpoint Management.

  Ejemplo de usuario: Al abrir la aplicación Citrix Secure Web en el dispositivo, el usuario debe introducir su PIN de Citrix antes de poder navegar por sitios web si el período de inactividad ha caducado.

- **Sesión de micro VPN requerida**

  Por qué usar esta directiva: Si una aplicación requiere acceso a una aplicación web (servicio web) para ejecutarse, habilite esta directiva. Citrix Endpoint Management solicita entonces al usuario que se conecte a la red empresarial o que tenga una sesión activa antes de usar la aplicación.

Ejemplo de usuario: Cuando un usuario intenta abrir una aplicación MDX que tiene habilitada la directiva de sesión de micro VPN requerida: no puede usar la aplicación hasta que se conecte a la red. La conexión debe usar un servicio de datos móviles o Wi-Fi.

- **Período máximo sin conexión**

  Por qué usar esta directiva: Utilice esta directiva como una opción de seguridad adicional. La directiva garantiza que los usuarios que ejecutan una aplicación sin conexión durante un período especificado deben volver a confirmar el derecho a la aplicación y actualizar las directivas.

  Ejemplo de usuario: Si configura una aplicación MDX con un Período máximo sin conexión, el usuario puede abrir y usar la aplicación sin conexión hasta que caduque el período del temporizador sin conexión. En ese momento, el usuario debe volver a conectarse a la red a través de un servicio de datos móviles o Wi-Fi y volver a autenticarse, si se le solicita.

Políticas de acceso varias

- **Período de gracia para la actualización de aplicaciones (horas)**

  Por qué usar esta política: El período de gracia para la actualización de aplicaciones es el tiempo disponible para el usuario antes de que deba actualizar una aplicación que tiene una versión más reciente disponible en la tienda de aplicaciones. Al expirar este período, el usuario debe actualizar la aplicación antes de poder acceder a los datos de la misma. Al establecer este valor, tenga en cuenta las necesidades de su personal móvil, especialmente los usuarios que podrían experimentar largos períodos sin conexión cuando viajan internacionalmente.

  Ejemplo de usuario: Carga una nueva versión de Citrix Secure Mail en la tienda de aplicaciones y, a continuación, establece un período de gracia de actualización de la aplicación de 6 horas. Los usuarios de Citrix Secure Hub tienen entonces 6 horas para actualizar Citrix Secure Mail antes de ser redirigidos a la tienda de aplicaciones.

- **Período de sondeo activo (minutos)**

  Por qué usar esta política: El período de sondeo activo es el intervalo en el que Citrix Endpoint Management comprueba las aplicaciones para determinar cuándo realizar acciones de seguridad, como Bloqueo de aplicaciones y Borrado de aplicaciones.

  Ejemplo de usuario: Si establece la política de período de sondeo activo en 60 minutos y luego envía el comando Bloqueo de aplicaciones, el bloqueo se produce dentro de los 60 minutos posteriores al último sondeo.

Políticas de comportamiento de dispositivos no conformes

Cuando un dispositivo no cumple los requisitos mínimos de conformidad, la política de comportamiento de dispositivos no conformes le permite seleccionar la acción que debe realizarse. Para obtener más información, consulte Comportamiento de dispositivos no conformes.

Políticas de interacción de aplicaciones

Por qué usar estas políticas: Utilice las políticas de interacción de aplicaciones para controlar el flujo de documentos y datos de las aplicaciones MDX a otras aplicaciones del dispositivo. Por ejemplo, puede evitar que un usuario:

- mueva datos a sus aplicaciones personales fuera del contenedor
- pegue datos de fuera del contenedor en las aplicaciones en contenedores

Ejemplo de usuario: Establece una política de interacción de aplicaciones en Restringido, lo que significa que un usuario puede copiar texto de Citrix Secure Mail a Citrix Secure Web. El usuario no puede copiar esos datos en su navegador personal Safari o Chrome que está fuera del contenedor. Además, un usuario puede abrir un documento adjunto de Citrix Secure Mail en Citrix Files o QuickEdit. El usuario no puede abrir el documento adjunto en sus propias aplicaciones personales de visualización de archivos que están fuera del contenedor.

Políticas de restricciones de aplicaciones

Por qué usar estas directivas: Use las directivas de restricción de aplicaciones para controlar a qué funciones pueden acceder los usuarios desde una aplicación MDX mientras está abierta. Las restricciones ayudan a garantizar que no se produzca ninguna actividad maliciosa mientras la aplicación está en ejecución. Las directivas de restricción de aplicaciones varían ligeramente entre iOS y Android. Por ejemplo, en iOS puede bloquear el acceso a iCloud mientras la aplicación MDX está en ejecución. En Android, puede detener el uso de NFC mientras la aplicación MDX está en ejecución.

Ejemplo de usuario: Supongamos que habilita la directiva de restricción de aplicaciones para bloquear el dictado en iOS en una aplicación MDX. Como resultado, el usuario no puede usar la función de dictado en el teclado de iOS mientras la aplicación MDX está en ejecución. Por lo tanto, los datos que los usuarios dictan no se pasan al servicio de dictado en la nube de terceros no seguro. Cuando el usuario abre su aplicación personal fuera del contenedor, la opción de dictado permanece disponible para el usuario para sus comunicaciones personales.

Directivas de acceso a la red de aplicaciones

Por qué usar estas directivas: Use las directivas de acceso a la red de aplicaciones para proporcionar acceso desde una aplicación MDX en el contenedor del dispositivo a los datos que se encuentran dentro de su red corporativa. La opción Tunneled - Web SSO solo permite la tunelización del tráfico HTTP y HTTPS. Esa opción proporciona inicio de sesión único (SSO) para el tráfico HTTP y HTTPS y autenticación PKINIT.

Ejemplo de usuario: Cuando un usuario abre una aplicación MDX que tiene la tunelización habilitada, el explorador abre un sitio de intranet sin necesidad de que el usuario inicie una VPN. La aplicación accede automáticamente al sitio interno mediante la tecnología de micro VPN.

Directivas de geolocalización y geocercado de aplicaciones

Por qué usar estas directivas: Las directivas que controlan la geolocalización y el geocercado de aplicaciones incluyen la longitud del punto central, la latitud del punto central y el radio. Esas directivas tienen acceso a los datos de las aplicaciones MDX en un área geográfica específica. Las directivas definen un área geográfica mediante un radio de coordenadas de latitud y longitud. Si un usuario intenta usar una aplicación fuera del radio definido, la aplicación permanece bloqueada y el usuario no puede acceder a los datos de la aplicación.

Ejemplo de usuario: Un usuario puede acceder a los datos de fusiones y adquisiciones mientras se encuentra en la ubicación de su oficina. Cuando se mueve fuera de la ubicación de su oficina, estos datos confidenciales se vuelven inaccesibles.

Directivas de la aplicación Citrix Secure Mail

- **Servicios de red en segundo plano**

  Por qué usar esta directiva: Los servicios de red en segundo plano en Citrix Secure Mail utilizan la Secure Ticket Authority (STA), que es efectivamente un proxy SOCKS5 para conectarse a través de NetScaler Gateway. STA admite conexiones de larga duración y proporciona una mayor duración de la batería en comparación con la micro VPN. Por lo tanto, STA es ideal para el correo que se conecta constantemente. Citrix recomienda que configure estos ajustes para Citrix Secure Mail. El asistente de NetScaler para XenMobile configura automáticamente STA para Citrix Secure Mail.

  Ejemplo de usuario: Cuando STA no está habilitado y un usuario de Android abre Citrix Secure Mail, se le pide que abra una VPN, que permanece abierta en el dispositivo. Cuando STA está habilitado y el usuario de Android abre Citrix Secure Mail, Citrix Secure Mail se conecta sin problemas sin necesidad de VPN.

- **Intervalo de sincronización predeterminado**

Por qué usar esta directiva: Esta configuración especifica los días predeterminados de correo electrónico que se sincronizan con Citrix Secure Mail cuando el usuario accede a Citrix Secure Mail por primera vez. Dos semanas de correo electrónico tardan más en sincronizarse que tres días de correo electrónico. Más datos para sincronizar prolongan el proceso de configuración para el usuario.

Ejemplo de usuario: Supongamos que el intervalo de sincronización predeterminado se establece en tres días cuando el usuario configura Citrix Secure Mail por primera vez. El usuario puede ver cualquier correo electrónico en su bandeja de entrada que haya recibido desde el presente hasta tres días en el pasado. Si un usuario quiere ver correos electrónicos que tienen más de tres días, puede realizar una búsqueda. Citrix Secure Mail muestra entonces los correos electrónicos más antiguos almacenados en el servidor. Después de instalar Citrix Secure Mail, cada usuario puede cambiar esta configuración para adaptarla mejor a sus necesidades.

Políticas de dispositivo y comportamiento de casos de uso

Las políticas de dispositivo, a veces denominadas políticas MDM, determinan cómo Citrix Endpoint Management administra los dispositivos. Aunque muchas políticas son comunes a todos los dispositivos, cada dispositivo tiene un conjunto de políticas específicas para su sistema operativo. La siguiente lista incluye algunas de las políticas de dispositivo y explica cómo podría utilizarlas. Para obtener una lista de todas las políticas de dispositivo, consulte el artículo en Políticas de dispositivo.

- **Política de inventario de aplicaciones**

  Por qué usar esta política: Para ver las aplicaciones instaladas por un usuario, implemente la política de inventario de aplicaciones en un dispositivo. Si no implementa la política, solo podrá ver las aplicaciones que un usuario instaló desde la tienda de aplicaciones, no las aplicaciones instaladas personalmente. Utilice la política de inventario de aplicaciones para bloquear la ejecución de ciertas aplicaciones en dispositivos corporativos.

  Ejemplo de usuario: Un usuario con un dispositivo administrado por MDM no puede deshabilitar esta funcionalidad. Las aplicaciones instaladas personalmente por el usuario son visibles para los administradores de Citrix Endpoint Management.

- **Política de bloqueo de aplicaciones**

  Por qué usar esta política: La política de bloqueo de aplicaciones, para Android, le permite colocar aplicaciones en una lista de permitidos o una lista de bloqueados. Por ejemplo, para las aplicaciones permitidas, puede configurar un dispositivo de quiosco. Normalmente, solo

implementa la política de bloqueo de aplicaciones en dispositivos propiedad de la empresa, ya que limita las aplicaciones que los usuarios pueden instalar. Puede establecer una contraseña de anulación para proporcionar acceso de usuario a las aplicaciones bloqueadas.

Ejemplo de usuario: Supongamos que implementa una política de bloqueo de aplicaciones que bloquea la aplicación Angry Birds. El usuario puede instalar la aplicación Angry Birds desde Google Play, pero cuando abre la aplicación, un mensaje le informa que su administrador bloqueó la aplicación.

- **Política de programación de conexiones**

  Por qué usar esta política: La política de programación de conexiones permite que los dispositivos Windows Mobile se conecten a Citrix Endpoint Management para la administración de MDM, el envío de aplicaciones y la implementación de políticas. Para dispositivos Android y Android Enterprise, utilice Google Firebase Cloud Messaging (FCM) en su lugar. FCM controla las conexiones a Citrix Endpoint Management. Las opciones de programación son las siguientes:

  - **Nunca:** Conectarse manualmente. Los usuarios deben iniciar la conexión desde Citrix Endpoint Management en sus dispositivos. Citrix no recomienda esta opción para implementaciones de producción porque le impide implementar políticas de seguridad en los dispositivos. Como resultado, los usuarios no reciben nuevas aplicaciones ni políticas. La opción **Nunca** está habilitada de forma predeterminada.
  - **Cada:** Se conecta en el intervalo elegido. Cuando envía una política de seguridad, como un bloqueo o un borrado, Citrix Endpoint Management procesa la política en el dispositivo la próxima vez que este se conecta.
  - **Definir programación:** Citrix Endpoint Management intenta volver a conectar el dispositivo del usuario al servidor de Citrix Endpoint Management después de una pérdida de conexión de red. Citrix Endpoint Management supervisa la conexión transmitiendo paquetes de control a intervalos regulares dentro del plazo que usted defina.

  Ejemplo de usuario: Desea implementar una política de código de acceso en los dispositivos inscritos. La política de programación garantiza que los dispositivos se conecten al servidor a intervalos regulares para recopilar la nueva política.

- **Política de credenciales**

  Por qué usar esta política: A menudo utilizada con una política de red, la política de credenciales le permite implementar certificados para la autenticación en recursos internos que requieren autenticación de certificado.

Ejemplo de usuario: Usted implementa una política de red que configura una red inalámbrica en el dispositivo. La red Wi-Fi requiere un certificado para la autenticación. La política de credenciales implementa un certificado que luego se almacena en el almacén de claves del sistema operativo. El usuario puede seleccionar el certificado cuando se conecta al recurso interno.

- **Política de Exchange**

  Por qué usar esta política: Con Citrix Endpoint Management, tiene dos opciones para entregar correo electrónico de Microsoft Exchange ActiveSync.

  - **Aplicación Citrix Secure Mail:** Entregue correo electrónico utilizando la aplicación Citrix Secure Mail que distribuye desde la tienda de aplicaciones pública o la tienda de aplicaciones.
  - **Aplicación de correo electrónico nativa:** Habilite el correo electrónico de ActiveSync para el cliente de correo electrónico nativo en el dispositivo. Puede usar macros para rellenar los datos del usuario a partir de sus atributos de Active Directory, como `${user.username}` para rellenar el nombre de usuario y `${user.domain}` para rellenar el dominio del usuario.

  Ejemplo de usuario: Cuando envía la política de Exchange, envía los detalles del servidor de Exchange al dispositivo. Citrix Secure Hub solicita al usuario que se autentique y su correo electrónico comienza a sincronizarse.

- **Política de ubicación**

  Por qué usar esta política: La política de ubicación le permite geolocalizar dispositivos en un mapa, si el dispositivo tiene el GPS habilitado para Citrix Secure Hub. Después de implementar esta política y luego enviar un comando de localización desde Citrix Endpoint Management, el dispositivo responde con las coordenadas de ubicación.

  Ejemplo de usuario: Cuando implementa la política de ubicación y el GPS está habilitado en el dispositivo: Si los usuarios extravían su dispositivo, pueden iniciar sesión en el portal de autoayuda de Citrix Endpoint Management y elegir la opción de localizar para ver la ubicación de su dispositivo en un mapa. Un usuario elige si permite que Citrix Secure Hub use los servicios de ubicación. No puede forzar el uso de los servicios de ubicación cuando los usuarios inscriben un dispositivo ellos mismos. Otra consideración para usar esta política es el efecto en la duración de la batería.

- **Política de código de acceso**

Por qué usar esta política: La política de código de acceso le permite aplicar un código PIN o una contraseña en un dispositivo administrado. Esta política de código de acceso le permite establecer la complejidad y los tiempos de espera para el código de acceso en el dispositivo.

Ejemplo de usuario: Cuando implementa una política de código de acceso en un dispositivo administrado, Citrix Secure Hub solicita al usuario que configure un código de acceso o PIN. El código de acceso o PIN le da al usuario acceso a su dispositivo durante el inicio o cuando expira el temporizador de inactividad.

- **Política de eliminación de perfiles**

  Por qué usar esta política: Suponga que implementa una política para un grupo de usuarios y más tarde debe eliminar esa política de un subconjunto de usuarios. Puede eliminar la política para los usuarios seleccionados creando una política de eliminación de perfiles. Luego, use las reglas de implementación para implementar la política de eliminación de perfiles solo para usuarios específicos.

  Ejemplo de usuario: Cuando implementa una política de eliminación de perfiles en los dispositivos de los usuarios, es posible que los usuarios no noten el cambio. Por ejemplo, si la política de eliminación de perfiles elimina una restricción que deshabilitó la cámara del dispositivo, el usuario no se entera del cambio. Considere informar a los usuarios cuando los cambios afecten su experiencia de usuario.

- **Política de restricciones**

  Por qué usar esta política: La política de restricciones le ofrece muchas opciones para bloquear y controlar las características y funcionalidades del dispositivo administrado. Puede habilitar cientos de opciones de restricción para los dispositivos compatibles. Por ejemplo, puede: deshabilitar la cámara o el micrófono en un dispositivo, aplicar reglas de itinerancia y aplicar el acceso a servicios de terceros como las tiendas de aplicaciones.

  Ejemplo de usuario: Si implementa una restricción en un dispositivo iOS, es posible que el usuario no pueda acceder a iCloud o a la App Store de Apple.

- **Política de términos y condiciones**

  Por qué usar esta política: Puede ser necesario informar a los usuarios de las implicaciones legales de tener su dispositivo administrado. Además, es posible que desee asegurarse de que los usuarios sean conscientes de los riesgos de seguridad cuando los datos corporativos se envían al dispositivo. El documento de Términos y condiciones le permite publicar reglas y avisos antes de que el usuario se inscriba.

Ejemplo de usuario: Un usuario ve la información de Términos y condiciones durante el proceso de inscripción. Si se niegan a aceptar las condiciones establecidas, el proceso de inscripción finaliza y no pueden acceder a los datos corporativos. Puede generar un informe para proporcionar a los equipos de RR. HH./Legal/Cumplimiento para mostrar quién aceptó o rechazó los términos.

- **Política de VPN**

  Por qué usar esta política: Utilice la política de VPN para proporcionar acceso a sistemas de back-end mediante tecnología VPN Gateway más antigua. La política es compatible con varios proveedores de VPN, incluidos Cisco AnyConnect, Juniper y Citrix VPN. También es posible vincular esta política a una CA y habilitar la VPN a petición, si la puerta de enlace VPN admite esta opción.

  Ejemplo de usuario: Con la política de VPN habilitada, el dispositivo de un usuario abre una conexión VPN cuando el usuario accede a un dominio interno.

- **Política de clip web**

  Por qué usar esta política: Utilice la política de clip web si desea enviar a los dispositivos un icono que se abra directamente a un sitio web. Un clip web tiene un enlace a un sitio web y puede incluir un icono personalizado. En un dispositivo, un clip web se parece a un icono de aplicación.

  Ejemplo de usuario: Un usuario puede hacer clic en un icono de clip web para abrir un sitio de Internet y acceder a los servicios necesarios. Usar un enlace web es más conveniente que escribir una dirección de enlace en un navegador.

- **Política de red**

  Por qué usar esta política: La política de red le permite implementar detalles de la red Wi-Fi, como el SSID, los datos de autenticación y los datos de configuración, en un dispositivo administrado.

  Ejemplo de usuario: Cuando implementa la política de red, el dispositivo se conecta automáticamente a la red Wi-Fi y autentica al usuario para que pueda acceder a la red.

- **Política de la tienda de Endpoint Management**

  Por qué usar esta política: La tienda de aplicaciones es una tienda de aplicaciones unificada donde los administradores pueden publicar todas las aplicaciones corporativas y los recursos de datos que necesitan sus usuarios. Un administrador puede añadir:

- Aplicaciones web, aplicaciones SaaS y aplicaciones habilitadas para MAM SDK o aplicaciones encapsuladas en MDX
- Aplicaciones de productividad móvil de Citrix
- Aplicaciones móviles nativas como archivos .ipa o .apk
- Aplicaciones de Apple App Store y Google Play
- Enlaces web
- Aplicaciones virtuales de Citrix publicadas mediante Citrix StoreFront

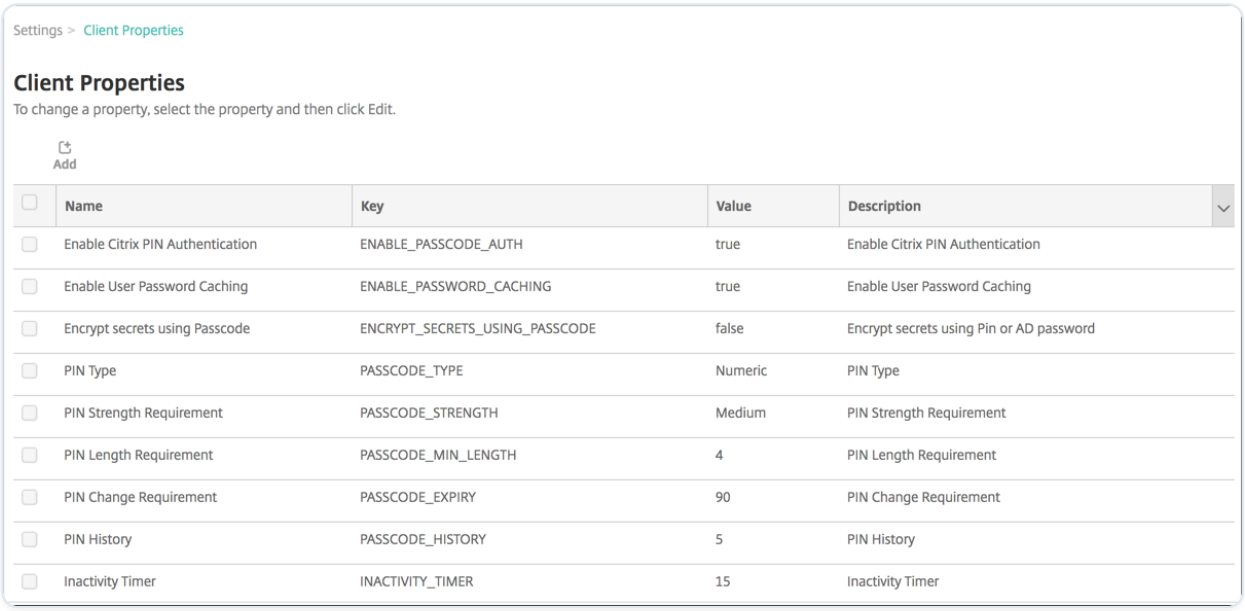
Ejemplo de usuario: Después de que un usuario inscribe su dispositivo en Citrix Endpoint Management, accede a la tienda de aplicaciones a través de la aplicación Citrix Secure Hub. El usuario puede ver todas las aplicaciones y servicios corporativos disponibles para él. Los usuarios pueden hacer clic en una aplicación para instalarla, acceder a los datos, calificar y revisar la aplicación, y descargar actualizaciones de la aplicación desde la tienda de aplicaciones.

Propiedades de cliente

Las propiedades de cliente contienen información que se proporciona directamente a Citrix Secure Hub en los dispositivos de usuario. Puede usar estas propiedades para configurar ajustes avanzados, como el PIN de Citrix. Puede obtener las propiedades de cliente del soporte de Citrix.

Las propiedades de cliente están sujetas a cambios con cada versión de Citrix Secure Hub y, ocasionalmente, para las aplicaciones cliente. Para obtener más información sobre las propiedades de cliente configuradas con mayor frecuencia, consulte Referencia de propiedades de cliente, más adelante en este artículo.

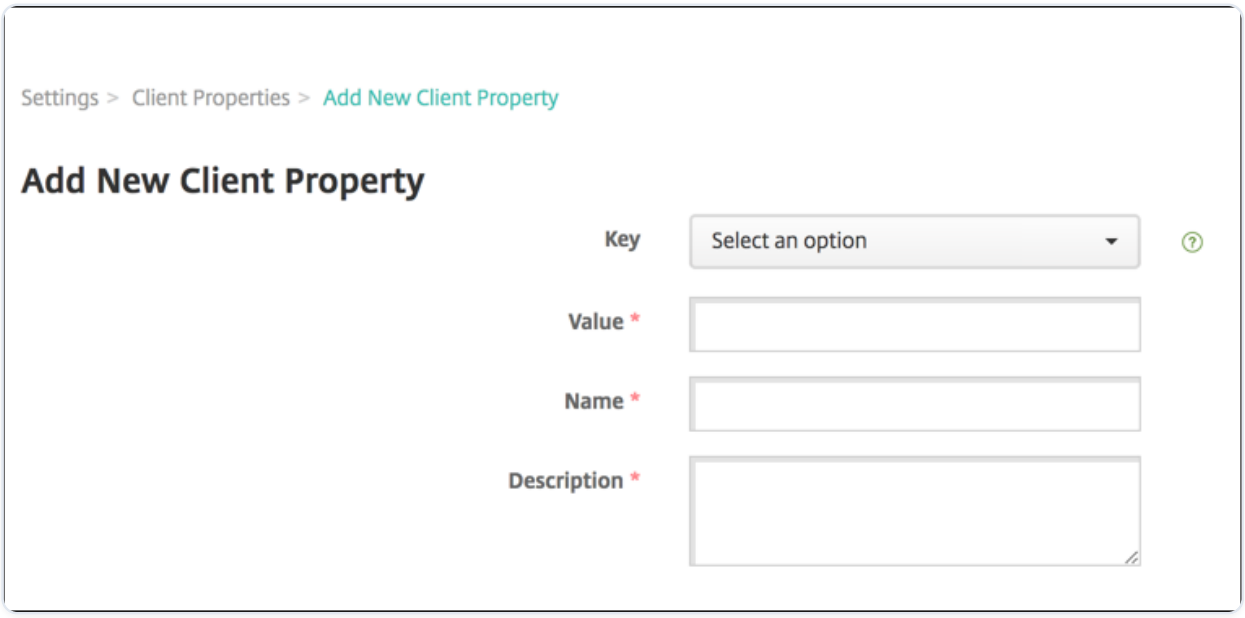
1. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje en la esquina superior derecha. Aparecerá la página **Configuración**.
2. En **Cliente**, haga clic en **Propiedades de cliente**. Aparecerá la página **Propiedades de cliente**. Desde esta página, puede agregar, modificar y eliminar propiedades de cliente.



Name	Key	Value	Description
Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	true	Enable Citrix PIN Authentication
Enable User Password Caching	ENABLE_PASSWORD_CACHING	true	Enable User Password Caching
Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
PIN Type	PASSCODE_TYPE	Numeric	PIN Type
PIN Strength Requirement	PASSCODE_STRENGTH	Medium	PIN Strength Requirement
PIN Length Requirement	PASSCODE_MIN_LENGTH	4	PIN Length Requirement
PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
PIN History	PASSCODE_HISTORY	5	PIN History
Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer

Para agregar una propiedad de cliente

1. Haga clic en **Agregar**. Aparecerá la página **Agregar nueva propiedad de cliente**.



2. Configure estos ajustes:

   - **Clave:** Haga clic en la clave de propiedad que desea agregar de la lista desplegable. **Importante:** Póngase en contacto con el soporte de Citrix antes de actualizar la configuración. Puede solicitar una clave especial.
   - **Valor:** El valor de la propiedad seleccionada.
   - **Nombre:** Un nombre para la propiedad.
   - **Descripción:** Una descripción de la propiedad.

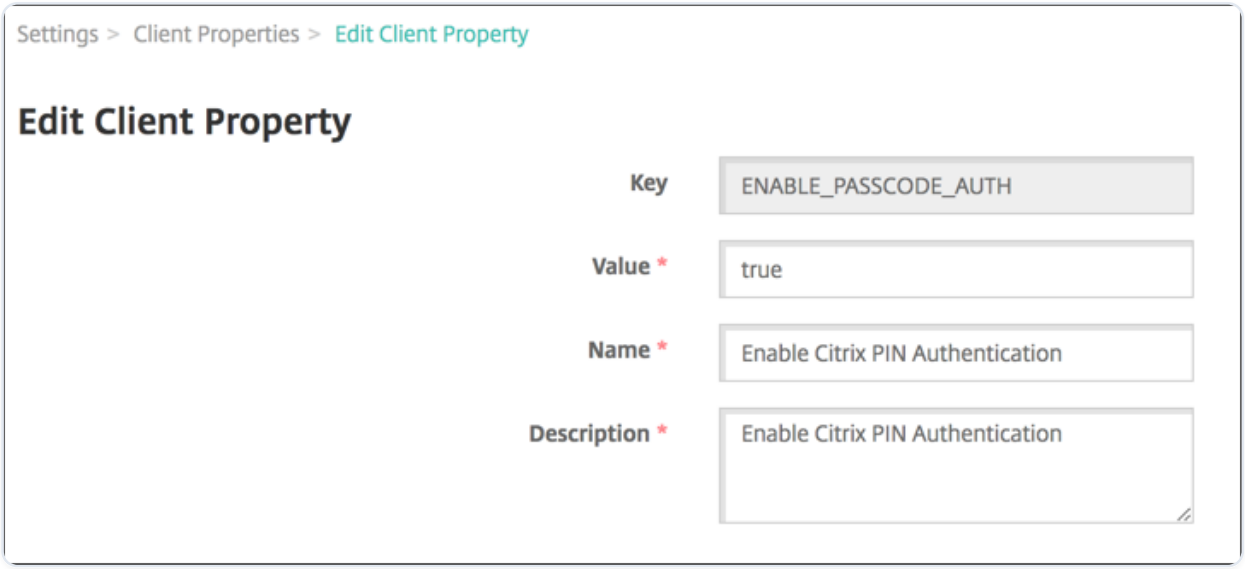
3. Haga clic en **Guardar**.

Para editar una propiedad de cliente

1. En la tabla **Propiedades de cliente**, seleccione la propiedad de cliente que desea editar.

   Seleccione la casilla de verificación junto a una propiedad de cliente para abrir el menú de opciones encima de la lista de propiedades de cliente. Haga clic en cualquier otro lugar de la lista para abrir el menú de opciones en el lado derecho de la lista.

2. Haga clic en **Editar**. Aparecerá la página **Editar propiedad de cliente**.



3. Cambie la siguiente información según corresponda:

   - **Clave:** No puede cambiar este campo.
   - **Valor:** El valor de la propiedad.
   - **Nombre:** El nombre de la propiedad.
   - **Descripción:** La descripción de la propiedad.

4. Haga clic en **Guardar** para guardar los cambios o en **Cancelar** para dejar la propiedad sin cambios.

Para eliminar una propiedad de cliente

1. En la tabla **Propiedades de cliente**, seleccione la propiedad de cliente que desea eliminar.

   Puede seleccionar más de una propiedad para eliminar marcando la casilla de verificación junto a cada propiedad.

2. Haga clic en **Eliminar**. Aparecerá un cuadro de diálogo de confirmación. Vuelva a hacer clic en **Eliminar**.

Referencia de propiedades de cliente

Las propiedades de cliente predefinidas y su configuración predeterminada para Citrix Endpoint Management son las siguientes:

- **ALLOW_CLIENTSIDE_PROXY**
  - Nombre para mostrar: ALLOW_CLIENTSIDE_PROXY
  - Si sus usuarios quieren usar un proxy que han configurado en sus teléfonos iOS, deje esta directiva personalizada establecida en el valor predeterminado **true**.

    Algunos usuarios ya podrían tener un proxy configurado en **Ajustes > Wi-Fi > Configurar proxy** en sus dispositivos. Si Citrix Secure Hub no se abre para esos usuarios, realice una de las siguientes acciones:

    - Quite la configuración del proxy del dispositivo y, a continuación, reinicie Citrix Secure Hub.
    - Conecte el dispositivo a otra red Wi-Fi. Después de que Citrix Secure Hub se vuelva a autenticar, obtiene la propiedad **ALLOW_CLIENTSIDE_PROXY** y se abre.
  - Si **ALLOW_CLIENTSIDE_PROXY** es **false** y los usuarios configuran un proxy en su dispositivo, Citrix Endpoint Management detecta el proxy. Sin embargo, Citrix Secure Hub no utiliza el proxy y muestra un mensaje de error. Si un dispositivo se conecta a un punto de acceso o enrutador que tiene un proxy habilitado, Citrix Endpoint Management no detecta el proxy. Para la máxima seguridad, le recomendamos que utilice el anclaje de certificados (certificate pinning). Para obtener información sobre cómo habilitar el anclaje de certificados para Citrix Secure Hub, consulte Anclaje de certificados.
  - Para configurar esta directiva de cliente personalizada, vaya a **Ajustes > Propiedades de cliente**, agregue la clave personalizada **ALLOW_CLIENTSIDE_PROXY** y establezca el **Valor**.
- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - Nombre para mostrar: Período de autodestrucción del contenedor MDX
  - La autodestrucción impide el acceso a Citrix Secure Hub y a las aplicaciones administradas después de un número específico de días de inactividad. Una vez transcurrido el límite de tiempo, las aplicaciones dejan de ser utilizables. La eliminación de datos incluye la limpieza de los datos de la aplicación para cada aplicación instalada, incluida la caché de la aplicación y los datos del usuario.

El tiempo de inactividad es cuando el servidor no recibe una solicitud de autenticación para validar al usuario durante un período de tiempo específico. Supongamos que esta propiedad es de 30 días. Si el usuario no utiliza la aplicación durante más de 30 días, la directiva surte efecto.

Esta directiva de seguridad global se aplica a las plataformas iOS y Android y es una mejora de las directivas existentes de bloqueo y borrado de aplicaciones.

  - Para configurar esta política global, vaya a **Settings > Client Properties** y añada la clave personalizada **CONTAINER_SELF_DESTRUCT_PERIOD**.
  - Valor: Número de días

- **DEVICE_LOGS_TO_IT_HELP_DESK**
  - Nombre para mostrar: Enviar registros del dispositivo al servicio de asistencia de TI
  - Esta propiedad habilita o deshabilita la capacidad de enviar registros al servicio de asistencia de TI.
  - Valores posibles: **true** o **false**
  - Valor predeterminado: **false**
- **DISABLE_LOGGING**
  - Nombre para mostrar: Deshabilitar el registro
  - Utilice esta propiedad para evitar que los usuarios recopilen y carguen registros de sus dispositivos. Esta propiedad deshabilita el registro para Citrix Secure Hub y para todas las aplicaciones MDX instaladas. Los usuarios no pueden enviar registros de ninguna aplicación desde la página de soporte. Aunque aparece el cuadro de diálogo de composición de correo, los registros no se adjuntan. Un mensaje indica que el registro está deshabilitado. Esta configuración también le impide actualizar la configuración de registro en la consola de Citrix Endpoint Management para Citrix Secure Hub y las aplicaciones MDX.

    Cuando esta propiedad se establece en **true**, Citrix Secure Hub establece **Bloquear registros de aplicaciones** en **true**. Como resultado, las aplicaciones MDX dejan de registrarse cuando se aplica la nueva directiva.
  - Valores posibles: **true** o **false**
  - Valor predeterminado: **false** (el registro no está deshabilitado)
- **ENABLE_CRASH_REPORTING**

- Nombre para mostrar: Habilitar informes de errores
- Si es **true**, Citrix recopila informes de fallos y diagnósticos para ayudar a solucionar problemas con Citrix Secure Hub para iOS y Android. Si es **false**, no se recopilan datos.
- Valores posibles: **true** o **false**
- Valor predeterminado: **true**

- **ENABLE_CREDENTIAL_STORE**
  - Nombre para mostrar: Habilitar almacén de credenciales
  - Habilitar el almacén de credenciales significa que los usuarios de Android o iOS introducen su contraseña una sola vez al acceder a las aplicaciones de productividad móvil de Citrix. Puede usar el almacén de credenciales tanto si habilita el PIN de Citrix como si no. Si no habilita el PIN de Citrix, los usuarios introducen su contraseña de Active Directory. Citrix Endpoint Management admite el uso de contraseñas de Active Directory con el almacén de credenciales solo para Citrix Secure Hub y las aplicaciones de la tienda pública. Si utiliza contraseñas de Active Directory con el almacén de credenciales, Citrix Endpoint Management no admite la autenticación PKI.
  - La inscripción automática en Citrix Secure Mail requiere que establezca esta propiedad en **true**.
  - Para configurar esta directiva de cliente personalizada, vaya a **Settings > Client Properties**, añada la clave personalizada **ENABLE_CREDENTIAL_STORE** y establezca el **Value** en **true**.

- **ENABLE_PASSCODE_AUTH**
  - Nombre para mostrar: Habilitar autenticación con PIN de Citrix
  - Esta propiedad le permite activar la funcionalidad de PIN de Citrix. Con el PIN o código de acceso de Citrix, se pide a los usuarios que definan un PIN para usarlo en lugar de su contraseña de Active Directory. Esta configuración se habilita automáticamente cuando ENABLE_PASSWORD_CACHING está habilitado o cuando Citrix Endpoint Management utiliza la autenticación de certificados.

    Para la autenticación sin conexión, el PIN de Citrix se valida localmente y se permite a los usuarios acceder a la aplicación o al contenido que solicitaron. Para la autenticación en línea, el PIN o código de acceso de Citrix desbloquea la contraseña o el certificado de Active Directory, que luego se envía para autenticarse con Citrix Endpoint Management.

Si ENABLE_PASSCODE_AUTH es true y ENABLE_PASSWORD_CACHING es false, la autenticación en línea siempre solicita la contraseña porque Citrix Secure Hub no la guarda.

- Valores posibles: **true** o **false**
- Valor predeterminado: **false**

- **ENABLE_PASSWORD_CACHING**
  - Nombre para mostrar: Habilitar el almacenamiento en caché de contraseñas de usuario
  - Esta propiedad permite que las contraseñas de Active Directory se almacenen en caché localmente en el dispositivo móvil. Cuando se establece esta propiedad en **true**, también debe establecer la propiedad **ENABLE_PASSCODE_AUTH** en **true**. Con el almacenamiento en caché de contraseñas de usuario habilitado, Citrix Endpoint Management solicita a los usuarios que establezcan un PIN o código de acceso de Citrix.
  - Valores posibles: **true** o **false**
  - Valor predeterminado: **false**
- **ENABLE_TOUCH_ID_AUTH**
  - Nombre para mostrar: Habilitar autenticación Touch ID
  - Para los dispositivos que admiten la autenticación Touch ID, esta propiedad habilita o deshabilita la autenticación Touch ID en el dispositivo. Requisitos:

    Los dispositivos de usuario deben tener el PIN de Citrix o LDAP habilitado. Si la autenticación LDAP está desactivada (por ejemplo, porque solo se utiliza la autenticación basada en certificados), los usuarios deben establecer un PIN de Citrix. En este caso, Citrix Endpoint Management requiere el PIN de Citrix incluso si la propiedad de cliente **ENABLE_PASSCODE_AUTH** es **false**.

    Establezca **ENABLE_PASSCODE_AUTH** en **false** para que, cuando los usuarios inicien una aplicación, deban responder a una solicitud para usar Touch ID.
  - Valores posibles: **true** o **false**
  - Valor predeterminado: **false**
- **ENABLE_WORXHOME_CEIP**
  - Nombre para mostrar: Habilitar CEIP de Citrix Secure Hub

- Esta propiedad activa el Programa de mejora de la experiencia del cliente. Esa función envía periódicamente datos anónimos de configuración y uso a Citrix. Los datos ayudan a Citrix a mejorar la calidad, la fiabilidad y el rendimiento de Citrix Endpoint Management.
- Valor: **verdadero** o **falso**
- Valor predeterminado: **falso**

- **ENCRYPT_SECRETS_USING_PASSCODE**
  - Nombre para mostrar: Cifrar secretos mediante código de acceso
  - Esta propiedad almacena datos confidenciales en el dispositivo en una bóveda secreta en lugar de en un almacén nativo basado en la plataforma, como el llavero de iOS. Esta propiedad permite un cifrado fuerte de los artefactos clave y añade entropía de usuario. La entropía de usuario es un código PIN aleatorio generado por el usuario que solo este conoce.

    Citrix recomienda habilitar esta propiedad para ayudar a proporcionar una mayor seguridad en los dispositivos de los usuarios. Como resultado, los usuarios experimentan más solicitudes de autenticación para el PIN de Citrix.
  - Valores posibles: **verdadero** o **falso**
  - Valor predeterminado: **falso**
- **INACTIVITY_TIMER**
  - Nombre para mostrar: Temporizador de inactividad
  - Esta propiedad define cuánto tiempo pueden los usuarios dejar su dispositivo inactivo y luego acceder a una aplicación sin que se les solicite un PIN o código de acceso de Citrix. Para habilitar esta configuración para una aplicación MDX, establezca la configuración de Código de acceso de la aplicación en Activado. Si la configuración de Código de acceso de la aplicación está establecida en Desactivado, los usuarios son redirigidos a Citrix Secure Hub para realizar una autenticación completa. Cuando cambia esta configuración, el valor surte efecto la próxima vez que se solicita a los usuarios que se autentiquen.

    En iOS, el Temporizador de inactividad también rige el acceso a Citrix Secure Hub para aplicaciones MDX y no MDX.
  - Valores posibles: Cualquier número entero positivo
  - Valor predeterminado: **15** (minutos)
- **ON_FAILURE_USE_EMAIL**

  - Nombre para mostrar: En caso de fallo, usar el correo electrónico para enviar registros del dispositivo al servicio de asistencia de TI
  - Esta propiedad habilita o deshabilita la capacidad de usar el correo electrónico para enviar registros del dispositivo a TI.
  - Valores posibles: **true** o **false**
  - Valor predeterminado: **true**

- **PASSCODE_EXPIRY**
  - Nombre para mostrar: Requisito de cambio de PIN
  - Esta propiedad define cuánto tiempo es válido el PIN o código de acceso de Citrix, después de lo cual el usuario se ve obligado a cambiar su PIN o código de acceso de Citrix. Cuando se cambia esta configuración, el nuevo valor se establece solo cuando el PIN o código de acceso de Citrix actual caduca.
  - Valores posibles: **1** a **99** recomendado. Para eliminar los restablecimientos de PIN, establezca el valor en un número alto (por ejemplo, 100.000.000.000). Si estableció originalmente el período de caducidad entre 1 y 99 días y luego lo cambió a un número grande durante ese período: los PIN seguirán caducando al final del período inicial, pero nunca más después.
  - Valor predeterminado: **90** (días)

- **PASSCODE_HISTORY**
  - Nombre para mostrar: Historial de PIN
  - Esta propiedad define el número de PIN o códigos de acceso de Citrix utilizados anteriormente que los usuarios no pueden reutilizar al cambiar su PIN o código de acceso de Citrix. Cuando se cambia esta configuración, el nuevo valor se establece la próxima vez que los usuarios restablezcan su PIN o código de acceso de Citrix.
  - Valores posibles: **1** a **99**
  - Valor predeterminado: **5**

- **PASSCODE_MAX_ATTEMPTS**
  - Nombre para mostrar: Intentos de PIN
  - Esta propiedad define cuántos intentos erróneos de PIN o código de acceso de Citrix pueden realizar los usuarios antes de que se les solicite una autenticación completa.

Después de que los usuarios realicen correctamente una autenticación completa, se les solicitará que creen un PIN o código de acceso de Citrix.

- Valores posibles: Cualquier número entero positivo
- Valor predeterminado: **15**

- **PASSCODE_MIN_LENGTH**
  - Nombre para mostrar: Requisito de longitud del PIN
  - Esta propiedad define la longitud mínima de los PIN de Citrix.
  - Valores posibles: **4** a **10**
  - Valor predeterminado: **6**
- **PASSCODE_STRENGTH**
  - Nombre para mostrar: Requisito de fortaleza del PIN
  - Esta propiedad define la fortaleza de un PIN o código de acceso de Citrix. Cuando cambie esta configuración, se solicitará a los usuarios que creen un PIN o código de acceso de Citrix la próxima vez que se les solicite autenticarse.
  - Valores posibles: **Baja**, **Media**, **Alta** o **Fuerte**
  - Valor predeterminado: **Media**
  - Las reglas de contraseña para cada configuración de fortaleza, basadas en la configuración de PASSCODE_TYPE, son las siguientes:

Reglas para códigos de acceso numéricos:

FORTALEZA DEL CÓDIGO DE ACCESO	REGLAS PARA EL TIPO DE CÓDIGO DE ACCESO NUMÉRICO	PERMITIDO	NO PERMITIDO
Baja	Todos los números, cualquier secuencia permitida	444444, 123456, 654321	
Media (configuración predeterminada)	Todos los números no pueden ser iguales ni consecutivos.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321

FORTALEZA DEL CÓDIGO DE ACCESO	REGLAS PARA EL TIPO DE CÓDIGO DE ACCESO NUMÉRICO	PERMITIDO	NO PERMITIDO
Alta	Los números adyacentes no pueden ser iguales.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
Fuerte	No utilice el mismo número más de dos veces. No utilice tres o más números consecutivos seguidos. No utilice tres o más números consecutivos en orden inverso.	102983, 085085, 824673, 132312	132132, 131313, 902030

Reglas para códigos de acceso alfanuméricos:

FORTALEZA DEL CÓDIGO DE ACCESO	REGLAS PARA EL TIPO DE CÓDIGO DE ACCESO ALFANUMÉRICO	PERMITIDO	NO PERMITIDO
Baja	Debe tener al menos un número y una letra	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	ejemplo, ejemplo, ejemplo
Media (configuración predeterminada)	Además de las reglas para la fuerza de contraseña baja, las letras y todos los números no pueden ser iguales. Las letras no pueden ser consecutivas y los números no pueden ser consecutivos.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, o aaa111; abcd12, bcd123, 123abc, xy1234, xyz345, o cba123

FORTALEZA DEL CÓDIGO DE ACCESO	REGLAS PARA EL TIPO DE CÓDIGO DE ACCESO ALFANUMÉRICO	PERMITIDO	NO PERMITIDO
Alta	Incluya al menos una letra mayúscula y una letra minúscula.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
Fuerte	Incluya al menos un número, un símbolo especial, una letra mayúscula y una letra minúscula.	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

- **PASSCODE_TYPE**
  - Nombre para mostrar: Tipo de PIN
  - Esta propiedad define si los usuarios pueden definir un PIN numérico de Citrix o una contraseña alfanumérica. Cuando selecciona **Numérico**, los usuarios solo pueden usar números (PIN de Citrix). Cuando selecciona **Alfanumérico**, los usuarios pueden usar una combinación de letras y números (contraseña).

    Si cambia esta configuración, los usuarios deben establecer un nuevo PIN o contraseña de Citrix la próxima vez que se les solicite autenticarse.
  - Valores posibles: **Numérico** o **Alfanumérico**
  - Valor predeterminado: **Numérico**
- **REFRESHINTERVAL**
  - Nombre para mostrar: REFRESHINTERVAL
  - Por defecto, Citrix Endpoint Management hace ping al AutoDiscovery Server (ADS) para obtener certificados anclados cada 3 días. Para cambiar el intervalo de actualización, vaya a **Settings > Client Properties**, añada la clave personalizada **REFRESHINTERVAL** y establezca el **Valor** en el número de horas.
  - Valor predeterminado: **72** horas (3 días)
- **SEND_LDAP_ATTRIBUTES**

- Para implementaciones solo de MAM de dispositivos Android, iOS o macOS: Puede configurar Citrix Endpoint Management para que los usuarios que se inscriben en Citrix Secure Hub con credenciales de correo electrónico se inscriban automáticamente en Citrix Secure Mail. Como resultado, los usuarios no tienen que proporcionar información adicional ni realizar pasos adicionales para inscribirse en Citrix Secure Mail.
- Para configurar esta directiva de cliente global, vaya a **Settings > Client Properties**, añada la clave personalizada **SEND_LDAP_ATTRIBUTES** y establezca el **Valor** de la siguiente manera.
- Valor: `userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName=${user.displayName},mail=${user.mail}`
- Los valores de atributo se especifican como macros, de forma similar a las directivas MDM.
- Aquí tiene una muestra de respuesta del servicio de cuentas para esta propiedad:

  ```
  <property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,em name="SEND_LDAP_ATTRIBUTES"/>
  ```

- Para esta propiedad, Citrix Endpoint Management trata los caracteres de coma como terminadores de cadena. Por lo tanto, si un valor de atributo incluye una coma, preceda la coma con una barra invertida. La barra invertida evita que el cliente interprete la coma incrustada como el final del valor del atributo. Represente los caracteres de barra invertida con `"\\"`.

- **HIDE_THREE_FINGER_TAP_MENU**
  - Cuando esta propiedad no está configurada o está configurada como **false**, los usuarios pueden acceder al menú de funciones ocultas tocando con tres dedos en sus dispositivos. El menú de funciones ocultas permitía a los usuarios restablecer los datos de la aplicación. Configurar esta propiedad como **true** deshabilita el acceso de los usuarios al menú de funciones ocultas.
  - Para configurar esta política de cliente global, vaya a **Configuración > Propiedades del cliente**, añada la clave personalizada **HIDE_THREE_FINGER_TAP_MENU** y establezca el **Valor**.
- **TUNNEL_EXCLUDE_DOMAINS**
  - Nombre para mostrar: Dominios excluidos del túnel
  - De forma predeterminada, MDX excluye del micro túnel VPN algunos puntos finales de servicio que los SDK y las aplicaciones de Mobile Apps utilizan para diversas funciones.

Por ejemplo, esos puntos finales incluyen servicios que no requieren enrutamiento a través de redes empresariales, como Google Analytics, servicios de Citrix Cloud™ y servicios de Active Directory. Utilice esta propiedad de cliente para añadir dominios adicionales a la lista de dominios excluidos.

- Para configurar esta política de cliente global, vaya a **Configuración > Propiedades del cliente**, añada la clave personalizada **TUNNEL_EXCLUDE_DOMAINS** y establezca el **Valor**.
- Valor: Los dominios adicionales que desea excluir del túnel, escriba una lista de sufijos de dominio separados por comas. Por ejemplo:

```
app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.launchdarkly.com,hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com,features.netscalergatewaystaging.net,features.r
```

Las propiedades de cliente personalizadas para Citrix Endpoint Management son las siguientes:

ENABLE_MAM_NFACTOR_SSO:

- Esta propiedad le permite habilitar o deshabilitar el SSO nFactor de MAM durante la inscripción o el inicio de sesión de MAM para Secure Hub al utilizar la política de autenticación avanzada en NetScaler® Gateway. Si el valor se establece en **true**, el SSO nFactor de MAM se habilita durante la inscripción o el inicio de sesión de MAM para Secure Hub.
- Para configurar esta propiedad, vaya a **Configuración > Propiedades del cliente** y haga clic en **Agregar**. Seleccione **Clave personalizada** en el menú desplegable **Clave** y actualice la siguiente información según corresponda:
  - Clave - ENABLE_MAM_NFACTOR_SSO
  - Valor - true o false
  - Nombre - ENABLE_MAM_NFACTOR_SSO
  - Descripción - Añadir la descripción relevante

MICROSOFT_CERTIFICATE_STRONG_MAPPING:

- Esta propiedad controla si los certificados de cliente existentes se renuevan para admitir la función de asignación segura de certificados al anexar el Identificador de seguridad (SID) al Nombre alternativo del sujeto (SAN) cuando se utiliza Secure Mail con una Infraestructura de

clave pública (PKI) de Microsoft. Si el valor se establece en **true**, los certificados de cliente existentes se renovarán para incluir el SAN SID.

- Esta propiedad solo se aplica a la PKI de Microsoft.
- Para configurar esta propiedad, vaya a **Configuración > Propiedades del cliente** y haga clic en **Agregar**. Seleccione **Clave personalizada** en el menú desplegable **Clave** y actualice la siguiente información según corresponda:
  - Clave - MICROSOFT_CERTIFICATE_STRONG_MAPPING
  - Valor - true o false
  - Nombre - MICROSOFT_CERTIFICATE_STRONG_MAPPING
  - Descripción - Renovar certificados de cliente para incluir SAN SID

aeDeviceCertRenewSupport:

- Esta propiedad controla si los usuarios finales pueden ver el estado de salud del certificado del dispositivo y solucionar automáticamente los problemas de certificado desde la aplicación Citrix Secure Hub. Si el valor se establece en **true**, esta función se habilita.
- Para configurar esta propiedad, vaya a **Configuración > Propiedades del cliente** y haga clic en **Agregar**. Seleccione **Clave personalizada** en el menú desplegable **Clave** y actualice la siguiente información según corresponda:
  - Clave - aeDeviceCertRenewSupport
  - Valor - true o false
  - Nombre - aeDeviceCertRenewSupport
  - Description - Habilitar el estado de salud del certificado del dispositivo y la corrección automática de problemas de certificados

Opciones de inscripción de usuarios

Puede hacer que los usuarios inscriban sus dispositivos en Citrix Endpoint Management de varias maneras. Antes de considerar los detalles, decida qué dispositivos quiere inscribir en MDM+MAM, MDM o MAM. Para obtener más información sobre esos modos de administración, consulte Modos de administración.

En el nivel más alto, hay cuatro opciones de inscripción:

- **Invitación de inscripción:** Envíe una invitación de inscripción o una URL de invitación a los usuarios. Las invitaciones de inscripción y las URL no están disponibles para dispositivos Windows.
- **Portal de autoayuda:** Configure un portal que los usuarios puedan visitar para descargar Citrix Secure Hub, solicitar la inscripción y ver la información del dispositivo.
- **Inscripción manual:** Envíe un correo electrónico, un manual o alguna otra comunicación para informar a los usuarios de que el sistema está activo y que pueden inscribirse. Luego, los usuarios descargan Citrix Secure Hub e inscriben sus dispositivos manualmente.
- **Empresa:** Otra opción para la inscripción de dispositivos es a través de un Programa de implementación de Apple y Google Android Enterprise. A través de cada uno de estos programas, puede comprar dispositivos preconfigurados y listos para que los usen los empleados. Para obtener más información, consulte los artículos del Programa de implementación de Apple en Soporte de Apple y la documentación de Google Android Enterprise en el sitio web de Android Enterprise.

Invitación de inscripción

Puede enviar una invitación de inscripción por correo electrónico a usuarios con dispositivos iOS, macOS, Android Enterprise y Android heredado. Las invitaciones de inscripción no están disponibles para dispositivos Windows.

También puede enviar un enlace de instalación a través de SMTP a usuarios con dispositivos iOS, macOS, Android Enterprise, Android o Windows. Para obtener más información, consulte Inscribir dispositivos.

Si elige utilizar el método de invitación de inscripción, puede:

- Elegir los modos de seguridad de inscripción **URL de invitación**, **URL de invitación + PIN** o **URL de invitación + Contraseña**.
- Utilizar cualquier combinación de los modos.
- Habilitar o deshabilitar los modos desde la página **Configuración** de Citrix Endpoint Management.

Para obtener información sobre cada modo de seguridad de inscripción, consulte Configurar modos de seguridad de inscripción.

Las invitaciones tienen muchos propósitos. El uso más común de las invitaciones es notificar a los usuarios que el sistema está disponible y que pueden inscribirse. Las URL de invitación son únicas. Después de que un usuario utiliza una URL de invitación, esta ya no está disponible.

Puede utilizar esta propiedad para limitar los usuarios o dispositivos que se inscriben en su sistema.

Al configurar un perfil de inscripción, puede controlar el número de dispositivos que los usuarios específicos pueden inscribir, en función de los grupos de Active Directory. Por ejemplo, puede permitir que su división de Finanzas tenga solo un dispositivo por usuario.

Tenga en cuenta los costes adicionales y los inconvenientes de ciertas opciones de inscripción. Para enviar invitaciones mediante SMTP se requiere infraestructura adicional. Para obtener más información sobre esta opción, consulte Notificaciones.

Además, para enviar invitaciones por correo electrónico, asegúrese de que los usuarios tengan una forma de acceder al correo electrónico fuera de Citrix Secure Hub. Puede utilizar los modos de seguridad de inscripción con contraseña de un solo uso (OTP) como alternativa a las contraseñas de Active Directory para la inscripción de MDM.

Portal de autoservicio

Se puede acceder al Portal de autoservicio en la misma URL que utilizan los administradores para acceder a la consola de Citrix Endpoint Management. Los usuarios finales ven el Portal de autoservicio en lugar de la consola de administración. Los usuarios pueden descargar Citrix Secure Hub, solicitar la inscripción y ver la información del dispositivo en el Portal de autoservicio.

Para configurar un portal, actualice estas propiedades del servidor en **Parámetros > Propiedades del servidor**:

- `shp.console.enable`: Establezca en **True** para proporcionar acceso al Portal de autoservicio.
- `enable.new.shp`: Establezca en **True** para permitir a los usuarios habilitar sus dispositivos desde el Portal de autoservicio.

Inscripción manual

Con la inscripción manual, los usuarios se conectan a Citrix Endpoint Management a través de AutoDiscovery o introduciendo la información del servidor. Con AutoDiscovery, los usuarios inician sesión solo con su dirección de correo electrónico o sus credenciales de Active Directory en formato de nombre principal de usuario (UPN). Sin AutoDiscovery, deben introducir la dirección del servidor y sus credenciales de Active Directory. Para obtener más información sobre cómo configurar AutoDiscovery, consulte Configurar el servicio AutoDiscovery de Citrix Endpoint Management.

Puede facilitar la inscripción manual de varias maneras. Puede crear una guía, distribuirla a los usuarios y hacer que se inscriban ellos mismos. Puede hacer que su departamento de TI inscriba manualmente grupos de usuarios en franjas horarias determinadas. Puede utilizar cualquier método similar en el que los usuarios deban introducir sus credenciales o la información del servidor.

Incorporación de usuarios

Una vez que tenga su entorno configurado, debe decidir cómo incorporar a los usuarios a su entorno. Una sección anterior de este artículo analiza los detalles de los modos de seguridad de inscripción de usuarios. Esta sección analiza la forma en que se comunica con los usuarios.

Inscripción abierta frente a invitación selectiva

Al incorporar usuarios, puede permitir la inscripción a través de dos métodos básicos:

- Inscripción abierta. De forma predeterminada, cualquier usuario con credenciales LDAP y la información del entorno de Citrix Endpoint Management puede inscribirse.
- Inscripción limitada. Puede limitar el número de usuarios permitiendo únicamente la inscripción a los usuarios con invitaciones. También puede limitar la inscripción abierta mediante un grupo de Active Directory.

Con el método de invitación, también puede limitar el número de dispositivos que un usuario puede inscribir. En la mayoría de las situaciones, la inscripción abierta es aceptable, pero hay algunas cosas que considerar:

- Para la inscripción de MAM, puede limitar fácilmente la inscripción abierta mediante la pertenencia a un grupo de Active Directory.
- Para la inscripción de MDM, puede limitar el número de dispositivos que pueden inscribirse en función de la pertenencia a un grupo de Active Directory. Si solo permite dispositivos corporativos en su entorno, esa limitación no suele ser un problema. Sin embargo, es posible que desee considerar este método en un entorno de trabajo BYOD si desea limitar el número de dispositivos en su entorno.

La invitación selectiva se realiza con menos frecuencia porque requiere un poco más de trabajo que la inscripción abierta. Para que los usuarios inscriban sus dispositivos en su entorno, debe enviar una invitación única a cada usuario. Para obtener información sobre cómo enviar una invitación de inscripción, consulte Invitaciones de inscripción.

Envíe una invitación para cada usuario o grupo que desee inscribir en su entorno. Ese proceso puede llevar mucho tiempo, dependiendo del tamaño de su organización. Es posible utilizar

grupos de Active Directory para crear invitaciones en lotes, pero debe llevar a cabo este enfoque por fases.

Primer contacto con los usuarios

Después de decidir si usar la inscripción abierta o la invitación selectiva y de configurar esos entornos, informe a los usuarios sobre sus opciones de inscripción.

Si utiliza el método de invitación selectiva, los mensajes de correo electrónico forman parte del proceso. También puede enviar correos electrónicos a través de la consola de Citrix Endpoint Management para la inscripción abierta. Para obtener más información, consulte Invitaciones de inscripción.

En cualquier caso, tenga en cuenta que para el correo electrónico necesita un servidor SMTP. Esos servidores pueden suponer un coste adicional a considerar al tomar su decisión. Considere cómo espera que los nuevos usuarios accedan a la información. Si desea que todos los usuarios accedan a su correo electrónico a través de Citrix Endpoint Management, enviarles un correo electrónico de invitación podría ser problemático.

También puede enviar comunicaciones por otros medios fuera de Citrix Endpoint Management para un entorno de inscripción abierta. Para esa opción, asegúrese de incluir toda la información relevante. Informe a los usuarios dónde pueden obtener la aplicación Citrix Secure Hub y qué método usar para inscribirse. Si tiene la detección desactivada, también proporcione a los usuarios la dirección del servidor de Citrix Endpoint Management. Para obtener más información sobre la detección, consulte Configurar el servicio AutoDiscovery de Citrix Endpoint Management.

Aprovisionamiento y desaprovisionamiento de aplicaciones

El aprovisionamiento de aplicaciones gira en torno a la gestión del ciclo de vida de las aplicaciones móviles: preparar, configurar, entregar y administrar aplicaciones móviles dentro del entorno de Citrix Endpoint Management. A veces, el desarrollo o la modificación del código de la aplicación también pueden formar parte del proceso de aprovisionamiento. Citrix Endpoint Management está equipado con varias herramientas y procesos que puede utilizar para el aprovisionamiento de aplicaciones.

Antes de leer este artículo sobre el aprovisionamiento de aplicaciones, le recomendamos que lea Aplicaciones y Comunidades de usuarios. Cuando haya finalizado el tipo de aplicaciones que su organización planea entregar a los usuarios, podrá entonces definir el proceso para administrar las aplicaciones a lo largo de su ciclo de vida.

Tenga en cuenta los siguientes puntos al definir su proceso de aprovisionamiento de aplicaciones:

- **Creación de perfiles de aplicaciones:** Su organización podría empezar con un número limitado de aplicaciones. Sin embargo, el número de aplicaciones que administra puede aumentar rápidamente a medida que aumentan las tasas de adopción por parte de los usuarios y crece su entorno. Defina perfiles de aplicaciones específicos de antemano para facilitar la administración del aprovisionamiento de aplicaciones. La creación de perfiles de aplicaciones le ayuda a categorizar las aplicaciones en grupos lógicos desde una perspectiva no técnica. Por ejemplo, puede crear perfiles de aplicaciones basados en los siguientes factores:
  - Versión: Versión de la aplicación para el seguimiento
  - Instancias: Muchas instancias que se implementan para diferentes conjuntos de usuarios, por ejemplo, con diferentes niveles de acceso
  - Plataforma: iOS, Android o Windows
  - Público objetivo: Usuarios estándar, departamentos, ejecutivos de nivel C
  - Propiedad: Departamento propietario de la aplicación
  - Tipo: MDX, pública, web y SaaS, o enlaces web
  - Ciclo de actualización: Con qué frecuencia se actualiza la aplicación
  - Licencias: Requisitos de licencia y propiedad
  - Directivas de MAM SDK o MDX: Para aplicar las capacidades de MDX a sus aplicaciones móviles
  - Acceso a la red: Tipo de acceso, como la tunelización de tráfico HTTP y HTTPS con inicio de sesión único (Tunelizado - SSO web).

Ejemplo:

FACTOR	CITRIX SECURE MAIL	CORREO	INTERNO	EPIC ROVER
Versión	10.1	10.1	X.x	X.x
Instancia	VIP	Médicos	Clínico	Clínico
Plataforma	iOS	iOS	iOS	iOS
Usuarios de destino	Usuarios VIP	Médicos	Usuarios clínicos	Usuarios clínicos
Propiedad	TI	TI	TI	TI

FACTOR	CITRIX SECURE MAIL	CORREO	INTERNO	EPIC ROVER
Tipo	MDX	MDX	Nativa	Pública
Ciclo de actualización	Trimestral	Trimestral	Anual	N/D
Licencias	N/D	N/D	N/D	Compra por volumen
Directivas MDX	Sí	Sí	Sí	No
Acceso a la red	VPN	VPN	VPN	Público

- **Control de versiones de aplicaciones:** Mantener y realizar un seguimiento de las versiones de las aplicaciones es una parte fundamental del proceso de aprovisionamiento. El control de versiones suele ser transparente para los usuarios. Solo reciben notificaciones cuando hay una nueva versión de la aplicación disponible para descargar. Desde su perspectiva, revisar y probar cada versión de la aplicación en un entorno que no sea de producción también es fundamental para evitar afectar a un sitio de producción.

  También es importante evaluar si se requiere una actualización específica. Las actualizaciones de aplicaciones suelen ser de dos tipos: una actualización menor, como una corrección de un error específico, o una versión principal, que introduce cambios significativos. En cualquier caso, revise cuidadosamente las Notas de la versión de la aplicación para evaluar si la actualización es necesaria.
- **Desarrollo de aplicaciones:** Al integrar el SDK de MAM en las aplicaciones móviles que desarrolla, aplica las capacidades de MDX a esas aplicaciones. Consulte Información general del SDK de MAM.

  El SDK de MAM reemplaza a MDX Toolkit, cuya retirada está programada para julio de 2023. Para obtener información sobre el ajuste de aplicaciones, consulte MDX Toolkit. El proceso de aprovisionamiento de aplicaciones para una aplicación ajustada difiere del proceso de aprovisionamiento para una aplicación estándar no ajustada.
- **Seguridad de las aplicaciones:** Usted define los requisitos de seguridad de las aplicaciones individuales o los perfiles de aplicaciones como parte del proceso de aprovisionamiento. Puede asignar los requisitos de seguridad a políticas MDM o MAM específicas antes de

implementar las aplicaciones. Esa planificación simplifica y acelera la implementación de aplicaciones. Por ejemplo:

  - Puede que implemente ciertas aplicaciones de forma diferente.
  - Es posible que desee realizar cambios arquitectónicos en su entorno de Citrix Endpoint Management. Los cambios dependen del tipo de cumplimiento de seguridad que requieran las aplicaciones. Por ejemplo, una aplicación en particular podría requerir cifrado SSL de extremo a extremo o geofencing.

- **Entrega de aplicaciones:** Citrix Endpoint Management le permite entregar aplicaciones como aplicaciones MDM o como aplicaciones MAM. Las aplicaciones MDM aparecen en la tienda de aplicaciones. Esta tienda le permite entregar cómodamente aplicaciones públicas o nativas a los usuarios. Aparte de aplicar restricciones a nivel de dispositivo, no se necesitan otros controles de aplicaciones. Sin embargo, la entrega de aplicaciones mediante MAM permite un control total sobre la entrega de aplicaciones y sobre la propia aplicación. La entrega de las aplicaciones a través de MAM suele ser más adecuada.
- **Mantenimiento de aplicaciones:**
  - Realice una auditoría inicial: Haga un seguimiento de la versión de la aplicación presente en su entorno de producción y del último ciclo de actualización. Tome nota de las características específicas o las correcciones de errores que requirieron la actualización.
  - Establezca líneas base: Mantenga una lista de las últimas versiones estables de cada aplicación. Esté preparado para volver a una versión anterior de la aplicación si surgen problemas inesperados después de una actualización. Desarrolle un plan de reversión. Pruebe las actualizaciones de aplicaciones en un entorno de prueba antes de implementarlas en producción. Si es posible, implemente la actualización primero en un subconjunto de usuarios de producción y luego en toda la base de usuarios.
  - Suscríbase a las notificaciones de actualización de software de Citrix® y a las notificaciones de cualquier proveedor de software de terceros: Mantenerse al día con las últimas versiones de las aplicaciones es fundamental. Una versión de acceso anticipado (EAR) podría estar disponible para pruebas con antelación.
  - Diseñe una estrategia para notificar a los usuarios: Defina una estrategia para notificar a los usuarios cuando haya actualizaciones de aplicaciones disponibles. Prepare a los usuarios con formación antes de la implementación. Considere enviar varias notificaciones antes de actualizar la aplicación. Dependiendo de la aplicación, el mejor método de notificación podría ser las notificaciones por correo electrónico o los sitios web.

La gestión del ciclo de vida de las aplicaciones implica el ciclo de vida completo de una aplicación, desde su implementación inicial hasta su retirada. El ciclo de vida de una aplicación tiene estas fases:

1. Requisitos para las especificaciones: Comience con el caso de negocio y los requisitos de usuario.
2. Desarrollo: Validar que la aplicación satisface las necesidades del negocio.
3. Pruebas: Identificar usuarios de prueba, problemas y errores.
4. Implementación: Implementar la aplicación para los usuarios de producción.
5. Mantenimiento: Actualizar la versión de la aplicación. Implementar la aplicación en un entorno de prueba antes de actualizarla en un entorno de producción.

Operaciones basadas en el panel de control

Puede ver información de un vistazo al acceder al panel de control de su consola de Citrix Endpoint Management. Con esta información, puede ver los problemas y los éxitos rápidamente mediante el uso de widgets.

El panel de control suele ser la pantalla que aparece al iniciar sesión por primera vez en la consola de Citrix Endpoint Management. Para acceder al panel de control desde cualquier otra parte de la consola, haga clic en **Analizar**. Haga clic en **Personalizar** en el panel de control para editar el diseño de la página y los widgets que aparecen.

- **Mis paneles de control:** Puede guardar hasta cuatro paneles de control. Puede editar estos paneles de control por separado y ver cada uno seleccionando el panel de control guardado.
- **Estilo de diseño:** En esta fila, puede seleccionar cuántos widgets aparecen en su panel de control y cómo están distribuidos.
- **Selección de widgets:** Puede elegir qué información aparece en su panel de control.
    - **Notificaciones:** Marque la casilla de verificación encima de los números de la izquierda para añadir una barra de notificaciones encima de sus widgets. Esta barra muestra el número de dispositivos compatibles, dispositivos inactivos y dispositivos borrados o inscritos en las últimas 24 horas.
    - **Dispositivos por plataforma:** Muestra el número de dispositivos administrados y no administrados por plataforma.
    - **Dispositivos por operador:** Muestra el número de dispositivos administrados y no administrados por operador. Haga clic en cada barra para ver un desglose por plataforma.

- **Dispositivos administrados por plataforma:** Muestra el número de dispositivos administrados por plataforma.
- **Dispositivos no administrados por plataforma:** Muestra el número de dispositivos no administrados por plataforma. Los dispositivos que aparecen en este gráfico pueden tener un agente instalado, pero se les han revocado los privilegios o se han borrado.
- **Dispositivos por estado de ActiveSync Gateway:** Muestra el número de dispositivos agrupados por estado de ActiveSync Gateway. La información muestra el estado Bloqueado, Permitido o Desconocido. Puede hacer clic en cada barra para desglosar los datos por plataforma.
- **Dispositivos por propiedad:** Muestra el número de dispositivos agrupados por estado de propiedad. La información muestra el estado de propiedad corporativa, propiedad del empleado o desconocido.
- **Implementaciones de grupos de entrega fallidas:** Muestra el número total de implementaciones fallidas por paquete. Solo aparecen los paquetes que tienen implementaciones fallidas.
- **Dispositivos por motivo de bloqueo:** Muestra el número de dispositivos bloqueados por ActiveSync
- **Aplicaciones instaladas:** Con este widget, puede escribir el nombre de una aplicación y un gráfico mostrará información sobre ella.
- **Uso de licencias de aplicaciones de compra por volumen:** Muestra estadísticas de uso de licencias para aplicaciones de compra por volumen de Apple.

Casos de uso

A continuación, se muestran algunos ejemplos de las muchas formas en que puede utilizar los widgets del panel para supervisar su entorno.

- Ha implementado aplicaciones de productividad móvil de Citrix y está recibiendo tickets de soporte sobre fallos en la instalación de estas aplicaciones en los dispositivos. Utilice los widgets **Dispositivos no conformes** y **Aplicaciones instaladas** para ver los dispositivos que no tienen instaladas las aplicaciones de productividad móvil de Citrix.
- Quiere supervisar los dispositivos inactivos para poder eliminarlos de su entorno y recuperar licencias. Utilice el widget **Dispositivos inactivos** para realizar un seguimiento de esta estadística.
- Está recibiendo tickets de soporte relacionados con la sincronización incorrecta de datos. Es posible que desee utilizar los widgets **Dispositivos por estado de ActiveSync Gateway** y

Dispositivos por motivo de bloqueo para determinar si el problema está relacionado con ActiveSync.

Informes

Una vez configurado el entorno y registrados los usuarios, puede ejecutar informes para obtener información sobre su implementación. Citrix Endpoint Management incluye varios informes integrados para ayudarle a obtener una mejor imagen de los dispositivos que se ejecutan en su entorno. Para obtener más información, consulte Informes.

Control de acceso basado en roles y compatibilidad con Citrix Endpoint Management

Citrix Endpoint Management utiliza el control de acceso basado en roles (RBAC) para restringir el acceso de usuarios y grupos a las funciones del sistema de Citrix Endpoint Management, como la consola de Citrix Endpoint Management, el portal de autoayuda y la API pública. Este artículo describe los roles integrados en Citrix Endpoint Management e incluye consideraciones para decidir un modelo de soporte para Citrix Endpoint Management que utilice RBAC.

Roles integrados

Puede cambiar el acceso concedido a los siguientes roles integrados y puede agregar roles. Para ver el conjunto completo de permisos de acceso y funciones asociados a cada rol y su configuración predeterminada, descargue (/es-es/citrix-endpoint-management/downloads/rbac-defaults.pdf). Para obtener una definición de cada función, consulte (/es-es/citrix-endpoint-management/users/rbac-roles-and-permissions.html).

Rol de administrador

Acceso predeterminado concedido:

- Acceso completo al sistema, excepto al portal de autoayuda.
- De forma predeterminada, los administradores pueden realizar algunas tareas de soporte, como comprobar la conectividad y crear paquetes de soporte.

Consideraciones:

- ¿Necesitan algunos o todos sus administradores acceso al portal de autoayuda? Si es así, puede editar el rol de administrador o agregar roles de administrador.
- Para restringir aún más el acceso a algunos administradores o grupos de administradores, agregue roles basados en la plantilla de administrador y edite los permisos.

Usuario

Acceso predeterminado concedido:

- Acceso al portal de autoayuda, que permite a los usuarios autenticados generar enlaces de inscripción. Los enlaces les permiten inscribir sus dispositivos o enviarse una invitación de inscripción.
- Acceso restringido a la consola de Citrix Endpoint Management: funciones del dispositivo (como borrar, bloquear/desbloquear dispositivo; bloquear/desbloquear contenedor; ver ubicación y establecer restricciones geográficas; hacer sonar el dispositivo; restablecer la contraseña del contenedor); agregar, eliminar y enviar invitaciones de inscripción.

Consideraciones:

- El rol de Usuario le permite habilitar a los usuarios para que se ayuden a sí mismos.
- Para admitir dispositivos compartidos, cree un rol de usuario para la inscripción de dispositivos compartidos.

Consideraciones para un modelo de soporte de Citrix Endpoint Management

Los modelos de soporte que puede adoptar pueden variar ampliamente y pueden involucrar a terceros que manejan el soporte de nivel 1 y 2, mientras que los empleados manejan el soporte de nivel 3 y 4. Independientemente de cómo distribuya la carga de soporte, tenga en cuenta las consideraciones de esta sección específicas para su implementación de Citrix Endpoint Management y su base de usuarios.

¿Los usuarios tienen dispositivos corporativos o BYO? La pregunta principal que influye en el soporte es quién posee los dispositivos de usuario en su entorno de Citrix Endpoint Management. Si sus usuarios tienen dispositivos corporativos, es posible que ofrezca un nivel de soporte más bajo, como una forma de bloquear los dispositivos. En ese caso, podría proporcionar un servicio de asistencia técnica que ayude a los usuarios con problemas de dispositivos y cómo usarlos. Dependiendo de los tipos de dispositivos que necesite admitir, considere cómo podría usar los roles de aprovisionamiento y soporte de dispositivos RBAC para su servicio de asistencia técnica.

Si sus usuarios tienen dispositivos BYO, su organización podría esperar que los usuarios encuentren sus propias fuentes de soporte para dispositivos. En ese caso, el soporte que su organización proporciona es más un rol administrativo centrado en problemas específicos de Citrix Endpoint Management.

¿Cuál es su modelo de soporte para equipos de escritorio? Considere si su modelo de soporte para equipos de escritorio es apropiado para otros dispositivos corporativos. ¿Puede usar la misma organización de soporte? ¿Qué capacitación adicional podrían necesitar?

¿Desea dar a los usuarios acceso al portal de autoayuda de Citrix Endpoint Management? Aunque algunas organizaciones prefieren no conceder a los usuarios acceso a Citrix Endpoint Management, dar a los usuarios algunas capacidades de autoayuda puede aliviar la carga de su organización de soporte. Si el rol de usuario predeterminado para RBAC incluye permisos que no desea conceder, considere la posibilidad de crear un rol con solo los permisos que desea incluir. Puede crear tantos roles como sea necesario para satisfacer sus requisitos.

Envío de invitaciones de inscripción de grupo en Citrix Endpoint Management

Puede enviar invitaciones de inscripción a grupos y grupos anidados en Citrix Endpoint Management. Las invitaciones de inscripción no están disponibles para dispositivos Windows.

Al configurar la invitación de grupo, puede especificar una o varias plataformas de dispositivos. También puede etiquetar dispositivos para, por ejemplo, diferenciar los dispositivos propiedad de la empresa de los dispositivos propiedad de los empleados. A continuación, establece el tipo de autenticación para los dispositivos de usuario.

> **Nota:**
>
> Si tiene previsto utilizar plantillas de notificación personalizadas, debe configurarlas antes de configurar los modos de seguridad de inscripción. Para obtener más información sobre las plantillas de notificación, consulte Crear y actualizar plantillas de notificación.
>
> Para obtener más información sobre las configuraciones básicas de cuentas de usuario, roles y modos de seguridad e invitaciones de inscripción, consulte Cuentas de usuario, roles e inscripción.

Pasos generales

1. En la consola de Citrix Endpoint Management, vaya a **Administrar > Invitaciones de inscripción**.
2. Haga clic en **Agregar** en la parte superior izquierda de la pantalla y, a continuación, haga clic en **Agregar invitación**.

3. Haga clic en **Grupo** en el menú **Destinatario**.

   Este paso le permite elegir una o varias plataformas. Si tiene una combinación de diferentes plataformas de sistemas operativos en su empresa, elija todas las plataformas. Solo desactive la selección de plataforma si está seguro de que ningún usuario está utilizando esa plataforma en particular.

4. Puede optar por etiquetar dispositivos durante el proceso de invitación. Elija **Corporativo** o **Empleado**.

   El etiquetado facilita la separación de los dispositivos propiedad de la empresa y los dispositivos propiedad de los empleados.

5. En la lista **Dominio**, elija el dominio en el que existe el grupo.
6. En la lista **Grupo**, seleccione el grupo de Active Directory al que desea enviar las invitaciones.
7. El **Modo de inscripción** le permite establecer el tipo de seguridad de inscripción que prefiera para los usuarios.

   - Nombre de usuario + Contraseña
   - Alta seguridad
   - URL de invitación
   - URL de invitación + PIN
   - URL de invitación + Contraseña
   - Dos factores
   - Nombre de usuario + PIN

> **Nota:**
>
> Hemos dejado de admitir el modo de seguridad de inscripción **Alta seguridad**. Para enviar invitaciones de inscripción, solo puede usar los modos de seguridad de inscripción **URL de invitación**, **URL de invitación + PIN** o **URL de invitación + Contraseña**. Para los dispositivos que se inscriben con **Nombre de usuario + Contraseña**, **Dos factores** o **Nombre de usuario + PIN**, los usuarios deben descargar Citrix Secure Hub e introducir sus credenciales manualmente.

8. Para las plantillas de **Descarga del agente**, **URL de inscripción**, **PIN de inscripción** y **Confirmación de inscripción**, elija la plantilla de notificación personalizada que haya creado anteriormente. O bien, elija la predeterminada que aparece en la lista.

   Para estas plantillas de notificación, use la configuración de su servidor SMTP configurado en Citrix Endpoint Management. Configure primero la información de su SMTP antes de continuar.

   > **Nota:**
   >
   > Las opciones **Caduca después de** y **Intentos máximos** cambian según la opción de **Modo de inscripción** que elija. No puede cambiar estas opciones.

9. Seleccione Activado para **Enviar invitación** y, a continuación, haga clic en **Guardar y enviar** para completar el proceso.

Compatibilidad con grupos anidados

Puede usar grupos anidados para enviar invitaciones. Normalmente, los grupos anidados se utilizan en entornos a gran escala donde los grupos con permisos similares están vinculados entre sí.

Vaya a **Settings > LDAP** y, a continuación, habilite la opción **Support nested group**.

Solución de problemas y limitaciones conocidas

Problema: Se envían invitaciones a usuarios a pesar de que se les ha eliminado de un grupo de Active Directory.

Solución: Dependiendo del tamaño de su entorno de Active Directory, los cambios pueden tardar hasta seis horas en propagarse a todos los servidores. Si un usuario o grupo anidado se elimina recientemente, Citrix Endpoint Management podría seguir considerando a esos usuarios como parte del grupo.

Por lo tanto, es mejor esperar hasta seis horas antes de enviar otra invitación de grupo a sus usuarios.

Configuración de la autenticación basada en certificados con EWS para las notificaciones push de Citrix Secure Mail

Para que funcionen las notificaciones push de Citrix Secure Mail, debe hacer lo siguiente:

- Configure Exchange Server para la autenticación basada en certificados. Este requisito es especialmente necesario cuando Citrix Secure Hub está inscrito en Citrix Endpoint Management con autenticación basada en certificados.
- Configure el directorio virtual de Active Sync y Exchange Web Services (EWS) en el servidor de correo de Exchange con autenticación basada en certificados.

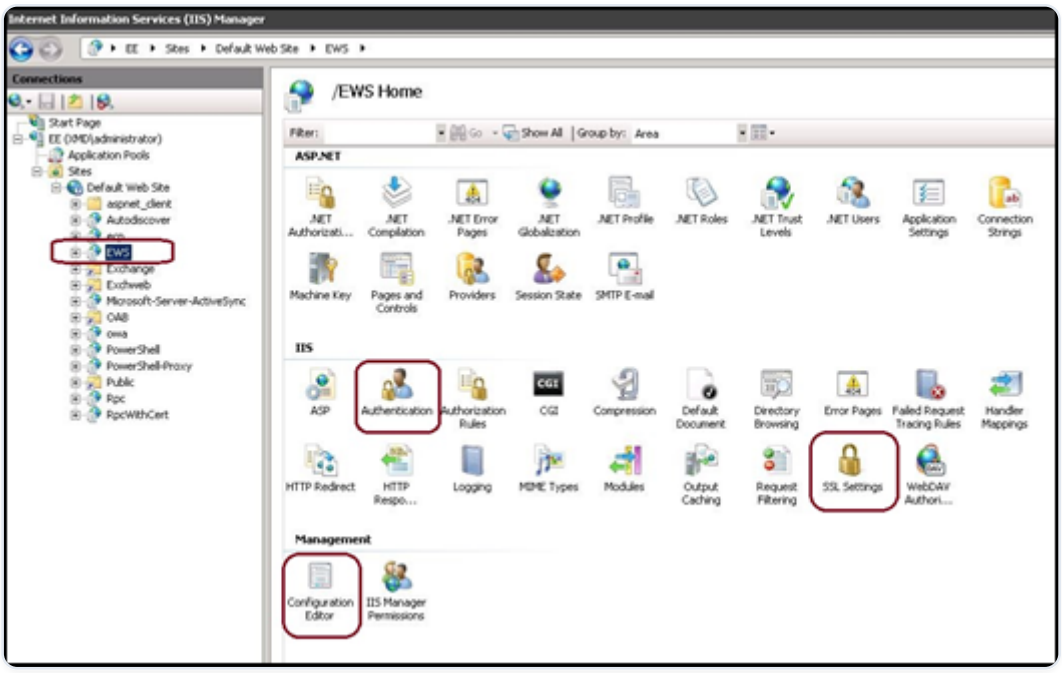
A menos que complete estas configuraciones, la suscripción a las notificaciones push de Citrix Secure Mail fallará y no se producirán actualizaciones de insignias en Citrix Secure Mail.

Este artículo describe los pasos para configurar la autenticación basada en certificados. Las configuraciones son específicamente para el directorio virtual de EWS en el servidor de Exchange.

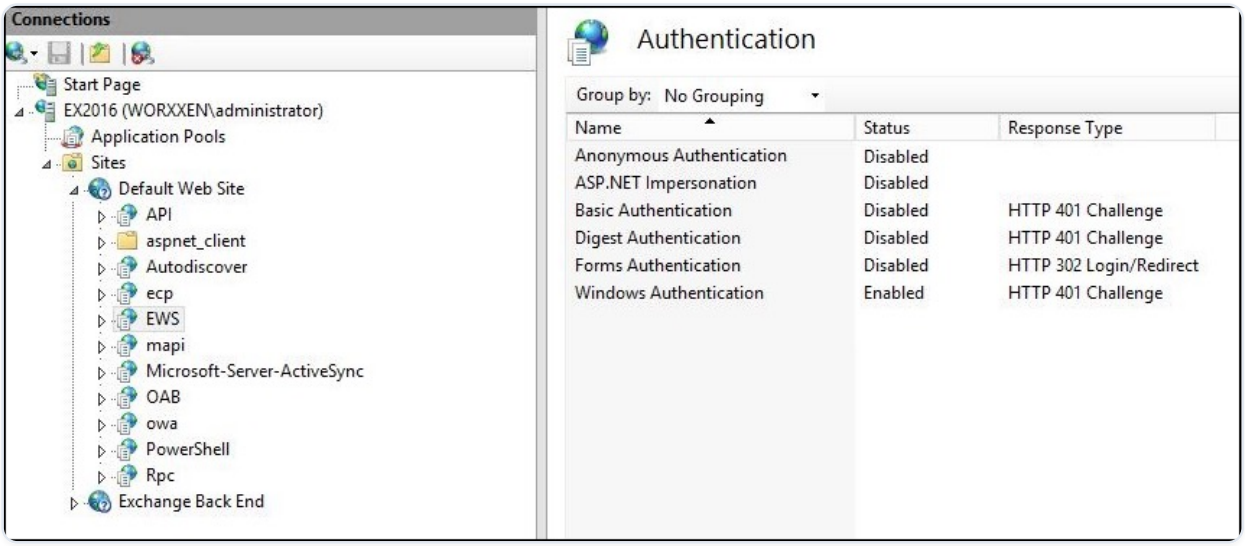
Para empezar con la configuración, haga lo siguiente:

1. Inicie sesión en el servidor o servidores donde está instalado el directorio virtual de EWS.
2. Abra la Consola del Administrador de IIS.
3. En **Default Web Site**, haga clic en el directorio virtual de EWS.

   Los complementos de Autenticación, SSL y Editor de configuración se encuentran en el lado derecho de la Consola del Administrador de IIS.



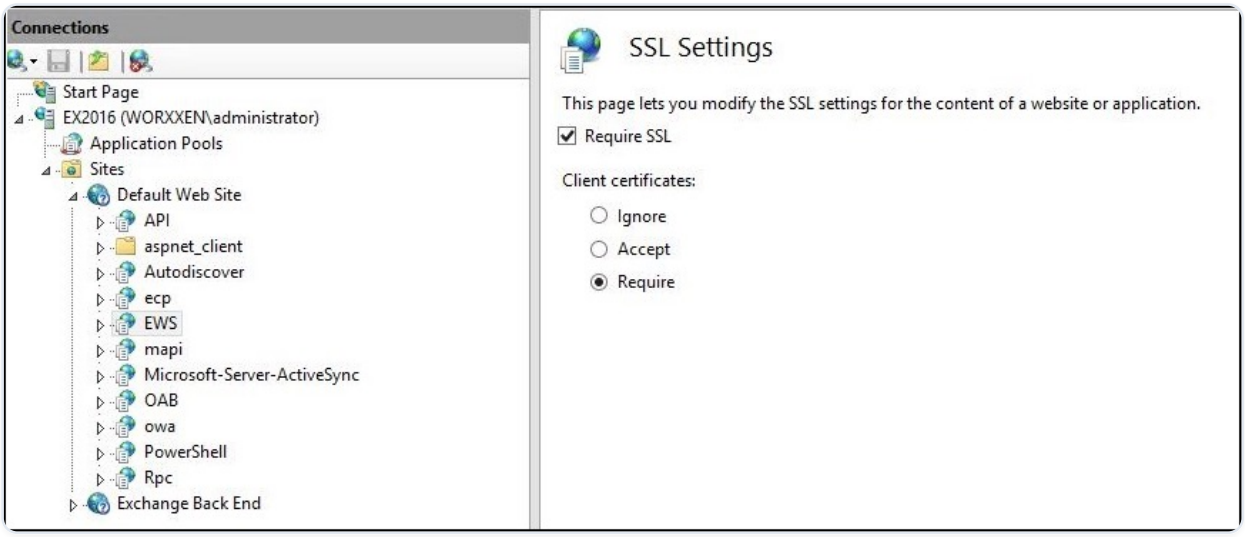
4. Asegúrese de que la configuración de **Autenticación** para EWS esté configurada como se muestra en la siguiente figura.



5. Configure la **Configuración de SSL** para el directorio virtual de EWS.

   a. Seleccione la casilla **Requerir SSL**.

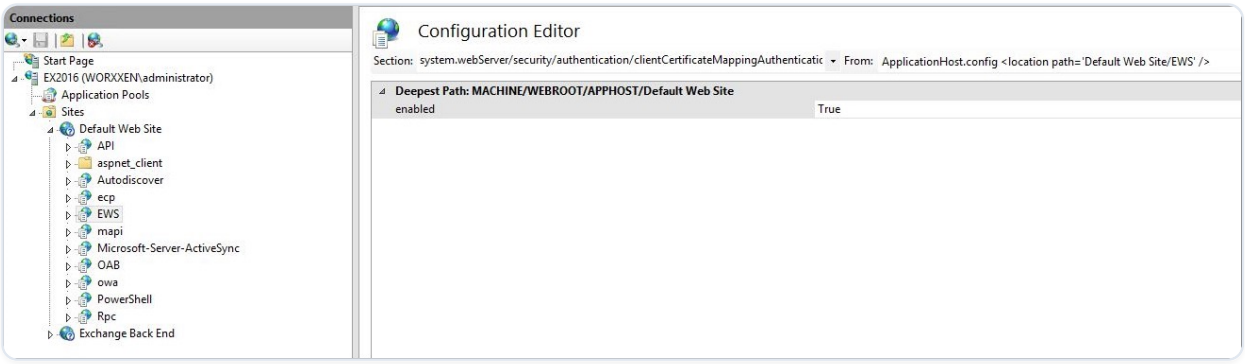
   b. En **Certificados de cliente**, haga clic en **Requerir**. O, si otros clientes de correo EWS utilizan un nombre de usuario y una contraseña para autenticarse en el servidor de Exchange, haga clic en **Aceptar**.



6. Haga clic en **Editor de configuración**. Vaya a la siguiente sección en la lista desplegable **Sección**:

   - **system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. Establezca el valor de **enabled** en **True**.



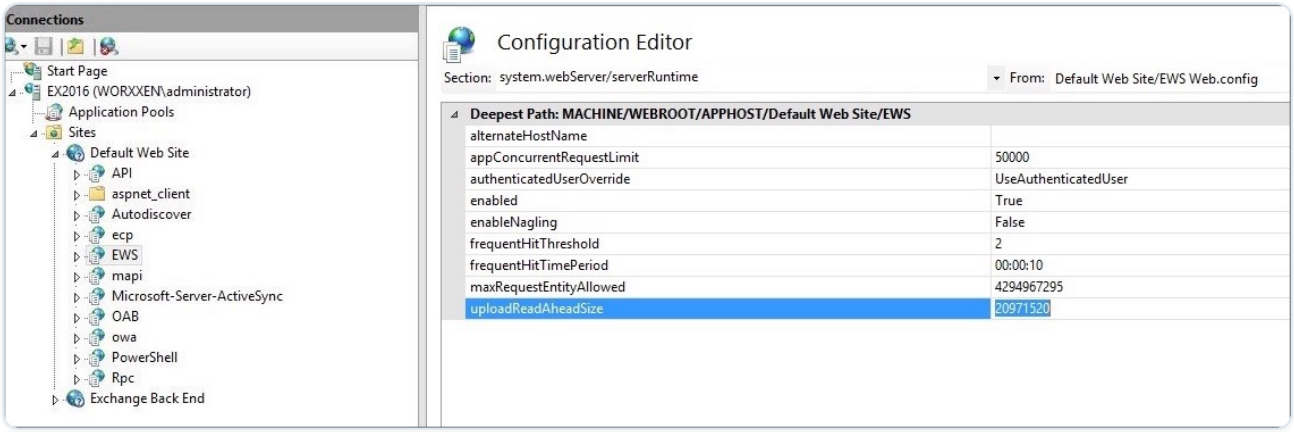
8. Haga clic en **Editor de configuración**. Vaya a la siguiente sección en la lista desplegable **Sección**:

   - **system.webServer/serverRuntime**

9. Establezca el valor de **uploadReadAheadSize** en **10485760** (10 MB) o **20971520** (20 MB) o en un valor según lo requiera su organización.

> **Importante:**
>
> Si no establece este valor correctamente, la autenticación basada en certificados al suscribirse a las notificaciones push de EWS puede fallar con un código de error 413.
>
> No establezca este valor en **0**.

Para obtener más información, consulte el artículo de Microsoft, Tiempo de ejecución del servidor IIS de Microsoft.



Para obtener más información sobre la resolución de problemas de Citrix Secure Mail con las notificaciones push de iOS, consulte este artículo del Centro de conocimientos de asistencia de Citrix.

Información relacionada

Notificaciones push para Citrix Secure Mail para iOS

Configuración de un servidor local de Atestación de estado del dispositivo

Puede habilitar la Atestación de estado del dispositivo (DHA) para dispositivos móviles con Windows 10 y Windows 11 a través de un servidor Windows local. Para habilitar DHA localmente, primero debe configurar un servidor DHA.

Después de configurar el servidor DHA, cree una directiva de Citrix Endpoint Management para habilitar el servicio DHA local. Para obtener más información, consulte Directiva de dispositivo de Atestación de estado del dispositivo.

Requisitos previos para un servidor DHA

- Un servidor que ejecute Windows Server Technical Preview 5 o posterior, instalado con la opción de instalación Experiencia de escritorio.
- Uno o varios dispositivos cliente con Windows 10 y Windows 11. Estos dispositivos deben tener TPM 1.2 o 2.0 y ejecutar la versión más reciente de Windows.
- Estos certificados:
  - **Certificado SSL de DHA:** Un certificado SSL x.509 que se encadena a una raíz de confianza empresarial con una clave privada exportable. Este certificado protege las comunicaciones de datos de DHA en tránsito, incluidas:
    - comunicaciones de servidor a servidor (servicio DHA y servidor MDM)
    - comunicaciones de servidor a cliente (servicio DHA y un dispositivo Windows 10 o Windows 11)
  - **Certificado de firma de DHA:** Un certificado x.509 que se encadena a una raíz de confianza empresarial con una clave privada exportable. El servicio DHA utiliza este certificado para la firma digital.
  - **Certificado de cifrado de DHA:** Un certificado x.509 que se encadena a una raíz de confianza empresarial con una clave privada exportable. El servicio DHA también utiliza este certificado para el cifrado.
- Elija uno de estos modos de validación de certificados:

- **EKCert:** El modo de validación EKCert está optimizado para dispositivos en organizaciones que no están conectadas a Internet. Los dispositivos que se conectan a un servicio DHA que se ejecuta en modo de validación EKCert no tienen acceso directo a Internet.
- **AIKCert:** El modo de validación AIKCert está optimizado para entornos operativos que sí tienen acceso a Internet. Los dispositivos que se conectan a un servicio DHA que se ejecuta en modo de validación AIKCert deben tener acceso directo a Internet y pueden obtener un certificado AIK de Microsoft.

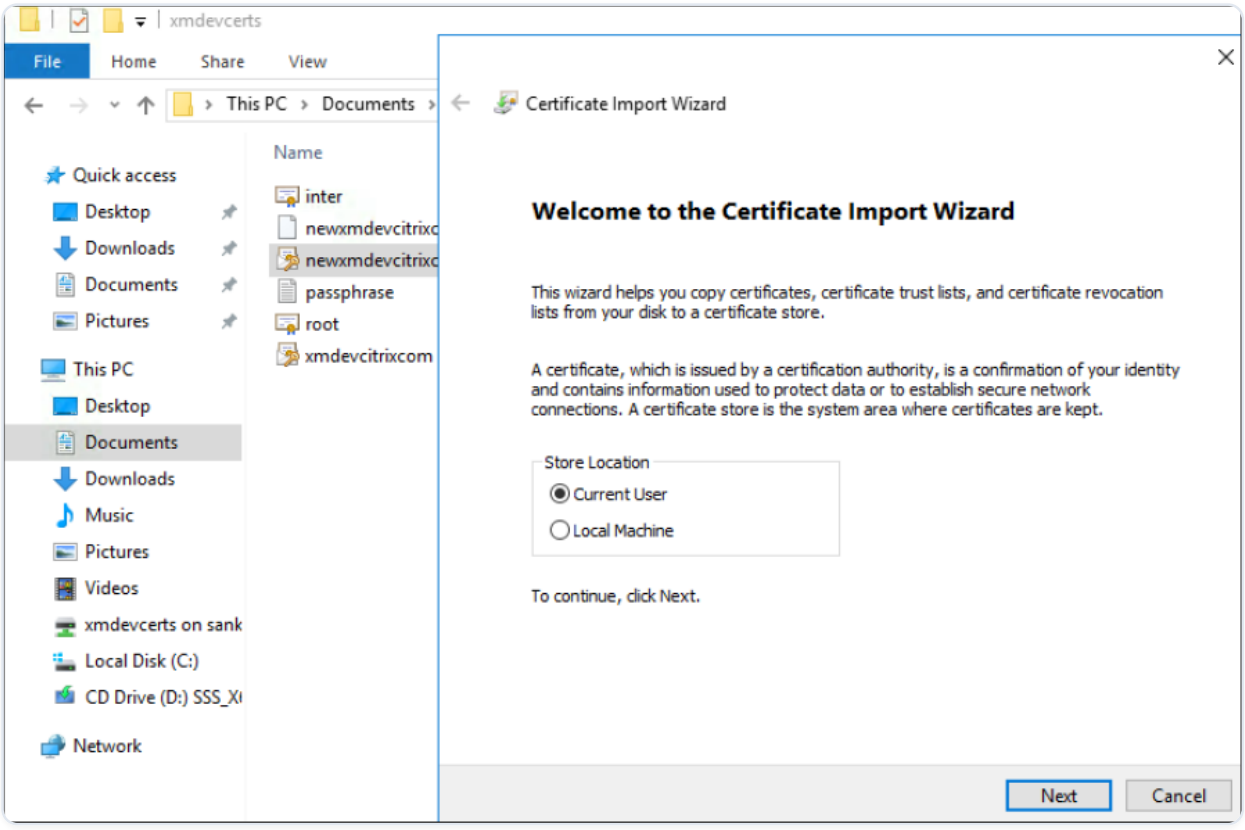
Agregar el rol de servidor DHA al servidor Windows

1. En el servidor Windows, si el Administrador del servidor no está abierto, haga clic en **Inicio** y, a continuación, en **Administrador del servidor**.
2. Haga clic en **Agregar roles y características**.
3. En la página **Antes de empezar**, haga clic en **Siguiente**.
4. En la página **Seleccionar tipo de instalación**, haga clic en **Instalación basada en roles o en características** y, a continuación, en **Siguiente**.
5. En la página **Seleccionar servidor de destino**, haga clic en **Seleccionar un servidor del grupo de servidores**, seleccione el servidor y, a continuación, haga clic en **Siguiente**.
6. En la página **Seleccionar roles de servidor**, seleccione la casilla **Atestación de estado del dispositivo**.
7. Opcional: Haga clic en **Agregar características** para instalar otros servicios de rol y características necesarios.
8. Haga clic en **Siguiente**.
9. En la página **Seleccionar características**, haga clic en **Siguiente**.
10. En la página **Rol de servidor web (IIS)**, haga clic en **Siguiente**.
11. En la página **Seleccionar servicios de rol**, haga clic en **Siguiente**.
12. En la página **Servicio de atestación de estado del dispositivo**, haga clic en **Siguiente**.
13. En la página **Confirmar selecciones de instalación**, haga clic en **Instalar**.
14. Cuando la instalación haya finalizado, haga clic en **Cerrar**.

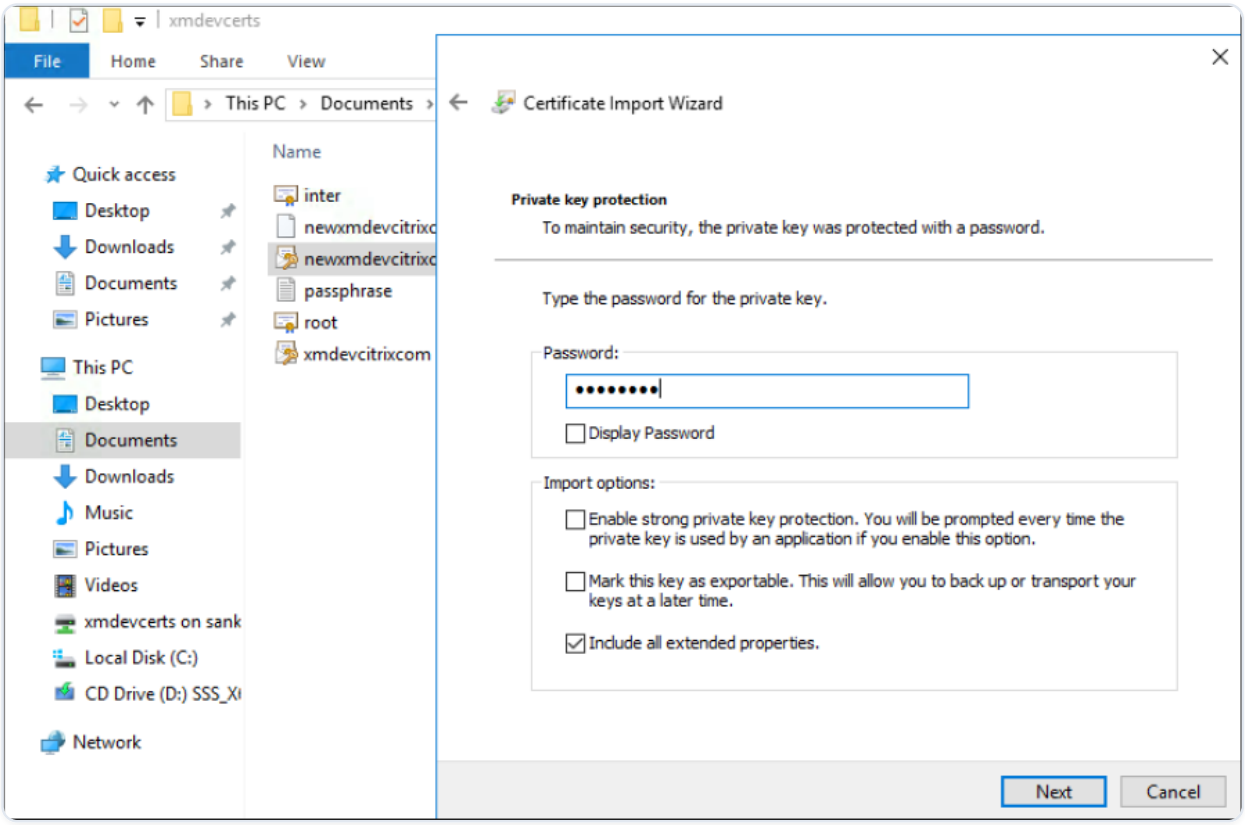
Añadir el certificado SSL al almacén de certificados del servidor

1. Vaya al archivo del certificado SSL y selecciónelo.

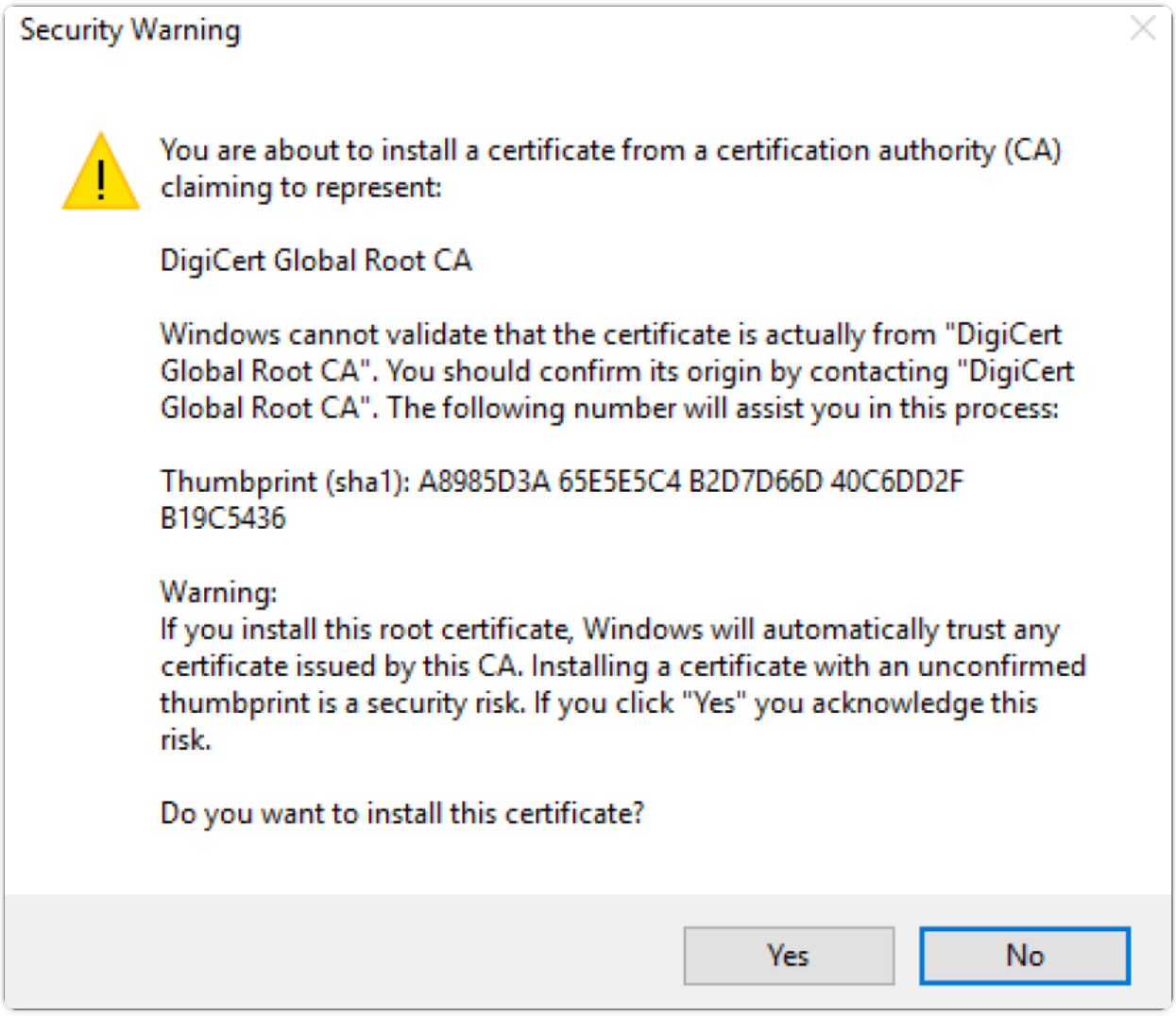
2. Para la ubicación del almacén, seleccione **Usuario actual** y, a continuación, haga clic en **Siguiente**.



3. Escriba la contraseña de la clave privada.
4. Asegúrese de que la opción de importación **Incluir todas las propiedades extendidas** esté seleccionada. Haga clic en **Siguiente**.



5. Cuando aparezca esta ventana, haga clic en **Sí**.



6. Confirme que el certificado está instalado:

   a. Abra una ventana del símbolo del sistema.

   b. Escriba `mmc` y pulse la tecla **Intro**. Para ver los certificados en el almacén de la máquina local, debe tener el rol de administrador.

   c. En el menú Archivo, haga clic en **Agregar o quitar complemento**.

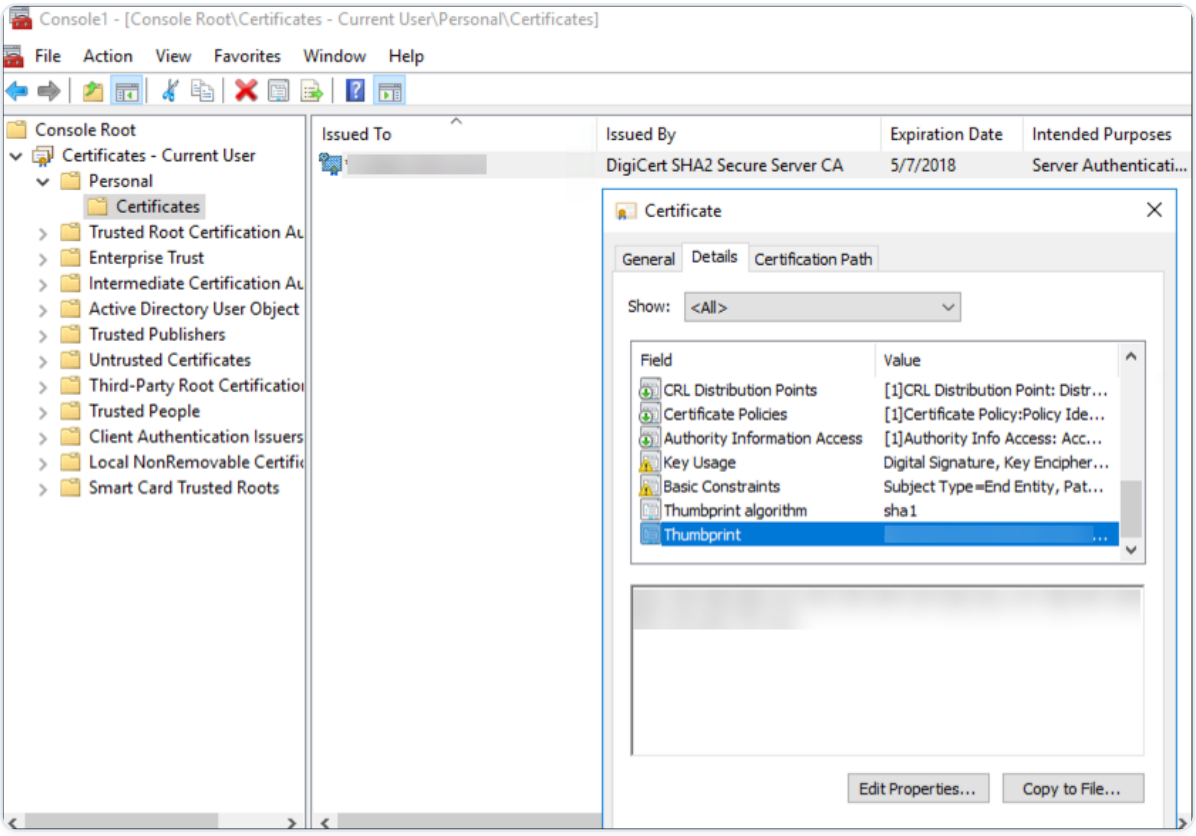
   d. Haga clic en **Agregar**.

   e. En el cuadro de diálogo Agregar complemento independiente, seleccione **Certificados**.

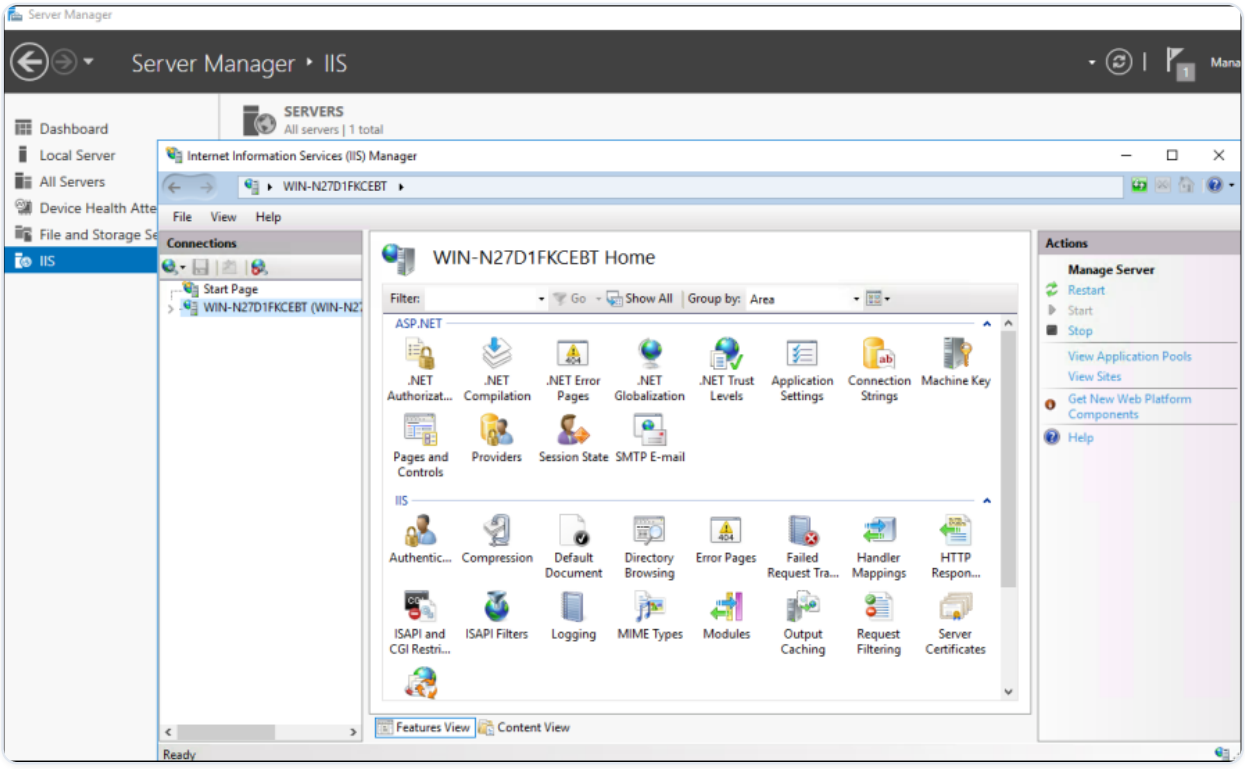
   f. Haga clic en **Agregar**.

   g. En el cuadro de diálogo del complemento Certificados, seleccione **Mi cuenta de usuario**. (Si ha iniciado sesión como titular de una cuenta de servicio, seleccione **Cuenta de servicio**.)

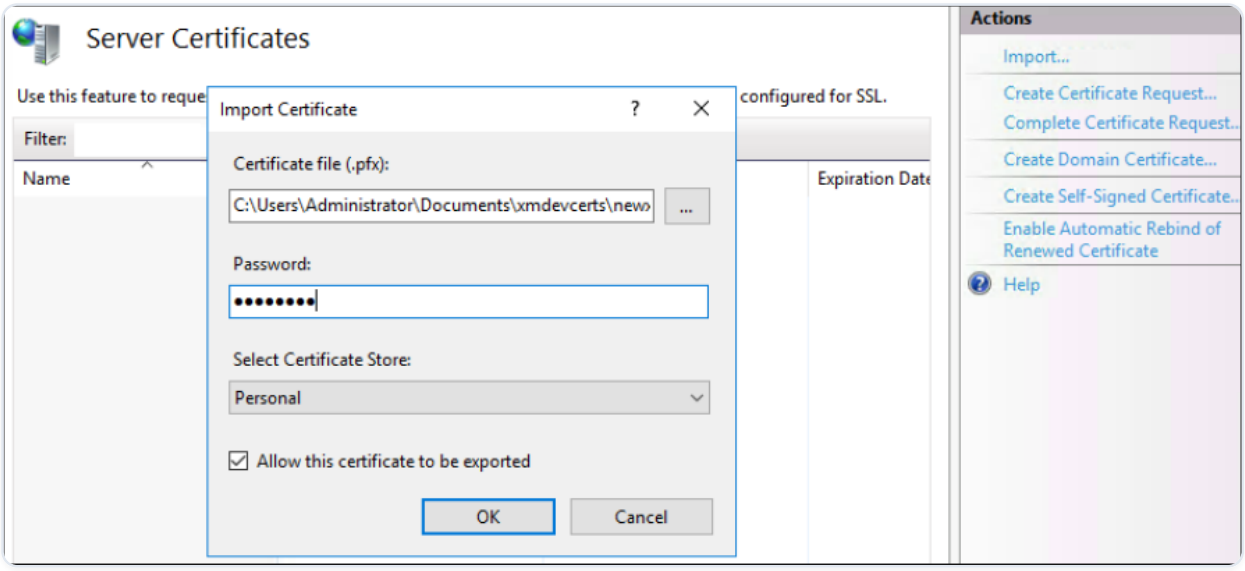
   h. En el cuadro de diálogo Seleccionar equipo, haga clic en **Finalizar**.



7. Vaya a **Administrador del servidor > IIS** y seleccione **Certificados de servidor** de la lista de iconos.

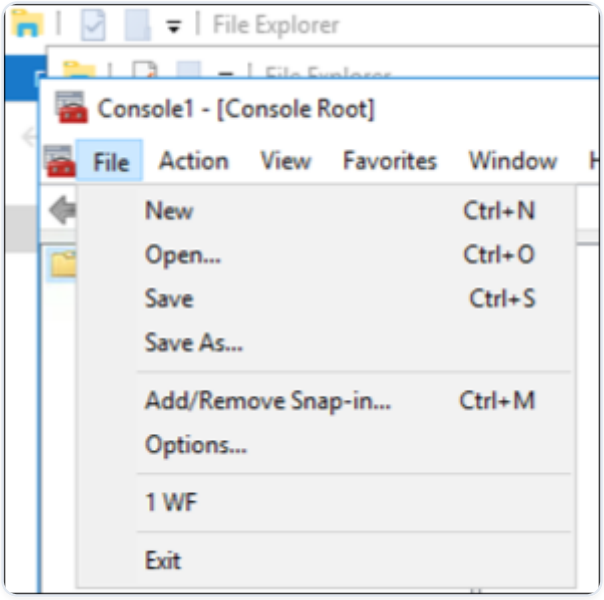


8. En el menú Acción, seleccione **Importar...** para importar el certificado SSL.

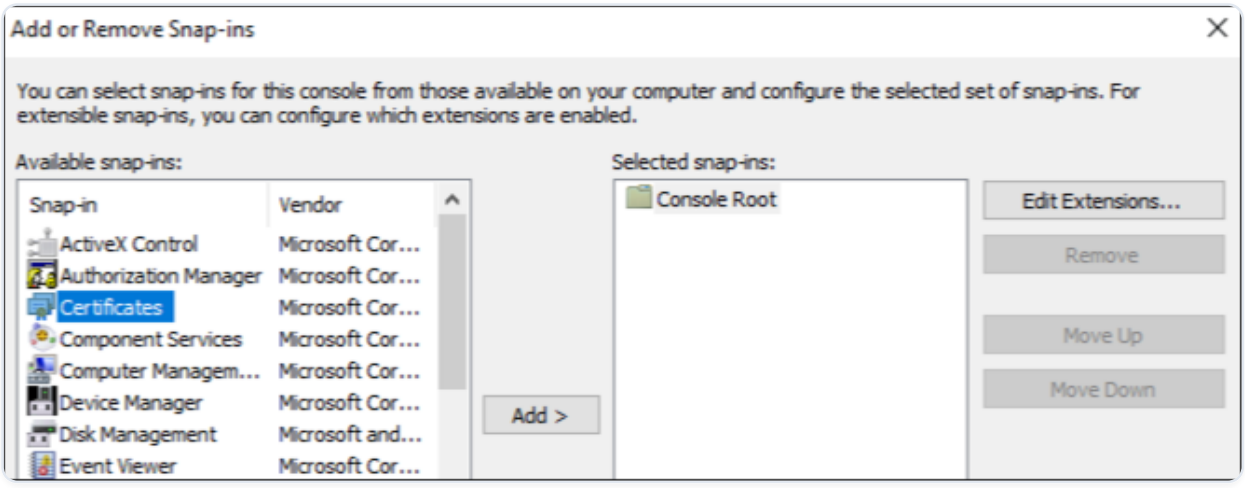


Recuperar y guardar la huella digital del certificado

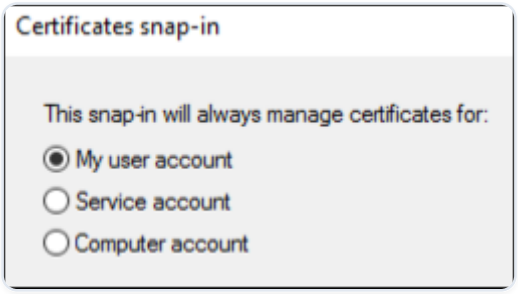
1. En la barra de búsqueda del Explorador de archivos, escriba `mmc`.
2. En la ventana Raíz de la consola, haga clic en **Archivo > Agregar o quitar complemento**.



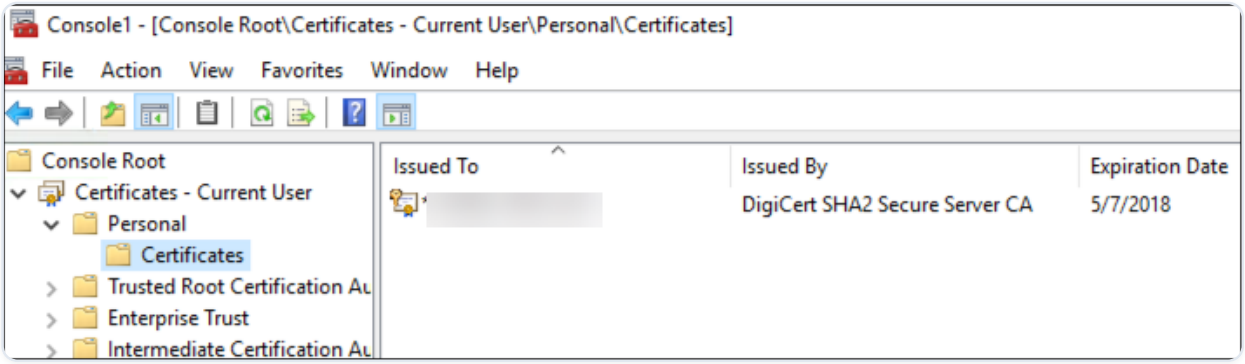
3. Seleccione el certificado de un complemento disponible y agréguelo a los complementos seleccionados.



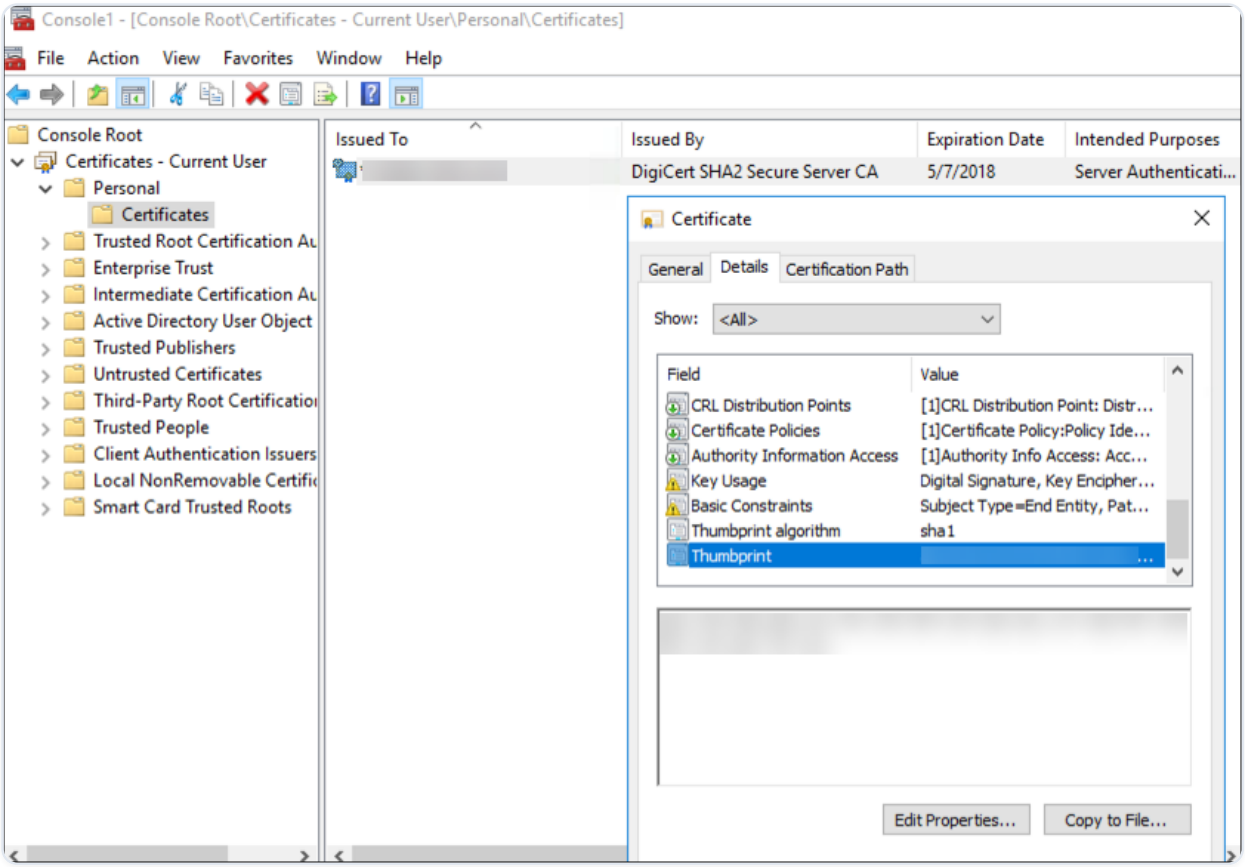
4. Seleccione **Mi cuenta de usuario**.



5. Seleccione el certificado y haga clic en **Aceptar**.



6. Haga doble clic en el certificado y seleccione la ficha **Detalles**. Desplácese hacia abajo para ver la huella digital del certificado.



7. Copie la huella digital en un archivo. Elimine los espacios al usar la huella digital en los comandos de PowerShell.

Instalar los certificados de firma y cifrado

Ejecute estos comandos de PowerShell en el servidor Windows para instalar los certificados de firma y cifrado.

Sustituya el marcador de posición ReplaceWithThumbprint y enciérrelo entre comillas dobles, tal como se muestra.

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.Thumbprint
-like "ReplaceWithThumbprint"}



$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName



$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys\" +
$keyname icacls $keypath /grant IIS_IUSRS`:R
```

```
```

Extraer el certificado raíz de TPM e instalar el paquete de certificados de confianza

Ejecute estos comandos en el servidor Windows:

```
mkdir .\TrustedTpm



expand -F:\* .\TrustedTpm.cab .\TrustedTpm



cd .\TrustedTpm



.\setup.cmd
```

Configurar el servicio DHA

Ejecute este comando en el servidor Windows para configurar el servicio DHA.

Sustituya el marcador de posición ReplaceWithThumbprint.

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
ReplaceWithThumbprint



-SigningCertificateThumbprint ReplaceWithThumbprint



-SslCertificateStoreName My -SslCertificateThumbprint
ReplaceWithThumbprint
```

```
-SupportedAuthenticationSchema "AikCertificate"
```

Ejecute estos comandos en el servidor Windows para configurar la directiva de cadena de certificados para el servicio DHA:

```
$policy = Get-DHASCertificateChainPolicy



$policy.RevocationMode = "NoCheck"



Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

Responda a estas indicaciones de la siguiente manera:

```
  Confirm



    Are you sure you want to perform this action?



    Performing the operation "Install-DeviceHealthAttestation" on target
"[Machine Name]".



    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"): A



    Adding SSL binding to website 'Default Web Site'.



    Add SSL binding?
```

```
    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.

    Add application pool?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding web application 'DeviceHealthAttestation' to website 'Default
Web Site'.

    Add web application?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y

    Adding firewall rule 'Device Health Attestation Service' to allow
inbound connections on port(s) '443'.

    Add firewall rule?

    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

```
    Setting initial configuration for Device Health Attestation Service.


    Set initial configuration?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Registering User Access Logging.


    Register User Access Logging?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
```

Comprobar la configuración

Para comprobar si el DHASActiveSigningCertificate está activo, ejecute este comando en el servidor:

`Get-DHASActiveSigningCertificate`

Si el certificado está activo, se muestran el tipo de certificado (Firma) y la huella digital.

Para comprobar si el DHASActiveSigningCertificate está activo, ejecute estos comandos en el servidor:

Sustituya el marcador de posición ReplaceWithThumbprint y enciérrelo entre comillas dobles, como se muestra.

```
Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
-Force
```

```
Get-DHASActiveEncryptionCertificate
```

Si el certificado está activo, aparece la huella digital.

Para realizar una comprobación final, vaya a esta URL:

`https://<dha.myserver.com>/DeviceHeathAttestation/ValidateHealthCertificate/v1`

Si el servicio DHA se está ejecutando, aparece “Method not allowed” (Método no permitido).



Historial de documentos de Citrix Endpoint Management

En la tabla siguiente se describen cambios importantes en la documentación de producto de Citrix Endpoint Management. Para recibir notificaciones sobre estas actualizaciones, suscríbase al feed RSS.

FECHA	CAMBIO	DESCRIPCIÓN
05 May 2025	Se actualizaron artículos para la versión 25.5.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 25.5.0.
26 Feb 2025	Se actualizaron artículos para la versión 25.3.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 25.3.0.
13 Jan 2025	Se actualizaron artículos para la versión 25.1.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 25.1.0.
21 Nov 2024	Se actualizaron artículos para la versión 24.10.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 24.10.0.
09 Aug 2024	Se actualizaron artículos para la versión 24.8.0 de Citrix Endpoint Management	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix

FECHA	CAMBIO	DESCRIPCIÓN
		Endpoint Management 24.8.0.
03 Jun 2024	Se actualizaron artículos para la versión 24.6.0 de Citrix Endpoint Management	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 24.6.0.
16 Apr 2024	Se actualizaron artículos para la versión 24.4.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 24.4.0.
07 Feb 2024	Se actualizaron artículos para la versión 24.1.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 24.1.0.
06 Dec 2023	Se actualizaron artículos para la versión 23.12.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 23.12.0.
04 Dec 2023	Revierta a la versión 23.9.0 de Citrix Endpoint Management.	Para obtener más información, consulte Citrix Endpoint Management 23.9.0.
11 Oct 2023	Se actualizaron artículos para la versión 23.9.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 23.9.0.
22 Sep 2023	Se eliminaron las referencias relacionadas con Citrix	Se retiró la compatibilidad con Citrix Endpoint Management Government.

FECHA	CAMBIO	DESCRIPCIÓN
	Endpoint Management Government	
22 Aug 2023	Se quitaron los artículos y referencias relacionados con ChromeOS y tvOS	Elementos eliminados y obsoletos: ChromeOS y tvOS.
28 Jul 2023	Se actualizaron artículos para la versión 23.7.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 23.7.0.
20 Jul 2023	Se eliminaron el artículo y las referencias relacionadas con Microsoft Store para Empresas	Microsoft Store para Empresas dejará de ser compatible. Microsoft ya no desarrolla esta plataforma. Para obtener más información, consulte la documentación de Microsoft.
14 Jun 2023	Se actualizaron artículos para la versión 23.6.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 23.6.0.
08 May 2023	Se actualizaron artículos para la versión 23.4.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 23.4.0.
13 Mar 2023	Se actualizaron artículos para la versión 23.2.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 23.2.0.

FECHA	CAMBIO	DESCRIPCIÓN
23 Jan 2023	Se actualizaron artículos para la versión 23.1.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 23.1.0.
13 Dec 2022	Se actualizaron artículos para la versión 22.12.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 22.12.0.
01 Nov 2022	Se actualizaron artículos para la versión 22.10.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 22.10.0.
14 Sep 2022	Se actualizaron artículos para la versión 22.9.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 22.9.0.
11 Aug 2022	Se actualizaron artículos para la versión 22.7.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 22.7.0.
06 Jun 2022	Se actualizaron artículos para la versión 22.6.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 22.6.0.
02 May 2022	Se actualizaron artículos para la versión 22.5.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 22.5.0.

FECHA	CAMBIO	DESCRIPCIÓN
28 Mar 2022	Se actualizaron artículos para la versión 22.4.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 22.4.0.
01 Mar 2022	Se actualizaron artículos para la versión 22.3.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 22.3.0.
07 Feb 2022	Se actualizaron artículos para la versión 22.2.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 22.2.0.
06 Jan 2022	Se actualizaron artículos para la versión 22.1.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 22.1.0.
30 Nov 2021	Se actualizaron artículos para la versión 21.12.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.12.0.
05 Nov 2021	Se actualizaron artículos para la versión 21.11.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.11.0.
22 Oct 2021	Se actualizaron artículos para la versión 21.10.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.10.1.

FECHA	CAMBIO	DESCRIPCIÓN
21 Oct 2021	Se anunció la retirada de la restricción Permitir conexión automática a hotspots del Sensor Wi-Fi para dispositivos con Windows 10.	Para obtener información, consulte Elementos retirados y la documentación de Microsoft.
05 Oct 2021	Se actualizaron artículos para la versión 21.10.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.10.0.
24 Sep 2021	Se anunció una versión Technical Preview pública para la autenticación de proveedores de identidades sin Cloud Connector.	Para obtener más información sobre esta función, consulte Autenticación de proveedores de identidades.
15 Sep 2021	Se actualizaron artículos para la versión 21.9.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.9.1.
06 Sep 2021	Se actualizaron artículos para la versión 21.9.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.9.0.
18 Aug 2021	Se actualizaron artículos para la versión 21.8.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.8.0..
22 Jul 2021	Se actualizaron artículos para la versión 21.7.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.7.1.

FECHA	CAMBIO	DESCRIPCIÓN
09 Jul 2021	Se anunció la retirada del uso del modo de inscripción Alta seguridad y la configuración de invitación de inscripción en Self Help Portal.	Para obtener información, consulte Elementos retirados.
06 Jul 2021	Se actualizaron artículos para la versión 21.7.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.7.0.
23 Jun 2021	La plataforma Android para Workspace está disponible en versión Technical Preview pública. Una vez configurado Android para Workspace, los usuarios pueden inscribirse en Citrix Endpoint Management mediante la aplicación Citrix Workspace.	Para obtener más información, consulte Android para Workspace.
14 Jun 2021	Se actualizaron artículos para la versión 21.6.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.6.0.
24 May 2021	Se actualizaron artículos para la versión 21.5.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.5.1.
11 May 2021	Fecha actualizada de la retirada de los dispositivos compartidos MDX	Para obtener más información, consulte Elementos retirados.
06 May 2021	Se actualizaron artículos para la versión 21.5.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix

FECHA	CAMBIO	DESCRIPCIÓN
		Endpoint Management 21.5.0.
03 May 2021	Se agregó documentación sobre el problema conocido CXM-89333.	Para obtener información, consulte Problemas conocidos en Citrix Endpoint Management 21.4.0.
26 Apr 2021	Descripción actualizada de la acción de seguridad Localizar	Consulte Acciones de seguridad.
22 Apr 2021	Se agregó un ejemplo de acción.	Consulte Acciones automatizadas.
21 Apr 2021	Se anunció la retirada de la función que usaba un IMEI de dispositivo o un número de serie para generar una URL de invitación.	Para obtener información, consulte Elementos retirados.
20 Apr 2021	Se agregó la integración en el acceso de condicional de Azure AD.	Para obtener información, consulte Integración en el acceso condicional de Azure AD (Technical Preview).
15 Apr 2021	Se agregó un artículo sobre iPads compartidos.	Consulte iPads compartidos.
13 Apr 2021	Se actualizaron artículos para la versión 21.4.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.4.0.
31 Mar 2021	Se agregó una descripción de los requisitos de la VPN por aplicación.	Consulte Directiva de VPN y Directiva de configuraciones administradas.
09 Mar 2021	Se actualizaron artículos para la versión 21.3.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix

FECHA	CAMBIO	DESCRIPCIÓN
		Endpoint Management 21.3.0.
09 Mar 2021	Se agregó el anuncio sobre la migración de los registros del servicio de detección automática	Consulte Migración de los registros del servicio de detección automática.
24 Feb 2021	Se agregó un anuncio sobre la preparación necesaria antes de actualizar la versión de los dispositivos de punto final a iOS 14.5.	Consulte Antes de actualizar la versión de los dispositivos de punto final a iOS 14.5.
12 Feb 2021	Se actualizaron artículos para la versión 21.2.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.2.0.
25 Jan 2021	Se actualizaron artículos para la versión 21.1.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.1.1.
06 Jan 2021	Se actualizaron artículos para la versión 21.1.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 21.1.0.
09 Dec 2020	Se agregó contenido de vista previa acerca de la inscripción de dispositivos Android Enterprise con Azure Active Directory y Okta como plataformas de identidad.	Para obtener más información detallada sobre los cambios, consulte Citrix Endpoint Management 20.12.0.

FECHA	CAMBIO	DESCRIPCIÓN
04 Dec 2020	Se actualizaron artículos para la versión 20.12.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.12.0.
10 Nov 2020	Se agregó una tabla de varias comprobaciones de conectividad que puede realizar Citrix Endpoint Management.	Consulte Detalles de comprobación de la conectividad.
06 Nov 2020	Se actualizaron artículos para la versión 20.11.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.11.0.
28 Oct 2020	Se agregó una solución temporal necesaria si se actualiza a la versión más reciente de Citrix ADC.	Consulte Antes de actualizar la versión de un Citrix ADC local a 13.0-64.35 o una versión posterior.
23 Oct 2020	Se actualizaron artículos para la versión 20.10.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.10.1.
22 Oct 2020	Se agregó un flujo de trabajo de alto nivel para la configuración de Android Enterprise.	Consulte Introducción a Android Enterprise.
22 Oct 2020	Se agregó un artículo en el que se detallan los diferentes métodos de distribuir aplicaciones de Android Enterprise.	Consulte Distribuir aplicaciones de Android Enterprise y Android para Workspace.

FECHA	CAMBIO	DESCRIPCIÓN
07 Oct 2020	Se actualizaron artículos para la versión 20.10.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.10.0.
22 Sep 2020	Se actualizaron artículos para la versión 20.9.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.9.1.
04 Sep 2020	Se actualizaron artículos para la versión 20.9.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.9.0.
20 Aug 2020	Se actualizaron artículos para la versión 20.8.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.8.0.
14 Aug 2020	Se agregó una descripción de la simplificación del proceso de inscripción para la inscripción en bloque de dispositivos Windows de forma inmediata.	Consulte Inscripción en bloque de dispositivos de forma inmediata.
31 Jul 2020	Se actualizó el artículo sobre inscripción en bloque de dispositivos Windows.	Consulte Inscribir dispositivos Windows en bloque.
23 Jul 2020	Se actualizaron artículos para la versión 20.7.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.7.1.

FECHA	CAMBIO	DESCRIPCIÓN
10 Jul 2020	Se actualizaron artículos para la versión 20.7.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.7.0.
02 Jul 2020	Se agregó una línea de tiempo y un plan de acción para la retirada del cifrado MDX.	Consulte Preparar los dispositivos Android para cambios futuros.
25 Jun 2020	Se actualizaron artículos para la versión 20.6.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.6.0.
19 Jun 2020	Se modificaron los términos "lista negra" y "lista blanca" en la documentación. Se cambiaron a "lista de bloqueados" y "lista de permitidos".	La consola de Citrix Endpoint Management actualmente contiene los términos "lista negra" y "lista blanca". Hemos actualizado la documentación. Estamos en proceso de cambiar los términos en la consola del producto para una próxima versión.
18 Jun 2020	Se anunció la retirada del contenedor Samsung SEAMS.	Consulte Elementos retirados.
09 Jun 2020	Se agregó una tabla de los niveles funcionales de bosque y dominio que Citrix Cloud Connector permite usar con Citrix Endpoint Management.	Consulte Niveles funcionales admitidos de Active Directory.

FECHA	CAMBIO	DESCRIPCIÓN
05 Jun 2020	Se agregó un artículo que proporciona resultados de las pruebas de carga de Citrix Cloud Connector para las inscripciones de dispositivos Android e iOS.	Consulte Consideraciones de escala y tamaño para los Cloud Connectors.
02 Jun 2020	Se actualizaron artículos para la versión 20.5.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.5.0.
27 May 2020	Se amplió contenido al publicar aplicaciones administradas de Intune. Se quitó contenido relacionado con el empaquetado de aplicaciones de terceros.	Consulte Integración de Citrix Endpoint Management en Microsoft Endpoint Manager.
13 May 2020	Se amplió la información sobre los roles y permisos de usuario de Citrix Endpoint Management	Consulte Usar la función RBAC.
05 May 2020	Se actualizaron artículos para la versión 20.4.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.4.1.
04 May 2020	Se agregó una nota sobre los nuevos requisitos de los certificados TLS para los certificados de confianza en iOS, iPadOS y macOS	Consulte Certificados.
30 Apr 2020	Se agregó contenido de vista previa sobre el uso de Azure Active Directory para la autenticación	Consulte Autenticación con Azure Active Directory a través de Citrix Cloud.

FECHA	CAMBIO	DESCRIPCIÓN
29 Apr 2020	Se agregó documentación de la versión Technical Preview sobre la compatibilidad de Citrix Endpoint Management con la autenticación con credenciales de Okta	Consulte Autenticación con Okta a través de Citrix Cloud.
13 Apr 2020	Se actualizaron artículos para la versión 20.4.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.4.0.
26 Mar 2020	Se actualizaron artículos para la versión 20.3.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.3.0.
20 Mar 2020	Se agregó un artículo que detalla los pasos para distribuir diferentes tipos de aplicaciones iOS.	Consulte Distribuir aplicaciones de Apple.
13 Mar 2020	Se agregó una sección sobre la protección de dispositivos móviles empresariales contra ciberataques avanzados.	Consulte Integración en el software Mobile Threat Defense.
13 Feb 2020	Se actualizaron artículos para la versión 20.2.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.2.1.
08 Jan 2020	Se actualizaron artículos para la versión 20.1.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 20.1.0.

FECHA	CAMBIO	DESCRIPCIÓN
03 Dec 2019	Se actualizaron artículos para la versión 19.12.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.12.0.
08 Nov 2019	Se actualizaron artículos para la versión 19.11.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.11.0.
16 Oct 2019	Se actualizaron artículos para la versión 19.10.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.10.0.
16 Oct 2019	Se agregó una sección sobre la transición de Google a Android Enterprise.	Consulte Crear perfiles de inscripción.
25 Sep 2019	Se actualizaron artículos para la versión 19.9.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.9.1.
10 Sep 2019	Se actualizaron artículos para la versión 19.9.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.9.0.
08 Aug 2019	Se actualizaron artículos para la versión 19.8.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.8.0.

FECHA	CAMBIO	DESCRIPCIÓN
07 Aug 2019	Se actualizó un artículo de Android Enterprise para aclarar los conceptos de Android Enterprise. Se agregaron recomendaciones al artículo sobre la migración a Android Enterprise.	Consulte Android Enterprise y Migrar de la administración de dispositivos a Android Enterprise.
31 Jul 2019	Se agregó el artículo sobre la migración desde la administración de dispositivos antiguos de Android a Android Enterprise.	Consulte Migrar de la administración de dispositivos a Android Enterprise.
16 Jul 2019	Se actualizaron artículos para la versión 19.7.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.7.1.
27 Jun 2019	Se actualizaron artículos para la versión 19.6.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.6.1.
06 Jun 2019	Se actualizaron artículos para la versión 19.6.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.6.0.
24 May 2019	Se actualizó la terminología de Android Enterprise para que coincida con la documentación actual de Google Android Enterprise.	Se actualizó el artículo Android Enterprise.
20 May 2019	Nueva sección sobre la compatibilidad con SSO para dispositivos móviles en	Se agregó una sección al artículo "Agregar aplicaciones" sobre cómo

FECHA	CAMBIO	DESCRIPCIÓN
	aplicaciones SaaS nativas desde dispositivos iOS y Android.	configurar SSO para dispositivos móviles.
20 May 2019	Nueva sección sobre la integración de Citrix Gateway Service en Citrix Endpoint Management.	La versión Technical Preview de Citrix Gateway Service está disponible para los clientes que tengan habilitado Workspace y una suscripción a Citrix Gateway Service. Se agregó una sección al artículo "Incorporarse como usuario y configurar recursos": Configurar el uso de Citrix Gateway con Citrix Endpoint Management.
10 May 2019	Nueva sección sobre Entrust PKI.	Se agregó una sección al artículo Entidades de PKI sobre Entrust PKI.
09 May 2019	Se actualizaron artículos para la versión 19.5.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.5.0.
01 May 2019	Nueva sección sobre cómo configurar redes VPN para Android Enterprise: Cree una directiva de dispositivo de configuración administrada para la aplicación Citrix SSO.	Se agregó una sección al artículo "Directiva de configuraciones administradas": Configurar perfiles de VPN para Android Enterprise.
17 Apr 2019	Se actualizaron artículos para la versión 19.4.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.4.1.

FECHA	CAMBIO	DESCRIPCIÓN
04 Apr 2019	Nueva sección sobre la activación automática.	Se agregó una sección al artículo "Android Enterprise": Activación automática.
02 Apr 2019	Se actualizaron artículos para el Conector de Gateway para la versión 8.5.3 de Exchange ActiveSync.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Novedades en la versión 8.5.3.
02 Apr 2019	Nuevos problemas resueltos en la versión 19.3.1 de Citrix Endpoint Management.	Para obtener información, consulte Problemas resueltos en Citrix Endpoint Management 19.3.1.
26 Mar 2019	Se actualizó la sección FCM con pasos sobre la actualización de versiones.	Para obtener información detallada sobre FCM, consulte Firebase Cloud Messaging.
26 Mar 2019	Se actualizó la sintaxis de nombres de almacenes Citrix Secure Hub.	Se agregó una nota sobre el requisito alfanumérico del nombre de almacén en Personalizar la marca en el almacén de aplicaciones y Citrix Secure Hub.
11 Mar 2019	Se actualizaron artículos para la versión 19.3.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.3.0.
22 Feb 2019	Se actualizaron artículos para la versión 19.2.1 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.2.1.

FECHA	CAMBIO	DESCRIPCIÓN
11 Feb 2019	Se actualizaron artículos para la versión 19.2.0 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.2.0.
25 Jan 2019	Se actualizaron artículos para la versión 19.1.2 de Citrix Endpoint Management.	Para obtener un resumen de las funciones nuevas y modificadas, consulte Citrix Endpoint Management 19.1.2.