



Citrix Endpoint Management

Contents

Citrix Endpoint Management	9
Novedades	14
Avisos legales de terceros	21
Elementos retirados	21
Requisitos del sistema	37
Compatibilidad de Citrix Endpoint Management	51
Sistemas operativos compatibles para los dispositivos	52
Compatibilidad con los siguientes idiomas	54
Cumplimiento del estándar FIPS 140-2	56
Acerca de Citrix Endpoint Management	57
Integración de Citrix Endpoint Management con Microsoft Endpoint Manager	73
Incorporarse como usuario y configurar recursos	91
Consideraciones de escala y tamaño para los Cloud Connectors	103
Preparar la inscripción de dispositivos y la entrega de recursos	104
Certificados y autenticación	121
Cargar, actualizar y renovar certificados	126
NetScaler Gateway y Citrix Endpoint Management	139
Disponibilidad de la autenticación con dominio o dominio y token de seguridad	151
Autenticación con certificado de cliente o certificado y dominio	157
Entidades de PKI	180
Proveedores de credenciales	199
Certificados APNs	207
SAML para Single Sign-On en Citrix Files	217

Autenticación con Azure Active Directory a través de Citrix Cloud	228
Autenticación con Azure Active Directory a través de NetScaler Gateway para la inscripción de MAM	232
Autenticación con Okta a través de Citrix Cloud	236
Autenticación con Okta a través de NetScaler Gateway para la inscripción de MAM	239
Autenticación con un dispositivo NetScaler Gateway local a través de Citrix Cloud	248
Autenticación nFactor	251
Inscripción, roles y cuentas de usuario	254
Perfiles de inscripción	272
Notificaciones	278
Configurar roles con RBAC	285
Licencias	307
Administración de dispositivos	307
Alexa for Business	338
Migrar de la administración de dispositivos a Android Enterprise	352
Android Enterprise	358
Distribuir aplicaciones de Android Enterprise	413
Android Enterprise heredado para clientes de Google Workspace (anteriormente G Suite)	441
Sistema operativo Android	480
Firebase Cloud Messaging	487
Android SafetyNet	492
API Play Integrity	497
Samsung	500
Control de acceso de red	502

iOS	509
macOS	527
Implementar dispositivos mediante los Programas de implementación de Apple	534
Inscribir dispositivos Apple en bloque	551
Integración en funciones de Apple Educación	558
iPads compartidos	575
Distribuir aplicaciones de Apple	587
Control de acceso de red	618
Tableta y escritorio Windows	625
Inscribir dispositivos Windows en bloque	635
Directivas de dispositivo	640
Directiva de duplicación AirPlay	669
Directiva de AirPrint	672
Directiva de permisos de aplicación	673
Directiva de APN	675
Directiva de acceso a aplicaciones	678
Directiva de atributos de aplicación	680
Directiva de configuración de aplicaciones	682
Directiva de inventario de aplicaciones	685
Directiva de protección de aplicaciones	687
Directiva de bloqueo de aplicaciones	689
Directiva de notificaciones de aplicaciones	694
Directiva de desinstalación de aplicaciones	696
Directiva de restricciones de desinstalación de aplicaciones	698

Directiva de dispositivo para actualizar automáticamente aplicaciones administradas	699
Directiva de BitLocker	700
Directiva de dispositivos Bluetooth	707
Directiva de calendario (CalDAV)	708
Directiva de red de telefonía móvil	710
Directiva de programación de conexiones	711
Directiva de contactos (CardDAV)	713
Directiva de XML personalizado	715
Directiva de Defender	719
Directiva de Device Guard	720
Directiva de Device Health Attestation	721
Directiva de nombre de dispositivo	723
Directiva de configuración de la educación	724
Directiva de opciones de Endpoint Management	727
Directiva de desinstalación de Citrix Endpoint Management	729
Directiva de Exchange	730
Directiva de archivos	736
Directiva de FileVault	738
Directiva de firewall	741
Directiva de fuentes	743
Directiva de diseño de pantalla de inicio	745
Directiva de importación de perfiles de iOS y macOS	747
Directiva de dispositivos de administración de Keyguard	750
Directiva de quiosco	754

Directiva de configuración del Launcher	757
Directiva de LDAP	758
Directiva de localización geográfica	761
Directiva de mensaje de pantalla bloqueada	768
Directiva de correo	769
Directiva de configuraciones administradas	772
Directiva de dominios administrados	785
Directiva de máximo de usuarios residentes	787
Directiva de opciones de MDM	788
Directiva de redes	790
Directiva de uso de red	805
Directiva de Office	806
Directiva de información de la organización	808
Directiva de actualización del SO	808
Directiva de código de acceso	821
Directiva de período de gracia de bloqueo de código de acceso	834
Directiva de hotspot personal	834
Directiva de eliminación de perfiles	835
Directiva de perfil de datos	836
Directiva de eliminación de perfiles de datos	836
Directiva de proxy	837
Directiva de restricciones	839
Directiva de itinerancia	891
Directiva de SCEP	892

Directivas de Siri y dictado	896
Directiva de cuenta SSO	897
Directiva de tiendas	899
Directiva de calendarios suscritos	899
Directiva de términos y condiciones	900
Directiva de túnel	901
Directiva de VPN	903
Directiva de fondo de pantalla	943
Directiva de filtro de contenido web	945
Directiva de clip web	947
Directiva de Agente de Windows	949
Directiva de configuración de GPO de Windows	953
Directiva de Windows Hello para empresas	956
Agregar aplicaciones	958
Tipos de conectores de aplicaciones	1011
Citrix Launcher	1012
Agregar aplicaciones mediante las compras por volumen de Apple	1016
Utilice ShareFile con Citrix Endpoint Management	1024
SmartAccess para aplicaciones HDX	1040
Actualizar la versión de aplicaciones MDX o de empresa	1058
Agregar contenido multimedia	1060
Implementar recursos	1064
Macros	1080
Acciones automatizadas	1117

Supervisar y ofrecer asistencia	1129
Comprobaciones de conectividad	1137
Proveedor de servicios móviles	1143
Informes	1144
API de REST	1154
ActiveSync Gateway	1156
Conector de Citrix Endpoint Management para Exchange ActiveSync	1159
Conector de NetScaler Gateway para Exchange ActiveSync	1210
Conceptos avanzados	1227
Implementar Citrix Endpoint Management	1227
Modos de administración	1229
Requisitos de dispositivo	1233
Seguridad y experiencia del usuario	1234
Aplicaciones	1253
Comunidades de usuarios	1261
Estrategia de correo electrónico	1269
Integrar Citrix Endpoint Management	1278
Integración en NetScaler Gateway y Citrix ADC	1286
Consideraciones sobre SSO y proxies para aplicaciones MDX	1293
Autenticación	1298
Propiedades de servidor	1314
Directivas de aplicación y de dispositivo	1330
Propiedades de cliente	1342
Opciones de inscripción de usuarios	1355

Aprovisionar y desaprovisionar aplicaciones	1359
Operaciones del panel de mandos	1362
Control de acceso basado en roles y asistencia de Citrix Endpoint Management	1364
Proceso de asistencia de Citrix	1366
Enviar invitaciones de inscripción a grupos en Citrix Endpoint Management	1367
Configurar la autenticación por certificado en EWS para notificaciones push de Citrix Secure Mail	1369
Configurar un servidor Device Health Attestation local	1373

Citrix Endpoint Management

March 1, 2024

Citrix Endpoint Management es una solución para gestionar terminales que ofrece capacidades de Administración de dispositivos móviles (MDM) y de administración de aplicaciones móviles (MAM). Con Citrix Endpoint Management, puede gestionar directivas de dispositivos y aplicaciones y proporcionar aplicaciones a usuarios. La información de su empresa se mantiene protegida con una seguridad estricta en cuanto a la identidad, los dispositivos, las aplicaciones, los datos y las redes.

Responsabilidades de Citrix y del cliente

El equipo Citrix Cloud Operations gestiona varias tareas de infraestructura y supervisión. Gracias a eso, usted puede centrarse en la experiencia del usuario y en la administración de dispositivos, aplicaciones y directivas.

Responsabilidades de Citrix:

- Nodos del servidor Citrix Endpoint Management
- Integración y configuración iniciales de NetScaler Gateway (servicio o local)
- Equilibrador de carga de NetScaler Gateway
- Base de datos
- Configuración del software de Cloud Connector
- Integración de la autenticación de SAML con ShareFile
- Supervisión de los sitios Citrix Endpoint Management: instancia, base de datos, conectividad de empresa (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 se han instalado Cloud Connectors y Gateway Connector (para Citrix Gateway Service)
- LDAP/Active Directory
- DNS
- ShareFile: configuración inicial de ShareFile, instalación de controladores de zonas de almacenamiento, actualizaciones de Citrix Files
- Configuración de Citrix Endpoint Management: dispositivos, directivas, aplicaciones, acciones, grupos de entrega y certificados de cliente

Integración en Microsoft Endpoint Manager

Citrix Endpoint Management se integra en Microsoft Endpoint Manager (MEM). Esa integración agrega todo el valor de una red micro VPN de Citrix Endpoint Management a las aplicaciones compatibles con Microsoft Intune, como el explorador web Microsoft Edge. Con la integración, puede:

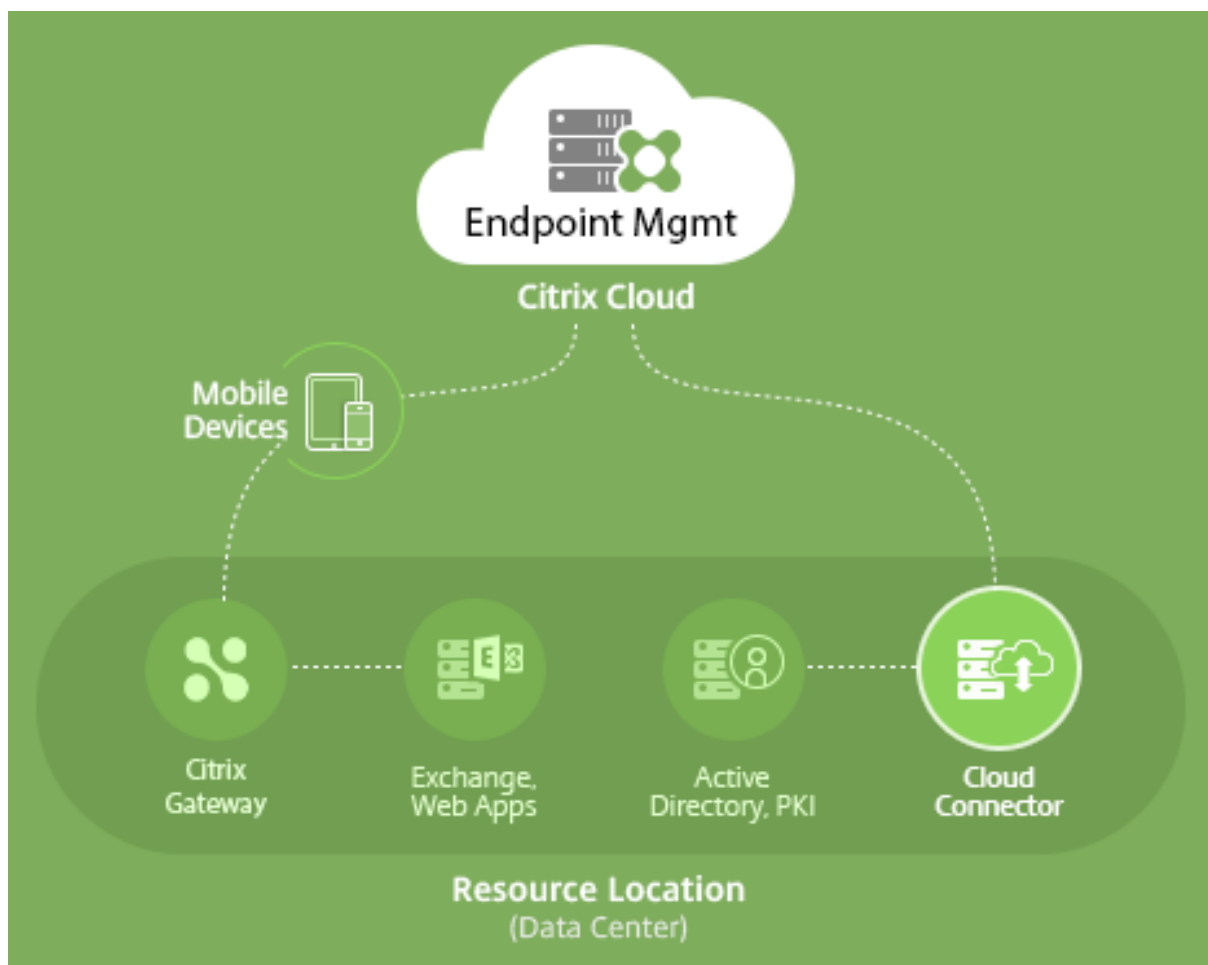
- Aplicaciones seguras de Office 365 con acceso condicional con Azure AD. Para obtener más información, consulte [Integración en el acceso condicional de Azure AD](#).
- Empaquetar sus propias aplicaciones de línea de negocio con Intune y Citrix para ofrecer capacidades micro VPN dentro de un contenedor de administración de aplicaciones móviles (MAM) de Intune.
- Administrar y entregar aplicaciones Office 365, aplicaciones de línea de negocio y Citrix Secure Mail en un solo contenedor. Este método de administración ofrece la máxima seguridad y productividad. Por ejemplo, puede:
 - Bloquear dispositivos o sistemas operativos individuales
 - Personalizar directivas de ActiveSync por dispositivo, usuario o grupo de usuarios
 - Cuarentena al nivel del dispositivo
 - Supervisión conexiones o dispositivos individuales
 - Evitar los riesgos de seguridad del almacenamiento en caché de credenciales y datos

Use MDM+MAM de Citrix Endpoint Management o MDM de Intune para administrar dispositivos. Para obtener más información, consulte [Integración de Citrix Endpoint Management en Microsoft Endpoint Manager](#).

Cloud Connector y ubicaciones de recursos

Puede conectarse a Citrix Endpoint Management a través de Cloud Connector. Cloud Connector actúa como un canal de comunicación entre Citrix Cloud y las ubicaciones de sus recursos. Cloud Connector permite administrar una nube sin necesidad de configurar redes ni infraestructuras complejas (como redes VPN o túneles IPsec).

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



Para obtener más información sobre Cloud Connector y las ubicaciones de recursos, consulte [Acerca de Citrix Endpoint Management](#)

Introducción a Citrix Endpoint Management

Sugerencia:

XenMobile Migration Service

Si utiliza XenMobile Server local, nuestro servicio XenMobile Migration Service puede ayudarle a comenzar a usar el servicio Citrix Endpoint Management. La migración desde XenMobile Server a Citrix Endpoint Management no requiere que vuelva a inscribir los dispositivos.

Para obtener más información, contacte con el representante de ventas, el ingeniero de sistemas o Partner de Citrix local.

Para obtener más información sobre nuestro servicio de migración, consulte [Tres motivos para pasar al servicio Citrix Endpoint Management](#).

Para ver por qué recurrir a migrar a Citrix Endpoint Management, cómo hacerlo y sus ventajas, consulte [CEM Migration Service Course Catalog](#) o la guía [Citrix Endpoint Management \(CEM\) Migration Service](#).

Durante el período de evaluación o adquisición de Citrix Endpoint Management, el equipo de operaciones de Citrix Endpoint Management le ofrece asistencia continua de incorporación al servicio. Ese equipo también se comunica con usted para asegurarse de que los servicios básicos de Citrix Endpoint Management se han configurado y se ejecutan correctamente. En esta imagen se muestran los pasos para incorporarse y empezar a utilizar el servicio.



Si quiere registrarse para una cuenta de Citrix y solicitar una prueba de Citrix Endpoint Management, póngase en contacto con su representante de ventas de Citrix. Cuando tenga todo listo para continuar, vaya a <https://onboarding.cloud.com>.

Para obtener información general sobre cómo empezar a utilizar y configurar Citrix Endpoint Management, vea este corto vídeo.

[Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.](#)

¿Quiere obtener más información antes de comenzar? Consulte estos recursos:

Documentación de Citrix Endpoint Management: Ofrece la documentación completa de Citrix Endpoint Management, desde la incorporación de usuarios hasta la configuración avanzada. En el artículo “Novedades”, se describen las nuevas funciones y correcciones. Citrix le notifica en cuanto está disponible ese artículo para una nueva versión.

Citrix Endpoint Management Onboarding Handbook: Este manual engloba toda la información disponible sobre Citrix Endpoint Management, para que pueda seguir habilitando e incorporando Citrix Endpoint Management sin problemas. Puede usar este documento para registrar cambios en sus procesos internos y documentar diseños funcionales y de alto nivel.

Citrix Endpoint Management Deployment Handbook: La planificación de una implementación de Citrix Endpoint Management implica muchas cuestiones a considerar. El manual contiene recomendaciones, preguntas frecuentes y casos de uso para su entorno de Citrix Endpoint Management.

SalesIQ: Más recursos para nuestros socios de Citrix.

Siguientes pasos

Para obtener información sobre el proceso de incorporación de Citrix Endpoint Management, consulte [Incorporarse como usuario y configurar recursos](#).

Después de la incorporación, consulte [Preparar la inscripción de dispositivos y la entrega de recursos](#).

Anuncios de retirada

Para obtener información avanzada sobre las funciones de Citrix Endpoint Management que se están retirando gradualmente, consulte [Elementos retirados](#).

Asistencia para Citrix Endpoint Management

Para obtener más información sobre cómo obtener acceso a información relacionada y herramientas compatibles en la consola de Citrix Endpoint Management, consulte [Supervisión y asistencia](#).

Las actualizaciones continuas de Citrix Endpoint Management se publican aproximadamente cada dos semanas. Para usted, como cliente, este proceso es transparente. Las actualizaciones iniciales solo se aplican en los sitios internos de Citrix; luego se aplican gradualmente en los entornos de los clientes. Entregamos actualizaciones de manera incremental en fases para ofrecer la calidad de los productos y maximizar su disponibilidad.

Los clientes de Citrix Endpoint Management reciben comunicaciones y actualizaciones directamente de parte del equipo de operaciones en la nube de Citrix Endpoint Management. Esas actualizaciones lo mantienen al día, puesto que recibe así las funciones nuevas, los problemas conocidos y los problemas resueltos, entre otros.

El equipo de Citrix Cloud Operations mantiene los entornos de Citrix Endpoint Management con los parches graduales más recientes de Citrix Endpoint Management. Para obtener parches o correcciones específicas que sean necesarias antes de aplicar el parche gradual, contacte con el servicio de asistencia técnica de Citrix.

Si su entorno presenta problemas, póngase en contacto con el servicio de asistencia técnica de Citrix o el equipo de cuentas de Citrix. Esos problemas pueden ser de la inscripción de dispositivos móviles, el acceso a la consola de Citrix Endpoint Management o problemas de Citrix Secure Mail.

Si necesita que se realicen cambios o integraciones de NetScaler Gateway en Cloud o Citrix Endpoint Management, envíe una solicitud a través de la asistencia técnica de Citrix.

A continuación, se presentan ejemplos de los cambios que puede solicitar:

- Integración de Citrix Files en NetScaler Gateway en la nube

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

Contrato de nivel de servicio

En Citrix Endpoint Management se tienen en cuenta las prácticas recomendadas del sector con el fin de lograr un alto grado de disponibilidad de los servicios y alta escalabilidad de nube.

Para obtener detalles completos sobre el compromiso de Citrix con la disponibilidad de los servicios de Citrix Cloud, consulte el [Acuerdo de nivel de servicio](#).

Novedades

March 1, 2024

Citrix aspira a entregar nuevas funciones y actualizaciones de sus productos a los clientes de Citrix Endpoint Management tan pronto como estén disponibles. Las nuevas versiones añaden valor al producto y no hay motivo para retrasar el momento de actualizar.

- Las actualizaciones continuas de Citrix Endpoint Management se publican aproximadamente cada dos semanas.
- Estas actualizaciones no provocan ningún tiempo de inactividad para los usuarios de la instancia o del dispositivo.
- No todas las versiones contienen funciones nuevas, y algunas actualizaciones incluyen correcciones y mejoras de rendimiento.

Para usted, como cliente, este proceso es transparente. Las actualizaciones iniciales solo se aplican en los sitios internos de Citrix; luego se aplican gradualmente en los entornos de los clientes. La entrega de actualizaciones incrementalmente en fases ayuda a ofrecer la seguridad de los productos y maximizar su disponibilidad.

También recibe comunicaciones y actualizaciones de Citrix Endpoint Management directamente de parte del equipo de operaciones de Citrix Endpoint Management Cloud. Esas actualizaciones lo mantienen al día, puesto que recibe así las funciones nuevas, los problemas conocidos y los problemas resueltos, entre otros.

Para obtener más información, incluida la disponibilidad del servicio y la escalabilidad en la nube,

consulte el [Contrato de nivel de servicio](#) de Citrix Endpoint Management. Para supervisar las interrupciones de servicio y el mantenimiento programado, consulte el [Panel de estado del servicio](#).

Las directivas clásicas se retiran de Citrix ADC

Citrix anunció recientemente la retirada de algunas funciones basadas en directivas clásicas a partir de la compilación 56.20 de Citrix ADC 12.0. Los avisos de retirada de Citrix ADC no afectan a las integraciones existentes de Citrix Endpoint Management con NetScaler Gateway. Citrix Endpoint Management sigue siendo compatible con las directivas clásicas y no es necesario hacer nada.

Antes de actualizar la versión de los dispositivos de punto final a iOS 14.5

Antes de actualizar la versión de un dispositivo de punto final a iOS 14.5, Citrix recomienda lo siguiente para mitigar cierres inesperados de las aplicaciones:

- Actualice la versión de Citrix Secure Mail y Citrix Secure Web a 21.2.X o a una posterior. Consulte [Actualizar la versión de aplicaciones MDX o de empresa](#).
- Si utiliza MDX Toolkit, empaquete todas las aplicaciones iOS de terceros con MDX Toolkit 21.3.X o una versión posterior y actualice la versión de dichas aplicaciones en la consola de Citrix Endpoint Management. Compruebe la [página de descargas](#) de MDX Toolkit para asegurarse de que dispone de la versión más reciente.

Antes de actualizar la versión de un Citrix ADC local a 13.0-64.35 o una versión posterior

Si utiliza la versión local de Citrix ADC y la actualiza a la versión 13.0-64.35 o a una posterior: Implemente la solución temporal descrita en Problemas conocidos en Citrix Endpoint Management 20.10.1.

Citrix Endpoint Management 24.1.0

Esta versión resuelve varios problemas para mejorar el rendimiento y la estabilidad generales. No se agregaron nuevas funciones.

Citrix Endpoint Management 23.12.0

Se agregó un nuevo campo obligatorio “Dominio” en los parámetros de 802.1x para Android: Se agregó un nuevo campo **Dominio** en la página de configuración de directivas de **red de la plataforma**

Android Enterprise para el tipo de autenticación **EAP 802.1x**. Para obtener más información, consulte [Parámetros de 802.1x para Android](#).

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.

Problemas conocidos actuales

Problemas conocidos en Citrix Endpoint Management 22.6.0

De forma intermitente, la selección de los tres tipos de registro (**Depuración**, **Auditoría de administración** y **Auditoría de usuarios**) para descargar en **Solución de problemas y asistencia > Registros** no funciona. Solo se descargan los registros de depuración. Como solución temporal, puede descargar cada registro por separado o abrir el explorador web en modo incógnito para descargar todos los registros tras marcar las tres casillas. [CXM-105334]

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 temporal, guarde la aplicación sin cargar ningún icono. [CXM-105395]

Las directivas de Samsung Knox/SAFE siguen activas en dispositivos inscritos incluso después de retirarse y no se pueden inhabilitar ni configurar. Como solución temporal, desinscriba el dispositivo e inscríbalo de nuevo. [CXM-104303]

Problemas conocidos en Citrix Endpoint Management 22.4.0

Al buscar un usuario de Active Directory inscrito en la ficha **Supervisar**, no se muestran los dispositivos inscritos para el usuario. Aun así, puede ver las directivas y las aplicaciones asignadas al usuario y realizar todas las acciones de seguridad en **Administrar > Dispositivos**. Esto afecta a los dispositivos iOS y Android inscritos. [CXM-104283]

Las aplicaciones privadas no consiguen publicarse con Android Enterprise por un problema en los servicios de Google. Actualizaremos nuestra documentación cuando el problema se haya resuelto. [CXM-103690]

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 aunque tuvieran un permiso personalizado antes de la migración. Como solución temporal, puede actualizar los permisos de administrador en la página Administración de acceso e identidad de Citrix Cloud con el acceso necesario. [CXM-102765]

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 modificar usuarios locales también pueden agregar o modificar usuarios locales en Citrix Cloud. Estos permisos incluyen cambiar las contraseñas de los usuarios locales. Para solucionar este problema, puede llamar a Asistencia para que se bloquee el acceso directo de administrador local a la consola y, así, permitir solamente el acceso de administrador de Citrix Cloud. [CXM-102780]

Problemas conocidos en Citrix Endpoint Management 21.11.0

En dispositivos iOS inscritos solo en MAM, las aplicaciones de empresa no consiguen instalarse. [CXM-101852]

El uso de la directiva **Actualizar automáticamente aplicaciones administradas** para Android Enterprise no se aplica en dispositivos cuando la versión del servidor de CEM se actualiza a 21.11.0. El error de la directiva afecta a las actualizaciones de aplicaciones en el dispositivo. Como solución temporal, un administrador puede modificar y guardar la directiva para actualizar los valores predeterminados. [CXM-102446]

Problemas conocidos en Citrix Endpoint Management 21.10.0

La directiva de VPN no funciona correctamente en dispositivos Windows 11 administrados. Hemos notificado este problema a Microsoft y estamos trabajando con ellos para resolverlo. En cuanto haya novedades, se lo haremos saber.

Problemas conocidos en Citrix Endpoint Management 21.9.1

En dispositivos Android inscritos en el perfil de trabajo en el modo de dispositivos propiedad de la empresa, es posible que los usuarios vean errores que indican que no pueden instalar ni buscar aplicaciones en su perfil personal. Si ven esos errores, actualice la aplicación Google Play Store e inténtelo de nuevo. [CXM-100678]

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. Quitan su cuenta de la aplicación Microsoft Authenticator.
4. Inician una aplicación de Office 365 y cierran sesión.

Como solución temporal, desinscriba el dispositivo de Citrix Endpoint Management y vuelva a inscribirlo. [CXM-90235]

Problemas conocidos en Citrix Endpoint Management 21.4.0

La reinscripción falla en dispositivos iOS si el usuario que intenta reinscribirse es un usuario de Azure Active Directory diferente del usuario inscrito originalmente en el dispositivo. Como solución temporal, desinscriba al usuario original de la aplicación Microsoft Authenticator del dispositivo antes de reinscribirse. [CXM-90218]

Problemas conocidos en Citrix Endpoint Management 21.2.0

Al agregar Citrix Secure Web como una aplicación MDX para Android Enterprise, Google Play administrado no puede encontrar la aplicación por medio de su identificador. Si busca “Citrix Secure Web”, en lugar del identificador de la aplicación, Google Play administrado puede encontrarla. Se trata de un problema de Google. [CXM-91991]

Es posible que no se pueda importar el certificado de escucha SSL. Vuelva a empaquetar el almacén de claves de certificado a partir de los pasos descritos en [CTX-297153](#). [XMHELP-3346]

Problemas conocidos en Citrix Endpoint Management 20.10.1

Si actualiza Citrix ADC local a la versión 13.0-64.35 o a una posterior y Citrix Endpoint Management no está habilitado para Workspace, fallan Single Sign-On en Citrix Files o la URL de dominio de ShareFile. El usuario no puede iniciar sesión. Este error solo ocurre en exploradores con la opción **Inicio de sesión de empleados**.

Para evitar 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](#)

Después de completar la solución temporal, los usuarios podrán autenticarse mediante Single Sign-On (SSO) en Citrix Files o en la URL del dominio de ShareFile desde un explorador con la opción **Inicio de sesión de empleados**. [CXM-88400]

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, se produce un error al hacer clic en el botón **Probar conexión**. Para resolver este problema, inhabilite la autenticación de varios factores para ShareFile. Obtenga más información sobre este problema y la solución temporal en esta [página de asistencia](#). [CXM-79240]

Problemas conocidos en Citrix Endpoint Management 20.1.0

Al agregar usuarios a una biblioteca en Citrix Cloud, Citrix Endpoint Management indica que el proceso se ha realizado correctamente, pero los usuarios no se agregan. [CXM-73726]

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 quiere eliminar y, a continuación, haga clic en **Modificar**. Anule la selección de **Android Enterprise** y seleccione cualquier otra plataforma de la lista de plataformas. Guarde la aplicación. A continuación, puede eliminar la aplicación. [CXM-74468]

Problemas conocidos en Citrix Endpoint Management 19.5.0

Al inscribir un dispositivo de Citrix Ready Workspace Hub, defina la dirección MAC de Ethernet (eth0) en la lista de permitidos; si no, se produce un error en la inscripción. [CXM-43141]

Problemas conocidos en Citrix Endpoint Management 19.4.1

Al pasar de una ficha a otra en las opciones de la directiva de dispositivo GPO de Windows, se omiten los botones de opción y las casillas de verificación. [CXM-58277]

Problemas conocidos en Citrix Endpoint Management 19.2.1

Si desinscribe una empresa de Android Enterprise eliminándola a través de la consola de administración de Google, es posible que se produzca un error al intentar inscribir la empresa de nuevo. Utilice siempre la consola de Citrix Endpoint Management para desinscribir una empresa de Android Enterprise, como se describe en [Desinscribir una empresa de Android Enterprise](#). Los clientes de Google Workspace deben seguir las instrucciones de [Desinscribir una empresa de Android Enterprise](#). [CXM-62709] [CXM-62950]

Problemas conocidos en Citrix Endpoint Management 19.2.0

Al crear una aplicación de la tienda pública en Citrix Endpoint Management 10.18.3, en la página de configuración de aplicaciones del 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 no responden y no permiten buscar aplicaciones. El problema se produce al crear aplicaciones de tiendas públicas para iOS o Android. [CXM-46820]

Problemas conocidos en Citrix Endpoint Management 10.19.1

Después de completar el proceso de registro en la página **Parámetros > Android Enterprise**, aparece el mensaje de error: **A configuration error occurred. Please try again**. Al cerrar el mensaje de error, se guarda la configuración de Android Enterprise, aunque **Habilitar Android Enterprise** esté **desactivado**. Para evitar este problema, reduzca la cantidad de categorías de aplicaciones a 30 o menos. [CXM-60899]

Problemas conocidos en Citrix Endpoint Management 10.18.5

Cuando una aplicación Chrome se configura como una aplicación obligatoria para ChromeOS, es posible que los usuarios deban cerrar la sesión y volver a iniciarla para instalar la aplicación. Este problema de terceros tiene el ID de error de Google #76022819. [CXM-48060]

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 vuelva a iniciar sesión desde la aplicación Citrix Secure Hub o Self Help Portal. [CXM-45730]

Problemas conocidos en Citrix Endpoint Management 10.7.4

Si configura Citrix Endpoint Management para Single Sign-On (SSO) mediante el proveedor de identidades de Citrix con Azure Active Directory: cuando un administrador o usuario de Citrix Endpoint Management se redirige a la pantalla de **inicio de sesión de Azure Active Directory**, la pantalla contiene el mensaje “Página de inicio de sesión para Citrix Secure Hub”. El mensaje debería ser “Página de inicio de sesión para la consola de Citrix Endpoint Management”. [CXM-42309]

Avisos legales de terceros

April 30, 2020

Citrix Endpoint Management puede incluir software de terceros con licencias definidas según los términos del siguiente documento:

[Avisos de terceros para Citrix Endpoint Management](#)

Elementos retirados

March 1, 2024

Los anuncios de este artículo comunican por adelantado las funciones de Citrix Endpoint Management que se están retirando progresivamente, de modo que pueda tomar a tiempo las decisiones empresariales pertinentes. Citrix examina el uso que hacen los clientes de una función que está por retirar y los comentarios que tengan sobre la eliminación de la función para determinar cuándo retirarla. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas. Para obtener información detallada sobre el ciclo de vida útil de los productos, consulte el artículo [Product Lifecycle Support Policy](#).

Importante:

Gracias por usar la herramienta Citrix Endpoint Management Analyzer. Gracias a nuestra cadencia de lanzamiento frecuente y estable, esta herramienta ya no es necesaria. Citrix ha decidido interrumpir este servicio a partir del 31 de marzo de 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 eliminados y obsoletos

En la lista siguiente se muestran las funciones de Citrix Endpoint Management que se han retirado o eliminado.

Los elementos *retirados* no se quitan inmediatamente. Citrix sigue ofreciendo los elementos retirados hasta eliminarlos en una versión futura.

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

Para obtener información sobre las aplicaciones móviles de productividad que han alcanzado el fin de su vida, consulte [Fin de vida y aplicaciones retiradas](#).

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Oferta de Citrix Endpoint Management Government	Se retiró la compatibilidad con la oferta de Citrix Endpoint Management Government.	Enero de 2022	Julio de 2022	Edición estándar de Citrix Endpoint Management
API de SafetyNet Attestation	Se ha retirado el soporte para Android SafetyNet Attestation según el anuncio de Google aquí .	Julio de 2023	Noviembre de 2023	API Play Integrity
Chrome OS	Compatibilidad retirada con Chrome OS.	Julio de 2022	Mayo de 2023	No hay alternativa
tvOS	Compatibilidad con tvOS retirada.	Julio de 2022	Mayo de 2023	No hay alternativa
Windows Information Protection	Retirada de Windows Information Protection según el anuncio de Microsoft aquí .	Agosto de 2022	Octubre de 2022	No hay alternativa

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Citrix Endpoint Management Analyzer	Ya no se desarrolla la herramienta Citrix Endpoint Management Analyzer.	Julio de 2022	Objetivo: 31 de marzo de 2023	No hay alternativa
Administrar dispositivos Workspace Hub	Ya no se admiten dispositivos de Citrix Ready Workspace Hub.	Enero de 2022	Junio de 2022	No hay alternativa
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 .	Julio de 2021	Objetivo: Marzo de 2023	No hay alternativa
Samsung SAFE	Compatibilidad con Samsung SAFE retirada.	Enero de 2022	Junio de 2022	Use Android Enterprise.
XML personalizado para Zebra	Función retirada de XML personalizado en dispositivos Zebra.	Enero de 2022	Junio de 2022	Use la Configuración administrada de Android Enterprise.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Identidades de PKI: Genérica, Symantec PKI, DigiCert y Entrust	Compatibilidad retirada para las entidades de PKI genéricas, administradas por DigiCert y de adaptador Entrust.	Junio de 2021	Enero de 2022	No hay alternativa
Android para Workspace	Fin de compatibilidad con Android para Workspace	Enero de 2022	Abril de 2022	No hay alternativa
Puerta de enlace SMS del operador	Función retirada de notificaciones de puerta de enlace SMS de Nexmo	Enero de 2022	Abril de 2022	Usar las notificaciones de servidor SMTP
Proveedor de servicios móviles (MSP)	Se ha retirado la interfaz MSP para consultar dispositivos BlackBerry y otros dispositivos Exchange ActiveSync y emitir operaciones	Enero de 2022	Abril de 2022	No hay alternativa

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
MDX Toolkit	Se retira la funcionalidad para MDX Toolkit en favor del SDK de Mobile App Management (MAM). Durante esta transición, podrá usar aplicaciones MDX empaquetadas y aplicaciones desarrolladas por el SDK de MAM.	Marzo de 2020	Julio de 2023	Para seguir administrando sus aplicaciones de empresa, use el SDK de MAM.
Rol de RBAC: Inscripción de dispositivos compartidos e inscripción de dispositivos COSU	Se retiran los parámetros predefinidos del control de acceso por roles para la inscripción de dispositivos compartidos y la inscripción de dispositivos COSU.	Julio de 2021	Diciembre de 2021	Configure dispositivos iOS mediante Apple School Manager o Apple Business Manager . Configure dispositivos COSU (dedicados) Android mediante perfiles de inscripción .

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Restricción Permitir conexión automática a hotspots del Sensor Wi-Fi para dispositivos con Windows.	Se retira la restricción Permitir conexión automática a hotspots del Sensor Wi-Fi para dispositivos con Windows 10. Windows 10 ya no ofrece esta función. Para obtener información, consulte la documentación de Microsoft .	Octubre de 2021	Febrero de 2022	No hay alternativa
MDX: Servidor de Gateway alternativo	Se retira la autenticación de nivel superior para dispositivos iOS y Android.	Marzo de 2020	Septiembre de 2021	No hay alternativa
MDX: Micro VPN (modo de túnel completo)	Se retiró el túnel completo de red privada virtual (VPN) 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.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
MDX: Compatibilidad con archivos PAC	Se retiró el archivo de configuración automática de proxy (PAC) con una implementación de túnel completo de VPN para los 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 MDX compartidos	Se retiró la compatibilidad con dispositivos compartidos para las aplicaciones MDX.	Marzo de 2020	Septiembre de 2021	Para Android Enterprise, use dispositivos compartidos inscritos como dispositivos dedicados. Para iOS, use Apple School Manager o GroundControl. Use Android Enterprise.
Android Sony	Ya no se admiten los dispositivos Android Sony ni las directivas específicas de Sony.	Enero de 2021	Febrero de 2022	Use Android Enterprise.
Android HTC	Ya no se admiten los dispositivos Android HTC ni las directivas específicas de HTC.	Enero de 2021	Febrero de 2022	Use Android Enterprise.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Android - Amazon	Ya no se admiten dispositivos Android de Amazon ni directivas específicas de Amazon.	Enero de 2021	Febrero de 2022	Use Android Enterprise.
Knox Mobile Enrollment (AD heredado)	Knox Mobile Enrollment (KME) se retiró del modo de administrador de dispositivos heredado en todas las versiones de Android.	4 de mayo de 2021	Septiembre de 2021	Utilice KME para inscribirse en el modo Android Enterprise. Android 8, 9, 10 y 11 admiten Android Enterprise.
Modo de inscripción de alta seguridad	Ya no se permite generar invitaciones de inscripción con el modo de seguridad de inscripción Alta seguridad .	Julio de 2021	Febrero de 2022	Consulte Invitaciones de inscripción para ver una lista de los modos de seguridad de inscripción admitidos.
Credenciales derivadas	Desarrollo detenido de las credenciales derivadas y de la aplicación Citrix Derived Credential Manager.	Marzo de 2021	Diciembre de 2021	Consulte iOS para obtener una lista de los tipos de autenticación admitidos en iOS.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Puertos de salida del servicio de notificaciones push de Apple (APNs)	Apple dejará de desarrollar el protocolo binario heredado de APNs a partir del 31 de marzo de 2021. Apple recomienda que se utilice en su lugar la API del proveedor de APNs basada en HTTP/2. Como parte de este cambio, no se admitirán los puertos 2195 ni 2196, utilizados para enviar notificaciones de APNs a *.push.apple.com.	Octubre de 2020	Marzo de 2021	Utilice el puerto 443 en su lugar. Consulte Requisitos de red y firewall .
MDX Service	Se retiró la funcionalidad para MDX Service en favor del SDK de Mobile App Management (MAM). Durante esta transición, podrá usar aplicaciones MDX empaquetadas con MDX Toolkit y aplicaciones desarrolladas por el SDK de MAM.	Marzo de 2020	Septiembre de 2021	MDX Toolkit

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Configuración de las invitaciones de inscripción en Self Help Portal	Ya no se permite a los usuarios generar invitaciones de inscripción desde Self Help Portal.	Julio de 2021	Julio de 2021	Póngase en contacto con el administrador para generar invitaciones de inscripción en la consola de Citrix Endpoint Management.
Configuración de invitación de inscripción	Ya no se permite usar IMEI de dispositivo, números de serie ni UDID para crear invitaciones de inscripción.	Abril de 2021	Julio de 2021	Al crear una invitación de inscripción, configure los parámetros disponibles en Administrar > Invitaciones de inscripción en la consola de Citrix Endpoint Management.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Algoritmos de firma de autenticación basados en certificados (no FIPS y cifrados débiles)	Se retiró el soporte de los siguientes algoritmos de firma: SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA, SHA1withDSA, RIPEMD160withRSA, RIPEMD128withRSA, RIPEMD256withRSA.	Mayo de 2020	Junio de 2021	Al crear una solicitud de firma de certificado (CSR) para un proveedor de credenciales en la consola de Citrix Endpoint Management (Configuración > Proveedores de credenciales > Solicitud de firma de certificado), elija un cifrado más sólido.
Aplicaciones móviles de Citrix y aplicaciones Workspace para Android 7.x y iOS 12.x	Ya no se admiten las versiones de Android 7.x y iOS 12.x de Citrix Secure Hub, Citrix Secure Mail, Citrix Secure Web y la aplicación Citrix Workspace.	Abril de 2021	Junio de 2021	Use, como mínimo, la versión actual y la anterior de todas las plataformas de los sistemas operativos principales. Los dispositivos antiguos siguen inscritos. Sin embargo, Citrix no prueba ni admite los dispositivos heredados.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Compatibilidad con token de software de RSA para Android	Se retiró la importación directa de tokens de software de RSA en Citrix Secure Hub para Android.	Enero de 2021	Febrero de 2021	Puede importar el token de software de RSA en la aplicación RSA SecurID disponible en Google Play. A continuación, puede usar el token para la autenticación de NetScaler Gateway.
Internet Explorer 11	Internet Explorer ya no es compatible con la consola de Citrix Endpoint Management.	Enero de 2021	Enero de 2021	Utilice la versión más reciente de estos exploradores web: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari
Comprobaciones de configuración de Gateway en Citrix Endpoint Management Analyzer	Ya no se ofrece la opción de comprobar la configuración de Gateway.	Noviembre de 2020	Noviembre de 2020	Utilice la comprobación de Citrix Insight Services en Analyzer para verificar si las configuraciones de Citrix ADC están listas para la implementación de Citrix Endpoint Management.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Aplicaciones publicadas para el modo Administrador de dispositivos heredado en dispositivos Android Enterprise	Ya no entregamos aplicaciones publicadas para la plataforma AD heredada a los dispositivos inscritos en Android Enterprise.	Octubre de 2020	Noviembre de 2020	Para los dispositivos Android Enterprise, debe publicar aplicaciones para la plataforma Android Enterprise. Para continuar publicando aplicaciones en modo AD heredado para dispositivos en modo AD, cree un grupo de entrega aparte para esas aplicaciones.
Modo de administrador de dispositivos heredado para dispositivos Android 10	Google ha retirado algunas API de Administrador de dispositivos. Citrix no admite dispositivos Android 10 inscritos en el modo Administrador de dispositivos después de actualizar la versión de Citrix Secure Hub al nivel 29 de la API de Android.	Febrero de 2020	Noviembre de 2020	Migre los dispositivos Android 10 a Android Enterprise.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Android TouchDown	DigiCert dejó de admitir Android TouchDown. Citrix retiró la página de la plataforma Android TouchDown que había en la directiva de dispositivo de Exchange.	Julio de 2018	Noviembre de 2020	Recomendación: Utilice Citrix Secure Mail.
Nuevas inscripciones de administrador de dispositivos para Android 10	Se retiró el soporte para nuevas inscripciones o reinscripciones en el modo de administrador de dispositivos antiguos en dispositivos Android 10. Los dispositivos ya inscritos continúan funcionando.	Febrero de 2020	Septiembre de 2020	Inscriba los nuevos dispositivos Android 10 (o una versión posterior) en Android Enterprise.

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Cifrado MDX	Se retiraron el cifrado MDX y la función de cifrado MDX de la consola de Citrix Endpoint Management.	Octubre de 2019	Septiembre de 2020	Habilite el cifrado de plataformas iOS o Android mediante nuestra función de administración de cifrados con comprobación adicional de cumplimiento de normas. Debe probar y planificar la migración del cifrado MDX antes de julio de 2020.
Windows Mobile/CE	Ya no se admiten dispositivos Windows Mobile/CE.	Abril de 2018	Septiembre de 2020	Use equipos de escritorio y portátiles Windows 10.
Contenedor SEAMS de Samsung	Ya no se admite el contenedor SEAMS de Samsung.	Junio de 2020	Agosto de 2020	Use Android Enterprise.
Remote Support	Ya no se desarrolla el cliente Remote Support.	Enero de 2019	Agosto de 2020	No hay alternativa

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Aplicaciones móviles de Citrix y aplicaciones Workspace para Android 6.x y iOS 11.x	Ya no se admiten 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	Use, como mínimo, la versión actual y la anterior de todas las plataformas de los sistemas operativos principales. 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 retiró el marco de extensión de red que le permitía personalizar las funciones de red para dispositivos iOS. Citrix Secure Hub 20.3.0.	Octubre de 2018	Marzo de 2020	No hay alternativa
Inicio de sesión de API con cuentas locales	Los administradores ya no podrán 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 API de REST .

Elemento	Descripción	Anuncio de la retirada	Eliminado	Alternativa
Certificados SSL (Secure Sockets Layer) autofirmados	Se retiró el soporte para certificados SSL autofirmados de todas las plataformas de dispositivos.	Mayo de 2020		Reemplace el certificado autofirmado existente por un certificado SSL de confianza procedente de una entidad de certificación (CA) conocida.

Requisitos del sistema

March 1, 2024

Mientras espera a que Citrix aprovisiona Citrix Endpoint Management, puede prepararse para la implementación de Citrix Endpoint Management instalando Cloud Connector. Aunque Citrix aloja y entrega su solución de Citrix Endpoint Management, se requiere que configure determinados puertos y vías de comunicación. Esa configuración conecta la infraestructura de Citrix Endpoint Management a los servicios de empresa, tales como Active Directory.

Requisitos de Cloud Connector

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

- Al menos dos máquinas Windows Server dedicadas que estén unidas a su dominio de Active Directory. Pueden ser máquinas físicas o virtuales. Para una instalación y un funcionamiento óptimos, la máquina donde se va a instalar Cloud Connector debe estar sincronizada con la hora UTC. Para obtener una lista completa de los requisitos más recientes, consulte el material de implementación que le facilite 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 para la plataforma, consulte [Citrix Cloud Connector](#).

Niveles funcionales admitidos de Active Directory

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

Nivel funcional de bosque	Nivel funcional de dominio	Controladores de dominio admitidos
Windows Server 2016	Windows Server 2016	Windows Server 2016, Windows Server 2019
Windows Server 2016	Windows Server 2019	Windows Server 2019
Windows Server 2019	Windows Server 2019	Windows Server 2019

Nota:

Los Windows Servers 2012 R2, 2012 y 2008 R2 ya no reciben asistencia porque han llegado a su fin de vida. Para obtener más información, consulte la [documentación sobre el ciclo de vida de los productos de Microsoft](#).

Requisitos de NetScaler Gateway

En estos casos, Citrix Endpoint Management requiere un NetScaler Gateway instalado en su ubicación de recursos:

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

Los requisitos:

- Autenticación de dominio (LDAP)
- NetScaler Gateway 12.1 o una versión posterior, con una licencia universal o de plataforma

Para obtener información detallada, consulte [Licencias](#).

- Certificado SSL público.

Para obtener información detallada, consulte [Crear y utilizar certificados SSL en un dispositivo Citrix ADC](#).

- Dirección IP pública no utilizada para el servidor virtual NetScaler Gateway
- Nombre de dominio completo (FQDN) que pueda resolverse públicamente para el servidor virtual NetScaler Gateway
- Certificados raíz e intermedios de Citrix Endpoint Management alojado en Cloud (suministrados en el paquete de script)
- Dirección IP privada no utilizada para asignarla como IP del equilibrador de carga del proxy
- Para conocer los requisitos de puertos, consulte Requisitos de puertos para 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 acerca de los requisitos de NetScaler Gateway, consulte el material de implementación que le facilite 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 intercambio y sincronización de archivos que ofrece Citrix Files están disponibles en la oferta Premium de Citrix Endpoint Management Service. El controlador de zonas de almacenamiento amplía el almacenamiento en la nube de software como servicio (SaaS) de Citrix Files al ofrecer almacenamiento privado de datos a su cuenta de Citrix Files.

Requisitos del controlador de zonas de almacenamiento:

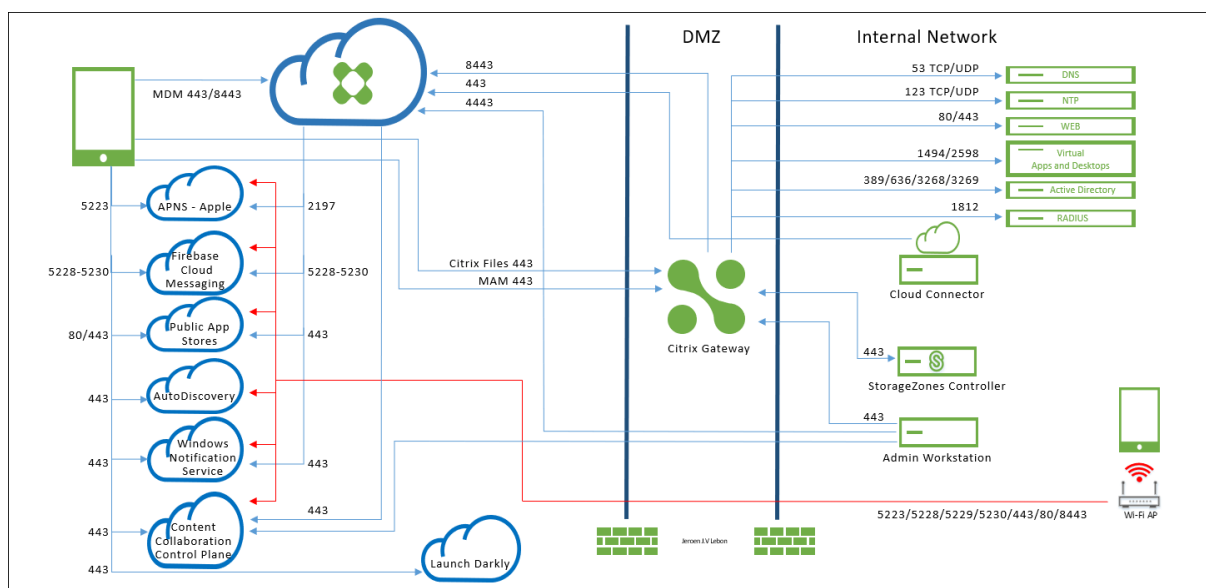
- Una máquina física o virtual dedicada
- Windows Server 2012 R2 (Datacenter, Standard o Essentials), Windows Server 2016, Windows Server 2019 o Windows Server 2022
- 2 CPU virtuales
- 4 GB de RAM
- 50 GB de espacio en disco
- Roles del servidor para el servidor web (IIS):
 - Desarrollo de aplicaciones: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

Requisitos de plataforma para Citrix Files:

- El instalador de Citrix Files requiere privilegios de administrador en el servidor Windows
- Nombre de usuario del administrador de Citrix Files

Requisitos de puertos

Para que dispositivos y aplicaciones puedan comunicarse con Citrix Endpoint Management, debe abrir puertos específicos en los firewalls. El siguiente diagrama muestra el flujo del tráfico de Citrix Endpoint Management.



En los siguientes apartados se ofrece una lista de los puertos que se deben abrir. Para obtener información sobre las direcciones URL que utilizan las aplicaciones móviles de productividad, consulte [Administrar marcas de función](#).

Requisitos de puertos para NetScaler Gateway

Abra 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 interna, como los sitios web de intranet

Para obtener más información sobre NetScaler Gateway, consulte [Configuración de parámetros para el 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 las conexiones DNS.	SNIP de NetScaler Gateway	Servidor DNS
80/443	NetScaler Gateway transfiere la conexión micro VPN al recurso de la red interna a través del segundo firewall.	SNIP de NetScaler Gateway	Sitios web de la intranet
123 (TCP y UDP)	Se usa para los servicios del protocolo de tiempo de red (NTP).	SNIP de NetScaler Gateway	Servidor NTP
389	Se usa para conexiones de protocolo LDAP no seguras.	IP de NetScaler Gateway (o, si usa un equilibrador de carga, SNIP)	Servidor de autenticación LDAP o Microsoft Active Directory
443	Se usa para 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 con el objetivo de entregar aplicaciones web, aplicaciones para móvil y aplicaciones SaaS.	Internet	NetScaler Gateway

Puerto TCP	Descripción	Origen	Destino
443	Se utiliza para la comunicación de Cloud Connector: enumeración de LDAP, DNS, PKI y Citrix Workspace	Servidores de Cloud Connectors	https://*.citrixworkspacesapi.net , https://*.cloud.com (commercial), https://*.blob.core.windows.net/ , https://*.servicebus.windows.net
443	Se utiliza para acceder al portal Self-Help Portal de Citrix Endpoint Management, si está habilitado, a través del explorador.	Punto de acceso (explorador)	Citrix Endpoint Management (<a href="https://<sitename>/zdm/shp">https://<sitename>/zdm/shp)
636	Se usa para conexiones seguras de protocolo LDAP.	IP de NetScaler Gateway (o, si usa un equilibrador de carga, SNIP)	Servidor de autenticación LDAP o Active Directory
1494	Se usa para las conexiones ICA a aplicaciones Windows en la red interna. Citrix recomienda mantener este puerto abierto.	SNIP de NetScaler Gateway	Citrix Virtual Apps and Desktops
1812	Se utiliza para las conexiones RADIUS.	IP de NetScaler Gateway	Servidor de autenticación RADIUS

Puerto TCP	Descripción	Origen	Destino
2598	Se utiliza para las conexiones a aplicaciones Windows en la red interna mediante la función de fiabilidad de la sesión. Citrix recomienda mantener este puerto abierto.	SNIP de NetScaler Gateway	Citrix Virtual Apps and Desktops
3269	Se usa para conexiones seguras LDAP del catálogo global de Microsoft.	IP de NetScaler Gateway (o, si usa 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 administración de aplicaciones para móvil (MAM) y el almacén de aplicaciones.	SNIP de NetScaler Gateway	Citrix Endpoint Management
8443	El puerto Secure Ticket Authority (STA) se utiliza para el token de autenticación de Citrix Secure Mail.	SNIP de NetScaler Gateway	Citrix Endpoint Management

Requisitos de red y firewall

Para que dispositivos y aplicaciones puedan comunicarse con Citrix Endpoint Management, debe abrir puertos específicos en los firewalls. En las siguientes tablas, se ofrece una lista de esos puertos.

Abra 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 (https://*.sharefile.com , https://cwsproduction.blob.core.windows.net/downloads , https://*.servicebus.windows.net	
443		Consola de administración	https://*.citrixworkspacesapi.net , https://*.cloud.com (https://*.citrix.com , https://cwsproduction.blob.core.windows.net/downloads	

Puerto TCP	IP de origen	Descripción	Destino	IP de destino
443		Acceso al portal Self-Help Portal de Citrix Endpoint Management a través de un explorador (si el portal está habilitado)	Citrix Endpoint Management	
4443		Acceso a consola de Citrix Endpoint Management a través de un explorador	Citrix Endpoint Management	

Abra puertos desde Internet a la zona DMZ:

Puerto TCP	Descripción	IP de origen	Destino	IP de destino
443	Dispositivo cliente Citrix Endpoint Management		IP de NetScaler Gateway	
443	Dispositivo cliente Citrix Endpoint Management		VIP de NetScaler Gateway	
443	Dirección IP pública de Citrix Files	CTX208318	VIP de NetScaler Gateway	

Abra puertos desde la zona DMZ a la red interna:

Puerto TCP	Descripción	IP de origen	Destino	IP de destino
389 o 636	IP de NetScaler Gateway		IP de Active Directory	
53 (UDP)	IP 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	

Abra puertos desde la red interna a la zona DMZ:

Puerto TCP	Descripción	IP de origen	Destino	IP de destino
443	Cliente de administración		IP de NetScaler Gateway	

Abra puertos desde la red interna a Internet:

Puerto TCP	Descripción	IP de origen	Destino	IP de destino
443	IP del servidor Exchange (EAS)		Agentes de escucha para notificaciones push de Citrix Endpoint Management (1)	
443	IP del controlador de zonas de almacenamiento		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](#)

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

Puerto TCP	Descripción	IP de origen	Destino	IP de destino
8443 / 443	Dispositivo cliente Citrix Endpoint Management		Citrix Endpoint Management	
5223	Dispositivo cliente Citrix Endpoint Management		Servidores Apple APNS	17.0.0.0/8
5228	Dispositivo cliente Citrix Endpoint Management		Firebase Cloud Messaging	android.googleapis.com, fcm.googleapis.com
5229	Dispositivo cliente Citrix Endpoint Management		Firebase Cloud Messaging	android.googleapis.com, fcm.googleapis.com
5230	Dispositivo cliente Citrix Endpoint Management		Firebase Cloud Messaging	android.googleapis.com, fcm.googleapis.com
443	Dispositivo cliente Citrix Endpoint Management		Firebase Cloud Messaging	fcm.googleapis.com
443	Dispositivo cliente Citrix Endpoint Management		Servicio de notificaciones push de Windows	*.notify.windows.com

Puerto TCP	Descripción	IP de origen	Destino	IP de destino
443 / 80	Dispositivo cliente Citrix Endpoint Management		Tienda de aplicaciones iTunes de Apple	ax.apps.apple.com , *.mzstatic.com , vpp.itunes.apple.com
443 / 80	Dispositivo cliente 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 Citrix Endpoint Management		Tienda de aplicaciones de Microsoft	login.live.com , *.notify.windows.com
443	Dispositivo cliente Citrix Endpoint Management		Servicio de detección automática de Citrix Endpoint Management para iOS y Android	discovery.cem.cloud.us
443	Dispositivo cliente 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

Puerto TCP	Descripción	IP de origen	Destino	IP de destino
443	Dispositivo cliente Citrix Endpoint Management		Administración de Google Mobile, API de Google, API de Google Play Store	*.googleapis.com
443	Dispositivo cliente Citrix Endpoint Management		Durante la comprobación de conectividad, se buscan versiones de CloudDPC anteriores a 470. Las comprobaciones de conectividad de Android a partir de N MR1 requieren que https://www.google.com/generate_204 sea accesible, o que la red Wi-Fi en cuestión apunte a un archivo PAC accesible.	connectivitycheck.android.com, www.google.com

Requisito de puerto para la conectividad con AutoDiscovery Service

Esta configuración de puerto garantiza que los dispositivos Android que se conectan desde Citrix Secure Hub para Android puedan acceder al servicio de detección automática (AutoDiscovery Service/ADS) de Citrix Endpoint Management desde dentro de la red interna. La capacidad de acceder a ADS es importante en el momento de descargar las actualizaciones de seguridad que están disponibles a través del servicio ADS.

Nota:

Puede que las conexiones ADS no admitan su servidor proxy. En este caso, permita que la conexión ADS circunvale el servidor proxy.

Si quiere habilitar la fijación de certificados, debe cumplir los siguientes requisitos previos:

- **Obtenga certificados para el servidor de Citrix Endpoint Management y NetScaler Gateway:** Los certificados deben estar en formato PEM y deben ser certificados públicos y no las claves privadas.
- **Contacte con la asistencia de Citrix y solicite que se habilite la fijación de certificados:** Durante este proceso, se le solicitarán los certificados.

La fijación de certificados requiere que los dispositivos se conecten al servicio ADS antes de que el dispositivo se inscriba. Ese requisito garantiza que Citrix Secure Hub disponga de la información de seguridad más actualizada. Para que Citrix Secure Hub inscriba un dispositivo, éste debe contactar con el servicio ADS. Por lo tanto, es vital abrir el acceso al servicio ADS dentro de la red interna para permitir la inscripción de dispositivos.

Para que Citrix Secure Hub para Android/iOS acceda al servicio ADS, abra el puerto 443 para este nombre de dominio completo (FQDN):

FQDN	Puerto	Uso de IP y puerto
<code>discovery.cem.cloud.us</code>	443	Citrix Secure Hub: Comunicación ADS a través de CloudFront

Para obtener información sobre las direcciones IP admitidas, consulte [Cloud-based storage centers from AWS](#).

Requisitos de red de Android Enterprise

Para obtener información sobre las conexiones salientes que se deben tener en cuenta al configurar entornos de red para Android Enterprise, consulte el artículo [Android Enterprise Network Requirements](#) de la asistencia técnica de Google.

Requisitos de aplicación

Citrix Endpoint Management permite agregar y mantener hasta 300 aplicaciones. Si supera este límite, el sistema se volverá inestable.

Compatibilidad de Citrix Endpoint Management

November 29, 2023

Para utilizar las nuevas funciones, soluciones y actualizaciones de directivas, Citrix recomienda instalar la versión más reciente de:

- Citrix recomienda integrar el SDK de administración de aplicaciones móviles (MAM) con las aplicaciones de empresa para iOS y Android a fin de proporcionar funcionalidades MDX a dichas aplicaciones.

MDX Toolkit está programado para alcanzar el final de su vida útil (EOL) en julio de 2023. Para seguir administrando sus aplicaciones empresariales, debe incorporar el SDK de MAM.

- Aplicaciones móviles de productividad

En este artículo, se resumen las versiones de los componentes de Citrix Endpoint Management admitidos que se pueden integrar.

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

Aplicaciones móviles de productividad

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

Para obtener más información acerca del ritmo de publicación por fases cada dos semanas previsto para las aplicaciones móviles de productividad, consulte [Calendario de versiones](#). Para obtener información de asistencia, consulte [Compatibilidad con aplicaciones móviles de productividad](#).

SDK de MAM

El SDK de MAM proporciona funcionalidad MDX que no cubren las plataformas iOS y Android. Puede hacer que esas aplicaciones estén disponibles en un almacén interno o en tiendas públicas de aplicaciones. Consulte [SDK de aplicaciones MDX](#).

MDX Toolkit

MDX Toolkit está programado para alcanzar el final de su vida útil (EOL) en julio de 2023. Para seguir administrando sus aplicaciones empresariales, debe incorporar el SDK de MAM.

Citrix admite las tres versiones más recientes (n.n.n) de MDX Toolkit. Consulte [Novedades en MDX Toolkit](#).

Compatibilidad con exploradores web

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

- La versión más reciente de Google Chrome
- La versión más reciente de Mozilla Firefox
- La versión más reciente de Microsoft Edge
- La versión más reciente de Apple Safari

Sistemas operativos compatibles para los dispositivos

March 1, 2024

En este artículo se incluyen los dispositivos compatibles con la administración de la movilidad empresarial a través de Citrix Endpoint Management. Por motivos de seguridad y debido a restricciones de plataforma, Citrix Endpoint Management no admite todas las funciones en todas las plataformas.

Para ver las versiones más recientes de las aplicaciones móviles de productividad, consulte [Aplicaciones móviles de productividad admitidas](#).

Nota:

Citrix es compatible con las versiones actuales y las anteriores de todas las plataformas de los sistemas operativos principales. Algunas funciones de Citrix Endpoint Management no funcionan en versiones más antiguas de las plataformas.

Para ver los anuncios de elementos retirados, consulte [Elementos retirados](#).

Lista de compatibilidad de sistemas operativos

Citrix Endpoint Management es compatible con los siguientes sistemas operativos:

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

Citrix recomienda actualizar Android a la versión 10 como mínimo antes de usar Android Enterprise. Para obtener más información, consulte Consideraciones sobre Android.

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

Por ahora, Citrix Endpoint Management y las aplicaciones móviles de Citrix no admiten todas las nuevas funciones disponibles para iOS 14.x, iOS 15.x, iOS 16.x y iOS 17.x.

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

Por ahora, Citrix Endpoint Management y las aplicaciones móviles de Citrix no admiten todas las nuevas funciones de iPadOS 14.x, iPadOS 15.x, iPadOS 16.x i iPadOS 17.x.

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

Por ahora, Citrix Endpoint Management y las aplicaciones móviles de Citrix no admiten todas las nuevas funciones disponibles para macOS 11, macOS 12, macOS 13 y macOS 14.

- **Escritorios y tabletas con Windows 10 o 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 averiguar el nivel de compatibilidad de un sistema operativo específico.

Consideraciones sobre Android

Antes de actualizar el sistema operativo a Android 10 o a una versión posterior: Consulte [Migrar de la administración de dispositivos a Android Enterprise](#) para obtener información sobre cómo afecta la retirada de las API de administración de dispositivos de Google a los dispositivos con Android 10 o una versión posterior. Consulte también este [blog de Citrix](#).

- Google retiró las API de administración de dispositivos, lo que afecta a los dispositivos con Android 10 o una versión posterior. No se pueden inscribir dispositivos de Android 10 o una versión posterior en el modo de administración de dispositivos antiguos. 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 en las API de Google no afecta a los dispositivos inscritos en el modo solo MAM.
- Consulte también este [blog de Citrix](#).

Antes de actualizar:

- Compruebe que la infraestructura de su servidor cumple los requisitos de 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 correspondiente. Citrix solamente confía en los certificados que contienen un nombre SAN que coincida con el nombre del host.

Compatibilidad con los siguientes idiomas

November 29, 2023

Las aplicaciones móviles de productividad de Citrix y la consola de Citrix Endpoint Management están adaptadas para poder utilizarse en otros idiomas además del inglés. En la disponibilidad de idiomas se incluyen entradas de teclado y caracteres no incluidos en el alfabeto inglés, incluso aunque la aplicación propiamente dicha no esté traducida al idioma preferido del usuario. Para obtener más información sobre la globalización de todos los productos Citrix, consulte <https://support.citrix.com/article/CTX119253>.

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

Consola de Citrix Endpoint Management y Self-Help Portal

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

Aplicaciones móviles de productividad de Citrix

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

iOS y Android

Idioma	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
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
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 los idiomas con escritura de derecha a izquierda

En la tabla siguiente se resume el texto disponible en idiomas de Europa Central en cada aplicación. X indica que la función está disponible para esa plataforma. No hay compatibilidad con idiomas de derecha a izquierda en dispositivos Windows.

Aplicación	iOS	Android
Citrix Secure Hub	X	X
Citrix Secure Mail	X	X
Citrix Secure Web	X	X

Aplicación	iOS	Android
QuickEdit	X	X

Cumplimiento del estándar FIPS 140-2

March 1, 2024

US National Institute of Standards and Technologies (Instituto nacional de estándares y tecnologías de EE. UU., NIST) emite los estándares Federal Information Processing Standard (estándares federales de procesamiento de la información, conocidos por sus siglas en inglés, FIPS). Estos estándares FIPS especifican los requisitos de seguridad para los módulos de cifrado que se utilizan en los sistemas de seguridad. La publicación FIPS 140-2 es la segunda versión de este estándar. Para obtener más información sobre los módulos FIPS 140 validados por el instituto NIST, consulte [NIST Computer Security Resource Center](#).

Todas las operaciones de cifrado de datos en reposo (data at rest) y datos en tránsito (data in transit) en iOS utilizan módulos de cifrado validados por FIPS. En Android, todas las operaciones de cifrado de datos en reposo (data at rest) utilizan módulos de cifrado validados por FIPS que proporciona Citrix o módulos de cifrado de la plataforma que proporciona el fabricante del dispositivo. Póngase en contacto con su representante de Citrix para obtener más información sobre los módulos de los fabricantes de dispositivos.

En los dispositivos Windows compatibles, todas las operaciones de cifrado de datos en reposo y datos en tránsito para la administración de dispositivos móviles (MDM) utilizan módulos de cifrado validados por FIPS que proporciona Microsoft.

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

El almacén MDX Vault cifra aplicaciones MDX empaquetadas y los datos en reposo asociados en dispositivos iOS y Android mediante módulos criptográficos validados por FIPS.

Acerca de Citrix Endpoint Management

March 1, 2024

Citrix Endpoint Management es una solución unificada de administración de dispositivos de punto final que incorpora todas las aplicaciones y dispositivos de punto final en una sola vista unificada para mejorar la seguridad y aumentar la productividad. Para ver una introducción general sobre la solución unificada de administración de dispositivos, consulte el resumen técnico de Citrix Tech Zone, [Citrix Endpoint Management](#).

Citrix Endpoint Management ofrece la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM).

Con las funciones de MDM que ofrece Citrix Endpoint Management, puede:

- Implementar aplicaciones y directivas de dispositivo.
- Obtener inventarios de activos.
- Llevar a cabo acciones en los dispositivos, como borrarlos.

Con las funciones de MAM que ofrece Citrix Endpoint Management, puede:

- Proteger las aplicaciones y los datos en los dispositivos móviles BYOD.
- Entregar aplicaciones móviles de empresa.
- Bloquear aplicaciones y borrar los datos que contengan.

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

- Administrar dispositivos de empresa a través de MDM
- Implementar aplicaciones y directivas de dispositivo
- Obtener un inventario de activos
- Borrar dispositivos
- Entregar aplicaciones móviles de empresa
- Bloquear aplicaciones y borrar los datos en los dispositivos

En la siguiente tabla, se resumen las funciones de Citrix Endpoint Management disponibles para MDM, MAM o MDM+MAM.

Funciones (por plataforma)	MDM (1)	MAM (2)	MDM+MAM
Android Enterprise:			
Disponibilidad de la inscripción de dispositivos	Sí	Sí	Sí

Funciones (por plataforma)	MDM (1)	MAM (2)	MDM+MAM
Disponibilidad de la autenticación de dominios	Sí	No	Sí
Disponibilidad de la autenticación con dominio y token de seguridad	No	No	Sí
Disponibilidad de la autenticación con certificados de cliente	No	Sí	Sí
Compatibilidad con la autenticación con certificado de cliente y dominio	No	No	Sí
Compatibilidad con el certificado de cliente y token de seguridad	No	No	Sí
Compatibilidad con proveedores de identidades de Azure AD	Sí	No	Sí
Compatibilidad con proveedores de identidades de Okta	Sí	No	Sí
Single Sign-On en aplicaciones SaaS nativas	Sí	No	Sí
Compatibilidad con Citrix Content Delivery Network para aplicaciones empresariales	Sí	Sí	Sí
Compatibilidad con Citrix Content Delivery Network para aplicaciones MDX	Sí	Sí	Sí

Funciones (por plataforma)	MDM (1)	MAM (2)	MDM+MAM
Compatibilidad con dispositivos compartidos mediante el aprovisionamiento de dispositivos Android Enterprise (COSU) dedicados	Sí	No	Sí
Android (heredado):			
Disponibilidad de la inscripción de dispositivos	Sí	Sí	Sí
Disponibilidad de la autenticación con dominio o dominio y token de seguridad	No	No	Sí
Disponibilidad de la autenticación con certificados de cliente	No	Sí	Sí
Compatibilidad con la autenticación con certificado de cliente y dominio	No	No	Sí
Compatibilidad con el certificado de cliente y token de seguridad	No	No	Sí
Compatibilidad con proveedores de identidades de Azure AD y Citrix	Sí	No	Sí
Compatibilidad con proveedores de identidades de Okta	Sí	No	Sí
Single Sign-On en aplicaciones SaaS nativas	Sí	No	Sí

Funciones (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
Chrome:			
Disponibilidad de la inscripción de dispositivos	Sí	No	Sí
Compatibilidad con autenticación de nombre de usuario y contraseña	Sí	No	Sí
iOS:			
Disponibilidad de la inscripción de dispositivos	Sí	Sí	Sí
Disponibilidad de la autenticación con dominio o dominio y token de seguridad	No	No	Sí
Disponibilidad de la autenticación con certificados de cliente	No	Sí	Sí
Compatibilidad con la autenticación con certificado de cliente y dominio	No	No	Sí
Compatibilidad con proveedores de identidades de Azure AD y Citrix	Sí	No	Sí

Funciones (por plataforma)	MDM (1)	MAM (2)	MDM+MAM
Compatibilidad con proveedores de identidades de Okta	Sí	No	Sí
Single Sign-On en aplicaciones SaaS nativas	Sí	No	Sí
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 en Apple Education	Sí	No	Sí
macOS:			
Disponibilidad de la inscripción de dispositivos	Sí	No	No
Compatibilidad con dominio o dominio y contraseña de un solo uso	Sí	No	No
Compatibilidad con URL de invitación y contraseña de un solo uso	Sí	No	No
Windows:			
Disponibilidad de la inscripción de dispositivos	Sí	No	No

Funciones (por plataforma)	MDM (1)	MAM (2)	MDM+MAM
Inscripción automática de dispositivos con Windows 10 o Windows 11 a través de la aplicación Citrix Workspace	Sí	No	No
Disponibilidad de la autenticación con dominio o dominio y token de seguridad	Sí	No	No
Disponibilidad de la autenticación con certificados de cliente	Sí	No	No
Compatibilidad con la autenticación con certificado de cliente y dominio	Sí	No	No
Autenticación federada a través del proveedor de identidades de Azure AD o Citrix	Sí	No	No
Compatibilidad con Citrix Content Delivery Network para aplicaciones empresariales	Sí	No	No
Integración en Workspace Environment Management (3)	Sí	No	No

Notas:

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

(2) La inscripción en MAM requiere NetScaler Gateway.

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

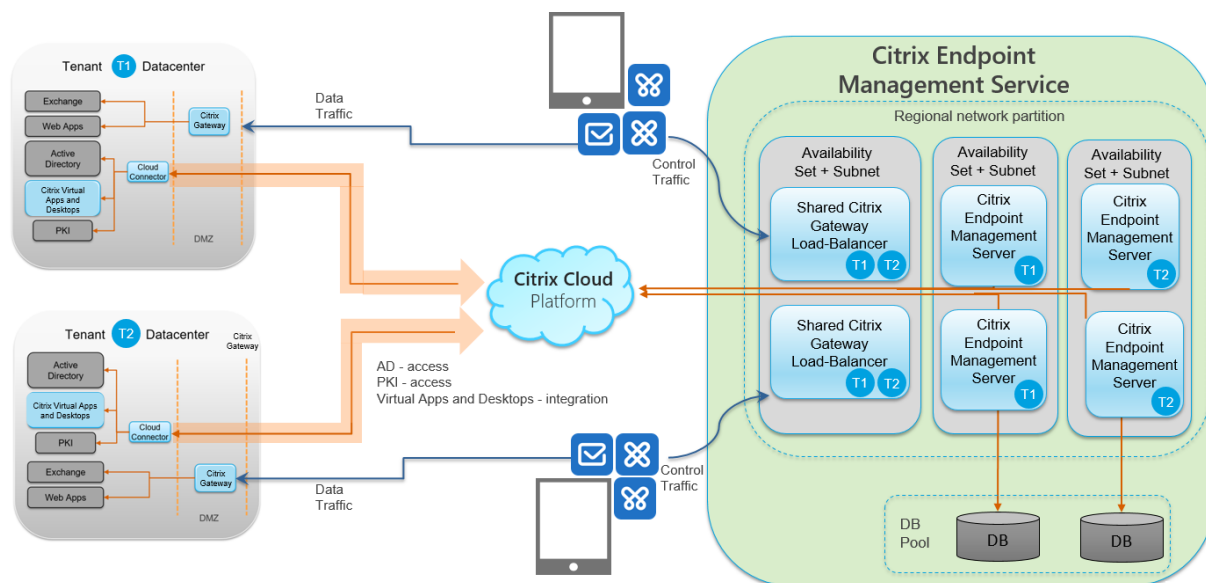
Para obtener más información, consulte [Modos de administración](#).

Arquitectura

Los requisitos de administración de dispositivos o de aplicaciones que tenga la organización son los que determinan los componentes de Citrix Endpoint Management que incluirá su arquitectura de Citrix Endpoint Management. Los componentes de Citrix Endpoint Management son módulos y se construyen unos sobre otros. Por ejemplo, su implementación incluye NetScaler Gateway:

- NetScaler Gateway proporciona a los usuarios acceso remoto a las aplicaciones móviles y realiza un seguimiento de los tipos de dispositivos de los usuarios.
- Citrix Endpoint Management es donde administra esas aplicaciones y dispositivos.

El diagrama siguiente ofrece una vista general de la arquitectura que tendría una implementación de Citrix Endpoint Management en la nube; también se ilustra la integración en su centro de datos.



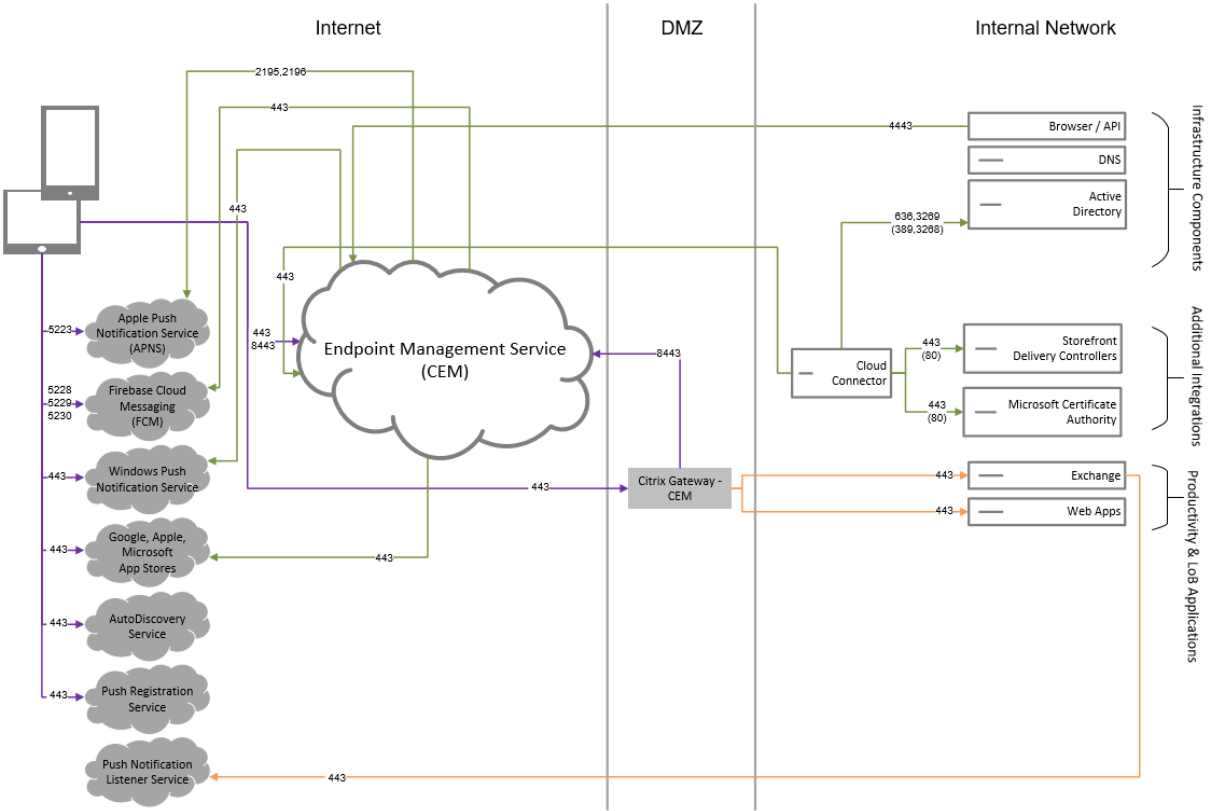
Las siguientes subsecciones contienen diagramas de arquitectura de referencia para:

- Citrix Endpoint Management
- Componentes opcionales como entidades de certificación externas, el conector de Citrix Endpoint Management para Exchange ActiveSync y el flujo de tráfico de MAM de Intune y MDM+MAM de Citrix Endpoint Management.

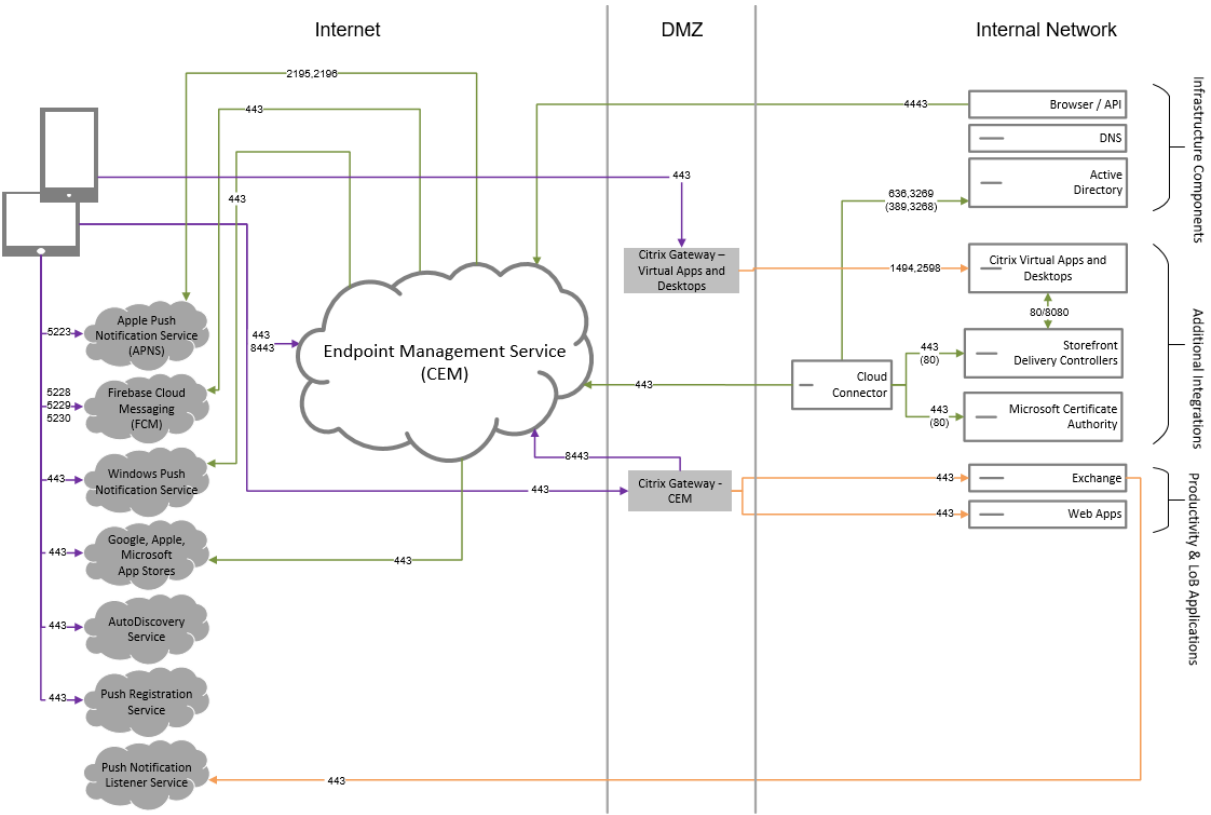
Para obtener más información acerca de los requisitos de Citrix ADC y NetScaler Gateway, consulte la documentación de productos Citrix en <https://docs.citrix.com/>.

Arquitectura de referencia para componentes principales

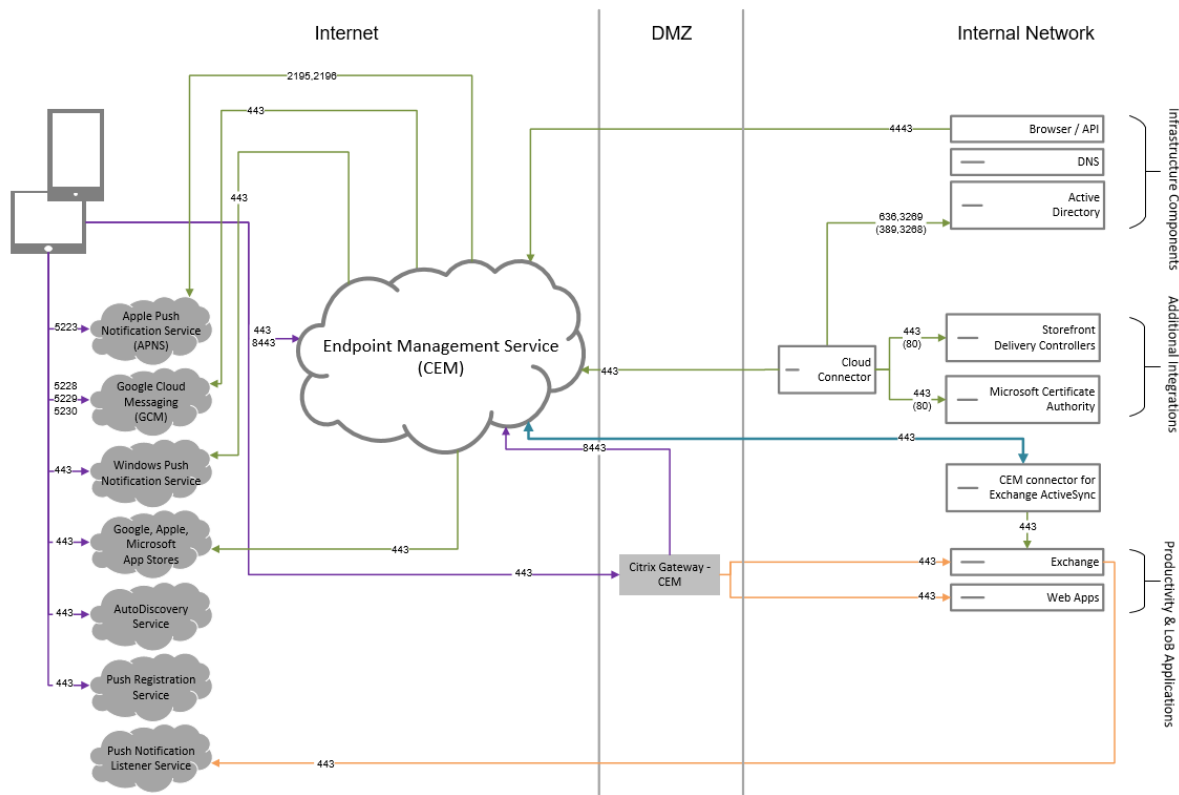
Para obtener información detallada acerca de los requisitos de puertos, consulte [Requisitos del sistema](#).



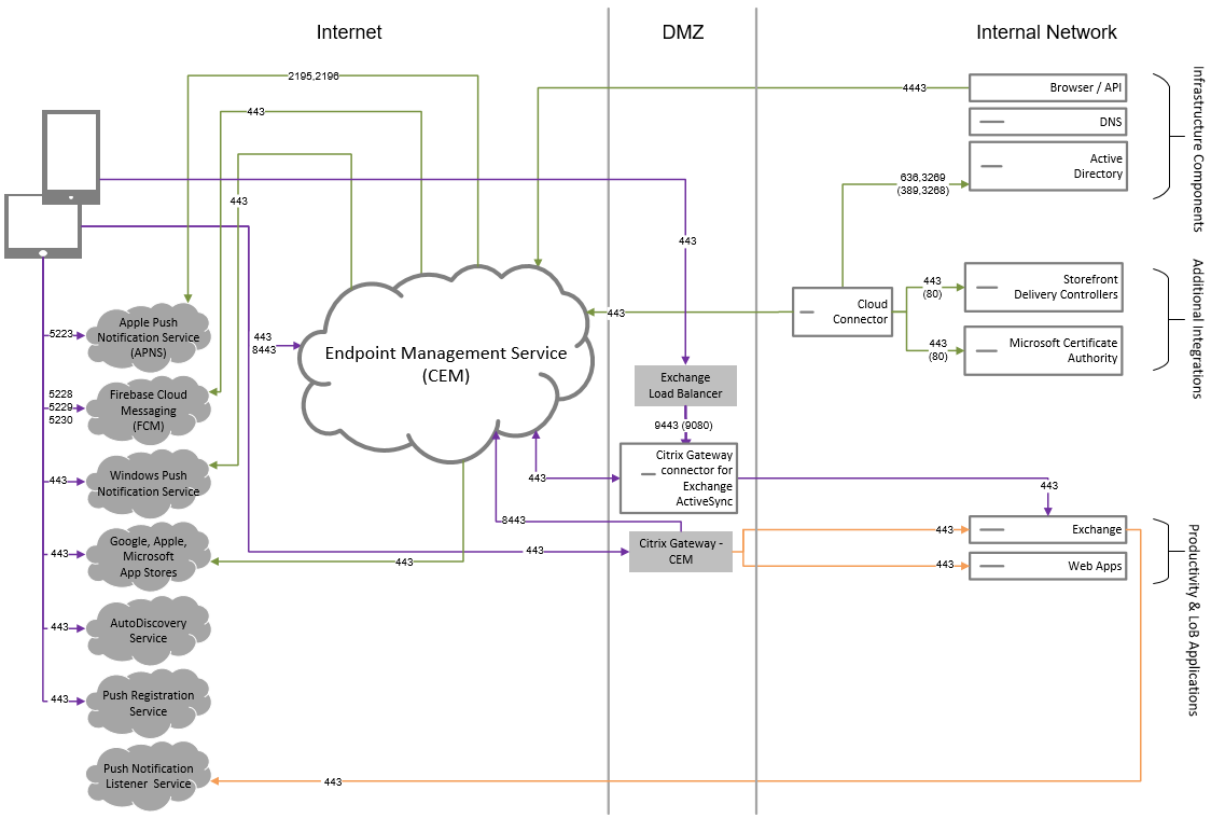
Arquitectura de referencia con Citrix Virtual Apps and Desktops



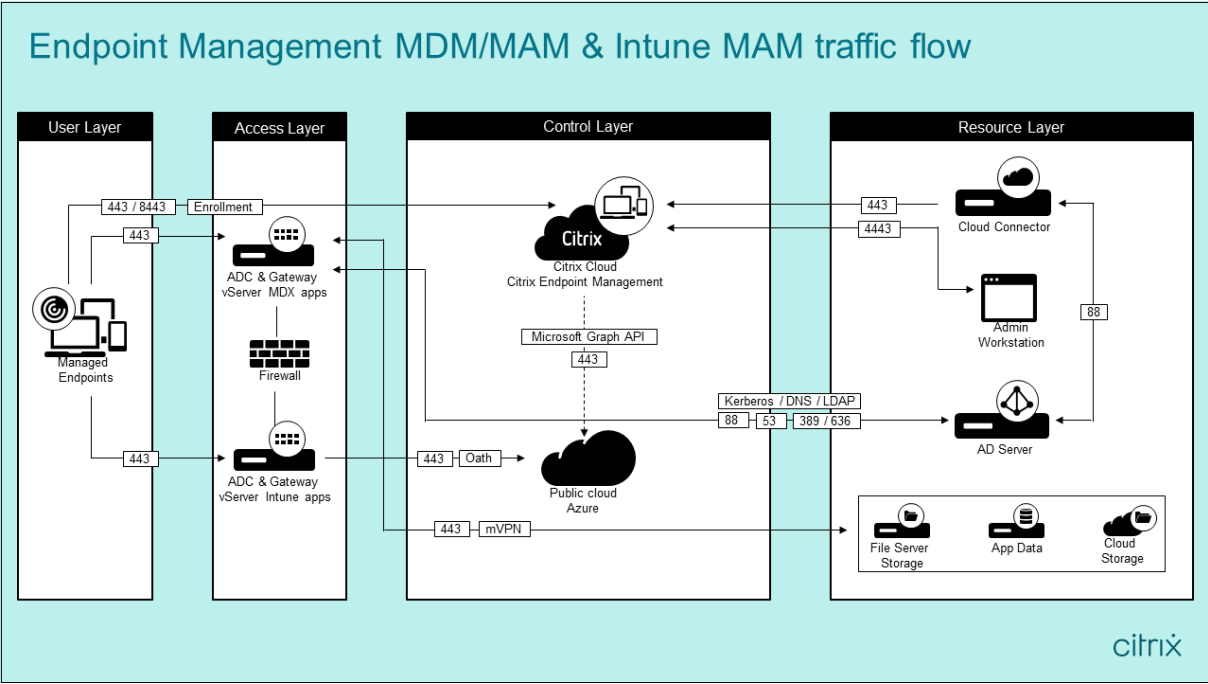
Arquitectura de referencia con el conector de Citrix Endpoint Management para Exchange ActiveSync



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



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



Ubicaciones de recursos

Coloque las ubicaciones de recursos donde mejor se adapten a las necesidades de su negocio. Por ejemplo, en una nube pública, una sucursal, una nube privada o un centro de datos. A continuación, se presentan los factores que determinan la selección de la ubicación:

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

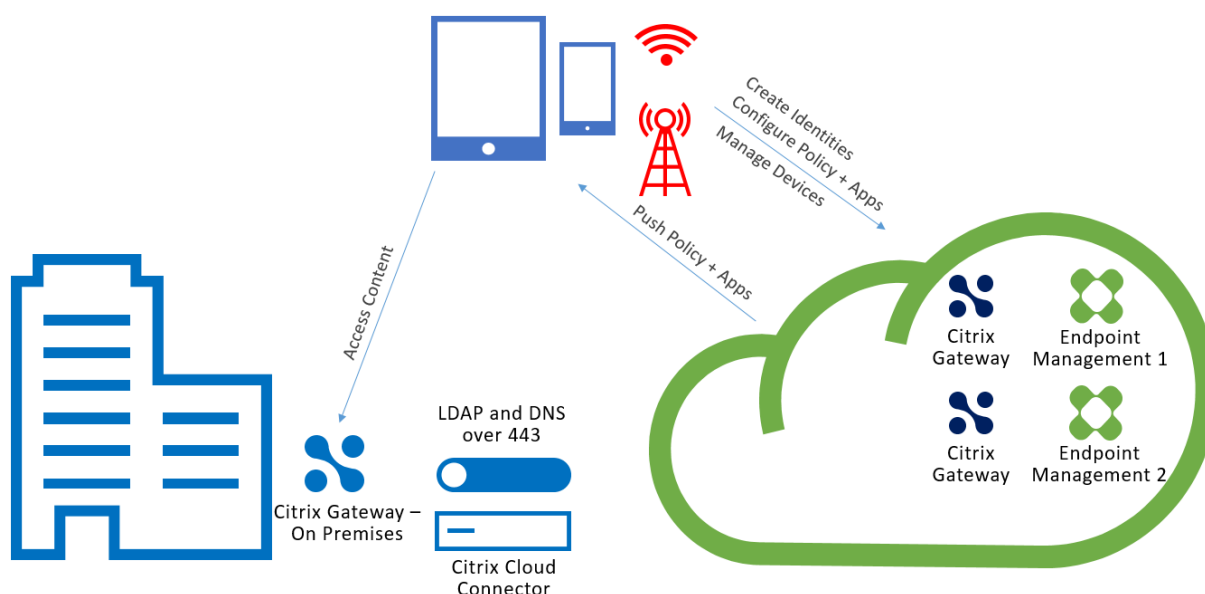
Puede crear cuantas ubicaciones de recursos quiera. Por ejemplo, puede:

- Crear una ubicación de recursos en el centro de datos para la oficina principal, en función de los suscriptores y las aplicaciones que necesitan situarse cerca de los datos.
- Agregar una ubicación de recursos separada para usuarios globales en una nube pública. O crear ubicaciones de recursos independientes en cada una de las sucursales para entregar aplicaciones que funcionan mejor cuando se sitúan cerca de los trabajadores de las sucursales.
- Agregar una ubicación de recursos adicional en otra red, que proporcione aplicaciones de carácter restringido. Esta estructura ofrece la ventaja de una visibilidad restringida para otros recursos y suscriptores, sin la necesidad de ajustar las demás ubicaciones de recursos.

Cloud Connector

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

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



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

Cloud Connector recibe la carga solo durante la inscripción de dispositivos. Para obtener más información, consulte [Consideraciones de escala y tamaño para los Cloud Connectors](#).

Una solución que ofrezca la administración de aplicaciones móviles (MAM) requiere una red micro VPN proporcionada por un NetScaler Gateway local. En este caso:

- Los siguientes componentes residen en el 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 (“on premises”).

Componentes Citrix Endpoint Management

Consola de Citrix Endpoint Management. Utilice la consola de administrador de Citrix Endpoint Management para configurar Citrix Endpoint Management. Para obtener más información sobre cómo usar la consola de Citrix Endpoint Management, consulte los artículos de [Citrix Endpoint Management](#). Citrix le notificará cuando los artículos “Novedades” de Citrix Endpoint Management se actualicen para una nueva versión.

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

- En Citrix Endpoint Management, el cliente de asistencia remota, llamado Citrix Endpoint Management Remote Support, no está disponible.

- Citrix no ofrece soporte a 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 asistencia** en la consola de Citrix Endpoint Management. Al hacerlo, debe hacer clic en **Descargar todo**.

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

- El SDK de administración de aplicaciones móviles (MAM) proporciona funcionalidad MDX que no cubren las plataformas iOS y Android. Puede habilitar MDX y proteger las aplicaciones iOS o Android. Puede hacer que esas aplicaciones estén disponibles en un almacén interno o en tiendas públicas de aplicaciones. Consulte [SDK de aplicaciones MDX](#).

Aplicaciones móviles de productividad. Las aplicaciones móviles de productividad desarrolladas por Citrix ofrecen un conjunto de herramientas de productividad y comunicación dentro del entorno de Citrix Endpoint Management. Las directivas de la empresa protegen esas aplicaciones. Para obtener más información, consulte [Aplicaciones móviles de productividad](#).

Conector de Citrix Endpoint Management para Exchange ActiveSync. El conector de Citrix Endpoint Management para Exchange ActiveSync ofrece acceso seguro al correo electrónico para los usuarios que usan aplicaciones móviles nativas de correo electrónico. El conector para Exchange ActiveSync ofrece el filtrado de ActiveSync en el nivel de servicio de Exchange. Así, el filtrado solo se produce una vez que el correo haya llegado al servicio de intercambio, en lugar de en cuanto entre en el entorno de Citrix Endpoint Management. El conector no requiere el uso de NetScaler Gateway. Puede implementar el conector sin cambiar la redirección del tráfico existente de ActiveSync. Para obtener más información, consulte [Conector de Citrix Endpoint Management para Exchange ActiveSync](#).

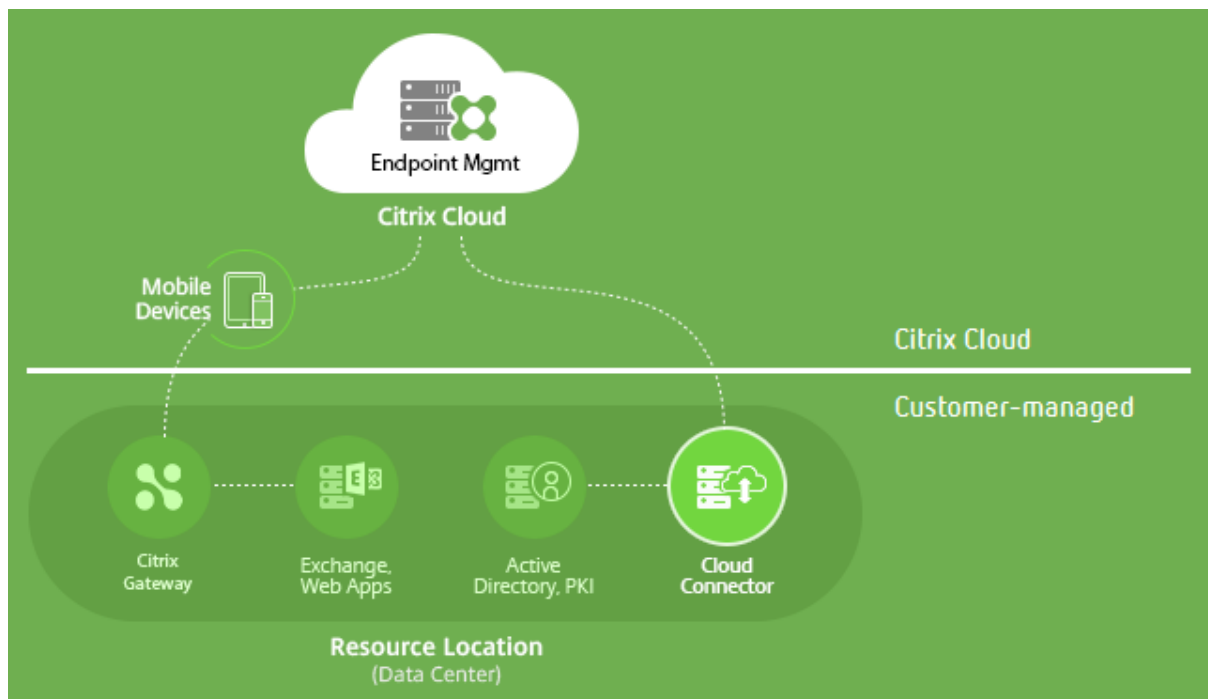
Conector de NetScaler Gateway para Exchange ActiveSync El conector de NetScaler Gateway para Exchange ActiveSync ofrece acceso seguro al correo electrónico para los usuarios que usan aplicaciones móviles nativas de correo electrónico. El conector para Exchange ActiveSync ofrece el filtrado de ActiveSync en el perímetro. El filtrado utiliza NetScaler Gateway como proxy para el tráfico de ActiveSync. Así, el componente de filtrado se encuentra en la ruta de tráfico del correo: lo intercepta 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](#).

Información técnica general sobre la seguridad de Citrix Endpoint Management

Citrix Cloud administra el plano de control para 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 arrendatario. El servicio de nube se integra en el centro de datos

del cliente a través de Citrix Cloud Connector. Los clientes de Citrix Endpoint Management que usan Cloud Connector suelen administrar NetScaler Gateway en sus centros de datos.

En la siguiente imagen se ilustra el servicio y sus límites de seguridad.



La información de esta sección:

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

Para obtener información acerca de la tecnología utilizada por Citrix Endpoint Management para ofrecer una seguridad integral, de extremo a extremo, consulte [Security and Productivity for the Mobile Enterprise](#).

Flujo de datos

El plano de control tiene acceso de lectura limitado a los objetos de usuario y grupo. Esos objetos residen 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 empresa (como el correo electrónico, la intranet y el tráfico de las aplicaciones Web) se transfieren 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 se compone de una combinación de componentes de arrendatario único y multiarrendatario. Sin embargo, según la arquitectura del servicio, los metadatos de clientes de cada arrendatario siempre se almacenan por separado y se protegen con 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 coteja esas credenciales con un directorio en el directorio del cliente a través de una conexión segura y las valida.
- **Credenciales de administrador:** Los administradores se autentican en Citrix Cloud, que utiliza el sistema de inicio de sesión de Citrix Online. Ese proceso genera un token web JSON (JWT) firmado y de un solo uso, lo que permite que el administrador acceda al servicio.
- **Credenciales de Active Directory:** El plano de control requiere credenciales vinculadas para leer los metadatos de usuario en Active Directory. Esas credenciales se cifran con el cifrado AES-256 y se guardan en una base de datos por arrendatario.

Consideraciones sobre la implementación

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

Más recursos

Se recomienda a los clientes que consulten los boletines de seguridad relacionados con sus productos Citrix. Para obtener información sobre boletines de seguridad nuevos y actualizados, consulte [Citrix Security Bulletins](#). Igualmente, considere la posibilidad de suscribirse para recibir alertas en [Alert Settings](#).

Consulte los siguientes recursos para obtener más información acerca de la 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 en el software Mobile Threat Defense

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

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

- Proteger contra malware, phishing, ataques a redes y ataques de tipo “Man in the middle”
- Determinar el estado de conformidad del dispositivo
- Determinar los niveles de riesgo
- Realizar acciones basadas en directivas para proteger aplicaciones, datos, dispositivos y redes móviles

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

- [Check Point](#)
- [Lookout](#)
- [Wandera](#)
- [Zimmerium](#)

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

Integración de Citrix Endpoint Management con Microsoft Endpoint Manager

March 1, 2024

La integración de Citrix Endpoint Management en Microsoft Endpoint Manager (MEM) agrega el valor de una red micro VPN de Citrix Endpoint Management a las aplicaciones compatibles con Microsoft Intune, como el explorador web Microsoft Edge.

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

Esta versión admite los siguientes casos de uso:

- MAM de Intune con MDM+MAM de Citrix Endpoint Management.

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

Importante:

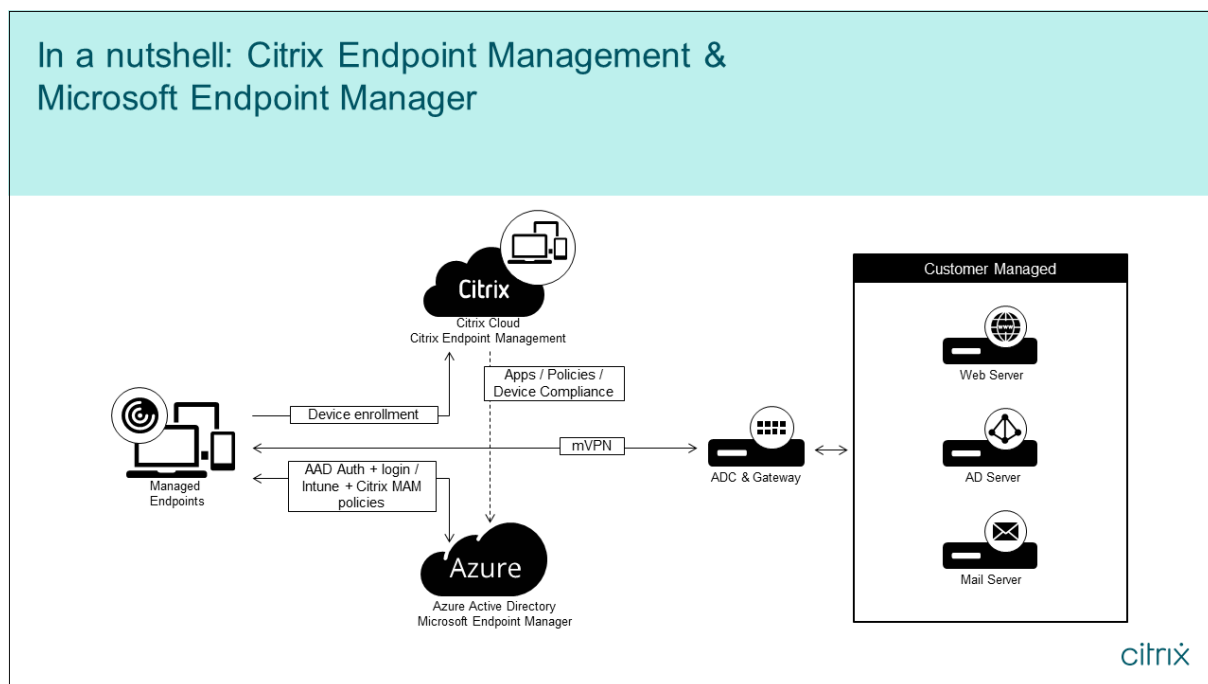
Para este caso de uso, Citrix Secure Mail no admite la integración en Intune. Citrix Secure Mail solo funciona con dispositivos inscritos en modo MDX.

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

Para obtener una guía gráfica e intuitiva para configurar la integración de Citrix Endpoint Management en MEM, consulte [Guía de introducción](#).

Para obtener información sobre la integración en el acceso condicional con Azure AD, consulte [Integración en el acceso condicional de Azure AD](#).

Este diagrama ofrece una descripción general de la integración de Citrix Endpoint Management en Microsoft Endpoint Manager.



Requisitos del sistema

Habilitación de MDX

- [SDK de MAM](#)

o bien

- [MDX Toolkit](#)

Microsoft

- Acceso a Azure Active Directory (con privilegios de administrador de arrendatarios)
- Arrendatario compatible con 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> (puerto 53 y 443)

Requisitos previos

- **Explorador Microsoft Edge:** Mobile Apps SDK está integrado en la aplicación del explorador Microsoft Edge para iOS y Android. Para obtener más información sobre Microsoft Edge, consulte la [documentación de Microsoft Edge](#).
- **Cuenta de Citrix Cloud:** Si quiere registrar una cuenta de Citrix y solicitar una prueba de Citrix Endpoint Management, póngase en contacto con un representante de Ventas de Citrix. Cuando tenga todo 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 a Azure AD. Puede utilizar cualquier servicio de correo electrónico gratuito.

- **Certificados APNs para iOS:** Debe configurar un certificado APNs para iOS. Para obtener más información sobre la configuración de estos certificados, consulte esta entrada del blog de Citrix: [Creating and Importing APNs Certificates](#).
- **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](#).

Configurar NetScaler Gateway

Si va a configurar una nueva implementación de Citrix Endpoint Management, instale uno de estos dispositivos NetScaler Gateway:

- NetScaler Gateway, serie VPX 3000 o una posterior
- NetScaler Gateway MPX o una instancia de SDX dedicada

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

- Configure NetScaler Gateway con una interfaz de administración y una IP de subred.
- Utilice TLS 1.2 para todas las comunicaciones de cliente a servidor. Para obtener información sobre la configuración de TLS 1.2 para NetScaler Gateway, consulte [CTX247095](#).

Si utiliza la integración de Citrix Endpoint Management en MEM con una implementación MDM+MAM de Citrix Endpoint Management, configure dos dispositivos Citrix Gateway. El tráfico de las aplicaciones MDX se dirige a través de un NetScaler Gateway. El tráfico de las aplicaciones Intune se redirige a través del otro dispositivo NetScaler Gateway. Configure:

- Dos IP públicas.
- Si quiere, una dirección IP de red traducida.
- Dos nombres DNS. Ejemplo: <https://mam.company.com>.
- Dos certificados SSL públicos. Configure los certificados que coincidan con el nombre DNS público reservado o utilice certificados comodín.
- Un equilibrador de carga de MAM con una dirección IP de RFC 1918 interna y no redirigible.
- 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 autenticuen, las aplicaciones solicitan permisos de aplicación que Microsoft Graph indica al usuario. Tras dar su consentimiento a las solicitudes de permisos, la aplicación puede acceder a los recursos y las API pertinentes. Algunas aplicaciones requieren el consentimiento del administrador global de Microsoft Azure AD. Para estos permisos delegados, el administrador global debe conceder a Citrix Cloud el permiso de solicitar tokens. Tras ello, los tokens habilitan estos permisos. Para obtener más información, consulte la [referencia sobre permisos de Microsoft Graph](#).

- **Permiso Iniciar sesión y leer el perfil del usuario:** Este permiso permite a los usuarios iniciar sesión y conectarse a Azure AD. Citrix no puede ver las credenciales de usuario.
- **Permiso Leer los perfiles básicos de todos los usuarios:** La aplicación lee las propiedades del perfil para los usuarios de la organización. Las propiedades incluyen el nombre simplificado, el nombre y el apellido, la dirección de correo electrónico y la foto de los usuarios de la organización.
- **Permiso Leer todos los grupos:** Este permiso permite que los grupos de Azure AD se especifiquen para la asignación de aplicaciones y directivas.

- **Permiso Acceder al directorio en nombre del usuario con la sesión iniciada:** Este permiso verifica la suscripción de Intune y habilita las configuraciones de NetScaler Gateway y VPN.
- **Permiso Leer y escribir en aplicaciones de Microsoft Intune:** La aplicación puede leer y escribir lo siguiente:
 - Propiedades administradas por Microsoft
 - Asignaciones de grupos y estado de las aplicaciones
 - Configuración 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 use para comunicarse con Azure AD e Intune.
- No tener el rol de administrador de Citrix. En vez de ello, el administrador de Citrix asigna cuentas de Azure AD a los usuarios con los privilegios de administrador de aplicaciones de Intune adecuados. Entonces, el administrador de Intune cumple la función de administrador de Citrix Cloud para administrar Intune desde Citrix Cloud.

Nota:

Citrix solo utiliza la contraseña del administrador global de Intune durante la instalación y redirige la autenticación a Microsoft. Citrix no puede acceder a la contraseña.

Para configurar la integración de Citrix Endpoint Management en MEM

1. Inicie sesión en el sitio de Citrix Cloud y solicite una versión de prueba para Citrix Endpoint Management.
2. Un ingeniero de ventas organizará una reunión para incorporarlo como usuario. Dígle que quiere integrar Citrix Endpoint Management en MEM. Una vez aprobada la solicitud que haya realizado, haga clic en **Administrar**.
3. Desde aquí puede hacer clic en el icono de engranaje situado en la parte superior derecha del sitio web, o bien puede hacer clic en **Configurar sitio**.
4. Siga el enlace del primer paso a la página **Administración de acceso e identidad**.
5. Haga clic en **Conectar** para conectar la instalación de Azure AD.
6. Escriba la dirección URL de inicio de sesión única que usa el administrador de Azure AD para iniciar sesión y, a continuación, haga clic en **Confirmar**.
7. Agregue una cuenta de administrador global de Azure AD y acepte la solicitud de permisos.

8. Confirme que la 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 al 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 quiere agregar. Haga clic en **Invitar** y conceda **acceso completo** o **acceso personalizado** al usuario antes de hacer clic en **Enviar invitación**.

Nota:

Citrix Endpoint Management requiere las siguientes reglas para el **acceso personalizado**: Library y Citrix Endpoint Management.

Una vez agregado, 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, debe 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 todo está configurado correctamente, la página muestra que el administrador de Azure AD ha iniciado sesión y que la suscripción de Intune es válida.

Para configurar NetScaler Gateway para micro VPN

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

En primer lugar, configure Azure AD para que se sincronice con Active Directory local. Este paso es necesario para 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 **Configure Micro VPN**.
3. Escriba un nombre para el servicio micro VPN y la URL externa de NetScaler Gateway y, a continuación, haga clic en **Siguiente**.

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

4. Haga clic en **Download Script**. El archivo ZIP contiene un archivo Léame con instrucciones para implementar el script. Aunque puede guardar el proceso y salir a partir de este punto del procedimiento, la micro VPN no estará configurada hasta que ejecute el script en la instalación de NetScaler Gateway.

Nota:

Cuando termine el proceso de configuración de NetScaler Gateway, si ve un estado de autenticación OAuth que no sea “COMPLETO”, consulte la sección “Solucionar problemas”.

Para configurar la administración de dispositivos

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

Nota:

El valor predeterminado de la consola es MDM de Intune. Para usar Intune como su proveedor de MDM, consulte la [documentación de Microsoft Intune](#).

1. Desde la consola de Citrix Cloud, en la integración de Citrix Endpoint Management en MEM, haga clic en **Manage**. Junto a **Device Management - Optional**, haga clic en **Configure MDM**.
2. Introduzca un nombre de sitio único, seleccione la región de Cloud más cercana y, a continuación, haga clic en **Request a Site**. Recibirá un mensaje de correo electrónico cuando el sitio esté listo.
3. Haga clic en **OK** para cerrar la solicitud. Seleccione una ubicación de Active Directory para asociarla al sitio o cree una ubicación de recursos y, a continuación, haga clic en **Siguiente**.
4. Haga clic en **Download Cloud Connector** y siga las instrucciones que aparecen en pantalla para instalar Citrix Cloud Connector. Después de la instalación, haga clic en **Probar conexión** para verificar la conexión entre Citrix Cloud y el Cloud Connector.
5. Haga clic en **Guardar y salir** para finalizar el proceso. Aparecerá la ubicación de recursos. Al hacer clic en **Finalizar**, volverá a la pantalla de configuración.
6. Ahora ya puede acceder a la consola de Citrix Endpoint Management desde el icono del sitio. Desde aquí, puede realizar tareas de administración de MDM y asignar directivas de dispositivo. Consulte [Directivas de dispositivo](#) para obtener más información acerca de las directivas de dispositivo.

Configurar aplicaciones administradas de Intune para entrega a dispositivos

Para configurar las aplicaciones administradas de Intune para entrega:

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

Agregar aplicaciones de Microsoft Intune a la biblioteca de Citrix Cloud

Para cada aplicación que quiera agregar:

1. En 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 azul del signo + situado en la parte superior derecha y, a continuación, haga clic en **Add a Mobile app**.
3. Si tiene Android Enterprise configurado en la consola de Citrix Endpoint Management, seleccione **Aplicaciones de Microsoft Intune** en **Elegir una aplicación**. Seleccione una plantilla de aplicación a personalizar o haga clic en **Upload my own App**.

Citrix suministra las plantillas de aplicación existentes, cada una de las cuales incluye un conjunto de directivas preconfiguradas. Se aplican las siguientes directivas a las aplicaciones que carguen los clientes:

- **Archivos MDX:** Incluye aplicaciones habilitadas para el SDK de MAM o aplicaciones empaquetadas con MDX, como:
 - Directivas de protección de aplicaciones de Intune y las directivas MDX predeterminadas en el paquete
 - Aplicaciones de tiendas públicas, como las directivas de protección de aplicaciones de Intune y las directivas MDX predeterminadas que coinciden con el ID del bundle o el ID del paquete
- **Archivos IPA:** Directivas de protección de aplicaciones de Intune.
- **Archivos APK:** Directivas de protección de aplicaciones de Intune.

Nota:

Si la aplicación no se empaqueta con Intune, la protección de aplicaciones Intune no se aplica.

4. Haga clic en **Upload my own App** y cargue su archivo MDX o Intune empaquetado.
5. Introduzca un nombre y una descripción para la aplicación, elija si la aplicación será opcional u obligatoria y, a continuación, haga clic en **Siguiente**.
6. Configure los parámetros de la aplicación. Las siguientes configuraciones permiten que los contenedores de Intune y Citrix Endpoint Management transfieran datos entre sí.
 - **Allow apps to receive data from other apps** (Permitir que las aplicaciones reciban datos de otras aplicaciones): Seleccione **Policy managed apps** (Aplicaciones administradas por directivas).
 - **Allow app to transfer data to other apps** (Permitir que la aplicación transfiera datos a otras aplicaciones): Seleccione **All apps** (Todas las aplicaciones).

- **Restrict cut, copy, paste with other apps** (Restringir cortar, copiar y pegar con otras aplicaciones): Seleccione **Policy managed apps (Aplicaciones administradas por directivas)**.
7. Configure los repositorios de almacenamiento para los datos guardados. En **Select which storage services corporate data can be saved to** (Seleccionar en qué servicios de almacenamiento se pueden guardar los datos corporativos), seleccione **LocalStorage**.
 8. Opcional: Establezca 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**.

Es posible que el proceso de configuración de la aplicación tarde unos instantes. Una vez completado el proceso, un mensaje indica 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 los grupos de usuarios pertinentes y haga clic para agregarlos. No puede agregar usuarios individuales.
 12. Cuando haya agregado todos los grupos, haga clic en la X para cerrar la ventana.

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 Active Directory local.

Agregar aplicaciones de Android Enterprise a la biblioteca de Citrix Cloud

Para agregar aplicaciones de Android Enterprise a la biblioteca de Citrix Cloud y establecer directivas de protección de aplicaciones de Intune, configure su entorno de nube de esta manera:

- Federe 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. Compruebe que los dispositivos de Android Enterprise se hayan inscrito en MDM+MAM. Para configurar Android Enterprise, consulte [Android Enterprise](#).

Con este procedimiento, se agregan 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 quiera agregar:

1. En 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 azul del signo + situado en la parte superior derecha y, a continuación, haga clic en **Add a Mobile app**.

3. En **Elegir una aplicación**, seleccione **Aplicaciones de Android Enterprise**.
4. Busque una aplicación y apruébela en la ventana de Google Play Store administrado. Una vez cerrada la ventana de Google, haga clic en **Siguiente**.
5. Agregue los detalles de la aplicación y, a continuación, haga clic en **Siguiente**.
6. Si buscó y seleccionó una aplicación móvil de productividad de Citrix, puede configurar directivas de micro VPN. Una vez configuradas dichas directivas, haga clic en **Siguiente**.
7. Configure las directivas de protección de aplicaciones de Intune. Haga clic en **Siguiente**.
8. Configure los parámetros de la aplicación. Las siguientes configuraciones permiten que los contenedores de Intune y Citrix Endpoint Management transfieran datos entre sí.
 - **Allow apps to receive data from other apps** (Permitir que las aplicaciones reciban datos de otras aplicaciones): Seleccione **Policy managed apps** (Aplicaciones administradas por directivas).
 - **Allow app to transfer data to other apps** (Permitir que la aplicación transfiera datos a otras aplicaciones): Seleccione **All apps** (Todas las aplicaciones).
 - **Restrict cut, copy, paste with other apps** (Restringir cortar, copiar y pegar con otras aplicaciones): Seleccione **Policy managed apps (Aplicaciones administradas por directivas)**.
9. Configure los repositorios de almacenamiento para los datos guardados. En **Select which storage services corporate data can be saved to** (Seleccionar en qué servicios de almacenamiento se pueden guardar los datos corporativos), seleccione **LocalStorage**.
10. Opcional: Establezca 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**.

Es posible que el proceso de configuración de la aplicación tarde unos instantes. Una vez completado el proceso, un mensaje indica 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 la tienda pública de aplicaciones.
12. Para asignar grupos de usuarios a la aplicación, haga clic en **Asignar usuarios**.
13. En el cuadro de búsqueda, busque los grupos de usuarios pertinentes y haga clic para agregarlos. No puede agregar usuarios individuales.
14. Cuando haya agregado todos los grupos, haga clic en la X para cerrar la ventana.

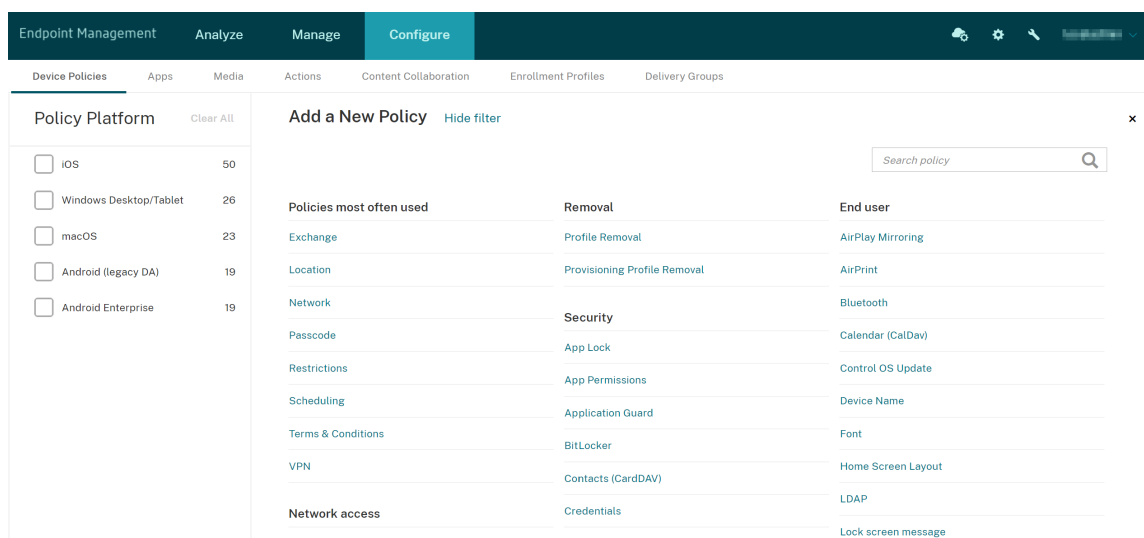
Es posible que vea un error al agregar grupos de usuarios. Este error se produce cuando el grupo de usuarios no se ha sincronizado con Active Directory local.

Controlar el tipo de datos transferidos entre aplicaciones administradas

Gracias a directivas de Citrix Endpoint Management, puede controlar el tipo de datos incluidos en contenedores de Citrix Endpoint Management o Intune que se pueden transferir entre aplicaciones administradas. Puede configurar una directiva Restricciones para permitir solo los datos etiquetados como “corporativos”. Configure una directiva Configuración de aplicaciones para etiquetar los datos.

Para configurar la directiva 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 nueva directiva**.



3. En la lista de directivas, haga clic en **Restricciones**.
4. En la página **Información de 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**, **desactive** la opción **Documentos de aplicaciones administradas en aplicaciones no administradas**. Al **desactivar** esta opción, se **desactivan** también las opciones **Las aplicaciones no administradas pueden leer contactos administrados** y **Las aplicaciones administradas pueden registrar contactos no administrados**. Haga clic en **Siguiente**.
7. Haga clic en **Siguiente** hasta que aparezca el botón **Guardar**. Haga clic en **Guardar**.

Configure la directiva 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**. Aparecerá la página **Agregar nueva directiva**.
3. En la lista de directivas, haga clic en **Configuración de aplicaciones**.
4. En la página **Información de 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 al **Contenido del diccionario**:

```
1 <dict>
2   <key>IntuneMAMUPN</key>
3   <string>${
4     user.userprincipalname }
5   </string>
6 </dict>
7 <!--NeedCopy-->
```

8. Haga clic en **Diccionario de comprobación**.
9. Haga clic en **Siguiente**.
10. Haga clic en **Guardar**.

Configurar grupos de entrega para las directivas de aplicaciones y dispositivos

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**. Aparecerá 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 y, a continuación, haga clic en **Siguiente**. 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**.

The screenshot shows the 'Delivery Groups' configuration page in Citrix Endpoint Management. The left sidebar has a navigation menu with the following items: 1 Delivery Group Info, 2 Assignments (selected), 3 Resource (optional), Policies, Apps, Media, Actions, ShareFile, Enrollment Profile, and 4 Summary. The main content area is titled 'Assignments' and includes a sub-header 'Manage user assignments *'. There are two radio button options: 'In Endpoint Management' (selected) and 'In Citrix Cloud'. Below these are two columns of text explaining the differences. Under 'In Endpoint Management', it says: 'Select this if you only need mobility management. Delivery groups assignments managed here will not be visible in Citrix Cloud.' Under 'In Citrix Cloud', it says: 'Use this if you plan on delivering additional services such as Virtual Apps, Sharefile, etc. Delivery Groups assignments can be managed through Citrix Cloud.' Below the radio buttons are two input fields: 'Select domain' and 'Include user groups' with a search button. At the bottom, there are radio buttons for 'Or' and 'And', a toggle for 'Deploy to anonymous user', and links to 'Filter by User Properties' and 'Filter by Device Properties'.

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

- **Seleccionar dominio:** En la lista, seleccione el dominio del que se elegirá a los usuarios.
- **Incluir grupos de usuarios:** Realice una de las siguientes acciones:
 - En la lista de grupos de usuarios, haga clic en los grupos a agregar. Los grupos seleccionados aparecerán en la lista **Grupos de usuarios seleccionados**.
 - Haga clic en **Buscar** para ver una lista de todos los grupos de usuarios del 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** situada junto a cada uno de los grupos que quiera quitar.
- Haga clic en **Buscar** para ver una lista de todos los grupos de usuarios del dominio seleccionado. Desplácese por la lista y desmarque la casilla de cada grupo que quiera 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 desmarque la casilla de cada grupo que quiera 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 obligatorias** o **Aplicaciones opcionales**. Haga clic en **Siguiente**.
- 9. Opcionalmente, configure los parámetros de las páginas **Medios**, **Acciones** e **Inscripciones**. También puede aceptar los valores predeterminados de cada página y hacer clic en **Siguiente**.
- 10. En la página **Resumen**, revise la configuración del grupo de entrega y haga clic en **Guardar** para crearlo.

Al publicar la aplicación en la consola de Intune, seleccione **Forzar administración de la aplicación**. A los usuarios de dispositivos no supervisados se les pide que autoricen 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

Ahora Citrix Secure Mail admite varias configuraciones. Puede empaquetar Citrix Secure Mail en un contenedor MAM de Intune que se conecte a un servidor local de Exchange. Puede conectar Citrix Secure Mail a cuentas alojadas de Exchange u Office 365. Sin embargo, esta versión no admite la autenticación basada en certificados, por lo que utilice LDAP en su lugar.

Importante:

Para utilizar Citrix Secure Mail en el modo MDX, debe usar MDM+MAM de Citrix Endpoint Management.

Citrix Secure Mail también rellena automáticamente los nombres de usuario. Para habilitar esta función, debe configurar las siguientes directivas personalizadas.

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Propiedades de 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 simplificado**, escriba `xms.store.idpuser_attrs`. Haga clic en **Guardar**.

4. Haga clic en **Propiedades de cliente** y, a continuación, haga clic 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 haga clic en **Guardar**.

Los siguientes pasos solo se aplican a los dispositivos iOS.

7. Vaya a **Configurar > Directivas de dispositivo**, haga clic en “Agregar” y, a continuación, seleccione la directiva **Configuración de aplicaciones**.
8. Escriba 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, indique el ID de paquete de la aplicación Citrix Secure Mail.
9. En el cuadro **Contenido del diccionario**, escriba el texto siguiente.

```
1 <dict>
2
3 <key>XenMobileUserAttributes</key>
4
5 <dict>
6
7 <key>userPrincipalName</key>
8
9 <string>${
10   user.userprincipalname }
11 </string>
12
13 <key>email</key>
14
15 <string>${
16   user.mail }
17 </string>
18
19 <key>displayName</key>
20
21 <string>${
22   user.displayName }
23 </string>
24
25 <key>sAMAccountName</key>
26
27 <string>${
28   user.samaccountname }
29 </string>
```

```
30
31 <key>aadupn</key>
32
33 <string>${
34   user.id_token.upn }
35 </string>
36
37 <key>aadtid</key>
38
39 <string>${
40   user.id_token.tid }
41 </string>
42
43 </dict>
44
45 <key>IntuneMAMUPN</key>
46
47 <string>${
48   user.id_token.upn }
49 </string>
50
51 </dict>
```

10. Desmarque la casilla **Escritorio/tableta Windows** y, a continuación, haga clic en **Siguiente**.
11. Seleccione los grupos de usuarios a los que quiera implementar la directiva. A continuación, haga clic en **Guardar**.

Solución de problemas

Problemas generales

Problema: Al abrir una aplicación, aparece el mensaje de error “Se requiere una directiva de aplicación”.

Solución: Agregue directivas en la API de Microsoft Graph.

Problema: Tiene conflictos de directiva.

Solución: Solo se permite una directiva por aplicación.

Problema: La aplicación no se puede conectar a recursos internos.

Solución: Compruebe que están abiertos los puertos del firewall correctos o rectifique ID de arrendatario, entre otros.

Problemas con NetScaler Gateway

En la tabla siguiente se muestran los problemas comunes con las configuraciones de NetScaler Gateway y sus soluciones respectivas. Para solucionar problemas, habilite más registros y consúltelos de

la siguiente manera:

1. En la interfaz de línea de comandos, ejecute el comando: `set audit syslogParams - logLevel ALL`
2. Consulte los registros desde el shell mediante `tail -f /var/log/ns.log`

Problema	Solución
No están disponibles los permisos que se deben configurar para la aplicación Gateway en Azure.	Compruebe si dispone de una licencia adecuada de Intune. Intente utilizar el portal manage.windowsazure.com para ver si se pueden agregar los permisos. Contacte con la asistencia de Microsoft si el problema persiste.
NetScaler Gateway no puede acceder a login.microsoftonline.com ni graph.windows.net .	Desde NS Shell, compruebe si puede acceder a este sitio web de Microsoft: <code>curl -v -k https://login.microsoftonline.com</code> . A continuación, compruebe si DNS está configurado en NetScaler Gateway y si la configuración del firewall es correcta (en caso de que el firewall obstaculice las solicitudes DNS).
Aparece un error en ns.log después de configurar OAuthAction.	Compruebe si las licencias de Intune están habilitadas y si la aplicación Azure Gateway tiene establecidos los permisos adecuados.
El comando Sh OAuthAction no muestra el estado de OAuth como completo.	Consulte la configuración de DNS y los permisos configurados en la aplicación de Azure Gateway.
El dispositivo Android o iOS no muestra la solicitud de autenticación dual.	Compruebe si el ID de dispositivo de factor dual logonSchema está vinculado al servidor virtual de autenticación.

Estado y condición del error de OAuth

Estado	Condición del error
COMPLETE	Operación correctamente realizada.
AADFORGRAPH	Secreto no válido, URL no resuelta, tiempo de espera de la conexión agotado
MDMINFO	* manage.microsoft.com está inactivo o inaccesible
GRAPH	El punto final del gráfico no está accesible

Estado	Condición del error
CERTFETCH	No se puede hablar con el token del dispositivo de punto final https://login.microsoftonline.com debido a un error de DNS. Para validar esta configuración, vaya a shell y escriba <code>curl https://login.microsoftonline.com</code> . Este comando debe validarse.

Limitaciones

En los siguientes elementos, se describen algunas limitaciones del uso de MEM con Citrix Endpoint Management.

- Cuando implementa aplicaciones con Citrix e Intune para admitir la micro VPN, si los usuarios proporcionan el nombre de usuario y la contraseña para acceder a sitios de resumen, aunque sus credenciales sean válidas, aparece un error. [CXM-25227]
- Después de cambiar el **túnel dividido** de **Sí** a **No** y de esperar a que caduque la sesión de la puerta de enlace actual, el tráfico externo va directamente, sin pasar por NetScaler Gateway, hasta que el usuario inicie un sitio interno en el modo VPN completo. [CXM-34922]
- Después de cambiar la directiva “Abrir en” de **solo aplicaciones administradas** a **todas las aplicaciones**, los usuarios no pueden abrir documentos en aplicaciones no administradas hasta que cierren y reinicien Citrix Secure Mail. [CXM-34990]
- Cuando el túnel dividido está **activado** en modo VPN completo y el DNS dividido cambia de local a remoto, los sitios internos no se pueden cargar. [CXM-35168]

Problemas conocidos

Cuando la directiva de mVPN **Habilitar redirección de http/https (con SSO)** está inhabilitada, Citrix Secure Mail no funciona. [CXM-58886]

Problemas conocidos de terceros

En Citrix Secure Mail para Android, cuando un usuario toca en la opción de **crear un evento**, la página de creación de eventos no se muestra. [CXM-23917]

Cuando implementa Citrix Secure Mail para iOS con Citrix e Intune para admitir la micro VPN, no se aplica la directiva de aplicación que oscurece la pantalla de Citrix Secure Mail cuando los usuarios mueven la aplicación al segundo plano. [CXM-25032]

Incorporarse como usuario y configurar recursos

March 1, 2024

Si es la primera vez que usa Citrix, Citrix Cloud o Citrix Endpoint Management, este artículo le guiará a través de la incorporación. Obtenga información sobre el flujo de trabajo y los detalles que necesita para comenzar.

- **¿Por dónde empiezo?**
 - Si no ha adquirido ninguna suscripción de Citrix Endpoint Management, consulte [Para nuevos clientes de Citrix](#).
 - Si tiene una suscripción de Citrix Endpoint Management, vaya directamente a [Cuando el botón Administrar está disponible](#).
 - Si el sitio de Citrix Endpoint Management está aprovisionado, vaya directamente a [Configurar la autenticación](#).
- **¿El orden de la configuración es importante?** 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 mediante mensajes tales como “Configurar después del aprovisionamiento”.
- **¿Qué hago después de la incorporación?** Después de completar la incorporación y la configuración de recursos descritas en este artículo, continúe con su configuración en la consola de Citrix Endpoint Management. Para obtener información sobre los próximos pasos, consulte [Preparar la inscripción de dispositivos y la entrega de recursos](#).

Para nuevos clientes de Citrix

Para los nuevos clientes de Citrix Cloud en Citrix Endpoint Management:

Si ya adquirió una suscripción de Citrix Endpoint Management, vaya directamente a [Cuando el botón Administrar está disponible](#).

Si no configuró ninguna cuenta de Citrix Cloud, consulte [Registrarse en Citrix Cloud](#).

Si ya ha configurado una cuenta de Citrix Cloud, pero no ha adquirido Citrix Endpoint Management, solicite una demostración de servicio.

1. Utilice sus credenciales de administrador de Citrix Cloud para iniciar sesión en su cuenta de Citrix Cloud. Aparecerá la página principal de Citrix Cloud.

Todas las cuentas de administrador de Citrix Cloud se crean de la siguiente manera:

- De manera predeterminada, los administradores de Citrix Cloud son administradores de Citrix Endpoint Management.
 - Los administradores de Citrix Cloud creados con acceso de clientes deben tener Citrix Endpoint Management seleccionado para que puedan administrar Citrix Endpoint Management.
2. En la página de inicio de Citrix Cloud, busque el mosaico de Citrix Endpoint Management Services y haga clic en **Solicitar demostración**.
 3. Complete el formulario de solicitud de demostración y envíelo. El botón del mosaico de Citrix Endpoint Management Services cambia a **Demostración solicitada**.

Si hace clic en el mosaico de los servicios de Citrix Endpoint Management antes de que se gestione su solicitud, aparecerá una pantalla donde se le pedirá que contacte con un representante o socio. Un representante de ventas de Citrix puede proporcionar más información y detalles sobre el servicio.

Mientras espera la prueba, puede prepararse para la implementación de Citrix Endpoint Management revisando los [Requisitos del sistema](#). Aunque Citrix aloja y entrega su solución de Citrix Endpoint Management, deberá gestionar algunos requisitos de comunicación y puertos.

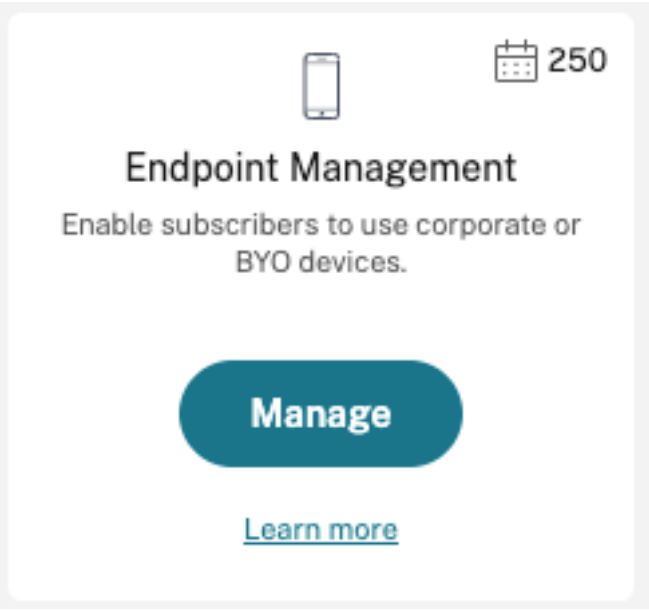
Continúe con la siguiente sección.

Cuando el botón Administrar está disponible

Este vídeo le guía a través del proceso de incorporación:

[Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.](#)

Cuando el servicio de Citrix Endpoint Management esté disponible, el botón del mosaico de Citrix Endpoint Management Services 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 del sitio y seleccione una región. A continuación, seleccione **Guardar y Continuar**.

Welcome to Endpoint Management!

We need some details about your site to enable device management

Site name

https://

|site

xm.cloud.com

Site region

Select Region ▼

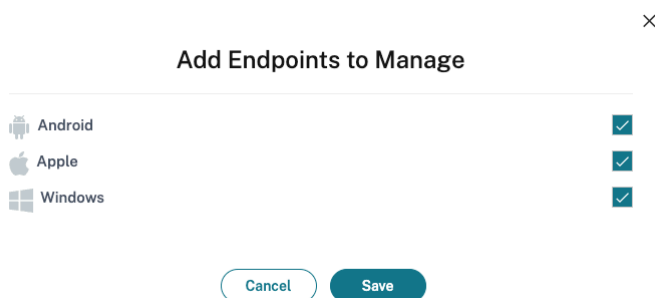
Nota:

Para solicitar las direcciones IP permitidas, póngase en contacto con el representante de Citrix

Support.

A continuación, la consola de Citrix Endpoint Management se inicia con un mensaje que indica que se está aprovisionando su conjunto y que algunas funciones de Citrix Endpoint Management se bloquearán durante el aprovisionamiento.

1. En la pantalla de **bienvenida**, haga clic en **Iniciar configuración**.
2. Seleccione los dispositivos de punto final que quiere administrar y haga clic en **Guardar**. Puede agregar o borrar dispositivos de punto final en cualquier momento para mostrarlos u ocultarlos en la consola. Mostrar y ocultar dispositivos de punto final no afecta a la configuración.



Le enviaremos un correo electrónico cuando se complete el aprovisionamiento.

Centro de recursos



Haga clic en el icono del **Centro de recursos** para ver vídeos de instrucciones sin salir de la consola.

Durante el aprovisionamiento

Mientras realizamos el aprovisionamiento de Citrix Endpoint Management, puede comenzar con la configuración.

Configurar ubicaciones de recursos

Necesita ubicaciones de recursos antes de configurar las conexiones de Protocolo ligero de acceso a directorios (LDAP) para Citrix Endpoint Management. Las ubicaciones de recursos tienen los recursos necesarios para prestar servicios de la nube a los suscriptores. Necesita una ubicación de recursos por cada dominio. Para obtener ayuda, consulte el artículo [Ubicaciones de recursos](#) de Citrix Cloud.

Mientras espera la prueba, puede prepararse para la implementación de Citrix Endpoint Management revisando los [Requisitos del sistema](#). 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 a los servicios de empresa, tales como Active Directory. La información que debe proporcionar se incluye en el manual de incorporación [Onboarding Handbook](#), en la sección “Citrix Endpoint Management Trial Sales Engineer engagement”.

Una vez que obtenga la autorización para acceder a la prueba, el botón de **Citrix Endpoint Management** cambiará a **Administrar**. Haga clic en **Administrar** para abrir la consola de Citrix Endpoint Management.

Configurar la autenticación

Una vez que se haya aprovisionado el sitio, podrá continuar con la configuración. Recomendamos configurar un proveedor de identidades (IDP) alojado en la nube o el protocolo ligero de acceso a directorios (LDAP) para importar grupos, cuentas de usuario y propiedades relacionadas.

Para configurar el IDP

Citrix Endpoint Management permite 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](#)
- [Autenticación con Okta a través de Citrix Cloud](#)
- [Autenticación con un dispositivo NetScaler Gateway local a través de Citrix Cloud](#)

Para configurar LDAP

Puede configurar una conexión en Citrix Endpoint Management a uno o varios directorios compatibles con LDAP para la autenticación por dominios. Citrix Endpoint Management admite grupos anidados en LDAP. Los grupos anidados se sincronizan diariamente a las 12 a.m. hora local.

Como parte de la configuración de LDAP, debe instalar al menos un Cloud Connector.

Para obtener una visión general rápida, vea este vídeo.

[Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.](#)

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 permitir la comunicación entre Citrix Cloud y sus recursos. Para obtener ayuda, consulte [Citrix Cloud Connector](#).

Si dispone de la configuración de LDAP y agrega Azure AD u Okta como proveedor de identidades, Citrix Endpoint Management sincroniza la información específica del IDP para los grupos de Active Directory de la base de datos de Citrix Endpoint Management. Esta configuración no afecta a los grupos de entrega e inscripciones de usuarios existentes. Sin embargo, luego no puede agregar parámetros de LDAP en Citrix Endpoint Management. Para obtener más información, consulte [Autenticación de proveedores de identidades](#)

Si cambia los parámetros **Alias del dominio** o **Buscar usuarios por** después de la inscripción, los usuarios deben volver a inscribirse. Para obtener más información sobre la configuración de LDAP, consulte [Autenticación con dominio o dominio y 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 en Citrix Endpoint Management, NetScaler Gateway proporciona un mecanismo para que los dispositivos accedan de manera remota a la red interna y a los recursos.

Citrix Endpoint Management requiere NetScaler Gateway en los siguientes casos:

- Necesita una micro VPN para que las aplicaciones de línea de negocio puedan acceder a los recursos de la red interna. Esas aplicaciones están empaquetadas con la tecnología MDX de Citrix. La micro VPN necesita NetScaler Gateway para conectarse a las infraestructuras back-end internas.
- Piensa usar Citrix Endpoint Management para administrar aplicaciones (MAM o MDM+MAM). NetScaler Gateway no es necesario para administrar dispositivos (MDM) solamente.
- Tiene previsto integrar Citrix Endpoint Management en Microsoft Endpoint Manager. (Requiere un NetScaler Gateway local.)

Para obtener una visión general rápida, vea este vídeo.

[Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.](#)

En esta tabla se resumen las funciones que ofrecen las soluciones de NetScaler Gateway en entornos locales.

Funcionalidades admitidas	NetScaler Gateway local
Citrix Secure Mail (STA) *	sí

Funcionalidades admitidas	NetScaler Gateway local
SSO web en túnel (Single Sign-On por web)	sí
VPN completo (no disponible para aplicaciones móviles de productividad de Citrix para iOS)	sí
VPN por aplicación	sí
Single Sign-On para dispositivos móviles (control de acceso)	no
Alta disponibilidad	sí**
Implementación de múltiples POP	sí***
Compatibilidad con proxies	sí
Túneles divididos	sí
DNS dividido	sí

* Configuración del servicio Secure Ticket Authority (STA) de Citrix Cloud

** Configuración local

*** Configuración de Global Server Load Balancing

Casos de uso de NetScaler Gateway locales

Utilice uno o varios dispositivos NetScaler Gateway locales con Citrix Endpoint Management cuando:

- Necesite capacidades de red VPN por aplicación.
- Requiera túneles completos, túneles divididos, túneles divididos inversos o DNS divididos. Recomendamos el valor “Túnel VPN completo” para conexiones que usan certificados de cliente o SSL de extremo a extremo para conectarse a un recurso de la red interna.
- Puede utilizar la integración de Citrix Endpoint Management en Microsoft Endpoint Manager.

El uso de dispositivos NetScaler Gateway locales implica una configuración y un mantenimiento significativos. Después de configurar LDAP y NetScaler Gateway en la consola de Citrix Endpoint Management, exporte un script desde esa consola. A continuación, ejecute el script en NetScaler Gateway.

1. En la página **Parámetros**, vaya al mosaico de **NetScaler Gateway** y, a continuación, haga clic en **Iniciar configuración**.
2. Seleccione **NetScaler Gateway (local)** como tipo.
3. Siga las instrucciones que aparecen en pantalla. Para obtener información, consulte [Configurar NetScaler Gateway local para usarlo con Citrix Endpoint Management](#).

Configurar el servidor de notificaciones

Para poder 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

Para inscribir y administrar dispositivos Apple, Citrix Endpoint Management requiere un certificado del servicio de notificaciones push de Apple (APNs) proveniente de Apple. Citrix Endpoint Management también necesita un certificado APNs si se van a usar notificaciones push en Citrix Secure Mail para Apple. Para obtener información sobre Citrix Endpoint Management y APNs, consulte [Notificaciones push en 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 de [Apple Developer Program](#).

Para obtener una visión general rápida, vea este vídeo.

[Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.](#)

Para configurar APNs con una solicitud de firma de certificado de Citrix:

1. En la página **Configuración**, expanda el mosaico de **Apple**.
2. En el mosaico **Certificado APNs**, haga clic en **Configurar** y, a continuación, siga las instrucciones que aparecen en pantalla.

Para obtener más información, consulte [Certificados y autenticación](#).

Configurar Android Enterprise

Citrix Endpoint Management está configurado por completo después de crear los grupos de entrega y asignar usuarios a los grupos de entrega a través de la biblioteca de Cloud. A partir de este momento, la administración de Citrix Endpoint Management se lleva a cabo desde Citrix Cloud. La interfaz combinada simplifica cambiar el proceso de cambiar 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 proveedor EMM. Si utiliza Google Play administrado, puede aprovisionar cuentas administradas de Google Play para dispositivos y usuarios finales. Las cuentas

de Google Play administrado proporcionan acceso a Google Play administrado, lo que permite a los usuarios instalar y utilizar las aplicaciones de trabajo que ponga a su disposición. Si su organización utiliza un servicio de identidad de terceros, puede vincular las cuentas de Google Play administrado a las cuentas de identidad existentes.

Puesto que las empresas de este tipo no están vinculadas a un dominio, puede crear más de una empresa para una sola organización. Por ejemplo, cada departamento o región de una organización puede inscribirse como una empresa diferente. Esta 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 EMM. Si su organización utiliza Google Workspace, entonces tiene un ID de empresa existente y cuentas de Google existentes para los usuarios. Para utilizar Citrix Endpoint Management con Google Workspace, sincronice con su directorio LDAP y recupere la información de la cuenta de Google procedente de Google mediante la API de Google Directory.

Las empresas de este tipo están vinculadas 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 mediante su plan de Google Workspace.

Para obtener una visión general rápida, vea este vídeo.

[Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.](#)

Para empezar:

1. En la página **Configuración**, expanda el mosaico de **Android**.
2. En el mosaico de **Android Enterprise**, haga clic en **Configurar**.
3. Elija **Google Play** o **G Suite**, según el modo en que proporcione a los usuarios acceso a las aplicaciones de Google.

Si ha configurado previamente la plataforma de Android Enterprise con Google Play, la interfaz de usuario le lleva a Google Play Store para reinscribirle. Haga clic en **Reinscribir**, vuelva a la consola de CEM y actualice la página.

4. Siga las instrucciones que aparecen en pantalla.

Consulte:

- [Crear una cuenta de Android Enterprise](#)

Configurar Firebase Cloud Messaging

Citrix le recomienda que utilice 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 dispositivos Android habilitados para FCM. Así, toda acción de seguridad o comando de implementación desencadena una notificación push para pedir al usuario que se reconecte al servidor de Citrix Endpoint Management. Consulte [Firebase Cloud Messaging](#).

Integrar en Microsoft Endpoint Manager

La integración de Citrix Endpoint Management en Microsoft Endpoint Manager agrega el valor de la red micro VPN de Citrix Endpoint Management a las aplicaciones compatibles con Microsoft Intune, como el explorador web Microsoft Edge.

Asimismo, la integración de Citrix Endpoint Management en MEM permite a las empresas empaquetar sus propias aplicaciones de línea de negocio con Intune y Citrix. El empaquetado de aplicaciones proporciona capacidades micro VPN dentro de un contenedor de administración de aplicaciones móviles (MAM) de Intune. La micro VPN de Citrix Endpoint Management permite a las aplicaciones acceder a recursos locales. Puede administrar y entregar aplicaciones Office 365, aplicaciones de línea de negocio y Citrix Secure Mail en un solo contenedor. Un único contenedor proporciona máxima seguridad y productividad.

- De manera predeterminada, los administradores de Citrix Cloud son administradores de Citrix Endpoint Management.
- Los administradores de Citrix Cloud creados con acceso de clientes deben tener Citrix Endpoint Management seleccionado para que puedan 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 (puede hacerlo en cualquier momento), acceda a la consola de Citrix Endpoint Management desde el panel de mandos 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 información, consulte [Configurar roles con RBAC](#).

Para la integración en MEM, consulte [Integración de Citrix Endpoint Management en 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 de **inicio** de Citrix Cloud y, a continuación, haga clic en **Administrar** en el mosaico de **Citrix Endpoint Management**. A continuación, puede verificar si inició sesión en Citrix Endpoint Management con su cuenta de Azure Active Directory.

1. En la página **Parámetros**, vaya al mosaico **Integrar en Microsoft EMS/Intune**.
2. Haga clic en **Ver más**. La interfaz de usuario indica si ha habilitado correctamente la conexión.

Integrate with Microsoft EMS/Intune

Integration with Microsoft Enterprise Mobility + Security (EMS)/Intune adds the value of Endpoint Management micro VPN to Microsoft Intune aware apps, such as Microsoft Managed Browser.
[Learn more](#)

Go to **Identity and Access Management** to manage Azure Active Directory authentication and administrators.

Microsoft EMS/Intune[Edit Micro VPN](#)

● Enabled

SUBSCRIPTION
Valid

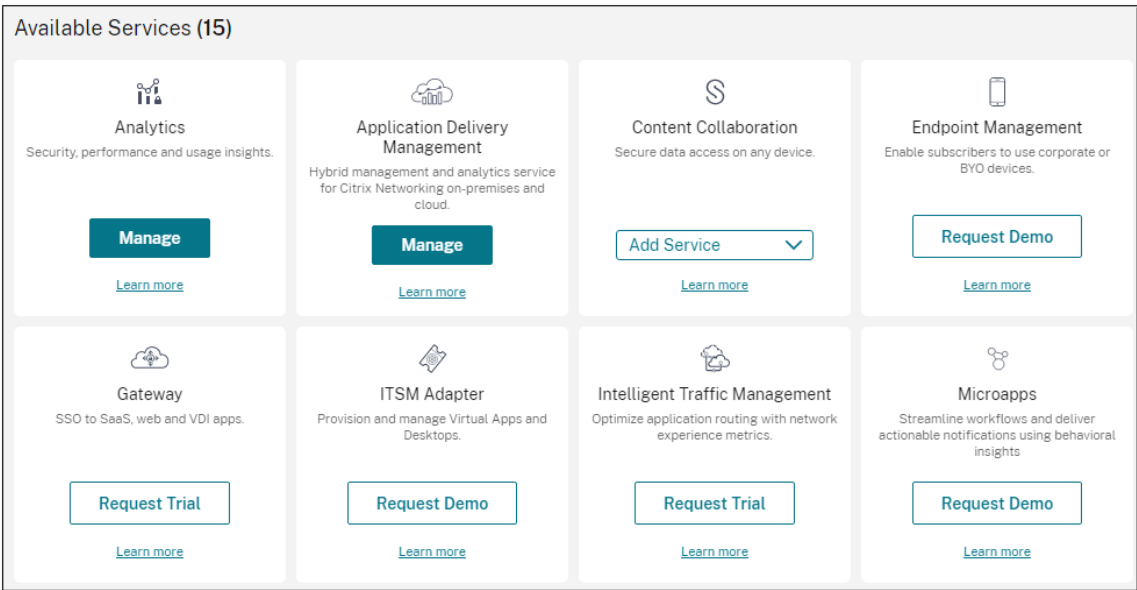
Micro VPN
TEST 83

En la consola de Citrix Cloud, puede cambiar los nombres de usuario o las contraseñas y eliminar o modificar usuarios locales. Consulte [Administración de acceso e identidad](#).

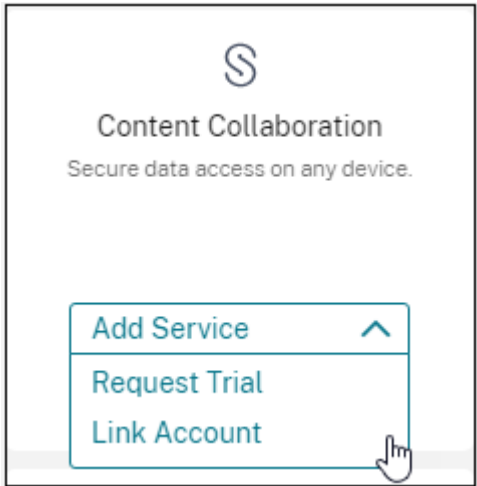
Vincular una cuenta existente de ShareFile a Citrix Cloud

Si tenía una cuenta de ShareFile que existía antes de registrarse en Citrix Cloud, debe vincular esa cuenta a Citrix Cloud. Para poder vincular la cuenta, su dirección de correo electrónico debe ser un administrador de la cuenta de ShareFile. Cuando tenga todo listo para continuar, vaya a <https://onboarding.cloud.com>.

1. Después de iniciar sesión, aparecerá una pantalla similar a la siguiente.



2. En la lista desplegable de **ShareFile**, elija **Vincular cuenta**.




3. Después de que se confirme su cuenta de ShareFile, aparecerá la página siguiente:


Add Content Collaboration Account

[Request Trial](#) [Link Account](#)

GEO Location

Select the geographical location for the account.

 USA ☐

 EU ☐

☐ I understand that I cannot change the region after set up.

Select a subdomain

Your subdomain is your unique URL for your Content Collaboration account. You can change this later.

https:// sharefile.com

Cancel

Request Trial

- Haga clic en la ficha **Vincular cuenta** para completar el proceso. Puede administrar al instante su cuenta de ShareFile desde Citrix Cloud.

Consideraciones de escala y tamaño para los Cloud Connectors

November 29, 2023

Al evaluar el servicio Citrix Endpoint Management para determinar el tamaño y la escalabilidad, investigue y pruebe la configuración de los Cloud Connectors en función de sus requisitos específicos. Cloud Connector recibe la carga solo durante la inscripción de dispositivos. Un tamaño insuficiente de las máquinas puede afectar negativamente al rendimiento del sistema.

Citrix requiere dos Cloud Connectors por ubicación de recursos. Instale Cloud Connector en un servidor dedicado que no comparta responsabilidades con ningún otro componente o producto. En nuestras pruebas, los Cloud Connectors se implementaron en conjuntos HA de alta disponibilidad (**no cuentan con equilibrio de carga**).

Probar configuración

- Dos Windows Server 2019 dedicados, 2 vCPU, 4 GB de memoria
- Inscripciones de dispositivos Android e iOS en MDM+MAM, divididas uniformemente en un período de 8 horas
- Citrix Endpoint Management configurado para inscribir 125 dispositivos por hora por 1000 dispositivos
 - 1000 dispositivos (125 inscripciones de dispositivo por hora)
 - 5000 dispositivos (625 inscripciones de dispositivo por hora)
 - 10 000 dispositivos (1250 inscripciones de dispositivo por hora)
 - 20 000 dispositivos (2500 inscripciones de dispositivo por hora)

Resultados de las pruebas

	1000 dispositivos	5000 dispositivos	10 000 dispositivos	20 000 dispositivos
Cloud Connector				
Promedio de CPU	2 %	2 %	4 %	4 %
Máximo de CPU	8 %	8 %	10 %	11 %
Promedio de memoria	73 %	73 %	75 %	75 %
Máximo de memoria	76 %	76 %	76 %	79 %

Preparar la inscripción de dispositivos y la entrega de recursos

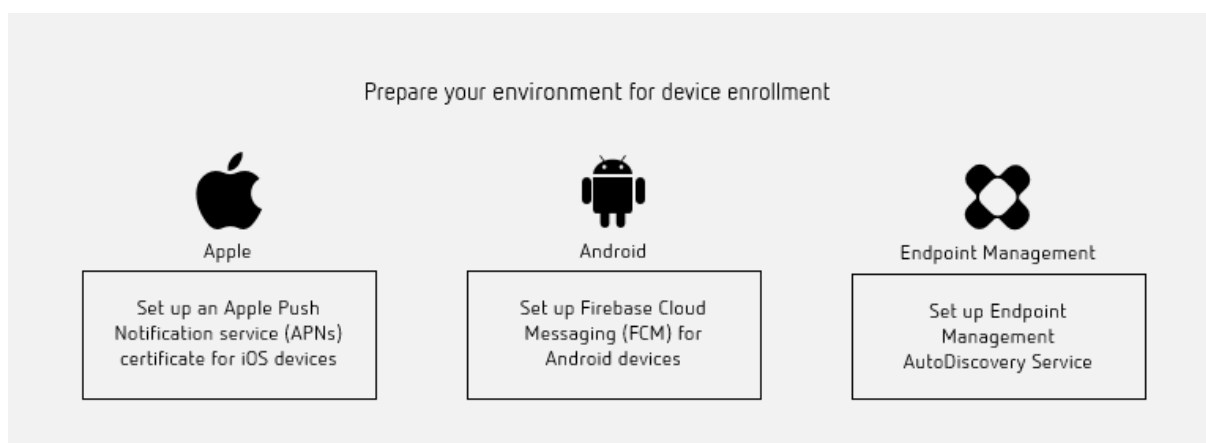
March 1, 2024

Importante:

Antes de continuar, debe completar todas las tareas descritas en [Incorporarse como usuario y configurar recursos](#).

Mantenga a sus usuarios informados sobre los próximos cambios. Consulte [Welcome to your Citrix User Adoption Kit](#).

Citrix Endpoint Management admite varias opciones de inscripción. En este artículo se describe la configuración básica necesaria para permitir que se inscriban todos los dispositivos compatibles. En el diagrama siguiente se resume la configuración básica.



Para obtener una lista de las plataformas compatibles, consulte [Sistemas operativos compatibles](#).

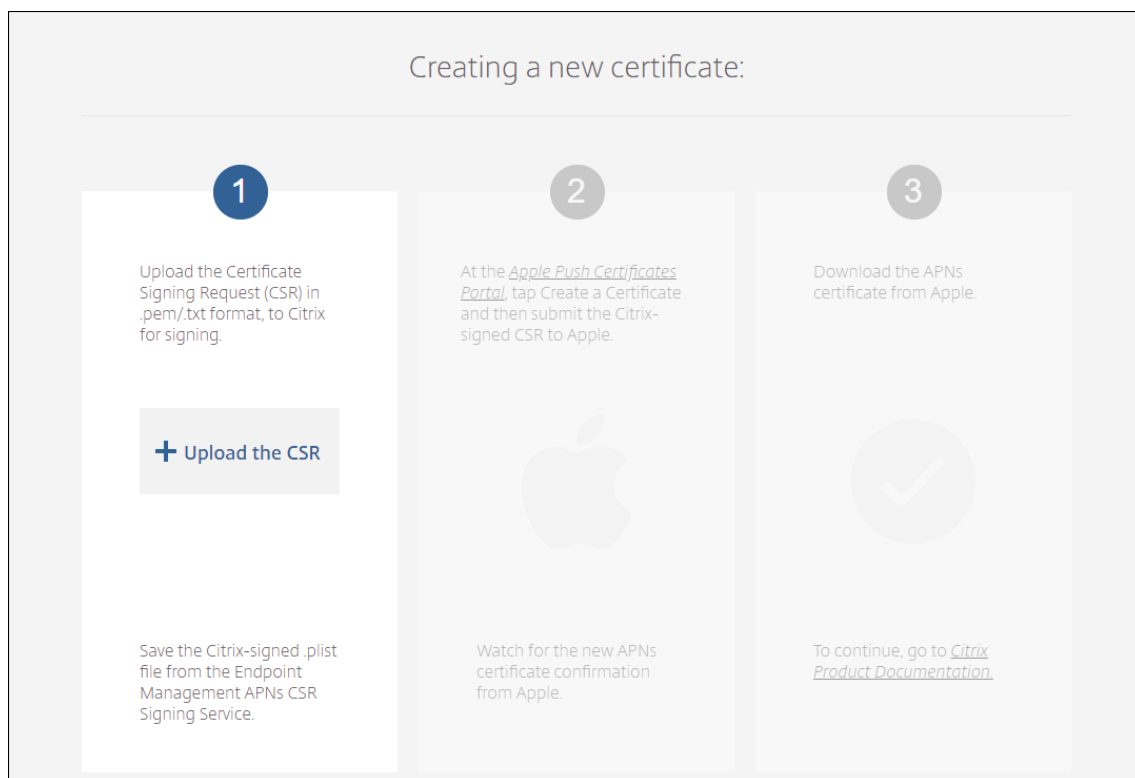
Configurar un certificado APNs (Apple Push Notification Service) para los dispositivos iOS

Importante:

Apple dejará de desarrollar el protocolo binario heredado de APNs a partir del 31 de marzo de 2021. Apple recomienda que se utilice en su lugar la API del proveedor de APNs basada en HTTP/2. A partir de la versión 20.1.0, Citrix Endpoint Management admite 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 sobre cómo comprobar la conectividad con APNs, consulte [Comprobaciones de conectividad](#).

Para inscribir y administrar dispositivos iOS, Citrix Endpoint Management requiere un certificado del servicio de notificaciones push de Apple (APNs) proveniente de Apple. Citrix Endpoint Management también necesita 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 de [Apple Developer Program](#).
- Para obtener un certificado APNs e importarlo en Citrix Endpoint Management, consulte [Certificados APNs](#).



- Para obtener más información acerca de Citrix Endpoint Management y APNs, consulte [Notificaciones push en 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 Citrix Endpoint Management. Toda acción de seguridad o comando de implementación desencadena una notificación push. La notificación solicita a los usuarios que vuelvan a conectarse a Citrix Endpoint Management.

- La configuración de FCM requiere que configure su cuenta de Google. Para crear credenciales de Google Play, consulte [Gestionar la información de tu cuenta de desarrollador](#). También puede utilizar Google Play para agregar, comprar y aprobar aplicaciones para implementarlas en el espacio de trabajo de Android Enterprise del dispositivo. Se puede utilizar Google Play para implementar aplicaciones privadas de Android, aplicaciones públicas o de terceros.
- Para configurar FCM, consulte [Firebase Cloud Messaging](#).

Configurar el servicio de detección automática de Citrix Endpoint Management

El servicio de detección automática simplifica el proceso de inscripción de los usuarios mediante detección de URL basada en direcciones de correo electrónico. El servicio de detección automática tam-

bién proporciona funciones como verificación de inscripción, fijación de certificados y otras ventajas 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 de detección automática, los usuarios:

- Pueden utilizar 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`.

Se recomienda utilizar el servicio de detección automática para entornos de alta seguridad. El servicio de detección automática admite la fijación de certificados de clave pública, que impide ataques de intermediarios (ataques de tipo “Man in the middle”). La fijación de certificados garantiza que se utilice el certificado firmado por la empresa cuando los clientes de Citrix se comuniquen con Citrix Endpoint Management. Para configurar la fijación de certificados para los sitios de Citrix Endpoint Management, póngase en contacto con Citrix Support. Para obtener información sobre la fijación de certificados, consulte [Fijación de certificados](#).

Para acceder al servicio de detección automática, vaya a <https://adsui.cloud.com> (acceso comercial).

Requisitos previos

- El nuevo servicio de detección automática de Citrix Cloud requiere la versión más reciente de Citrix Secure Hub:
 - Para iOS, Citrix Secure Hub 21.6.0 o una versión posterior
 - Para Android, Citrix Secure Hub 21.8.5 o una versión posterior

Es posible que los dispositivos con versiones anteriores de Citrix Secure Hub sufran interrupciones del servicio.

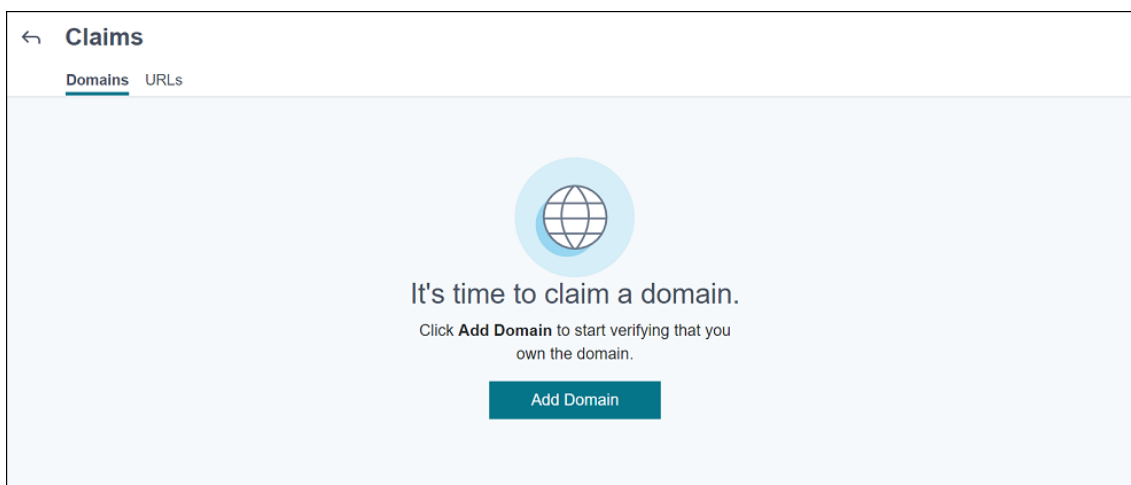
- Para acceder al nuevo servicio de detección automática, debe tener una cuenta de administrador de Citrix Cloud con acceso total. El servicio de detección automática no permite usar cuentas de administrador con acceso personalizado. Si no tiene cuenta, consulte [Registrarse en Citrix Cloud](#).

Citrix migró todos los registros existentes de la detección automática a Citrix Cloud sin interrumpir el servicio. Los registros migrados no aparecen automáticamente en la nueva consola. Debe recuperar los dominios en el nuevo servicio de detección automática para demostrar que le pertenecen. Para obtener más información, consulte [CTX312339](#).

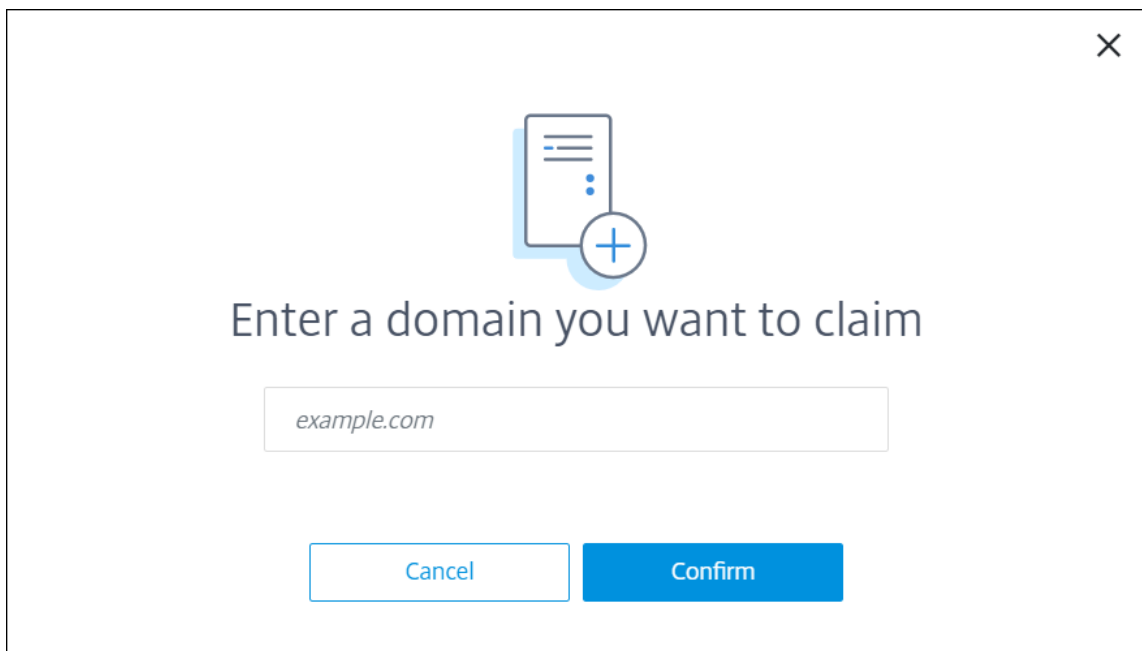
- Antes de empezar a usar el servicio de detección automática para las implementaciones de Citrix Endpoint Management, verifique y reclame su dominio. Puede reclamar hasta 10 dominios. La notificación asocia el dominio verificado al servicio de detección automática. Para reclamar más de 10 dominios, cree un tíquet de SRE o póngase en contacto con el servicio de asistencia técnica de Citrix.
- Utilice el parámetro Puerto MAM, en lugar de FQDN de NetScaler Gateway, para dirigir el tráfico MAM al centro de datos. Si introduce un nombre de dominio completo (FQDN) junto con el puerto de NetScaler Gateway, el dispositivo cliente utiliza la configuración del parámetro **Puerto MAM**.
- Si un bloqueador de anuncios impide que el sitio se abra, inhabilite el bloqueador de anuncios para todo el sitio web.

Reclamar un dominio

1. En la ficha **Notificaciones > Dominios**, haga clic en **Agregar dominio**.

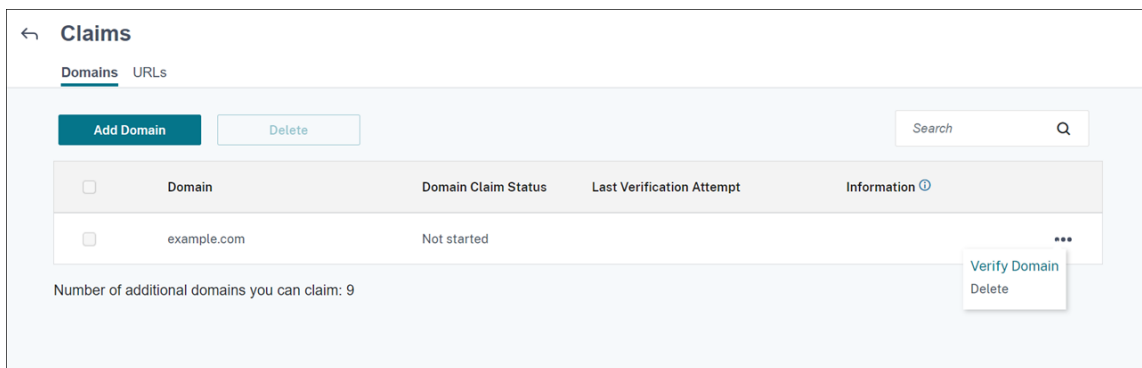


2. En el cuadro de diálogo que aparece, introduzca el nombre de dominio de su entorno de Citrix Endpoint Management y, a continuación, haga clic en **Confirmar**. Su dominio aparecerá en **Notificaciones > Dominios**.



A modal dialog box with a close button (X) in the top right corner. It features a blue icon of a document with a plus sign. The text "Enter a domain you want to claim" is centered. Below it is a text input field containing "example.com". At the bottom are two buttons: "Cancel" and "Confirm".

3. En el dominio que agregó, haga clic en el menú de puntos suspensivos y seleccione **Verificar dominio** para iniciar el proceso de verificación. Aparecerá la página **Verificar el dominio**.



The "Claims" management interface. It has a back arrow and the title "Claims". Below the title are tabs for "Domains" (selected) and "URLs". There are "Add Domain" and "Delete" buttons, and a search bar. A table lists domains with columns: Domain, Domain Claim Status, Last Verification Attempt, and Information. One domain, "example.com", is listed with a status of "Not started". A dropdown menu for the "example.com" row shows "Verify Domain" and "Delete" options. At the bottom, it says "Number of additional domains you can claim: 9".

Domain	Domain Claim Status	Last Verification Attempt	Information ⓘ
example.com	Not started		Verify Domain Delete

4. En la página **Verificar el dominio**, siga las instrucciones para comprobar que es propietario del dominio.

×

Verify your domain

Before you claim your domain, we must verify that you own it. Follow the steps below to verify and claim the domain.

- 1 Copy the DNS token that appears below. The token expires within 7 days. Click Copy to copy it.
- 2 Create a DNS TXT record in the zone file for your domain.
- 3 Paste the token you copied to the DNS TXT record.
- 4 Click Start DNS Check to start detecting the DNS TXT record.

DNS Token:

Copy

Verify Domain Later

Start DNS Check

- a) Haga clic en **Copiar** para copiar el token de DNS en el portapapeles.
- b) Cree un registro TXT de DNS en el archivo de zona de su dominio. Para ello, vaya al portal del proveedor que aloja su dominio y agregue el token de DNS que copió.

En la siguiente captura de pantalla, se muestra un portal de proveedor de alojamiento de dominios. Su portal puede tener un aspecto diferente.

Dashboard > DNS zones > .cloud.com >

@ .cloud.com

Save Discard Delete Users Metadata

Copy to clipboard

@ .cloud.com

Type

TXT

TTL * TTL unit

5 Minutes

Value

	...
	...
	...
	...

The quick brown fox jumps over the lazy dog.

- c) En Citrix Cloud, en la página **Verificar el dominio**, haga clic en **Iniciar comprobación de DNS** para iniciar la detección de su registro TXT de DNS. Si quiere verificar el dominio más adelante, haga clic en **Verificar dominio más tarde**.

El proceso de verificación tarda, por lo general, aproximadamente una hora. Sin embargo, puede tardar hasta dos días en dar una respuesta. Puede cerrar sesión e iniciar sesión de nuevo durante la comprobación de estado.

Una vez completada la configuración, el estado del dominio cambia de **Pendiente** a **Verificado**.

- Después de reclamar su dominio, introduzca la información sobre el servicio de detección automática. Haga clic en el menú de puntos suspensivos del dominio que agregó y, a continuación, en la opción para **agregar información de Citrix Endpoint Management**. Aparecerá la página **Información sobre el servicio de detección automática**.
- Introduzca la información siguiente y, a continuación, haga clic en **Guardar**.
 - FQDN del servidor de Citrix Endpoint Management:** Introduzca el nombre de dominio completo del servidor de Citrix Endpoint Management. Por ejemplo: `example.xml.cloud.com`. Este parámetro se utiliza para el control de tráfico de MDM y MAM.
 - FQDN de NetScaler Gateway:** Introduzca el nombre de dominio completo de NetScaler Gateway, con el formato FQDN o FQDN:puerto. Por ejemplo: `example.com`. Esta configuración se utiliza para dirigir el tráfico MAM al centro de datos. Para implementaciones de solo MDM, deje este campo en blanco.

Nota:

Citrix recomienda utilizar el parámetro **Puerto MAM**, en lugar de **FQDN de NetScaler Gateway**, para controlar el tráfico MAM. Si introduce un nombre de dominio completo (FQDN) junto con el puerto de NetScaler Gateway, el dispositivo cliente utiliza la configuración del parámetro **Puerto MAM**.

- **Nombre de la instancia:** Introduzca el nombre de la instancia del servidor de Citrix Endpoint Management configurado anteriormente. Si no está seguro del nombre de instancia, deje el valor predeterminado, **zdm**.
- **Puerto MDM:** Introduzca el puerto utilizado para el tráfico de control de 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 de MAM, la inscripción MAM, la inscripción iOS y la enumeración de aplicaciones. Para los servicios basados en la nube, el valor predeterminado es 8443.

Solicitar detección automática para dispositivos Windows

Para inscribir dispositivos Windows, lleve a cabo lo siguiente:

1. Póngase en contacto con Citrix Support y cree una solicitud de asistencia para habilitar la detección automática de Windows.
2. Obtenga un certificado SSL sin comodín firmado públicamente para [enterpriseenrollment.mycompany.com](#). La parte [mycompany.com](#) es el dominio que contiene las cuentas que los usuarios utilizan para inscribirse. Adjunte el certificado SSL en formato .pfx y su contraseña a la solicitud de asistencia creada en el paso anterior.

Para utilizar más de un dominio para inscribir dispositivos Windows, también puede utilizar un multidominio con la siguiente estructura:

- Un nombre SubjectDN con un nombre CN que especifica el dominio principal al que está relacionado (por ejemplo, [enterpriseenrollment.mycompany1.com](#)).
 - Las redes de área de almacenamiento apropiadas para el resto de los dominios (por ejemplo, [enterpriseenrollment.mycompany2.com](#), [enterpriseenrollment.mycompany3.com](#), entre otros).
3. Cree un registro de nombre canónico (CNAME) en el servidor DNS y asigne la dirección del certificado SSL ([enterpriseenrollment.mycompany.com](#)) a [autodisc.xm.cloud.com](#).

Cuando un usuario de un dispositivo Windows se inscribe con un UPN, el servidor de inscripción de Citrix:

- Proporciona los detalles del servidor de Citrix Endpoint Management.
- Indica al dispositivo que solicite un certificado válido de Citrix Endpoint Management.

A partir de ahora, puede inscribir todos los dispositivos compatibles. Vaya a la siguiente sección si quiere prepararse para la entrega de recursos a los dispositivos.

Integración en el acceso condicional de Azure AD

Puede configurar Citrix Endpoint Management para aplicar la compatibilidad con el acceso condicional de Azure AD a aplicaciones de Office 365. Esta función le permite implementar la metodología Zero Trust para usuarios de dispositivos al implementar aplicaciones de Office 365. Puede usar el estado del dispositivo, el nivel de riesgo, la ubicación y las protecciones de los dispositivos para aplicar acciones automatizadas y definir el acceso a las aplicaciones de Office 365 en dispositivos iOS y de Android Enterprise administrados.

Para aplicar el cumplimiento de normas en los 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 y las licencias de Intune y Microsoft Office 365.
- Citrix Secure Hub 21.4.0 y versiones 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 información, consulte [Autenticación con Azure Active Directory a través de Citrix Cloud](#).
- Dé su consentimiento a la aplicación de AAD multiarrendatario de Citrix para permitir que las aplicaciones móviles se autenticuen con la aplicación cliente de AAD. Solo es necesario si el administrador global de Azure establece el valor de **Los usuarios pueden registrar aplicaciones** en **No**. Configure este parámetro en Azure Portal, en **Azure Active Directory > Users > User Settings**. 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 explorador web como la aplicación de la tienda pública requerida.
- Inhabilite el parámetro **Valores predeterminados de seguridad** en la consola de Azure AD. Al iniciar la configuración de Azure AD, reemplaza los valores predeterminados de seguridad por

directivas de acceso condicional de Azure AD más detalladas. Para obtener más información sobre los valores predeterminados de seguridad, consulte la [documentación de Microsoft](#).

Configurar el cumplimiento de normas en los dispositivos mediante directivas de acceso condicional de Azure AD

Los pasos generales para configurar el cumplimiento de normas en los dispositivos mediante directivas de acceso condicional de Azure AD son los siguientes:

1. Configuración de Citrix Endpoint Management:

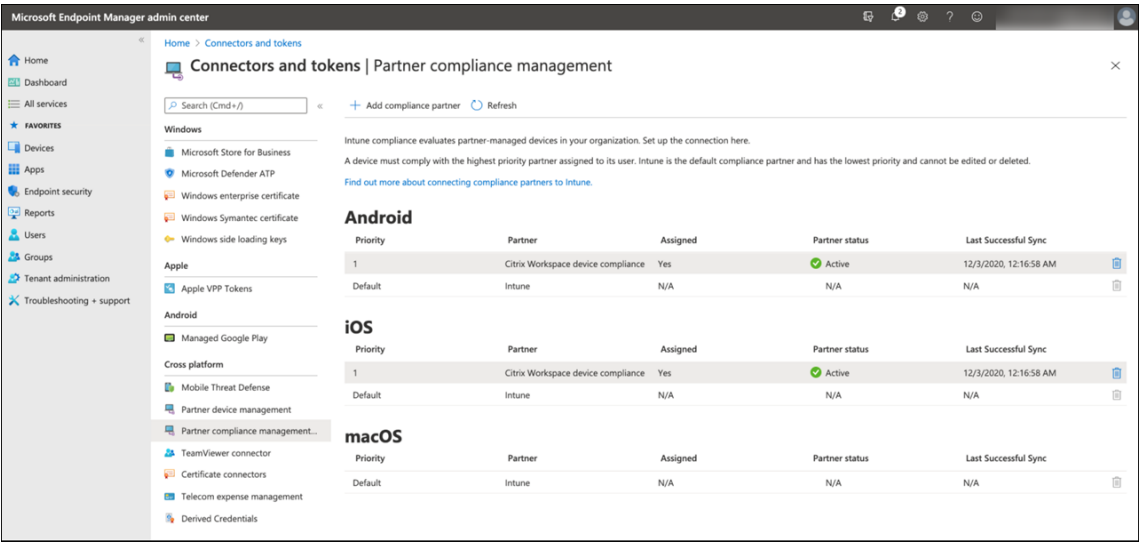
- En el centro de administración de Microsoft Endpoint Manager, agregue **Citrix Workspace device compliance** como el socio del cumplimiento de normas para cada plataforma de dispositivos y asigne grupos de usuarios.
- En Citrix Endpoint Management, sincronice la información del centro de administración de Microsoft Endpoint Manager.

2. Configuración de Azure AD: En el portal de Azure AD, establezca directivas de acceso condicional para aplicaciones individuales de Office 365.

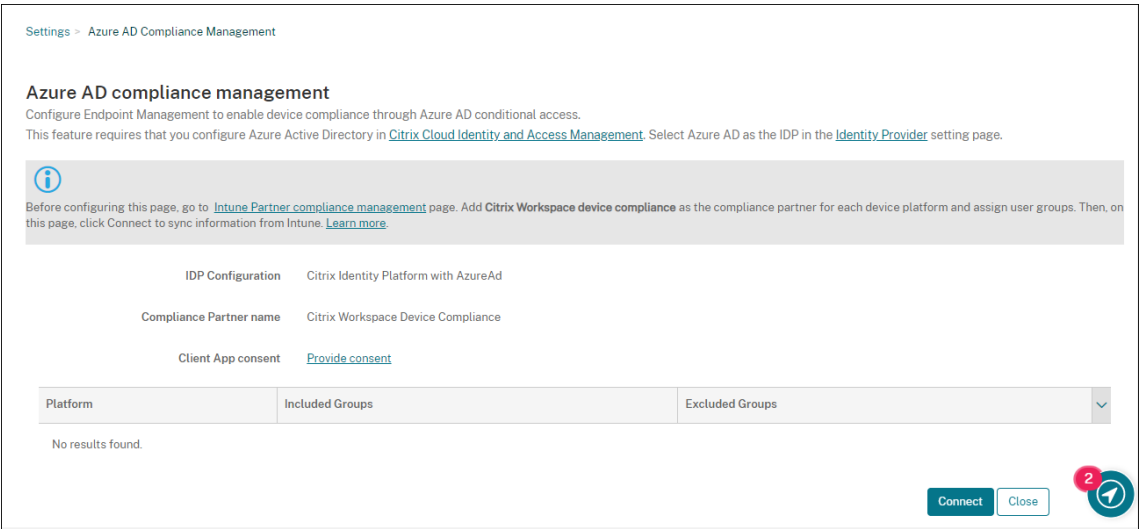
3. Configuración de Citrix Endpoint Management: Una vez configuradas las directivas de acceso condicional para aplicaciones de Office 365, agregue la aplicación Microsoft Authenticator y las aplicaciones de Office 365 como aplicaciones de la tienda públicas de aplicaciones en Citrix Endpoint Management. Asigne estas aplicaciones públicas al grupo de entrega y configúrelas como aplicaciones necesarias.

Configurar Citrix Endpoint Management para la administración de cumplimiento de Azure AD

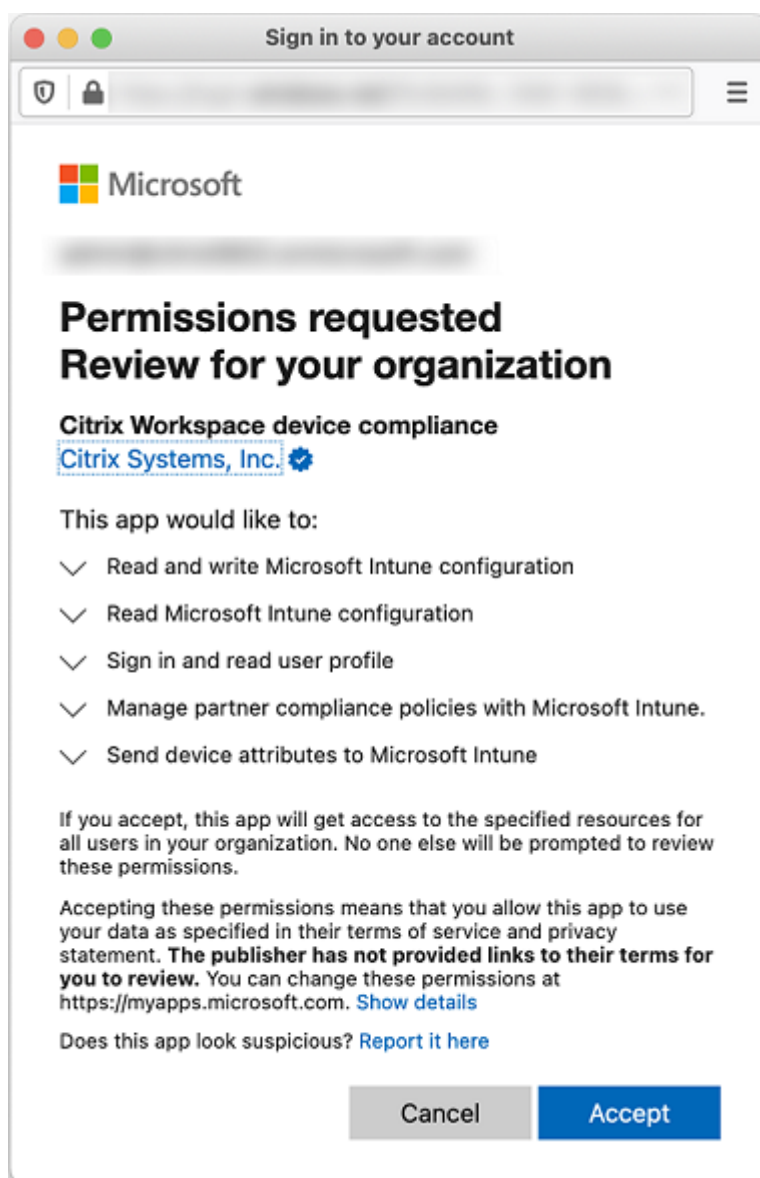
1. Inicie sesión en el [Centro de administración de Microsoft Endpoint Manager](#) y vaya a **Tenant administration > Connectors and tokens > Device compliance management**. Haga clic en **Add compliance partner** y elija **Citrix Workspace device compliance** como socio del cumplimiento de normas para cada plataforma de dispositivos. A continuación, asigne grupos de usuarios.



2. En Citrix Endpoint Management, vaya a **Parámetros > Administración de cumplimiento de normas de Azure AD**.
3. Si quiere, establezca el consentimiento global para que los usuarios no necesiten dar su consentimiento en cada dispositivo. Junto a **Consentimiento de aplicaciones cliente**, haga clic en **Dar consentimiento**. Introduzca sus credenciales de administrador global Azure AD y siga las indicaciones para dar consentimiento global a las aplicaciones cliente.
4. Haga clic en **Conectar** para sincronizar la información del centro de administración de Microsoft Endpoint Manager.



Un cuadro de diálogo le solicita que acepte los permisos de esta configuración. Haga clic en **Aceptar**. Una vez completada la configuración, las plataformas de dispositivos sincronizados aparecen en la lista.



Configurar directivas de acceso condicional en Azure AD

En el portal de Azure AD, configure directivas de acceso condicional para aplicaciones de Office 365 con el fin de aplicar el cumplimiento de normas en los dispositivos. Vaya a **Dispositivos > Acceso condicional > Directivas > Nueva directiva**. Para obtener más información, consulte la [documentación de Microsoft](#).

Para configurar el cumplimiento de normas en los dispositivos para aplicaciones administradas por Intune:

- [Configurar aplicaciones administradas de Intune para entrega a dispositivos](#)
- [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

Una vez configuradas las directivas de acceso condicional para aplicaciones de Office 365, agregue la aplicación Microsoft Authenticator y las aplicaciones de Office 365 como aplicaciones de la tienda públicas de aplicaciones en Citrix Endpoint Management. Asigne estas aplicaciones públicas al grupo de entrega y configúrelas como aplicaciones necesarias. Para obtener información, consulte [Agregar una aplicación de la tienda pública de aplicaciones](#).

Flujo de trabajo de la autenticación de usuarios

1. Los nuevos usuarios deben inscribir dispositivos en Citrix Endpoint Management con credenciales de Azure AD. Los usuarios que se hayan inscrito anteriormente con credenciales de Azure AD no necesitan volver a inscribir sus dispositivos.
2. Citrix Endpoint Management envía Microsoft Authenticator y las aplicaciones de Office 365 configuradas a los dispositivos como aplicaciones necesarias. Si configuró una aplicación de explorador web como la aplicación de tienda pública necesaria para la plataforma Android, Citrix Endpoint Management la envía también 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 una aplicación de Office 365 disponible, el dispositivo le pide que toque el enlace de **registro en Azure AD** para iniciar el proceso de registro.
5. Una vez que el usuario haya tocado 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. A continuación, la aplicación Microsoft Authenticator se cierra y Citrix Secure Hub se vuelve a abrir.
6. Citrix Secure Hub muestra un mensaje que indica que se ha completado el registro de dispositivos de Azure AD. Ahora el usuario puede usar aplicaciones de Microsoft para acceder a sus recursos en la nube.

Una vez finalizado el registro, Azure AD marca el dispositivo como administrado y conforme en la consola.

Directivas de dispositivo predeterminadas y aplicaciones móviles de productividad

Si lleva a cabo la incorporación desde Citrix Endpoint Management 19.5.0 o una versión posterior, se preconfiguran algunas directivas de dispositivos y aplicaciones móviles de productividad. Esta configuración permite:

- Implementar inmediatamente la funcionalidad básica en los dispositivos
- Comenzar con las configuraciones básicas recomendadas para un espacio de trabajo seguro

Para las plataformas Android, Android Enterprise, iOS, macOS y Windows Desktop/Tablet, el sitio contiene las siguientes directivas de dispositivo preconfiguradas:

- **Directiva de códigos de acceso:** La directiva de código de acceso está **activada**, con todos los parámetros predeterminados de código de acceso habilitados.
- **Directivas de inventario de aplicaciones:** La directiva de inventario de aplicaciones está **activada**.
- **Directivas de restricciones:** La directiva de restricciones está **activada**, con todos los parámetros predeterminados de restricciones habilitados.

Estas directivas se encuentran en el grupo de entrega **AllUsers**, que contiene todos los usuarios locales y de Active Directory. Se recomienda utilizar el grupo de entrega AllUsers solo para las pruebas iniciales. A continuación, cree sus grupos de entrega e inhabilite el grupo de entrega AllUsers. Puede reutilizar las aplicaciones y directivas de dispositivos preconfiguradas en los grupos de entrega.

Todas las directivas de dispositivo de Citrix Endpoint Management están documentadas en [Directivas de dispositivo](#). Este artículo incluye información sobre cómo utilizar la consola para modificar las directivas de dispositivos. Para obtener información sobre directivas de dispositivo comunes, consulte [Directivas de dispositivo y comportamiento en casos de uso](#).

Para las plataformas iOS y Android, su sitio contiene las siguientes aplicaciones de productividad móvil preconfiguradas:

- **Citrix Secure Mail**
- **Citrix Secure Web**
- **Citrix Files**

Estas aplicaciones se encuentran en el grupo de entrega **AllUsers**.

Para obtener más información, consulte [Acerca de las aplicaciones móviles de productividad](#).

Continuar la configuración de Citrix Endpoint Management

Después de completar la configuración básica para la inscripción de dispositivos, la forma en que configure Citrix Endpoint Management varía mucho según sus casos de uso. Por ejemplo:

- ¿Cuáles son sus requisitos de seguridad y cómo quiere establecer el equilibrio entre esos requisitos y la experiencia de usuario?
- ¿Qué plataformas de dispositivo admite?
- ¿Los dispositivos son propiedad de los usuarios o de la empresa?
- ¿Qué directivas de dispositivo quiere enviar a los dispositivos?
- ¿Qué tipos de aplicaciones entrega a los usuarios?

En esta sección, se ofrece una guía sobre las diversas opciones de configuración, ya que se remite a los artículos disponibles en este conjunto de la documentación que puedan ayudarlo.

A medida que complete la configuración en sitios de terceros, tome nota de la información y su ubicación, como referencia para cuando configure parámetros en la consola de Citrix Endpoint Management.

- Seguridad y autenticación. En Citrix Endpoint Management, se usan certificados para crear conexiones seguras y para autenticar usuarios. Citrix proporciona certificados comodín para su instancia de Citrix Endpoint Management.
 - Para ver una descripción de los componentes de autenticación y las configuraciones recomendadas por nivel de seguridad, consulte el artículo [Autenticación](#) en “Conceptos avanzados”. Asimismo, consulte [Seguridad y experiencia del usuario](#).
 - Para obtener una descripción general sobre los componentes de autenticación utilizados durante las operaciones de Citrix Endpoint Management, consulte [Certificados y autenticación](#).
 - Puede elegir entre los siguientes tipos de autenticación. En la configuración de la autenticación, se incluyen tareas en las consolas de Citrix Endpoint Management y NetScaler Gateway.
 - * [Disponibilidad de la autenticación con dominio o dominio y token de seguridad](#)
 - * [Autenticación con certificado de cliente o certificado y dominio](#)
 - Para entregar certificados a los usuarios, configure:
 - * [Entidades de 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 siguen los pasos de inscripción necesarios para que los usuarios inscriban sus dispositivos en Citrix Endpoint Management. Para obtener información, consulte [Configurar modos de seguridad de inscripción](#).
 - Para permitir que los usuarios se autenticuen 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 una gran cantidad de dispositivos:
 - ★ [Implementar dispositivos mediante el Programa de implementación de Apple](#)
 - ★ [Inscribir en bloque dispositivos Apple](#)
 - ★ [Inscribir dispositivos Windows en bloque](#)
- Para inscribir dispositivos Android, cree una cuenta de administrador de Android Enterprise. Consulte [Android Enterprise](#). O consulte [Android Enterprise heredado para clientes de Google Workspace](#).
- Puede utilizar invitaciones de inscripción o enviar notificaciones para la inscripción.
 - ★ [Invitaciones de inscripción](#).
 - ★ [Notificaciones](#).
- Para obtener más información sobre la inscripción, consulte [Administrar dispositivos](#) y los artículos de ese nodo.
- Directivas de dispositivo y administración
 - Directivas de dispositivo (MDM). Todas las directivas de dispositivo de Citrix Endpoint Management están documentadas en [Directivas de dispositivo](#). Para obtener información sobre directivas de dispositivo comunes, consulte [Directivas de dispositivo y comportamiento en casos de uso](#).
 - Propiedades de cliente. En las propiedades de cliente, se ofrece información que se proporciona directamente a Citrix Secure Hub en los dispositivos de los usuarios. Consulte [Propiedades de cliente](#) y [Propiedades de cliente de Citrix Endpoint Management](#).
 - Grupos de entrega. Para ver un ejemplo de caso de uso relacionado con 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 las aplicaciones iOS mediante las compras por volumen de Apple. Para obtener más información, consulte [Compras por volumen de Apple](#).
 - Asimismo, puede utilizar Citrix Endpoint Management para implementar libros de iBooks que obtiene a través de las compras por volumen de Apple. Consulte [Agregar contenido multimedia](#).
 - Citrix ofrece aplicaciones móviles de productividad, incluidos Citrix Secure Mail y Citrix Secure Web. Consulte [Acerca de las aplicaciones móviles de productividad](#).
 - Como alternativa a Citrix Secure Mail, puede enviar clientes nativos de correo 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 documentos y datos de forma segura a aplicaciones de Microsoft Office 365, consulte [Permitir la interacción segura con aplicaciones Office 365](#) y [Directiva de Office](#).
- Para obtener información general sobre las directivas de aplicación, consulte [Directivas de aplicación y casos de uso](#).
- MDX Toolkit es una tecnología de empaquetado de aplicaciones que prepara aplicaciones de empresa para una implementación segura con Citrix Endpoint Management. El SDK de MAM reemplaza a MDX Toolkit. MDX Toolkit está programado para alcanzar su fin de vida (EOL) en julio de 2023.

Para obtener información sobre el SDK de MAM, consulte [Introducción al SDK de MAM](#).
- Para obtener más información acerca de las aplicaciones, consulte los demás artículos de [Agregar aplicaciones](#).
- En Citrix Endpoint Management, la función del control de acceso por roles (RBAC) permite asignar roles predefinidos o conjuntos de permisos a usuarios y grupos. Con estos permisos, se puede controlar el nivel de acceso de los usuarios a las funciones del sistema. Para obtener información, consulte [Configurar roles con RBAC](#).
- En Citrix Endpoint Management, puede crear acciones automatizadas para estipular la acción que se dará ante determinados eventos, ante propiedades de dispositivo o de usuario, o bien ante la existencia de ciertas aplicaciones en los dispositivos de usuario. Para obtener información, consulte [Acciones automatizadas](#).

Certificados y autenticación

March 1, 2024

Existen varios componentes que desempeñan un papel en la autenticación durante las operaciones de Citrix Endpoint Management:

- **Citrix Endpoint Management:** La seguridad y la experiencia de la inscripción se definen desde el servidor Citrix Endpoint Management. Las opciones para incorporar usuarios son:
 - Elaborar una inscripción abierta para todos o solo por invitación.

- Requerir la autenticación de dos o tres factores. Las propiedad de 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:** Con NetScaler Gateway, puede finalizar sesiones SSL de micro VPN. Asimismo, puede proteger la seguridad de los datos en tránsito en la red y definir la experiencia de autenticación cada vez que un usuario accede a una aplicación.
- **Citrix Secure Hub:** Citrix Secure Hub y Citrix Endpoint Management funcionan conjuntamente en las operaciones de inscripción. Presente en el dispositivo, Citrix Secure Hub es la entidad que se comunica con NetScaler Gateway. Cuando una sesión caduca, Secure Hub obtiene un tíquet de autenticación de NetScaler Gateway y lo envía a las aplicaciones MDX. Citrix recomienda usar fijación de certificados, que impide ataques de intermediarios (ataques de tipo “Man in the middle”). Para obtener más información, consulte la sección [Fijación de certificados](#) en el artículo Citrix Secure Hub.

Asimismo, Citrix Secure Hub favorece a la seguridad del contenedor MDX, ya que envía directivas, crea sesiones con NetScaler Gateway cuando se agota el tiempo de espera de las aplicaciones y define el tiempo de espera y la experiencia de autenticación MDX. Citrix Secure Hub también se encarga de detectar la liberación por jailbreak, así como de comprobar la geolocalización y las directivas que se apliquen.
- **Directivas MDX:** Las directivas MDX crean la caja fuerte de datos en el dispositivo. Las directivas MDX dirigen las conexiones de micro VPN de nuevo a NetScaler Gateway, aplican las restricciones del modo desconectado y las directivas de cliente (como los tiempos de espera).

Citrix Endpoint Management autentica a los usuarios en sus recursos mediante estos métodos de autenticación:

- Administración de dispositivos móviles (MDM)
 - Proveedores de identidades (IDP) alojados en la nube
 - Protocolo ligero de acceso a directorios (LDAP)
 - ★ URL de invitación y PIN
 - ★ Autenticación de dos factores
- Administración de aplicaciones móviles (MAM)
 - LDAP
 - Certificado
 - La autenticación MAM con token de seguridad requiere NetScaler Gateway.

Para obtener información adicional acerca de la configuración, consulte los siguientes artículos:

- [Cargar, actualizar y renovar certificados](#)

- [NetScaler Gateway y Citrix Endpoint Management](#)
- [Disponibilidad de la autenticación con dominio o dominio y token de seguridad](#)
- [Autenticación con certificado de cliente o certificado y dominio](#)
- [Entidades de PKI](#)
- [Proveedores de credenciales](#)
- [Certificados APNs](#)
- [SAML para Single Sign-On en Citrix Files](#)
- [Autenticación con Azure Active Directory a través de Citrix Cloud](#)
- [Autenticación con Okta a través de Citrix Cloud](#)
- [Autenticación con un dispositivo NetScaler Gateway local a través de Citrix Cloud](#)
- Para autenticarse en un servidor Wi-Fi, envíe un certificado a los dispositivos: [Directiva de redes](#)
- Para enviar un certificado único que no se utiliza para la autenticación, como un certificado raíz de CA interna, o una directiva específica: [Directiva Credenciales](#)

Certificados

Citrix Endpoint Management genera un certificado autofirmado de Secure Sockets Layer (SSL) durante la instalación para proteger los flujos de comunicación con el servidor. Reemplace ese certificado SSL por un certificado SSL de confianza procedente de una entidad de certificación conocida.

Citrix Endpoint Management también usa su propio servicio de infraestructura de clave pública (PKI) u obtiene certificados de la entidad de certificación para los certificados de cliente. Todos los productos Citrix admiten certificados comodín y de nombre alternativo de sujeto (SAN). Para la mayoría de las implementaciones, solo se necesitan dos certificados SAN o comodín.

La autenticación con certificados de cliente proporciona una capa de seguridad adicional para las aplicaciones móviles y permite que los usuarios pueden acceder sin problemas a aplicaciones HDX. Cuando se configura la autenticación con certificados de cliente, los usuarios introducen su PIN de Citrix para acceder con inicio de sesión único (Single Sign-On) 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 usa 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) proveniente de Apple. Para conocer los pasos a seguir, consulte [Certificados APNs](#).

En la siguiente tabla se muestran los formatos y los tipos de certificado para cada componente de Citrix Endpoint Management:

Componente Citrix Endpoint Management	Formato de certificado	Tipo de certificado requerido
NetScaler Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Raíz (NetScaler Gateway convierte automáticamente el formato PFX en PEM).
Citrix Endpoint Management	P12 (PFX en equipos basados en Windows)	SSL, SAML, APNs (Citrix Endpoint Management también genera una infraestructura de clave pública completa durante el proceso de instalación). Importante: Citrix Endpoint Management no admite certificados con extensión PEM. Para utilizar un certificado PEM, divida el 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 los certificados de cliente con longitudes de bits de 4096 y 2048.

Para NetScaler Gateway y Citrix Endpoint Management, se recomienda obtener certificados de servidor procedentes de una entidad de certificación pública (como Verisign, DigiCert o Thawte). Puede crear una solicitud de firma de certificado (CSR) desde la herramienta de configuración de NetScaler Gateway o de Citrix Endpoint Management. Después de crear la solicitud de firma de certificado, envíela a la entidad de certificación para que la firme. Cuando la entidad de certificación devuelva el certificado firmado, podrá 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. Verifique que todos los certificados cumplen los requisitos de Apple. Consulte la publicación de Apple: <https://support.apple.com/en-us/HT210176>.

Apple está reduciendo la duración máxima permitida de los certificados de servidor TLS. Este cambio solo afecta a los certificados de servidor emitidos después de septiembre de 2020. Con-

sulte la publicación de Apple: <https://support.apple.com/en-us/HT211025>.

Autenticación LDAP

Citrix Endpoint Management admite la autenticación por dominios para uno o varios directorios que cumplan 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 con dominio o dominio y token de seguridad](#).

Autenticación de proveedores 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 los IDP:

- Azure Active Directory a través de Citrix Cloud
 - La integración de Workspace es opcional
 - NetScaler Gateway configurado para la autenticación por certificados
 - Android Enterprise (Tech Preview; admite el modo BYOD, dispositivos totalmente administrados y perfiles de inscripción mejorados)
 - iOS para inscripciones MDM+MAM y MDM
 - Inscripciones de iOS y macOS para Apple Business Manager
 - Android heredado (AD)

Las funciones de inscripción automática, como Apple School Manager, no se admiten en estos momentos.

- Okta desde Citrix Cloud
 - La integración de Workspace es opcional
 - NetScaler Gateway configurado para la autenticación por certificados
 - Android Enterprise (Tech Preview; admite el modo BYOD, dispositivos totalmente administrados y perfiles de inscripción mejorados)
 - iOS para inscripciones MDM+MAM y MDM
 - Inscripciones de iOS y macOS para Apple Business Manager
 - Android heredado (AD)

Las funciones de inscripción automática, como Apple School Manager, no se admiten en estos momentos.

- NetScaler Gateway local desde Citrix Cloud

- NetScaler Gateway configurado para la autenticación por certificados
 - Android Enterprise (Tech Preview; admite el modo BYOD, dispositivos totalmente administrados y perfiles de inscripción mejorados)
 - iOS para inscripciones MDM+MAM y MDM
 - Android heredado (AD)
- Las funciones de inscripción automática, como el Programa de implementación de Apple, no se admiten en estos momentos.

Cargar, actualizar y renovar certificados

March 1, 2024

Se recomienda enumerar los certificados necesarios para la implementación de Citrix Endpoint Management. Utilice la lista para realizar un seguimiento de las fechas de caducidad y las contraseñas del certificado. Este artículo le ayuda a administrar certificados a lo largo de su vida útil.

Es posible que su entorno contenga estos certificados:

- Servidor Citrix Endpoint Management
 - Certificado SSL para el FQDN de MDM (necesario si migró de XenMobile Server a Citrix Endpoint Management; de lo contrario, Citrix administra este certificado)
 - Certificado SAML (para Citrix Files)
 - Certificados de CA raíz e intermedios para los certificados anteriores y otros recursos internos (StoreFront, Proxy, etc.)
 - Certificado APNs para la administración de dispositivos iOS
 - Certificado de usuario PKI para la conectividad con PKI (necesario si su entorno requiere autenticación basada en certificados)
- MDX Toolkit
 - Certificado de desarrollador de Apple
 - Perfil de datos de Apple (por aplicación)
 - Certificado APNs de Apple (para usar con Citrix Secure Mail)
 - Archivo JKS de Android

El SDK de MAM no empaqueta 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 StorageZones Controller de ShareFile
- Certificado SSL para el equilibrio de carga con Exchange (configuración de descarga)
- Certificado SSL para el equilibrio de carga con StoreFront
- Certificados de CA raíz e intermedios para los certificados anteriores

Nota:

El dispositivo cliente debe tener el certificado raíz o intermedio requerido para establecer la confianza con la entidad de certificación que emitió el certificado del servidor. De lo contrario, es posible que obtenga el error SSL 61. Para solucionar el problema:

1. Descargue u obtenga el archivo de certificado raíz o intermedio SSL (.crt o .cer) emitido por su proveedor de certificados SSL. Por lo general, el certificado raíz, intermedio o de servidor está presente en el paquete de certificados proporcionado por su proveedor de servicios SSL.
2. Instale el certificado raíz o 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

A cada certificado que cargue, le corresponderá una entrada en la tabla “Certificados”, con un resumen de su contenido. Al configurar componentes de integración con PKI que requieran un certificado, elija un certificado de servidor que cumpla los criterios. Por ejemplo, es posible que quiera configurar Citrix Endpoint Management para integrarlo en su entidad de certificación (CA) de Microsoft. La conexión a la entidad de certificación de Microsoft debe autenticarse con un certificado de cliente.

Citrix Endpoint Management puede contener o no la clave privada de un certificado determinado. Del mismo modo, Citrix Endpoint Management puede requerir o no una clave privada para los certificados que se carguen.

Esta sección ofrece instrucciones generales para cargar certificados. Para obtener más información sobre cómo crear, cargar y configurar los certificados de cliente, consulte [Autenticación de certificado de cliente o certificado + dominio](#).

Tiene dos opciones para cargar certificados:

- Cargue los certificados en la consola individualmente.
- Realice una carga en bloque de certificados con la API de REST. Esta opción solo está disponible para dispositivos iOS.

Al cargar certificados en la consola:

- Importe un almacén de claves. Luego, debe identificar la entrada en el repositorio del almacén de claves que quiere instalar, a menos que quiera cargar un formato PKCS #12.

- Importe un certificado.

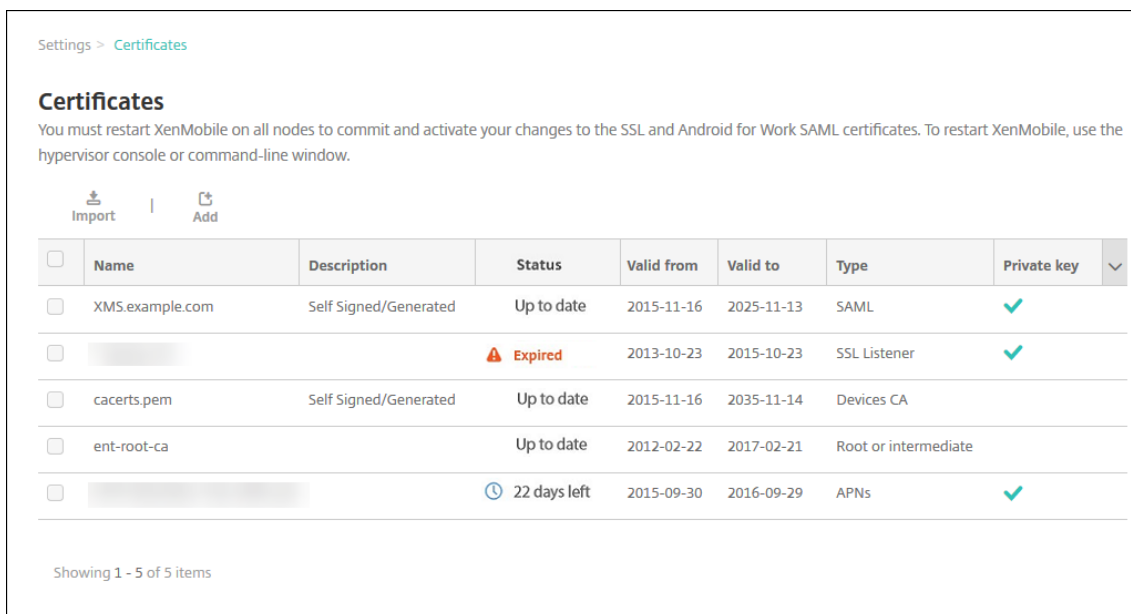
Puede cargar el certificado de CA (sin la clave privada) que usa la CA para firmar las solicitudes. También puede cargar un certificado de cliente SSL (con la clave privada) para la autenticación de clientes.

Cuando configure la entidad CA de Microsoft, especifique el certificado de CA. Seleccione el certificado de CA desde una lista de todos los certificados de servidor que sean certificados de CA. Del mismo modo, cuando configure la autenticación de cliente, podrá seleccionar un certificado de servidor de una lista que contiene 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 contener varias entradas. Al cargar entradas desde un almacén de claves, debe especificar el alias de entrada que identifica la entrada que quiere cargar. Si no se especifica ningún alias, se cargará la primera entrada del almacén. Como los archivos PKCS #12 suelen contener solo una entrada, el campo de alias no aparece cuando se selecciona PKCS #12 como tipo de almacén de claves.

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Use la barra de búsqueda para buscar y abrir el parámetro **Certificados**.



<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key	
<input type="checkbox"/>	XMS.example.com	Self Signed/Generated	Up to date	2015-11-16	2025-11-13	SAML	✓	
<input type="checkbox"/>			⚠ Expired	2013-10-23	2015-10-23	SSL Listener	✓	
<input type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	2015-11-16	2035-11-14	Devices CA		
<input type="checkbox"/>	ent-root-ca		Up to date	2012-02-22	2017-02-21	Root or intermediate		
<input type="checkbox"/>			🕒 22 days left	2015-09-30	2016-09-29	APNs	✓	

Showing 1 - 5 of 5 items

2. Haga clic en **Importar**. Aparecerá el cuadro de diálogo **Importar**.
3. Configure estos parámetros:

- **Importar:** Seleccione **Almacén de claves**.

Import ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import Keystore ▼

Keystore type PKCS#12 ▼

Use as Server ▼

Keystore file* **Browse**

Password*

Description

Cancel **Import**

- **Tipo de almacén de claves:** Seleccione **PKCS #12** en la lista.
- **Usar como:** En la lista, haga clic en la forma en que usará el certificado. Las opciones disponibles son:
 - **Servidor:** Los certificados de servidor son certificados utilizados de manera funcional por Citrix Endpoint Management. Usted carga los certificados de servidor en la consola web de Citrix Endpoint Management. En este grupo se incluyen: los certificados de la entidad de certificación (CA), los certificados de la entidad de registro (RA) y los certificados para la autenticación del cliente en los demás componentes de la infraestructura. Además, puede utilizar los certificados de servidor como un almacén para los certificados que quiera implementar en los dispositivos. Este uso se aplica especialmente a certificados de entidades de certificación utilizados para establecer una relación de confianza en el dispositivo.
 - **SAML:** La certificación de SAML (Security Assertion Markup Language) permite ofrecer acceso Single Sign-On a los servidores, los sitios web y las aplicaciones.
 - **APNs:** los certificados APNs de Apple permiten la administración de dispositivos móviles a través de Apple Push Network.

- **Escucha SSL:** La escucha de Secure Sockets Layer (SSL) notifica a Citrix Endpoint Management acerca de la actividad de cifrado SSL.
 - **Archivo de almacén de claves:** Busque el almacén de claves que quiere 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:** Escriba una descripción opcional del almacén de claves que le ayude a distinguirlo de otros almacenes.
4. Haga clic en **Importar**. El almacén de claves se agrega a la tabla “Certificados”.

Para importar un certificado

Al importar un certificado, Citrix Endpoint Management intenta crear 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 del almacén de claves forman una cadena. Cada certificado subsiguiente de la cadena debe ser el emisor del certificado anterior.

Si lo prefiere, puede agregar una descripción opcional para el certificado importado. La descripción solo se vincula al primer certificado de la cadena. Más tarde, podrá actualizar la descripción de los certificados restantes.

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Use la barra de búsqueda para buscar y abrir el parámetro **Certificados**.
2. En la página **Certificados**, haga clic en **Importar**. Aparecerá el cuadro de diálogo **Importar**. Configure las siguientes opciones:
 - **Importar:** Haga clic en **Certificado**.
 - **Usar como:** Seleccione la forma en que usará el certificado. Las opciones disponibles son:
 - **Servidor:** Los certificados de servidor son certificados utilizados de manera funcional por Citrix Endpoint Management. Usted carga los certificados de servidor en la consola web de Citrix Endpoint Management. En este grupo se incluyen: los certificados de la entidad de certificación (CA), los certificados de la entidad de registro (RA) y los certificados para la autenticación del cliente en los demás componentes de la infraestructura. Además, puede utilizar los certificados de servidor como un almacén para los certificados que quiera implementar en los dispositivos. Esta opción se aplica especialmente a entidades de certificación utilizadas para establecer una relación de confianza en el dispositivo.
 - **SAML:** La certificación de SAML (Security Assertion Markup Language) permite ofrecer acceso Single Sign-On (SSO) a los servidores, los sitios web y las aplicaciones.

- **Escucha SSL:** La escucha de Secure Sockets Layer (SSL) notifica a Citrix Endpoint Management acerca de la actividad de cifrado SSL.
- **Importación de certificado:** Busque el certificado que quiere importar. Seleccione el archivo y haga clic en **Abrir**.
- **Archivo de clave privada:** Busque el archivo de clave privada opcional del certificado. Junto con el certificado, la clave privada se usa para el cifrado y el descifrado. Seleccione el archivo y haga clic en **Abrir**.
- **Descripción:** Si quiere, escriba una descripción del certificado que le ayude a distinguirlo de otros certificados.

3. Haga clic en **Importar**. El certificado se agrega a la tabla “Certificados”.

Cargar certificados en bloque con la API de REST A veces no es razonable cargar certificados de uno en uno. En esos casos, realice una carga en bloque de certificados con la API de REST. Este método admite certificados en el formato P12. Para obtener más información acerca de la API de REST, consulte [API de REST](#).

1. Cambie el nombre de cada uno de los archivos de certificado en el formato `device_identity_value.p12`. `device_identity_value` puede ser el IMEI, el número de serie o el MEID de cada dispositivo.

A modo de ejemplo, elija utilizar números de serie como método de identificación. Hay un dispositivo con el número de serie `A12BC3D4EFGH`, así que el nombre del archivo de certificado que espera instalar en ese dispositivo deberá ser `A12BC3D4EFGH.p12`.

2. Cree un archivo de texto para almacenar las contraseñas de los certificados P12. En ese archivo, escriba el identificador de dispositivo y la contraseña de cada dispositivo en una línea nueva. Utilice el formato `device_identity_value=password`. Observe a continuación:

```
1 A12BC3D4EFGH.p12=password1!  
2 A12BC3D4EFIJ.p12=password2@  
3 A12BC3D4EFKL.p12=password3#  
4 <!--NeedCopy-->
```

3. Empaquete en un archivo ZIP todos los certificados y el archivo de texto que creó.
4. Inicie su cliente con API de REST, inicie sesión en Citrix Endpoint Management y obtenga un token de autenticación.
5. Importe los certificados, poniendo lo siguiente en el cuerpo del mensaje:

```
1 {  
2  
3     "alias": "",  
4     "useAs": "device",  
5     "uploadType": "keystore",
```

```

6     "keystoreType": "PKCS12",
7     "identityType": "SERIAL_NUMBER",           # identity type can be
        "SERIAL_NUMBER", "IMEI", "MEID"
8     "credentialFileName": "credential.txt"      # The credential file
        name in .zip
9 }
10
11 <!--NeedCopy-->

```

The screenshot shows a REST client interface with the following details:

- Method:** POST
- URL:** https://[redacted]/api/v1/certificates/import/keystore/device
- Body Type:** form-data
- Form Data:**

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> uploadFile	cert_p12.zip	
<input checked="" type="checkbox"/> certImportData	{ "alias": "", "useAs": "device", "uploadType": "keystore", "keystoreType": "PKCS12", "identityType": "SERIAL_NUMBER", "credentialFileName": "credential.txt" }	
<input type="checkbox"/> useAs		
<input type="checkbox"/> uploadType		
<input type="checkbox"/> description		
Key		Description
- Test Results:** Status: 200 OK, Time: 366 ms
- Response Body (JSON):**

```

1 {
2   "status": 0,
3   "message": "Success",
4   "successCount": 3,
5   "failedCount": 0,
6   "skipCount": 0
7 }

```

6. Cree una directiva de VPN con el tipo de credencial **Always on IKEv2** y el método de autenticación de dispositivo **Certificado de dispositivo basado en la identidad del dispositivo**. Seleccione el **tipo de identidad de dispositivo** que utilizó en los nombres de los archivos de certificado. Consulte [Directiva de VPN](#).
7. Inscriba un dispositivo iOS y espere a que se implemente la directiva de VPN. Para confirmar la instalación del certificado, compruebe la configuración de MDM en el dispositivo. También puede comprobar los detalles del dispositivo en la consola de Citrix Endpoint Management.



Devices

Users

Enrollment Invitations

Device details

2 Properties

3 User Properties

4 Assigned Policies

5 Apps

6 Media

7 Actions

8 Delivery Groups

9 iOS Profiles

administrator | iPhone

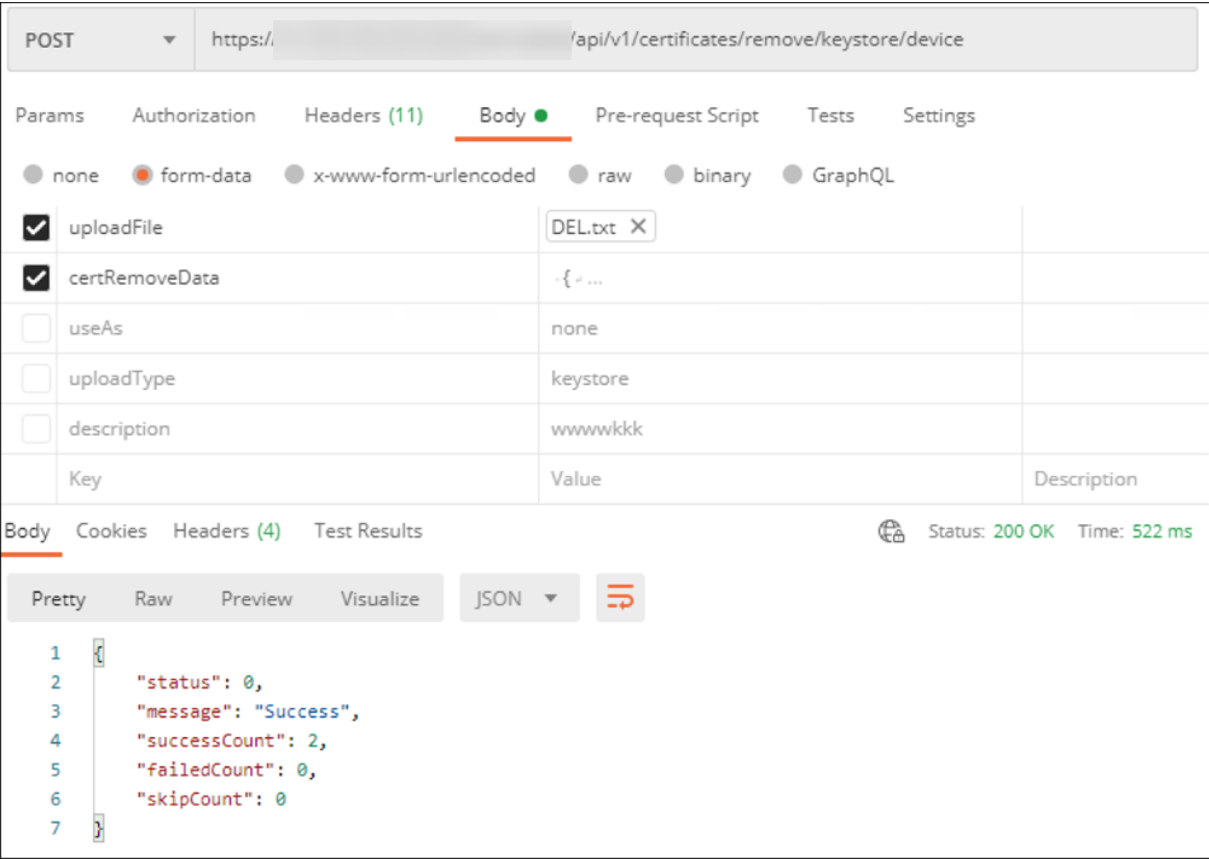
iOS Profiles

Last iOS profile inventory: 4/19/20 4:01:07 am

Name	Type	Organization	Description
+ MDM Configuration ()			
- Device Certificate Based on Device Identity Type (Citrix, id)			

También puede eliminar certificados en bloque mediante la creación de un archivo de texto con el valor `device_identity_value` listado para cada certificado que quiere eliminar. En la API de REST, llame a la API de eliminación y use esta solicitud, y sustituya `device_identity_value` por el identificador correspondiente:

```
1  ```\n2  {\n3\n4      "identityType"="device_identity_value"\n5  }\n6\n7  <!--NeedCopy-->  ```\n
```



Actualizar un certificado

Citrix Endpoint Management solo permite 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 certificado nuevo para reemplazar un certificado antiguo, no se puede eliminar ese certificado. Al configurar el parámetro “Entidades de PKI”, ambos certificados existen en el menú **Certificado de cliente SSL**. El certificado más reciente está por debajo de la lista con respecto al certificado antiguo.

Para actualizar los certificados

1. Para crear un certificado de sustitución, siga los pasos descritos en [Autenticación con certificado de cliente o certificado y dominio](#).

Importante:

No utilice la opción para crear un certificado con la clave privada existente. Al crear un certificado para actualizar un certificado que pronto caducará, la clave privada también debe ser nueva.

2. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Use la barra de búsqueda para buscar y abrir el parámetro **Certificados**.
3. En el cuadro de diálogo **Importar**, importe el nuevo certificado.

Al actualizar un certificado de servidor, los componentes que utilizaban el certificado anterior pasan automáticamente a utilizar el nuevo. Del mismo modo, si ha implementado el certificado de servidor en dispositivos, el certificado se actualizará automáticamente en la siguiente implementación.

Para actualizar un certificado APNs, siga los pasos necesarios para crear un certificado y, a continuación, vaya al Portal de certificados push de Apple. Para obtener más información, consulte [Para renovar un certificado APNs](#).

Si NetScaler Gateway se ha configurado para la descarga de SSL, debe actualizar el equilibrador de carga con el nuevo cacert.perm.

Nota:

Si migró de XenMobile local a Citrix Endpoint Management y piensa actualizar el certificado, contacte con Citrix Support después de completar los pasos anteriores. Debe proporcionarles una copia del nuevo certificado (en formato PFX), incluida la contraseña del certificado. Citrix Support actualizará NetScaler de la nube y reiniciará los nodos de arrendatarios para finalizar el proceso de actualización de certificados.

Para actualizar una entidad de certificación (CA) de servicio de PKI

Puede solicitar que Citrix Cloud Operations actualice o regenere las entidades internas de certificación de PKI en su entorno de Citrix Endpoint Management. Abra un caso de asistencia técnica para estas solicitudes.

- 1 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 pasa a ser no válido. No podrá seguir ejecutando operaciones seguras en su entorno ni acceder a los recursos de Citrix Endpoint Management.

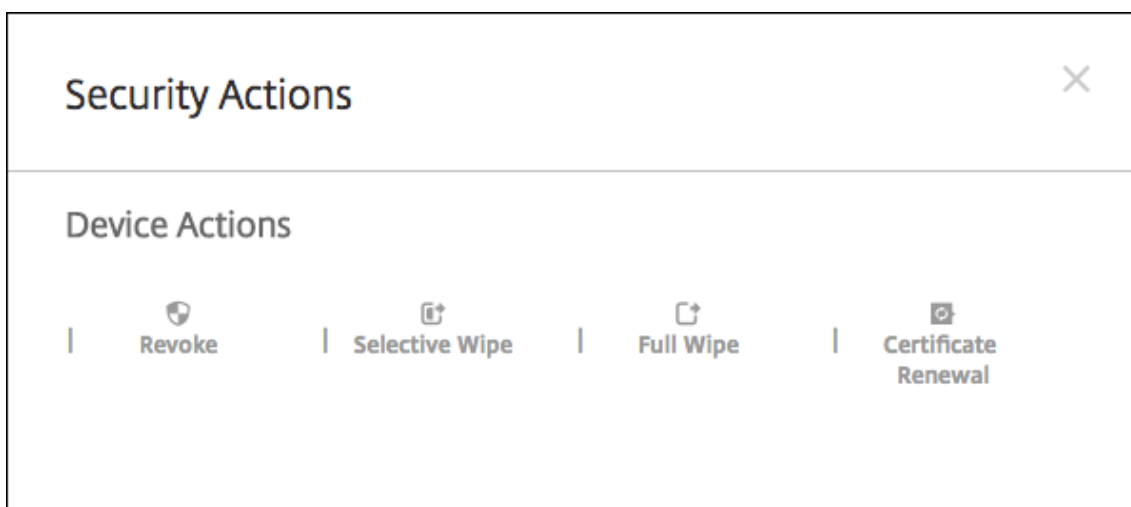
La entidad de certificación (CA) le pide que renueve su certificado SSL antes de la fecha de caducidad. Siga los pasos descritos anteriormente para actualizar el certificado y, a continuación, iniciar una renovación de certificados en los dispositivos inscritos.

Para dispositivos iOS, macOS, y Android compatibles, puede iniciar la renovación de certificados mediante la acción de seguridad Renovación de certificado. Los certificados de dispositivos se renuevan desde la consola de Citrix Endpoint Management o la API pública de REST. En caso de dispositivos Windows inscritos, los usuarios deben volver a inscribir sus dispositivos para recibir una nueva entidad de certificación (CA) de dispositivo.

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 CA.

Para renovar certificados de dispositivo mediante la consola

1. Vaya a **Administrar > Dispositivos** y seleccione los dispositivos cuyos certificados quiera renovar.
2. Haga clic en **Proteger** y en **Renovación de certificados**.



Los dispositivos inscritos continúan funcionando sin interrupciones. Citrix Endpoint Management emite un certificado de dispositivo cuando este se conecta de nuevo al servidor.

Para enviar consultas sobre los dispositivos que se encuentran en un grupo de CA emisora de certificados específico:

1. En **Administrar > Dispositivos**, expanda el panel **Filtros**.
2. En el panel **Filtros**, expanda **CA de emisión de certificados para dispositivos** y seleccione las CA emisoras que quiere renovar.

En la tabla de dispositivos, aparecen los dispositivos de las CA emisoras seleccionadas.

Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days
Enrolled	MOM	testuser0006 "testuser0006"	macOS			8/9/18 2:30:57 pm	4 days
Enrolled	MOM	testuser0001 "testuser0001"	macOS			8/9/18 2:31:36 pm	4 days
Enrolled	MOM	testuser0024 "testuser0024"	macOS			8/9/18 2:32:14 pm	4 days
Enrolled	MOM	testuser0023 "testuser0023"	macOS			8/9/18 2:32:20 pm	4 days
Enrolled	MOM	testuser0022 "testuser0022"	macOS			8/9/18 2:32:25 pm	4 days
Enrolled	MOM	testuser0021 "testuser0021"	macOS			8/9/18 2:32:31 pm	4 days
Enrolled	MOM	testuser0073 "testuser0073"	macOS			8/9/18 2:41:05 pm	4 days
Enrolled	MOM	testuser0082 "testuser0082"	macOS			8/9/18 2:42:42 pm	4 days

Para renovar certificados de dispositivo mediante la API de REST

Citrix Endpoint Management utiliza internamente las siguientes entidades de certificación (CA) para PKI: CA raíz, CA del dispositivo y CA del servidor. Esas CA se clasifican como un grupo lógico y se les proporciona un nombre de grupo. Durante el aprovisionamiento de Citrix Endpoint Management, el servidor genera tres CA y les asigna el nombre de grupo “predeterminado”.

La entidad de certificación emite las siguientes API para administrar y renovar los certificados de dispositivo. Los dispositivos ya inscritos continúan funcionando sin interrupciones. Citrix Endpoint Management emite un certificado de dispositivo cuando este se conecta de nuevo al servidor. Para obtener más información, descargue el documento PDF [Public API for REST Services](#).

- Envíe una lista de dispositivos que todavía utilicen la CA antigua (consulte la sección 3.16.2 en el PDF Public API for REST Services)
- Renovar certificado de dispositivo (véase la sección 3.16.58)
- Obtener todos los grupos de CA (véase la sección 3.23.1)

Certificado APNs para Citrix Secure Mail

Los certificados Apple Push Notification Service (APNs) caducan cada año. Debe crear un certificado SSL de APNs y actualizarlo en el portal de Citrix antes de que caduque. Si el certificado caduca, los usuarios sufrirán interrupciones del servicio de notificaciones push en Citrix Secure Mail. Tampoco podrá seguir enviando notificaciones push a sus aplicaciones.

Certificado APNs para la administración de dispositivos iOS

Para inscribir y administrar dispositivos iOS en Citrix Endpoint Management, debe configurar y crear un certificado del servicio de notificaciones push de Apple (APNs) proveniente 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 información más detallada, consulte [Certificados APNs](#).

Para ver el estado y la fecha de caducidad del certificado APNs, inicie sesión en el portal Apple Push Certificates Portal. Debe iniciar sesión con el mismo usuario con que creó el certificado.

Asimismo, Apple le enviará una notificación por correo electrónico entre 30 y 10 días antes de la fecha de caducidad. Esa notificación contendrá la siguiente información:

```
1 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.
2
3 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.
4
5 Thank You,
6
7 Apple Push Notification Service
8 <!--NeedCopy-->
```

MDX Toolkit (certificado de distribución iOS)

Una aplicación que se ejecute en un dispositivo iOS físico (aparte de las aplicaciones del App Store de Apple) presenta estos requisitos de firma:

- Debe firmar la aplicación con un perfil de datos.
- Debe firmar la aplicación con un certificado de distribución correspondiente.

Para comprobar que dispone de un certificado de distribución iOS válido, lleve a cabo lo siguiente:

1. Desde el portal Apple Enterprise Developer, cree un ID de aplicación explícito para cada aplicación que quiera empaquetar con MDX. Un ejemplo de ID de aplicación válido es: `com.CompanyName.ProductName`.
2. Desde el portal Apple Enterprise Developer, vaya a **Provisioning Profiles > Distribution** y cree un perfil de datos interno. Repita este paso para cada ID de aplicación que haya creado en el paso anterior.
3. Descargue todos los perfiles de datos. Para obtener más información, consulte [Empaquetado de aplicaciones móviles iOS](#).

Para confirmar que todos los certificados de servidor Citrix Endpoint Management son válidos, lleve a cabo lo siguiente:

1. En la consola de Citrix Endpoint Management, haga clic en **Parámetros > Certificados**.
2. Compruebe que todos los certificados (APNs, escucha de SSL, raíz e intermedio) son válidos.

Almacén de claves Android

El almacén de claves es un archivo que contiene certificados utilizados para firmar las aplicaciones Android. Cuando una clave caduca, los usuarios ya no pueden actualizar fácilmente la aplicación a una nueva versión.

NetScaler Gateway

Para obtener información más detallada sobre cómo gestionar la caducidad de los certificados en NetScaler Gateway, consulte [How to handle certificate expiry on NetScaler](#) en Knowledge Center de la asistencia de Citrix.

Un certificado caducado de NetScaler Gateway impide que los usuarios inscriban sus dispositivos y accedan a la tienda. El certificado caducado también impide que los usuarios se conecten al servidor Exchange cuando utilicen Citrix Secure Mail. Además, los usuarios no podrán conocer ni abrir las aplicaciones HDX (según el certificado caducado).

Command Center (Centro de comandos) y Expiry Monitor (Centro de supervisión de caducidad) son dos herramientas que pueden ayudarle a hacer un seguimiento de los certificados de NetScaler Gateway. Command Center le notifica cuándo caduca el certificado. Esas 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 StorageZones Controller de ShareFile
- Certificado SSL para el equilibrio de carga con Exchange (configuración de descarga)
- Certificado SSL para el equilibrio de carga con StoreFront
- Certificados de CA raíz e intermedios para los certificados anteriores

NetScaler Gateway y Citrix Endpoint Management

March 1, 2024

Cuando se integra en Citrix Endpoint Management, NetScaler Gateway proporciona un mecanismo para que los dispositivos accedan de manera remota a la red interna y a los recursos. Porque Citrix Endpoint Management crea una micro VPN que se extiende desde las aplicaciones presentes en el dispositivo hasta NetScaler Gateway.

Puede utilizar Citrix Gateway Service (Tech Preview) o un dispositivo NetScaler Gateway local, también conocido como NetScaler Gateway. Para obtener información general sobre las dos soluciones

de NetScaler Gateway, consulte [Configurar el uso de NetScaler Gateway con Citrix Endpoint Management](#).

Configurar la autenticación para el acceso de dispositivos remotos a la red interna

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Parámetros**.
2. En **Servidor**, haga clic en **NetScaler Gateway**. Aparecerá la página **NetScaler Gateway**. En el siguiente ejemplo, existe una instancia de NetScaler Gateway.

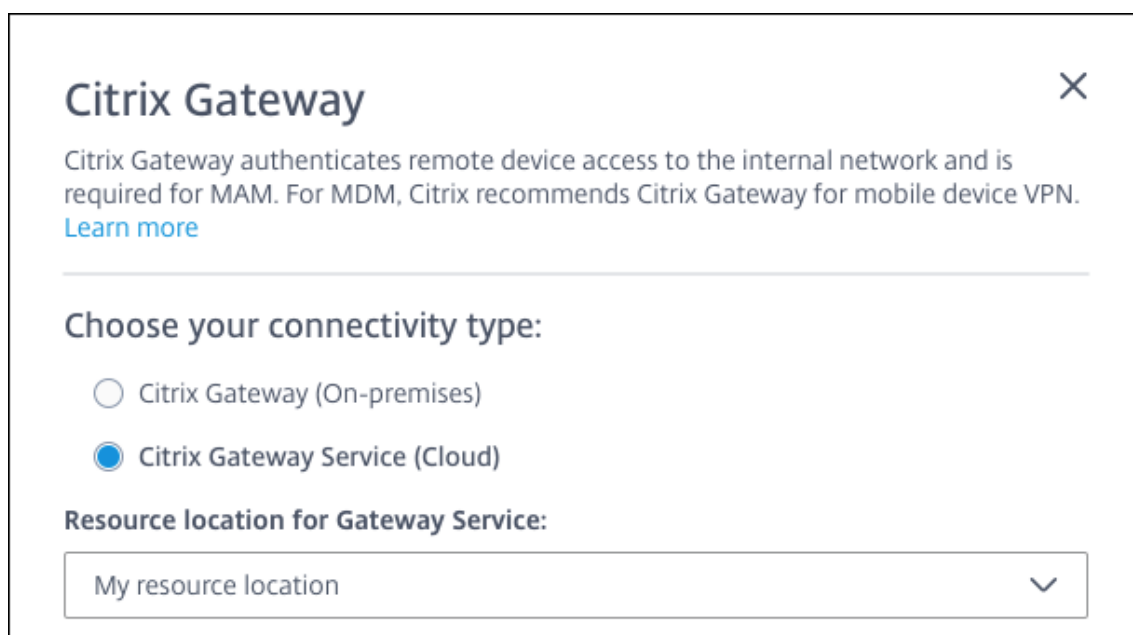
<input type="checkbox"/>	Name	Default	External URL	Logon Type	# of Callback URLs	
<input checked="" type="checkbox"/>	testNS	✓	https://testns.domain.com	Domain	0	

3. Configure estos parámetros:
 - **Autenticación:** Seleccione si quiere habilitar la autenticación. El valor predeterminado es **Activado**.
 - **Entregar certificado de usuario para autenticación:** Seleccione si quiere 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 del cliente. El valor predeterminado es **Desactivado**.
 - **Proveedor de credenciales:** En la lista, haga clic en el proveedor de credenciales que se va a utilizar. Para obtener más información, consulte [Proveedores de credenciales](#).
4. Haga clic en **Guardar**.

Agregar una instancia de Citrix Gateway Service (Tech Preview)

Después de guardar los parámetros de autenticación, puede agregar una instancia de NetScaler Gateway a Citrix Endpoint Management.

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Se abrirá la página **Parámetros**.
2. En la página **Parámetros**, vaya al mosaico de NetScaler Gateway y, a continuación, haga clic en **Iniciar configuración**. Aparecerá la página **NetScaler Gateway**.
3. Seleccione **Citrix Gateway Service (nube)** y especifique la ubicación del recurso.

A screenshot of the Citrix Gateway configuration dialog box. The title bar says "Citrix Gateway" with a close button (X) in the top right. Below the title, there is a paragraph: "Citrix Gateway authenticates remote device access to the internal network and is required for MAM. For MDM, Citrix recommends Citrix Gateway for mobile device VPN." followed by a blue link "Learn more". A horizontal line separates this from the next section, "Choose your connectivity type:", which has two radio button options: "Citrix Gateway (On-premises)" and "Citrix Gateway Service (Cloud)". The second option is selected. Below this is the section "Resource location for Gateway Service:" with a dropdown menu currently showing "My resource location" and a downward arrow icon.

- **Ubicación del recurso para Gateway Service:** Se necesita si utiliza Citrix Secure Mail. Especifique la ubicación del recurso para el servicio STA. La ubicación del recurso debe incluir un dispositivo NetScaler Gateway configurado. Si más adelante quiere quitar la ubicación de un recurso configurada para Gateway Service, actualice este parámetro.

Después de completar esa configuración, haga clic en **Conectar** para establecer la conexión. Se agregará el nuevo NetScaler Gateway. El icono de **Citrix Gateway Service (nube)** aparecerá en la página **Parámetros**. Para modificar una instancia, haga clic en **Ver más**. Si los Gateway Connectors no están disponibles en la ubicación de recursos seleccionada, haga clic en **Agregar Gateway Connector**. Siga las instrucciones en pantalla para instalar Gateway Connectors. También puede agregar Gateway Connectors más tarde.

4. Haga clic en **Guardar y exportar script**.

- **Guardar y exportar script.** Haga clic en el botón para guardar los parámetros y exportar un paquete de configuración. Puede cargar un script desde el paquete en NetScaler Gateway para configurarlo con los parámetros de Citrix Endpoint Management. Para obtener información, consulte “Configurar un NetScaler Gateway local para usarlo con Citrix Endpoint Management” más adelante en este artículo.

Ha agregado el nuevo NetScaler Gateway. El icono de **NetScaler Gateway** aparecerá en la página **Parámetros**. Para modificar una instancia, haga clic en **Ver más**.

Configurar un NetScaler Gateway local para usarlo con Citrix Endpoint Management

Para configurar un NetScaler Gateway local y usarlo con Citrix Endpoint Management, realice los pasos generales descritos en las secciones siguientes.

1. Compruebe que su entorno cumple los requisitos previos.
2. Exporte el paquete del script desde la consola de Citrix Endpoint Management.
3. Extraiga los archivos del paquete. Si solo utiliza directivas clásicas en NetScaler Gateway y está ejecutando Citrix ADC 13.0 o una versión anterior, utilice el script que indica “Classic” en el nombre de archivo. Si utiliza alguna directiva avanzada o está ejecutando Citrix ADC 13.1 o una versión posterior, utilice el script que indica “Advanced” en el nombre de archivo.
4. Ejecute el script correspondiente en el dispositivo NetScaler Gateway. Consulte el archivo Léame suministrado con los scripts para ver instrucciones detalladas actualizadas.
5. Pruebe la configuración.

Los scripts configuran los parámetros de NetScaler Gateway que necesita Citrix Endpoint Management:

- Servidores virtuales de NetScaler Gateway necesarios para MAM y MDM
- Directivas de sesión para los servidores virtuales de NetScaler Gateway
- Detalles del servidor de Citrix Endpoint Management
- Equilibrador de carga proxy para la validación de certificados
- Acciones y directivas de autenticación para el servidor virtual NetScaler Gateway. Los scripts describen los parámetros de configuración de LDAP.
- Directivas y acciones de tráfico de red para el servidor proxy
- Perfil de acceso sin cliente
- Registro DNS local estático en NetScaler Gateway
- Otros enlaces: directiva de servicio, certificado de CA

Los scripts no se ocupan de la siguiente configuración:

- Equilibrio de carga de Exchange
- Equilibrio de carga de Citrix Files
- Configuración del proxy ICA
- Descarga de SSL

Requisitos previos para utilizar 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 del script. Si cambia la configuración, vuelva a exportar el paquete del script.

Requisitos de NetScaler Gateway:

- Al utilizar la autenticación por certificados en el dispositivo NetScaler Gateway, debe crear certificados SSL en un dispositivo Citrix ADC. Consulte [Crear y utilizar certificados SSL en un dispositivo Citrix ADC](#).
- NetScaler Gateway (como mínimo la versión 11.0, compilación 70.12).
- La dirección IP de NetScaler Gateway está configurada y tiene conectividad con el servidor LDAP, a menos que LDAP tenga la carga equilibrada.
- La dirección IP de subred (SNIP) de NetScaler Gateway está configurada, tiene conectividad con los servidores back-end necesarios y tiene acceso de red pública por el puerto 8443/TCP.
- DNS puede resolver dominios públicos.
- NetScaler Gateway tiene las licencias Platform/Universal o Trial. Para obtener información, consulte <https://support.citrix.com/article/CTX126049>.

Exportar el paquete del script desde Citrix Endpoint Management

Después de guardar los parámetros de autenticación, puede agregar una instancia de NetScaler Gateway a Citrix Endpoint Management.

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Se abrirá la página **Parámetros**.
2. En la página **Parámetros**, vaya al mosaico de NetScaler Gateway y, a continuación, haga clic en **Iniciar configuración**. Aparecerá la página **NetScaler Gateway**.
3. Seleccione **NetScaler Gateway (local)** y configure estos parámetros:

Citrix Gateway

×

Citrix Gateway authenticates remote device access to the internal network and is required for MAM. For MDM, Citrix recommends Citrix Gateway for mobile device VPN. [Learn more](#)

Choose your connectivity type:

- 1 We recommend that you configure LDAP settings before Citrix Gateway. The script that you export after saving your Gateway configuration must include your LDAP settings.
- 2 Provide the Citrix Gateway details.

Name

Application name

External URL


Publicly accessible URL

Logon type

Domain

▼
- 3 Click **Save and Export Script** to save your settings and download a .tar.gz script bundle. The script bundle includes a Readme file with detailed installation instructions.

Save and Export Script



- **Nombre:** Escriba un nombre para la instancia de NetScaler Gateway.
- **URL externa:** Escriba la URL de acceso público de NetScaler Gateway. Por ejemplo: <https://receiver.com>.
- **Tipo de inicio de sesión:** Haga clic en un tipo de inicio de sesión. Los tipos pueden ser: **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 dispone de varios dominios, use **Certificado y dominio**. Para obtener más información, consulte Configurar la autenticación para varios dominios.

La autenticación por certificados en el dispositivo NetScaler Gateway requiere una configuración adicional. Por ejemplo, debe cargar el certificado de CA raíz en el dispositivo Citrix ADC. Consulte [Crear y utilizar certificados SSL en un dispositivo Citrix ADC](#).

Para obtener más información, consulte [Authentication](#) en Deployment Handbook.

4. Haga clic en **Guardar y exportar script**.

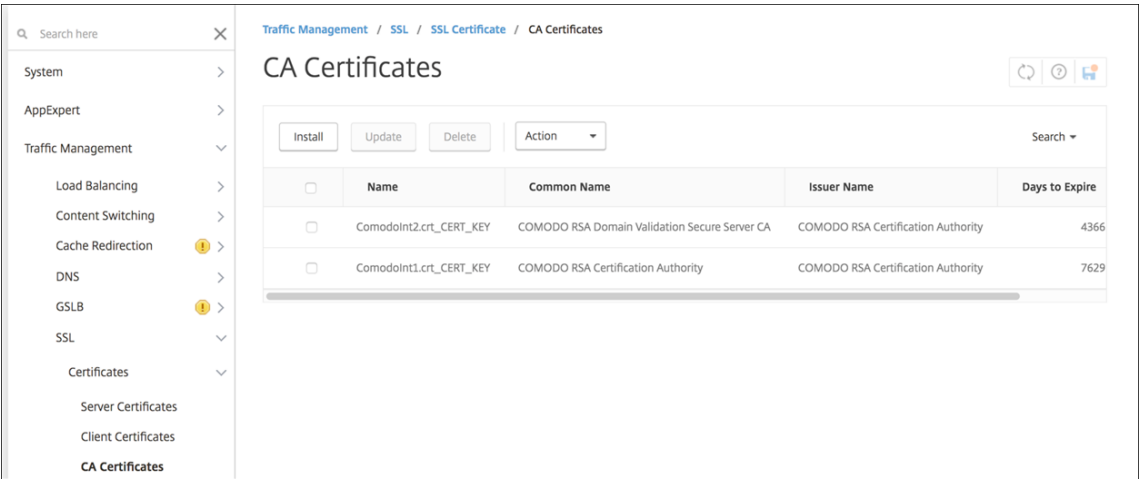
- **Guardar y exportar script.** Haga clic en el botón para guardar los parámetros y exportar un paquete de configuración. Puede cargar un script desde el paquete en NetScaler Gateway para configurarlo con los parámetros de Citrix Endpoint Management. Para obtener información, consulte “Configurar un NetScaler Gateway local para usarlo con Citrix Endpoint Management” más adelante en este artículo.

Ha agregado el nuevo NetScaler Gateway. El icono de **NetScaler Gateway** aparecerá en la página **Parámetros**. Para modificar una instancia, haga clic en **Ver más**.

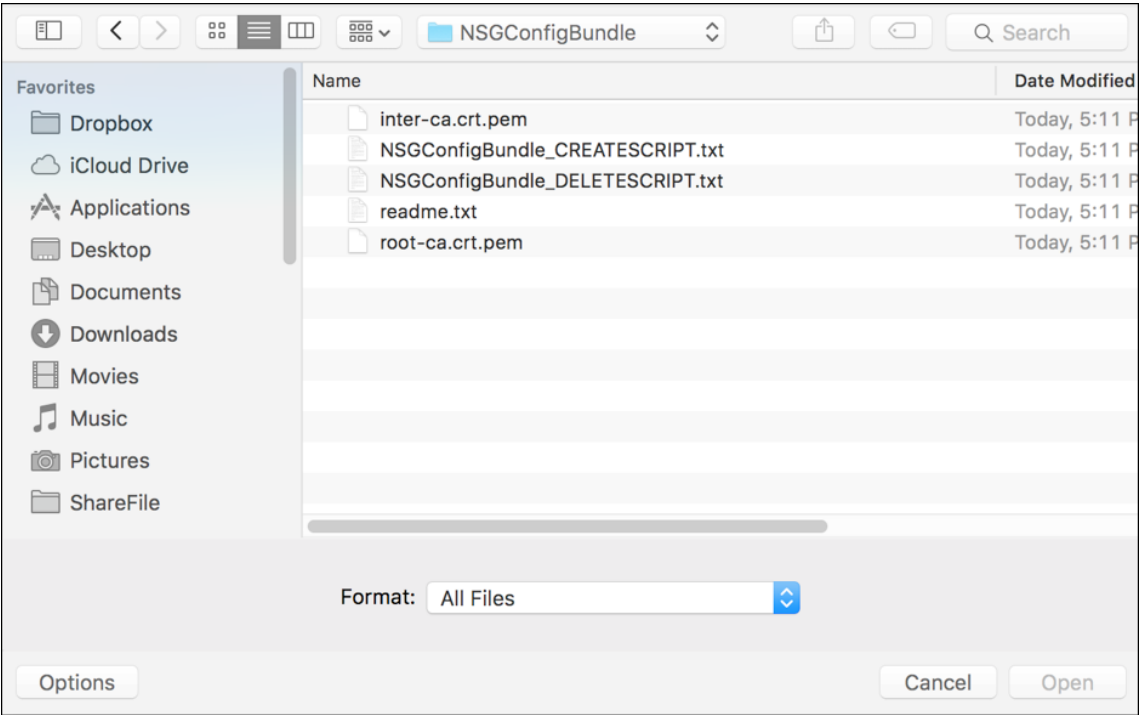
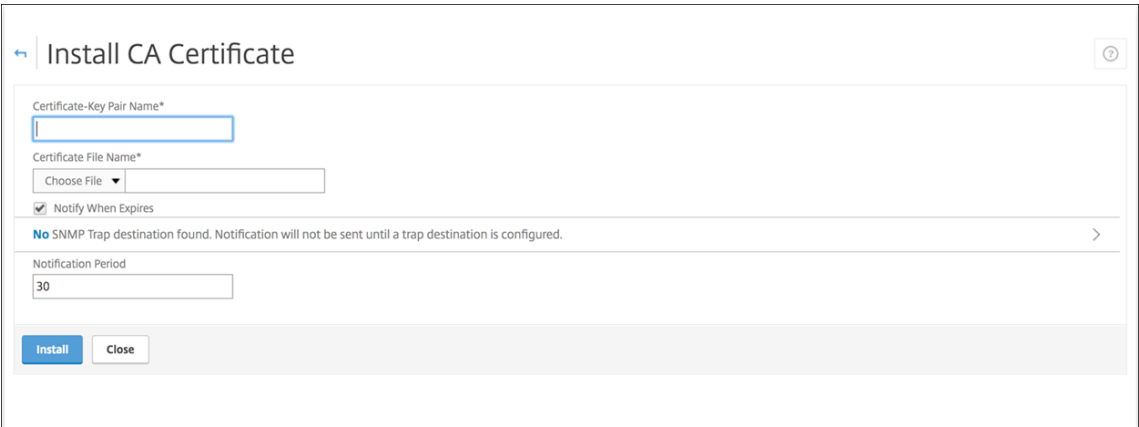
Instalar el script en el entorno

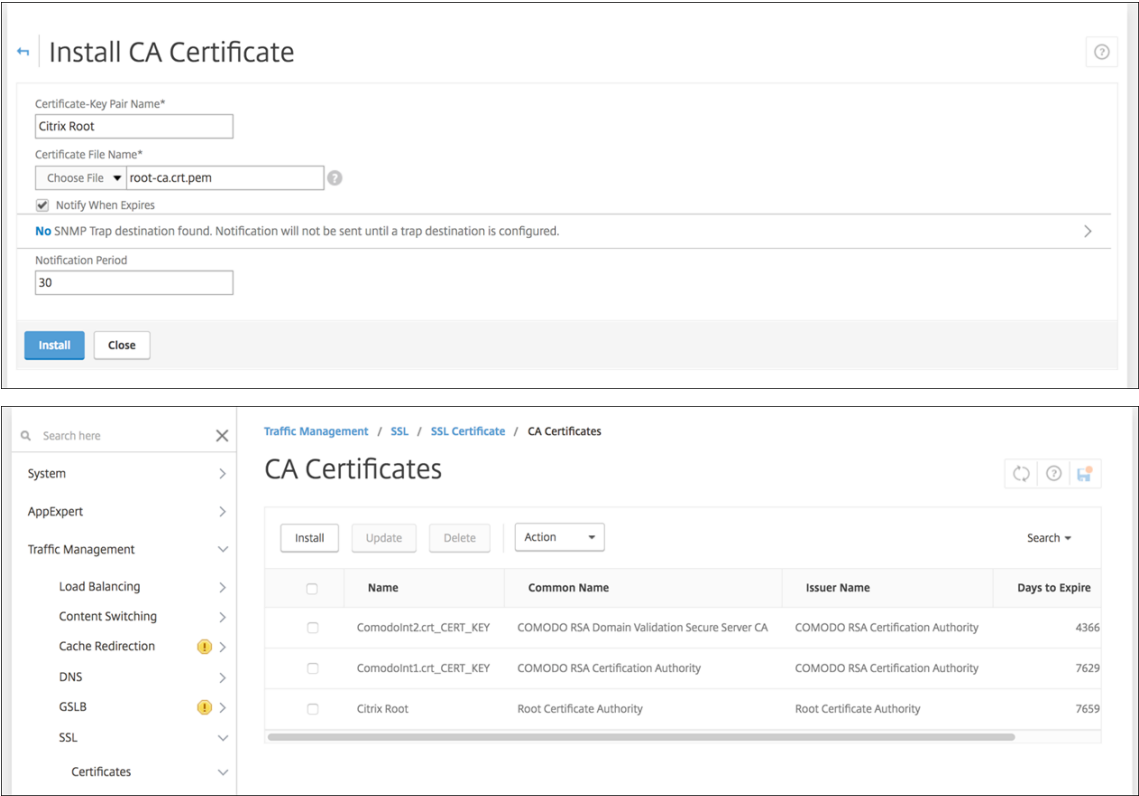
El paquete del script incluye lo siguiente:

- Un archivo Léame con instrucciones detalladas
 - Scripts que contienen los comandos de interfaz de línea de comandos de NetScaler que se usan para configurar los componentes necesarios en NetScaler
 - Certificado de CA raíz público y certificado de CA intermedio
 - Scripts que contienen los comandos de interfaz de línea de comandos de NetScaler necesarios para quitar la configuración de NetScaler
1. Cargue e instale los archivos de certificado (proporcionados en el paquete del script) en el dispositivo Citrix ADC, en el directorio `/nsconfig/ssl/`. Consulte [Crear y utilizar certificados SSL en un dispositivo Citrix ADC](#).



En los siguientes ejemplos se muestra cómo instalar el certificado raíz.





Debe instalar tanto el certificado raíz como el certificado intermedio.

2. Modifique el script (ConfigureCitrixGatewayScript_Classic.txt o ConfigureCitrixGatewayScript_Advanced.txt) para reemplazar todos los marcadores de posición con 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 modificado en el bash shell de NetScaler, como se describe en el archivo Léame incluido en el paquete del script. 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"
```

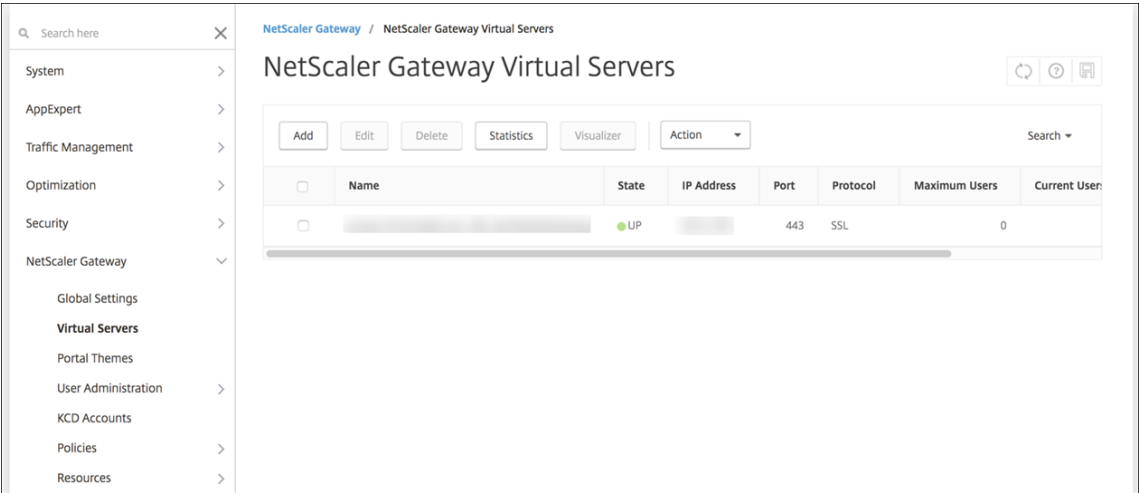
Cuando el script se complete, aparecerán las siguientes líneas.

```
exec: save ns config
Done
Done
root@ns#
```

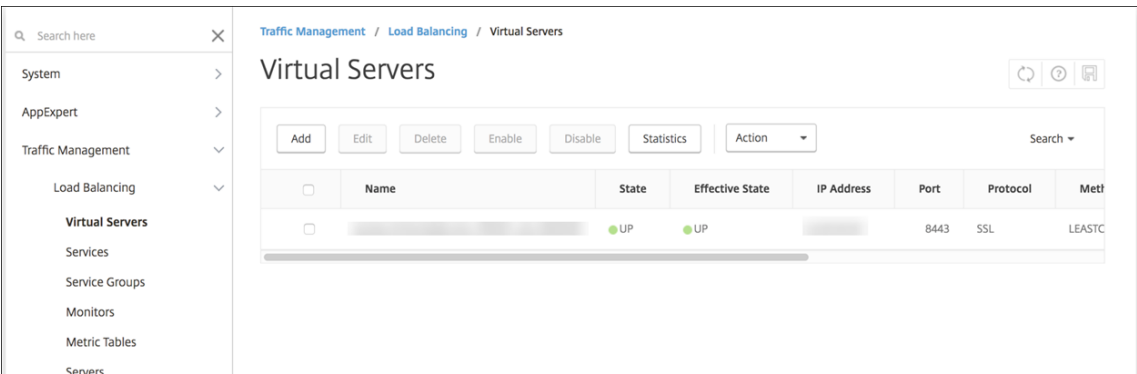
Probar la configuración

Para validar la configuración:

- 1. Compruebe que el servidor virtual NetScaler Gateway muestra el estado operativo (UP).



- 2. Compruebe que el servidor virtual de equilibrio de carga proxy muestra el estado operativo (UP).



3. Abra un explorador web, conéctese a la URL de NetScaler Gateway e intente autenticarse. Si la autenticación tiene éxito, se le redirigirá a un mensaje de página no encontrada: “HTTP Status 404 - Not Found”.
4. Inscriba un dispositivo y compruebe que obtiene la inscripción en MDM y MAM.

Configurar la autenticación para varios dominios

Si tiene varias instancias de Citrix Endpoint Management (por ejemplo, para entornos de prueba, desarrollo y producción) debe configurar manualmente NetScaler Gateway para los entornos adicionales (puede usar el asistente de NetScaler para XenMobile solamente una vez).

Configuración de NetScaler Gateway

Para configurar las directivas de autenticación de NetScaler Gateway y una directiva de sesión para un entorno de varios dominios:

1. En la herramienta de configuración de NetScaler Gateway, en la ficha **Configuración**, expanda **NetScaler Gateway > Directivas > Autenticación**.
2. En el panel de navegación, haga clic en **LDAP**.
3. Haga clic para modificar el perfil de LDAP. Cambie el **Atributo de nombre de inicio de sesión del servidor** a **userPrincipalName** o al atributo que quiera utilizar para las búsquedas. Tome nota del atributo que especifique. Proporciónelo cuando configure las opciones de LDAP en la consola de Citrix Endpoint Management.

Other Settings

Server Logon Name Attribute

sAMAccountName

Search Filter

Group Attribute

memberOf

Sub Attribute Name

cn

- Repita estos pasos para cada directiva de LDAP. Se requiere una directiva de LDAP diferente para cada dominio.
- En la directiva de sesión vinculada al servidor virtual de NetScaler Gateway, vaya a **Modificar perfil de sesiones > Aplicaciones publicadas**. Compruebe que la opción **Single Sign-On Domain** está en blanco.

Configurar Citrix Endpoint Management

Si quiere configurar LDAP para un entorno de Citrix Endpoint Management de varios dominios:

- En la consola de Citrix Endpoint Management, vaya a **Parámetros > LDAP** y agregue o modifique un directorio.

Settings > LDAP

LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Support nested groups NO

Add

Directory Type	Domain Name	Server/Port	User Base DN	Group Base DN	Default
<input type="checkbox"/> Microsoft Active Directory			dc=,dc=	dc=,dc=	<input checked="" type="checkbox"/>

Showing 1 - 1 of 1 items

- Proporcione la información correspondiente.
 - En **Alias de dominio**, especifique los dominios que se utilizarán para la autenticación de usuarios. Separe los dominios con una coma y no introduzca espacios entre ellos. Por ejemplo: dominio1.com,dominio2.com,dominio3.com
 - Asegúrese de que el campo **Buscar usuarios por** coincide con el valor de **Server Logon Name Attribute** especificado en la directiva LDAP de NetScaler Gateway.

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	Microsoft Active Directory
Primary server*	10.
Secondary server	IP Address or FQDN
Port*	389
Domain name*	Araujo.local
User base DN*	dc=,dc= ⓘ
Group base DN*	dc=,dc= ⓘ
User ID*	Administrator@
Password*	
Domain alias*	
XenMobile Lockout Limit	0 ⓘ
XenMobile Lockout Time	1 ⓘ
Global Catalog TCP Port	3268 ⓘ
Global Catalog Root Context	dc=example,dc=com ⓘ
User search by	userPrincipalName
Use secure connection	<input type="radio"/> NO

Descartar solicitudes de conexión entrantes a direcciones URL específicas

Si NetScaler Gateway en su entorno está configurado para la descarga de SSL, puede que prefiera que la puerta de enlace descarte las solicitudes de conexión entrantes para direcciones URL específicas. Si prefiere esa seguridad adicional, contacte con Citrix Cloud Operations y solicite que incluyan su IP en sus centros de datos locales.

Disponibilidad de la autenticación con dominio o dominio y token de seguridad

March 1, 2024

Citrix Endpoint Management admite la autenticación por dominios en uno o varios directorios que cumplan el protocolo ligero de acceso a directorios (LDAP). Puede configurar 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:

Una vez que los usuarios hayan inscrito sus dispositivos en Citrix Endpoint Management, Citrix Endpoint Management no admite que se cambie el modo de autenticación del modo de un

tipo de autenticación dominio a otro modo de autenticación. Por ejemplo, no puede cambiar el modo de autenticación de **Dominio de autenticación** a **Dominio + certificado** una vez que los usuarios se hayan inscrito.

Acerca de LDAP

El protocolo LDAP es un protocolo de aplicación de código abierto y no vinculado a ningún proveedor específico. Se utiliza para acceder a servicios de información sobre directorios distribuidos a través de una red de protocolo de Internet (IP) y para su mantenimiento. Los servicios de información de directorios se usan para compartir información acerca de usuarios, sistemas, redes, servicios y aplicaciones disponibles a través de la red.

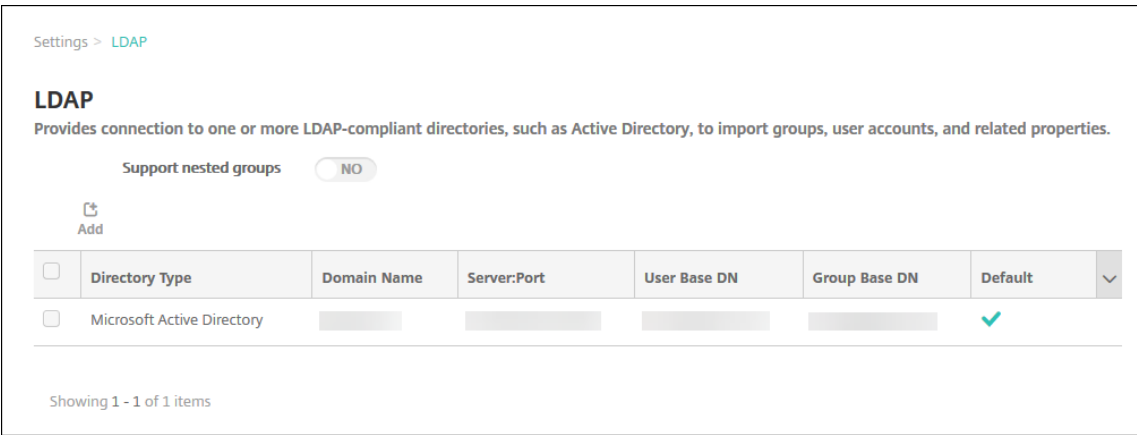
Un uso común de LDAP es proporcionar Single Sign-On a los usuarios, donde varios servicios comparten una sola contraseña (por usuario). Single Sign-On permite a los usuarios iniciar sesión una vez en el sitio web de la empresa para obtener acceso autenticado a la intranet corporativa.

Un cliente inicia una sesión LDAP al conectarse a un servidor LDAP, denominado Directory System Agent (DSA). El cliente envía una solicitud de operación al servidor, y el servidor responde con la autenticación pertinente.

Para agregar o modificar conexiones LDAP en Citrix Endpoint Management

Por regla general, las conexiones LDAP se configuran cuando se empieza a utilizar Citrix Endpoint Management, como se describe en [Para configurar LDAP](#). Si empezó a utilizar Endpoint Management antes de que estuvieran disponibles las pantallas mostradas en esa sección, 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**.

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	Microsoft Active Directory	
Primary server*	IP Address or FQDN	
Secondary server	IP Address or FQDN	
Port*	389	
Domain name*		
User base DN*	dc=example,dc=com	?
Group base DN*	dc=example,dc=com	?
User ID*		
Password*		
Domain alias*		
XenMobile Lockout Limit	0	?
XenMobile Lockout Time	1	?
Global Catalog TCP Port	3268	?
Global Catalog Root Context	dc=example,dc=com	?
User search by	userPrincipalName	
Use secure connection	<input type="radio"/> NO	

Cancel Save

4. Configure estos parámetros:

- **Tipo de directorio:** En la lista, haga clic en el tipo de directorio correspondiente. El valor predeterminado es **Microsoft Active Directory**.
- **Servidor principal:** Escriba el servidor principal usado para el protocolo LDAP; puede escribir la dirección IP o el nombre de dominio completo (FQDN).
- **Servidor secundario:** Si quiere, puede introducir la dirección IP o el nombre de dominio completo (FQDN) del servidor secundario (si se ha configurado). Este es un servidor de conmutación por error que se utilizará si no se puede establecer contacto con el servidor principal.
- **Puerto:** Escriba el número de puerto que utiliza el servidor LDAP. De forma predeterminada, el número de puerto es **389** para conexiones LDAP no protegidas. Use el número de puerto **636** para conexiones LDAP protegidas, el **3268** para conexiones LDAP no protegidas

de Microsoft o el **3269** para conexiones LDAP protegidas de Microsoft.

- **Nombre de dominio:** Introduzca el nombre de dominio.
- **DN base de usuarios:** Mediante un identificador único, escriba la ubicación de los usuarios en Active Directory. Los ejemplos de sintaxis son: `ou=users`, `dc=example` o `dc=com`.
- **DN base de grupos:** Escriba la ubicación de los grupos de 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 del nombre de dominio. Si cambia el parámetro **Alias del dominio** después de la inscripción, los usuarios deben volver a inscribirse.
- **Límite de bloqueo de Citrix Endpoint Management:** Escriba un número comprendido entre **0** y **999** para la cantidad de intentos fallidos de inicio de sesión. Si escribe **0** en este campo, indicará a Citrix Endpoint Management que nunca bloquee al usuario en función de los intentos fallidos de inicio de sesión. El valor predeterminado es **0**.

Debe decidir si establecer este límite de bloqueo en un valor inferior al de la directiva de bloqueo de LDAP. Con ello, evitará que haya usuarios bloqueados si Citrix Endpoint Management no puede autenticarse en el servidor LDAP. Por ejemplo, si la directiva de bloqueo LDAP es de 5 intentos, configure este límite de bloqueo en **4** o menos.
- **Duración de bloqueo de Citrix Endpoint Management:** Escriba un número comprendido entre **0** y **99999**; este dígito representará la cantidad de minutos que el usuario debe esperar una vez superado el límite de bloqueo. Un valor de **0** significa que no se obliga al usuario a esperar después de un bloqueo. El valor predeterminado es **1**.
- **Puerto TCP del catálogo global:** Escriba el número del puerto TCP destinado al servidor de catálogo global. De forma predeterminada, el número de puerto TCP está establecido en **3268**; para las conexiones SSL, utilice el número de puerto **3269**.
- **Contexto raíz del catálogo global:** Si quiere, puede escribir el valor del contexto raíz del catálogo global utilizado para habilitar una búsqueda en el catálogo global de Active Directory. Esta búsqueda se agrega a la búsqueda estándar LDAP en cualquier dominio y sin necesidad de especificar el nombre de dominio real.
- **Buscar usuarios 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 su ID de usuario en este formato al inscribirse. Si cambia el parámetro **Buscar usuarios por** después de la inscripción, los usuarios deben volver a inscribirse.

Si elige **userPrincipalName**, los usuarios escriben un nombre principal de usuario (UPN) en este formato:

- *nombre de usuario@dominio*

Si elige **sAMAccountName**, los usuarios escriben un nombre de administrador de cuentas de seguridad (SAM) en uno de estos formatos:

- *nombre de usuario@dominio*
- *dominio\nombre de usuario*

- **Usar conexión segura:** Seleccione si utilizar conexiones protegidas. De forma predeterminada, está **desactivado**.

5. Haga clic en **Guardar**.

Para eliminar un directorio compatible con LDAP

1. En la tabla **LDAP**, seleccione el directorio a eliminar.

Puede eliminar más de una propiedad. Para ello, marque la casilla de verificación situada junto a cada propiedad.

2. Haga clic en **Eliminar**. Aparecerá un cuadro de diálogo de confirmación. Vuelva a hacer clic en **Eliminar**.

Configurar la autenticación de dominio y token de seguridad

Puede configurar Citrix Endpoint Management para exigir a los usuarios que se autenticuen mediante el protocolo RADIUS con sus credenciales de LDAP más una contraseña de un solo uso.

Para una experiencia de uso 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 escribir repetidamente sus nombres de usuario ni contraseñas LDAP. Los usuarios escriben su nombre de usuario y contraseña para la inscripción, la caducidad de contraseñas y el bloqueo de cuentas.

Configurar parámetros de LDAP

Si quiere usar el protocolo LDAP para la autenticación, debe instalar un certificado SSL desde una entidad de certificación en Citrix Endpoint Management. Para obtener información, consulte [Cargar certificados](#).

1. En **Parámetros**, haga clic en **LDAP**.

2. Seleccione **Microsoft Active Directory** y, a continuación, haga clic en **Modificar**.

Settings > LDAP

LDAP
Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Support nested groups ☐ NO

Add | Edit | Delete

	Directory Type	Domain Name	Server:Port	User Base DN	Group Base DN	Default
<input checked="" type="checkbox"/>	Microsoft Active Directory			dc=,dc=net	dc=,dc=net	✓

3. Verifique que el campo “Puerto” tiene el valor **636** para conexiones LDAP seguras, o bien **3269** para conexiones LDAP seguras de Microsoft.
4. Cambie **Usar conexión segura** a **Sí**.

Port* 636

Domain name*

User base DN* ⓘ

Group base DN* ⓘ

User ID*

Password*

Domain alias* net

XenMobile Lockout Limit ⓘ 0

XenMobile Lockout Time ⓘ 1

Global Catalog TCP Port ⓘ 3269

Global Catalog Root Context ⓘ dc=example,dc=com

User search by userPrincipalName

Use secure connection ☒ YES

Cancel Save

Configurar parámetros de NetScaler Gateway

En los siguientes pasos se supone que ya ha agregado una instancia de NetScaler Gateway a Citrix Endpoint Management. Para agregar una instancia de NetScaler Gateway, consulte NetScaler Gateway y Citrix Endpoint Management .

1. En **Parámetros**, haga clic en **NetScaler Gateway**.
2. Seleccione NetScaler Gateway y, a continuación, haga clic en **Modificar**.
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, vaya a **Parámetros > Propiedades de cliente** y marque las casillas **Enable Citrix PIN Authentication** y **Enable User Password Caching**. Para obtener más información, consulte [Propiedades de cliente](#).

Configurar NetScaler Gateway para la autenticación de dominio y token de seguridad

Configure directivas y perfiles de sesión de NetScaler Gateway para los servidores virtuales que utilice con Citrix Endpoint Management. Para obtener información, consulte la documentación de NetScaler Gateway.

Autenticación con certificado de cliente o certificado y dominio

March 1, 2024

En Citrix Endpoint Management, la autenticación predeterminada es el nombre de usuario y la contraseña. Para agregar otra capa de seguridad para la inscripción y el acceso al entorno de Citrix Endpoint Management, considere la posibilidad de usar 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 con certificado y dominio tiene las mejores posibilidades de SSO junto con la seguridad que proporciona la autenticación de dos factores en NetScaler Gateway.

Para una experiencia de uso óptima, puede combinar la autenticación por certificado y dominio junto con el PIN de Citrix y el almacenamiento en caché de contraseñas de Active Directory. Con resultado, los usuarios no tienen que escribir repetidamente sus nombres de usuario ni contraseñas LDAP. Los usuarios escriben su nombre de usuario y contraseña para la inscripción, la caducidad de contraseñas y el bloqueo de cuentas.

Importante:

Una vez que los usuarios hayan inscrito sus dispositivos en Citrix Endpoint Management, Citrix Endpoint Management no admite que se cambie el modo de autenticación de dominio a otro modo de autenticación.

Si no permite LDAP y usa tarjetas inteligentes o métodos similares, la configuración de los certificados permite representar una tarjeta inteligente en Citrix Endpoint Management. Los usuarios se inscriben mediante un PIN único que Citrix Endpoint Management genera para ellos. Una vez que el usuario haya obtenido acceso, Citrix Endpoint Management crea e implementa el certificado utilizado a partir de entonces para autenticarse en el entorno de Citrix Endpoint Management.

Puede utilizar el asistente de NetScaler para XenMobile para llevar a cabo la configuración necesaria para Citrix Endpoint Management cuando se usa la autenticación con solo certificado o la autenticación con certificado y dominio en NetScaler Gateway. Puede ejecutar el asistente de NetScaler para XenMobile solamente una vez.

En los entornos de alta seguridad, donde el uso de las credenciales de LDAP fuera de una organización en redes públicas o no seguras se considera una amenaza acuciante a la seguridad de la organización. Para entornos altamente seguros, la autenticación de dos factores mediante un certificado del cliente y un token de seguridad es una posibilidad. Para obtener más información, consulte [Configurar Citrix Endpoint Management para la autenticación con certificado y token de seguridad](#).

La autenticación de certificado del cliente está disponible para dispositivos inscritos en MAM y MDM+MAM. Para usar la autenticación de certificado de cliente con esos dispositivos, debe configurar el servidor Microsoft, el servidor de Citrix Endpoint Management y, a continuación, NetScaler Gateway. Siga estos pasos generales, como se describe en este artículo.

En el servidor Microsoft:

1. Agregue el complemento de Certificados a la consola MMC (Microsoft Management Console).
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. Cree una entidad PKI para la autenticación por certificado.
3. Configure proveedores de credenciales.
4. Configure NetScaler Gateway para entregar un certificado de usuario para la autenticación.

Para obtener información sobre la configuración de NetScaler Gateway, consulte los siguientes artículos de la documentación de Citrix ADC:

- [Autenticación del cliente](#)
- [Infraestructura de los perfiles SSL](#)
- [Configuring and Binding a Client Certificate Authentication Policy](#).

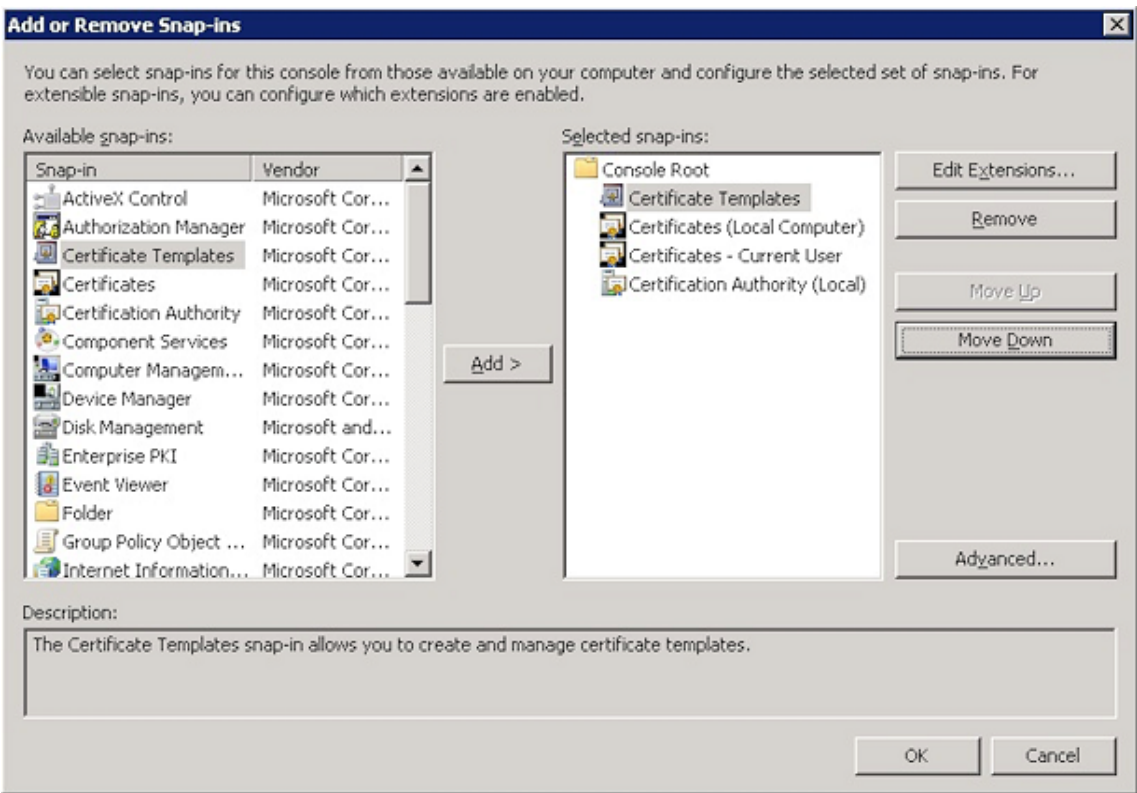
Requisitos previos

- Cuando cree plantillas de entidad para Servicios de certificado de Microsoft, no use caracteres especiales para evitar posibles problemas de autenticación en los dispositivos inscritos. Por ejemplo, no use estos caracteres en el nombre de la plantilla: : ! \$ () # % + * ~ ? | { } []

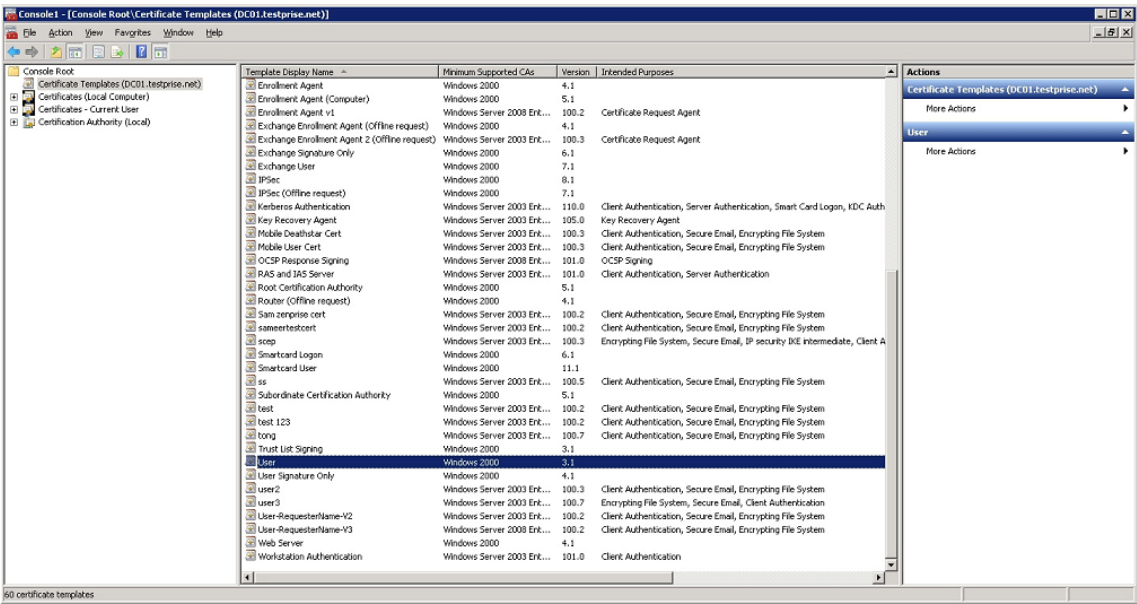
- Para configurar la autenticación basada en certificados para Exchange ActiveSync, consulte la [documentación de Microsoft sobre Exchange Server](#). Configure el sitio del servidor de la entidad de certificación (CA) para que Exchange ActiveSync requiera certificados de cliente.
- Si utiliza certificados de servidor privados para proteger el tráfico de ActiveSync hacia el servidor Exchange Server, compruebe que los dispositivos móviles tienen todos los certificados raíz e intermedios. De lo contrario, la autenticación basada en certificados falla durante la configuración de buzones de correo en Citrix Secure Mail. En la consola IIS de Exchange, debe:
 - Agregar un sitio web para que Citrix Endpoint Management lo use con Exchange y enlazar el certificado de servidor web.
 - Usar el puerto 9443.
 - Para ese sitio web, debe agregar dos aplicaciones, una para “Microsoft-Server-ActiveSync” y otra para “EWS”. En ambas aplicaciones, en **Configuración de SSL**, habilite **Requerir SSL**.

Agregar el complemento de Certificados a Microsoft Management Console

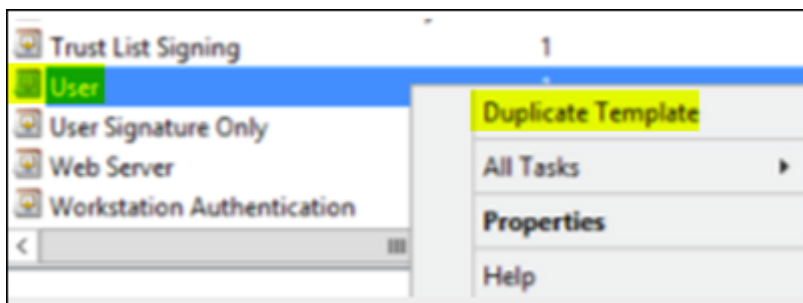
1. Abra la consola y haga clic en **Agregar o quitar complemento**.
2. Agregue los complementos siguientes:
 - Plantillas de certificado
 - Certificados (Equipo local)
 - Certificados (Usuario local)
 - Entidad de certificación (Local)



3. Expanda **Plantillas de certificado**.



4. Seleccione la plantilla **Usuario** y **Duplicar plantilla**.



5. Suministre el nombre para mostrar de la plantilla.

Importante:

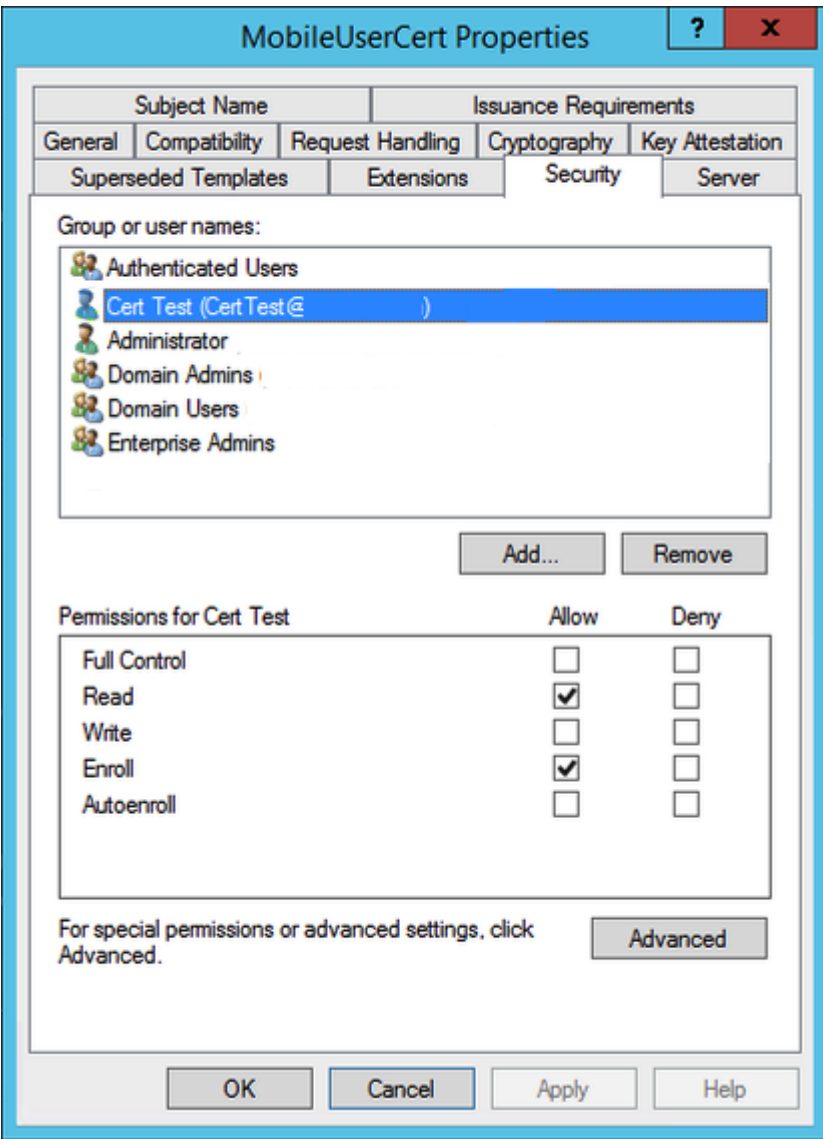
Marque la casilla **Publicar certificado en Active Directory** solo si es necesario. Si selecciona esta opción, todos los certificados de cliente de los usuarios se crearán en Active Directory, lo que podría desorganizar su base de datos de Active Directory.

6. Seleccione **Windows 2003 Server** como tipo de plantilla. En Windows 2012 R2 Server, en **Compatibilidad**, seleccione **Entidad de certificación** y defina **Windows 2003** como destinatario.
7. En **Seguridad**, haga clic en **Agregar** y seleccione la cuenta del usuario de AD que Citrix Endpoint Management utilizará para generar certificados.

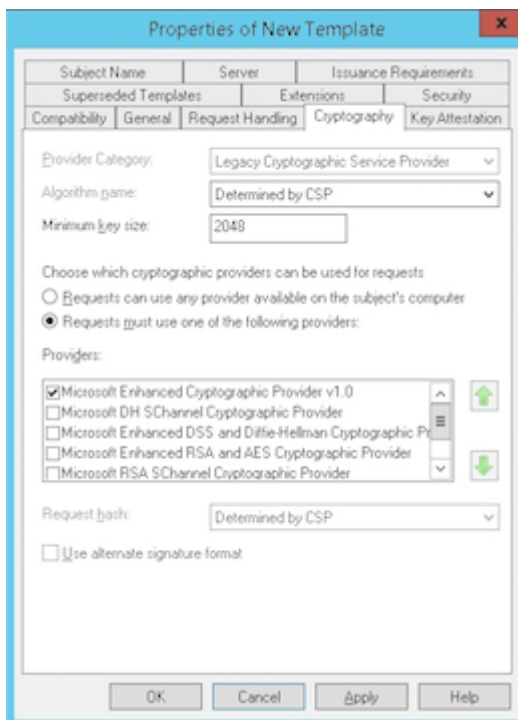
Importante:

Agregue solo el usuario de la cuenta de servicio aquí. Agregue el permiso **Inscribir** solo a esta cuenta de usuario de AD.

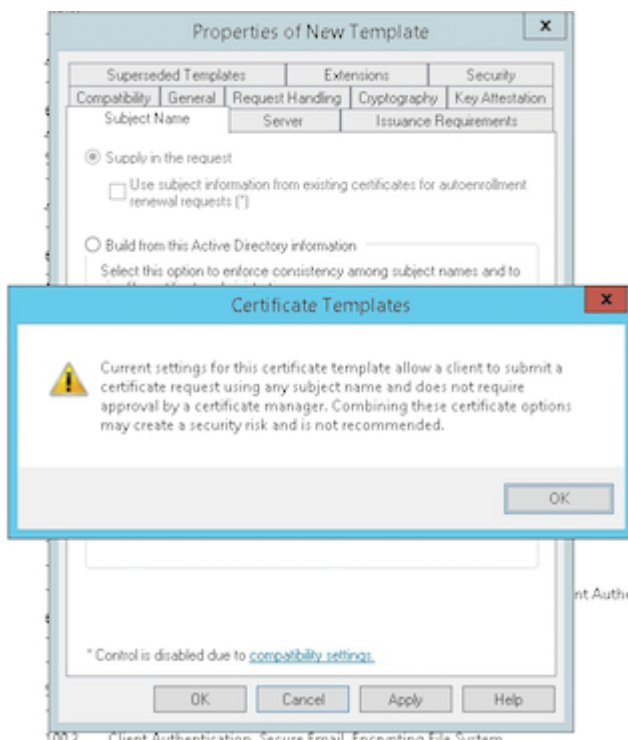
Como se describe más adelante en este artículo, creará un certificado de usuario PFX mediante la cuenta de servicio. Para obtener información, consulte [Crear un certificado PFX desde el servidor de CA](#).



8. En **Criptografía**, compruebe que indica el tamaño de la clave. Deberá indicar el tamaño de esa clave más adelante, durante la configuración de Citrix Endpoint Management.

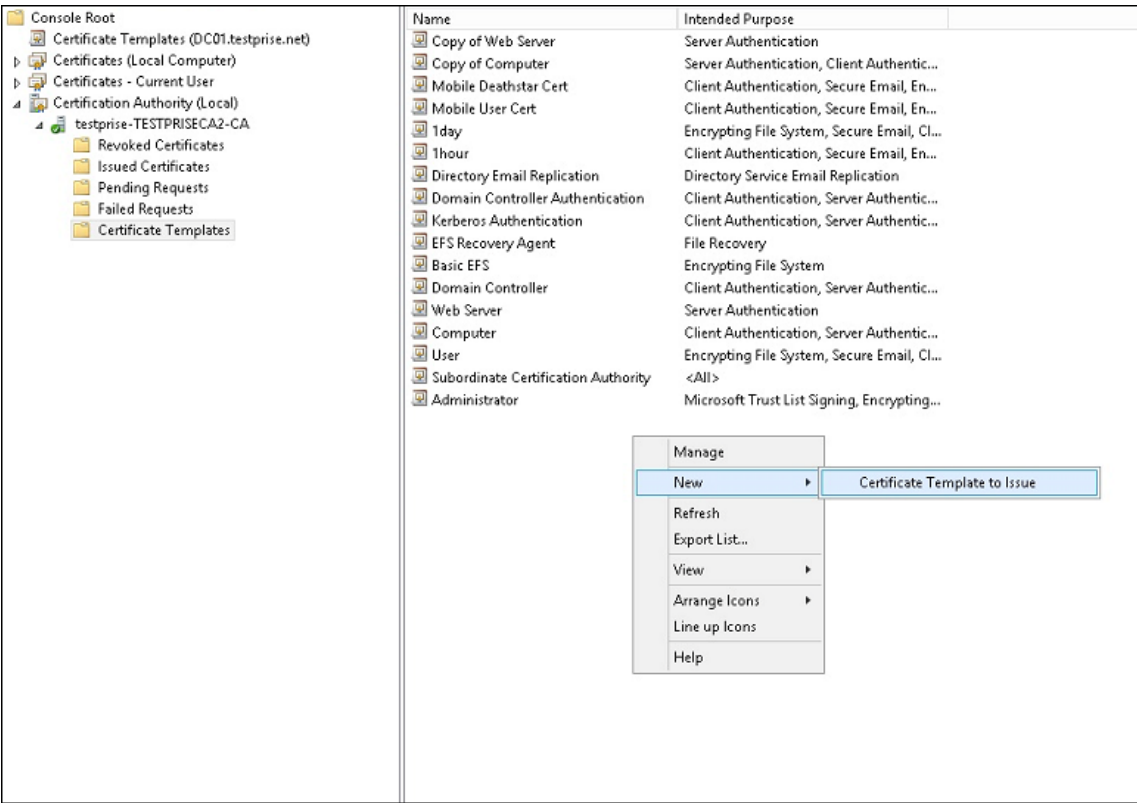


9. En **Nombre del sujeto**, seleccione **Proporcionado por el solicitante**. Aplique y guarde los cambios.

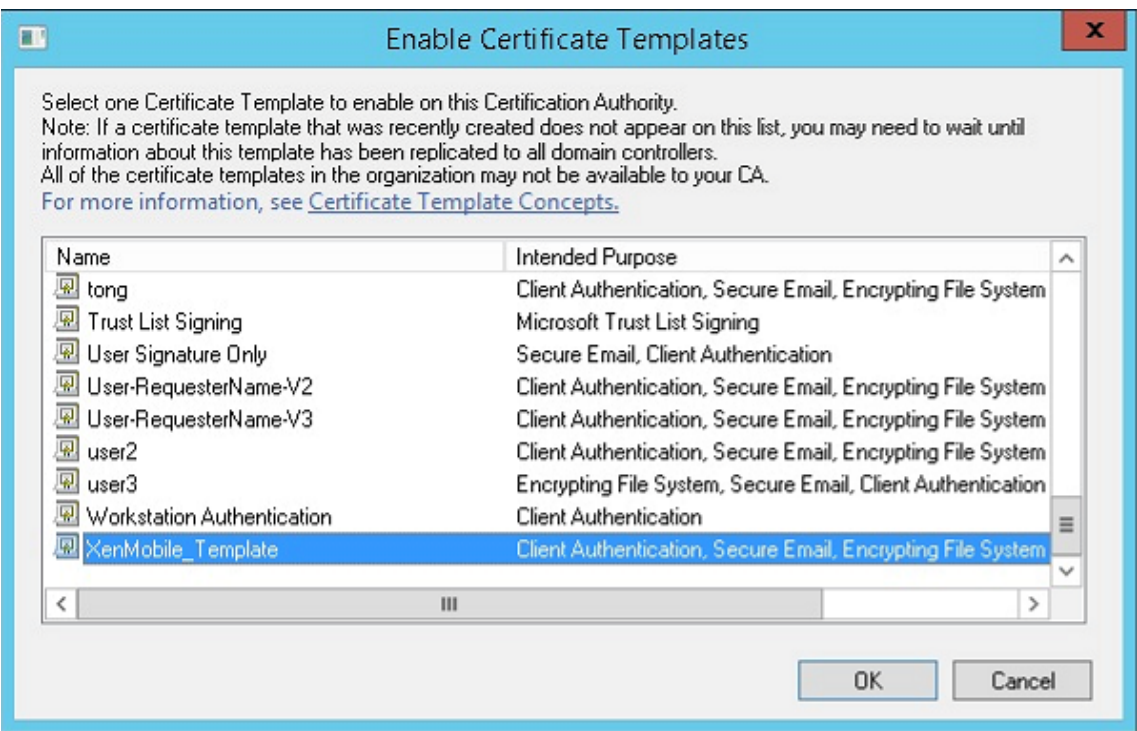


Agregar la plantilla a la entidad de certificación

1. Vaya a **Entidad de certificación** y seleccione **Plantillas de certificado**.
2. Haga clic con el botón secundario en el panel derecho y seleccione **Nueva > Plantilla de certificado que se va a emitir**.

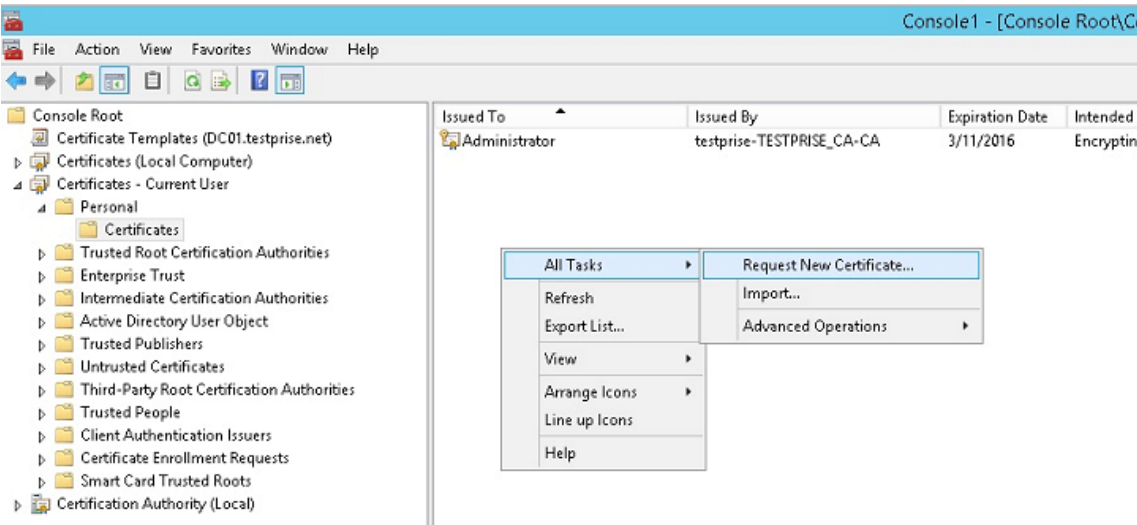


3. Seleccione la plantilla que creó en el paso anterior y haga clic en **Aceptar** para agregarla a la **Entidad de certificación**.

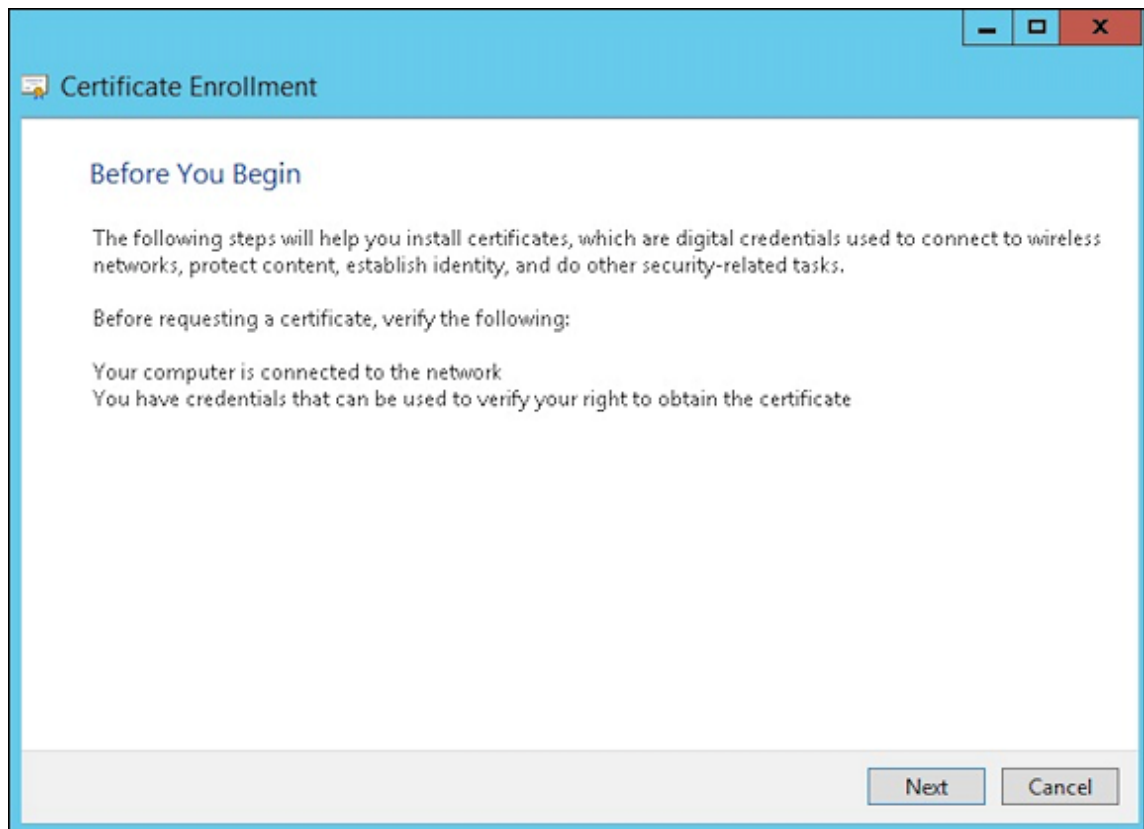


Crear un certificado PFX desde el servidor de CA

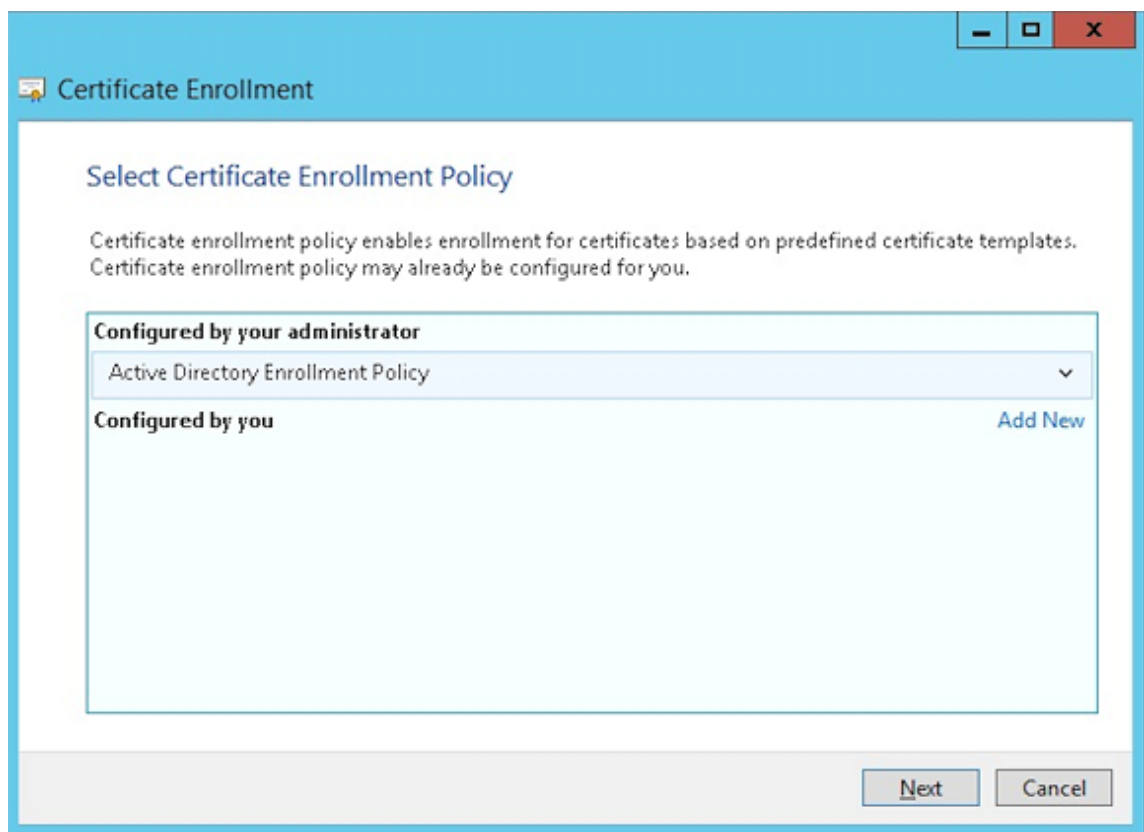
1. Cree un certificado .pfx de usuario con la cuenta de servicio con la que inició sesión. Este PFX se carga en Citrix Endpoint Management, el cual solicita un certificado de usuario de parte de los usuarios que inscriban sus dispositivos.
2. En **Usuario actual**, expanda **Certificados**.
3. Haga clic con el botón secundario en el panel derecho y después haga clic en **Solicitar un nuevo certificado**.



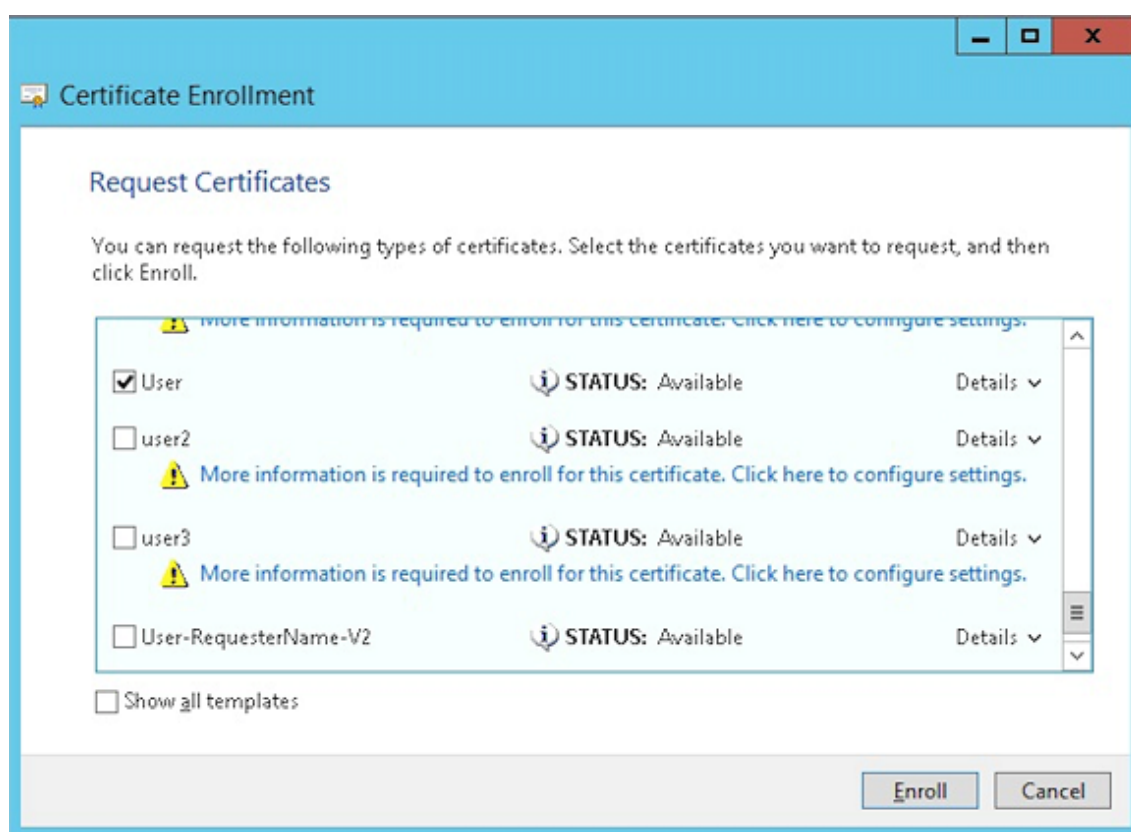
4. Aparecerá la pantalla **Inscripción de certificados**. Haga clic en **Siguiente**.



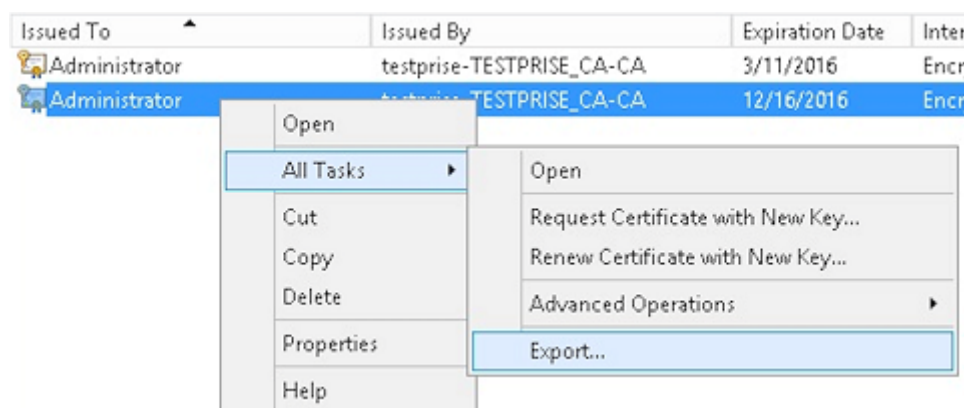
5. Seleccione **Directiva de inscripción de Active Directory** y haga clic en **Siguiente**.



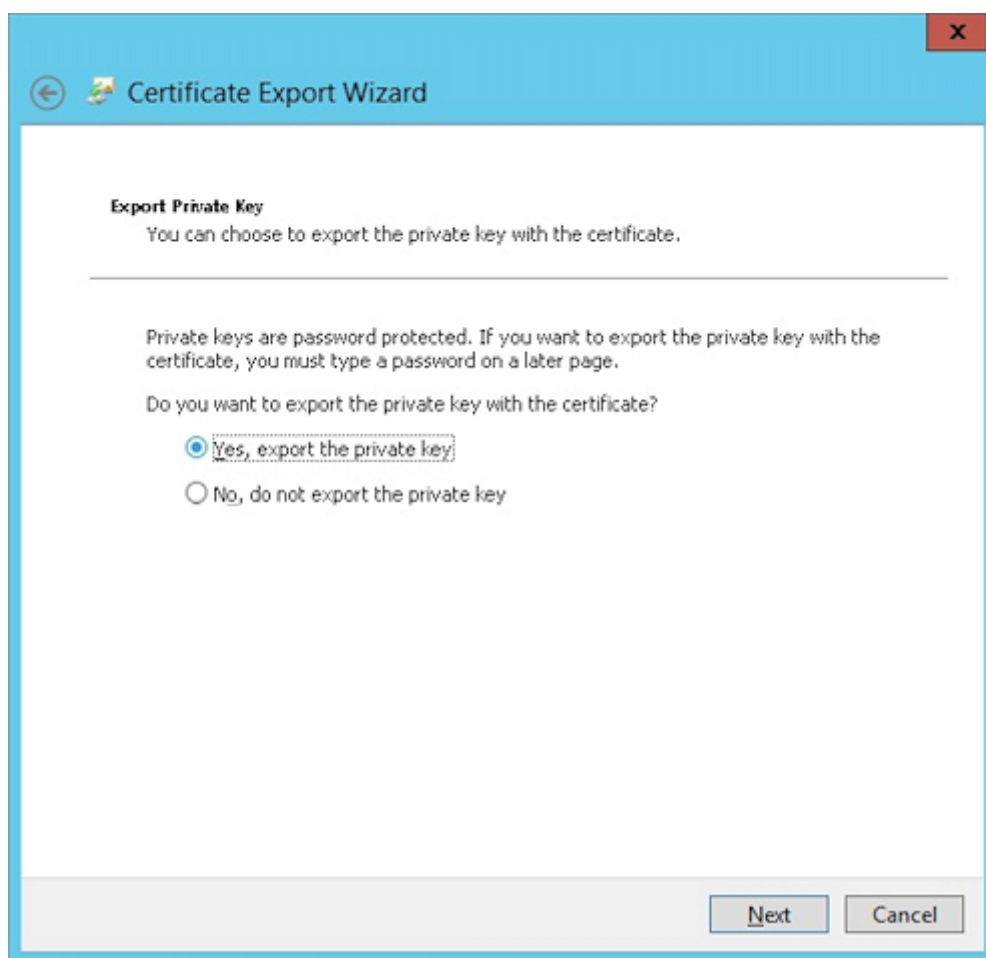
6. Seleccione la plantilla **Usuario** y haga clic en **Inscribir**.



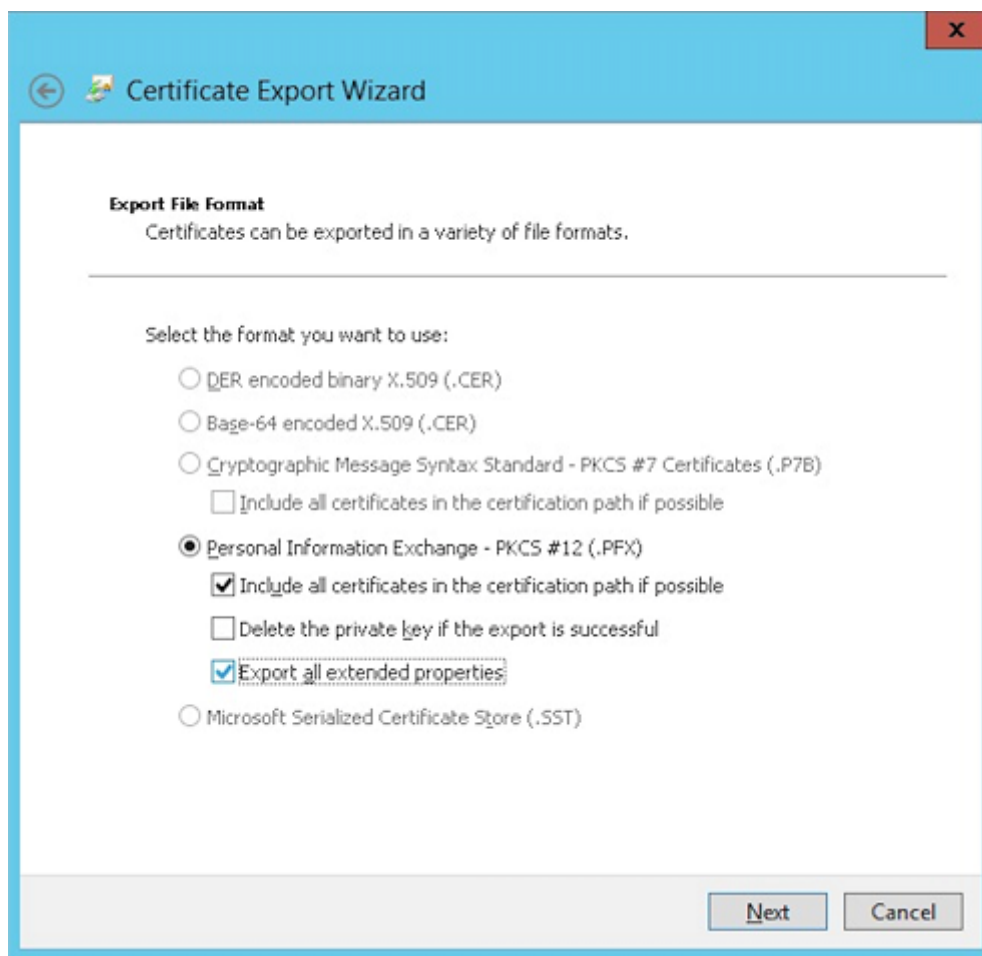
7. Exporte el archivo .pfx que creó en el paso anterior.



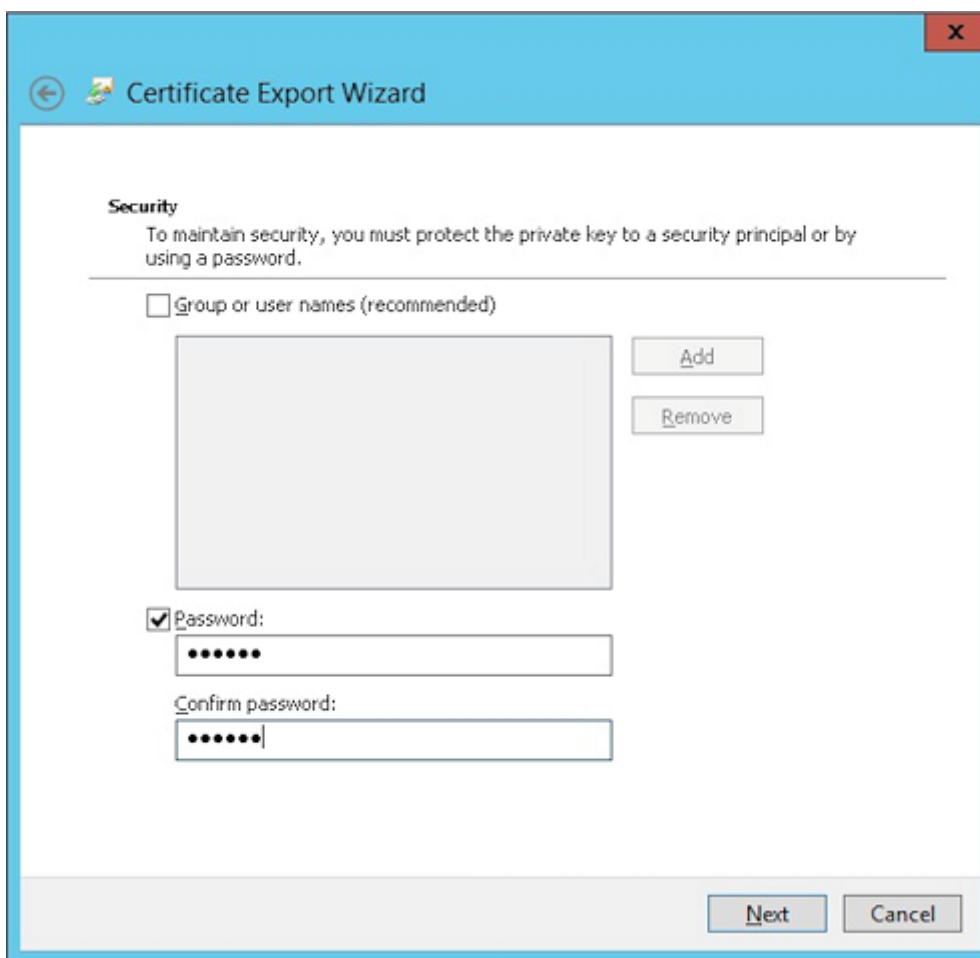
8. Haga clic en **Exportar la clave privada**.



9. Marque las casillas **Si es posible, incluir todos los certificados en la ruta de acceso de certificación** y **Exportar todas las propiedades extendidas**.



10. Defina la contraseña que va a usar para cargar este certificado en Citrix Endpoint Management.



11. Guarde el certificado en su disco duro.

Cargar el certificado en Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la pantalla **Parámetros**.
2. Haga clic en **Certificados** y, a continuación, en **Importar**.
3. Introduzca los parámetros siguientes:
 - **Importar:** Almacén de claves.
 - **Tipo de almacén de claves:** PKCS#12.
 - **Usar como:** Servidor.
 - **Archivo de almacén de claves:** Haga clic en "Examinar" para seleccionar el certificado PFX que acaba de crear.
 - **Contraseña:** Introduzca la contraseña que creó para este certificado.

Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time. Use the [APNs portal](#) on the Endpoint Management Tools page to create the APNs certificate.

Import Keystore

Keystore type PKCS#12

Use as Server

Keystore file * Browse

Password *

Description

Cancel Import

4. Haga clic en **Importar**.
5. Verifique que el certificado se ha instalado correctamente. Un certificado correctamente instalado se muestra como un certificado de usuario.

Crear la entidad PKI para la autenticación con certificados

1. En **Parámetros**, vaya a **Más > Administración de certificados > Entidades PKI**.
2. Haga clic en **Agregar** y, a continuación, haga clic en **Entidad de Servicios de certificados de Microsoft**. Aparecerá la pantalla **Entidad de Servicios de certificados de Microsoft: Información general**.
3. Introduzca los parámetros siguientes:
 - **Nombre:** Introduzca un nombre.
 - **URL raíz del servicio de inscripción web:** <https://RootCA-URL/certsrv/> Debe agregar la última barra diagonal (/) a la ruta de URL.
 - **certnew.cer page name:** 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 va a usar para emitir el certificado del cliente de Citrix Endpoint Management. Si no existe ningún certificado, siga el procedimiento descrito en la sección anterior para cargar certificados.

Settings > PKI Entities > Microsoft Certificate Services Entity

Microsoft Certificate Services Entity

1 General

2 Templates

3 HTTP Parameters

4 CA Certificates

Microsoft Certificate Services Entity: General Information

Name *

test

Web enrollment service root URL *

certnew.cer page name *

certnew.cer

certfnsh.asp *

certfnsh.asp

Authentication type

Client certificate

SSL client certificate

Select an option

Import SSL certificate

4. En **Plantillas**, agregue la plantilla que creó cuando configuró el certificado de Microsoft. No agregue espacios.

Microsoft Certificate Services Entity

1 General

2 Templates

3 HTTP Parameters

4 CA Certificates

Microsoft Certificate Services Entity: Templates

Specify the internal names of the templates your Microsoft CA supports. Every Credential Provider using this entity uses exactly one such template. When creating the provider, you will be prompted to select from the list defined here.

Templates

Templates *	Add
X509Template	

5. Omita el paso “Parámetros HTTP” y haga clic en **Certificados de CA**.
6. Seleccione el nombre de la CA raíz que le corresponda a su entorno. Esta CA raíz forma parte de la cadena importada desde el certificado del cliente de Citrix Endpoint Management.

Microsoft Certificate Services Entity

1 General

2 Templates

3 HTTP Parameters

4 CA Certificates

Microsoft Certificate Services Entity: CA Certificates

Indicate the certificates you want to use for this entity by selecting or clearing the check boxes. An entity is only valid when you select at least one certificate. Add all CA certificates that might be signers of certificates returned by this entity. Although entities may return certificates signed by different CAs, all certificates obtained through a given credential provider must be signed by the same CA. Accordingly, you will have to select one of the certificates configured here in the Distribution page of the Credential Provider setting.

<input type="checkbox"/>	Name	Serial number	Valid from	Valid to
<input checked="" type="checkbox"/>	training-AD-CA		02/22/2013	02/22/2023

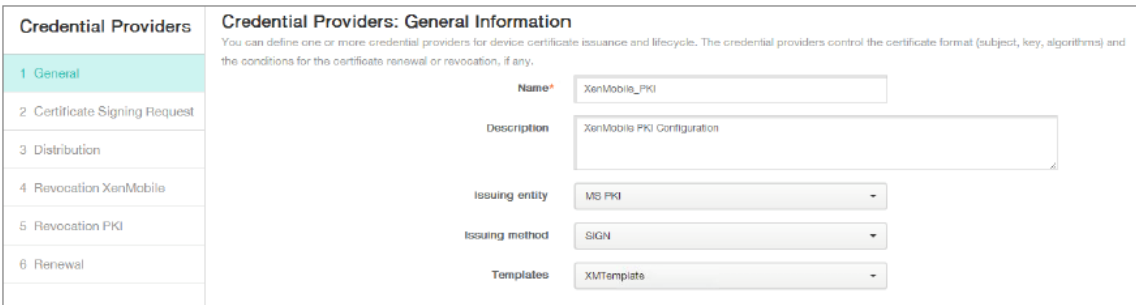
7. Haga clic en **Guardar**.

Configurar 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 parámetros siguientes:

- **Nombre:** Introduzca un nombre.
- **Descripción:** Introduzca una descripción.
- **Entidad de emisión:** Seleccione la entidad PKI creada anteriormente.
- **Método de emisión:** SIGN.
- **Plantillas:** Seleccione la plantilla agregada en el apartado de la entidad PKI.

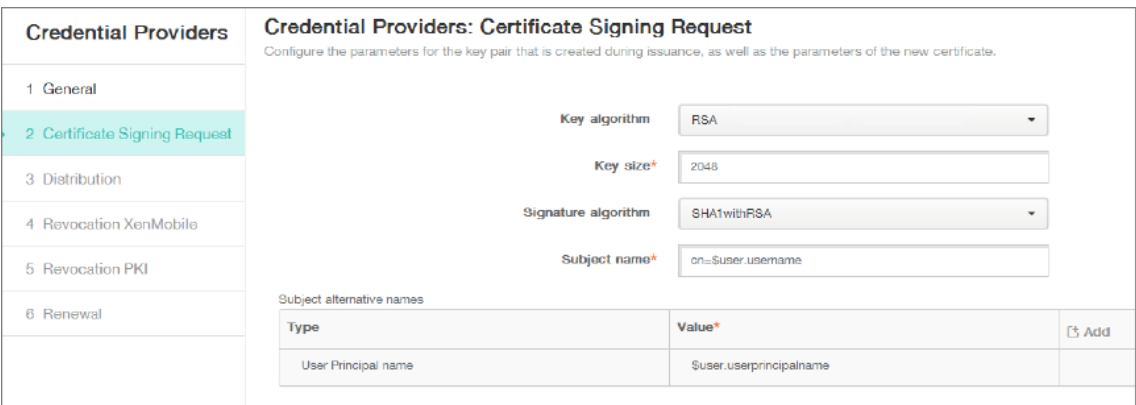


4. Haga clic en **Solicitud de firma de certificado** e introduzca los parámetros siguientes:

- **Algoritmo de clave:** RSA
- **Tamaño de clave:** 2048
- **Algoritmo de firma:** SHA256withRSA
- **Nombre del sujeto:** `cn=$user.username`

Para **Nombre alternativo del sujeto**, haga clic en **Agregar** e introduzca los parámetros siguientes:

- **Tipo:** Nombre principal del usuario.
- **Valor:** `$user.userprincipalname`



5. Haga clic en **Distribución** e introduzca los parámetros siguientes:

- **CA emisora de certificados:** Seleccione la CA emisora que firmó el certificado del cliente de Citrix Endpoint Management.

- **Seleccionar modo de distribución:** Marque **Preferir modo centralizado: Generación de clave en el lado del servidor.**

Credential Providers	Credential Providers: Distribution
1 General	Issuing CA certificate: ON-training-AD-CA, Serie
2 Certificate Signing Request	Select distribution mode
3 Distribution	<input checked="" type="radio"/> Prefer centralized: Server-side key generation
4 Revocation XenMobile	<input type="radio"/> Prefer distributed: Device-side key generation
	<input type="radio"/> Only distributed: Device-side key generation

6. Para las dos secciones siguientes (**Revocación Citrix Endpoint Management** y **Revocación PKI**), defina los parámetros, si es necesario. En este ejemplo, ambas opciones se omiten.
7. Haga clic en **Renovación**.
8. Habilite **Renovar certificados cuando caduquen**.
9. Deje todos los demás parámetros con los valores predeterminados o cámbielos si es necesario.

Credential Providers	Credential Providers: Renewal
1 General	Renew certificates when they expire: <input checked="" type="checkbox"/>
2 Certificate Signing Request	Renew when the certificate comes within*: 30 days of expiration
3 Distribution	<input type="checkbox"/> Do not renew certificates that have already expired
4 Revocation XenMobile	Send notification: <input type="checkbox"/>
5 Revocation PKI	Notify when the certificate nears expiration: <input type="checkbox"/>
6 Renewal	

10. Haga clic en **Guardar**.

Configurar Citrix Secure Mail para la autenticación con certificados

Cuando agregue Citrix Secure Mail a Citrix Endpoint Management, configure los parámetros de Exchange en **Parámetros de aplicación**.

Device Policies	Apps	Actions	ShareFile	Enrollment Profiles	Delivery Groups
MDX					
1 App Information		App Interaction			
		Explicit logoff notification	Shared devices only		
2 Platform		App Settings			
<input checked="" type="checkbox"/> iOS		WorxMail Exchange Server			
<input checked="" type="checkbox"/> Android		WorxMail user domain	testlab.com		
<input checked="" type="checkbox"/> Windows Phone		Background network services			
3 Approvals (optional)		Background services ticket expiration	168		
4 Delivery Group Assignments (optional)					

Configurar la entrega de certificados de NetScaler Gateway en Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la pantalla **Parámetros**.
2. En **Servidor**, haga clic en **NetScaler Gateway**.
3. Si NetScaler Gateway aún no está agregado, haga clic en **Agregar** y especifique los parámetros:
 - **Nombre:** Escriba 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**.
 - **Se requiere contraseña:** Desactivado.
 - **Establecer como predeterminado:** Activado.
4. En **Autenticación y Entregar certificado de usuario para autenticación**, seleccione **Sí**.

Settings > Citrix Gateway

Citrix Gateway

When you configure Citrix Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use Citrix Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication ☒

Deliver user certificate for authentication ☒

Credential provider

<input type="checkbox"/>	Name	Default	External URL	Logon Type	numeral of Callback URLs	Resource Location
--------------------------	------	---------	--------------	------------	--------------------------	-------------------

5. En **Proveedor de credenciales**, seleccione un proveedor y haga clic en **Guardar**.
6. Si va a usar atributos de sAMAccount en los certificados de usuario como alternativa al nombre principal de usuario (UPN), configure el conector de LDAP en Citrix Endpoint Management de este modo: vaya a **Parámetros > LDAP**, seleccione el directorio, haga clic en **Modificar** y seleccione **sAMAccountName** en **Buscar usuarios por**.

The screenshot shows a configuration form for Citrix Endpoint Management. It includes the following fields and controls:

- User base DN* (text input)
- Group base DN* (text input)
- User ID* (text input)
- Password* (password input)
- Domain alias* (text input)
- XenMobile Lockout Limit (text input, value: 0)
- XenMobile Lockout Time (text input, value: 1)
- Global Catalog TCP Port (text input, value: 3268)
- Global Catalog Root Context (text input, value: dc=example.dc=com)
- User search by (dropdown menu, value: sAMAccountName)
- Use secure connection (radio button, value: NO)
- Cancel button
- Save button

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, vaya a **Parámetros > Propiedades de cliente** y marque las casillas **Enable Citrix PIN Authentication** y **Enable User Password Caching**. Para obtener más información, consulte [Propiedades de cliente](#).

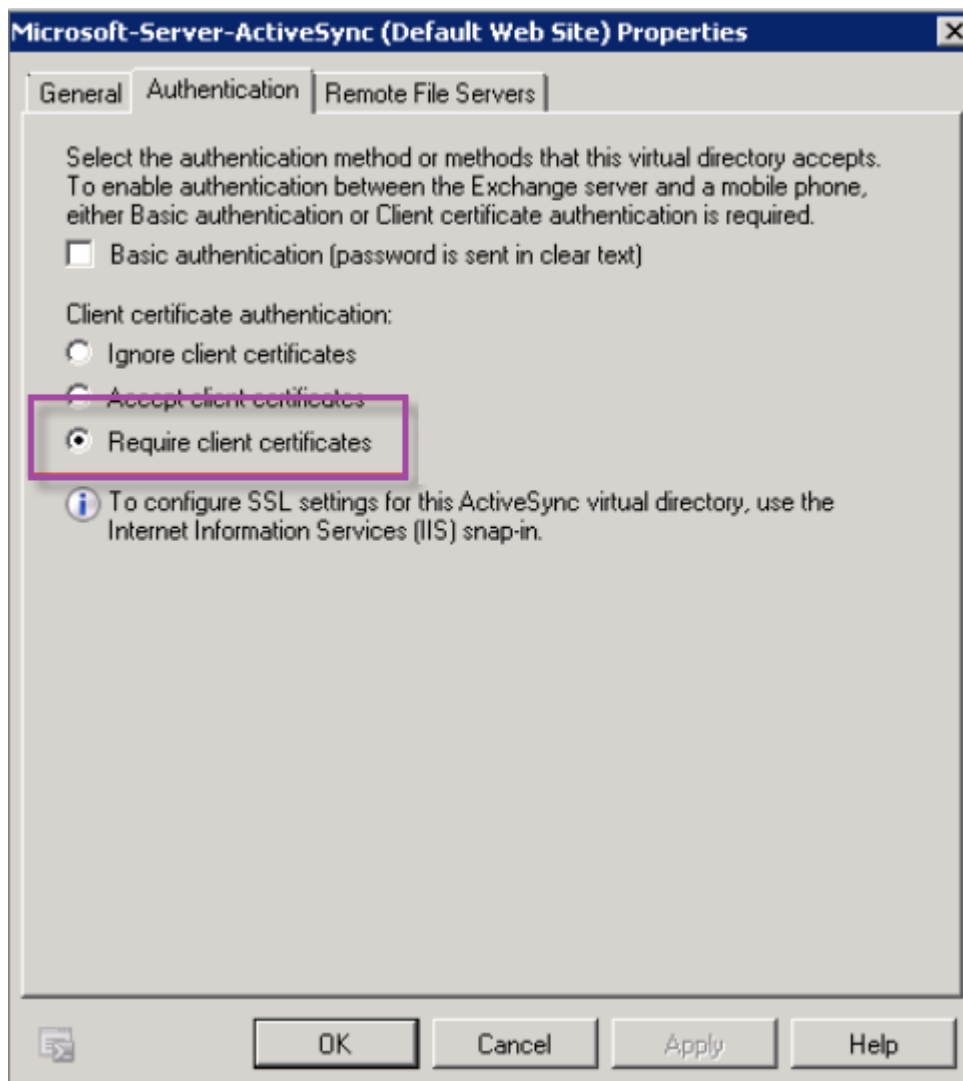
Solucionar problemas en la configuración de certificados de cliente

Después de definir correctamente la configuración anterior, además de configurar NetScaler Gateway, el flujo de trabajo del usuario es el siguiente:

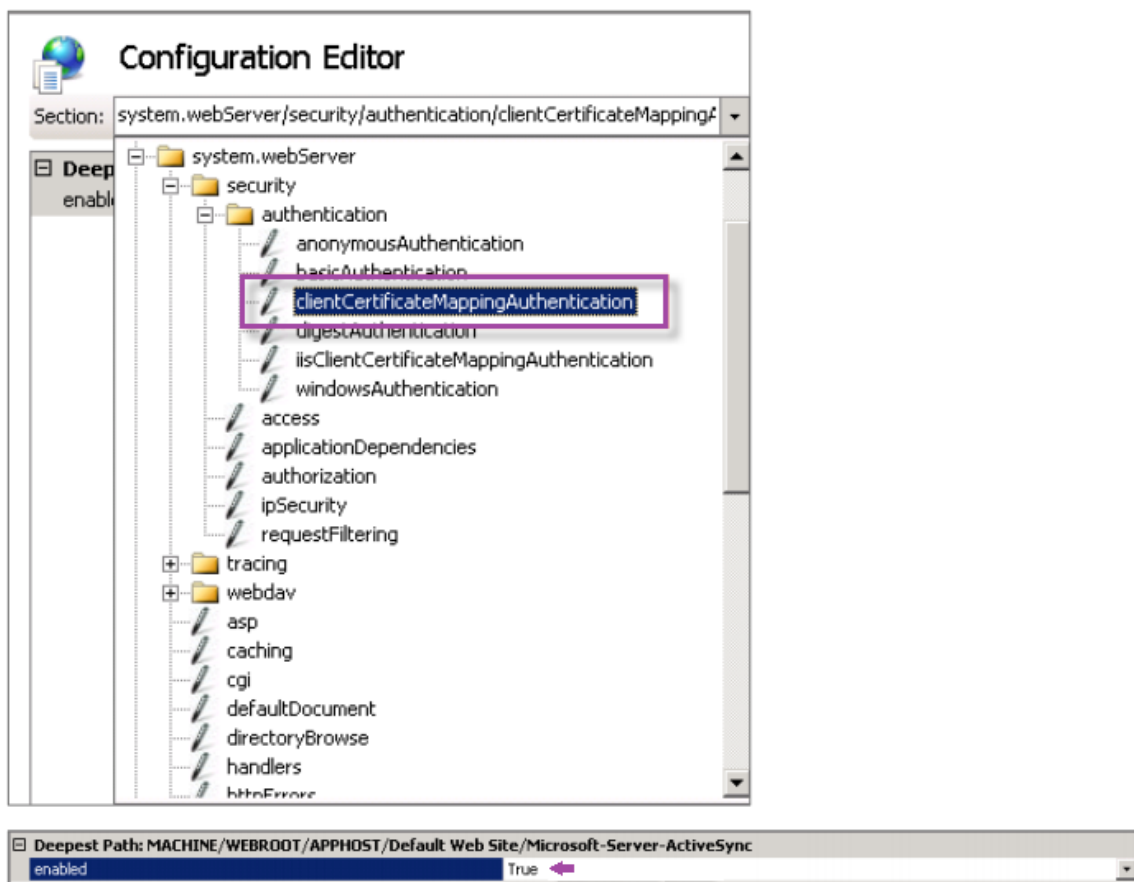
1. Los usuarios inscriben sus dispositivos móviles.
2. Citrix Endpoint Management solicita a los usuarios que creen un PIN de Citrix.
3. Se redirige a los usuarios al almacén de aplicaciones.
4. Cuando los usuarios inician Citrix Secure Mail, Citrix Endpoint Management no les pide credenciales para configurar el buzón. En su lugar, Citrix Secure Mail solicitará el certificado del cliente de Citrix Secure Hub y lo enviará a Microsoft Exchange Server para la autenticación. Si Citrix Endpoint Management pide credenciales cuando los usuarios inician Citrix Secure Mail, verifique si ha configurado todo correctamente.

Si los usuarios pueden descargar e instalar Citrix Secure Mail, pero durante la configuración de buzones Citrix Secure Mail no puede finalizar la configuración:

1. Si el servidor de Microsoft Exchange ActiveSync usa certificados de servidor SSL privados para proteger el tráfico, compruebe que los certificados raíz e intermedios están instalados en el dispositivo móvil.
2. Compruebe que el tipo de autenticación seleccionado para ActiveSync es **Requerir certificados de cliente**.



3. En Microsoft Exchange Server, visite el sitio **Microsoft-Server-ActiveSync** para ver si tiene habilitada la autenticación con asignación de certificados del cliente. De forma predeterminada, la autenticación con asignación de certificados del cliente está inhabilitada. La opción está en **Editor de configuración > Seguridad > Autenticación**.



Después de seleccionar **True**, debe hacer clic en **Aplicar** para que los cambios tengan efecto.

4. Revise la configuración de NetScaler Gateway en la consola de Citrix Endpoint Management: **Entregar certificado de usuario para autenticación** debe estar **activado** y **Proveedor de credenciales** debe tener seleccionado el perfil correcto.

Para determinar si el certificado del cliente se ha entregado a un dispositivo móvil

1. En la consola de Citrix Endpoint Management, vaya a **Administrar > Dispositivos** y seleccione el dispositivo.
2. Haga clic en **Modificar** o **Mostrar más**.
3. Vaya a la sección **Grupos de entrega** y busque esta entrada:

NetScaler Gateway Credentials: Requested credential, CertId=

Para validar si está habilitada la negociación de certificados de cliente

1. Ejecute este comando `netsh` para ver la configuración del certificado SSL que está vinculado en el sitio web de IIS:

```
netsh http show sslcert
```

2. Si el valor de **Negotiate Client Certificate** es **Disabled**, 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=23498dfsdfhaf98rhkjgf98  
appid={ 123asd456jd-a12b-3c45-d678-123456lkjhgf } certstorename=  
ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWit  
=Disable UsageCheck=Enable clientcertnegotiation=Enable
```

Si no puede entregar certificados raíz o intermedios a un dispositivo Windows Phone 8.1 a través de Citrix Endpoint Management:

- Envíe los archivos .cer de certificados raíz/intermedios por correo electrónico al dispositivo Windows Phone 8.1 e instálelos directamente.

Si Citrix Secure Mail no se puede instalar correctamente en Windows Phone 8.1, compruebe lo siguiente:

- El token de inscripción de la aplicación (archivo AETX) se entrega a través de Citrix Endpoint Management mediante la directiva de hub empresarial.
- El token de inscripción de la aplicación se creó con el mismo certificado de empresa del proveedor de certificados utilizado para empaquetar Citrix Secure Mail y firmar las aplicaciones de Citrix Secure Hub.
- Se usa el mismo ID de publicador para firmar y empaquetar Citrix Secure Hub, Citrix Secure Mail y el token de inscripción de la aplicación.

Entidades de PKI

March 1, 2024

La configuración de una entidad de infraestructura de clave pública (PKI) de Citrix Endpoint Management representa un componente que lleva a cabo operaciones de PKI (emisión, revocación e información de estado). Estos componentes son internos o externos a Citrix Endpoint Management. Los

componentes internos se conocen como discrecionales. Los componentes externos forman parte de su infraestructura corporativa.

Citrix Endpoint Management admite los siguientes tipos de entidades de infraestructura PKI:

- Servicios de certificados de Microsoft
- Entidades de certificación discrecionales (CA)

Citrix Endpoint Management admite los siguientes servidores de CA:

- Windows Server 2016
- Windows Server 2019

Nota:

Los Windows Servers 2012 R2, 2012 y 2008 R2 ya no reciben asistencia porque han llegado a su fin de vida. Para obtener más información, consulte la [documentación sobre el ciclo de vida de los productos de Microsoft](#).

Conceptos comunes de infraestructura de clave pública

Independientemente de su tipo, cada entidad de infraestructura de clave pública (PKI) tiene un subconjunto de las siguientes funciones:

- **Sign:** Emitir un nuevo certificado a partir de una solicitud de firma de certificado (CSR).
- **Fetch:** Recuperar un par de claves y un certificado existentes.
- **Revoke:** Revocar un certificado de cliente.

Acerca de los certificados de CA

Cuando configure una entidad de infraestructura PKI, deberá indicar a Citrix Endpoint Management el certificado de CA que va a actuar como firmante de los certificados que esta entidad emita (o de aquellos certificados que se obtengan de ella). Esa entidad PKI puede devolver certificados (ya sean recuperados o recién firmados) que haya firmado una cantidad indefinida de entidades de certificación (CA).

Debe proporcionar el certificado de cada una de estas entidades de certificación cuando configure la entidad de infraestructura PKI. Para ello, cargue los certificados en Citrix Endpoint Management y, a continuación, vincúelos en la entidad de infraestructura PKI. Para las entidades de certificación discrecionales, el certificado es implícitamente el certificado de firma de CA. Para las entidades externas, debe especificar manualmente el certificado.

Importante:

Cuando cree plantillas de entidad para Servicios de certificados de Microsoft, para evitar posibles problemas de autenticación en los dispositivos inscritos, no use caracteres especiales en el nombre de las plantillas. Por ejemplo, no use: ! : \$ () # % + * ~ ? | { } []

Servicios de certificados de Microsoft

Citrix Endpoint Management interactúa con Servicios de certificados de Microsoft a través de su interfaz de inscripción web. Citrix Endpoint Management admite solo la emisión de certificados nuevos a través de esa interfaz. Si la CA de Microsoft genera un certificado de usuario de NetScaler Gateway, NetScaler Gateway admite la renovación y la revocación de esos certificados.

Para crear una entidad PKI de la entidad de certificación de Microsoft en Citrix Endpoint Management, debe especificar la URL base de la interfaz web de los Servicios de servidor de certificados. Si lo prefiere, utilice la autenticación SSL de cliente para proteger la conexión entre Citrix Endpoint Management y la interfaz web de los Servicios de servidor de certificados.

Agregar una entidad de Servicios de certificados de Microsoft

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha de la consola. A continuación, haga clic en **Entidades PKI**.

2. En la página **Entidades PKI**, haga clic en **Agregar**.

Aparecerá un menú con los tipos de entidad de infraestructura de clave pública.

3. Haga clic en **Entidad de Servicios de certificados de Microsoft**.

Aparecerá 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 parámetros:

- **Nombre:** Escriba un nombre para la nueva entidad; es el nombre que utilizará para hacer referencia a esa entidad. Los nombres de entidad deben ser únicos.
- **URL raíz del servicio de inscripción web:** Especifique la URL base del servicio de inscripción web de la entidad de certificación de Microsoft. Por ejemplo: <https://192.0.0.1/certsrv/>. La URL puede usar HTTP sin formato o HTTP sobre SSL.
- **certnew.cer page name:** El nombre de la página certnew.cer. Use el nombre predeterminado a menos que se le haya cambiado el nombre por algún motivo.

- **certfnsh.asp**: El nombre de la página certfnsh.asp. Use el nombre predeterminado a menos que se le haya cambiado el nombre por algún motivo.
- **Tipo de autenticación**: Elija el método de autenticación que se va a utilizar.
 - **Ninguno**
 - **HTTP básica**: Proporcione el nombre de usuario y la contraseña necesarios para la conexión.
 - **Certificado del cliente**: Seleccione el certificado SSL de cliente correspondiente.
- **Usar Cloud Connector: Active** el parámetro para usar Cloud Connector para conexiones al servidor de PKI. A continuación, especifique una **Ubicación de recursos** y las **Rutas relativas permitidas** para la conexión.
 - **Ubicación de recursos**: Elija una de 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 utilizar un asterisco (*) como comodín.

Supongamos que la ubicación de recursos es `https://www.ServiceRoot/certsrv`. Para proporcionar acceso a todas las direcciones URL en esa ruta, introduzca `/*` en **Rutas relativas permitidas**.

Settings > PKI Entities > Edit Microsoft Certificate Services Entity

Microsoft Certificate Services Entity

- 1 General
- 2 Templates
- 3 HTTP Parameters
- 4 CA Certificates

Microsoft Certificate Services Entity: General Information

Name* AusterCA

Web enrollment service root URL*

certnew.cer page name* certnew.cer ⓘ

certfnsh.asp* certfnsh.asp ⓘ

Authentication type Client certificate ⓘ

SSL client certificate ⓘ

Import SSL certificate

Use Cloud Connector **ON** ⓘ

Resource Location* My Resource Location ⓘ

Allowed Relative Paths* *

5. Haga clic en **Probar conexión** para comprobar que el servidor está accesible. Si no se puede

establecer la conexión, aparecerá un mensaje donde se indica que falló la conexión. Compruebe los parámetros de configuración.

6. Haga clic en **Siguiente**.

Aparece la página **Entidad de Servicios de certificados de Microsoft: Plantillas**. En esta página, especifique los nombres internos de las plantillas que admite la entidad de certificación de Microsoft. Cuando cree proveedores de credenciales, seleccione una plantilla de la lista definida aquí. Todos los proveedores de credenciales que utilicen esta entidad se valen de una plantilla exactamente igual.

Para conocer los requisitos de plantillas de Servicios de certificados de Microsoft, consulte la documentación de Microsoft referente a su versión de servidor Microsoft. Citrix Endpoint Management no presenta requisitos para los certificados que distribuye, salvo 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 a agregar.

8. Haga clic en **Siguiente**.

Aparece la página **Entidad de Servicios de certificados de Microsoft: Parámetros HTTP**. En esta página, puede especificar parámetros personalizados que Citrix Endpoint Management agregará a la solicitud HTTP para la interfaz de inscripción web de Microsoft. Los parámetros personalizados son útiles solo 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 a agregar. A continuación, haga clic en **Siguiente**.

Aparece la página **Entidad de Servicios de certificados de Microsoft: Certificados de CA**. En esta página, debe indicar a Citrix Endpoint Management los firmantes de los certificados que el sistema va a obtener a través de esta entidad. Cuando se renueve el certificado de 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 se van a utilizar para la entidad.

11. Haga clic en **Guardar**.

La entidad se muestra en la tabla “Entidades PKI”.

Lista de revocación de certificados (CRL) de NetScaler Gateway

Citrix Endpoint Management solo admite la lista de revocación de certificados (CRL) cuando se trata de una entidad de certificación (CA) de terceros. Si dispone de una entidad de certificación de Microsoft configurada, Citrix Endpoint Management utiliza NetScaler Gateway para administrar la revocación.

Al configurar la autenticación por certificados de cliente, plantéese si es necesario configurar el parámetro de lista de revocación de certificados (CRL) de NetScaler Gateway, **Enable CRL Auto Refresh**. Este paso garantiza que el usuario de un dispositivo en modo solo MAM no pueda autenticarse con un certificado existente en el dispositivo.

Citrix Endpoint Management vuelve a emitir un certificado nuevo, porque no impide que un usuario genere otro certificado de usuario tras revocarse uno. Este parámetro aumenta la seguridad de las entidades PKI cuando la lista de revocación de certificados comprueba si hay entidades PKI caducadas.

Entidades de certificación (CA) discrecionales

Se crea una entidad de certificación discrecional al proporcionar a Citrix Endpoint Management un certificado de CA y la clave privada asociada. Citrix Endpoint Management gestiona la emisión, la revocación y la información de estado de certificados internamente en función de los parámetros especificados.

Cuando configure una entidad de certificación discrecional, puede activar el protocolo Online Certificate Status Protocol (OCSP) para esa entidad. Si habilita OCSP, la entidad de certificación agrega una extensión `id-pe-authorityInfoAccess` a los certificados que emita. La extensión apunta al respondedor OCSP interno de Citrix Endpoint Management que reside en la siguiente ubicación:

<https://<server>/<instance>/ocsp>

Al configurar el servicio OCSP, especifique un certificado de firma de OCSP para la entidad discrecional en cuestión. Puede usar el certificado de CA en sí como firmante. Para evitar una exposición innecesaria de la clave privada de la entidad de certificación (recomendado), cree un certificado de firma de OCSP delegado, firmado por la entidad de certificación, e incluya la extensión `id-kp-OCSPSigning` `extendedKeyUsage`.

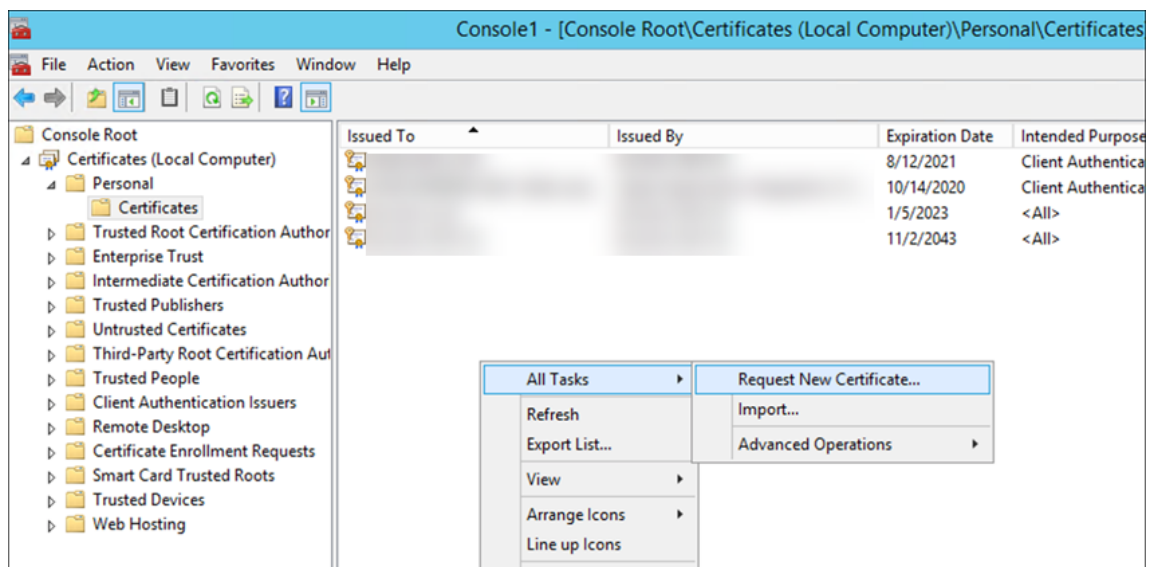
El servicio de respondedor OCSP de Citrix Endpoint Management admite respuestas de OCSP básicas y los siguientes algoritmos hash en las solicitudes:

- SHA-256
- SHA-384
- SHA-512

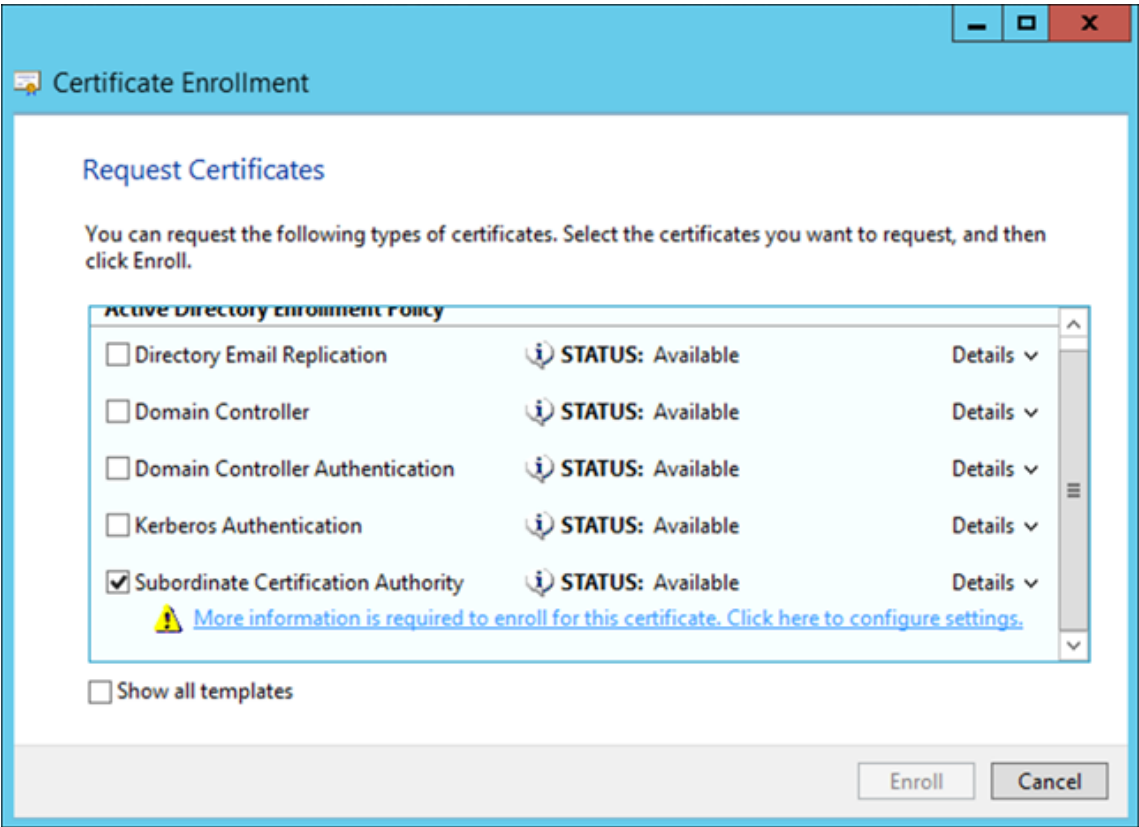
Las respuestas se firman con SHA-256 y el algoritmo de clave del certificado de firma (DSA, RSA o ECDSA).

Generar e importar un certificado para su entidad de certificación

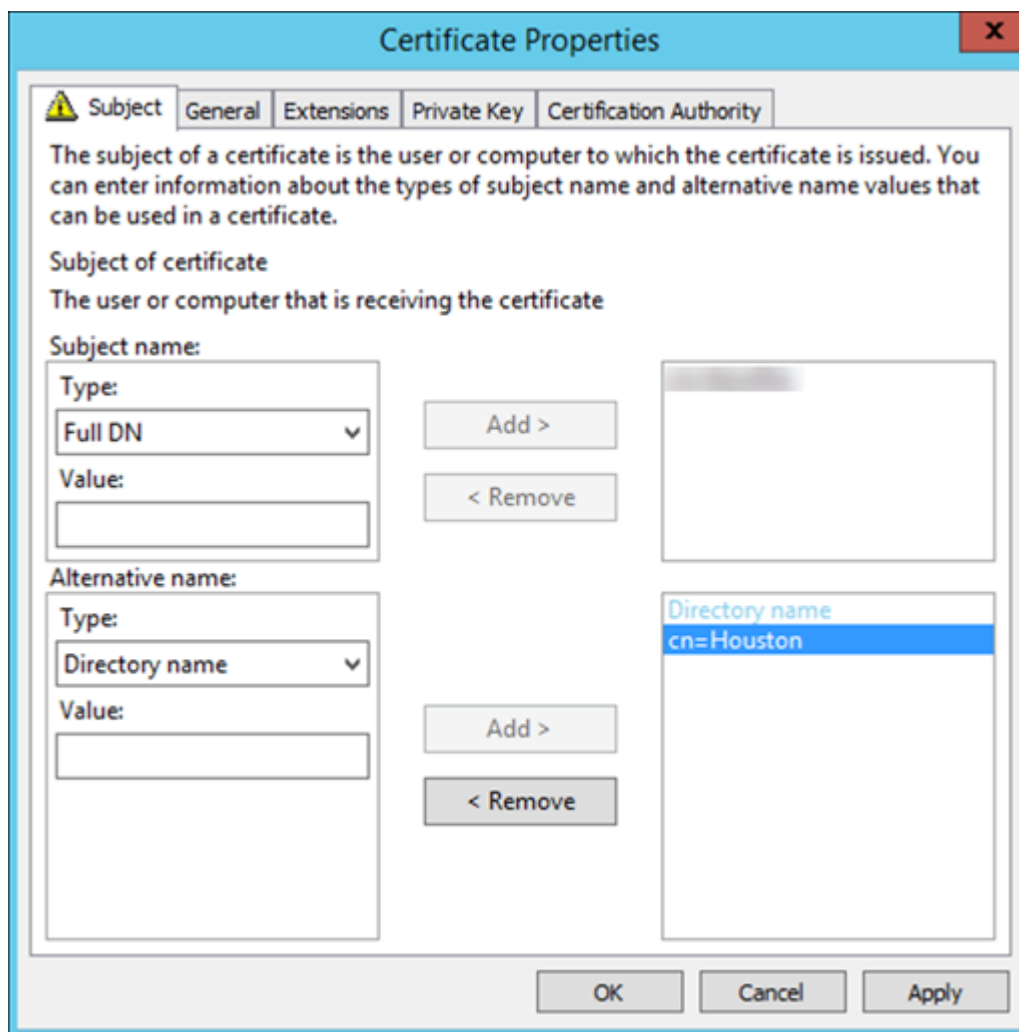
1. En el servidor, abra Microsoft Management Console (MMC) con su cuenta de sistema local y abra el complemento de certificados. En el panel de la derecha, haga clic con el botón secundario y, a continuación, haga clic en **Todas las tareas > Solicitar nuevo certificado**.



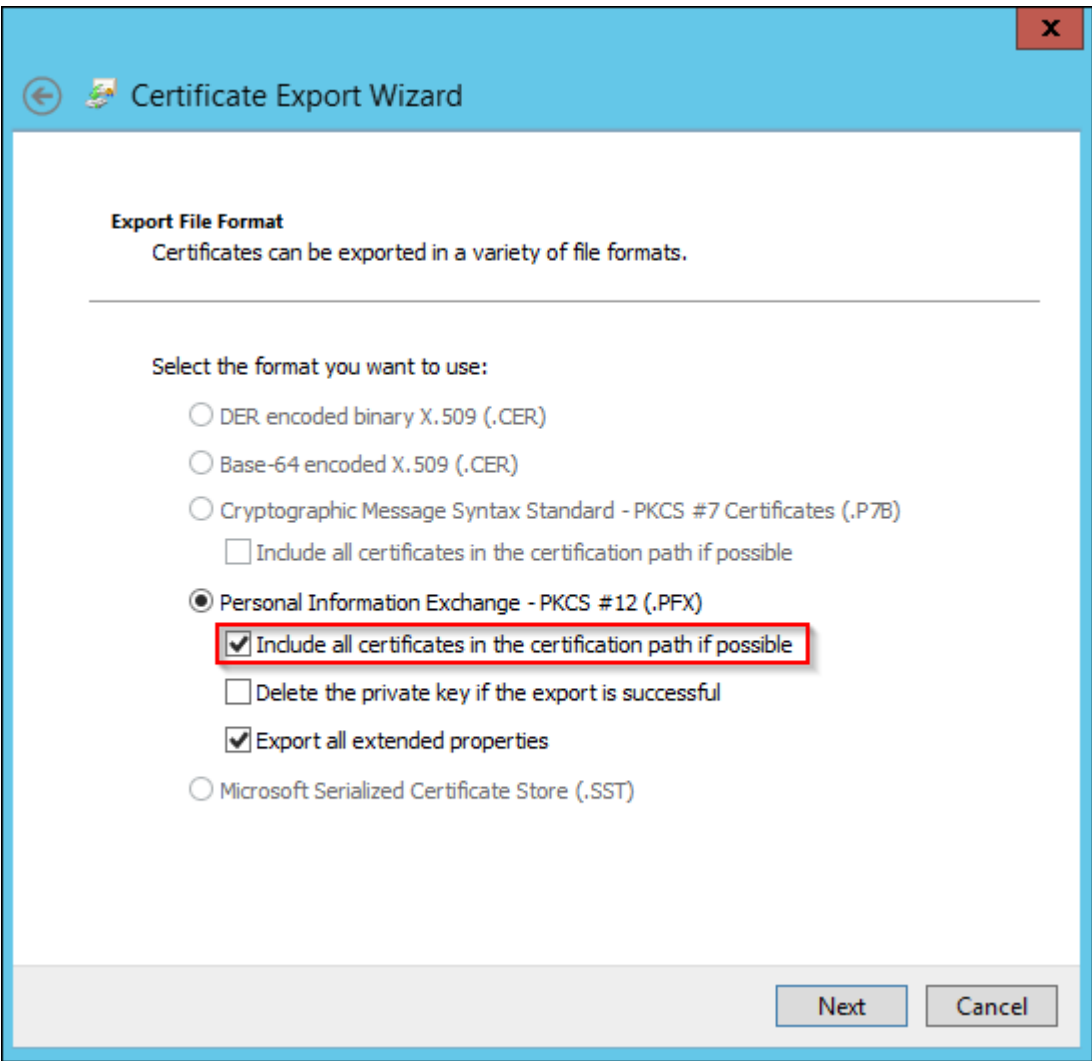
2. En el asistente que se abre, haga clic en **Siguiente** dos veces. En la lista **Solicitar certificados**, seleccione **Entidad de certificación subordinada** y, a continuación, haga clic en el enlace **Más información**.



3. En la ventana, escriba un **nombre de sujeto** y un **nombre alternativo**. Haga clic en **Aceptar**.



4. Haga clic en **Inscribir** y, a continuación, en **Finalizar**.
5. En MMC, haga clic con el botón secundario en el certificado creado. 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**.



6. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Certificados**.

Settings > Certificates

Certificates

To commit and activate your changes to the Android Enterprise SAML certificate, you must restart Endpoint Management on all nodes. Please contact Citrix Technical Support for assistance.

Use the [APNs portal](#) on the Endpoint Management Tools page to create the APNs certificate.

Import | Add

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key
<input type="checkbox"/>	DST Root CA X3		Up to date	9/30/00	9/30/21	Root or intermediate	
<input type="checkbox"/>	DiscretionayCA	Self-signed generated	Up to date	1/5/21	9/27/21	Server	✓

7. Haga clic en **Importar**. En la ventana que se abre, busque los archivos de certificado y de clave privada que exportó anteriormente.

Import

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time. Use the [APNs portal](#) on the Endpoint Management Tools page to create the APNs certificate.

Import Keystore

Keystore type PKCS#12

Use as Server

Keystore file * Browse

Password *

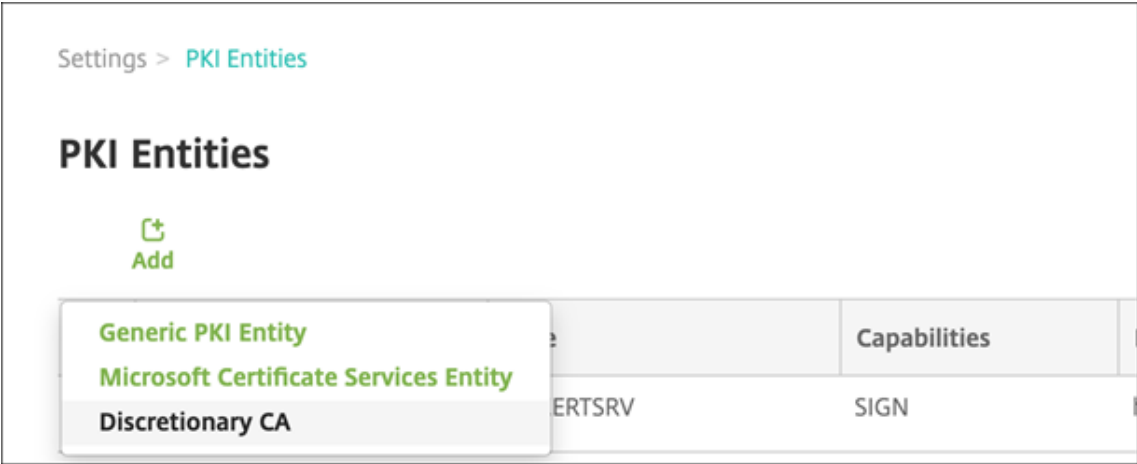
Description

Cancel Import

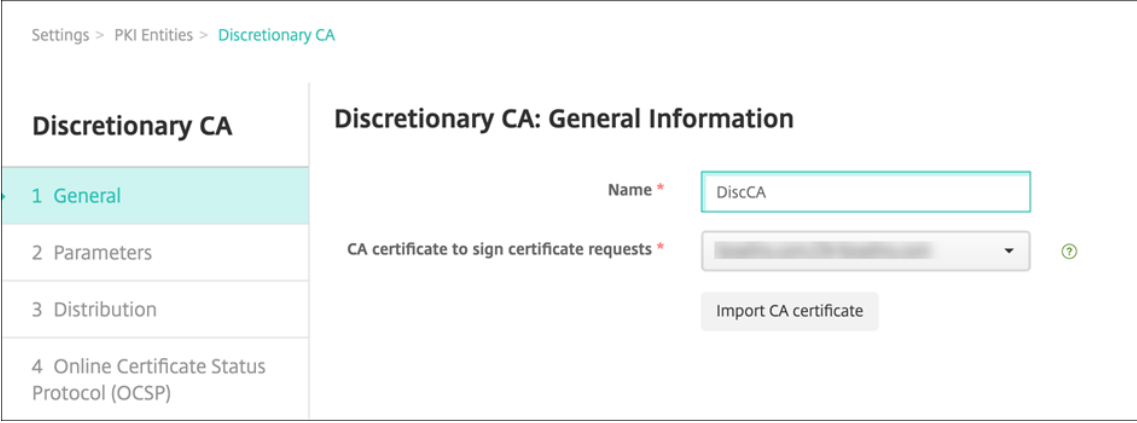
8. Haga clic en **Importar**. El certificado se agrega a la tabla.

Agregar entidades de certificación discrecionales

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha de la consola. A continuación, haga clic en **Más > Entidades PKI**.
2. En la página **Entidades PKI**, haga clic en **Agregar**.



3. Haga clic en **Entidad de certificación (CA) discrecional**.



4. En la página **CA discrecional: Información general**, configure lo siguiente:

- **Nombre:** Escriba un nombre descriptivo para la entidad de certificación discrecional.
- **Certificado de CA para firmar solicitudes de certificado:** Haga clic en un certificado de la entidad de certificación discrecional que se utilizará para firmar las solicitudes de certificados.

Esta lista de certificados se genera a partir de los certificados de CA con las claves privadas que se cargaron en Citrix Endpoint Management, en **Configurar > Parámetros > Certificados**.

5. Haga clic en **Siguiente**.

Settings > PKI Entities > [Edit Discretionary CA](#)

Discretionary CA

- General
- Parameters**
- Distribution
- Online Certificate Status Protocol (OCSP)

Discretionary CA: Parameters

Serial number generator * Sequential

Next serial number 27 ⓘ

Certificate valid for 365 days

Key usage

DigitalSignature ON

NonRepudiation OFF

KeyEncipherment ON

DataEncipherment OFF

Extended key usage

Name * + Add

6. En la página **CA discrecional: Parámetros**, configure lo siguiente:

- **Generador de números de serie:** La entidad de certificación discrecional genera números de serie para los certificados que emite. En esta lista, haga clic en **Secuencial** o en **No secuencial** para determinar el modo en que se generan los números.
- **Siguiente número de serie:** Escriba un valor para determinar el siguiente número a emitir.
- **Certificado válido para:** Escriba la cantidad de días durante los que el certificado será válido.
- **Uso de clave:** Identifique el propósito de los certificados emitidos por la entidad de certificación discrecional. Para ello, **active** las claves apropiadas. Una vez activadas, la entidad de certificación está limitada a la emisión de certificados para esos fines.
- **Uso mejorado de clave:** 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**.

Settings > PKI Entities > Edit Discretionary CA

Discretionary CA

- 1 General
- 2 Parameters
- 3 Distribution**
- 4 Online Certificate Status Protocol (OCSP)

Discretionary CA: Distribution

Select distribution mode

☒ Centralized: server-side key generation

☐ Distributed: device-side key generation

8. En la página **CA discrecional: Distribución**, seleccione un modo de distribución:

- **Centralizado: generación de claves en el lado del servidor.** Citrix recomienda la opción centralizada. Las claves privadas se generan y se almacenan en el servidor para, luego, distribuirse a los dispositivos de usuario.
- **Distribuido: generación de claves en el lado del dispositivo.** Las claves privadas se generan en los dispositivos de usuario. Este modo de distribución utiliza SCEP y requiere un certificado de cifrado de RA con la extensión **keyUsage keyEncryption**, así como un certificado de firma de RA con la extensión **keyUsage digitalSignature**. Se puede usar el mismo certificado para el cifrado y la firma.

9. Haga clic en **Siguiente**.

Settings > PKI Entities > Edit Discretionary CA

Discretionary CA

- 1 General
- 2 Parameters
- 3 Distribution
- 4 Online Certificate Status Protocol (OCSP)**

Discretionary CA: Online Certificate Status Protocol (OCSP)

If you enable OCSP support, Endpoint Management adds an AuthorityInfoAccess (RFC2459) extension to the certificates signed by this entity. The extension points to the instance's OCSP responder at [http://\\$server/\\$instance/ocsp](http://$server/$instance/ocsp).

Enable OCSP support for this CA ☒

OCSP signing CA certificate *

Import CA certificate

10. En la página **CA discrecional: Protocolo OCSP (Online Certificate Status Protocol)**, configure lo siguiente:

- Para agregar una extensión **AuthorityInfoAccess** (RFC2459) a los certificados firmados por esta entidad de certificación, establezca **Habilitar OCSP para esta CA** en **Sí**. Esta extensión apunta al respondedor OCSP de la entidad de certificación en <https://<server>/<instance>/ocsp>.
- Si ha habilitado OCSP, seleccione un certificado de firma de CA OCSP. Esta lista de certificados se genera a partir de los certificados de CA que se cargaron en Citrix Endpoint

Management.

Al habilitar la función, Citrix ADC puede comprobar el estado de los certificados. Citrix recomienda habilitarla.

11. Haga clic en **Guardar**.

La entidad de certificación discrecional se muestra 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:

Settings > Credential Providers > Edit credential provider

Credential Providers

- 1 General
- 2 Certificate Signing Request
- 3 Distribution
- 4 Revocation Endpoint Management
- 5 Revocation PKI
- 6 Renewal

Credential Providers: General Information

You can define one or more credential providers for device certificate issuance and lifecycle. The credential providers control the certificate format (subject, key, algorithms) and the conditions for the certificate renewal or revocation, if any.

Name * Discretionary Provider

Description test

Issuing entity Discretionary CA

Issuing method SIGN

- **Nombre:** Escriba un nombre exclusivo para la configuración del nuevo proveedor. Este nombre se usará posteriormente para identificar la configuración en otras partes de la consola de Citrix Endpoint Management.
 - **Descripción:** Describa el proveedor de credenciales. Aunque este campo sea opcional, una descripción puede resultar útil cuando necesite datos concretos acerca del proveedor de credenciales.
 - **Entidad emisora:** Seleccione **CA discrecional**.
 - **Método de emisión:** Haga clic en **Sign** o en **Fetch** para designar el método que usará el sistema para obtener certificados de la entidad configurada. Para la autenticación con certificado del cliente, use **Sign**.
3. Haga clic en **Siguiente**. En la página **Proveedores de credenciales: Solicitud de firma de certificado**, defina lo siguiente según la configuración de su certificado:

Settings > Credential Providers > [Edit credential provider](#)

Credential Providers

- 1 General
- 2 Certificate Signing Request**
- 3 Distribution
- 4 Revocation Endpoint Management
- 5 Revocation PKI
- 6 Renewal

Credential Providers: Certificate Signing Request

Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.

Key algorithm: RSA

Key size *: 2048

Signature algorithm: SHA256withRSA

Subject name *: cn=User.username

Subject alternative names

Type	Value *	Add
User Principal name	\$user.userprincipalname	

- **Algoritmo de clave:** Seleccione 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 utilizar **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:** Campo obligatorio. Escriba el nombre distintivo (DN) del nuevo sujeto del certificado. Use `CN=${ user.username }` para el nombre de usuario o `CN=${ user.samaccountname }` para usar sAMAccountName.
- Para agregar una nueva 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 del usuario.
- **Valor:** `$user.userprincipalname`

Al igual que para el nombre del sujeto, puede usar las macros de Citrix Endpoint Management en el campo Valor.

4. Haga clic en **Siguiente**. En la página **Proveedores de credenciales: Distribución**, configure lo siguiente:

- **CA emisora de certificados:** Seleccione el certificado de CA discrecional que agregó anteriormente.
- **Seleccionar modo de distribución:** Seleccione una de las siguientes maneras de generar y distribuir claves:
 - **Preferir modo centralizado: Generación de clave en el lado del servidor:** Citrix recomienda esta opción centralizada. Admite todas las plataformas compatibles con Citrix Endpoint Management y es necesaria cuando se usa la autenticación de NetScaler Gateway. Las claves privadas se generan y se almacenan en el servidor para, luego, distribuirse a los dispositivos de usuario.
 - **Preferir modo distribuido: Generación de clave en el lado del dispositivo:** Las claves privadas se generan y se almacenan en los dispositivos de usuario. Este modo de distribución utiliza SCEP y requiere un certificado de cifrado de RA con keyUsage keyEncryption, así como un certificado de firma de RA con KeyUsage digitalSignature. Se puede usar el mismo certificado para el cifrado y la firma.
 - **Solo distribuido: Generación de clave en el lado del dispositivo:** Esta opción funciona de la misma forma que **Preferir modo distribuido: Generación de clave en el lado del dispositivo**, salvo que no se permite ninguna otra opción si se produce un error en la generación de claves por parte del dispositivo o esta no está disponible.

Si selecciona **Preferir modo distribuido: Generación de clave en el lado del dispositivo** o **Solo distribuido: Generación de clave en el lado del dispositivo**, haga clic en el certificado de firma de RA y en el certificado de cifrado de RA. Se puede usar el mismo certificado tanto para el cifrado como para la firma. Aparecerán campos nuevos para esos certificados.

5. Haga clic en **Siguiente**. En la página **Proveedores de credenciales: Revocación Citrix Endpoint Management**, configure las condiciones en las que Citrix Endpoint Management marca internamente como revocados los certificados emitidos a través de esta configuración de proveedor. Configure las siguientes opciones:

Settings > Credential Providers > [Edit credential provider](#)

Credential Providers

- 1 General
- 2 Certificate Signing Request
- 3 Distribution
- 4 Revocation Endpoint Management**
- 5 Revocation PKI
- 6 Renewal

Credential Providers: Revocation Endpoint Management

Configure the conditions under which Endpoint Management should internally flag certificates, issued through this provider configuration, as revoked.

Revoke issued certificates ☒ When the certificate is renewed

☒ When the device is wiped or revoked

☒ When the device is deleted from Endpoint Management

When certificate is revoked

Send notification ☐ OFF

Revoke certificate on PKI ☐ OFF

- En **Revocar certificados emitidos**, seleccione una de las opciones que indican cuándo revocar los certificados.
 - Si quiere que Citrix Endpoint Management envíe una notificación cuando el certificado se revoque, **active** el parámetro **Enviar notificación** y seleccione una plantilla de notificaciones.
 - **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 PKI**, identifique las acciones que debe realizar en la infraestructura PKI si se revoca el certificado. También tiene la opción de crear un mensaje de notificación. Configure las siguientes opciones:

Credential Providers

- 1 General
- 2 Certificate Signing Request
- 3 Distribution
- 4 Revocation Endpoint Management
- 5 Revocation PKI**
- 6 Renewal

Credential Providers: Revocation PKI

Enable external revocation checks ☒ ON ⓘ

OCS responder CA certificate

When certificate is revoked

Send notification ☐ OFF

- **Habilitar comprobaciones de revocación externas:** **Active** esta configuración. Aparecerán campos adicionales relacionados con la infraestructura de clave pública de revocación.
- En la lista **Certificado de CA de respondedor OCS**, seleccione el nombre distintivo (DN) del sujeto del certificado.

Puede usar macros de Citrix Endpoint Management para los valores de los campos del 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 a realizar en la entidad de infraestructura PKI cuando se revoque el certificado:
 - No hacer nada.
 - Renovar el certificado.
 - Revocar y borrar el dispositivo.
- Si quiere que Citrix Endpoint Management envíe una notificación al revocarse un certificado, **active** el parámetro **Enviar notificación**.

Puede elegir entre dos opciones de notificación:

- Si selecciona **Seleccionar plantilla de notificaciones**, puede seleccionar un mensaje de notificación previamente escrito que puede personalizar. Estas plantillas se encuentran en la lista “Plantillas de notificaciones”.
- Si elige **Introducir detalles de notificación**, puede escribir su propio mensaje de notificación. Además de facilitar la dirección de correo electrónico del destinatario y el mensaje, puede configurar la frecuencia con que se envía la notificación.

7. Haga clic en **Siguiente**. En la página **Proveedores de credenciales: Renovación**, configure lo siguiente:

Settings > Credential Providers > [Edit credential provider](#)

Credential Providers	Credential Providers: Renewal
1 General	<p>Renew certificates when they expire <input checked="" type="checkbox"/> ON</p> <p>Renew when the certificate comes within * <input type="text" value="30"/> days of expiration</p> <p><input type="checkbox"/> Do not renew certificates that have already expired</p> <p>Send notification <input type="checkbox"/> OFF</p> <p>Notify when the certificate nears expiration <input type="checkbox"/> OFF</p>
2 Certificate Signing Request	
3 Distribution	
4 Revocation Endpoint Management	
5 Revocation PKI	
6 Renewal	

Active la opción **Renovar certificados** cuando caduquen. Aparecen más campos.

- En el campo **Renovar el certificado cuando queden**, escriba la antelación (la cantidad de días anteriores a la fecha de caducidad) con que debe realizarse la renovación.
- También puede seleccionar **No renovar certificados que ya han caducado**. En este caso, “ya caducado” significa que la fecha **NotAfter** del certificado ha pasado, no que ha sido revocado. Citrix Endpoint Management no renueva los certificados después de que hayan sido revocados internamente.

Si quiere que Citrix Endpoint Management envíe una notificación tras renovarse el certificado, **active** el parámetro **Enviar notificación**. Si quiere que Citrix Endpoint Management envíe una notificación cuando la fecha de caducidad se acerque, **active** el parámetro **Notificar cuando se acerque la fecha de caducidad**.

Para cualquiera de esas opciones, puede elegir entre dos opciones de notificación:

- **Seleccionar plantilla de notificaciones:** Seleccione un mensaje de notificación previamente escrito que puede personalizar. Estas plantillas se encuentran en la lista “Plantillas de notificaciones”.
- **Introducir detalles de 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

March 1, 2024

Los proveedores de credenciales son las configuraciones de certificado en cuestión que se usarán en las distintas partes del sistema de Citrix Endpoint Management. Los proveedores de credenciales definen los orígenes, los parámetros y los ciclos de vida de los certificados. Esas operaciones ocurren cuando los certificados forman parte de configuraciones del dispositivo o se trata de operaciones independientes (es decir, enviadas tal cual al dispositivo).

La inscripción de dispositivos limita el ciclo de vida de los certificados. Es decir, Citrix Endpoint Management no emite certificados antes de la inscripción, aunque Citrix Endpoint Management puede emitir algunos certificados como parte de la inscripción. Además, los certificados que emita la infraestructura de clave pública interna en el contexto de una inscripción se revocan cuando la inscripción en cuestión se revoca. Una vez que la relación de administración haya finalizado, no queda ningún certificado válido.

Puede usar una configuración de proveedores de credenciales en varios sitios, con lo que una sola configuración puede gestionar una cantidad infinita de certificados al mismo tiempo. Entonces, la unidad radica en el recurso de la 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, los parámetros de emisión de P determinan el certificado que se implementará en D. Del mismo modo, los parámetros de renovación previstos para D se aplicarán cuando se actualice C. Asimismo, los parámetros de revocación previstos para D también se aplicarán cuando C se elimine o cuando D se revoque.

De acuerdo con esas reglas, la configuración del proveedor de credenciales en Citrix Endpoint Management determina lo siguiente:

- El origen de los certificados.
- El método con que se obtienen los certificados: mediante la firma de un certificado nuevo o la obtención (recuperación) de un par de claves y un certificado existentes.
- Los parámetros para la emisión o la recuperación. Por ejemplo: los parámetros de la solicitud de firma de certificado (CSR), como el tamaño de la clave, el algoritmo de la clave y las extensiones del certificado.
- El modo en que los certificados se entregan al dispositivo.
- Las condiciones de revocación. Aunque todos los certificados se revocan en Citrix Endpoint Management cuando finaliza la relación de administración, se puede especificar una revocación anterior en la configuración. Por ejemplo, la configuración puede especificar revocar un certificado cuando se elimina la configuración asociada a él. Además, en algunas ocasiones, la revocación del certificado asociado en Citrix Endpoint Management se puede enviar a la infraestructura de clave pública (PKI) back-end. Es decir, la revocación de certificados en Citrix Endpoint Management puede causar la revocación de certificados en la PKI.
- Los parámetros de renovación. Los certificados que se obtienen mediante un proveedor de credenciales determinado se pueden renovar automáticamente cuando se acerque su fecha de caducidad. Además, independientemente de esas circunstancias, se pueden emitir notificaciones cuando se acerque esa fecha de caducidad.

La disponibilidad de las opciones de configuración depende principalmente del tipo de entidad PKI y del método de emisión que seleccione para el proveedor de credenciales.

Método de emisión de certificados

Puede obtener un certificado, el cual se conoce como método de emisión por firma.

Con este método, la emisión implica crear una nueva clave privada, crear una solicitud de firma de certificado y enviar esa solicitud a una entidad de certificación (CA) para su firma. Citrix Endpoint Management admite el método de firma tanto para las entidades de los Servicios de certificados de MS como para las entidades de CA discrecional.

Un proveedor de credenciales usa el método de emisión “sign”.

Entrega de certificados

En Citrix Endpoint Management, dispone de dos modos de entrega de certificados: centralizado y distribuido. El modo distribuido usa SCEP (Protocolo de inscripción de certificados simple) y solo está disponible en los casos en que el cliente admite el protocolo (solo para iOS). El modo distribuido es obligatorio en algunas situaciones.

Para que un proveedor de credenciales admita la entrega distribuida (mediante SCEP), se necesita un paso especial de configuración: se deben configurar certificados de una entidad de registro (RA). Los certificados de RA son necesarios porque, cuando se usa el protocolo SCEP, Citrix Endpoint Management actúa como un delegado (un registrador) para la entidad de certificación. Citrix Endpoint Management debe demostrar al cliente que tiene autoridad para actuar como tal. Esa autoridad se establece cargando en Citrix Endpoint Management los certificados mencionados anteriormente.

Se necesitan dos roles de certificados (aunque un solo certificado pueda satisfacer ambos requisitos): la firma de RA y el cifrado de RA. A continuación se presentan las restricciones de esos roles:

- El certificado de firma de RA debe tener una firma digital de uso de clave X.509.
- El certificado de cifrado de RA debe tener un cifrado de clave de uso de clave X.509.

Para configurar los certificados de RA del proveedor de credenciales, cárguelos en Citrix Endpoint Management y, a continuación, vincule su implementación a ellos en el proveedor de credenciales.

Se considera que un proveedor de credenciales admite la entrega distribuida solamente si tiene un certificado configurado para los roles de certificado. Puede configurar cada proveedor de credenciales para que prefiera el modo centralizado o el modo distribuido, o bien para que requiera el modo distribuido. El resultado real depende del contexto: si el contexto no admite el modo distribuido mientras que el proveedor de credenciales lo requiere, la implementación falla. Del mismo modo, si el contexto requiere el modo distribuido pero el proveedor de credenciales no lo admite, la implementación falla. En todos los demás casos, se respeta la preferencia asignada.

En la siguiente tabla se muestra la distribución de SCEP mediante Citrix Endpoint Management:

Contexto	Se admite SCEP	Se requiere SCEP
Servicio de perfil de iOS	Sí	Sí
Inscripción y administración de dispositivos móviles iOS	Sí	No
Perfiles de configuración de iOS	Sí	No
Inscripción de SHTTP	No	No
Configuración de SHTTP	No	No
Inscripción de tabletas Windows	No	No
Configuración de tabletas Windows	No, excepto la directiva de red, admitida en Windows 10 y Windows 11	No

Revocación de certificados

Existen tres tipos de revocación.

- **Revocación interna:** La revocación interna afecta al estado del certificado que mantiene Citrix Endpoint Management. Este estado se tiene en cuenta cuando Citrix Endpoint Management evalúa un certificado que se le presenta o cuando debe proporcionar información del estado OCSP de un certificado. La configuración del proveedor de credenciales determina el impacto sobre el estado cuando se dan varias condiciones. Por ejemplo, el proveedor de credenciales puede especificar que los certificados obtenidos mediante él deban marcarse como revocados cuando se eliminan del dispositivo.
- **Revocación propagada de forma externa:** También conocida como revocación de Citrix Endpoint Management, este tipo de revocación se aplica a certificados obtenidos de una infraestructura de clave pública externa. Este certificado se revoca en la infraestructura de clave pública cuando Citrix Endpoint Management lo revoca internamente si se cumplen las condiciones definidas en la configuración del proveedor de credenciales.
- **Revocación inducida externamente:** También conocida como infraestructura de clave pública de revocación, este tipo de revocación también se aplica solo a certificados obtenidos de una infraestructura de clave pública externa. Siempre que Citrix Endpoint Management evalúa el estado de un certificado concreto, también consulta ese estado en la infraestructura de clave pública. Si el certificado está revocado, Citrix Endpoint Management lo revoca internamente. Este mecanismo utiliza el protocolo OCSP.

Estos tres tipos no son exclusivos, sino que se aplican juntos. Una revocación externa u otro motivo pueden causar una revocación interna. Una revocación interna afecta potencialmente a una revocación externa.

Renovación de certificados

La renovación de un certificado es la combinación de una revocación del certificado existente y una emisión de otro certificado.

Citrix Endpoint Management intenta obtener el nuevo certificado antes de revocar el anterior, a fin de evitar la interrupción del servicio que se produce cuando la emisión falla. Para la entrega distribuida (compatible con SCEP), la revocación también ocurre solamente después de que el certificado se haya instalado correctamente en el dispositivo. De lo contrario, la revocación ocurre antes de que se envíe el nuevo certificado al dispositivo. Esa revocación no depende de la instalación del certificado.

La configuración de la revocación requiere que especifique una duración (en días). Cuando el dispositivo se conecta, el servidor comprueba si la fecha **NotAfter** del certificado es posterior a la fecha actual, menos el tiempo especificado. Si el certificado cumple esa condición, Citrix Endpoint Management intenta renovarlo.

Crear un proveedor de credenciales

La configuración de un proveedor de credenciales varía principalmente en la entidad de emisión y el método de emisión elegidos para el proveedor de credenciales. Puede distinguir entre los proveedores de credenciales que usan una entidad interna o una entidad externa:

- Una entidad discrecional, interna en Citrix Endpoint Management, es una entidad interna. El método de emisión para una entidad discrecional es siempre “sign”. Este método “sign” 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. El método de distribución seleccionado determina si el par de claves se genera en el dispositivo o en el servidor.
- Una entidad externa, que forma parte de la infraestructura corporativa, incluye la CA de Microsoft.

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha de la consola. A continuación, haga clic en **Parámetros > Proveedores de credenciales**.

2. En la página **Proveedores de credenciales**, haga clic en **Agregar**.

Aparecerá la página **Credential Providers: General Information**.

3. En la página **Credential Providers: General Information**, lleve a cabo lo siguiente:

- **Nombre:** Escriba un nombre exclusivo para la configuración del nuevo proveedor. Este nombre se usará posteriormente para identificar la configuración en otras partes de la consola de Citrix Endpoint Management.
- **Descripción:** Describa el proveedor de credenciales. Aunque este campo sea opcional, una descripción puede resultar útil cuando necesite datos concretos acerca del proveedor de credenciales.
- **Entidad de emisión:** Haga clic en la entidad emisora de certificados.
- **Método de emisión:** Haga clic en **Sign** o en **Fetch** para designar el método que usará el sistema para obtener certificados de la entidad configurada. Para la autenticación con certificado del cliente, use **Sign**.
- Si la lista **Plantilla** está disponible, seleccione la plantilla que agregó en el apartado de entidad PKI para el proveedor de credenciales.

Estas plantillas pasan a estar disponibles cuando se agregan entidades de Servicios de certificado de Microsoft en **Parámetros > Entidades PKI**.

4. Haga clic en **Siguiente**.

Aparecerá la página **Credential Providers: Certificate Signing Request**.

5. En la página **Proveedores de credenciales: Solicitud de firma de certificado**, defina lo siguiente según la configuración de su certificado:

- **Algoritmo de clave:** Seleccione 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 de las claves DSA es de 2048 bits. Para evitar falses negativos, los cuales dependen del hardware y software subyacentes, Citrix Endpoint Management no aplica tamaños de clave. Debe probar 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:** Campo obligatorio. Escriba el nombre distintivo (DN) del nuevo sujeto del certificado. Por ejemplo:
`CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`

For example, for client certificate authentication, use these settings:

- **Key algorithm:** RSA
 - **Key size:** 2048
 - **Signature algorithm:** SHA256withRSA
 - **Subject name:** `cn=${user.username}`
- Para agregar una nueva 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.

Para la autenticación con certificados de cliente, especifique:

- **Tipo:** Nombre principal del usuario.
- **Valor:** `${user.userprincipalname}`

Al igual que para Nombre del sujeto, puede usar las macros de Citrix Endpoint Management en el campo Valor.

6. Haga clic en **Siguiente**.

Aparecerá la página **Credential Providers: Distribution**.

7. En la página **Credential Providers: Distribution**, lleve a cabo lo siguiente:

- En la lista **Certificados de CA emisora**, haga clic en el certificado de CA ofrecido. Dado que el proveedor de credenciales usa una entidad de certificación discrecional, el certificado

de CA de ese proveedor siempre será el certificado de CA configurado en la propia entidad. El certificado de CA se presenta aquí para mantener la coherencia con las configuraciones que usan entidades externas.

- En **Seleccionar modo de distribución**, haga clic en una de las siguientes maneras de generar y distribuir claves:
 - **Preferir modo centralizado: Generación de clave en el lado del servidor:** Citrix recomienda esta opción centralizada. Admite todas las plataformas compatibles con Citrix Endpoint Management y es necesaria cuando se usa la autenticación de NetScaler Gateway. Las claves privadas se generan y se almacenan en el servidor para, luego, distribuirse a los dispositivos de usuario.
 - **Preferir modo distribuido: Generación de clave en el lado del dispositivo:** Las claves privadas se generan y se almacenan en los dispositivos de usuario. Este modo de distribución utiliza SCEP y requiere un certificado de cifrado de RA con keyUsage keyEncryption, así como un certificado de firma de RA con KeyUsage digitalSignature. Se puede usar el mismo certificado para el cifrado y la firma.
 - **Solo distribuido: Generación de clave en el lado del dispositivo:** Esta opción funciona de la misma forma que “Preferir modo distribuido: Generación de clave en el lado del dispositivo”, salvo que no se permite ninguna otra opción si se produce un error en la generación de claves por parte del dispositivo o esta no está disponible.

Si selecciona **Preferir modo distribuido: Generación de clave en el lado del dispositivo** o **Solo distribuido: Generación de clave en el lado del dispositivo**, haga clic en el certificado de firma de RA y en el certificado de cifrado de RA. Se puede usar el mismo certificado tanto para el cifrado como para la firma. Aparecerán campos nuevos para esos certificados.

8. Haga clic en **Siguiente**.

Aparecerá la página **Credential Providers: Revocation Citrix Endpoint Management**. En esta página, puede configurar las condiciones que se deben dar para que Citrix Endpoint Management marque internamente como revocados los certificados que se emitan con esta configuración de proveedor.

9. En la página **Credential Providers: Revocation Citrix Endpoint Management**, lleve a cabo lo siguiente:
- En **Revocar certificados emitidos**, seleccione una de las opciones que indican cuándo revocar los certificados.
 - Si quiere que Citrix Endpoint Management envíe una notificación cuando el certificado se revoque, **active** el parámetro **Enviar notificación** y seleccione una plantilla de notificaciones.
 - Si quiere revocar el certificado presente en la infraestructura de clave pública cuando este se haya revocado en Citrix Endpoint Management, **active** el parámetro **Revocar certifi-**

cado en PKI y, en la lista **Entidad**, haga clic en una plantilla. La lista “Entidad” muestra todas las entidades de infraestructura disponibles con capacidades de revocación. Cuando el certificado se revoque en Citrix Endpoint Management, se enviará una llamada de revocación a la infraestructura de clave pública seleccionada de la lista “Entidad”.

10. Haga clic en **Siguiente**.

Aparecerá la página **Credential Providers: Revocation PKI**. En esta página, puede identificar las acciones que se deben realizar en la infraestructura de clave pública si se revoca el certificado. También tiene la opción de crear un mensaje de notificación.

11. En la página **Credential Providers: Revocation PKI**, lleve a cabo lo siguiente si quiere revocar certificados procedentes de la infraestructura de clave pública:

- **Active** el parámetro **Habilitar comprobaciones de revocación externas**. Aparecerán campos adicionales relacionados con la infraestructura de clave pública de revocación.
- En la lista **Certificado de CA de respondedor OCSP**, haga clic en el nombre distintivo (DN) del sujeto del certificado.

Puede usar macros de Citrix Endpoint Management para los valores de los campos del 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 a realizar en la entidad de infraestructura PKI cuando se revoque el certificado:
 - No hacer nada.
 - Renovar el certificado.
 - Revocar y borrar el dispositivo.

- Si quiere que Citrix Endpoint Management envíe una notificación al revocarse un certificado, **active** el parámetro **Enviar notificación**.

Puede elegir entre dos opciones de notificación:

- Si selecciona **Seleccionar plantilla de notificaciones**, puede seleccionar un mensaje de notificación previamente escrito que puede personalizar. Estas plantillas se encuentran en la lista “Plantillas de notificaciones”.
- Si elige **Introducir detalles de notificación**, puede escribir su propio mensaje de notificación. Además de facilitar la dirección de correo electrónico del destinatario y el mensaje, puede configurar la frecuencia con que se envía la notificación.

12. Haga clic en **Siguiente**.

Aparecerá la página **Credential Providers: Renewal**. En esta página, puede determinar que Citrix Endpoint Management opere de la siguiente manera:

- Renovar el certificado. Si lo quiere, puede enviar una notificación para la renovación y excluir los certificados ya caducados de la operación.
- Emitir una notificación para aquellos certificados cuya fecha de caducidad se acerca (notificación antes de renovación).

13. En la página **Credential Providers: Renewal**, lleve a cabo lo siguiente si quiere renovar certificados cuando estos caduquen:

Active la opción **Renovar certificados** cuando caduquen. Aparecen más campos.

- En el campo **Renovar el certificado cuando queden**, escriba la antelación (la cantidad de días anteriores a la fecha de caducidad) con que debe realizarse la renovación.
- También puede seleccionar **No renovar certificados que ya han caducado**. En este caso, “ya caducado” significa que la fecha **NotAfter** del certificado ha pasado, no que ha sido revocado. Citrix Endpoint Management no renueva los certificados después de que hayan sido revocados internamente.

Si quiere que Citrix Endpoint Management envíe una notificación tras renovarse el certificado, **active** el parámetro **Enviar notificación**. Si quiere que Citrix Endpoint Management envíe una notificación cuando la fecha de caducidad se acerque, **active** el parámetro **Notificar cuando se acerque la fecha de caducidad**.

Para cualquiera de esas opciones, puede elegir entre dos opciones de notificación:

- **Seleccionar plantilla de notificaciones:** Seleccione un mensaje de notificación previamente escrito que puede personalizar. Estas plantillas se encuentran en la lista “Plantillas de notificaciones”.
- **Introducir detalles de 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 al certificado le queden**, escriba la antelación (la cantidad de días anteriores a la fecha de caducidad) con que debe enviarse la notificación.

14. Haga clic en **Guardar**.

El proveedor de credenciales aparecerá en la tabla “Proveedores de credenciales”.

Certificados APNs

December 13, 2023

Para inscribir y administrar dispositivos Apple en Citrix Endpoint Management, configure un certificado del servicio de notificaciones push de Apple (APNs) proveniente de Apple. El certificado permite la Administración de dispositivos móviles a través de Apple Push Network.

Resumen del flujo de trabajo:

Paso 1: Cree una solicitud de firma de certificado (CSR) con uno de estos métodos:

- Crear una solicitud de firma de certificado mediante Acceso a Llaveros en macOS (recomendado por Citrix)
- Crear una solicitud de firma de certificado mediante Microsoft IIS
- Para crear una solicitud de firma de certificado mediante OpenSSL

Paso 2: Firme la solicitud de firma de certificado en Citrix Endpoint Management Tools

Paso 3: Envíe la solicitud de firma de certificado (CSR) firmada a Apple para obtener el certificado APNs

Paso 4: Con el mismo equipo utilizado para el paso 1, complete la solicitud de firma de certificado y exporte un archivo PKCS #12:

- Crear un archivo PKCS #12 mediante Acceso a Llaveros en macOS
- Crear un archivo PKCS #12 mediante Microsoft IIS
- Creación de un archivo PKCS #12 mediante OpenSSL

Paso 5: [Importe un certificado APNs en Citrix Endpoint Management](#)

Paso 6: Renueve un certificado APNs

Crear una solicitud de firma de certificado

Se recomienda crear una solicitud de firma de certificado mediante Acceso a Llaveros en macOS. También puede crear una solicitud de firma de certificado mediante Microsoft IIS u OpenSSL.

Importante:

- Para el ID de Apple que se utiliza para crear el certificado:
 - The Apple ID must be a corporate ID and not a personal ID.
 - Record the Apple ID that you use to create the certificate.
 - To renew your certificate, use the same organization name and Apple ID. Using a different Apple ID to renew the certificate require device re-enrollment.
- Si revoca el certificado, ya sea accidental o intencionadamente, ya no podrá administrar los dispositivos.
- Si ha utilizado el programa iOS Developer Enterprise Program para crear un certificado

push para MDM, debe gestionar las acciones correspondientes a los certificados migrados del portal Apple Push Certificates Portal.

Crear una solicitud de firma de certificado 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 haga clic en **Asistente para Certificados > Solicitar un certificado de una entidad**.
3. El Asistente para Certificados solicitará que introduzca la información siguiente:
 - **Dirección de correo electrónico:** Dirección de correo electrónico perteneciente a la cuenta de la persona o del rol que administra el certificado.
 - **Nombre común:** Nombre común de la cuenta de la persona o del rol que administra el certificado.
 - **Dirección de correo de la CA:** Dirección de correo electrónico de la entidad de certificación.
4. Seleccione las opciones **Se guarda en el disco** y **Permitirme especificar la información del par de llaves** y, a continuación, haga clic en **Continuar**.
5. Asigne y escriba un nombre para el archivo de solicitud de firma de certificado, guárdelo en el equipo y, a continuación, haga clic en **Guardar**.
6. Para especificar la información del par de claves, seleccione un **Tamaño de la clave** de 2048 bits y el **Algoritmo RSA**. A continuación, haga clic en **Continuar**. El archivo de solicitud de firma de certificado está listo para su carga como parte del proceso de certificado APNs.
7. Haga clic en **Aceptar** cuando el Asistente para Certificados haya terminado el proceso de solicitud de la firma de certificado.
8. Para continuar, firme la solicitud CSR.

Crear una solicitud de firma de certificado mediante Microsoft IIS

El primer paso para generar una solicitud de certificado APNs consiste en crear una solicitud de firma de certificado (CSR). Para Windows, genere una solicitud CSR mediante Microsoft IIS.

1. Abra Microsoft IIS.
2. Haga doble clic en el icono de Certificados de servidor para IIS.
3. En la ventana **Certificados de servidor**, haga clic en **Crear una solicitud de certificado**.
4. Escriba la información de nombre distintivo (DN) correspondiente. Por ejemplo, puede escribir el nombre de dominio completo (FQDN) del servidor de Citrix Endpoint Management, como www.domain.com. A continuación, haga clic en **Siguiente**.

5. Seleccione el **Proveedor de cifrado Microsoft RSA SChannel** como proveedor de servicios de cifrado. Asimismo, seleccione **2048** para la longitud en bits y, a continuación, haga clic en **Siguiente**.
6. Escriba un nombre de archivo y especifique una ubicación para guardar la solicitud de firma de certificado y, a continuación, haga clic en **Finalizar**.
7. Para continuar, firme la solicitud CSR.

Para crear una solicitud de firma de certificado mediante OpenSSL

Si no puede usar un dispositivo macOS o Microsoft IIS para generar una solicitud de firma de certificado, use OpenSSL. Puede descargar e instalar OpenSSL desde el sitio web de OpenSSL.

1. En el equipo donde instale OpenSSL, ejecute este comando desde el shell o del símbolo del sistema.

```
openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.csr -newkey rsa:2048
```

2. Aparece el siguiente mensaje con información pertinente para asignar nombres de certificado. Escriba la información tal y como se indica.

```
1 You are about to be asked to enter information that will be
  incorporated into your certificate request.
2 What you are about to enter is what is called a Distinguished Name
  or a DN.
3 There are quite a few fields but you can leave some blank
4 For some fields there will be a default value,
5 If you enter '.', the field will be left blank.
6 -----
7 Country Name (2 letter code) [AU]:US
8 State or Province Name (full name) [Some-State]:CA
9 Locality Name (eg, city) []:RWC
10 Organization Name (eg, company) [Internet Widgits Pty Ltd]:
    Customer
11 Organizational Unit Name (eg, section) [:Marketing
12 Common Name (eg, YOUR name) []:John Doe
13 Email Address []:john.doe@customer.com
14 <!--NeedCopy-->
```

3. En el siguiente mensaje, escriba una contraseña para la clave privada de la solicitud CSR.

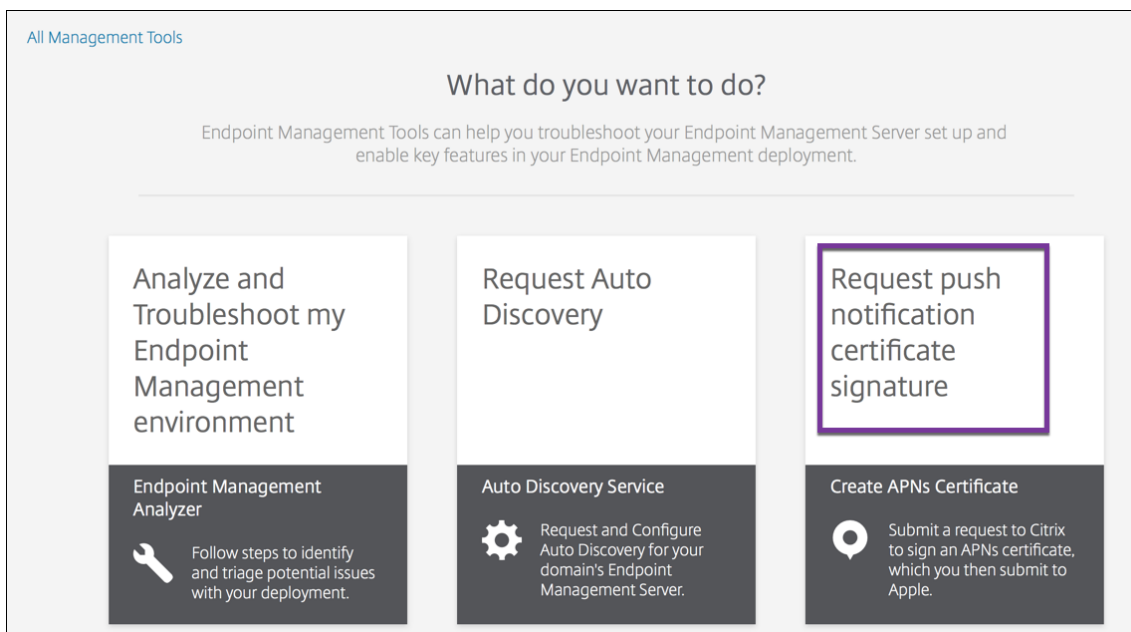
```
1 Please enter the following 'extra' attributes
2 to be sent with your certificate request
3 A challenge password []:
4 An optional company name []:
5 <!--NeedCopy-->
```

4. Para continuar, firme la solicitud de firma como se describe en la siguiente sección.

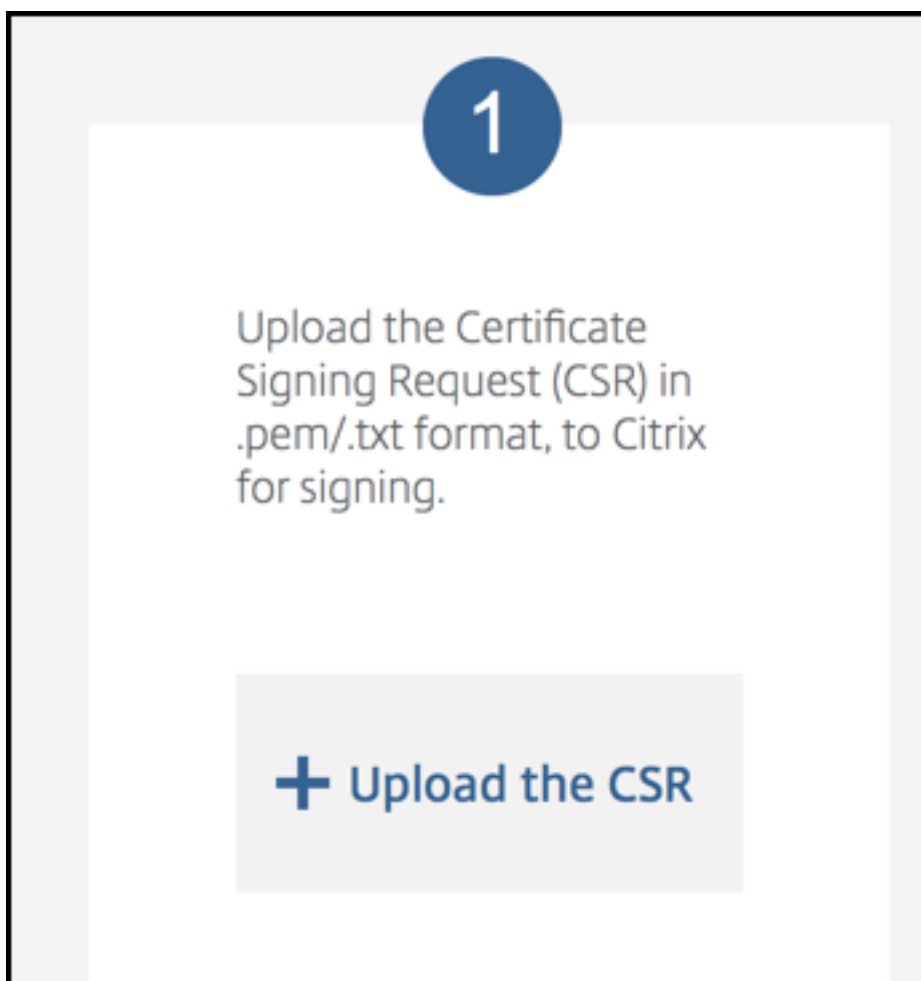
Firmar la solicitud de firma de certificado

Para utilizar un certificado con Citrix Endpoint Management, debe enviarlo a Citrix para su firma. Citrix firma la solicitud de firma de certificado con el certificado de firma de Administración de dispositivos móviles y devuelve el archivo firmado en un formato **.plist**.

1. En el explorador web, vaya al sitio web [Citrix Endpoint Management Tools](#) y haga clic en **Request push notification certificate signature**.



2. En la página **Creating a new certificate page**, haga clic en **Upload the CSR**.



3. Busque y seleccione el certificado.

Importante:

El certificado debe estar en el formato PEM o TXT. Si es necesario, para cambiar la extensión del nombre del archivo del certificado a .pem o .txt, haga clic con el botón secundario del mouse y cambie el nombre del archivo.

4. En la página **Citrix Endpoint Management APNs CSR Signing**, haga clic en **Sign**. La solicitud se firma y se guarda automáticamente en la carpeta de descargas definida.
5. Para continuar, envíe la solicitud de firma de certificado firmada como se describe en la siguiente sección.

Enviar la solicitud de firma de certificado firmada a Apple para obtener el certificado APNs

Después de recibir la solicitud de firma de certificado (CSR) firmada de Citrix, envíela a Apple para obtener el certificado de APNs necesario para importarlo en Citrix Endpoint Management.

Nota:

Algunos usuarios han informado de problemas para iniciar sesión en el portal de certificados push de Apple. Como alternativa, puede iniciar sesión en el [portal de Apple Developer](#). A continuación, puede seguir estos pasos:

1. En un explorador web, vaya al [Portal de certificados push de Apple](#).
2. Haga clic en **Create a Certificate**.
3. Si es la primera vez que crea un certificado con Apple, marque la casilla **I have read and agree to these terms and conditions** y, a continuación, haga clic en **Accept**.
4. Haga clic en **Choose File**, vaya al certificado firmado ubicado en el equipo y, a continuación, haga clic en **Upload**. Aparece un mensaje de confirmación donde se indica que la carga se ha realizado correctamente.
5. Haga clic en **Download** para obtener el certificado PEM.
6. Para continuar, rellene la solicitud de firma y exporte el archivo PKCS #12 como se describe en la siguiente sección.

Completar la solicitud de firma de certificado y exportar 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 tiene el archivo de certificado APNs y la clave privada. Los archivos PFX generalmente tienen la extensión PFX o P12. Puede utilizar archivos PFX o P12 indistintamente.

Importante:

Se recomienda guardar o exportar las claves personales y públicas del sistema local. Necesita esas claves para acceder a los certificados APNs y volver a utilizarlos. Sin las mismas claves, el certificado no es válido y debe repetir todo el proceso de solicitud CSR y APNs.

Crear un archivo PKCS #12 mediante Acceso a Llaveros en macOS

Importante:

Utilice el mismo dispositivo macOS para esta tarea que el que utilizó para generar la solicitud de firma de certificado.

1. En el dispositivo, busque el certificado de identidad de producción (PEM) recibido de Apple.
2. Inicie la aplicación Acceso a Llaveros y vaya a la ficha **Iniciar 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 comprobar que el certificado incluye una clave privada asociada.
4. Para comenzar a exportar el certificado a un certificado PKCS #12 (PFX), elija el certificado y la clave privada, haga clic con el botón secundario y seleccione **Exportar 2 elementos**.
5. Dé al archivo de certificado un nombre único para usarlo con Citrix Endpoint Management. No incluya espacios en el nombre. A continuación, elija una ubicación de carpeta para guardar el certificado, seleccione el formato de archivo PFX y haga clic en **Guardar**.
6. Escriba una contraseña para exportar el certificado. Citrix recomienda usar una contraseña única y segura. Además, compruebe que el certificado y la contraseña se encuentren en un lugar seguro para su uso y referencia posteriores.
7. La aplicación Acceso a Llaveros le solicitará la contraseña de inicio de sesión o el llavero seleccionado. Escriba la contraseña y, a continuación, haga clic en **Aceptar**. Ahora, el certificado guardado está listo para su uso 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:

Use el mismo servidor IIS para esta tarea que el que utilizó para generar la solicitud de firma de certificado.

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. 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, así como una contraseña, y, a continuación, haga clic en **Aceptar**.

Necesita la contraseña del certificado para importarlo a Citrix Endpoint Management.

7. Copie el certificado PFX al servidor en el que se instalará Citrix Endpoint Management.
8. Para continuar, consulte [Importar un certificado APNs en Citrix Endpoint Management](#).

Creación de un archivo PKCS #12 mediante OpenSSL

Si utiliza OpenSSL para crear una solicitud de firma de certificado, también puede usar OpenSSL para crear un certificado APNs PFX.

1. En un símbolo del sistema o shell, ejecute este comando. `Customer.privatekey.pem` es la clave privada de su solicitud de firma de certificado. `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. Escriba una contraseña para el archivo de certificado de extensión PFX. Recuerde esta contraseña porque necesitará volver a utilizarla al cargar el certificado en Citrix Endpoint Management.
3. Tome nota de la ubicación del archivo de certificado PFX. Copie el archivo al servidor de Citrix Endpoint Management a fin de poder usar la consola para cargar el archivo.
4. Para continuar, importe un certificado APNs en Citrix Endpoint Management, como se describe en la sección siguiente.

Importar un certificado APNs en Citrix Endpoint Management

Después de recibir un nuevo certificado APNs, importe ese certificado en Citrix Endpoint Management, ya sea para agregar el certificado por primera vez o para reemplazar un certificado existente.

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 P12 en su equipo.
5. Escriba la contraseña y, a continuación, haga clic en **Importar**.

Para obtener más información acerca de los certificados en Citrix Endpoint Management, consulte [Certificados y autenticación](#).

Para renovar un certificado APNs

Importante:

Si usa otro ID de Apple para el proceso de renovación, deberá volver a inscribir los dispositivos de usuario.

Para renovar un certificado APNs, siga los pasos necesarios 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, aparece el certificado existente o un certificado importado desde su cuenta anterior de desarrollador de Apple.

En el portal de certificados, la única diferencia cuando se renueva el certificado es que tiene que hacer clic en **Renew**. Debe tener una cuenta de desarrollador en el portal de certificados para acceder al sitio. Para renovar el certificado, utilice el mismo nombre de organización y el mismo ID de Apple.

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 solicitud CSR mediante Microsoft IIS, Acceso a Llaveros (macOS) u OpenSSL. Para obtener más información sobre cómo generar una solicitud CSR, consulte [Crear una solicitud de firma de certificado](#).
2. En su explorador web, vaya a [Citrix Endpoint Management Tools](#). A continuación, haga clic en **Request push notification certificate signature**.
3. Haga clic en **+ Upload the CSR**.
4. En el cuadro de diálogo, vaya a la solicitud CSR y haga clic en **Open y Sign**.
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 se va a renovar y, a continuación, haga clic en **Renew**.
8. Cargue el archivo `.plist`. Recibirá un archivo PEM de salida. Guarde el archivo PEM.
9. Con ese archivo PEM, complete la solicitud CSR (de acuerdo con el método que usó 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 este modo:

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**.

Import ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time. Use the [APNs portal](#) on the Endpoint Management Tools page to create the APNs certificate.

Import Keystore ▼

Keystore type PKCS#12 ▼

Use as APNs ▼

Keystore file * Browse

Password *

Description

Cancel Import

5. Para el **Archivo de almacén de claves**, haga clic en **Examinar** y vaya al archivo.
6. En **Contraseña**, escriba la contraseña del certificado.
7. Puede escribir una **descripción** opcional.
8. Haga clic en **Importar**.

Citrix Endpoint Management lo redirige de vuelta a la página **Certificados**. Se actualizan los campos **Nombre**, **Estado**, **Válido desde** y **Válido hasta**.

SAML para Single Sign-On en Citrix Files

March 1, 2024

Puede configurar Citrix Endpoint Management y ShareFile para que utilicen el lenguaje Security Assertion Markup Language (SAML) si quiere proporcionar el acceso de inicio de sesión único (Single Sign-On) a las aplicaciones móviles de Citrix Files. Esta funcionalidad incluye:

- Aplicaciones de Citrix Files que están habilitadas para el SDK de MAM o empaquetadas con MDX Toolkit
- Clientes de Citrix Files no empaquetados, como el sitio web, Outlook Plug-in o clientes de sincronización
- **En caso de aplicaciones empaquetadas de Citrix Files:** A los usuarios que inician sesión en Citrix Files se les redirige a Citrix Secure Hub para la autenticación de usuario y para obtener un token SAML. Después de una autenticación correcta, la aplicación de Citrix Files para móvil envía el token de 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 desde ShareFile a correos de Citrix Secure Mail sin iniciar sesión cada vez.
- **En caso de clientes no empaquetados de Citrix Files:** A los usuarios que inician sesión en Citrix Files desde un explorador web u otro cliente de Citrix Files se les redirige a Citrix Endpoint Management. Citrix Endpoint Management autentica a esos usuarios, quienes adquieren un token SAML que se envía a ShareFile. Después del primer inicio de sesión, los usuarios pueden acceder a los clientes de Citrix Files mediante Single Sign-On, sin iniciar sesión cada vez.

Si quiere usar Citrix Endpoint Management como un proveedor de identidades (IdP) SAML para ShareFile, debe configurar Citrix Endpoint Management para que use con cuentas Enterprise, como se describe en este artículo. También puede configurar Citrix Endpoint Management para que funcione solamente con conectores de zonas de almacenamiento. Para obtener más información, consulte [Uso de ShareFile con Citrix Endpoint Management](#).

Para obtener un diagrama detallado con una arquitectura como referencia, consulte [Arquitectura](#).

Requisitos previos

Debe cumplir los siguientes requisitos previos antes de configurar SSO en Citrix Endpoint Management y las aplicaciones de Citrix Files:

- El SDK de MAM 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 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 de ShareFile

Antes de configurar SAML para ShareFile, debe indicar la información de acceso de ShareFile de la siguiente manera:

1. En la consola web de Citrix Endpoint Management, haga clic en **Configurar > ShareFile**. Aparecerá la página de configuración **ShareFile**.

The screenshot shows the 'Content Collaboration' configuration page in Citrix Endpoint Management. The page title is 'Content Collaboration' with a dropdown arrow. Below the title is a subtitle: 'Configure settings to connect to the Content Collaboration and administrator service accounts for user account management.' The page is divided into several sections:

- Domain ***: A text input field containing '.sharefile.com'.
- Assign to delivery groups**: A section with a search bar labeled 'Type to search' and a 'Search' button. Below the search bar is a list of delivery groups with checkboxes: 'AllUsers', 'Local Policy', 'o87', and 'Local'.
- Content Collaboration Administrator Account Login**: A section with two text input fields: 'User name *' (containing '.com') and 'Password *' (containing 'Enter new password'). Below these fields is a green 'Test Connection' button.
- User account provisioning**: A toggle switch currently set to 'OFF'.
- App internal name**: A text input field containing 'ShareFile_SAML'.
- SAML certificate**: A section with a 'Name' text input field containing '.example.com'.

At the bottom of the page, it says 'Advanced Content Collaboration Configuration'.

2. Configure estos parámetros:

- **Dominio:** Escriba el nombre del subdominio de ShareFile. Por ejemplo: `example.sharefile.com`.
- **Asignar a grupos de entrega:** Seleccione o busque los grupos de entrega que podrán usar SSO en ShareFile.
- **Inicio de sesión de 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 este parámetro inhabilitado. Usar la herramienta ShareFile User Management Tool 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 realizan la autenticación 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 entidad o emisor 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 Modificar los parámetros de Single Sign-On para Citrix Files.com.

Configurar SAML para aplicaciones MDX empaquetadas de Citrix Files

No es necesario usar la configuración de NetScaler Gateway para Single Sign-On con aplicaciones de Citrix Files preparadas con el SDK de MAM. Para configurar el acceso de clientes de Citrix Files no empaquetados, como el sitio web, Outlook Plug-in o los clientes de sincronización, consulte [Configurar NetScaler Gateway para otros clientes de Citrix Files](#).

Para configurar SAML en aplicaciones MDX de Citrix Files empaquetadas:

1. Descargue ShareFile para los clientes de Citrix Endpoint Management. Consulte [Descargas de Citrix.com](#).
2. Prepare la aplicación móvil de Citrix Files con el SDK de MAM. Para obtener información detallada, consulte [Introducción al SDK de MAM](#).
3. En la consola de Citrix Endpoint Management, cargue la aplicación para móvil preparada de Citrix Files. Para obtener información sobre cómo cargar aplicaciones MDX, consulte [Para agregar una aplicación MDX a Citrix Endpoint Management](#).
4. Para comprobar los parámetros de SAML, inicie sesión en ShareFile con el nombre de usuario y contraseña de administrador que ha configurado anteriormente.
5. Compruebe que ShareFile y Citrix Endpoint Management están configurados en la misma zona horaria. Compruebe que Citrix Endpoint Management muestra la hora correcta con respecto a la zona horaria configurada. Si no, Single Sign-On podría fallar.

Validar la aplicación móvil de Citrix Files

1. En el dispositivo de usuario, instale y configure Citrix Secure Hub.
2. Desde el almacén de aplicaciones, descargue e instale la aplicación para móvil de Citrix Files.

3. Inicie la aplicación móvil de Citrix Files. Citrix Files se inicia sin solicitar el nombre de usuario ni la contraseña.

Validar con Citrix Secure Mail

1. En el dispositivo de usuario (si no se ha hecho aún), instale y configure Citrix Secure Hub.
2. Desde el almacén de aplicaciones, descargue, instale y configure Citrix Secure Mail.
3. Abra un nuevo correo electrónico y toque en **Adjuntar desde ShareFile**. Los archivos disponibles para adjuntar al mensaje de correo electrónico se muestran sin solicitar el nombre de usuario ni la contraseña.

Configurar NetScaler Gateway para otros clientes de Citrix Files

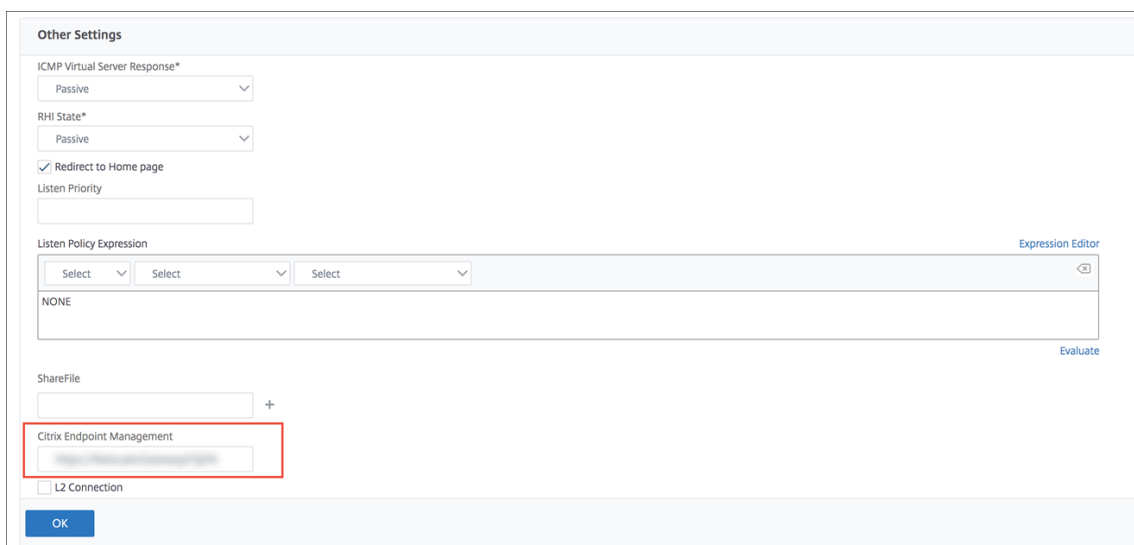
Si quiere configurar el acceso para clientes no empaquetados de Citrix Files (como el sitio web, el plugin para Outlook o los clientes de sincronización), debe configurar NetScaler Gateway para que admita Citrix Endpoint Management como proveedor de identidades SAML de la siguiente manera.

- Inhabilite la redirección de la página principal.
- Cree un perfil y una directiva de sesión de Citrix Files.
- Configure directivas en el servidor virtual de NetScaler Gateway.

Inhabilitar la redirección de la página principal

Inhabilite el comportamiento predeterminado para las solicitudes que provienen de la ruta /cginfra. Esa acción permite a los usuarios ver la URL interna solicitada original, en lugar de la página de inicio configurada.

1. Modifique la configuración del servidor virtual de NetScaler Gateway que se usa para los inicios de sesión de Citrix Endpoint Management. En NetScaler Gateway, vaya a **Other Settings** y, a continuación, desmarque la casilla **Redirect to Home Page**.



2. En **ShareFile** (ahora denominado ShareFile), escriba el nombre del servidor interno y el número de puerto de Citrix Endpoint Management.
3. En **Citrix Endpoint Management**, escriba la dirección URL de Citrix Endpoint Management.
Esta configuración autoriza solicitudes a la URL que ha especificado mediante la ruta /cginfra.

Crear un perfil de solicitudes y una directiva de sesión de Citrix Files

Configure los siguientes parámetros para crear un perfil de solicitudes y una directiva de sesión de Citrix Files:

1. En la herramienta de configuración de NetScaler Gateway, en el panel de navegación de la izquierda, 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. Para crear una acción nueva, haga clic en el botón **+**. Aparecerá la página **Create NetScaler Gateway Session Profile**.

Configure NetScaler Gateway Session Profile

Name
Sharefile_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration | **Client Experience** | Security | Published Applications

Accounting Policy
None

Override Global

☐ Display Home Page ☒

Home Page
none

URL for Web-Based Email
[Empty]

Split Tunnel*
OFF

Session Time-out (mins)
1

Client Idle Time-out (mins)
[Empty]

Clientless Access*
Allow

Clientless Access URL Encoding*
Obscure

Clientless Access Persistent Cookie*
DENY

Plug-in Type*
Windows/MAC OS X

☒ Single Sign-on to Web Applications ☒

Credential Index*
PRIMARY

KCD Account
[Empty]

Configure estos parámetros:

- **Name:** Escriba **ShareFile_Profile**.
- Haga clic en la ficha **Client Experience** y, a continuación, configure los siguientes parámetros:
 - **Home Page:** Escriba **none**.
 - **Tiempo de espera de la sesión (min):** Escriba **1**.
 - **Single Sign-On to Web Applications:** Marque este parámetro.
 - **Credential Index:** En la lista, haga clic en **PRIMARY**.
- Haga clic en la ficha **Published Applications**.

Configure NetScaler Gateway Session Profile

Configure NetScaler Gateway Session Profile

Name
Sharefile_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security **Published Applications**

Override Global

ICA Proxy*
ON ☒

Web Interface Address
 ☒ ?

Web Interface Address Type*
IPV4

Web Interface Portal Mode*
NORMAL ☐

Single Sign-on Domain
citrix ☒

Citrix Receiver Home Page
 ☐

Account Services Address
 ☐

OK Close

Configure estos parámetros:

- **ICA Proxy:** En la lista, haga clic en **ON**.
- **Web Interface Address:** Escriba la URL del servidor Citrix Endpoint Management.
- **Single Sign-On Domain:** Escriba el nombre del dominio de Active Directory.

Al configurar el perfil de sesión de NetScaler Gateway, el sufijo de dominio de **Single Sign-On Domain** debe coincidir con el alias de dominio de Citrix Endpoint Management definido en el protocolo LDAP.

5. Haga clic en **Create** para definir el perfil de sesión.
6. Haga clic en **Expression Editor**.

Configure estos parámetros:

- **Value:** Escriba **NSC_FSRD**.
- **Header Name:** Escriba **COOKIE**.

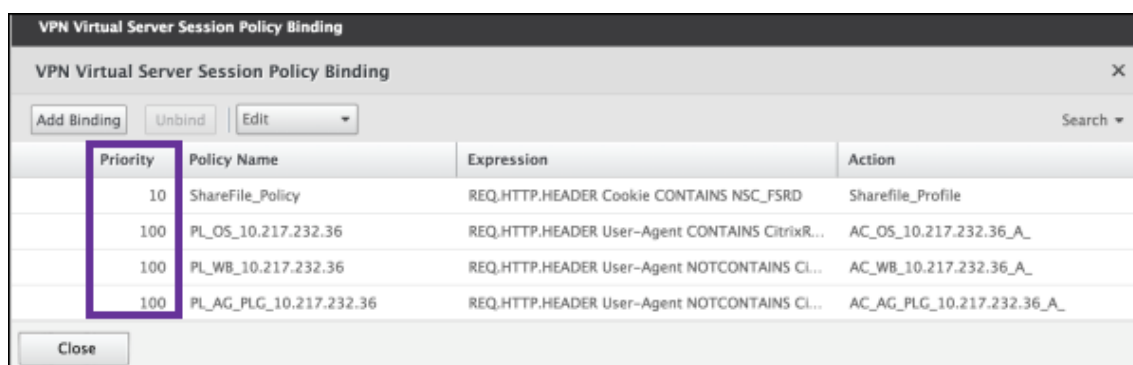
7. Haga clic en **Create** y, luego, en **Close**.

Configurar directivas en el servidor virtual de NetScaler Gateway

Configure los siguientes parámetros en el servidor virtual de NetScaler Gateway.

1. En la herramienta de configuración de NetScaler Gateway, en el panel de navegación de la izquierda, haga clic en **NetScaler Gateway > Virtual Servers**.
2. En el panel **Details**, haga clic en el servidor virtual de NetScaler Gateway.
3. Haga clic en **Edit**.

4. Haga clic en **Configured policies > Session policies** y, a continuación, haga clic en **Add binding**.
5. Seleccione **ShareFile_Policy**.
6. Modifique el número de **Priority** generado automáticamente de la directiva seleccionada, de modo que esta tenga la prioridad más alta (el número más bajo) en relación con las demás directivas de la lista, tal y como se muestra en la siguiente imagen. Por ejemplo:



Priority	Policy Name	Expression	Action
10	ShareFile_Policy	REQ.HTTP.HEADER Cookie CONTAINS NSC_FSRD	Sharefile_Profile
100	PL_OS_10.217.232.36	REQ.HTTP.HEADER User-Agent CONTAINS CitrixR...	AC_OS_10.217.232.36_A_
100	PL_WB_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Cl...	AC_WB_10.217.232.36_A_
100	PL_AG_PLG_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Cl...	AC_AG_PLG_10.217.232.36_A_

7. Haga clic en **Done** y, a continuación, guarde la configuración activa de NetScaler Gateway.

Modificar los parámetros de Single Sign-On para Citrix Files.com

Realice los siguientes cambios para aplicaciones Citrix Files que se hayan empaquetado con MDX o no.

Importante:

Se anexa un nuevo número al nombre interno de la aplicación:

- Cada vez que modifique o vuelva a crear la aplicación Citrix Files
- Cada vez que cambie la configuración de ShareFile en Citrix Endpoint Management

Por eso, también debe actualizar la URL de inicio de sesión en el sitio web de Citrix Files, para reflejar el nombre actualizado de la aplicación.

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 **Administración** y, a continuación, seleccione **Configurar Single Sign-On**.
3. Modifique el campo **URL de inicio de sesión** de la siguiente manera:

Esta es una **URL de inicio de sesión** de ejemplo antes de las modificaciones: https://xms.citrix.lab/samlsp/webssso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1.

The screenshot shows the 'Basic Settings' page in the Citrix Endpoint Management console. The 'Login URL' field is highlighted with a red oval. The page includes a navigation bar with links: Home, Manage Users, Send a File, Request a File, Admin, My Settings, and Apps. On the left, there is a sidebar with links: Password Policy, Configure Single Sign-On, Edit Super User Group, Reporting, Notification History, Login Code Sample, Remote Upload Wizard, and View/Print Receipts. The main content area has the following settings:

Basic Settings	
Enable SAML:	<input checked="" type="checkbox"/> ?
ShareFile Issuer / Entity ID:	XMS.example.com ?
Your IDP Issuer / Entity ID:	<input type="text"/> ?
X.509 Certificate:	Saved Change ?
Login URL:	<input type="text"/> ?
Logout URL:	<input type="text"/> ?

- Introduzca el nombre de dominio completo (FQDN) del servidor virtual externo de NetScaler Gateway y **/cginfra/https** delante del FQDN del servidor Citrix Endpoint Management. A continuación, agregue **8443** después del FQDN de Citrix Endpoint Management.

Esta es una URL modificada de ejemplo: https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/webssso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1

- Cambie el parámetro **&app=ShareFile_SAML_SP** al nombre interno de la aplicación Citrix Files. De forma predeterminada, el nombre interno es **ShareFile_SAML**. Sin embargo, cada vez que cambie la configuración, se agregará un número al nombre interno (**ShareFile_SAML_2**, **ShareFile_SAML_3**, etc.). Puede buscar el **nombre interno de la aplicación** en la página **Configurar > ShareFile**.

Esta es una URL modificada de ejemplo: https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/webssso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1

- Agregue **&nssso=true** al final de la URL.

Este es un ejemplo de la URL final: https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/webssso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true.

4. En **Parámetros optativos**, marque la casilla **Habilitar autenticación web**.

Optional Settings

Require SSO Login: ☐ ?

SSO IP Range: ?

SP-Initiated SSO certificate: HTTP Redirect with no signature ?

Enable Web Authentication: ☒ ?

SP-Initiated Auth Context: User Name and Password Minimum ?

Active Profile Cookies: ?

☒ Save Cancel

Validar la configuración

Lleve a cabo lo siguiente para validar la configuración.

1. Apunte el explorador web a <https://<subdomain>sharefile.com/saml/login>.

Se le redirigirá al formulario de inicio de sesión de NetScaler Gateway. Si no se le redirige, compruebe los parámetros de configuración anteriores.

2. Escriba el nombre de usuario y la contraseña del entorno de Citrix Endpoint Management y NetScaler Gateway que haya configurado.

Aparecerán sus carpetas de Citrix Files en <subdomain>.sharefile.com. Si no ve las carpetas de Citrix Files, compruebe que ha indicado correctamente las credenciales de inicio de sesión.

Autenticación con Azure Active Directory a través de Citrix Cloud

March 1, 2024

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 utilizar Citrix Secure Hub con MDM+MAM, configure Citrix Endpoint Management de modo que se pueda usar NetScaler Gateway para la inscripción de MAM. Para obtener más información, consulte [NetScaler Gateway y Citrix Endpoint Management](#).

Citrix Endpoint Management utiliza el servicio de Citrix Cloud llamado “Identidad de Citrix” para la federación con Azure Active Directory. Citrix recomienda usar el proveedor de identidades 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 que no estén inscritos en Apple Business Manager o Apple School Manager
- Dispositivos iOS y macOS inscritos en Apple Business Manager
- Dispositivos Android Enterprise (Tech Preview) para el modo BYOD y el modo totalmente administrado

La autenticación con Azure AD a través de Citrix Cloud presenta estas limitaciones:

- No está disponible para cuentas locales de Citrix Endpoint Management.
- No admite la autenticación a través de Azure AD para invitaciones de inscripción. Si envía una invitación de inscripción a los usuarios y esa invitación contiene una URL de inscripción, los usuarios deberán autenticarse a través de LDAP en lugar de Azure AD.

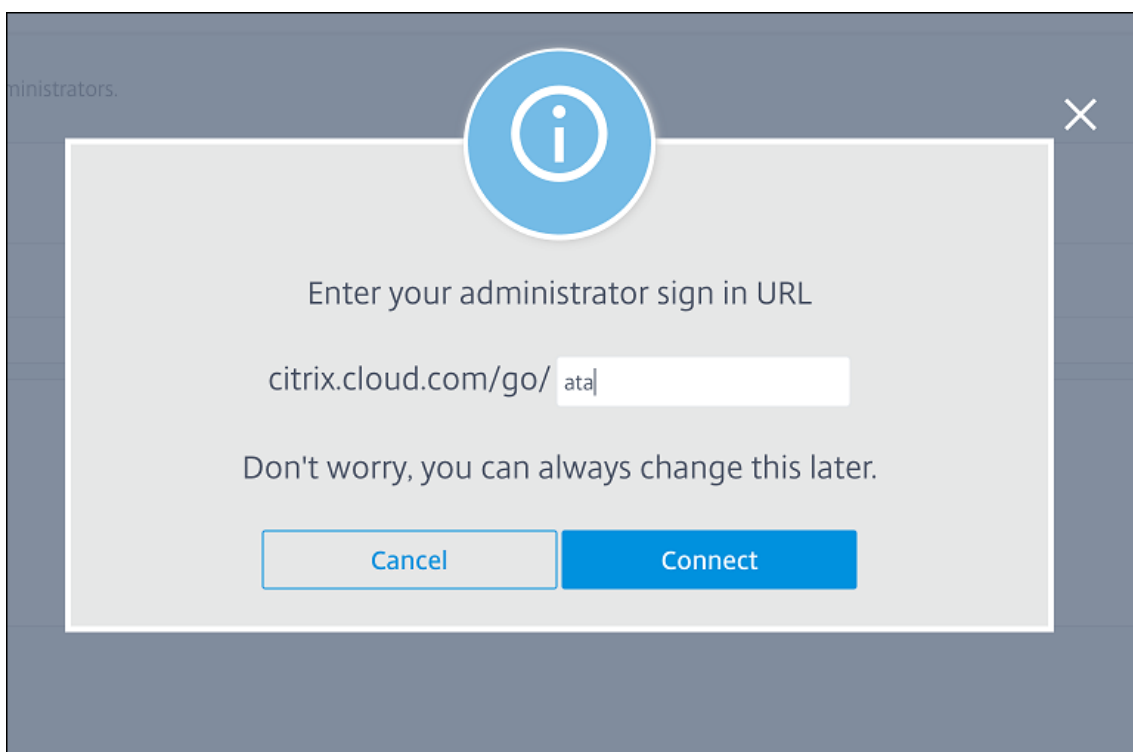
Requisitos previos

- Credenciales de usuario de Azure Active Directory
- Los grupos de usuarios de Active Directory deben coincidir con los grupos de usuarios de Azure Active Directory.
- Los nombres de usuario y las direcciones de correo electrónico de Active Directory deben coincidir con los de Azure Active Directory.
- Cuenta de Citrix Cloud, con Citrix Cloud Connector instalado para la sincronización de servicios de directorio.
- NetScaler Gateway. Citrix recomienda habilitar la autenticación basada en certificados o Azure AD para disponer de Single Sign-On de manera integral. Si utiliza la autenticación LDAP en NetScaler Gateway para la inscripción MAM, los usuarios finales ven un mensaje de autenticación doble durante la inscripción. Para obtener más información, consulte [Autenticación con certificado de cliente o certificado y dominio](#).
- En los perfiles de inscripción para Android Enterprise, **desactive** la opción **Permitir a los usuarios rechazar la administración de dispositivos**. Si los usuarios rechazan la administración de dispositivos, no pueden inscribirse con un proveedor de identidades para autenticarse. Para obtener más información, consulte [Seguridad de la inscripción](#).

Configurar Citrix Cloud para que use Azure Active Directory como proveedor de identidades

Para configurar este servicio de modo que pueda usarse 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. En el menú de Citrix Cloud, vaya a la página **Administración de acceso e identidad** y conéctese a Azure Active Directory.
3. Escriba su URL de inicio de sesión de administrador y haga clic en **Conectar**.



4. Una vez iniciada la sesión, su cuenta de Azure Active Directory se conecta a Citrix Cloud. La página **Administración de acceso e identidad > Autenticación** muestra las cuentas a usar para iniciar sesión en las 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**. Después de completar la configuración, puede inscribir dispositivos de usuario a través de Citrix Secure Hub.

Configurar Identidad de Citrix como tipo de IDP para Citrix Endpoint Management

Esta configuración solo se aplica 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 esta manera.

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > 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 del proveedor de identidades que creará.
 - **Tipo de IDP:** Elija **Citrix Identity Platform**.
 - **Dominio de autenticación:** Elija **Azure Active Directory**. Este dominio corresponde al dominio del proveedor de identidades de la página de Citrix Cloud **Configuración de Workspace > Autenticación**.
3. Haga clic en **Siguiente**. En la página **Uso de notificaciones IDP**, configure lo siguiente:
 - **Tipo de identificador de usuario:** De forma predeterminada, este campo se establece como **userPrincipalName**. Asegúrese de configurar todos los usuarios con el mismo identificador, tanto en Active Directory local como en Azure Active Directory. Citrix Endpoint Management utiliza este identificador para asignar usuarios del proveedor de identidades con usuarios de Active Directory local.
 - **Cadena de identificador del usuario:** Este campo se rellena automáticamente.
4. Haga clic en **Siguiente**, revise la información de la página **Resumen** y, a continuación, haga clic en **Guardar**.

Ahora, los usuarios de Citrix Secure Hub, la consola de Citrix Endpoint Management y Self-Help Portal pueden iniciar sesión con sus credenciales de Azure Active Directory. Los usuarios de Citrix Secure Hub que estén unidos a un dominio pueden usar Citrix Secure Hub para iniciar sesión con sus credenciales de Azure AD. Citrix Secure Hub utiliza la autenticación por certificado de cliente para los dispositivos MAM.

Secuencia de autenticación en Citrix Secure Hub

Citrix Endpoint Management sigue este 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 transfiere la solicitud de autenticación a Identidad de Citrix, que a su vez la transfiere a Azure Active Directory.

3. El usuario escribe su nombre de usuario y su contraseña de Azure Active Directory.
4. Azure Active Directory valida al usuario y envía un código a Identidad de Citrix.
5. Identidad de Citrix envía el código a Citrix Secure Hub, que a su vez lo envía a Citrix Endpoint Management.
6. Citrix Endpoint Management obtiene un token de identificación mediante el código y el secreto, y, a continuación, valida la información del usuario que está en el token de identificación. Citrix Endpoint Management devuelve un ID de sesión.

Autenticación con Azure Active Directory a través de NetScaler Gateway para la inscripción de MAM

March 1, 2024

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

Si debe configurar Citrix Endpoint Management para que use 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 proveedor de identidades para los dispositivos inscritos en MDM. Para ver más información sobre la configuración de 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 funciones relevantes en función de la plataforma correspondiente:
 - iOS:
 - * iOS-V3Form-MAM
 - * iOS-SAMLAuth-MAM
 - Android:
 - * Android-V3Form-MAM
 - * Android-SAMLAuth-MAM

Nota:

Para habilitar la marca de función relevante en su entorno, rellene el [formulario de Podio](#).

- Para Android, habilite **Android Enterprise**.

Nota:

Esta función no se ha probado ni verificado en el modo antiguo de Administrador de dispositivos (DA) de Android. Este modo no es compatible.

Configurar Azure AD para MAM como proveedor de identidades

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**.

Settings > Citrix Gateway

Citrix Gateway

When you configure Citrix Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use Citrix Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication ☒

Deliver user certificate for authentication ☐

Credential provider Cred

Save

Add

<input type="checkbox"/>	Name	Default	External URL	Logon Type	numeral of Callback URLs	Resource Location
<input type="checkbox"/>	ag	✓	https://net-nag1-wsccs.cloud.gtm	Identity provider(Preview)	0	

- d) Asegúrese de que el **tipo de inicio de sesión** de la puerta de enlace sea *Proveedor de identidades*.
 - e) Haga clic en **Guardar**.
2. Configure Azure AD como proveedor de identidades de SAML mediante [Configurar Azure AD como proveedor de identidades de SAML](#).
 3. Configure NetScaler ADC como proveedor de servicios de SAML con la directiva avanzada mediante [Configurar NetScaler ADC como proveedor de servicios \(SP\) de SAML](#).

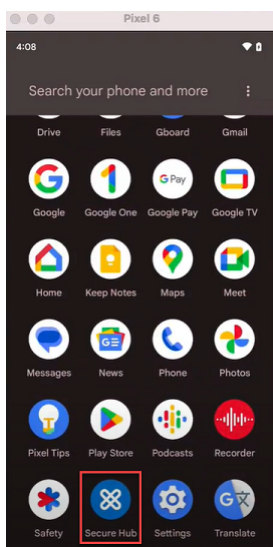
4. Cree un servidor virtual AAA con [Para configurar un servidor virtual de autenticación mediante la GUI](#).
5. Configure el servidor virtual AAA mediante [Configurar el servidor virtual de autenticación](#).
6. Cree y configure el perfil de autenticación mediante [Perfiles de autenticación](#).
7. Enlace el perfil de autenticación con el servidor virtual de Gateway y guarde todas las configuraciones.

Azure AD ahora se incluye como proveedor de identidades para los dispositivos inscritos en MAM, de modo que puede autenticarlos con Azure AD.

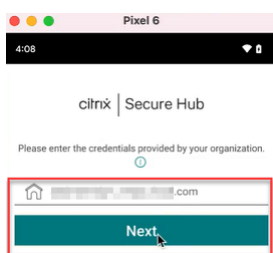
Comportamiento esperado

En el siguiente ejemplo se usa un dispositivo Android:

1. En su dispositivo móvil, abra la aplicación Citrix Secure Hub.

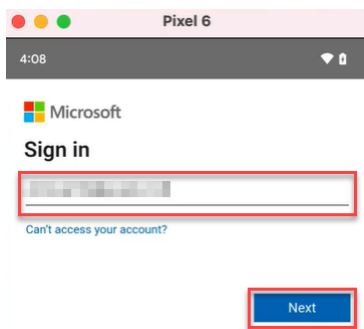


2. Proporcione los permisos requeridos.
3. En la página de inicio de sesión, introduzca las credenciales proporcionadas por su organización y, a continuación, pulse **Siguiente**.

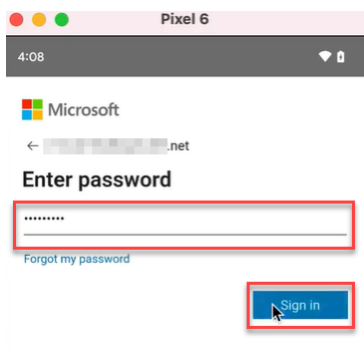


Se le redirigirá a la página de inicio de sesión de Microsoft.

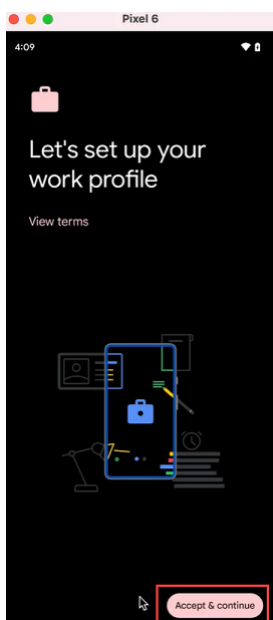
4. En la página de inicio de sesión de Microsoft, introduzca su ID de correo electrónico y, a continuación, pulse **Siguiente**.



5. Introduzca la contraseña y después toque **Iniciar sesión**.



6. En la página **Configuremos su perfil de trabajo**, toque **Aceptar y continuar**.



7. Cree el PIN de la aplicación Citrix Secure Hub y confírmelo.



Se le redirigirá correctamente a la página de inicio de Citrix Secure Hub.

Autenticación con Okta a través de Citrix Cloud

March 1, 2024

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 utilizar Citrix Secure Hub con MDM+MAM, configure Citrix Endpoint Management de modo que se pueda usar NetScaler Gateway para la inscripción de MAM. Para obtener más información, consulte [NetScaler Gateway y Citrix Endpoint Management](#).

Citrix Endpoint Management utiliza el servicio de Citrix Cloud, identidad de Citrix, para la federación con Okta. Citrix recomienda usar el proveedor de identidades Citrix, en lugar de una conexión directa a Okta.

Citrix Endpoint Management admite la autenticación con Okta en las siguientes plataformas:

- Dispositivos iOS y macOS que no estén inscritos en Apple Business Manager o Apple School Manager
- Dispositivos iOS y macOS inscritos en Apple Business Manager
- Dispositivos Android Enterprise (Tech Preview) para el modo BYOD y el modo totalmente administrado

La autenticación con Okta a través de Citrix Cloud tiene las siguientes limitaciones:

- No está disponible para cuentas locales de Citrix Endpoint Management.
- No admite la autenticación a través de Okta para invitaciones de inscripción. Si envía una invitación de inscripción a los usuarios y esa invitación contiene una URL de inscripción, los usuarios deberán autenticarse a través de LDAP, en lugar de Okta.

Requisitos previos

- Credenciales de usuario de Okta
- Los grupos de usuarios de Active Directory deben coincidir con los grupos de usuarios de Okta.
- Los nombres de usuario y las direcciones de correo electrónico de Active Directory deben coincidir con los de Okta.
- Cuenta de Citrix Cloud, con Citrix Cloud Connector instalado para la sincronización de servicios de directorio
- NetScaler Gateway. Citrix recomienda habilitar la autenticación basada en certificados para ofrecer Single Sign-On de manera integral. Si utiliza la autenticación LDAP en NetScaler Gateway para la inscripción MAM, los usuarios finales ven un mensaje de autenticación doble durante la inscripción. Para obtener más información, consulte [Autenticación con certificado de cliente o certificado y dominio](#).
- En los perfiles de inscripción para Android Enterprise, **desactive** la opción **Permitir a los usuarios rechazar la administración de dispositivos**. Si los usuarios rechazan la administración de dispositivos, no pueden inscribirse con un proveedor de identidades para autenticarse. Para obtener más información, consulte [Seguridad de la inscripción](#).

Configurar Citrix Cloud para que use Okta como proveedor de identidades

Para configurar el Okta en Citrix Cloud, consulte [Conectar Okta como proveedor de identidades con Citrix Cloud](#).

Configurar Identidad de Citrix como tipo de IDP para Citrix Endpoint Management

Esta configuración solo se aplica 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 esta manera:

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Proveedor de identidades (IDP)** y, a continuación, haga clic en **Agregar**.
2. En la página **Proveedor de identidades (IDP)**, configure lo siguiente:

Settings > Identity Provider (IDP) > Add IDP

Identity Provider (IDP)	Discovery URL
1 Discovery URL	Set up a connection to your identity provider (IDP).
2 IDP Claims Usage	
3 Summary	IDP Configuration

IDP Name *

IDP Type *

Auth Domain *

- **Nombre de IDP:** Escriba un nombre único para la conexión del proveedor de identidades que va a crear.
- **Tipo de proveedor de identidades:** Elija **Proveedor de identidades Citrix**.
- **Dominio de autenticación:** Seleccione el dominio de Citrix Cloud. Si aún no sabe cuál elegir, puede consultar su dominio en la página **Administración de acceso e identidad > Autenticación** de Citrix Cloud.

3. Haga clic en **Siguiente**. En la página **Uso de notificaciones IDP**, configure lo siguiente:

The screenshot shows the 'Add IDP' configuration page. On the left, there is a sidebar with a list of steps: '1 Discovery URL', '2 IDP Claims Usage' (which is highlighted), and '3 Summary'. The main content area is titled 'IDP Claims Usage' and includes the instruction 'Choose the type of user identifier that IDP is providing.' Below this, there is an information icon and a note: 'Endpoint Management uses the User Identifier string to retrieve the user information from the jwt token provided by Citrix Identity Provider.' At the bottom, there are two fields: 'User Identifier type' with a dropdown menu showing 'userPrincipalName', and 'User Identifier string' with a text input field containing '\$(id_token).ctx_user.upn'.

- **Tipo de identificador de usuario:** Este campo se establece como **userPrincipalName**. Asegúrese de configurar todos los usuarios con el mismo identificador en Active Directory local y en Okta. Citrix Endpoint Management utiliza este identificador para asignar usuarios del proveedor de identidades con usuarios de Active Directory local.
- **Cadena de identificador del usuario:** Este campo se rellena automáticamente.

Una vez finalizada esta configuración, los usuarios de Citrix Secure Hub que estén unidos a un dominio pueden usar Citrix Secure Hub para iniciar sesión con sus credenciales de Okta. Citrix Secure Hub utiliza la autenticación por certificado de cliente para los dispositivos MAM.

Secuencia de autenticación en Citrix Secure Hub

Citrix Endpoint Management sigue este 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 transfiere la solicitud de autenticación a Identidad de Citrix, que a su vez la transfiere a Okta.
3. El usuario escribe su nombre de usuario y contraseña.
4. Okta valida al usuario y envía un código a Identidad de Citrix.
5. Identidad de Citrix envía el código a Citrix Secure Hub, que a su vez lo envía a Citrix Endpoint Management.
6. Citrix Endpoint Management obtiene un token de identificación mediante el código y el secreto, y, a continuación, valida la información del usuario que está en el token de identificación. Citrix Endpoint Management devuelve un ID de sesión.

Autenticación con Okta a través de NetScaler Gateway para la inscripción de MAM

March 1, 2024

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

Si debe configurar Citrix Endpoint Management para que use Okta 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 Okta a través de Citrix Cloud como IdP para los dispositivos inscritos en 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 en función de la plataforma correspondiente:
 - iOS:
 - ★ iOS-V3Form-MAM
 - ★ iOS-SAMLAuth-MAM
 - Android:
 - ★ Android-V3Form-MAM
 - ★ Android-SAMLAuth-MAM

Nota:

Para habilitar la marca de función relevante en su entorno, rellene el [formulario de Podio](#).

- Descargue e instale la versión más reciente de Citrix Secure Hub.
- Asegúrese de que el servicio de Okta esté disponible para su organización y de que los usuarios y grupos pertinentes 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**.

Settings > Citrix Gateway

Citrix Gateway

When you configure Citrix Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use Citrix Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication ☒

Deliver user certificate for authentication ☐

Credential provider Cred

Save

Add

<input type="checkbox"/>	Name	Default	External URL	Logon Type	numeral of Callback URLs	Resource Location
<input type="checkbox"/>	ag	<input checked="" type="checkbox"/>	https://test-nsgp.xmga.cloud.com	Identity provider(Preview)	0	

4. Asegúrese de que el **tipo de inicio de sesión** de la puerta de enlace sea *Proveedor de identidades*.
5. Haga clic en **Guardar**.

Preparar NetScaler Gateway local

1. Si no tiene un dispositivo NetScaler Gateway local configurado para Citrix Endpoint Management, lleve a cabo los siguientes 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 **Edit**.
 - d) Haga clic en el menú desplegable **Tipo de inicio de sesión** y seleccione *Solo dominio*.

Endpoint Management Analyze Manage Configure

Settings > Citrix Gateway > Add New Citrix Gateway (on-premises)

Add New Citrix Gateway (on-premises)

Name

Alias

External URL .com

Logon Type Domain only

Password Required ☒

Set as Default ☒

Export Configuration Script

e) Haga clic en **Exportar script de configuración**.

The screenshot shows the 'Add New Citrix Gateway (on-premises)' configuration page in the Citrix Endpoint Management console. The page has a dark blue header with navigation tabs: 'Endpoint Management', 'Analyze', 'Manage', and 'Configure'. The user is logged in as 'Administrator'. The breadcrumb trail is 'Settings > Citrix Gateway > Add New Citrix Gateway (on-premises)'. The form contains the following fields and controls:

- Name ***: Text input with 'gateway' entered.
- Alias**: Empty text input.
- External URL ***: Text input with 'https://gateway_url.com' entered.
- Logon Type**: Dropdown menu set to 'Domain only'.
- Password Required**: Toggle switch turned on.
- Set as Default**: Toggle switch turned on.
- Export Configuration Script**: A button with a question mark icon, highlighted with a red box.
- Callback URL ***: Empty text input.
- Virtual IP ***: Empty text input.
- Add**: A button with a plus icon.
- Cancel** and **Save** buttons are at the bottom right.

El **script de configuración de exportación** se descargó.

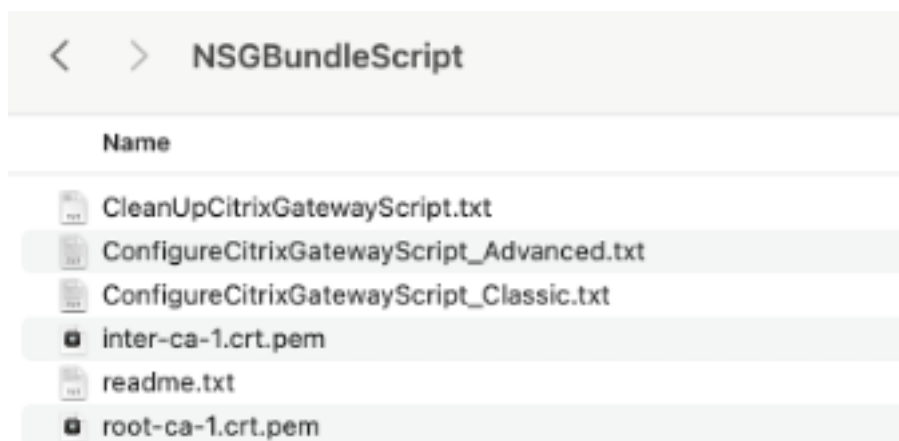
f) Haga clic en el menú desplegable **Tipo de inicio de sesión** y seleccione *Proveedor de identidades*.

This screenshot shows the same configuration page as before, but with the 'Logon Type' dropdown menu open and highlighted with a red box. The selected option is 'Identity provider(Preview)'. The other fields remain the same as in the previous screenshot.

g) Haga clic en **Guardar**.

h) Abra el archivo zip descargado y extraiga los archivos que incluye.

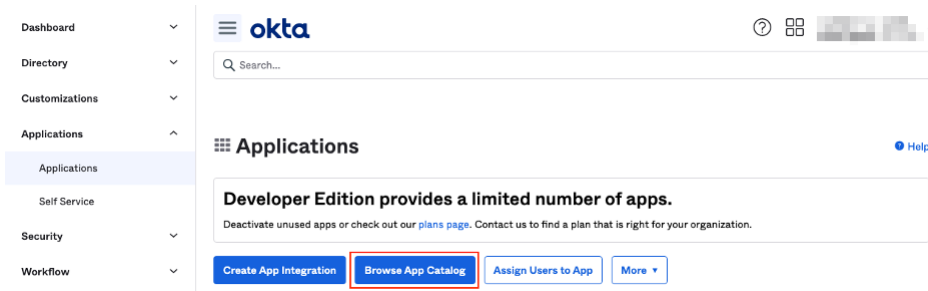
i) Ejecute los scripts en los archivos .txt extraídos para preparar el dispositivo NetScaler Gateway local.



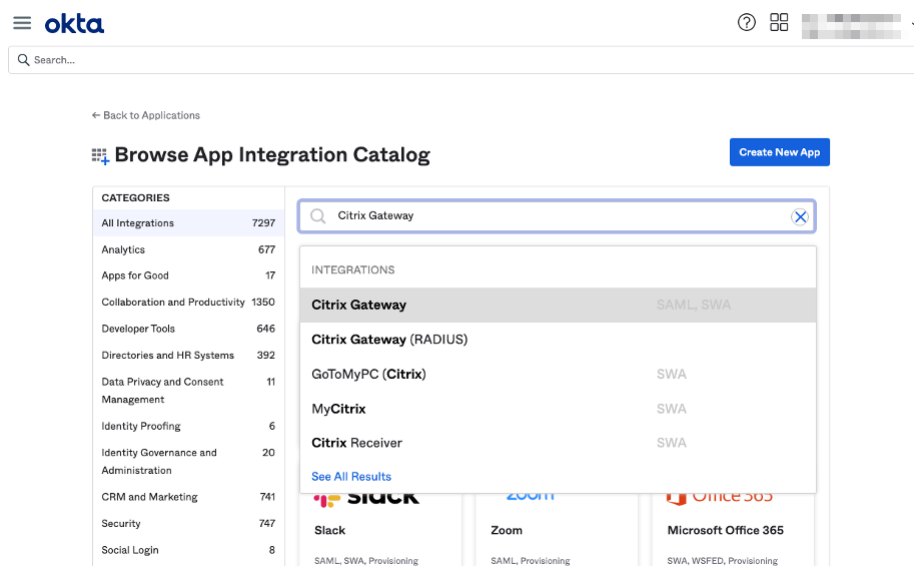
2. Inicie sesión en la consola de administración de Citrix ADC y, a continuación, vaya a **NetScaler Gateway > Servidores virtuales**.
3. Haga clic en la puerta de enlace correspondiente a su configuración de Citrix Endpoint Management.
4. Desvincule cualquier directiva de autenticación que haya en el dispositivo NetScaler Gateway local.

Configurar Okta

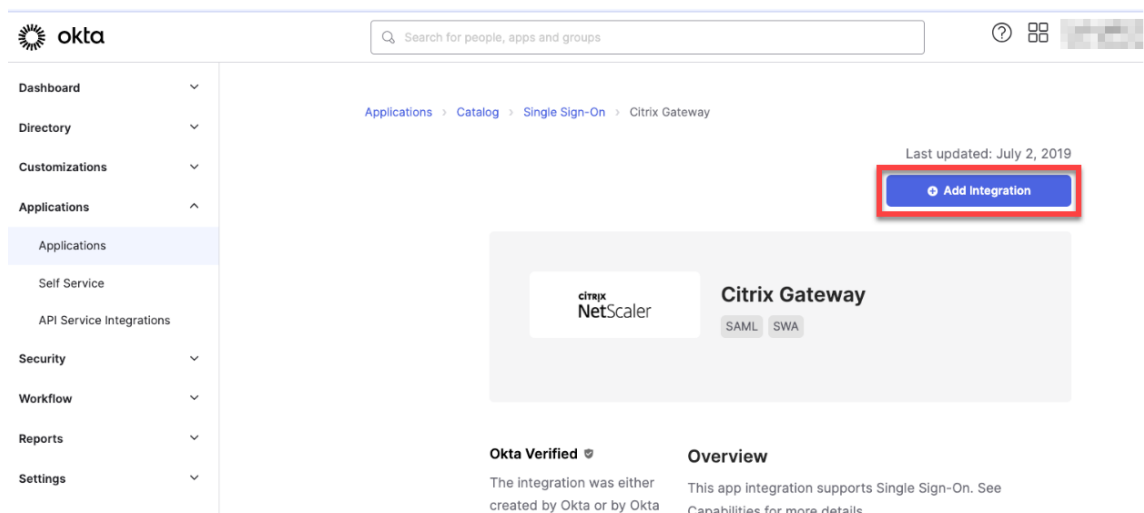
1. Inicie sesión en Okta como administrador.
2. Haga clic en **Applications > Applications > Browse App Catalog**.



3. Escriba **NetScaler Gateway** en la barra de búsqueda de **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 **URL de inicio de sesión** y, a continuación, haga clic en **Siguiente**.

Okta Search for people, apps and groups

Add Citrix Gateway

1 General Settings 2 Sign-On Options

General settings - Required

Application label: Citrix Gateway
This label displays under the app on your home page

Login URL: https://your-gateway-url
For SWA authentication, please enter your full login URL. E.g.: https://subdomain.acme.com/vpn/index.html or https://subdomain.acme.com/.../Login.do
If your login page requires a double passcode or token, user passwords should be entered in the following format: password:passcode (password will always be followed by a '#' and then the passcode or token value).
For SAML authentication, please enter your base URL. E.g.: https://subdomain.acme.com

Application Visibility: ☐ Do not display application icon to users
☐ Do not display application icon in the Okta Mobile App

Browser plugin auto-submit: ☒ Automatically log in when user lands on login page

Cancel Next

General settings
All fields are required to add this application unless marked optional.

Nota:

La URL introducida en el campo **URL de inicio de sesión** 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 **SAML2.0**.

Okta Search for people, apps and groups

Add Citrix Gateway

1 General Settings 2 Sign-On Options

Sign-On Options - Required

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application. Application username is determined by the user profile mapping. [Configure profile mapping](#)

☐ Secure Web Authentication

☒ SAML 2.0

Default Relay State:
All IDP-initiated requests will include this RelayState.

Attributes (Optional) [Learn More](#)

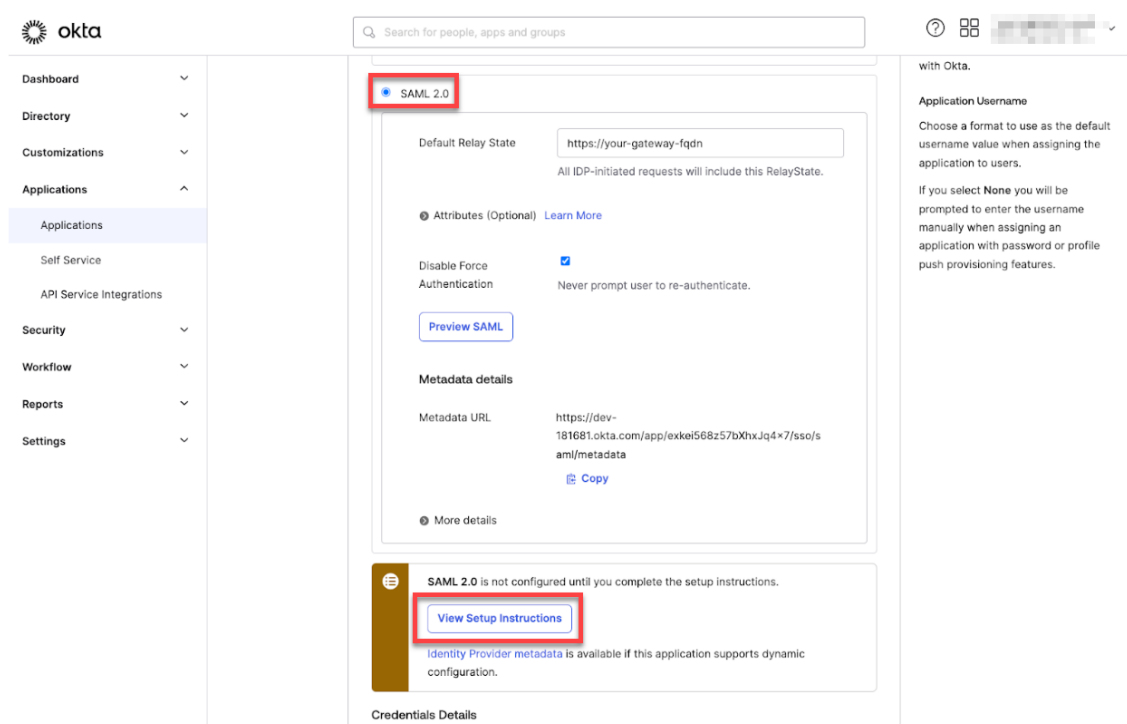
Disable Force Authentication: ☒ Never prompt user to re-authenticate.

Preview SAML

About
SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username
Choose a format to use as the default username value when assigning the application to users.
If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

8. Haga clic en **Ver instrucciones de instalación** y siga las instrucciones que se proporcionan en la página para crear la directiva de SAML en la consola de administración de Citrix Gateway local.



Nota:

- Después de instalar el certificado de CA al configurar las versiones 11.1 o posteriores de Netscaler Gateway, cree una acción de SAML. Para crear una acción de SAML, vaya a **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Actions > SAML Actions**. Haga clic en **Add** y rellene la información que se indica en la página anterior. No siga la navegación que se indica en la página, es decir, **Netscaler Gateway > Policies > Authentication > SAML > Servers**.
- Además, no siga los pasos especificados para crear una directiva de SAML, ya que en esos pasos se usa la directiva clásica. Ahora usamos la directiva avanzada. Siga el paso 9 para crear una directiva de SAML mediante una directiva avanzada.

9. Cree una directiva de SAML correspondiente para la acción de SAML y enlace la directiva al servidor virtual de autenticación de la siguiente manera:

- Vaya a **Security > AAA-Application Traffic > Policies > Authentication > Advanced Policies** y haga clic en **Add**.
- En la página **Crear directiva de autenticación**, proporcione los siguientes detalles:
 - **Nombre:** especifique un nombre de la directiva de SAML.
 - **Tipo de acción:** seleccione **SAML** como el tipo de acción de autenticación.
 - **Acción:** seleccione el perfil del servidor SAML con el que enlazar la directiva de SAML.
 - **Expresión:** muestra el nombre de la regla la expresión que utiliza la directiva de SAML para determinar si el usuario debe autenticarse en el servidor SAML. En el cuadro de

texto, establezca el valor **rule** = **true** para que la directiva de SAML entre en vigor y se ejecute la acción de SAML correspondiente.

- c) Enlace la directiva de 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 enlace, consulte [Enlazar la directiva de autenticación](#).
10. Cree un servidor virtual AAA con [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. Enlace el perfil de autenticación con el servidor virtual de Gateway y guarde todas las configuraciones.
14. Tras crear la directiva de SAML en la consola de administración de Citrix Gateway local, haga clic en Listo.

Ahora, podrá 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.

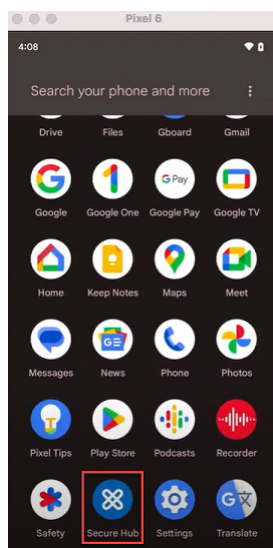
15. Asigne los usuarios y los grupos pertinentes a la aplicación SAML que acaba de crear.

Okta ahora se incluye como proveedor de identidades para los dispositivos inscritos en MAM y puede usar Okta para autenticarlos.

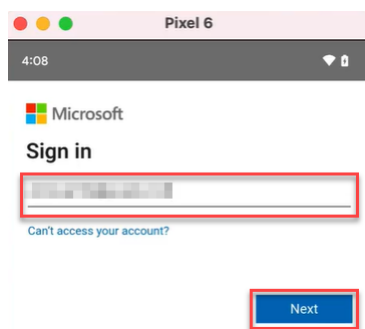
Comportamiento esperado

En el siguiente ejemplo se usa un dispositivo Android:

1. En su dispositivo móvil, abra la aplicación Citrix Secure Hub.

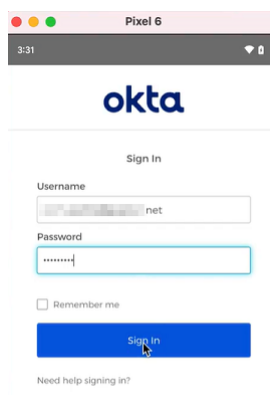


2. Proporcione los permisos requeridos.
3. En la página de inicio de sesión, introduzca las credenciales proporcionadas por su organización y, a continuación, pulse **Siguiente**.

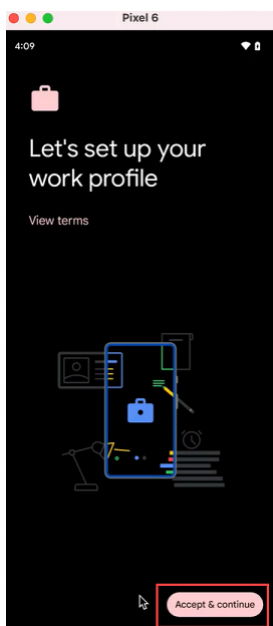


Se le redirigirá a la página de inicio de sesión de Okta.

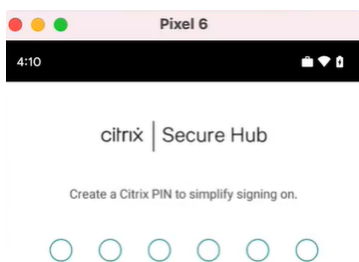
4. En la página de inicio de sesión de Okta, introduzca sus credenciales y, a continuación, pulse **Iniciar sesión**.



5. En la página **Configuremos su perfil de trabajo**, toque **Aceptar y continuar**.



6. Cree el PIN de la aplicación Citrix Secure Hub y confírmelo.



Se le redirigirá correctamente a la página de inicio de Citrix Secure Hub.

Autenticación con un dispositivo NetScaler Gateway local a través de Citrix Cloud

March 1, 2024

Citrix Endpoint Management permite la autenticación con dispositivos NetScaler Gateway locales 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 mediante credenciales de dispositivos NetScaler Gateway locales a través de Citrix Cloud. Para utilizar Citrix Secure Hub con MDM+MAM, configure Citrix Endpoint Management de modo que se pueda usar NetScaler Gateway para la inscripción.

ción de MAM. Para obtener más información, consulte [NetScaler Gateway y Citrix Endpoint Management](#).

Citrix Endpoint Management permite la autenticación con dispositivos NetScaler Gateway locales a través de Citrix Cloud para estas plataformas:

- Dispositivos iOS
- Dispositivos Android Enterprise para el modo BYOD y el modo 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 y esa invitación contiene una URL de inscripción, los usuarios deberán autenticarse a través de LDAP, en lugar de un NetScaler Gateway local como proveedor de identidades.

Citrix recomienda habilitar la autenticación basada en certificados para ofrecer Single Sign-On de manera integral. Si utiliza la autenticación LDAP en NetScaler Gateway para la inscripción MAM, los usuarios finales ven un mensaje de autenticación doble durante la inscripción. Para obtener más información, consulte [Autenticación con certificado de cliente o certificado y dominio](#).

Requisitos previos

- NetScaler Gateway. Citrix recomienda habilitar la autenticación basada en certificados para ofrecer Single Sign-On de manera integral. Si utiliza la autenticación LDAP en NetScaler Gateway para la inscripción MAM, los usuarios finales ven un mensaje de autenticación doble durante la inscripción. Para obtener más información, consulte [Autenticación con certificado de cliente o certificado y dominio](#).
- Cuenta de Citrix Cloud con Citrix Cloud Connector instalado para la sincronización de servicios de directorio.
- Citrix Secure Hub 20.5.0 y versiones posteriores.

Configurar Citrix Cloud para que use NetScaler Gateway como proveedor de identidades

Para configurar la autenticación de NetScaler Gateway en Citrix Cloud, consulte [Conectar un dispositivo NetScaler Gateway local como proveedor de identidades con Citrix Cloud](#).

Configurar el proveedor de identidades Citrix como tipo de IDP para Citrix Endpoint Management

Esta configuración solo se aplica 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 esta manera.

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > 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 del proveedor de identidades que creará.
 - **Tipo de proveedor de identidades:** Elija **Proveedor de identidades Citrix**.
 - **Dominio de autenticación:** Elija **NetScaler Gateway**. Este dominio corresponde al dominio del proveedor de identidades de la página de Citrix Cloud **Configuración de Workspace > Autenticación**.
3. Haga clic en **Siguiente**. En la página **Uso de notificaciones IDP**, configure lo siguiente:
 - **Tipo de identificador de usuario:** De forma predeterminada, este campo se establece como **userPrincipalName**.
 - **Cadena de identificador del usuario:** Este campo se rellena automáticamente.
4. Haga clic en **Siguiente**, revise la información de la página **Resumen** y, a continuación, haga clic en **Guardar**.

Ahora puede inscribir dispositivos de usuario a través de Citrix Secure Hub mediante un dispositivo NetScaler Gateway local como proveedor de identidades.

Secuencia de autenticación en Citrix Secure Hub

Citrix Endpoint Management sigue este flujo para autenticar a los usuarios con un dispositivo NetScaler Gateway local como proveedor de identidades en dispositivos inscritos a través de Citrix Secure Hub:

1. Un usuario inicia Citrix Secure Hub.
2. Citrix Secure Hub transfiere la solicitud de autenticación a Identidad de Citrix, que a su vez la transfiere a un dispositivo NetScaler Gateway local.
3. El usuario escribe su nombre de usuario y contraseña.
4. Un dispositivo NetScaler Gateway local valida al usuario y envía un código a Identidad de Citrix.
5. Identidad de Citrix envía el código a Citrix Secure Hub, que a su vez lo envía a Citrix Endpoint Management.

6. Citrix Endpoint Management obtiene un token de identificación mediante el código y el secreto, y, a continuación, valida la información del usuario que está en el token de identificación. Citrix Endpoint Management devuelve un ID de sesión.

Autenticación nFactor

March 1, 2024

La autenticación nFactor le permite usar todos los modos de autenticación actualmente posibles con NetScaler cuando usa Citrix Secure Hub. Mejora la seguridad de las aplicaciones porque requiere que los usuarios proporcionen varias 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 sobre cómo configurarlos, consulte [Autenticación y autorización](#).

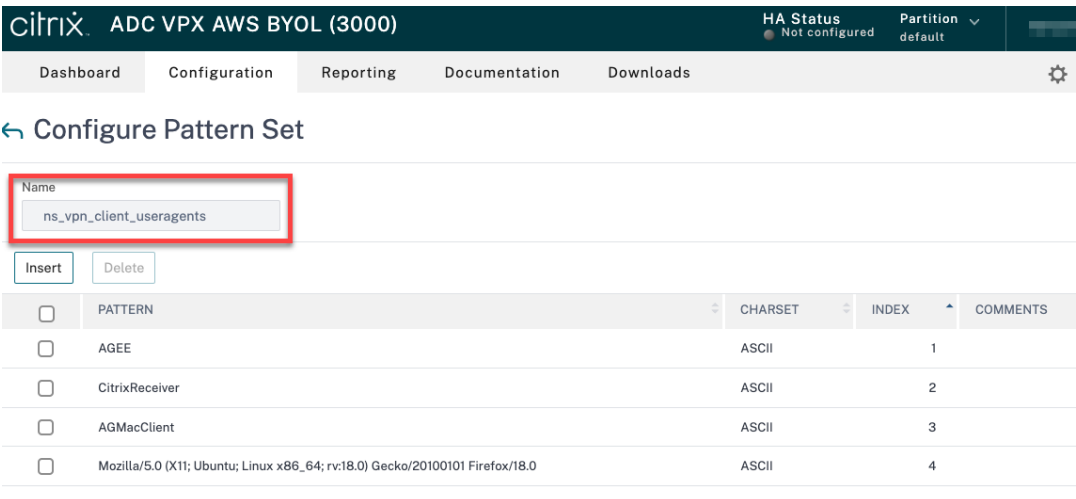
Citrix Endpoint Management admite estos tipos de autenticación con la autenticación nFactor:

- Locales
- Protocolo ligero de acceso a directorios (LDAP)
- RADIUS
- SAML
- Autenticación de certificados de cliente

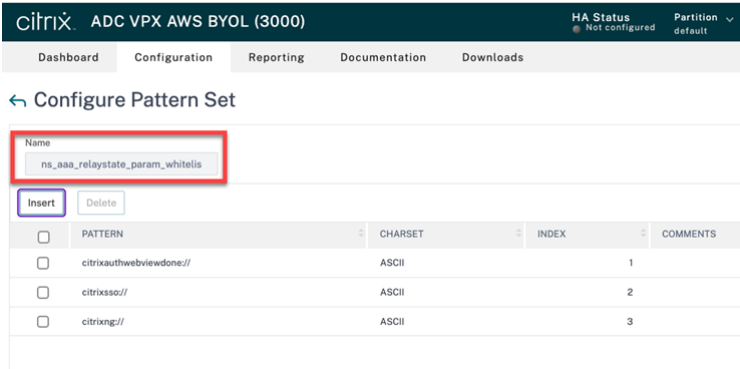
Requisitos previos

Para configurar Citrix Endpoint Management para que utilice la autenticación nFactor, asegúrese de que se cumplen estos requisitos previos:

- Asegúrese de utilizar NetScaler 13.0 o una versión posterior.
- Asegúrese de haber configurado estos parámetros de los conjuntos de patrones en NetScaler para sus dispositivos Android e iOS:
 - Ns_vpn_client_useragents



- Ns_aaa_relaystate_param_whitelist



- Asegúrese de haber instalado la versión más reciente de Citrix Secure Hub desde Apple o Google Play.
- Asegúrese de utilizar la directiva de autenticación avanzada en NetScaler Gateway.
- Asegúrese de establecer la propiedad de cliente **ENABLE_MAM_NFACTOR_SSO** en **True** tanto para las instancias locales como para las de la nube. Para obtener más información sobre la propiedad **ENABLE_MAM_NFACTOR_SSO**, consulte [Referencia de propiedades de cliente](#).

Nota:

Si la propiedad del cliente **Habilitar SSO nFactor** es **False**, debe asegurarse de que las directivas de autenticación clásicas estén enlazadas a NetScaler Gateway.

Configurar la autenticación nFactor

Configure la autenticación nFactor de esta manera para Citrix Endpoint Management en función de cómo esté configurado su NetScaler Gateway:

- 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 [Definir 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 estos 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 [Convertir expresiones de directiva mediante la herramienta NSPEPI](#).

Definir la configuración de NetScaler Gateway mediante la directiva avanzada

Para configurar la autenticación nFactor para Citrix Endpoint Management en NetScaler Gateway mediante la directiva de autenticación avanzada, consulte [Configurar la autenticación nFactor](#).

Nota:

- Puede elegir el tipo de autenticación correspondiente entre los tipos de autenticación compatibles.
- Si utiliza el tipo de autenticación SAML, puede configurar SAML mediante MAM IDP mediante uno de estos métodos:
 - Para configurar el uso de Azure Active Directory, consulte [Autenticación con Azure Active Directory a través de NetScaler Gateway para la inscripción de MAM](#).
 - Para configurar el uso de Okta, consulte [Autenticación con Okta a través de NetScaler Gateway para la inscripción de MAM](#).

Inscripción, roles y cuentas de usuario

March 1, 2024

Las tareas de configuración de usuarios se realizan en la consola de Citrix Endpoint Management, desde la ficha **Administrar** y la página **Parámetros**. A menos que se indique lo contrario, los pasos para las siguientes tareas se proporcionan en este artículo.

- Invitaciones y modo de seguridad de inscripción
 - Haga clic en **Parámetros > Inscripción** para configurar hasta siete modos de seguridad de inscripción y enviar invitaciones de inscripción. Cada modo de seguridad de inscripción tiene su propio nivel de seguridad y una serie de pasos que los usuarios deberán seguir para inscribir sus dispositivos.
- Roles para cuentas de usuario y grupos
 - En **Parámetros > Control de acceso por roles** puede asignar roles predefinidos o conjuntos de permisos a usuarios y grupos. Con estos permisos, se puede controlar el nivel de acceso de los usuarios a las funciones del sistema. Para obtener información, consulte [Configurar roles con RBAC](#).
 - En **Parámetros > Plantillas de notificaciones** puede crear o actualizar plantillas de notificaciones que se van a usar en acciones automatizadas, inscripciones y el envío de mensajes de notificación estándar a los usuarios. Puede configurar plantillas de notificaciones para enviar mensajes a través de dos canales diferentes: Citrix Secure Hub o SMTP. Para ver más información: [Creación y actualización de plantillas de notificaciones](#).
- Cuentas de usuario y grupos:
 - En **Administrar > Usuarios**, puede agregar cuentas de usuario manualmente, o puede usar un archivo CSV de aprovisionamiento para importar cuentas y administrar grupos locales. Sin embargo, la mayoría de las implementaciones de Citrix Endpoint Management se conectan a LDAP para obtener información sobre usuarios y grupos. Es posible que prefiera crear cuentas de usuario localmente en casos de uso como los siguientes:
 - ★ En entornos, como el comercio, donde los dispositivos se comparten, en lugar de dedicarse a usuarios individuales.
 - ★ Si utiliza un directorio no compatible, como Novell eDirectory.
 - En **Parámetros > Flujos de trabajo**, puede utilizar flujos de trabajo para administrar la creación y la eliminación de cuentas de usuario.

Acerca de las cuentas de usuario

Una cuenta de usuario de Citrix Endpoint Management es para un usuario local, Active Directory o un usuario 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. En una cuenta de usuario de nube, se utiliza el mismo nombre de usuario que en la cuenta de administrador de Citrix Cloud y tiene el rol de administrador de forma predeterminada. La cuenta del usuario de nube ofrece el inicio Single Sign-On y lleva a cabo otras funciones administrativas.

Para agregar administradores a una cuenta de Citrix Cloud, consulte [Invitar a nuevos administradores](#).

Cuando se trata de usuarios de nube:

- Puede cambiar los roles y las propiedades de los usuarios de la nube desde 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 acceso e identidad > Administradores**. Haga clic en los puntos suspensivos que hay al final de la fila del usuario y seleccione **Eliminar administrador**.
- No puede agregar usuarios de la nube a un grupo local.

Configurar modos de seguridad de inscripción

Los modos de seguridad de inscripción de dispositivos se configuran para especificar un nivel de seguridad y una plantilla de notificación para la inscripción de los dispositivos en Citrix Endpoint Management.

Citrix Endpoint Management ofrece seis modos de seguridad de inscripción, cada uno con su propio nivel de seguridad y unos pasos propios que los usuarios deberán 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 información, consulte [Invitaciones de inscripción](#).

Nota:

Si va a utilizar plantillas de notificaciones personalizadas, debe definir esas plantillas antes de configurar los modos de seguridad para la inscripción. Para obtener más información acerca de las plantillas de notificaciones, consulte [Crear o actualizar plantillas de notificaciones](#).

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Parámetros**.

- Haga clic en **Inscripción**. Aparecerá la página **Enrollment**. Cuenta con una tabla de todos los modos de seguridad de inscripción disponibles. De manera predeterminada, están habilitados todos los modos de seguridad de inscripción.
- Seleccione un modo de seguridad de inscripción de la lista para modificarlo. A continuación, configure el modo como predeterminado o inhabílitelo.

Marque la casilla situada junto a un modo de seguridad de inscripción para ver el menú de opciones. También puede hacer clic en cualquier lugar de la lista para ver el menú de opciones a la derecha de la lista.

Consejo:

Al modificar 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 modificar un modo de seguridad de inscripción](#) en este artículo. El valor aparece en las páginas de configuración de invitaciones a la inscripción de usuarios y grupos.

Settings > Enrollment

Enrollment
Enable and disable enrollment modes for users. You can also enable the Self Help Portal to allow users to generate enrollment links that let them download Secure Hub and enroll their devices, or to send themselves an enrollment invitation.

<input type="checkbox"/>	Name	Enabled	Default	Self Help Portal	Expire after	Attempts	PIN length	PIN type	Templates	▼
<input type="checkbox"/>	User name + Password	✓	✓							
<input type="checkbox"/>	High Security	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL	✓			1 day(s)					
<input type="checkbox"/>	Invitation URL + PIN	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL + Password	✓			1 day(s)	3				
<input type="checkbox"/>	Two Factor	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	User name + PIN	✓			1 day(s)	3	8	numeric		

Showing 1 - 7 of 7 items

Dispone de las siguientes opciones de modo de seguridad de inscripción, en función de la plataforma:

- Nombre de usuario y contraseña
- URL de invitación
- URL de invitación y PIN

- URL de invitación y contraseña
- Dos factores
- Nombre de usuario + PIN

Para obtener información sobre los modos de seguridad de inscripción específicos de cada plataforma, consulte [Modos de seguridad de inscripción por plataforma](#).

Puede utilizar las invitaciones de inscripción como una forma eficaz de restringir la capacidad de inscripción a usuarios o grupos específicos. Para enviar invitaciones de inscripción, puede utilizar solamente 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 utilizar invitaciones de inscripción con PIN de un solo uso (a veces llamados OTP) como una solución para la autenticación de dos factores. Con las invitaciones de inscripción con PIN de un solo uso, puede controlar la cantidad de dispositivos que un usuario puede inscribir. Las invitaciones de OTP no están disponibles para dispositivos Windows.

Para modificar un modo de seguridad de inscripción

1. En la lista **Inscripción**, seleccione un modo de seguridad de inscripción y, a continuación, haga clic en **Modificar**. Aparecerá la página **Modificar modo de inscripción**. Las opciones que verá dependerán del modo que seleccione.

The screenshot shows the 'Edit Enrollment Mode' configuration page. At the top, the breadcrumb trail is 'Settings > Enrollment > Edit Enrollment Mode'. The title 'Edit Enrollment Mode' is displayed. Below the title, the 'Name' field is set to 'High Security'. The 'Expire after*' field is set to '1' with a 'Days' dropdown menu and a help icon. The 'Maximum attempts*' field is set to '3' with a help icon. The 'PIN Length*' field is set to '8' with a 'Numeric' dropdown menu. Below these fields is a section titled 'Notification templates' which contains three dropdown menus: 'Template for enrollment URL', 'Template for Enrollment PIN', and 'Template for enrollment confirmation', all currently set to '-- SELECT ONE --'. At the bottom right, there are 'Cancel' and 'Save' buttons.

2. Cambie la siguiente información como corresponda:

- **Caduca después de:** Introduzca 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 invitaciones a la inscripción de usuarios y grupos.

Introduzca **0** para impedir que la invitación caduque.

- **Días:** En la lista desplegable, haga clic en **Días** o **Horas**, de acuerdo con la fecha límite de caducidad que ha introducido en **Caduca después de**.
- **Máximo de intentos:** Escriba la cantidad de intentos de inscripción que un usuario puede llevar a cabo antes de que se bloquee el proceso de inscripción. Este valor aparece en las páginas de configuración de invitaciones a la inscripción de usuarios y grupos.
Introduzca **0** para permitir una cantidad ilimitada de intentos.
- **Longitud del PIN:** Escriba un número para definir la longitud del PIN generado.
- **Numérico:** En la lista desplegable, haga clic en **Numérico** o **Alfanumérico** para el tipo de PIN.
- **Plantillas de notificaciones:**

- **Plantilla para URL de inscripción:** En la lista desplegable, seleccione una plantilla para la URL de inscripción. Por ejemplo, la plantilla de invitaciones de inscripción envía a los usuarios un correo electrónico. Para obtener más información acerca de las plantillas de notificaciones, consulte [Crear o actualizar plantillas de notificaciones](#).
- **Plantilla para PIN de inscripción:** En la lista desplegable, seleccione una plantilla para el PIN de inscripción.
- **Plantilla para confirmación de la inscripción:** En la lista desplegable, seleccione la plantilla a utilizar para informar al usuario de que la inscripción se ha realizado correctamente.

3. Haga clic en **Guardar**.

Para establecer un modo de seguridad de inscripción como predeterminado

El modo de seguridad de inscripción predeterminado se usa para todas las solicitudes de inscripción de dispositivos, a menos que se seleccione otro modo. Si no hay ningún modo de seguridad de inscripción establecido como predeterminado, debe crear una solicitud de inscripción para cada inscripción de dispositivo.

1. Si el modo de seguridad de inscripción que quiere utilizar 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 y contraseña**, **Dos factores** o **Nombre de usuario y PIN**.

2. Seleccione el modo de seguridad de inscripción y haga clic en **Predeterminado**. A partir de ahora, el modo seleccionado es el predeterminado. Si se había establecido otro modo de seguridad de inscripción como predeterminado, ese modo deja de serlo.

Para inhabilitar un modo de seguridad de inscripción

Al inhabilitar un modo de seguridad de inscripción, ese modo no se podrá usar ni para las invitaciones de grupo a las inscripciones ni en el portal Self Help Portal. Puede cambiar el modo de inscripción que se permite a los usuarios. Para ello, deberá inhabilitar un modo de seguridad de inscripción y habilitar otro.

1. Seleccione un modo de seguridad de inscripción.

El modo de seguridad de inscripción predeterminado no se puede inhabilitar. Si quiere inhabilitar el modo de seguridad de inscripción predeterminado, primero debe quitar su estado predeterminado.

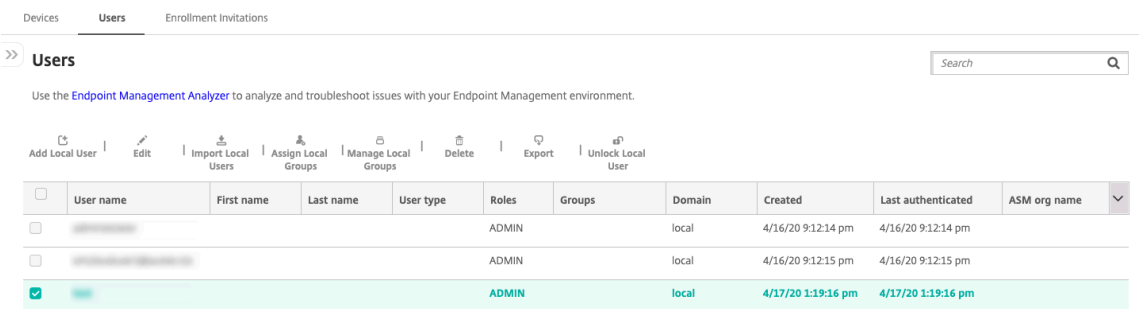
2. Haga clic en **Inhabilitar**. El modo de seguridad de inscripción deja de estar habilitado.

Agregar, modificar, desbloquear o eliminar cuentas de usuarios locales

Puede agregar cuentas de usuario local a Citrix Endpoint Management de forma manual, o bien 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 incluye Citrix Endpoint Management. Para ver 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**.



Users										
<input type="checkbox"/>	User name	First name	Last name	User type	Roles	Groups	Domain	Created	Last authenticated	ASM org name
<input type="checkbox"/>					ADMIN		local	4/16/20 9:12:14 pm	4/16/20 9:12:14 pm	
<input type="checkbox"/>					ADMIN		local	4/16/20 9:12:15 pm	4/16/20 9:12:15 pm	
<input checked="" type="checkbox"/>					ADMIN		local	4/17/20 1:19:16 pm	4/17/20 1:19:16 pm	

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**.

The screenshot shows the 'Add Local User' form within the 'Users' tab of the Citrix Endpoint Management console. The form includes the following fields and options:

- User name***: A text input field with the placeholder 'Enter user name'.
- Password**: A text input field with the placeholder 'Enter new password'.
- Role***: A dropdown menu currently set to 'ADMIN'.
- Membership**: A list of groups with checkboxes:
 - ☐ local\Device Enrollment Program Group
 - ☐ local\MSP
- Manage Groups**: A blue button located to the right of the membership list.
- Footer**: A bar containing a link to '- User Properties' and an 'Add' button.

2. Configure estos parámetros:

- **Nombre de usuario:** Este es un campo obligatorio. Escriba el nombre. Puede incluir lo siguiente en los nombres: espacios, letras mayúsculas y letras minúsculas.
- **Contraseña:** Escriba una contraseña opcional de usuario. La contraseña debe tener al menos 14 caracteres y debe satisfacer 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 incluir palabras de diccionario ni palabras restringidas, como el nombre de usuario de Citrix o la dirección de correo electrónico
 - No incluir más de tres caracteres o patrones de teclado secuenciales y repetidos, como 1111, 1234 o asdf
- **Rol:** En la lista desplegable, haga clic en el rol del usuario. Para obtener información sobre roles, consulte [Configurar roles con RBAC](#). Las opciones posibles son:

- ADMIN
- DEVICE_PROVISIONING
- SUPPORT
- USER

- **Pertenencia a grupos:** En la lista desplegable, haga clic en el grupo o en los grupos a los que agregar el usuario.
- **Propiedades de usuario:** Agregue propiedades de usuario opcionales. Para cada propiedad de usuario que quiera agregar, haga clic en **Agregar** y haga lo siguiente:
 - **Propiedades de usuario:** En la lista, haga clic en una propiedad y, a continuación, escriba el atributo de la propiedad de usuario en el campo que hay 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, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en la **X** situada a la derecha. La propiedad se elimina inmediatamente.

Para modificar una propiedad de usuario, haga clic en la propiedad y realice los cambios. Haga clic en **Listo** para guardar los cambios del elemento o haga clic en **Cancelar** para no guardarlos.

3. Haga clic en **Guardar**. Después de crear un usuario, el campo **Tipo de usuario** de una cuenta de usuario local permanece en blanco.

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**. Aparecerá la página **Modificar usuario local**.

The screenshot shows the 'Edit Local User' interface. At the top, there are three tabs: 'Devices', 'Users' (selected), and 'Enrollment Invitations'. Below the tabs, the title 'Edit Local User' is displayed. The form includes the following fields and controls:

- User name***: A text input field containing 'administrator'.
- Password**: A text input field with the placeholder text 'Enter new password'.
- Role***: A dropdown menu currently showing 'ADMIN'.
- Membership**: A list of groups with checkboxes. The visible groups are 'local\Device Enrollment Program Group' and 'local\MSP', both of which are currently unchecked.
- Manage Groups**: A blue button located to the right of the membership list.
- User Properties**: A section header at the bottom of the form.
- Add**: A button located at the bottom right of the form.

2. Cambie la siguiente información como corresponda:

- **Nombre de usuario:** No puede cambiar el nombre de usuario.
- **Contraseña:** Cambie o agregue una contraseña de usuario.
- **Rol:** En la lista desplegable, haga clic en el rol del usuario.
- **Pertenencia a grupos:** En la lista desplegable, haga clic en el grupo o en los grupos a los que agregar la cuenta de usuario o modificarla. Para quitar la cuenta de usuario de un grupo, quite la marca de la casilla situada junto al nombre del grupo.
- **Propiedades de usuario:** Realice una de las siguientes acciones:
 - Para cambiar cada propiedad de usuario, haga clic en ella y realice los cambios. Haga clic en **Listo** para guardar los cambios del elemento o haga clic en **Cancelar** para no guardarlos.
 - Para cada propiedad de usuario que quiera agregar, haga clic en **Agregar** y haga lo siguiente:
 - ★ **Propiedades de usuario:** En la lista, haga clic en una propiedad y, a continuación, escriba el atributo de la propiedad de usuario en el campo que hay junto a la propiedad.
 - ★ Haga clic en **Listo** para guardar la propiedad de usuario o haga clic en **Cancelar**.
 - Para cada propiedad de usuario que quiera eliminar, coloque el cursor sobre la línea que la contiene y, a continuación, haga clic en la **X** situada a la derecha. La propiedad se elimina inmediatamente.

3. Haga clic en **Guardar** para guardar los cambios o en **Cancelar** para no guardarlos.

Para desbloquear una cuenta de usuario local

Una cuenta de usuario local se bloquea de acuerdo con estas propiedades de servidor:

- `local.user.account.lockout.time`
- `local.user.account.lockout.limit`

Para obtener más información, consulte [Definiciones de las propiedades de servidor](#).

Cuando se bloquea una cuenta de usuario local, puede desbloquearla desde la consola de Citrix Endpoint Management.

1. En la página **Usuarios**, en la lista de cuentas de usuario, seleccione una cuenta.
2. Haga clic en **Desbloquear usuario**. Aparecerá un cuadro de diálogo de confirmación.
3. Haga clic en **Desbloquear** para desbloquear la cuenta de usuario o haga clic en **Cancelar** para no hacer ningún cambio.

No se pueden abrir usuarios 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, seleccione una cuenta.
Puede seleccionar varias cuentas de usuario para eliminarlas. Para ello, marque la casilla situada junto a cada cuenta de usuario que quiera seleccionar.
2. Haga clic en **Eliminar**. Aparecerá un cuadro de diálogo de confirmación.
3. Haga clic en **Eliminar** para eliminar la cuenta de usuario o en **Cancelar** para no eliminarla.

Para eliminar usuarios de Active Directory

Para eliminar uno o varios usuarios de Active Directory a la vez, selecciónelos y haga clic en **Eliminar**.

Si un usuario eliminado tiene dispositivos inscritos y usted quiere reinscribirlos, elimine los dispositivos antes de reinscribirlos. Para eliminar un dispositivo, vaya a **Administrar > Dispositivos**, seleccione el dispositivo y, a continuación, haga clic en **Eliminar**.

Importar cuentas de usuario

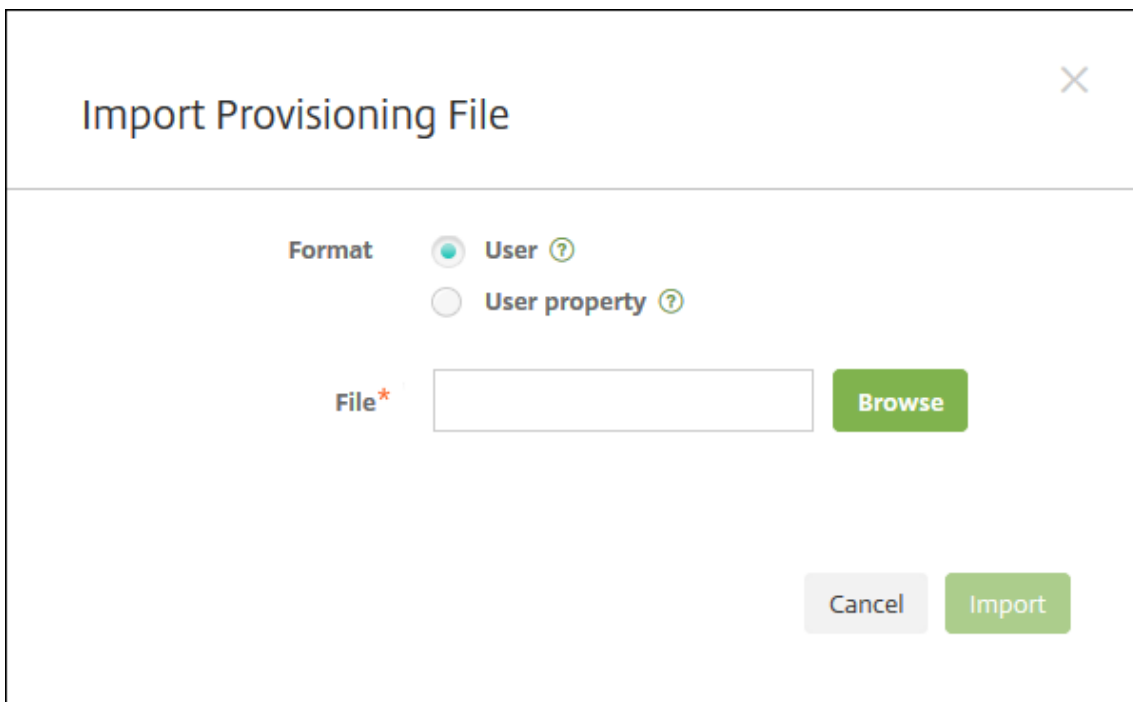
Puede importar propiedades y cuentas de usuarios locales desde un archivo de formato CSV llamado “archivo de aprovisionamiento”, el cual puede crear manualmente. Para obtener información acerca de los formatos de los archivos de aprovisionamiento, consulte [Formatos de archivo de aprovisionamiento](#).

Nota:

- Para usuarios locales, use 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 mediante las credenciales LDAP correspondientes.
- Si importa cuentas de usuario al directorio interno de usuarios de Citrix Endpoint Management, inhabilite el dominio predeterminado para acelerar el proceso de importación. Tenga en cuenta que inhabilitar el dominio afecta a las inscripciones. Puede volver a habilitar el dominio predeterminado después de la importación de usuarios internos.
- Los usuarios locales pueden tener el formato de Nombre principal del usuario (UPN). Sin embargo, Citrix recomienda no usar el dominio administrado. Por ejemplo, si ejemplo.com está administrado, no cree un usuario local con este formato UPN: `usuario@ejemplo.com`.

Después de preparar un archivo de aprovisionamiento, siga estos pasos para importar el archivo en 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**. Aparece el cuadro de diálogo **Importar archivo de aprovisionamiento**.

A dialog box titled "Import Provisioning File" with a close button (X) in the top right corner. It contains a "Format" section with two radio buttons: "User" (selected) and "User property". Below this is a "File" label with a red asterisk, followed by a text input field and a green "Browse" button. At the bottom right are "Cancel" and "Import" buttons.

Import Provisioning File

Format

☒ User ?

☐ User property ?

File*

Browse

Cancel Import

3. Seleccione **Usuario** o **Propiedad** para el formato del archivo de aprovisionamiento que va a importar.
4. Para seleccionar el archivo de aprovisionamiento que quiere usar, haga clic en **Examinar** y vaya a la ubicación de ese 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 en Citrix Endpoint Management. Utilice uno de los siguientes formatos para el 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:

- Use un punto y coma (;) para separar los campos que contenga el archivo de aprovisionamiento. Si parte de un campo tiene un punto y coma, debe anteponérsele un carácter de barra diagonal inversa (\). Por ejemplo, la propiedad **propertyV; test;1;2** debe escribirse como **propertyV;test;1;2** en el archivo de aprovisionamiento.

- Los valores válidos de **Rol** son los roles predefinidos USER, ADMIN, SUPPORT y DEVICE_PROVISIONING, además de cualquier rol adicional que haya definido.
- Use el carácter de punto (.) como separador para crear una jerarquía de grupo. No use un punto en los nombres de grupo.
- En los archivos de aprovisionamiento de atributos, use minúsculas para los atributos de las propiedades. La base de datos distingue entre mayúsculas y minúsculas.

Ejemplo del contenido de un archivo de aprovisionamiento de usuarios La entrada `user01;pwd\;01;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` significa:

- **Usuario:** user01
- **Contraseña:** pwd; 01
- **Rol:** USER
- **Grupos:**
 - myGroup.users01
 - myGroup.users02
 - myGroup.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 del contenido de un archivo de aprovisionamiento de atributos de usuario La entrada `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` significa:

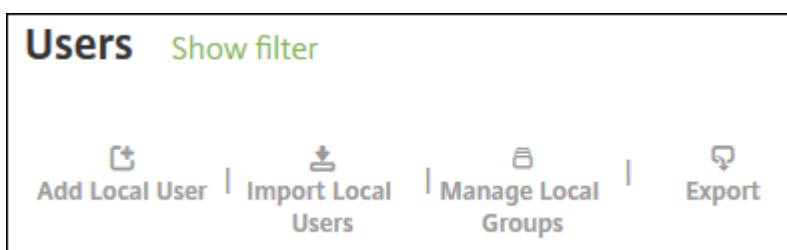
- **Usuario:** user01
- **Propiedad 1**
 - **nombre:** propertyN
 - **valor:** propertyV;test;1;2
- **Propiedad 2:**
 - **nombre:** prop 2
 - **valor:** valor de prop2

Agregar o quitar grupos

Puede administrar grupos desde el cuadro de diálogo **Administrar grupos** de la consola de Citrix Endpoint Management. Para ver este cuadro, vaya a las páginas **Usuarios**, **Agregar usuario local** o **Modificar usuario local**. No hay ningún comando de modificación de grupos.

Para agregar un grupo local

1. Lleve a cabo una de las siguientes acciones:
 - En la página **Usuarios**, haga clic en **Administrar grupos locales**.



- Ya sea en la página **Agregar usuario local** o **Modificar usuario local**, haga clic en **Administrar grupos**.

User name* User01

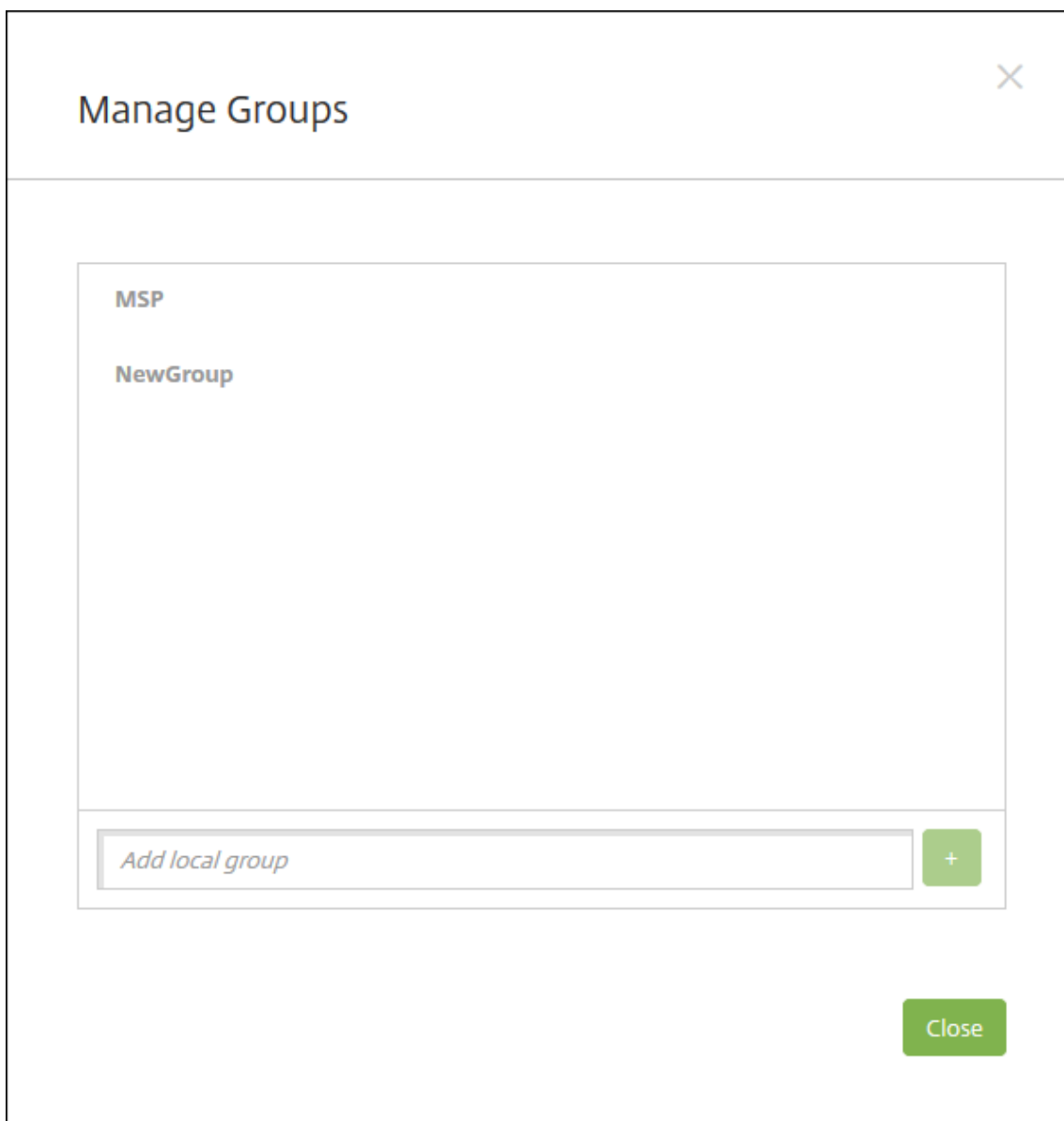
Password Enter new password

Role* SUPPORT

Membership ☒ local\MSP

Manage Groups

Aparecerá el cuadro de diálogo **Administrar grupos**.



2. Bajo 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**.

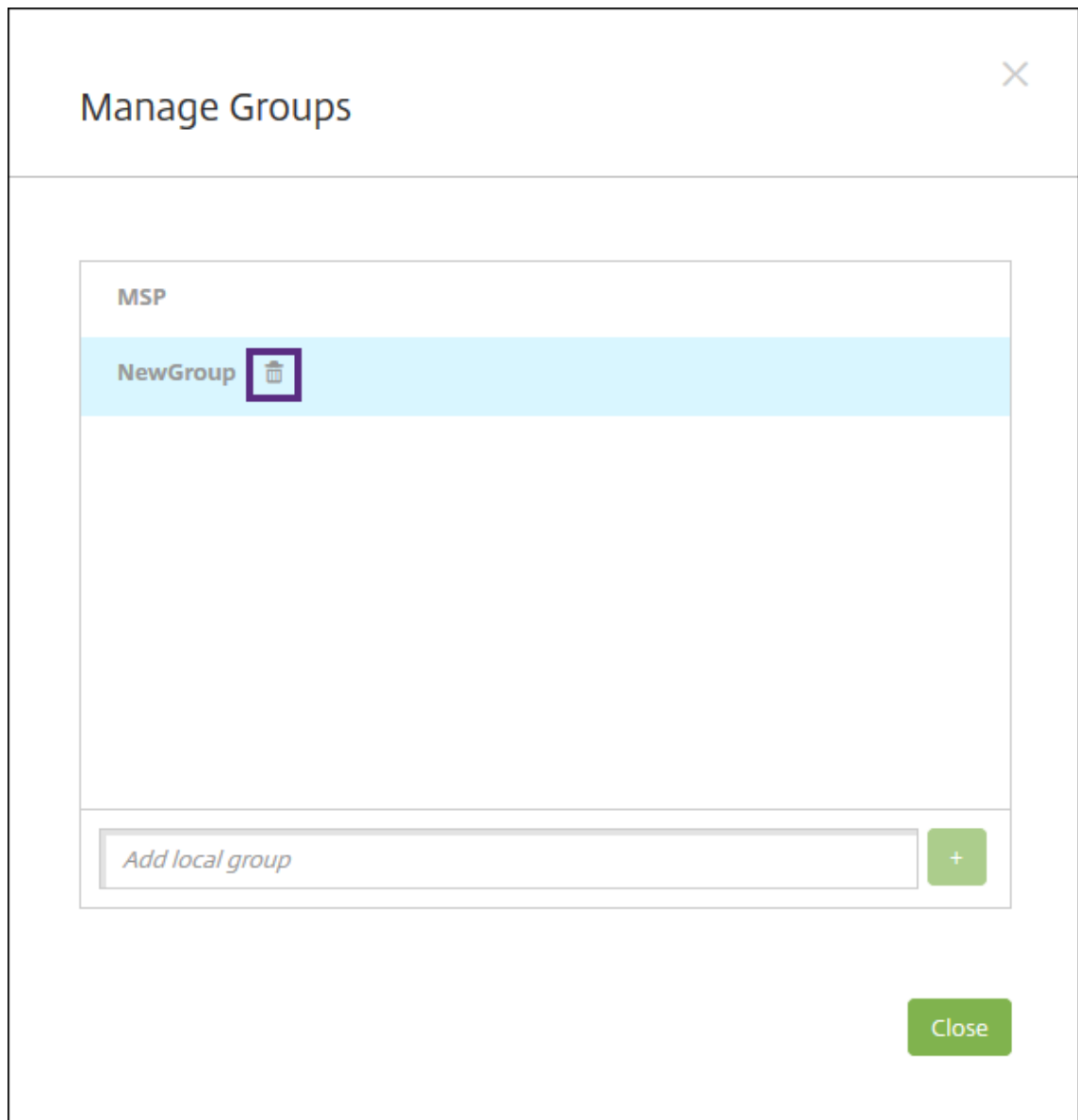
Para quitar un grupo

Quitar un grupo no tiene ningún efecto sobre las cuentas de usuario. Quitar un grupo simplemente elimina la asociación de usuarios con ese grupo. Los usuarios pierden acceso a las aplicaciones o a los perfiles proporcionados por los grupos de entrega asociados con ese grupo. Sin embargo, cualquier otra asociación de grupo permanece intacta. Si los usuarios no están asociados a ningún otro grupo local, se asocian al nivel superior.

1. Lleve a cabo una de las siguientes acciones:

- En la página **Usuarios**, haga clic en **Administrar grupos locales**.
- Ya sea en la página **Agregar usuario local** o **Modificar usuario local**, haga clic en **Administrar grupos**.

Aparecerá el cuadro de diálogo **Administrar grupos**.



2. En el cuadro de diálogo **Administrar grupos**, haga clic en el grupo a eliminar.
3. Haga clic en el icono con forma de papelera situado a la derecha del nombre de grupo. Aparecerá un cuadro de diálogo de confirmación.
4. Haga clic en **Eliminar** para confirmar la operación y eliminar el grupo.

Importante:

Esta operación no se puede deshacer.

5. En el cuadro de diálogo **Administrar grupos**, haga clic en **Cerrar**.

Crear y administrar flujos de trabajo

Puede utilizar flujos de trabajo para administrar la creación y la eliminación de cuentas de usuario. Antes de crear un flujo de trabajo, es necesario identificar las personas dentro de su organización que tienen la autoridad de aprobar solicitudes de cuentas de usuario. Después, utilice la plantilla de flujo de trabajo para crear y aprobar solicitudes de cuentas de usuario.

Al configurar Citrix Endpoint Management por primera vez, se definen los parámetros de correo electrónico referentes al flujo de trabajo; estos parámetros se deben establecer antes de utilizar los flujos de trabajo. Puede cambiar los parámetros de correo electrónico del flujo de trabajo en cualquier momento. Estos parámetros incluyen servidor de correo electrónico, puerto, 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**, se pueden configurar varios flujos de trabajo para su uso con configuraciones de aplicaciones. Al configurar flujos de trabajo en la página “Flujos de trabajo”, puede seleccionar el flujo de trabajo cuando configure la aplicación.
- Cuando configure un conector de aplicaciones en la aplicación, proporcione un nombre de flujo de trabajo y después defina a las personas que aprueban solicitudes de cuentas de usuario. Consulte [Agregar aplicaciones](#).

Se puede asignar hasta tres niveles de aprobación del tipo administrador para cuentas de usuario. Si necesita que otras personas aprueben la cuenta de usuario, puede buscar y seleccionar aprobadores adicionales por nombre o dirección de correo electrónico. Cuando Citrix Endpoint Management las encuentre, podrá agregarlas al flujo de trabajo. Todas las personas en el 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 con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Parámetros**.
2. Haga clic en **Flujos de trabajo**. Aparecerá la página **Flujos de trabajo**.
3. Haga clic en **Agregar**. Aparecerá la página **Agregar flujo de trabajo**.

Settings > Workflows > [Add Workflow](#)

Add Workflow


Name*

Description

Email Approval Templates Workflow Approval Request 

Levels of manager approval 1 level

Select Active Directory domain agsag.com

Find additional required approvers  [Search](#)

Selected additional required approvers

[Cancel](#) [Save](#)

4. Configure estos parámetros:

- **Nombre:** Escriba un nombre único para el flujo de trabajo.
- **Descripción:** Si quiere, escriba una descripción del flujo de trabajo.
- **Plantillas de correo electrónico de aprobación:** En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar al flujo de trabajo. En la consola de Citrix Endpoint Management, puede crear plantillas de correo electrónico en la sección **Plantillas de notificaciones** de **Parámetros**. Al hacer clic en el icono con forma de ojo situado a la derecha del campo, aparece una vista previa de la plantilla que quiere configurar.
- **Niveles de aprobación administrativa:** En la lista, seleccione la cantidad de niveles de aprobación administrativa necesarios para este flujo de trabajo. El valor predeterminado es **1 nivel**. Las opciones posibles son:
 - No se necesita
 - 1 nivel
 - 2 niveles
 - 3 niveles

- **Seleccionar dominio de Active Directory:** En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
- **Buscar aprobadores adicionales requeridos:** Escriba un nombre en el campo de búsqueda y, a continuación, haga clic en **Buscar**. Los nombres se originan en Active Directory.
- Cuando el nombre aparezca en el campo, marque la casilla situada al lado. El nombre y la dirección de correo electrónico aparecen en la lista **Aprobadores adicionales requeridos 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 requeridos seleccionados** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla situada junto a cada nombre que quiera quitar.

5. Haga clic en **Guardar**. El flujo de trabajo creado se muestra en la página **Flujos de trabajo**.

Después de crear el flujo de trabajo, puede ver sus detalles, las aplicaciones que tiene asociadas, o bien puede eliminarlo. El flujo de trabajo no se puede modificar una vez creado. Si necesita un flujo de trabajo con otros niveles de aprobación o con otros aprobadores, cree otro flujo de trabajo.

Para ver los detalles de un flujo de trabajo y cómo eliminar uno

1. En la página **Flujos de trabajo**, en la lista de los flujos de trabajo existentes, seleccione un flujo concreto. Para ello, haga clic en la fila de la tabla o marque la casilla situada junto al flujo de trabajo.
2. Para eliminar un flujo de trabajo determinado, haga clic en **Eliminar**. Aparecerá un cuadro de diálogo de confirmación. Vuelva a hacer clic en **Eliminar**.

Importante:

Esta operación no se puede deshacer.

Perfiles de inscripción

March 1, 2024

Un perfil de inscripción especifica lo siguiente:

- Opciones de inscripción para administración de dispositivos en dispositivos Android iOS y Windows.
- Opciones de inscripción para administración de aplicaciones en 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 que ha superado el límite de inscripción de dispositivos.
 - Si se debe permitir que un usuario rechace la administración de dispositivos.

Puede utilizar perfiles de inscripción para combinar diferentes casos de uso y rutas de migración de dispositivos en una sola consola de Citrix Endpoint Management. Entre los casos de uso, se incluyen:

- Administración de dispositivos móviles (solo MDM)
- MDM+Administración de aplicaciones móviles (MAM)
- Solo MAM
- Inscripciones de propiedad de la empresa
- Inscripciones BYOD (con la posibilidad de excluir la inscripción en MDM)
- Migración de inscripciones en Administrador de dispositivos Android a inscripciones en Android Enterprise (totalmente administrado, perfil de trabajo, dispositivo dedicado)
- Inscripción automática de dispositivos con Windows 10 o Windows 11 a través de la aplicación Citrix Workspace para Windows (Tech Preview)

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 utilizar el perfil de inscripción predeterminado denominado Global o especificar otro perfil de inscripción.

Las funciones del perfil de inscripción por plataforma incluyen lo siguiente.

- **Para dispositivos Android:** Debe especificar la administración y el modo propietario del dispositivo. Por ejemplo: Dispositivo propiedad de la empresa, totalmente administrado con perfil de trabajo y perfil de trabajo BYOD.

Los nuevos dispositivos se inscriben en Android Enterprise de forma predeterminada. Puede optar por administrar los dispositivos con el modo de administrador de dispositivos Android (AD) antiguo. Los nuevos dispositivos también se inscriben en la administración de aplicaciones de forma predeterminada.

Para obtener información sobre la especificación del nivel de seguridad y los pasos necesarios para la inscripción, consulte [Inscripción, roles y cuentas de usuario](#).

- **Para dispositivos iOS:** Debe especificar el tipo de administración de dispositivos, ya sea **Inscripción de usuarios de Apple**, **Inscripción de dispositivos Apple** o **No administrar dispositivos**. El modo **Inscripción de usuarios de Apple** está disponible en versión Tech Preview pública. Para habilitar esta función, póngase en contacto con su equipo de asistencia.

Si selecciona Inscripción de usuarios de Apple, puede optar por usar un dominio personalizado para los ID de Apple administrados y configurar ese dominio.

Los nuevos dispositivos se inscriben en la administración de dispositivos Apple de forma predeterminada. Los nuevos dispositivos también se inscriben en la administración de aplicaciones de forma predeterminada.

- **Para dispositivos con Windows 10 o Windows 11:** Debe especificar si quiere utilizar la administración de dispositivos Citrix para Windows. Los nuevos dispositivos 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 prueba hasta que tenga la oportunidad de crear perfiles de inscripción.

Si se incorpora a Citrix Endpoint Management 20.2.1 o una versión posterior, el perfil de inscripción Global tiene parámetros predefinidos. En las siguientes capturas de pantalla, se muestra la configuración predeterminada del perfil de inscripción Global. Solo las implementaciones MAM muestran un subconjunto de estas opciones.

Enrollment Profile	Enrollment Info
1 Enrollment Info	<p>Set the number of devices a user can enroll. The default is unlimited, which lets users enroll an unlimited number of devices.</p> <p>Enrollment profile name *</p> <p>Total number of devices a user can enroll</p>
2 Platforms	
Android	
iOS	
Windows	
3 Assignment (optional)	

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

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

Apple User Enrollment

Apple Device enrollment

Do not manage devices

Use custom domain for Managed Apple ID

On

Managed Apple ID custom domain

example.appleid.com

Application management

Citrix MAM

On

User consent

Allow users to decline device management

On

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Device management ? Management <input checked="" type="radio"/> Fully managed ? <input type="radio"/> Do not manage devices ?
Android	User consent Allow users to decline device management <input checked="" type="checkbox"/> On ?
iOS	Workspace integration ? Enrollment through Workspace app <input type="checkbox"/> Off ?
Windows	
3 Assignment (optional)	

Perfiles de inscripción, grupos de entrega e inscripción

Los perfiles de inscripción y los grupos de entrega interactúan de la siguiente manera:

- Puede asociar un perfil de inscripción a uno o más grupos de entrega.
- Si un usuario pertenece a varios grupos de entrega que tienen perfiles de inscripción diferentes, 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. Supongamos, por ejemplo, que tiene lo siguiente:
 - Dos perfiles de inscripción, llamados “EP1” y “EP2”.
 - Dos grupos de entrega, llamados “DG1” y “DG2”.
 - “DG1” está asociado a “EP1”.
 - “DG2” está asociado a “EP2”.

Si el usuario de la inscripción 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 solo se aplica a los dispositivos de un grupo de entrega que tenga un perfil de inscripción configurado para MDM (administración de dispositivos).
- Después de inscribir un dispositivo, para hacer algunos cambios en un perfil de inscripción será necesario reinscribirlo:
 - Cambiar la configuración para pasar un dispositivo de MDM+MAM a la inscripción MAM o MDM. Puede producirse una degradación al actualizar un perfil de inscripción o mover un dispositivo a un grupo de entrega diferente.
 - Agregar MAM a un perfil de inscripción configurado para MDM.

- Agregar MDM a un perfil de inscripción configurado para MAM.
- Cambiar a un perfil de inscripción diferente no afecta a los dispositivos ya inscritos. Los usuarios deberán desinscribir y, a continuación, volver a inscribir esos dispositivos para que los cambios surtan efecto.

Para crear un perfil de inscripción

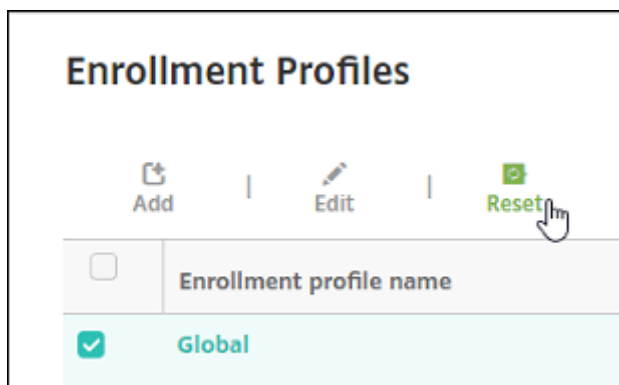
1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Perfiles de inscripción**.
2. En la página **Información de inscripción**, escriba un nombre descriptivo para el perfil. De forma predeterminada, un usuario puede inscribir una cantidad de dispositivos ilimitada. Seleccione un valor para limitar la cantidad 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 plataformas. Para obtener información acerca de los parámetros de inscripción específicos de las plataformas, consulte:

- Android Enterprise: [Crear perfiles de inscripción](#)
- iOS: [Métodos de inscripción admitidos](#)
- Escritorios y tabletas Windows: [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 tengan perfiles de inscripción diferentes. 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**.

En la página **Configurar > Perfiles de inscripción**, aparecerá una lista de sus perfiles de inscripción. Para modificar el perfil Global o restablecerlo a los valores predeterminados originales, seleccione la fila del perfil Global y haga clic en **Restablecer**. El perfil Global no se puede eliminar.



Notificaciones

November 29, 2023

Puede utilizar notificaciones en Citrix Endpoint Management para los siguientes propósitos:

- Comunicarse con grupos específicos de usuarios para ciertas funciones relacionadas con el sistema. También puede destinar estas notificaciones a ciertos usuarios. Por ejemplo, usuarios con dispositivos iOS, usuarios cuyos dispositivos no cumplen los requisitos de cumplimiento o usuarios con dispositivos que son propiedad de los empleados, entre otros.
- Para inscribir usuarios y sus dispositivos
- Para notificar automáticamente a los usuarios (mediante acciones automatizadas) cuando se den ciertas condiciones. Por ejemplo:
 - Cuando un dispositivo de usuario está a punto de ser bloqueado del dominio corporativo debido a un problema de cumplimiento
 - Cuando el dispositivo ha sido liberado por jailbreak o rooting

Para obtener información detallada acerca de las acciones automatizadas, consulte [Acciones automatizadas](#).

Para poder enviar notificaciones con Citrix Endpoint Management, debe configurar una puerta de enlace y un servidor de notificaciones. Puede definir un servidor de notificaciones en Citrix Endpoint Management para configurar servidores SMTP. Esos servidores envían notificaciones de correo electrónico a los usuarios. Puede usar notificaciones para enviar mensajes a través de SMTP.

- SMTP es un protocolo basado en texto orientado a la conexión 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 constan de comandos originados por un cliente SMTP (la persona que envía el mensaje) y las respuestas correspondientes del servidor SMTP.

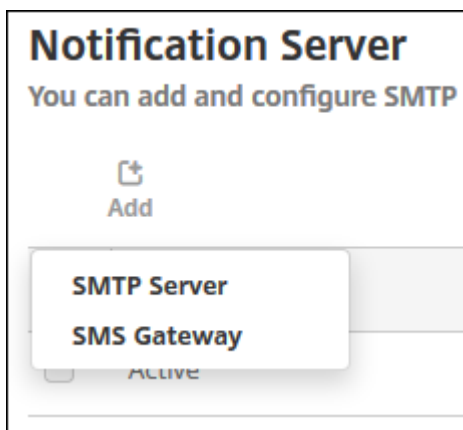
Requisitos previos

- 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 acerca de la configuración. Si el servidor es un servidor de servicio de correo electrónico, busque la información de configuración correspondiente en el sitio web del proveedor del servicio.
- Solo puede usar un servidor SMTP activo. Este canal de comunicación solo permite una configuración activa.

- Debe abrir el puerto 25 desde Citrix Endpoint Management (ubicado en la zona DMZ de la red) para apuntarlo al servidor SMTP de la red interna. Eso permite a Citrix Endpoint Management enviar correctamente las notificaciones.

Configurar un servidor SMTP

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Parámetros**.
2. En **Notificaciones**, haga clic en **Servidor de notificaciones**. Aparecerá 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**. A continuación, vaya a Agregar un servidor SMTP y consulte los pasos que se deben seguir para configurar este parámetro.

Agregar un servidor SMTP

Settings > Notification Server > Add SMTP Server

Add SMTP Server

You need to configure the SMTP notifications server to send messages to users. If the SMTP server is hosted on an internal server, you get the server information from your IT department. If the server is a hosted email service, you can find information from the service provider's website. Only one SMTP server is activated at one time.

Name*	<input type="text"/>
Description	<input type="text"/>
SMTP Server*	<input type="text"/>
Secure channel protocol	<div>None</div>
SMTP server port*	<div>25</div>
Authentication	<div>OFF</div>
Microsoft Secure Password Authentication (SPA)	<div>OFF</div>
From name*	<input type="text"/>
From email*	<input type="text"/>

▶ Advanced Settings

1. Configure estos parámetros:

- **Nombre:** Escriba el nombre asociado a esta cuenta del servidor SMTP.
- **Descripción:** Si quiere, 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:** En la lista, haga clic en **SSL**, **TLS** o **Ninguno** para definir el protocolo de canal seguro que utiliza el servidor (si el servidor está configurado para usar la autenticación segura). El valor predeterminado es **Ninguno**.
- **Puerto del servidor SMTP:** Escriba el puerto que usa el servidor SMTP. De forma predeterminada, el puerto está configurado en 25. En cambio, si las conexiones SMTP usan el

protocolo SSL de canal seguro, establezca el puerto en 465.

- **Autenticación:** Seleccione **Sí** o **No**. El valor predeterminado es **Desactivado**.
 - Si habilita **Authentication**, configure los siguientes parámetros:
 - **Nombre de usuario:** Escriba el nombre de usuario que se usará para la autenticación.
 - **Contraseña:** Escriba la contraseña de autenticación del usuario.
 - **Autenticación de contraseña segura (SPA) de Microsoft:** Si el servidor SMTP usa la autenticación SPA, haga clic en **Sí**. El valor predeterminado es **Desactivado**.
 - **Nombre de remitente:** Escriba el nombre que aparece en el cuadro **De** cuando un cliente recibe un correo electrónico de notificación procedente de este servidor. Por ejemplo, Departamento de TI de la empresa.
 - **Correo electrónico de remitente:** Escriba la dirección de correo electrónico utilizada 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 prueba por correo electrónico.
 3. Expanda **Parámetros avanzados** y, a continuación, configure estos parámetros:
 - **Cantidad de reintentos de SMTP:** Escriba la cantidad de veces que se intentará volver a enviar un mensaje fallido enviado desde el servidor SMTP. El valor predeterminado es 5.
 - **Tiempo de espera de SMTP:** Escriba la duración del tiempo de espera (en segundos) al enviar una solicitud SMTP. Aumente este valor si el envío de mensajes falla continuamente por culpa de los tiempos de espera que se agotan. Tenga cuidado al reducir este número, porque podría aumentar la cantidad de mensajes sin entregar y de mensajes cuyo tiempo de espera se ha agotado. De forma predeterminada, es de 30 segundos.
 - **Número máximo de destinatarios de SMTP:** Escriba la cantidad máxima 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 notificaciones

En Citrix Endpoint Management, puede crear o actualizar plantillas de notificaciones que se van a usar en acciones automatizadas, inscripciones y mensajes de notificaciones estándar a los usuarios. Puede configurar plantillas de notificaciones para enviar mensajes a través de dos canales diferentes: Citrix Secure Hub o SMTP.

Citrix Endpoint Management incluye muchas plantillas de notificaciones predefinidas. Esas plantillas reflejan los distintos tipos de eventos a los que Citrix Endpoint Management responde automáticamente para cada dispositivo del sistema.

Nota:


Si quiere utilizar los canales de SMTP para enviar notificaciones a los usuarios, debe configurar los canales antes de activarlos. Citrix Endpoint Management solicitará configurar los canales cuando usted agregue las plantillas de notificaciones, si no están ya configurados.

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Parámetros**.
2. Haga clic en **Plantillas de notificaciones**. Aparecerá la página **Plantillas de notificaciones**.

Settings > Notification Templates

Notification Templates

Create notification templates to use in automated actions, enrollment, and standard notification message delivery to users.

 Add

<input type="checkbox"/>	Name	Channels	Type	Deletable	Manual sending supported	▼
<input type="checkbox"/>	ActiveSync Gateway Blocked	Worx Home	ActiveSync Gateway blocked device			
<input type="checkbox"/>	Android Download Link	SMTP, SMS	Android Download Link			
<input type="checkbox"/>	APNS cert expiration	SMTP	APNS Cert Expiration			
<input type="checkbox"/>	Certificate renewal	Worx Home	Certificate is renewed			
<input type="checkbox"/>	Enrollment	SMTP, SMS	Enrollment Notification			
<input type="checkbox"/>	Enrollment Confirmation	SMTP, SMS	Enrollment Confirmation			
<input type="checkbox"/>	Enrollment Invitation	SMTP, SMS	Enrollment Invitation			
<input type="checkbox"/>	Enrollment PIN	SMTP, SMS	Enrollment PIN			
<input type="checkbox"/>	Failed Samsung KNOX attestation	Worx Home	Failed Samsung KNOX attestation		✓	
<input type="checkbox"/>	iOS Download Link	SMTP, SMS	iOS Download Link			

Showing 1 - 10 of 25 items

Showing 1 of 3

Agregar una plantilla de notificaciones

1. Haga clic en **Agregar**. Si no se ha definido ningún servidor SMTP, aparece un mensaje sobre el uso de las notificaciones SMTP. Puede optar por configurar el servidor SMTP ahora o más tarde.

Si elige configurar el servidor SMTP ahora, se le redirigirá a la página **Servidor de notificaciones**, en la página **Parámetros**. Después de configurar los canales que se van a utilizar, puede volver a la página **Plantillas de notificaciones** para continuar agregando o modificando plantillas de notificaciones.

Importante:

Si decide definir la configuración del servidor SMTP más adelante, no podrá activar esos canales al agregar o modificar una plantilla de notificaciones. Por eso, esos canales no están disponibles para enviar notificaciones de usuario.

2. Configure estos parámetros:

- **Nombre:** Escriba un nombre descriptivo para la plantilla.
- **Descripción:** Escriba una descripción para la plantilla.
- **Tipo:** En la lista, haga clic en el tipo de notificación. Solo se muestran los canales admitidos para el tipo de notificación seleccionado. Solo se permite una plantilla de caducidad de certificados APNS, que es la plantilla predefinida. No se puede agregar una plantilla de este tipo.

Nota:

En algunos tipos de plantilla, aparece la frase “Se admite el envío manual” debajo del tipo. Estos tipos de plantilla están disponibles en la lista **Notificaciones** del **panel de mandos** y en la página **Dispositivos**. Desde esas ubicaciones, puede enviar manualmente la notificación a los usuarios. Independientemente del canal utilizado, el envío manual no está disponible para las plantillas que utilicen las siguientes macros en los campos “Asunto” o “Mensaje”:

- `${outofcompliance.reason(whitelist_blacklist_apps_name)}`
- `${outofcompliance.reason(smg_block)}`

Nota:

La consola de Citrix Endpoint Management contiene los términos “lista negra” y “lista blanca”. Estamos cambiando esos términos en una próxima versión a “lista de bloqueados” y “lista de permitidos”.

3. En **Canales, indique la información de cada canal que se va a utilizar para esta notificación. Puede elegir un canal cualquiera o todos. Los canales que seleccione dependen de la forma en que quiera enviar notificaciones:**

- Si elige **Citrix Secure Hub**, solo los dispositivos iOS y Android recibirán las notificaciones, que aparecerán en la bandeja de notificaciones de los dispositivos en cuestión.
- Si elige **SMTP**, los usuarios que se inscribieron con su dirección de correo electrónico reciben el mensaje.

Citrix Secure Hub:

- **Activar:** Haga clic para habilitar el canal de notificación.

- **Mensaje:** Escriba el mensaje que se enviará al usuario. Este campo es necesario si usa Citrix Secure Hub. Para obtener información sobre cómo usar las macros, consulte [Macros](#).
- **Archivo de sonido:** Seleccione el sonido de notificación que oirá el usuario cuando reciba la notificación.

SMTP:

- **Activar:** Haga clic para habilitar el canal de notificación.
Solo puede activar la notificación SMTP después de configurar el servidor SMTP.
 - **Remitente:** Escriba un remitente optativo para la notificación, que puede consistir en un nombre, una dirección de correo electrónico o ambos.
 - **Destinatario:** Este campo contiene una macro previamente generada para todas las notificaciones salvo las ad hoc. De este modo, se garantiza que las notificaciones se envían a la dirección correcta de destino de SMTP. Citrix recomienda no modificar macros de plantillas. Puede agregar más destinatarios (como un administrador corporativo). Para ello, agregue sus direcciones respectivas en este campo. Utilice un punto y coma (;) para separar las macros y otras direcciones. Para enviar notificaciones ad hoc, puede especificar destinatarios concretos o puede seleccionar los 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 cómo usar las macros, consulte [Macros](#).
4. Haga clic en **Agregar**. Cuando todos los canales se hayan configurado correctamente, aparecen en este orden en la página **Plantillas de notificaciones**: SMTP y Citrix Secure Hub. Los canales configurados incorrectamente aparecen después de los canales configurados correctamente.

Modificar una plantilla de notificaciones

1. Seleccione una plantilla de notificaciones. Aparecerá la página de modificación específica de esa plantilla. Puede modificar la plantilla, excepto el campo **Tipo**, y activar o desactivar canales.
2. Haga clic en **Guardar**.

Eliminar una plantilla de notificaciones

Solo podrá eliminar las plantillas de notificación que usted haya agregado. No podrá eliminar las plantillas de notificación predefinidas.

1. Seleccione una plantilla de notificaciones existente.
2. Haga clic en **Eliminar**. Aparecerá un cuadro de diálogo de confirmación.
3. Haga clic en **Eliminar** para eliminar la plantilla de notificaciones o en **Cancelar** para cancelar la operación.

Configurar roles con RBAC

March 1, 2024

La función del control de acceso por roles (RBAC) Citrix Endpoint Management le permite asignar roles a usuarios y grupos. Los roles son conjuntos de permisos que controlan el nivel de acceso de los usuarios a las funciones del sistema.

Citrix Endpoint Management incluye estos roles de usuario predeterminados. Puede usar los roles predeterminados como plantillas que personalizar para crear sus propios roles de usuario.

- **Administrador:** Concede acceso completo al sistema.
- **Usuario:** Permite a los usuarios inscribir dispositivos y acceder a Self Help Portal.

Puede usar la función RBAC en Citrix Endpoint Management para:

- Crear y modificar roles de usuario.
- Asignar roles a grupos de usuarios locales y grupos de Active Directory (AD).
- Asignar roles a administradores en Citrix Cloud a través de **Administración de acceso e identidad > Administradores**. Consulte Agregar roles a administradores de Citrix Cloud.

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 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. Si no, también 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. En una cuenta de administrador de la nube, se utiliza el mismo nombre de usuario que en la cuenta de administrador de Citrix Cloud. Cree roles de RBAC en la consola de Citrix Endpoint

Management y asigne roles a estos usuarios a través de **Administración de acceso e identidad > Administradores** en Citrix Cloud.

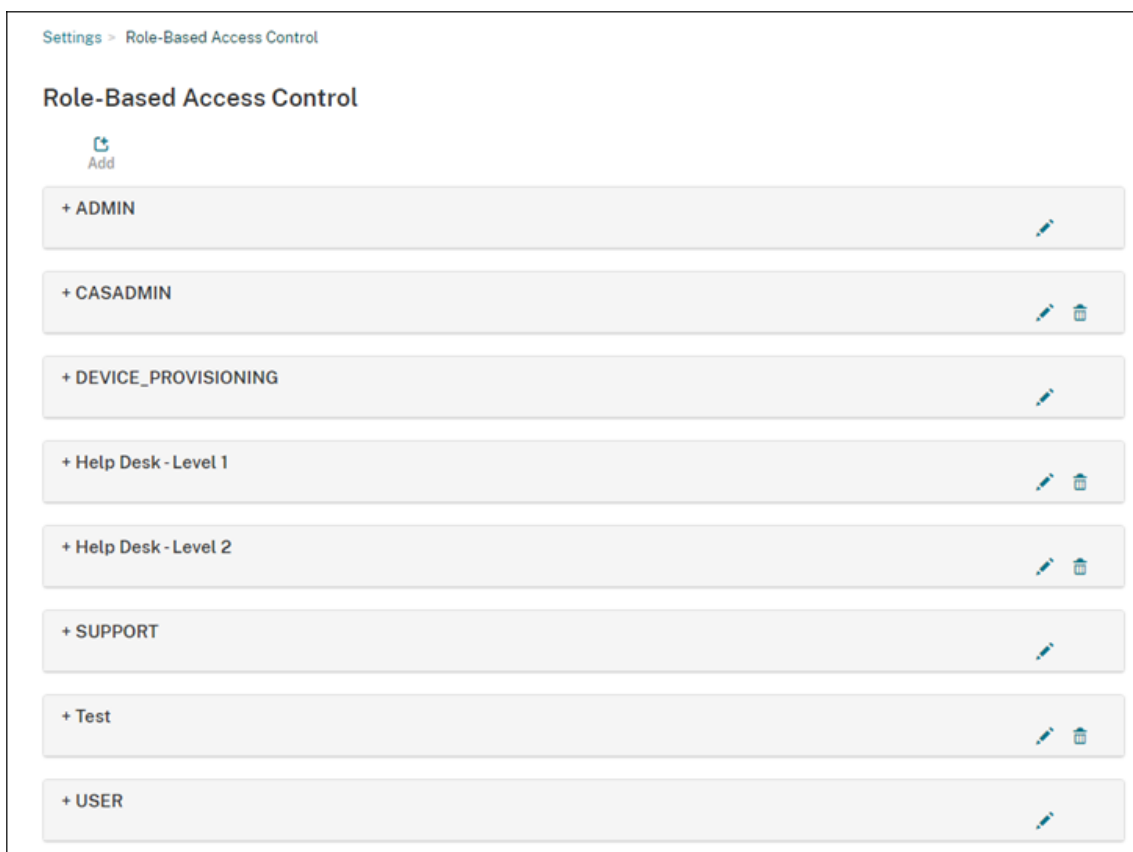
- **Grupos de Active Directory:** Todos los usuarios de un grupo de Active Directory tienen los mismos permisos. Si un usuario pertenece a varios grupos de Active Directory, todos los permisos se combinan para definir los permisos de ese usuario concreto. Supongamos, por ejemplo, que los usuarios del grupo A de Active Directory pueden localizar dispositivos de administradores y que los usuarios del grupo B de Active Directory pueden borrar dispositivos de empleados. Un usuario que pertenezca a ambos grupos puede localizar y borrar los dispositivos de administradores y empleados. Si un usuario pertenece a grupos con permisos en conflicto, prevalecerán los permisos habilitados.

Para obtener más información, consulte [Acerca de las cuentas de usuario](#).

Crear o modificar roles

1. En la consola de Citrix Endpoint Management, para acceder a la página **Parámetros**, haga clic en el icono con forma de engranaje situado en la esquina superior derecha.
2. Haga clic en **Control de acceso por roles**. La página **Control de acceso por roles** muestra los roles de usuario predeterminados y los roles agregados.

Haga clic en el signo más (+) situado junto a un rol para ver todos los permisos del rol en cuestión.



3. Para agregar un rol, haga clic en **Agregar**. O bien, para modificar un rol, haga clic en el icono del lápiz situado a la derecha de un rol existente.

Nota:

Para eliminar un rol, haga clic en la papelera que hay a la derecha de un rol que haya definido. No se pueden eliminar los roles de usuario predeterminados.

4. En la página **Agregar rol**, escriba la información siguiente:
 - **Nombre de RBAC:** Indique un nombre descriptivo para el nuevo rol de usuario. No se puede cambiar el nombre de un rol existente.
 - **Plantilla de RBAC:** Si quiere, seleccione una plantilla como punto de partida del nuevo rol (al modificar 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 **Acceso autorizado** y **Funciones de consola**. Citrix Endpoint Management completa esos campos con los permisos de acceso y funciones predefinidos para la plantilla seleccionada.

5. Para personalizar el rol, marque o desmarque las casillas **Acceso autorizado** y **Funciones de consola**.

Haga clic en el triángulo situado junto a una función de consola para mostrar y seleccionar los permisos específicos de esa función. Al hacer clic en la casilla del nivel superior, no se seleccionan los permisos individuales. Seleccione opciones individuales después de expandir el permiso de nivel superior.

6. **Aplicar permisos:** Haga clic en **Para grupos de usuarios específicos** para aplicar permisos a los grupos que seleccione.

Por ejemplo, si un administrador RBAC tiene permisos para acceder al grupo de usuarios ActiveDirectory:

- El administrador solo tiene acceso a la información de los usuarios que se encuentran en el grupo ActiveDirectory.
- El administrador no puede ver ningún otro usuario local o de AD. El administrador puede ver la información de los usuarios que sean 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

7. Haga clic en **Siguiente** e introduzca esta siguiente información para asignar el rol a grupos de usuarios.

- **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 afinar la búsqueda.
- **Incluir grupos de usuarios:** En la lista que aparezca, seleccione los grupos de usuarios a los que asignar el rol.

8. Haga clic en **Guardar**.

Agregar roles a Citrix Cloud administradores

En lugar de asignar roles de RBAC a administradores de Citrix Cloud a través de la consola de Citrix Endpoint Management, asigne roles desde la consola de Citrix Cloud.

1. En la consola de Citrix Cloud, vaya a **Administración de acceso e identidad > Administradores**.

2. Seleccione un proveedor de identidades y, a continuación, escriba una dirección de correo electrónico para agregar un administrador. Haga clic en **Invitar**.

Haga clic en ... al final de una fila de administrador existente para modificar esos permisos.

3. Haga clic en **Acceso personalizado**. Al asignar permisos al administrador, puede seleccionar los roles de RBAC creados en la consola de Citrix Endpoint Management.

4. Haga clic en **Enviar invitación** para enviar una invitación a un nuevo administrador o haga clic en **Guardar** para terminar de modificar un administrador.

Roles predefinidos

Cada rol predefinido de RBAC tiene determinados permisos de funciones y de acceso asociados. En estas tablas se describe cada uno de los permisos correspondientes al rol de administrador y al rol de usuario. No puede eliminar ni modificar los roles predefinidos.

- Para obtener una lista completa de permisos predeterminados para cada rol integrado, descargue [Role-Based Access Control Defaults](#).
- Para obtener información sobre las cuentas de usuario de Citrix Endpoint Management, consulte [Acerca de las cuentas de usuario](#).

Importante:

En el permiso Parámetros, el permiso RBAC otorga acceso total a los usuarios administradores, incluida la capacidad de asignar sus propios permisos. Conceda este acceso solamente a los usuarios a los que quiere dar la capacidad de manipular todo lo que hay en el sistema de Citrix Endpoint Management.

Rol de administrador

El rol predefinido de administrador ofrece un acceso específico en Citrix Endpoint Management. De forma predeterminada, las opciones **Acceso autorizado** (excepto Self Help Portal), **Funciones de consola** y **Aplicar permisos** están habilitadas.

Puede cambiar el rol de usuarios locales que tienen asignado 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 locales y de la nube con el rol de administrador tienen acceso total.

Acceso autorizado para los administradores

Acceso de administrador a la consola

Los administradores pueden acceder a todas las funciones de la consola de Citrix Endpoint Management.

Acceso al portal Self Help Portal

De forma predeterminada, los administradores no pueden acceder a Self Help Portal (los usuarios con el [rol Usuario](#) pueden acceder solamente a Self Help Portal).

Acceso a Remote Support	Los administradores tienen acceso a la función Remote Support.
Acceso a API públicas	Los administradores pueden acceder a la API pública para llevar a cabo, previa programación, acciones disponibles en la consola de Citrix Endpoint Management. Esas acciones pueden ser: administración de certificados, licencias, aplicaciones, dispositivos, grupos de entrega y usuarios locales.

Funciones de consola para administradores Los administradores tienen acceso sin restricciones a todas las funciones de la consola de Citrix Endpoint Management.

Panel de mandos	El panel de mandos es la primera página que los administradores ven después de iniciar sesión en la consola de Citrix Endpoint Management. El panel de pandos muestra información básica sobre notificaciones y dispositivos.
Informes	En la página Análisis > Informes , se ofrecen informes predefinidos que permiten analizar las implementaciones de dispositivos y aplicaciones.
Dispositivos	La página Administrar > Dispositivos es donde se administran los dispositivos de los usuarios. En esta página, puede agregar dispositivos individuales o importar un archivo de aprovisionamiento de dispositivos para agregar varios dispositivos a la vez.
Grupos y usuarios locales	La página Administrar > Usuarios es donde se agregan, modifican o eliminan usuarios locales y grupos de usuarios locales.
Inscripción	La página Administrar > Invitaciones de inscripción es donde se define cómo invitar a los usuarios a inscribir sus dispositivos en Citrix Endpoint Management.

Directivas	La página Configurar > Directivas de dispositivo es donde se gestionan las directivas de los dispositivos; por ejemplo, directivas de VPN y de redes.
Aplicación	La página Configurar > Aplicaciones es donde se administran las varias aplicaciones que los usuarios pueden instalar en sus dispositivos.
Archivos multimedia	La página Configurar > Multimedia es donde se administran los medios para contenido multimedia que los usuarios pueden instalar en sus dispositivos.
Acción	La página Configurar > Acciones es donde se administran las respuestas para desencadenar eventos.
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	En la página Configurar > Perfiles de inscripción se especifica de qué forma los usuarios pueden inscribir sus dispositivos.
Alexa for Business	La página Parámetros es donde se administran los perfiles de Alexa for Business.
Parámetros	La página Parámetros es donde se definen los parámetros del sistema (como propiedades de cliente y servidor, certificados y proveedores de credenciales). Importante: Estos parámetros incluyen el permiso RBAC. El permiso RBAC otorga acceso total a los administradores, incluida la capacidad de asignar sus propios permisos. Conceda este acceso solamente a los usuarios a los que quiere dar la capacidad de manipular todo lo que hay en el sistema de Citrix Endpoint Management.
Asistencia	La página Solución de problemas y asistencia es donde se realizan las actividades de solución de problemas (como ejecutar diagnósticos y generar registros).

Restricciones de dispositivos para administradores Los administradores acceden a las funciones de los dispositivos mediante la consola. Desde ella, pueden establecer restricciones para los dispositivos, configurar y enviar notificaciones a los dispositivos y administrar las aplicaciones presentes en los dispositivos, entre otros.

Borrado completo de dispositivo	Borra todos los datos y aplicaciones de un dispositivo, incluidas las tarjetas de memoria (si el dispositivo las tuviera).
Borrar restricción	Quita una o varias restricciones de dispositivo.
Borrado selectivo de dispositivo	Borra todas las aplicaciones y datos empresariales del dispositivo, pero no afecta a las aplicaciones y datos personales.
Ver ubicaciones	Muestra la ubicación y establece restricciones geográficas en el dispositivo. Incluye: Localizar dispositivo, Seguimiento del dispositivo.
Bloquear dispositivo	Bloquea remotamente un dispositivo de modo que los usuarios no puedan usarlo.
Desbloquear dispositivo	Desbloquea remotamente un dispositivo de modo que los usuarios puedan usarlo.
Bloquear contenedor	Bloquea remotamente el contenedor de datos empresariales de un dispositivo.
Desbloquear contenedor	Desbloquea remotamente el contenedor de datos empresariales de un dispositivo.
Restablecer contraseña de contenedor	Restablece la contraseña del contenedor de datos empresariales.
Habilitar anulación del bloqueo de activación de ASM	En un dispositivo iOS supervisado, almacena un código de circunvalación cuando habilite el Bloqueo de activación. Si necesita borrar el dispositivo, use este código para quitar automáticamente el Bloqueo de activación.
Obtener usuarios residentes	Ofrece una lista de 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	Obliga al cierre de sesión del usuario actual.

Eliminar usuario residente	Elimina la sesión actual de un usuario específico. El usuario puede volver a iniciar sesión.
Hacer sonar el dispositivo	Hace sonar remotamente un dispositivo Windows al máximo volumen durante 5 minutos.
Reiniciar el dispositivo	Reinicia los dispositivos Windows desde la consola de Citrix Endpoint Management.
Implementar en dispositivo	Envía aplicaciones, notificaciones y restricciones, entre otros, a un dispositivo.
Modificar dispositivo	Modifica los parámetros de un dispositivo.
Notificación a dispositivo	Envía una notificación a un dispositivo.
Agregar o quitar dispositivo	Agrega o quita dispositivos de Citrix Endpoint Management.
Importar dispositivos	Importa, en Citrix Endpoint Management, un grupo de dispositivos a partir de un archivo.
Exportar tabla de dispositivos	Recaba información sobre dispositivos a partir de la página “Dispositivos” y la exporta en un archivo CSV.
Revocar dispositivo	Prohíbe a un dispositivo que se conecte a Citrix Endpoint Management.
Bloqueo de aplicaciones	Deniega el acceso a todas las aplicaciones de un dispositivo. En Android, esta restricción impide a los usuarios iniciar sesión en Citrix Endpoint Management. En iOS, los usuarios pueden iniciar sesión, pero no pueden acceder a las aplicaciones.
Borrado de aplicaciones	En Android, esta restricción elimina la cuenta de Citrix Endpoint Management del usuario. En iOS, esta restricción elimina la clave de cifrado que los usuarios necesitan para acceder a las funciones de Citrix Endpoint Management.
Ver inventario de software	Muestra el software instalado en un dispositivo.
Solicitar duplicación AirPlay	Solicita iniciar el streaming de AirPlay.
Detener duplicación AirPlay	Detiene el streaming de AirPlay.

Habilitar el modo perdido	En la página Administrar > Dispositivos , puede colocar un dispositivo supervisado en modo perdido para bloquearlo en la pantalla de bloqueo. Después, puede localizar el dispositivo en caso de hurto o pérdida de este.
Inhabilitar el modo perdido	En la página Administrar > Dispositivos , puede inhabilitar el modo perdido de un dispositivo establecido en ese modo.
Actualización de SO del dispositivo	Puede implementar una directiva de actualización del SO en los dispositivos.
Apagar dispositivo	Apaga los dispositivos iOS desde la consola de Citrix Endpoint Management.
Reiniciar dispositivo	Reinicia los dispositivos iOS desde la consola de Citrix Endpoint Management.
Renovar certificado de inscripción de dispositivos	Renueva un certificado de CA del dispositivo.

Grupos y usuarios locales La página **Administrar > Usuarios** es donde se administran usuarios locales y grupos de usuarios locales en 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 usuarios y exportar la tabla de inscripción en un archivo CSV.

Agregar o eliminar inscripción	Agrega o quita una invitación de inscripción a usuarios o grupos de usuarios.
Notificar al usuario	Envía una invitación de inscripción a usuarios o grupos de usuarios.
Exportar la tabla de invitaciones de inscripción	Recaba información sobre inscripciones a partir de la página “Inscripción” y la exporta en un archivo CSV.

Directivas

Agregar o eliminar directiva	Agrega o quita una directiva de dispositivo o de aplicación.
Modificar directiva	Cambia una directiva de dispositivo o de aplicación.
Cargar directiva	Carga una directiva de dispositivo o de aplicación.
Clonar directiva	Copia una directiva de dispositivo o de aplicación.
Inhabilitar directiva	Inhabilita una directiva existente de aplicación.
Exportar directiva	Recaba información sobre directivas de dispositivo a partir de la página “Directivas de dispositivo” y la exporta en un archivo CSV.
Asignar directiva	Asigna una directiva de dispositivo a uno o varios grupos de entrega.

Aplicación En Citrix Endpoint Management, los administradores gestionan las aplicaciones desde la página **Configurar > Aplicaciones**.

Agregar o eliminar aplicaciones empresariales o de almacenes de aplicaciones	Agrega o quita una aplicación de tienda pública de aplicaciones o una aplicación de empresa (no habilitada para MDX).
--	---

Modificar aplicaciones empresariales o de almacén de aplicaciones	Modifica una aplicación de tienda pública de aplicaciones o una aplicación de empresa (no habilitada para MDX).
Agregar/eliminar aplicación MDX, web y SaaS	Agrega/quita una aplicación habilitada para MDX, una aplicación de su red interna (aplicación web) o una aplicación de una red pública (SaaS) a/de Citrix Endpoint Management.
Modificar aplicaciones MDX, web y SaaS	Modifica 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.
Agregar o quitar categoría	Agrega o elimina una categoría en que pueden aparecer aplicaciones en el almacén de aplicaciones.
Asignar aplicación pública o de empresa a grupo de entrega	Asigna una aplicación de tienda pública de aplicaciones o una aplicación habilitada para MDX a un grupo de entrega para su implementación.
Asignar aplicación MDX, de enlace web o SaaS a grupo de entrega	Asigna a un grupo de entrega una aplicación habilitada para MDX, que no requiere Single Sign-On (WebLink) o proveniente de una red pública (SaaS).
Exportar tabla de aplicaciones	Recaba información sobre aplicaciones a partir de la página Apps y la exporta en un archivo CSV.

Archivos multimedia Administra el contenido multimedia de un tienda pública de aplicaciones o de una licencia de compras por volumen.

Agregar o eliminar libros de empresa o de almacén de aplicaciones

Asignar libros públicos/de empresa a grupo de entrega

Modificar libros de empresa o de almacén de aplicaciones

Acción

Agregar/eliminar acción	Agregar o quitar una acción definida por un desencadenante y una respuesta asociada. Un desencadenante es un evento, una propiedad de dispositivo o usuario, o un nombre de aplicación instalada.
Modificar acción	Cambiar una acción definida por un desencadenante y una respuesta asociada. Un desencadenante es un evento, una propiedad de dispositivo o usuario, o un nombre de aplicación instalada.
Asignar acción a grupo de entrega	Asigna una acción a un grupo de entrega para la implementación en los dispositivos de los usuarios.
Exportar acción	Recaba información sobre acciones a partir de la página “Acciones” y la exporta en un archivo CSV.

Grupo de entrega Los administradores gestionan los grupos de entrega desde la página **Configurar > Grupos de entrega**.

Agregar o eliminar grupo de entrega	Crea o elimina un grupo de entrega, que agrega usuarios concretos y acciones, aplicaciones y directivas opcionales.
Modificar grupo de entrega	Modifica un grupo de entrega existente, lo que modifica usuarios y acciones, aplicaciones y directivas opcionales.
Implementar grupo de entrega	Pone el grupo de entrega disponible para su uso.
Exportar grupo de entrega	Recaba información sobre grupos de entrega a partir de la página “Grupo de entrega” y la exporta en un archivo CSV.

Perfil de inscripción Administra perfiles de inscripción.

Agregar/eliminar perfil de inscripción

Modificar perfil de inscripción

Asignar perfil de inscripción a grupo de entrega

Alexa for Business Administrar perfiles de Alexa for Business.

Agregar/eliminar/modificar salas

Agregar/eliminar/modificar perfiles de sala

Agregar/eliminar/modificar grupos de skills

Parámetros para administradores Los administradores configuran diferentes parámetros en la página **Parámetros**.

RBAC	Asignación de RBAC. Importante: Este permiso otorga acceso total a los administradores, incluida la capacidad de asignar sus propios permisos. Conceda este acceso solamente a los usuarios a los que quiere dar la capacidad de manipular todo lo que hay en el sistema de Citrix Endpoint Management.
LDAP	Administra uno o varios directorios que cumplen el protocolo LDAP (como Active Directory) para importar grupos, cuentas de usuario y propiedades relacionadas.
Inscripción	Habilita el portal Self Help Portal y los modos de seguridad de inscripción para usuarios.
Administración de versiones	Muestra la versión actual instalada. Incluye:
Certificados	Actualización de administración de versiones
	Modificar certificado APNS

Plantillas de notificaciones	Crea plantillas de notificaciones para utilizarlas en acciones automatizadas, inscripciones y la entrega de mensajes de notificación estándar a los usuarios.
Flujos de trabajo	Administra la creación, la aprobación y la eliminación de cuentas de usuario a utilizar con configuraciones de aplicaciones.
Proveedores de credenciales	Agrega uno o varios proveedores de credenciales autorizados para emitir certificados de dispositivo. Los proveedores de credenciales controlan el formato de los certificados y las condiciones de renovación o revocación de estos.
Entidades de PKI	Administra entidades de infraestructura de clave pública (genéricas, de Microsoft Certificate Services o entidades de certificación discrecional).
Probar conexión de PKI	Use el botón Probar conexión , ubicado en la página Parámetros > Entidades de PKI , para asegurarse de que es posible acceder al servidor.
Propiedades de cliente	Administra diferentes propiedades en los dispositivos de los usuarios, como el tipo de código de acceso, su nivel de seguridad o su caducidad.
Asistencia del cliente	Establece las maneras en que los usuarios pueden ponerse en contacto con los servicios de asistencia (teléfono, correo electrónico o correo de tíquet de asistencia).
Personalización de marca de clientes	Puede crear un nombre de almacén personalizado y vistas predeterminadas del almacén de aplicaciones. Agrega un logotipo personalizado que aparecerá en el almacén de aplicaciones o Citrix Secure Hub.
Puerta de enlace SMS del operador	Establece puertas de enlace SMS del operador para configurar notificaciones que Citrix Endpoint Management envía a través de ellas.
Servidor de notificaciones	Establece una puerta de enlace SMTP para enviar correos electrónicos a los usuarios.

ActiveSync Gateway	Administra el acceso de usuario a usuarios y dispositivos con ayuda de reglas y propiedades.
Google Chrome	Configure Citrix Endpoint Management para comunicarse con su cuenta de Google Workspace.
Programa de implementación de Apple	Agrega una cuenta del Programa de implementación de Apple a Citrix Endpoint Management.
Inscripción de dispositivos en Apple Configurator	Configure parámetros de Apple Configurator en la consola de Citrix Endpoint Management.
Configuración de compras por volumen de iOS	Agrega cuentas de compras por volumen de Apple.
NetScaler Gateway	Configura los parámetros de NetScaler Gateway (ahora denominado NetScaler Gateway) en Citrix Endpoint Management.
Control de acceso de red	Establece las condiciones que determinan si un dispositivo no cumple las condiciones de modo que no pueda acceder a la red.
Propiedades de servidor	Agrega o modifica las propiedades de servidor. Requiere reiniciar Citrix Endpoint Management en todos los nodos.
Aplicaciones y escritorios virtuales	Permite que los usuarios agreguen aplicaciones y escritorios virtuales de Citrix Virtual Apps and Desktops a través de la aplicación Citrix Workspace.

Citrix Files	Cuando se usa Citrix Endpoint Management con cuentas Enterprise: Configure los parámetros para conectarse a ShareFile y a las cuentas de servicio de administrador para la administración de cuentas de usuario. Requiere las credenciales existentes de administrador y el dominio de Citrix Files. Cuando se utiliza Citrix Endpoint Management con conectores de zonas de almacenamiento: Configure Citrix Endpoint Management para que apunte a los recursos compartidos de red y a las ubicaciones de SharePoint definidas en los conectores de zonas de almacenamiento.
Android Enterprise	Configura parámetros de servidor Android Enterprise.
Proveedor de identidades (IDP)	Configura un proveedor de identidades.
Herramientas de Citrix Endpoint Management	Accede a la página Citrix Endpoint Management Tools.
Inscripción en bloque de Windows	Configura los parámetros de inscripción en bloque para Windows.

Asistencia Los administradores pueden llevar a cabo varias tareas de asistencia.

Comprobaciones de conectividad de NetScaler Gateway	Realiza varias comprobaciones de conectividad de NetScaler Gateway mediante la dirección IP. Requiere nombre de usuario y contraseña.
Comprobaciones de conectividad de Citrix Endpoint Management	Realiza comprobaciones de conectividad de funciones seleccionadas de Citrix Endpoint Management (como la base de datos, DNS o Google Plan).
Documentación sobre los productos Citrix	Accede al sitio público de documentación de Citrix Endpoint Management.
Citrix Knowledge Center	Accede al sitio de asistencia de Citrix para buscar artículos de la base de conocimientos.

Registros	Ver y descargar archivos de registros.
Macros	Rellena datos de dispositivo o usuario en el campo de texto de un perfil, directiva, notificación o plantilla de inscripción. Configure una sola directiva e impleméntela en una gran base de usuarios. Así, obtendrá valores específicos para cada usuario de destino.
Configuración de PKI	Importa y exporta información de la configuración de PKI.
Utilidad de firma APNS	Envía una solicitud de certificados de firma Apple Push Network (APNs) o carga un certificado APNs de Citrix Secure Mail para iOS.
Citrix Insight Services	Carga registros en Citrix Insight Services (CIS) para obtener asistencia con diferentes problemas.
Estado del dispositivo del conector de NetScaler Gateway para Exchange ActiveSync	Envía consultas a Citrix Endpoint Management sobre el estado de un dispositivo enviado al conector de Exchange ActiveSync. La consulta se basa en el ID de ActiveSync del dispositivo.

Restringir acceso de grupos Los usuarios administradores pueden aplicar permisos a todos los grupos de usuarios.

Funciones de consola para el aprovisionamiento de dispositivos Los usuarios con el rol de aprovisionamiento de dispositivos tienen restringido el acceso a las siguientes funciones de la consola de Citrix Endpoint Management. De forma predeterminada, cada una de las siguientes funciones está habilitada.

Restricciones de dispositivo

Modificar dispositivo	Modifica los parámetros de un dispositivo.
Agregar o quitar dispositivo	Agrega o quita dispositivos de Citrix Endpoint Management.

Parámetros para el aprovisionamiento de dispositivos Los usuarios con el rol de aprovisionamiento de dispositivos pueden acceder a la página **Parámetros**, pero no tienen los derechos necesarios para 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

Self Help Portal	Da a los usuarios acceso solamente al portal Self Help Portal en Citrix Endpoint Management.
------------------	--

Funciones de la consola para usuarios Los usuarios tienen el siguiente acceso restringido a la consola de Citrix Endpoint Management.

Acceso restringido de dispositivos para usuarios

Borrado completo de dispositivo	Borra todos los datos y aplicaciones de un dispositivo, incluidas las tarjetas de memoria (si el dispositivo las tuviera).
Borrado selectivo de dispositivo	Borra todas las aplicaciones y datos empresariales del dispositivo, pero no afecta a las aplicaciones y datos personales.
Ver ubicaciones	Muestra la ubicación y establece restricciones geográficas en el dispositivo. Inclúa: Localizar dispositivos (ver la ubicación de un dispositivo) y Seguimiento de dispositivos (realizar el seguimiento de la ubicación de un dispositivo a lo largo del tiempo).
Bloquear dispositivo	Bloquea remotamente un dispositivo de modo que no se pueda usar.
Desbloquear dispositivo	Desbloquea remotamente un dispositivo de modo que se pueda usar.

Bloquear contenedor	Bloquea remotamente el contenedor de datos empresariales de un dispositivo.
Desbloquear contenedor	Desbloquea remotamente el contenedor de datos empresariales de un dispositivo.
Restablecer contraseña de contenedor	Restablece la contraseña del contenedor de datos empresariales.
Habilitar anulación del bloqueo de activación de ASM	En un dispositivo iOS supervisado, almacena un código de circunvalación cuando habilite el Bloqueo de activación. Si necesita borrar el dispositivo, use este código para quitar automáticamente el Bloqueo de activación.
Obtener usuarios residentes	Ofrece una lista de 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	Obliga al cierre de sesión del usuario actual.
Eliminar usuario residente	Elimina la sesión actual de un usuario específico. El usuario puede volver a iniciar sesión.
Hacer sonar el dispositivo	Hace sonar remotamente un dispositivo Windows al máximo volumen durante 5 minutos.
Reiniciar el dispositivo	Reinicia un dispositivo Windows.
Bloqueo de aplicaciones	Deniega 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 aplicaciones	En Android, esta restricción elimina la cuenta de Citrix Endpoint Management del usuario. En iOS, esta restricción elimina la clave de cifrado que los usuarios necesitan para acceder a las funciones de Citrix Endpoint Management.
Ver inventario de software	Muestra el software instalado en un dispositivo.

Restricciones de inscripción para usuarios

Agregar o eliminar inscripción

Agrega o quita una invitación de inscripción a usuarios o grupos de usuarios.

Notificar al usuario

Envía una invitación de inscripción a usuarios o grupos de usuarios.

Restringir el acceso de grupos para todos los roles En el caso de los roles predefinidos, este permiso está configurado de forma predeterminada y puede aplicarse a todos los grupos de usuarios. No se puede modificar el rol.

Licencias

November 29, 2023

Para obtener información sobre el uso de licencias de Citrix, consulte:

- [Supervisar el uso activo y de licencias en los servicios de la nube](#)
- [Supervisar uso activo y de licencias en Citrix Endpoint Management](#)

Administración de dispositivos

March 1, 2024

Citrix Endpoint Management puede aprovisionar, proteger e inventariar una amplia gama de tipos de dispositivo desde una sola consola de administración.

- Puede utilizar un conjunto común de directivas de dispositivo para administrar los dispositivos compatibles. Para ver rápidamente las directivas de dispositivo disponibles por plataforma:
 1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Directivas de dispositivo**.
 2. Haga clic en **Agregar** y, a continuación, seleccione las plataformas que quiera ver.

Para obtener más información, consulte [Filtrar la lista de las directivas de dispositivo agregadas](#).

- Puede proteger la información de su empresa gracias a reglas de seguridad estrictas en cuanto a la identidad, los dispositivos de la empresa y BYOD, las aplicaciones, los datos y las redes. Para ello, especifique la identidad de usuario que se utilizará para autenticarse en los dispositivos y defina cómo mantener separados los datos personales y de empresa en los dispositivos.
- Entregue aplicaciones a los usuarios finales, independientemente del dispositivo o sistema operativo. Puede proteger su información al nivel de aplicación al mismo tiempo que ofrece una administración de aplicaciones móviles al nivel de toda la empresa.
- Puede utilizar unos controles de aprovisionamiento y configuración para configurar los dispositivos. Estos controles incluyen la inscripción de dispositivos, la aplicación de directivas y los privilegios de acceso.
- Puede utilizar controles de seguridad y cumplimiento para crear un nivel base de seguridad personalizado gracias a desencadenantes basados en acciones. Por ejemplo, puede bloquear un dispositivo, borrar los datos que contenga o notificar al usuario de ese dispositivo de que no cumple las reglas de cumplimiento definidas.
- Puede utilizar controles de actualización del sistema operativo para impedir o aplicar actualizaciones a los sistemas operativos. Esta función es fundamental para prevenir la pérdida de datos causada por vulnerabilidades específicas de cada sistema operativo.

Para acceder a los artículos referentes a cada plataforma compatible, expanda la sección “Administrar dispositivos” en el índice de contenido. En esos artículos se ofrecen datos específicos sobre cada plataforma de dispositivo. En el resto de este artículo se describe cómo realizar tareas generales de administración de dispositivos.

Flujos de trabajo de administración de dispositivos

En los diagramas de flujo de trabajo que contiene esta sección se ofrece una secuencia recomendada para tareas de administración de dispositivos.

1. **Requisitos previos recomendados para agregar dispositivos y aplicaciones:** Realizar la siguiente configuración de antemano permite configurar dispositivos y aplicaciones sin causar interrupciones en el servicio.



Consulte:

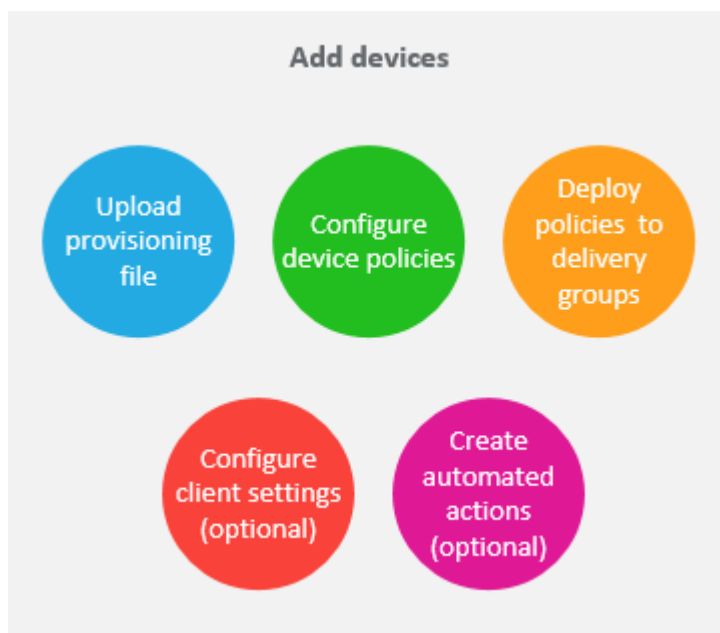
[Implementar recursos](#)

[Configurar roles con RBAC](#)

[Crear y actualizar plantillas de notificaciones](#)

[Crear y administrar flujos de trabajo](#)

2. Agregar dispositivos:



Consulte:

[Preparar la inscripción de dispositivos y la entrega de recursos](#)

[Directivas de dispositivo](#)

[Implementación 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 heredado. Haga esto si piensa usar invitaciones de inscripción.

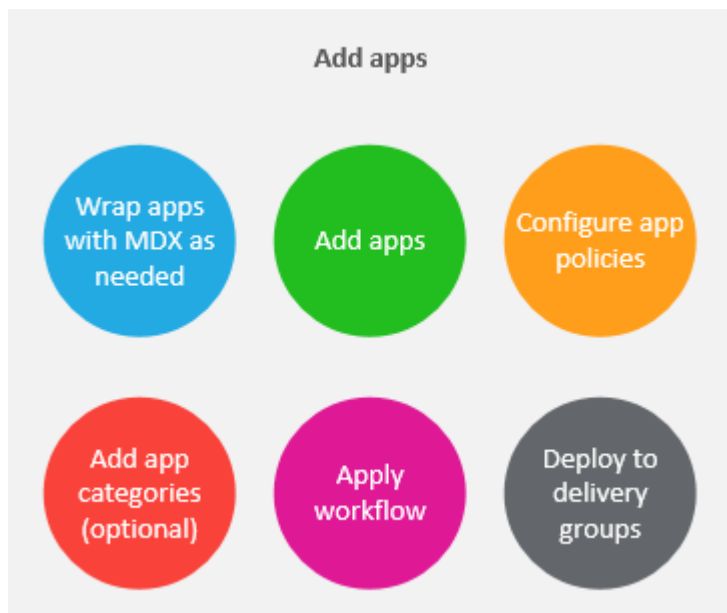


Consulte:

[Configurar modos de seguridad de inscripción](#)

[Enviar una notificación a dispositivos](#)

4. **Agregar aplicaciones:**



Consulte:

[SDK de MAM](#)

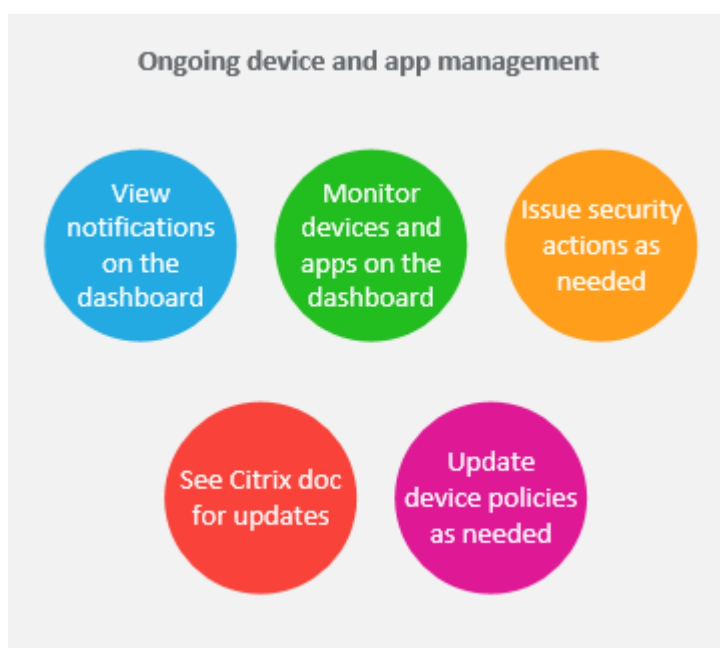
[Agregar aplicaciones](#)

[Acerca de las categorías de aplicaciones](#)

[Aplicar flujos de trabajo](#)

[Implementación en grupos de entrega](#)

5. **Realizar una administración continua de dispositivos y aplicaciones:** Además de utilizar el panel de control de Citrix Endpoint Management, se le recomienda consultar el contenido de [Novedades](#) de cada versión. El artículo “Novedades” ofrece información sobre las acciones necesarias, como la configuración de nuevas directivas de dispositivo.



Consulte:

[Supervisar y ofrecer asistencia](#)

[Informes](#)

[Acciones de seguridad](#)

[Novedades](#)

[Directivas de dispositivo](#)

Invitaciones de inscripción

Para poder administrar dispositivos del usuario de forma remota y segura, dichos dispositivos deben inscribirse en Citrix Endpoint Management. El software cliente de Citrix Endpoint Management debe

estar instalado en el dispositivo del usuario y el usuario debe haberse autenticado. A continuación, se instalan Citrix Endpoint Management y el perfil del usuario. Para obtener detalles de inscripción para plataformas de dispositivos compatibles, consulte los artículos de dispositivos en esta sección.

En la consola de Citrix Endpoint Management:

- Puede enviar una invitación de inscripción a usuarios de 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 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, recibirán la invitación. Los usuarios locales reciben la invitación en el correo electrónico especificado en las propiedades de usuario.

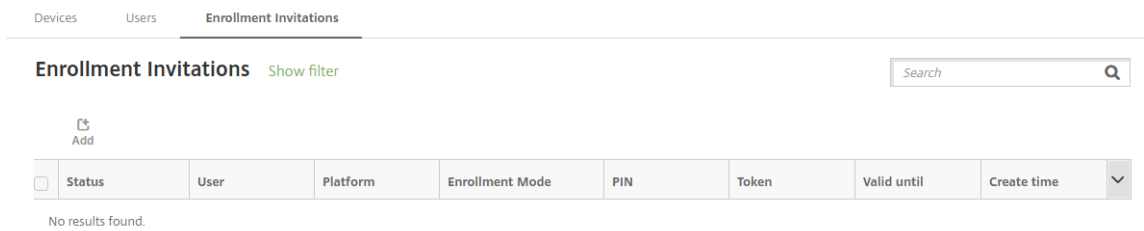
Después de que los usuarios se inscriban, sus dispositivos aparecen como administrados en **Administrar > Dispositivos**. El estado de la URL de invitación aparece como **Canjeado**.

Requisitos previos

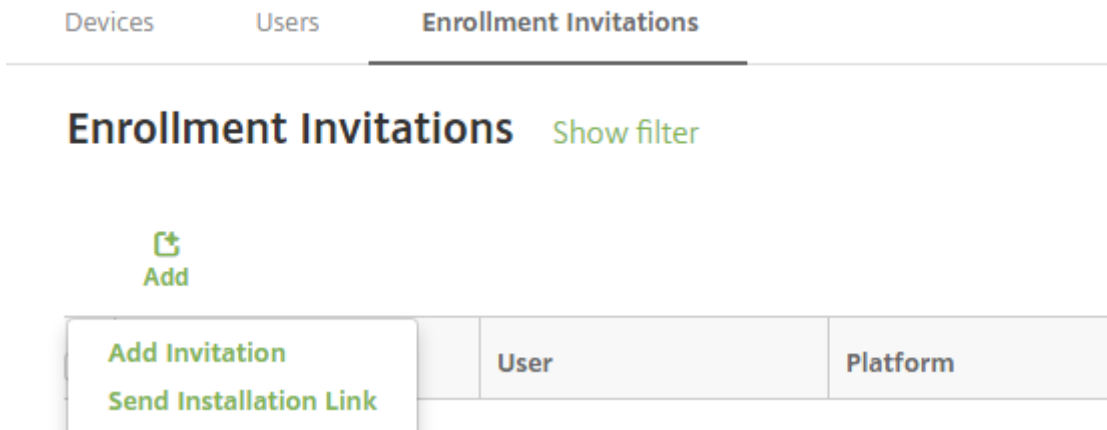
- LDAP configurado
- Si utiliza grupos y usuarios locales:
 - Uno o varios grupos locales.
 - Usuarios locales asignados a grupos locales.
 - Los grupos de entrega se asocian con grupos locales.
- Si usa Active Directory:
 - Los grupos de entrega se asocian con grupos de Active Directory.

Crear invitación de inscripción

1. En la consola de Citrix Endpoint Management, haga clic en **Administrar > Inscripciones**. Aparecerá la página **Invitaciones de inscripción**.



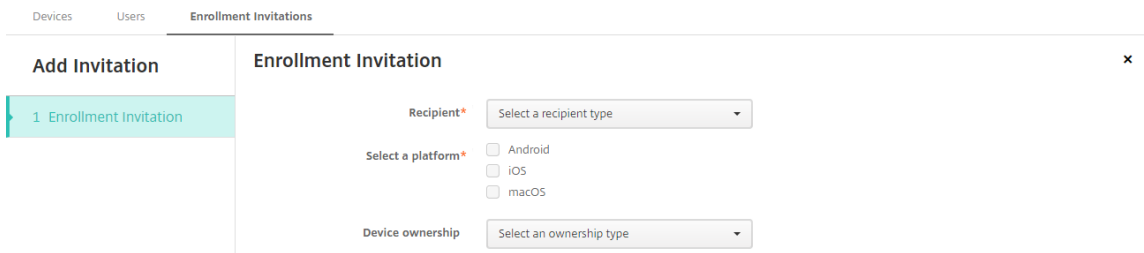
2. Haga clic en **Agregar**. Aparecerá un menú con opciones de inscripción.



- Para enviar una invitación de inscripción a un usuario o un grupo, haga clic en **Agregar invitación**.
- Si quiere enviar un enlace de instalación para la 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 parámetros:

- **Destinatario:** Elija **Grupo** o **Usuario**.
- **Seleccionar una plataforma:** Si el **Destinatario** es un **Grupo**, se seleccionan todas las plataformas. Puede cambiar las plataformas seleccionadas. Si el **Destinatario** es un **Usuario**, no se selecciona ninguna plataforma. Seleccione una plataforma.

Para crear una invitación de inscripción para dispositivos Android Enterprise, seleccione **Android**.

- **Propietario del dispositivo:** Seleccione **Empresa** o **Empleado**.

Aparecerán parámetros para usuarios o grupos, como se describe en las secciones siguientes.

Para enviar una invitación de inscripción a un usuario

The screenshot shows the 'Add Invitation' form in the Citrix Endpoint Management console. The 'Enrollment Invitation' tab is selected. The form includes the following fields and options:

- Recipient***: A dropdown menu with 'User' selected.
- Select a platform***: Three radio buttons for 'Android', 'iOS', and 'macOS'.
- Device ownership**: A dropdown menu with 'Select an ownership type'.
- User name***: A text input field with a help icon.
- Enrollment mode***: A dropdown menu with 'User name + Password' selected.
- Template for agent download**: A dropdown menu with 'Select a template'.
- Template for enrollment URL**: A dropdown menu with 'Select a template'.
- Template for enrollment confirmation**: A dropdown menu with 'Select a template'.
- Expire after**: A dropdown menu with 'Never' selected.
- Maximum Attempts**: A text input field with '0'.
- Send invitation**: A toggle switch currently set to 'OFF'.

1. Configure estos parámetros 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, defina la propiedad de correo electrónico del usuario de forma acorde para poder enviarle notificaciones. Si el usuario está en Active Directory, si LDAP está configurado.
- **Número de teléfono:** Este parámetro no aparece si se selecciona más de una plataforma o si se selecciona solo macOS. Si quiere, introduzca el número de teléfono del usuario.
- **Operador:** Este parámetro no aparece si se seleccionan varias plataformas, o si se selecciona solo macOS. Seleccione un operador para asociarlo con el 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 y contraseña**. Algunas de las siguientes opciones no están disponibles para todas las plataformas:
 - **Nombre de usuario y contraseña**
 - **URL de invitación**

- **URL de invitación y PIN**
- **URL de invitación y contraseña**
- **Dos factores**
- **Nombre de usuario + PIN**

Hemos retirado el modo de inscripción **Alta seguridad**. Para enviar invitaciones de inscripción, puede utilizar solamente 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 manualmente sus credenciales.

Para obtener más información, consulte [Modos de seguridad de inscripción por plataforma](#). Un PIN de inscripción se denomina también un PIN de un solo uso. Este tipo de PIN es válido solamente cuando se inscribe el usuario.

Nota:

Cuando seleccione un modo de seguridad de inscripción que incluya un PIN, aparecerá el campo **Plantilla para PIN de inscripción**. Deberá hacer 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 URL de inscripción:** Elija **Invitación de inscripción**.
 - **Plantilla para confirmación de la inscripción:** Elija **Confirmación de la inscripción**.
 - **Caduca después de:** Este campo se establece cuando se configura el modo de seguridad de inscripción y se indica cuándo caduca la inscripción. Para obtener más información sobre cómo configurar modos de seguridad de inscripción, consulte [Configurar modos de seguridad de inscripción](#).
 - **Máximo de intentos:** Este campo se define al configurar el modo de seguridad de inscripción e indica el máximo de veces que tiene lugar el proceso de inscripción.
 - **Enviar invitación:** **Active** la opción para enviar la invitación inmediatamente. **Desactívela** para agregar la invitación a la tabla en la página **Invitaciones de inscripción** sin enviarla.
2. Haga clic en **Guardar y enviar** si habilitó **Enviar invitación**. De lo contrario, haga clic en **Guardar**. La invitación aparecerá en la tabla de la página **Invitaciones de inscripción**.

DevicesUsersEnrollment Invitations

Enrollment Invitations

Show filter

Search

Q

AddExport

<input type="checkbox"/>	Status	User	Platform	Enrollment Mode	PIN	Token	Valid until	Create time	▼
<input type="checkbox"/>	PENDING		Android	User name + Password				05/03/2017 10:32:24 am	
<input type="checkbox"/>	PENDING		macOS	User name + Password				05/01/2017 07:33:38 pm	
<input type="checkbox"/>	PENDING		iOS	User name + Password				05/01/2017 07:29:02 pm	

Para enviar una invitación de inscripción a un grupo

En la imagen siguiente, se muestran los parámetros de una invitación de inscripción para un grupo.

DevicesUsersEnrollment Invitations

Add Invitation

1 Enrollment Invitation

Enrollment Invitation

Recipient*

Group

Select a platform*

☒ Android☒ iOS☒ macOS

Device ownership

Select an ownership type

Domain*

Select a domain

Group*

Select a group

Enrollment mode*

User name + Password

Template for agent download

Select a template

Template for enrollment URL

Select a template

Template for enrollment confirmation

Select a template

Expire after

Never

Maximum Attempts

0

Send invitation

OFF

1. Configure estos parámetros:
- **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 quiere que se inscriban los usuarios del grupo. El valor predeterminado es **Nombre de usuario y contraseña**. Algunas de las siguientes opciones no están disponibles para todas las plataformas:
 - **Nombre de usuario y contraseña**
 - **URL de invitación**

- **URL de invitación y PIN**
- **URL de invitación y contraseña**
- **Dos factores**
- **Nombre de usuario + PIN**

Hemos retirado el modo de inscripción **Alta seguridad**. Para enviar invitaciones de inscripción, puede utilizar solamente 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 manualmente sus credenciales.

Solo aparecen los modos de seguridad de inscripción que son válidos para cada plataforma seleccionada. Para obtener más información, consulte [Modos de seguridad de inscripción por plataforma](#).

Nota:

Cuando seleccione un modo de seguridad de inscripción que incluya un PIN, aparecerá el campo **Plantilla para PIN de inscripción**. Deberá hacer 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 URL de inscripción:** Elija **Invitación de inscripción**.
 - **Plantilla para confirmación de la inscripción:** Elija **Confirmación de la inscripción**.
 - **Caduca después de:** Este campo se establece cuando se configura el modo de seguridad de inscripción y se indica cuándo caduca la inscripción. Para obtener más información sobre cómo configurar modos de seguridad de inscripción, consulte [Configurar modos de seguridad de inscripción](#).
 - **Máximo de intentos:** Este campo se define al configurar el modo de seguridad de inscripción e indica el máximo de veces que tiene lugar el proceso de inscripción.
 - **Enviar invitación:** **Active** la opción para enviar la invitación inmediatamente. **Desactívela** para agregar la invitación a la tabla en la página **Invitaciones de inscripción** sin enviarla.
2. Haga clic en **Guardar y enviar** si habilitó **Enviar invitación**. De lo contrario, haga clic en **Guardar**. La invitación aparecerá en la tabla de la página **Invitaciones de inscripción**.

DevicesUsersEnrollment Invitations










Devices

Show filter

Search

Q

AddImportExportRefresh

	Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP account name	
<input type="checkbox"/>	  	MDM MAM			iOS	10.1.1	iPad	01/20/2017 02:00:09 pm	2 days	Default DEP Account	
<input type="checkbox"/>	  	MDM MAM			iOS	10.1.1	iPhone	12/15/2016 05:14:24 pm	38 days		
<input type="checkbox"/>	  	MDM MAM			iOS	10.1.1	iPhone	01/20/2017 02:51:41 pm	2 days		

Showing 1 - 3 of 3 itemsItems per page: 10

Para enviar un enlace de instalación

Para poder enviar un enlace de instalación para la inscripción, antes debe configurar canales (SMTP) en el servidor de notificaciones. Puede hacerlo desde la página **Parámetros**. Para obtener más información, consulte [Notificaciones](#).

DevicesUsersEnrollment Invitations

Send Link

1 Details

Send Installation Link

Recipients *

Email *Phone number *Add

Channels

SMTP

Channel cannot be activated until you define the SMTP server in the Notification Server section in Settings.

Sender

Subject

Enroll Your Device

Message

Enroll your device to gain access to company email and intranet. For instructions visit: \${zdmserver.hostPath}/enroll

SMS

Channel cannot be activated until you define the SMS server in the Notification Server section in Settings.

Message

Download XenMobile Agent: \${zdmserver.hostPath}/enroll

1. Configure estos parámetros y haga clic en **Guardar**.
- **Destinatario:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada destinatario:

– **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.
- © 1999–2024 Cloud Software Group, Inc. All rights reserved.

318

Nota:

Para eliminar un destinatario existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. Aparecerá un cuadro de diálogo de confirmación. Haga clic en **Eliminar** para eliminar el elemento, o bien haga clic en **Cancelar** para conservarlo.

Para modificar un destinatario, coloque el cursor sobre la línea que lo contiene. A continuación, haga clic en el icono de lápiz situado a la derecha. Realice los cambios necesarios y, a continuación, haga clic en **Guardar** para guardar los cambios, o bien en **Cancelar** para descartarlos.

- **Canales:** Seleccione el canal que se va a usar para enviar el enlace de instalación para la inscripción. Puede enviar notificaciones a través de **SMTP**. Estos canales no se pueden activar hasta que se configuren los parámetros de servidor en la página **Parámetros**, en **Servidor de notificaciones**. Para obtener más información, consulte [Notificaciones](#).
- **SMTP:** La configuración de estos parámetros es opcional. Si no escribe nada en estos campos, se utilizarán los valores predeterminados que haya especificado en la plantilla de notificaciones definida para la plataforma seleccionada:
 - **Remitente:** Escriba un remitente opcional.
 - **Asunto:** Aquí puede escribir un asunto para el mensaje. Por ejemplo: “Inscriba su dispositivo”.
 - **Mensaje:** Escriba el mensaje opcional que se enviará al destinatario. Por ejemplo: “Inscriba su dispositivo para tener acceso a las aplicaciones y al correo electrónico de la organización”.

2. Haga clic en **Enviar**.

Nota:

Si su entorno hace uso de nombres sAMAccountName, después de que los usuarios reciban la invitación y hagan clic en el enlace, deberán modificar el nombre de usuario para completar la autenticación. El nombre de usuario aparece con el formato `sAMAccountName@domainname.com`. Los usuarios deben quitar la parte `@domainname.com`.

Modos de seguridad de inscripción por plataforma

En esta tabla se muestran los modos de seguridad que puede utilizar para inscribir dispositivos de usuario. En la tabla, **Sí** indica qué plataformas de dispositivos permiten modos de inscripción y administración específicos con distintos perfiles de inscripción.

Modo de seguridad de inscripción MDM	Modo de seguridad de inscripción MAM en NetScaler Gateway		Modos de administración de inscripción	Permite diferentes perfiles de inscripción		Android Enterprise (heredado)		iOS (modo de inscripción de usuarios)		iOS	macOS	Windows
Azure AD y Okta como proveedores de identidades a través de Citrix Cloud	Certificados del cliente	MDM+MAM o MDM	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No	No	No

Modo de seguridad de inscripción MDM	Modo de seguridad de inscripción MAM en NetScaler Gateway		Modos de administración	Permite diferentes perfiles de inscripción	Android (heredado)	Android Enterprise	iOS (modo de inscripción de usuarios)			iOS	macOS	Windows
Nombre de usuario y contraseña	LDAP, LDAP + certificado de cliente y certificado de cliente únicamente	MDM+MAM o MDM o MAM (el modo solo MAM no admite certificados de cliente en NetScaler Gateway)	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
URL de invitación	Certificado del cliente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	No	No	No	No	No
URL de invitación y PIN	Certificado del cliente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	No	No	No	No	No

	Modo de seguridad de inscripción MAM en NetScaler Gateway	Modos de administración	Permite diferentes perfiles de inscripción	Android (heredado)	Android Enterprise	iOS (modo de inscripción de usuarios)	iOS	macOS	Windows	
URL de invitación y contraseña	LDAP, LDAP + certificado de cliente y certificado de cliente únicamente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	No	No	
Autenticación de dos factores (nombre de usuario + contraseña + PIN)	LDAP, LDAP + certificado de cliente y certificado de cliente únicamente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	Sí	No	
Nombre de usuario + PIN	Certificado del cliente	MDM+MAM o MDM	Sí	Sí	Sí	No	Sí	Sí	No	
	Ninguno									

A continuación se describe cómo se comportan los modos de seguridad de inscripción en dispositivos iOS, Android y Android Enterprise:

- **Nombre de usuario y contraseña** (predeterminado)
 - Envía a un usuario una sola notificación que tiene 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 a un usuario una sola notificación que tiene 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, inscribirlo**. El usuario toca **Sí, inscribirlo** para inscribir el dispositivo en Citrix Endpoint Management.
- **URL de invitación y PIN**
 - Envía a un usuario los siguientes correos electrónicos:
 - ★ Un correo electrónico con una URL de inscripción, la cual permite al usuario inscribir el dispositivo en Citrix Endpoint Management a través de Citrix Secure Hub.
 - ★ Un mensaje con un PIN de un solo uso que el usuario debe escribir al inscribir el dispositivo, junto con la contraseña del usuario de Active Directory (o local).
 - Con este modo, el usuario solo se inscribe mediante la URL de inscripción incluida en la notificación. Si el usuario pierde la notificación de invitación, no podrá inscribirse. No obstante, se puede enviar otra invitación.
- **URL de invitación y contraseña**
 - Envía a un usuario una sola notificación que tiene 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.
- **Dos factores**
 - Envía al usuario una sola notificación que tiene 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 a un usuario los siguientes correos electrónicos:

- ★ Un correo electrónico con una URL de inscripción, la cual permite al usuario descargar e instalar Citrix Secure Hub. Después de abrir 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 mensaje con un PIN de un solo uso que el usuario debe escribir al inscribir el dispositivo, junto con la contraseña del usuario de Active Directory (o local).
- Si el usuario pierde la notificación de invitación, no podrá inscribirse. No obstante, se puede enviar otra invitación.

A continuación, se describe cómo se comportan los modos de seguridad de inscripción en dispositivos macOS:

- **Nombre de usuario y contraseña**

- Envía a un usuario una sola notificación que tiene una URL de inscripción. Cuando el usuario hace clic en la URL, se abre el explorador Safari. Aparecerá una página de inicio de sesión en la que se solicita al usuario que escriba un nombre de usuario y una contraseña para inscribir el dispositivo en Citrix Endpoint Management.

- **Dos factores**

- Envía al usuario una sola notificación que tiene una URL de inscripción y un PIN de un solo uso. Cuando el usuario hace clic en la URL, se abre el explorador Safari. Aparecerá una página de inicio de sesión en la que se muestran dos campos que permiten al usuario escribir una contraseña y el PIN.

- **Nombre de usuario + PIN**

- Envía a un usuario los siguientes correos electrónicos:
 - ★ Un correo electrónico con una URL de inscripción. Cuando el usuario hace clic en la URL, se abre el explorador Safari. Aparecerá una página de inicio de sesión en la que se solicita al usuario que escriba un nombre de usuario y una contraseña para inscribir el dispositivo en Citrix Endpoint Management.
 - ★ Un mensaje con un PIN de un solo uso que el usuario debe escribir al inscribir el dispositivo, junto con la contraseña del usuario de Active Directory (o local).
- Si el usuario pierde la notificación de invitación, no podrá inscribirse. No obstante, se puede enviar otra invitación.

No puede enviar invitaciones de inscripción a los dispositivos Windows. Los usuarios de Windows se inscriben directamente a través de sus dispositivos. Para obtener información sobre la inscripción de dispositivos Windows, consulte [Dispositivos Windows](#).

Acciones de seguridad

Puede realizar acciones de seguridad en dispositivos y aplicaciones desde la página **Administrar > Dispositivos**. Las acciones de seguridad en los dispositivos son: revocar, bloquear, desbloquear y borrar. Las acciones de seguridad en las aplicaciones son: bloquear y borrar.

- **Omisión del bloqueo de activación:** En dispositivos iOS supervisados, quita el Bloqueo de activación antes de la activación del dispositivo. Este comando no requiere el ID de Apple ni la contraseña personal 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.
- **Eliminación de aplicaciones:** Elimina la cuenta de usuario que consta en Citrix Secure Hub y desinscribe el dispositivo. Los usuarios no pueden inscribirse de nuevo hasta que use la acción **Anular borrado de aplicaciones**.
- **Bloqueo de activación del Programa de implementación de ASM:** Crea un código de anulación del bloqueo de activación para dispositivos iOS inscritos en Apple School Manager.
- **Renovación de certificados:** Para dispositivos iOS, macOS y Android compatibles, la acción de seguridad “Renovación de certificado” inicia la renovación del certificado. 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 entidad de certificación.
- **Desactivar restricciones:** En dispositivos iOS supervisados, este comando permite que Citrix Endpoint Management borre la contraseña de restricciones y los parámetros de restricciones configurados por el usuario.
- **Habilitar o inhabilitar el modo perdido:** Coloca un dispositivo iOS supervisado en el modo Perdido y envía un mensaje, un número de teléfono y una nota al pie que aparecen en el dispositivo. La segunda vez que se envíe este comando, el dispositivo sale del modo Perdido.
- **Habilitar seguimiento:** En dispositivos Android o iOS, este comando permite a Citrix Endpoint Management sondear la ubicación de dispositivos concretos con la frecuencia que defina. Para ver las coordenadas y la ubicación del dispositivo en un mapa, vaya a **Administrar > Dispositivos**, seleccione un dispositivo y, a continuación, haga clic en **Modificar**. La información del dispositivo se encuentra en la ficha **General**, en **Seguridad**. Utilice **Habilitar seguimiento** para hacer seguimiento del dispositivo de forma continua. Citrix Secure Hub informa periódicamente de la ubicación cuando el dispositivo está en funcionamiento.
- **Borrado completo:** Borra inmediatamente todos los datos y todas las aplicaciones que hubiera presentes en un dispositivo, incluidas las tarjetas de memoria. Los dispositivos borrados per-

manecen en la lista de dispositivos de la página **Administrar > Dispositivos** para las auditorías. Puede quitar un dispositivo borrado de la lista de dispositivos.

- En caso de dispositivos Android, esta solicitud puede incluir la opción de borrar las tarjetas de memoria.
- Para dispositivos Android Enterprise totalmente administrados con un perfil de trabajo (dispositivos COPE), puede realizar un borrado completo después de la eliminación del perfil de trabajo mediante un borrado selectivo.
- Para dispositivos iOS y macOS, el borrado se aplica inmediatamente, incluso aunque el dispositivo esté bloqueado.

Para dispositivos iOS 11 e iPadOS 12 (versión mínima): Tras confirmar el borrado completo, puede optar por conservar el plan de datos móviles que hubiera presente en el dispositivo.

Para dispositivos con iOS 11.3 (versión mínima): Tras confirmar el borrado completo, evita que los dispositivos iOS realicen la configuración por proximidad. Al configurar un nuevo dispositivo iOS, los usuarios normalmente pueden usar un dispositivo iOS ya configurado para configurar el suyo. Puede bloquear esta configuración por proximidad en dispositivos cuyos datos hayan sido borrados y estén bajo la administración de Citrix Endpoint Management.

- Si el usuario apaga el dispositivo antes de que se elimine el contenido de la tarjeta de memoria, aún podría tener acceso a los datos del dispositivo.
 - Puede cancelar la solicitud de borrado hasta que se envíe al dispositivo.
- **Localizar:** Busca un dispositivo y notifica su ubicación con un mapa en la página **Administrar > Dispositivos**, en **Detalles del dispositivo > General**. Localizar es una acción que tiene lugar una sola vez. Use **Localizar** para mostrar la ubicación actual del dispositivo en el momento en que se realiza la acción. Para realizar un seguimiento continuo del dispositivo durante un período de tiempo, 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 conceda permiso de localización durante la inscripción. El usuario puede optar por no conceder permiso de localización. Si el usuario no concede el permiso durante la inscripción, Citrix Endpoint Management vuelve a solicitarlo cuando envía el comando de **localización**.
 - Al aplicar esta funcionalidad a dispositivos iOS o Android Enterprise, tenga en cuenta las siguientes limitaciones:

- ★ Para dispositivos Android Enterprise, esta solicitud falla, a menos que la directiva [Localización](#) haya establecido el modo de ubicación para el dispositivo en **Alta precisión** o **Ahorro de batería**.
- ★ Para los dispositivos iOS, el comando solo se ejecuta correctamente si los dispositivos se encuentran en el modo perdido de MDM.
- **Bloqueo:** Bloquea a distancia un dispositivo. El bloqueo es útil si roban un dispositivo y este debe estar bloqueado. Cuando se envía este comando, Citrix Endpoint Management genera un código PIN y lo establece en el dispositivo. Para acceder al dispositivo, el usuario deberá teclear ese código PIN. Use el comando **Cancelar bloqueo de dispositivo** para quitar el bloqueo desde la consola de Citrix Endpoint Management.
- **Bloquear y restablecer contraseña:** Bloquea a distancia un dispositivo y restablece el código de acceso en él.
 - No se ofrece en los dispositivos siguientes:
 - ★ Dispositivos inscritos en Android Enterprise en el modo de perfil de trabajo
 - ★ Dispositivos con una versión de Android anterior a Android 7.0
 - En dispositivos inscritos en Android Enterprise en el modo de perfil de trabajo y que tienen Android 7.0 o una versión posterior:
 - ★ El código de acceso bloquea el perfil de trabajo. El dispositivo no se bloquea.
 - ★ Si no se envía ningún código de acceso o el código enviado no cumple los requisitos y el perfil de trabajo no tiene ningún código de acceso: el dispositivo se bloquea.
 - ★ Si no se envía ningún código de acceso o el código enviado no cumple los requisitos, pero el perfil de trabajo tiene un código de acceso: el perfil de trabajo se bloquea, pero el dispositivo no.
- **Notificar (Hacer sonar):** Reproduce un sonido en dispositivos Android.
- **Reiniciar:** Reinicia dispositivos con Windows 10 o Windows 11. En Windows Tablet y PC aparece un mensaje sobre el reinicio pendiente. El reinicio se produce cinco minutos después.
- **Solicitar o detener duplicación AirPlay:** Inicia y detiene la duplicación AirPlay en los dispositivos iOS supervisados.
- **Reiniciar o apagar:** Reinicia o apaga inmediatamente dispositivos iOS supervisados.
- **Revocar:** Prohíbe a un dispositivo que se conecte a Citrix Endpoint Management.
- **Revocar o autorizar:** Realiza las mismas acciones que el borrado selectivo. Después de la revocación, puede volver a autorizar el dispositivo para la reinscripción.
- **Hacer sonar:** Si el dispositivo está en el modo perdido, esta acción reproduce un sonido en un dispositivo iOS supervisado. El sonido se reproduce hasta que se saque al dispositivo del modo perdido o hasta que el usuario quite el sonido.

- **Rotar clave personal de recuperación:** Si ha habilitado la directiva de dispositivo FileVault, esta acción genera una nueva clave personal de recuperación y reemplaza la clave antigua por esta nueva clave. Puede cancelar esta solicitud mientras la solicitud está aún pendiente. Para ello, haga clic en **Cancelar rotación de la clave personal de recuperación**.
- **Borrado selectivo:** Borra todas las aplicaciones y los datos de empresa de un dispositivo, pero no afecta a las aplicaciones ni los datos personales. Después de un borrado selectivo, utilice la acción **Autorizar** para volver a autorizar el dispositivo para que el usuario correspondiente pueda volver a inscribirlo. Los dispositivos borrados permanecen en la lista de dispositivos de la página **Administrar > Dispositivos** para las auditorías. Puede quitar un dispositivo borrado de la lista de dispositivos.
 - Borrar un dispositivo Android de forma selectiva no lo desconecta de Device Manager ni de la red corporativa. Para evitar que el dispositivo acceda a Device Manager, también debe revocar los certificados de dispositivo.
 - Borrar selectivamente los datos de un dispositivo Android también revoca el dispositivo. Puede volver a inscribir el dispositivo solo después de reautorizarlo o eliminarlo de la consola.
 - Para dispositivos Android Enterprise totalmente administrados con un perfil de trabajo (dispositivos COPE), puede realizar un borrado completo después de la eliminación del perfil de trabajo mediante un borrado selectivo. O bien, puede volver a inscribir el dispositivo con el mismo nombre de usuario. Al reinscribir el dispositivo, se vuelve a crear el perfil de trabajo.
 - Para dispositivos iOS y macOS, este comando elimina cualquier perfil instalado a través de MDM.
 - El borrado selectivo en un dispositivo Windows también elimina el contenido de la carpeta de perfil del usuario que haya iniciado sesión en el dispositivo en ese momento. En un borrado selectivo, no se elimina ningún clip web que entregue a los usuarios a través de una configuración. Los clips web se eliminan cuando los usuarios desinscriben sus dispositivos de forma manual. No se puede volver a inscribir un dispositivo en el que se ha realizado el borrado selectivo.
- **Desbloquear:** Borra el código de acceso que se envía al dispositivo cuando este se bloquea. Este comando no abre el dispositivo.

En **Administrar > Dispositivos**, la página **Detalles del dispositivo** muestra también las propiedades de seguridad del dispositivo. Entre esas propiedades, se encuentran: el ID seguro, el bloqueo del dispositivo, la omisión del bloqueo de activación, así como otra información en función del tipo de plataforma. El campo **Borrado completo del dispositivo** contiene el código PIN del usuario. El usuario debe introducir ese código después de que se haya borrado el dispositivo. Si el usuario no consigue recordar el código, usted puede buscarlo en “Detalles del dispositivo”.

Se pueden automatizar algunas acciones. Para obtener información detallada, consulte [Acciones automatizadas](#).

Quitar un dispositivo de la consola de Citrix Endpoint Management

Importante:

Cuando se quita un dispositivo de la consola de Citrix Endpoint Management, las aplicaciones administradas y los datos permanecen en el dispositivo. Para quitar las aplicaciones administradas y los datos que contiene el 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 el dispositivo administrado y, a continuación, haga clic en **Eliminar**.

Devices

Users

Enrollment Invitations

Devices

Show filter

Search

Add

Edit

Secure

Notify

Delete

Import

Export

Refresh

<input type="checkbox"/>	Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Inactivity days	Available storage space	Device name	XenMobile agent version	
<input checked="" type="checkbox"/>		<div>MDM</div> <div>MAM</div>			Android	5.1.1	SM-T900	0 day	13.05 GB	Android(0)	10.6.0	

Borrar datos selectivamente de un dispositivo

1. Vaya a **Administrar > Dispositivos**, seleccione un dispositivo administrado y haga clic en **Proteger**.
2. En **Acciones de seguridad**, haga clic en **Borrado selectivo**.
3. En los dispositivos Android (y únicamente en ellos), desconecte el dispositivo de la red corporativa. Para ello, después de que se borre el dispositivo, en **Acciones de seguridad**, haga clic en **Revocar**.

Para anular una solicitud de borrado selectivo antes de que se haya llevado a cabo, en **Acciones de seguridad**, haga clic en **Cancelar borrado selectivo**.

Eliminar un dispositivo

Este procedimiento elimina las aplicaciones administradas y los datos que contiene un dispositivo. Asimismo, se elimina el dispositivo de la lista “Dispositivos” en la consola de Citrix Endpoint Management. Puede utilizar la API de REST pública de Citrix Endpoint Management para eliminar dispositivos en bloque.

1. Vaya a **Administrar > Dispositivos**, seleccione un dispositivo administrado y haga clic en **Proteger**.

- Haga clic en **Borrado selectivo**. Cuando se le solicite, haga clic en **Ejecutar borrado selectivo**.
- Para verificar que el comando de borrado se ha realizado, actualice **Administrar > Dispositivos**. En la columna **Modo**, el color anaranjado de MAM y MDM indica que el comando de borrado se ha realizado.

Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Inactivity days	Available storage space	Device name	XenMobile agent version
	MDM MAM			Android	5.1.1	SM-T900	0 day	13.05 GB	Android(0)	10.6.0

- En **Administrar > Dispositivos**, seleccione el dispositivo y haga clic en **Eliminar**. Cuando se le solicite, haga clic en **Eliminar** de nuevo.

Bloquear, desbloquear, borrar o anular el borrado de aplicaciones

- Vaya a **Administrar > Dispositivos**, seleccione un dispositivo administrado y haga clic en **Proteger**.
- En el cuadro de diálogo **Acciones de seguridad**, haga clic en la acción de aplicaciones pertinente.

También puede utilizar el cuadro de diálogo **Acciones de seguridad** para consultar el estado del dispositivo de un usuario cuya cuenta se haya inhabilitado o eliminado de Active Directory. La presencia de las acciones “Desbloqueo de aplicaciones” o “Anular borrado de aplicaciones” indica que hay aplicaciones que se han bloqueado o borrado.

Borrar y anular el borrado de aplicaciones

- Vaya a **Administrar > Dispositivos**. Seleccione un dispositivo.
- Borrado de aplicaciones
 - Haga clic en **Proteger > Borrado de aplicaciones**. Aparece un cuadro de diálogo con este mensaje: **¿Seguro que quiere borrar las aplicaciones de este dispositivo?** Haga clic en **Borrar aplicaciones**.
- Anular borrado de aplicaciones
 - Haga clic en **Proteger > Anular borrado de aplicaciones**. Aparece un cuadro de diálogo con este mensaje: **¿Seguro que quiere que la aplicación anule el borrado de aplicaciones de este dispositivo?** Haga clic en **Anular borrado de aplicaciones del dispositivo**.
- Reinscriba el dispositivo como el mismo usuario y en el mismo modo.

5. Inicie una aplicación MDX desde la página **Mis aplicaciones**.
6. Inicie Citrix Secure Hub.

Obtener información acerca de dispositivos

La base de datos de Citrix Endpoint Management almacena una lista de dispositivos móviles. Para rellenar la consola de Citrix Endpoint Management con los datos de los dispositivos, puede agregar los dispositivos de forma manual o importar una lista de dispositivos desde un archivo. Para obtener más información acerca de formatos del archivo de aprovisionamiento de dispositivos, consulte [Formatos del archivo de aprovisionamiento de dispositivos](#) más adelante en este artículo.

En la página **Administrar > Dispositivos** de la consola de Citrix Endpoint Management, se ofrece una lista de cada dispositivo y la siguiente información:

- **Estado:** Los iconos indican el estado de implementación, si está administrado, si ha sido liberado por jailbreak y si ActiveSync Gateway está disponible.
- **Modo:** Indica el modo del dispositivo (por ejemplo, MDM o MDM+MAM).
- Se ofrece otra información del dispositivo, como **Nombre de usuario**, **Plataforma del dispositivo**, **Último acceso** y **Días de inactividad**. Estos son los encabezados predeterminados que aparecen.

Para personalizar la tabla **Dispositivos**, haga clic en la flecha hacia abajo en el último encabezado. A continuación, seleccione los encabezados adicionales que quiera mostrar en la tabla o borre los que quiera quitar.

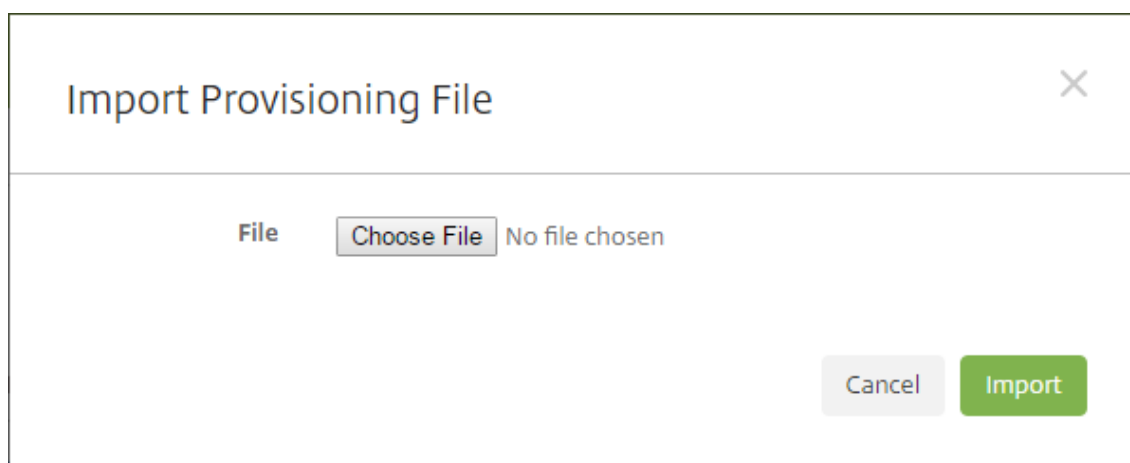
Last access	Inactivity days	▼
	✓ Status	
	✓ Mode	
	✓ User name	
	Serial number	
	IMEI/MEID	
	ActiveSync ID	
	WiFi MAC address	
	Bluetooth MAC address	
	✓ Device platform	
	✓ Operating system version	
	✓ Device model	
	✓ Last access	
	✓ Inactivity days	
	Shareable	
	Shared status	
	DEP registered	

Puede agregar dispositivos manualmente, importarlos desde un archivo de aprovisionamiento, modificar los datos de los dispositivos, personalizar las propiedades de usuario de Active Directory, realizar acciones para aumentar la seguridad en ellos y enviarles notificaciones. También puede exportar todos los datos de la tabla de dispositivos a un archivo CSV para generar un informe personalizado. El servidor exporta todos los atributos de dispositivo. Si se aplican filtros, Citrix Endpoint Management los tendrá en cuenta 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 móviles. También puede crear su propio archivo de aprovisionamiento de dispositivos. Para obtener más información, consulte Formatos del archivo de aprovisionamiento de dispositivos más adelante en este artículo.

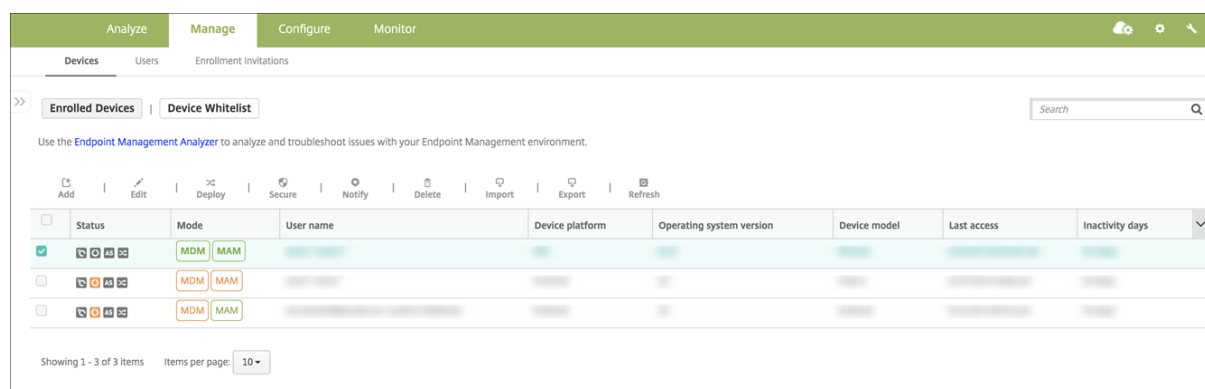
1. Vaya a **Administrar > Dispositivos** y haga clic en **Importar**. Aparece el cuadro de diálogo **Importar archivo de aprovisionamiento**.



2. Haga clic en **Elegir archivo** y, a continuación, vaya al archivo que quiere importar.
3. Haga clic en **Importar**. El archivo importado aparecerá en la tabla **Dispositivos**.
4. Para modificar la información del dispositivo, selecciónelo y, a continuación, haga clic en **Modificar**. Para obtener información sobre las páginas que contiene **Detalles del dispositivo**, consulte Obtener información acerca de dispositivos.

Implementar en dispositivo

Puede forzar a uno o a varios dispositivos a conectarse con Citrix Endpoint Management. Los dispositivos seleccionados reciben recursos inmediatamente sin esperar la próxima comprobación programada.

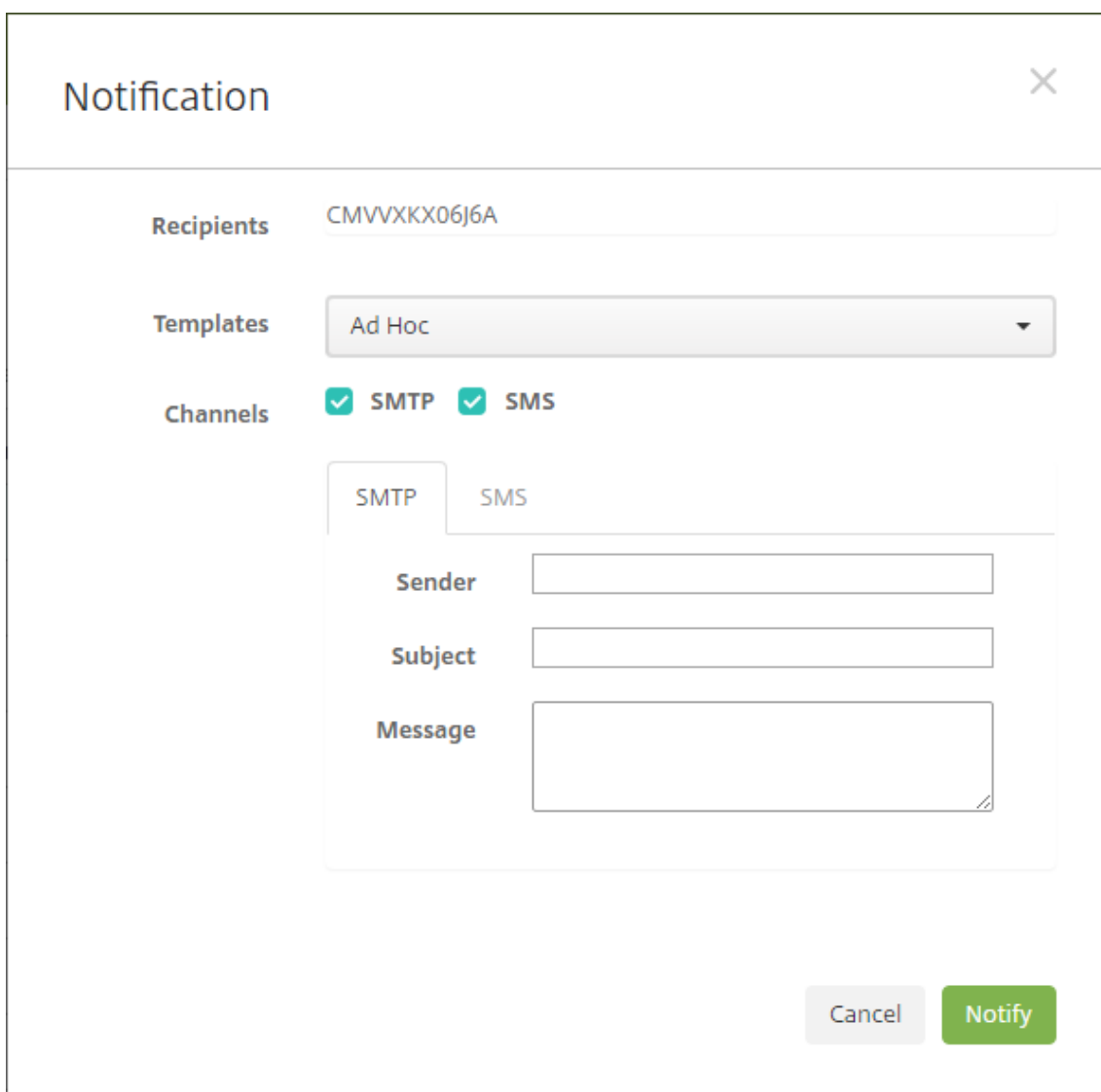


1. Vaya a **Administrar > Dispositivos**, seleccione un dispositivo administrado de MDM o MDM+MAM y, a continuación, haga clic en **Implementar**.
2. En el cuadro de diálogo, haga clic en **Implementar** para confirmar la acción.

Enviar una notificación a dispositivos

Puede enviar notificaciones a los dispositivos desde la página Dispositivos. Para obtener más información acerca de las notificaciones, consulte [Notificaciones](#).

1. En la página **Administrar > Dispositivos**, elija los dispositivos a los que quiera enviar una notificación.
2. Haga clic en **Notificar**. Aparecerá el cuadro de diálogo **Notificación**. En el campo **Destinatarios**, se ofrece una lista de todos los dispositivos que van a recibir la notificación.



Notification [X]

Recipients CMVVXKX06J6A

Templates Ad Hoc

Channels ☒ SMTP ☒ SMS

SMTP **SMS**

Sender [Input Field]

Subject [Input Field]

Message [Text Area]

Cancel Notify

3. Configure estos parámetros:
 - **Plantillas:** En la lista desplegable, haga clic en el tipo de notificación que quiere enviar. Los campos **Asunto** y **Mensaje** se rellenarán con el texto configurado de la plantilla que eligió, excepto en el caso de haber elegido **Ad hoc**.

- **Canales:** Seleccione cómo enviar el mensaje. El valor predeterminado es **SMTP**. Haga clic en las fichas para ver el formato del mensaje para cada canal.
- **Remitente:** Escriba un remitente opcional.
- **Asunto:** Escriba el asunto para un mensaje **Ad hoc**.
- **Mensaje:** Escriba el mensaje para un mensaje **Ad hoc**.

4. Haga clic en **Notificar**.

Exportar la tabla Dispositivos

1. Filtre la tabla **Dispositivos** según lo que quiera que aparezca en el archivo de exportación.
2. Haga clic en el botón **Exportar** situado sobre 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 manualmente los dispositivos de usuario

En Citrix Endpoint Management, puede etiquetar manualmente un dispositivo de las siguientes maneras:

- Durante el proceso de inscripción por invitación.
- Durante el proceso de inscripción mediante el portal Self Help Portal.
- Al agregar el propietario del dispositivo a las propiedades de este.

Tiene la opción de etiquetar el dispositivo como propiedad de la empresa o del empleado. Cuando se usa el portal Self Help Portal para inscribir un dispositivo, también se puede etiquetarlo como propiedad de la empresa o propiedad del empleado. También puede etiquetar un dispositivo manualmente siguiendo este procedimiento.

1. Agregue una propiedad al dispositivo desde la ficha **Dispositivos** en la consola de Citrix Endpoint Management.
2. Agregue la propiedad denominada **Propietario** y elija **Empresa** o **BYOD** (propiedad del empleado).

DevicesUsersEnrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Assigned Policies

5 Apps

6 Media

7 Actions

8 Delivery Groups

9 iOS Profiles

10 iOS Provisioning Profiles

11 Certificates

12 Connections

13 MDM Status

iPhone

Properties

+ BatteryAdd

+ Location informationAdd

+ Network informationAdd

+ Security informationAdd

+ Storage spaceAdd

- System informationAdd

Owned by

Corporate

BYOD

DoneCancel

Active iTunes account

Yes

Baseband firmware version

2.16.00

Cloud backup enabled

No

Color

BLACK

DEP account name

DEP

DEP profile assigned

01/08/2017 06:47:15

Personalizar atributos de usuario de Active Directory

Puede personalizar determinados 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 una clave personalizada en **Parámetros > Propiedades de servidor**. En el campo **Valores**, puede quitar y restaurar posteriormente los atributos de usuario opcionales de Active Directory que Citrix Endpoint Management proporciona de forma predeterminada. Para obtener información, consulte [Propiedades de servidor](#).

Después de modificar la lista de valores predeterminados y guardar los cambios, puede ver los atributos de usuario actualizados de Active Directory en **Administrar > Dispositivos > Propiedades de usuario**. Citrix Endpoint Management actualiza la consola después de que el usuario inicie sesión en el dispositivo o durante la próxima conexión programada del dispositivo. Si comete un error ortográfico o agrega un valor que no se admite, Citrix Endpoint Management ignorará los cambios.

La eliminación de los atributos de usuario opcionales de Active Directory puede afectar a la funcionalidad siguiente:

- **Aprovisionamiento de la cuenta de usuario:** si quita los valores de nombre y apellido, Citrix Endpoint Management no podrá aprovisionar la cuenta de usuario para ShareFile y Salesforce.
- **Invitaciones de inscripción:** Si quita el correo electrónico o los datos del teléfono móvil del usuario, este no podrá recibir la invitación de inscripción.
- **Acciones de notificación de dispositivo:** Si quita los datos de correo electrónico del usuario, este no podrá recibir las notificaciones a través de SMTP.

- **Single Sign-On en Citrix Secure Mail:** Si quita el valor del nombre simplificado, el usuario no podrá iniciar sesión en Citrix Secure Mail por el inicio de sesión único.
- **Reglas de propiedad de usuario y reglas de implementación:** Si quita alguno de los atributos opcionales que se utilizan para configurar las reglas de propiedad de usuario y las reglas de implementación, las configuraciones existentes pueden verse afectadas.
- **Acciones:** Si elimina cualquiera de los atributos opcionales que se utilizan para establecer una acción automatizada en **Configurar > Acciones**, las configuraciones existentes pueden verse afectadas.
- **Informes personalizados:** Si elimina cualquiera de los atributos opcionales que se utilizan en los informes personalizados, las configuraciones existentes pueden verse afectadas.

Buscar dispositivos

Para una búsqueda rápida, el ámbito predeterminado de las búsquedas incluye solo 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 la búsqueda a través de una nueva propiedad del servidor, **include.device.properties.during.search**, cuyo valor predeterminado 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 del archivo de aprovisionamiento de dispositivos

Muchos operadores móviles o fabricantes de dispositivos proporcionan listas de dispositivos móviles autorizados. Puede usar estas listas para evitar tener que introducir una larga lista de dispositivos móviles manualmente. Citrix Endpoint Management es compatible con un formato de archivo de importación común para los tres tipos de dispositivo admitidos: Android, iOS y Windows.

Un archivo de aprovisionamiento que cree manualmente debe tener el formato siguiente:

```
SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;  
propertyName2;propertyValue2; ... propertyNameN;propertyValueN
```

Tenga en cuenta lo siguiente:

- Para saber cuáles son los valores válidos para cada propiedad, consulte el PDF [Valores y nombres de propiedades de dispositivo](#).
- Use el conjunto de caracteres UTF-8.
- Use un punto y coma (;) para separar los campos que contenga el archivo de aprovisionamiento. Si parte de un campo tiene un punto y coma, debe anteponérsele un carácter de barra diagonal inversa (\).

Por ejemplo, para esta propiedad:

`propertyV;test;1;2`

Coloque una barra diagonal inversa de la siguiente manera:

`propertyV\;test\;1\;2`

- El número de serie es obligatorio para dispositivos iOS porque es el identificador del dispositivo iOS.
- Para otras plataformas de dispositivos, se debe incluir el número de serie o el IMEI.
- Los valores válidos para **OperatingSystemFamily** son: **WINDOWS**, **ANDROID** o **iOS**.

Ejemplo de un archivo de aprovisionamiento de dispositivos:

```
1 `1050BF3F517301081610065510590391;15244201625379901;WINDOWS;propertyN;
   propertyV\;test\;1\;2;prop 2
2 2050BF3F517301081610065510590392;25244201625379902;ANDROID;propertyN;
   propertyV$*&&ééétest
3 3050BF3F517301081610065510590393;35244201625379903;iOS;test;
4 4050BF3F517301081610065510590393;;iOS;test;
5 ;55244201625379903;ANDROID;test.testé;value;`
```

Cada línea del archivo describe un dispositivo. La primera entrada del ejemplo significa lo siguiente:

- SerialNumber: 1050BF3F517301081610065510590391
- IMEI: 15244201625379901
- OperatingSystemFamily: WINDOWS
- PropertyName: propertyN
- PropertyValue: propertyV\;test\;1\;2;prop 2

Alexa for Business

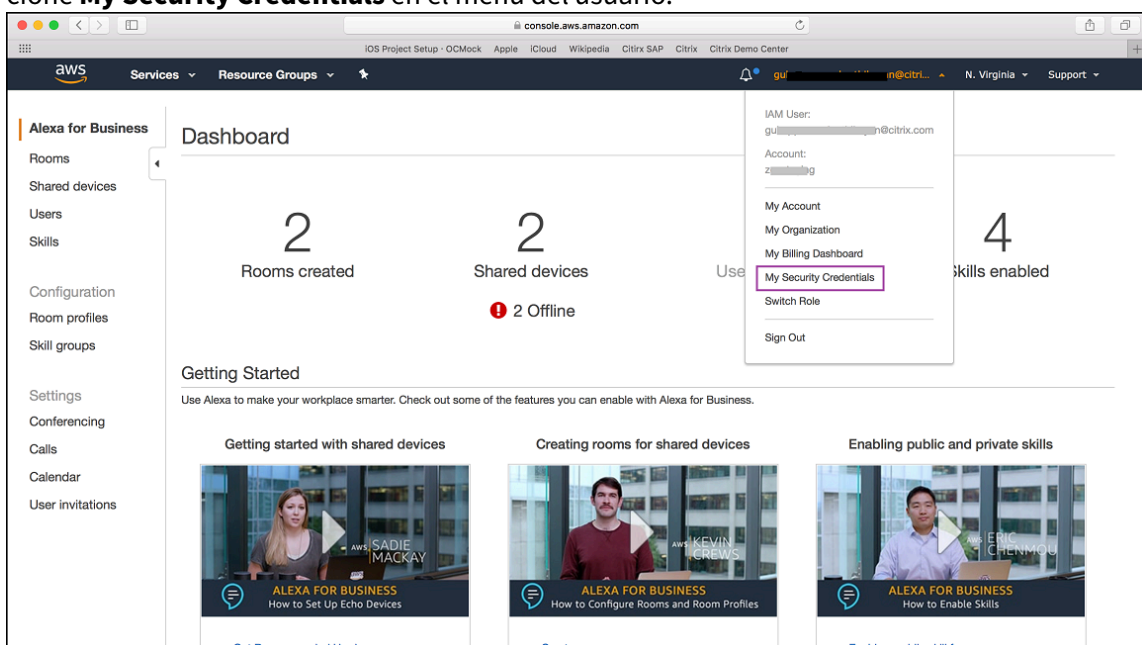
November 29, 2023

El servicio Alexa for Business de Amazon Web Services (AWS) permite administrar una gran cantidad de dispositivos habilitados para Alexa con fines empresariales, como la asistencia en salas de conferencias. Citrix Endpoint Management le permite configurar y administrar estos dispositivos en la consola de Citrix Endpoint Management. Citrix Endpoint Management no implementa directivas directamente en los dispositivos Alexa. En vez de ello, Citrix Endpoint Management actualiza los servicios de AWS y es AWS quien entrega las configuraciones a los dispositivos Alexa.

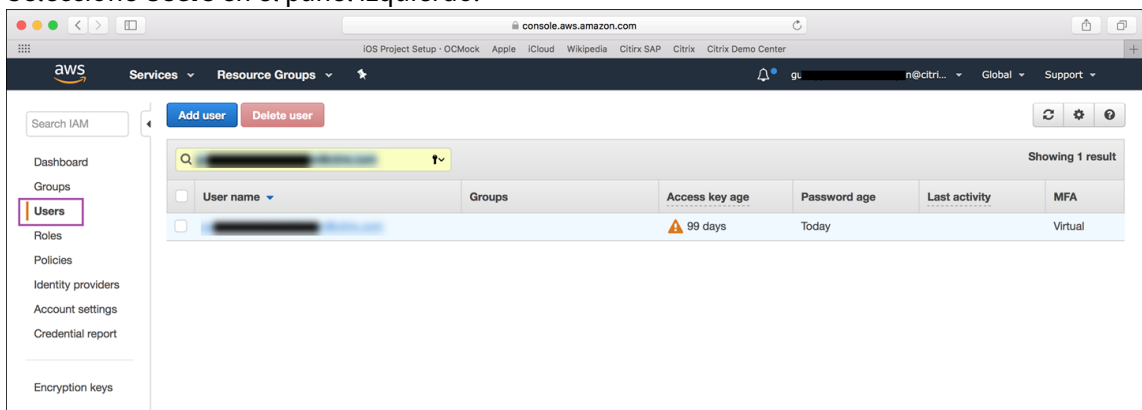
Para obtener información sobre el uso de Alexa for Business, consulte [Alexa for Business Administration Guide](#).

Autenticar su cuenta de AWS en Citrix Endpoint Management

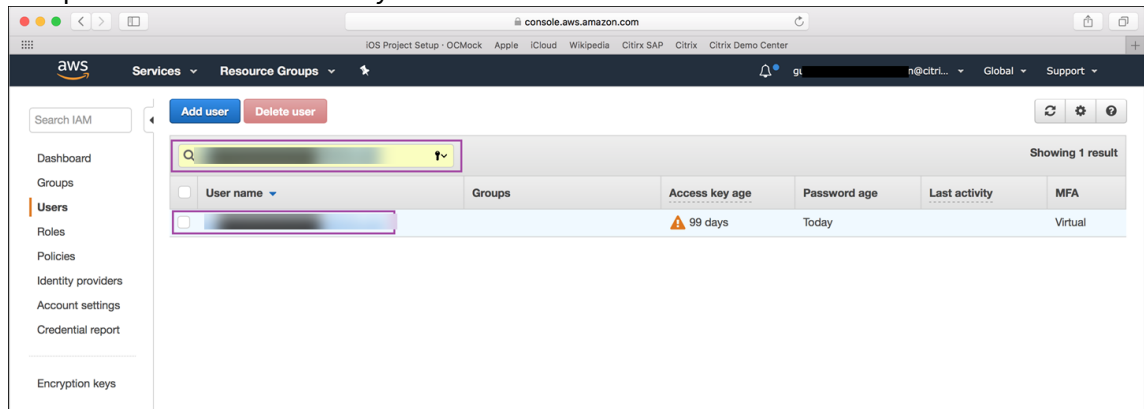
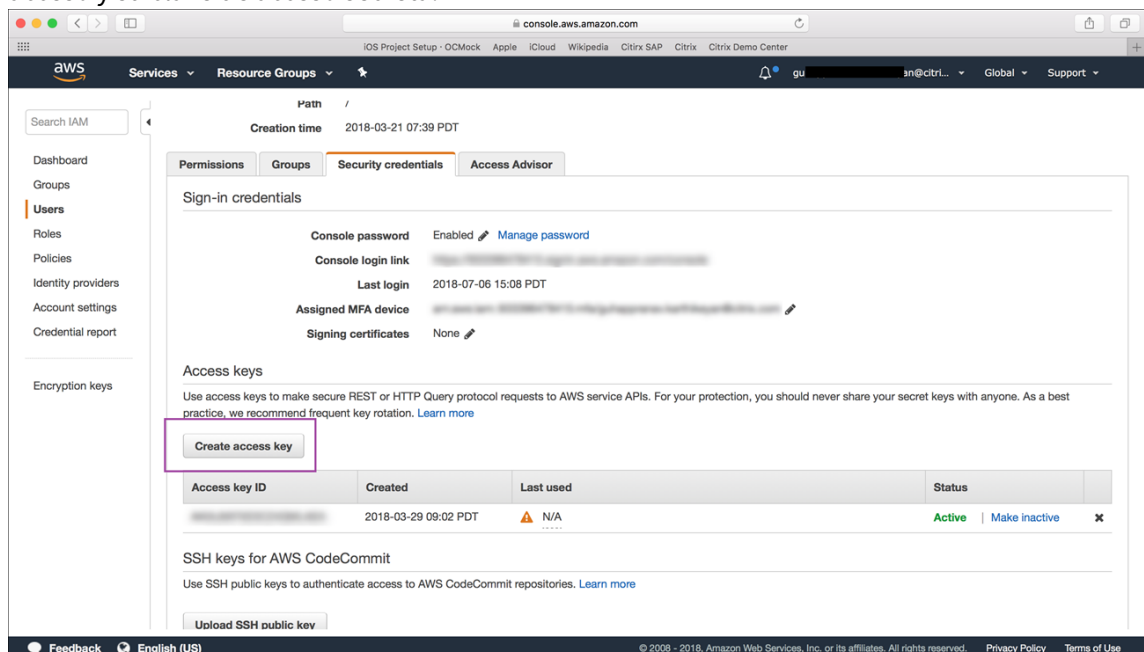
1. Para obtener las credenciales de su cuenta de AWS, inicie sesión en la consola de AWS y seleccione **My Security Credentials** en el menú del usuario.



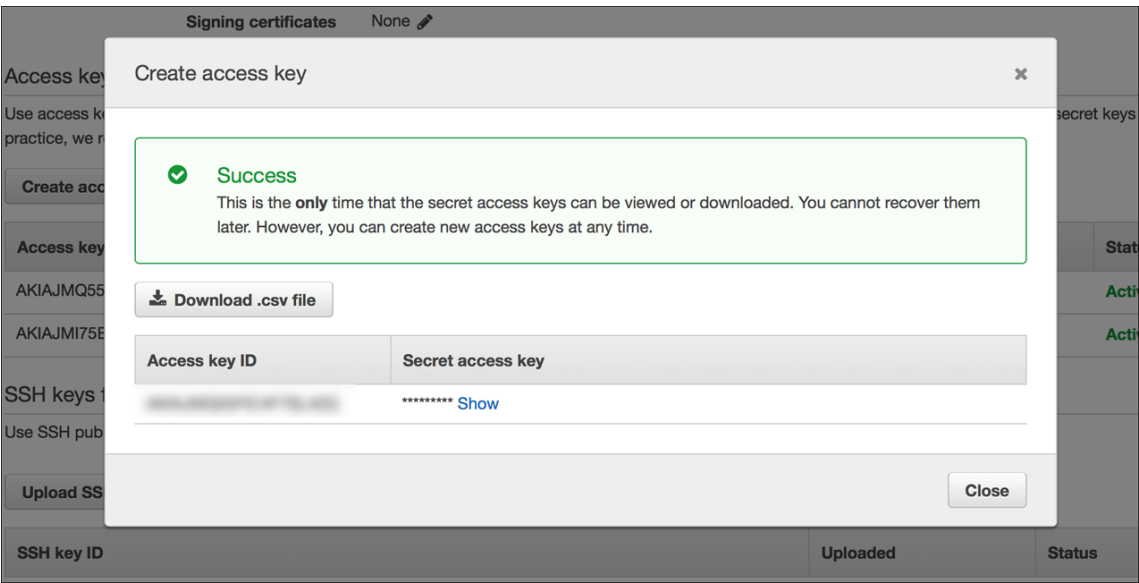
2. Seleccione **Users** en el panel izquierdo.



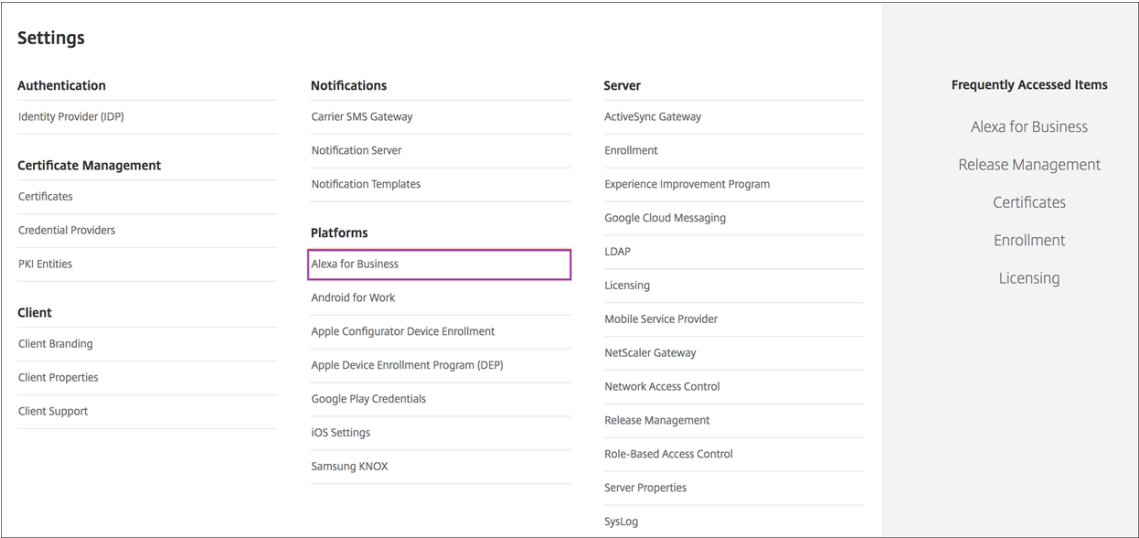
3. Busque su nombre de usuario y selecciónelo.

4. En la ficha **Security Credentials**, haga clic en **Create access key** para generar su ID de clave de acceso y su clave de acceso secreta.

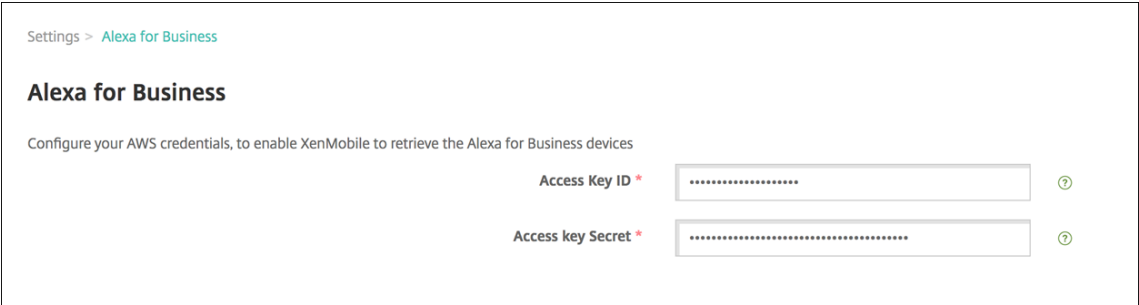
5. Descargue el ID de la clave de acceso y la clave de acceso secreta. Guárdelas o tome nota de ellas.



6. En la consola de Citrix Endpoint Management, haga clic en el icono de engranaje para ir a **Parámetros**.
7. En **Plataformas**, seleccione **Alexa for Business**.



8. Escriba el ID de la clave de acceso y la clave de acceso secreta. Haga clic en **Guardar**.



Configurar Alexa for Business en Citrix Endpoint Management

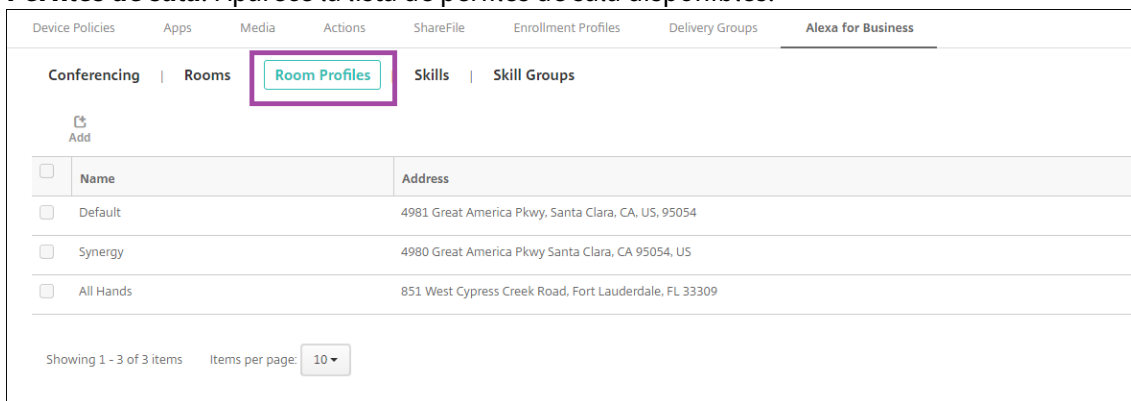
Citrix Endpoint Management le permite configurar:

- Los parámetros de los perfiles de sala que se aplican a las salas que contienen los dispositivos con Alexa
- Las salas que representan las salas físicas que contienen los dispositivos
- Los grupos de skills que se asignan a salas o dispositivos
- Skills de Alexa provenientes del almacén de skills de Alexa que se pueden agregar a grupos de skills
- Las funciones de conferencia que permiten elegir un proveedor de conferencias y controlar la forma en que los usuarios programan las reuniones y se conectan a ellas en las salas

Configurar perfiles de sala

Un perfil de sala es un conjunto de parámetros comunes que se pueden aplicar a una colección de salas que contienen los dispositivos Alexa. Puede agregar, modificar y eliminar perfiles de sala.

1. En la consola de Citrix Endpoint Management, seleccione **Parámetros > Alexa for Business > Perfiles de sala**. Aparece la lista de perfiles de sala disponibles.



Device Policies		Apps		Media		Actions		ShareFile		Enrollment Profiles		Delivery Groups		Alexa for Business	
Conferencing		Rooms		Room Profiles		Skills		Skill Groups							
Add															
<input type="checkbox"/>	Name	Address													
<input type="checkbox"/>	Default	4981 Great America Pkwy, Santa Clara, CA, US, 95054													
<input type="checkbox"/>	Synergy	4980 Great America Pkwy Santa Clara, CA 95054, US													
<input type="checkbox"/>	All Hands	851 West Cypress Creek Road, Fort Lauderdale, FL 33309													
Showing 1 - 3 of 3 items		Items per page:		10											

2. Para agregar un perfil de sala, haga clic en **Agregar**. Para modificar un perfil de sala, selecciónelo y haga clic en **Modificar**.
3. Escriba los parámetros del perfil de sala:

Device Policies Apps Media Actions ShareFile Enrollment Profiles Delivery Groups **Alexa for Business**

Add room profile

Profile name * Synergy

Address * 4980 Great America Parkway

Time zone * America/Los_Angeles

▼ Device settings

Wake word Alexa

Temperature units ☒ US (Fahrenheit) ☐ Metric (Celsius)

Distance units ☒ US (Feet, inches) ☐ Metric (Meters)

Maximum volume 10

Device setup mode ☒ On ☐ Off

▼ Outbound calling

Outbound calling ☒ Enabled ☐ Disabled

Address book

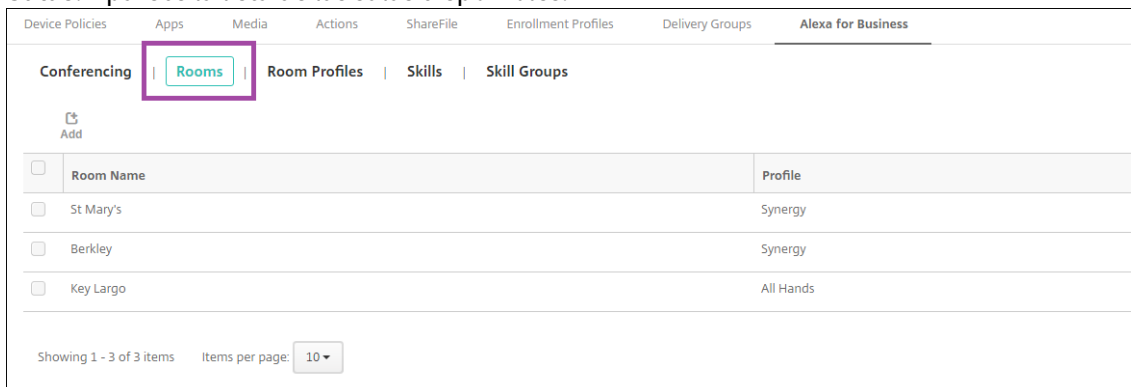
- **Nombre de perfil:** Escriba el nombre del perfil.
- **Dirección:** Escriba la dirección física (calle) del edificio donde se encuentran las salas que contienen los dispositivos Alexa.
- **Zona horaria:** Elija la zona horaria del lugar.
- **Frase de activación:** Elija la palabra de activación a la que responden los dispositivos Alexa.
- **Unidades de temperatura:** Seleccione las unidades en que los dispositivos con Alexa informan de la temperatura.
- **Unidades de distancia:** Seleccione las unidades en que los dispositivos con Alexa informan de la distancia.
- **Volumen máximo:** Elija el volumen máximo para Alexa.
- **Modo de configuración de dispositivo:** Seleccione si los dispositivos con Alexa pueden reconfigurarse forzándolos al modo de configuración del dispositivo.
- **Llamada saliente:** Active o desactive la capacidad de llamadas salientes de los dispositivos con Alexa.
- **Libreta de direcciones:** Defina la libreta de direcciones para los dispositivos con Alexa.

4. Haga clic en **Guardar**.

Configurar salas

Las salas que configure en la consola de Citrix Endpoint Management representan las salas de conferencias, las salas de reuniones y otras salas físicas del edificio. Al configurar una sala, se asocia un dispositivo Alexa a la sala y se agrega un grupo de skills al dispositivo. Puede agregar, modificar y eliminar salas.

1. En la consola de Citrix Endpoint Management, seleccione **Configurar > Alexa for Business > Salas**. Aparece la lista de las salas disponibles.



2. Para agregar una sala, haga clic en **Agregar**. Para modificar una sala, selecciónela y haga clic en **Modificar**.
3. Indique los parámetros de esta sala:

The screenshot shows the 'Room details' form. It includes a sidebar with '1 Room details', '2 Add Echo devices', and '3 Add skill groups'. The main form area has the following fields: 'Room Name' (text input), 'Room calendar email' (text input), and 'Room Profile' (dropdown menu with 'Default' selected). A description at the top states: 'A room maps to a physical location where you place a shared device for end user interaction. Examples of rooms include conference rooms, lobbies, and hotel rooms. All Alexa devices in a room inherit all the skills and settings configured for that room.'

- **Nombre de la sala:** Escriba el nombre de la sala de conferencias, la 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 sala:** Elija el nombre de la configuración del perfil para la sala.
4. Haga clic en **Siguiente**.
 5. Para asociar un dispositivo Alexa a la sala, haga clic en **Agregar**.
 6. Seleccione un dispositivo y haga clic en **Agregar**. El dispositivo seleccionado aparece en la pantalla **Agregar dispositivos Echo**.

Add Echo devices

☐

Serial number

Device Model

▼

☒

Dot

Showing 1 - 1 of 1 items

Cancel

Add

7. Haga clic en **Siguiente**.
8. Para agregar grupos de skills a los dispositivos Alexa en la sala, haga clic en **Agregar**.

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery GroupsAlexa for Business

Alexa for Business

1 Room details

2 Add Echo devices

3 Add skill groups

Add skill groups

Alexa for Business uses skill groups to enable skills on the Alexa devices in your rooms. All skills in a group are enabled for all devices in a room, when the group is assigned to the room. Select skill groups to add to your room.

Add

Delete

☐

Name

Description

▼

No results found.

9. Seleccione los grupos de skills que quiere agregar a los dispositivos Alexa de la sala. Haga clic en **Agregar**. Los grupos de skills seleccionados aparecen en la página **Agregar grupos de skills**.

Add skill groups

☐

Name

Description

▼

☐

Catering

Food related skills

☐

testSG2

test

☐

testSG3

test

☐

testSG1

test

Showing 1 - 4 of 4 items

Cancel

Add

10. Haga clic en **Guardar**.

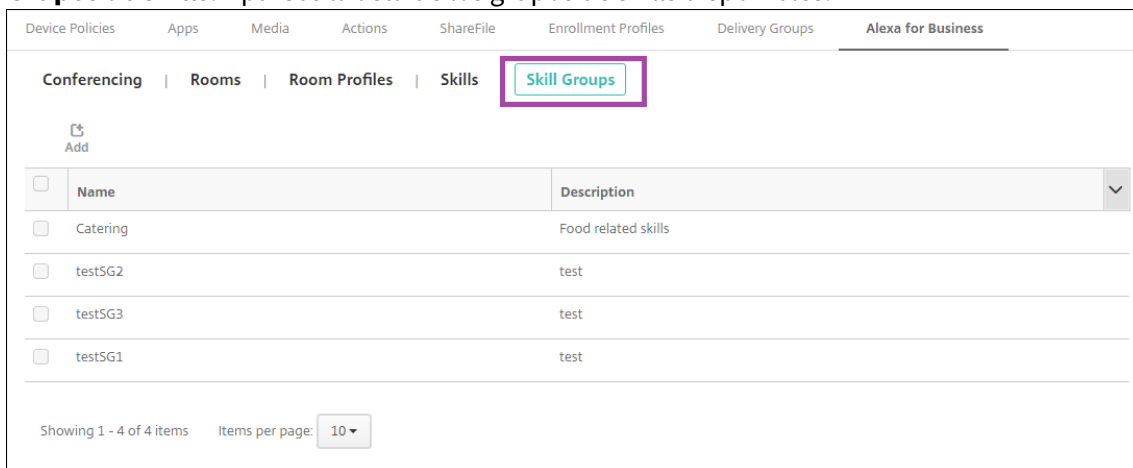
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

345

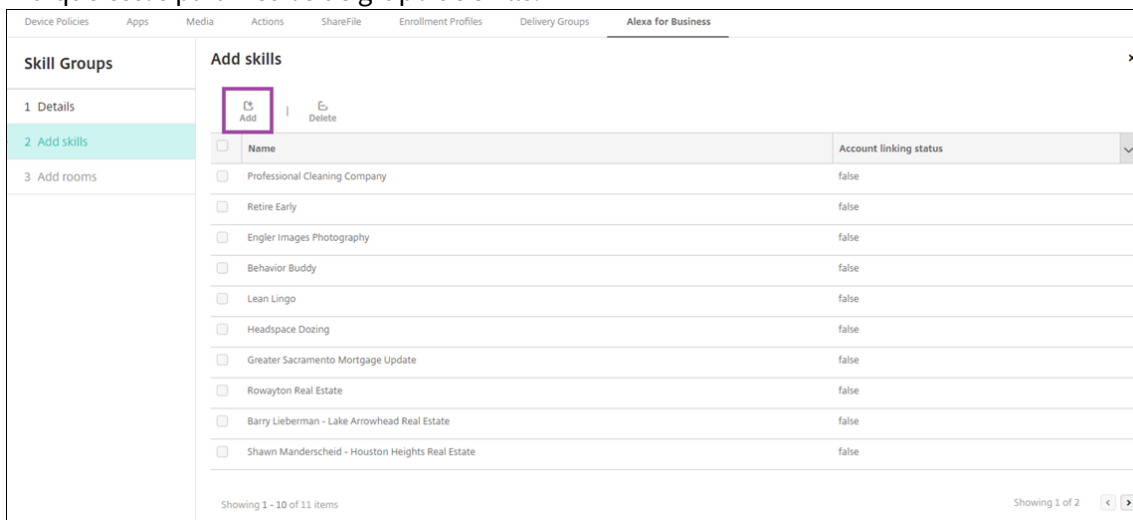
Configurar grupos de skills

Los grupos de skills son colecciones de funciones que se pueden aplicar a una sala. Puede crear un grupo de skills y luego asignarlo a una sala. Las skills permiten usar un dispositivo Alexa para, por ejemplo, iniciar y finalizar una reunión en línea o revisar una lista de elementos de la agenda. Puede agregar, modificar y eliminar grupos de skills.

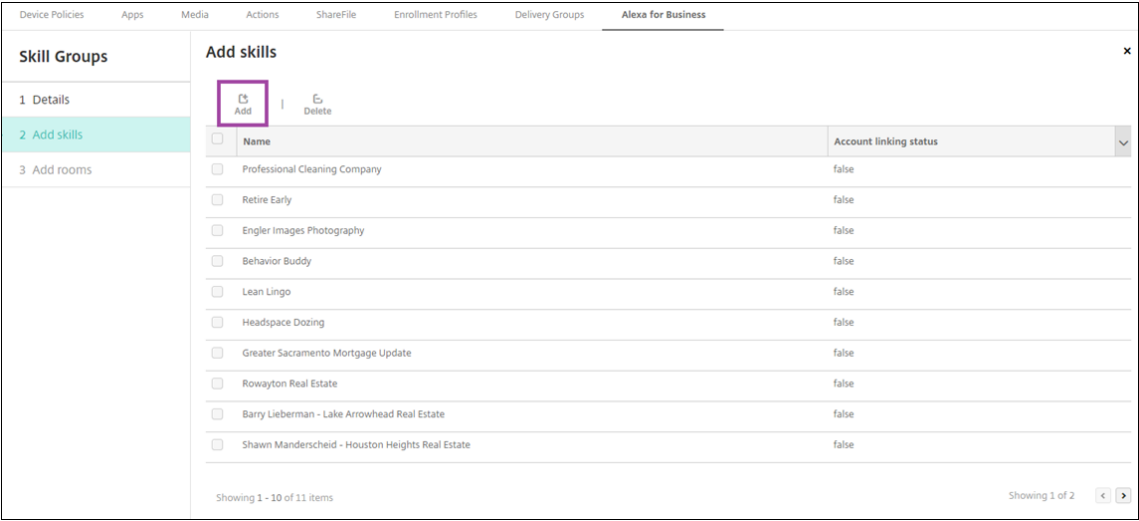
1. En la consola de Citrix Endpoint Management, seleccione **Configurar > Alexa for Business > Grupos de skills**. Aparece la lista de los grupos de skills disponibles.



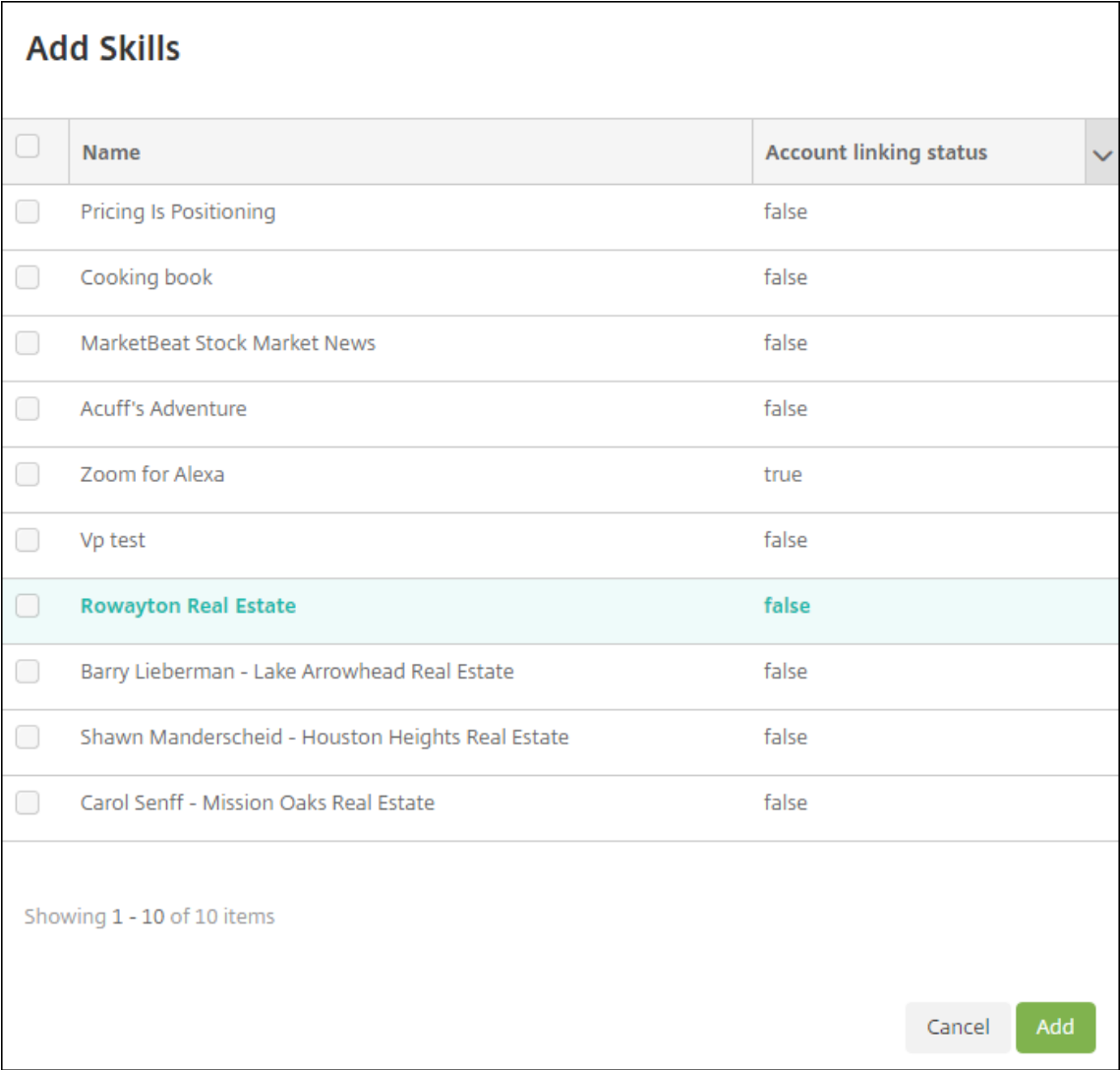
2. Para agregar un grupo de skills, haga clic en **Agregar**. Seleccione el grupo de skills que quiera modificar y haga clic en **Modificar**.
3. Indique estos parámetros de grupo de skills:



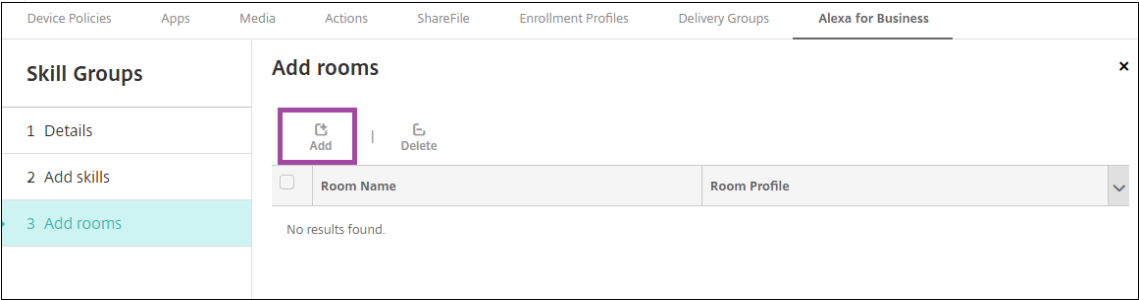
- **Nombre:** Escriba el nombre del grupo de skills.
 - **Descripción:** Escriba una breve descripción del grupo de skills.
4. Haga clic en **Siguiente**.
 5. Para agregar skills a un grupo de skills, haga clic en **Agregar**.



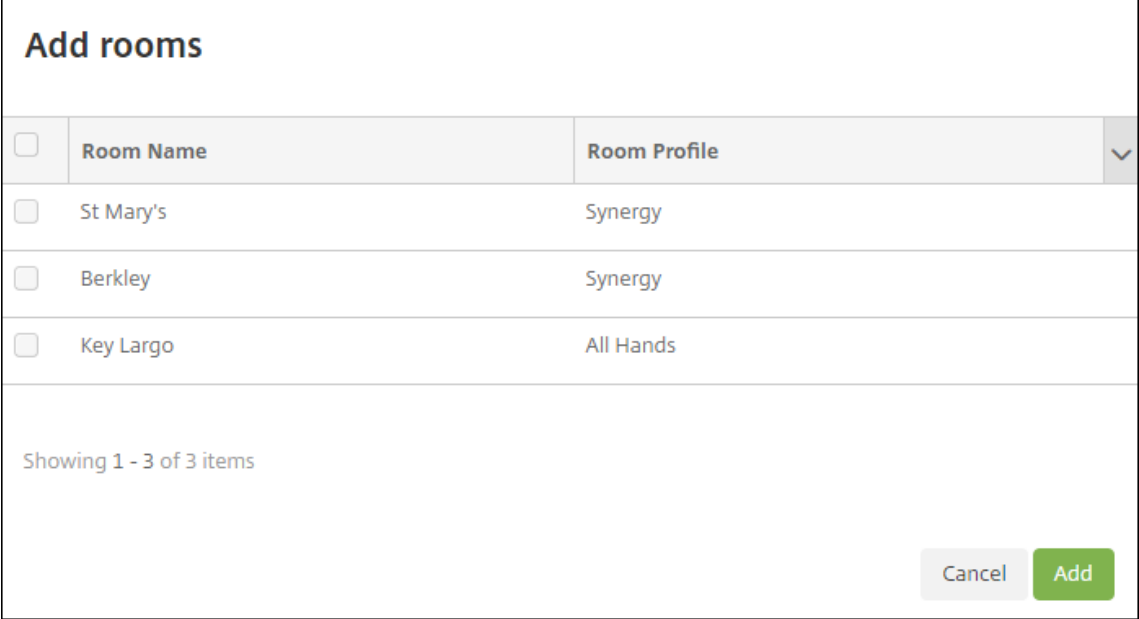
6. Seleccione las skills que quiere incluir en el grupo de skills y haga clic en **Agregar**. Las skills seleccionadas aparecen en la página **Agregar skills**.



7. Para agregar el grupo de skills a los dispositivos Alexa en las salas que indique, haga clic en **Agregar**.



8. Seleccione las salas.



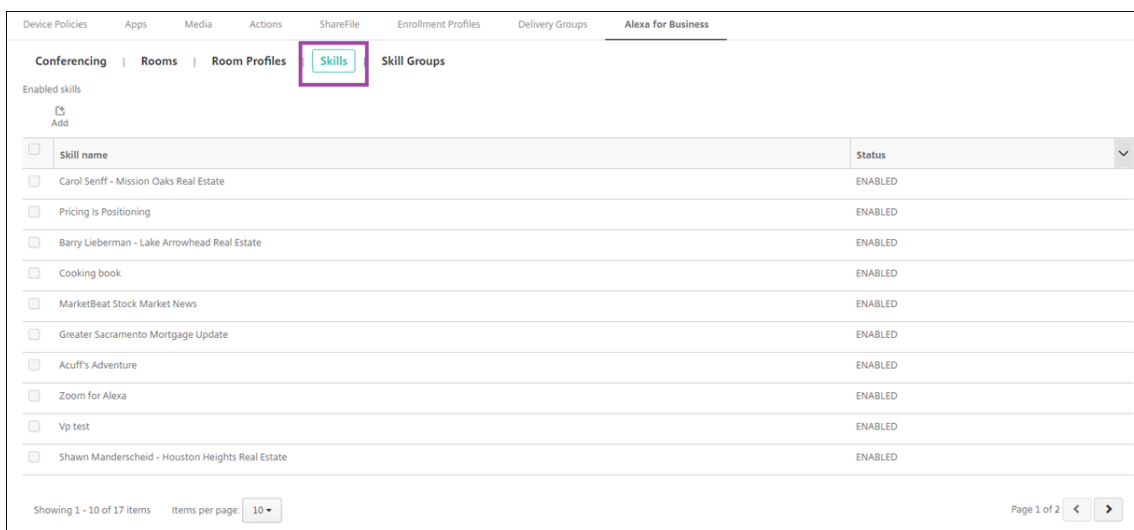
9. Haga clic en **Guardar**.

Poner skills a disposición de los grupos de skills

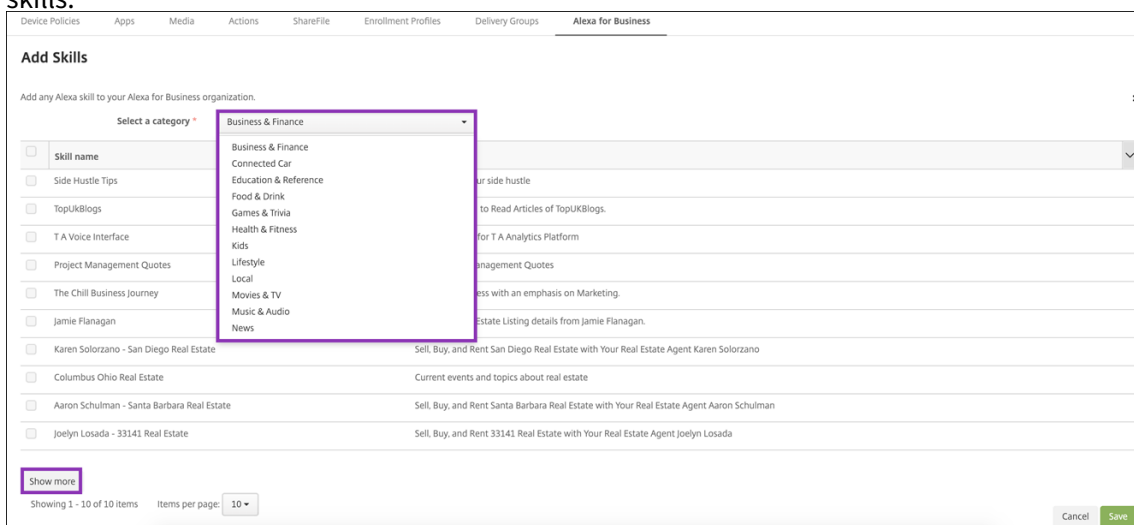
Configure la lista de las skills de Alexa disponibles que se van a incluir en los grupos de skills de Alexa for Business que quiera tener en su organización. Estas skills provienen de la tienda pública de skills de Alexa, o bien se trata de skills privadas que se hayan publicado en su organización.

Agregar skills a la organización

1. En la consola de Citrix Endpoint Management, seleccione **Configurar > Alexa for Business > Skills**. Aparecerá la lista de las skills habilitadas.



2. Para agregar una skill, haga clic en **Agregar**.
3. Para ver más skills de Alexa, seleccione una categoría y haga clic en **Mostrar más**. Al hacer clic en **Mostrar más**, se agrega un máximo de 10 skills a la lista de las skills disponibles que se pueden agregar a la organización. Puede volver a hacer clic en **Mostrar más** para agregar más skills.



4. Seleccione las skills que quiere agregar a la organización.
5. Haga clic en **Guardar**.

Quitar skills de la organización

1. En la consola de Citrix Endpoint Management, seleccione **Configurar > Alexa for Business > Skills**. Aparecerá la lista de las skills habilitadas.
2. Seleccione las skills que quiere quitar de la organización.
3. Haga clic en **Inhabilitar**.

Device Policies | Apps | Media | Actions | ShareFile | Enrollment Profiles | Delivery Groups | **Alexa for Business**

Conferencing | Rooms | Room Profiles | Skills | Skill Groups

Enabled skills

Add | Disable

<input type="checkbox"/>	Skill name	Status
<input type="checkbox"/>	Carol Seriff - Mission Oaks Real Estate	ENABLED
<input checked="" type="checkbox"/>	Pricing Is Positioning	ENABLED
<input type="checkbox"/>	Barry Lieberman - Lake Arrowhead Real Estate	ENABLED
<input type="checkbox"/>	Cooking book	ENABLED
<input type="checkbox"/>	MarketBeat Stock Market News	ENABLED
<input type="checkbox"/>	Greater Sacramento Mortgage Update	ENABLED
<input type="checkbox"/>	Acuff's Adventure	ENABLED
<input type="checkbox"/>	Zoom for Alexa	ENABLED
<input checked="" type="checkbox"/>	Vp test	ENABLED
<input checked="" type="checkbox"/>	Shawn Manderscheid - Houston Heights Real Estate	ENABLED

Showing 1 - 10 of 17 items Items per page: 10 Page 1 of 2

Configurar funciones de conferencias

Las funciones de conferencias permiten definir los proveedores de servicios de conferencias (como Google Hangouts o Amazon Chime). Estos proveedores son quienes controlan la forma en que las personas se unen a las conferencias en las salas que contienen dispositivos Alexa. Puede agregar, modificar y eliminar los proveedores de conferencias. También puede establecer un proveedor de conferencias predeterminado.

1. En la consola de Citrix Endpoint Management, seleccione **Configurar > Alexa for Business > Conferencia**. Aparece la lista de perfiles de sala disponibles.

Device Policies | Apps | Media | Actions | ShareFile | Enrollment Profiles | Delivery Groups | **Alexa for Business**

Conferencing | Rooms | Room Profiles | Skills | Skill Groups

Add

<input type="checkbox"/>	Name	Conferencing Provider	Default
<input type="checkbox"/>	nightwatch_test	GOOGLE_HANGOUTS	Default
<input type="checkbox"/>	Amazon Chime	CHIME	
<input type="checkbox"/>	Example	CHIME	
<input type="checkbox"/>	test test	ZOOM	
<input type="checkbox"/>	test	CHIME	
<input type="checkbox"/>	test SFB	SKYPE_FOR_BUSINESS	

2. Para agregar un proveedor de conferencias, haga clic en **Agregar**. Para modificar un proveedor de conferencias, seleccione el perfil de sala que quiera modificar y haga clic en **Modificar**.
3. Escriba los parámetros del perfil de sala:

- **Proveedor de servicios de conferencias:** Seleccione un proveedor de conferencias de la lista.
- **Nombre:** Escriba el nombre a asignar al proveedor de conferencias.
- **Código PIN de reunión:** Especifique si requerir un PIN para unirse a la reunión.
- **Parámetros del acceso telefónico RTC**
 - **Código de país:** Escriba el código del país.
 - **Número de teléfono:** Escriba el número de teléfono.
 - **Demora de envío de ID de reunión:** Especifique la cantidad de segundos que deben transcurrir antes de que se envíe el ID de reunión.
 - **Demora de envío de código PIN de reunión:** Especifique la cantidad de segundos que deben transcurrir antes de que se envíe el PIN.
- **Parámetros SIP/H323:** Los parámetros de acceso telefónico SIP/H323 se utilizan para unirse a las reuniones mediante el 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 > Conferencia**. Aparece la lista de perfiles de sala disponibles.
2. Seleccione el proveedor de conferencias que quiere establecer como predeterminado.
3. Haga clic en **Establecer como predeterminado**.

Migrar de la administración de dispositivos a Android Enterprise

November 29, 2023

Este artículo describe consideraciones y recomendaciones para migrar desde la administración de dispositivos Android antiguos a Android Enterprise. Google va a retirar la API de administración de dispositivos Android. Esta API admitía aplicaciones de empresa en dispositivos Android. Android Enterprise es la solución moderna de administración que recomiendan Google y Citrix.

Citrix Endpoint Management pasará a utilizar Android Enterprise como método de inscripción pre-determinado para los dispositivos Android. Una vez que Google haya retirado las API, la inscripción fallará en los dispositivos Android Q en el modo de administración de dispositivos.

Android Enterprise admite los modos de dispositivos totalmente administrados y de perfil de trabajo. La publicación de Google, [Android Enterprise Migration Bluebook](#), detalla en qué se diferencian la administración de dispositivos antiguos y Android Enterprise. Le recomendamos que lea la información sobre migración de Google.

Le recomendamos que también consulte el artículo de Citrix Tech Zone, [Migration from Android Device Administrator to Android Enterprise with Citrix Endpoint Management](#).

Impacto de los elementos retirados de la administración de dispositivos

Google ha retirado las API de Administrador de dispositivos y no las admite desde el 2 de noviembre de 2020. Estas API no funcionarán en dispositivos con Android 10 o una versión posterior después de actualizar Citrix Secure Hub al nivel 29 de API de Android:

- **Inhabilitar cámara:** controla el acceso a las cámaras del dispositivo.
- **Keyguard features:** Controla las funciones relacionadas con el bloqueo de dispositivos, como la biometría y los patrones.
- **Contraseña con caducidad:** obliga a los usuarios a cambiar su contraseña después de un período de tiempo configurable.
- **Limit password:** Establece requisitos restrictivos para las contraseñas.

Requisitos y recomendaciones

- Si puede actualizar la versión de un dispositivo a Android 10 o una versión posterior, debe inscribirlo en Android Enterprise.
 - Los dispositivos Android 11 deben inscribirse en Android Enterprise.

- A partir de septiembre de 2020 (para dispositivos Android 10): Citrix no admite nuevas inscripciones o reinscripciones de dispositivos en el modo de administración de dispositivos. Los dispositivos ya inscritos continuarán funcionando hasta el 2 de noviembre de 2020, como se indica en la sección anterior.
- Para los dispositivos con Android 9 y versiones anteriores, se admite el modo de administración de dispositivos antiguos. Sin embargo, se recomienda transferir esos dispositivos a Android Enterprise lo antes posible.
- Para dispositivos nuevos o existentes inscritos en el modo solo MAM de Citrix, no es necesario realizar ninguna acción. Las API de Google retiradas no afectan de ninguna manera a los dispositivos en el modo solo MAM. Sin embargo, con el paso al cifrado de plataforma, se recomienda encarecidamente cambiar 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 del dispositivo.

Análisis

La fase de análisis de la migración consiste en:

- Comprender la configuración de Android heredado
- Documentar la configuración antigua para que se puedan asignar funciones antiguas a las funciones de Android Enterprise

Análisis recomendado

1. Evalúe Android Enterprise en Citrix Endpoint Management: Totalmente administrado, totalmente administrado con perfil de trabajo, dispositivo dedicado, perfil de trabajo (BYOD).
2. Analice las funciones actuales de la administración de dispositivos y compárelas con Android Enterprise.
3. Documente los casos de uso de la administración de dispositivos.

Para documentar los casos de uso de la administración de dispositivos:

1. Cree una hoja de cálculo y enumere los grupos de directivas actuales que hay en la consola de Citrix Endpoint Management.
2. Cree casos de uso independientes en función de los grupos de directivas existentes.
3. Para cada caso de uso, documente lo siguiente:
 - Nombre

- Propietario de una empresa
- Modelo de identidad de usuario
- Requisitos de dispositivo
 - Seguridad
 - Administración
 - Usabilidad
- Inventario de dispositivos
 - Marca y modelo
 - Versión de SO
- Apps

4. Para cada aplicación, indique lo siguiente:

- Nombre de la aplicación
- Nombre del paquete
- Método de alojamiento
- Si la aplicación es pública o privada
- Si la aplicación es obligatoria (verdadero/falso)

Asignación de requisitos

En función del análisis completado, determine los requisitos de las funciones de Android Enterprise.

Asignación recomendada de requisitos

1. Determine el modo de administración y el método de inscripción:
 - Perfil de trabajo (BYOD): Requiere volver a inscribirse. No es necesario restablecer los valores de fábrica.
 - Totalmente administrado: Requiere restablecer los valores de fábrica. Inscriba dispositivos mediante códigos QR, conexiones de transmisión de datos en proximidad (NFC), identificadores de controladores de directivas de dispositivo (DPC) o aprovisionamiento automático.
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 a su correspondiente versión de Android.

4. Determine el SO de Android mínimo en función de los requisitos de las funciones (7.0, 8.0, 9.0).
5. Elija un modelo de identidad:
 - Recomendado: Cuenta de Google Play administrado.
 - Usar cuentas de Google Workspace solamente si es cliente de Google Cloud Identity
6. Cree una estrategia de dispositivos:
 - Sin acción: Si los dispositivos cumplen el nivel mínimo de SO.
 - Actualización: Si los dispositivos son compatibles con el SO y pueden actualizarse a su versión.
 - Reemplazo: Si los dispositivos no se pueden actualizar al nivel del SO compatible.

Estrategia de migración de aplicaciones recomendada

Después de completar la asignación de requisitos, mueva las aplicaciones de la plataforma Android a la plataforma Android Enterprise. Para obtener información detallada sobre la publicación de aplicaciones, consulte [Agregar aplicaciones](#).

- Aplicaciones de la tienda pública de aplicaciones
 1. Seleccione las aplicaciones que quiere migrar y, a continuación, modifique las aplicaciones para desmarcar el parámetro de Google Play y seleccionar **Android Enterprise** como plataforma.
 2. Seleccione el grupo de entrega. Si una aplicación es obligatoria, muévela a la lista **Aplicaciones obligatorias** del grupo de entrega.

Después de guardar una aplicación, aparecerá en la tienda de Google Play. Si tiene un perfil de trabajo, las aplicaciones aparecen en la tienda de Google Play en el perfil de trabajo.

- Aplicaciones privadas (de empresa)

Las aplicaciones privadas se desarrollan en equipos internos o en un desarrollador externo. Le recomendamos que publique las aplicaciones privadas mediante Google Play.

1. Seleccione las aplicaciones que quiere migrar y, a continuación, modifique las aplicaciones para seleccionar **Android Enterprise** como plataforma.
2. Cargue el archivo APK y, a continuación, configure los parámetros de la aplicación.
3. Publique la aplicación en el grupo de entrega requerido.

- Aplicaciones MDX

1. Seleccione las aplicaciones que quiere migrar y, a continuación, modifique las aplicaciones para seleccionar **Android Enterprise** como plataforma.
2. Cargue el archivo MDX. Siga el proceso de aprobación de las aplicaciones.
3. Seleccione las directivas MDX.

Para las aplicaciones MDX de Enterprise, recomendamos cambiarlas a aplicaciones empaquetadas en modo MDX SDK:

- Opción 1: Aloje el archivo 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 de empresa. Publique el archivo APK en Citrix Endpoint Management y seleccione la plataforma **Android Enterprise** para el archivo MDX.

Migración de directivas de dispositivos Citrix

En cuanto a las directivas que están disponibles para las plataformas **Android (AD heredado)** y **Android Enterprise**, modifique la directiva correspondiente y seleccione la plataforma **Android Enterprise**.

- Para Android Enterprise, considere el método de inscripción de dispositivos. Algunas opciones de directiva solo están disponibles para dispositivos en modo de perfil de trabajo o modo totalmente administrado. Consulte [Configurar directivas de aplicaciones y de dispositivo para Android Enterprise](#).
- Si utiliza la directiva Exchange para dispositivos AD heredados, cree una directiva Configuraciones administradas para configurar los parámetros del correo electrónico.
- Para asegurarse de que destina una directiva a los dispositivos previstos (Android Enterprise frente a AD heredado), agregue una regla de implementación a la directiva. Por ejemplo, para la plataforma AD heredada, utilice esta regla de implementación:

```
1 Limit by known device property name Android Enterprise
2 Enabled Device? Isn't equal to true
3 <!--NeedCopy-->
```

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 AD heredado.

Prueba de concepto

Después de migrar aplicaciones a Android Enterprise, puede configurar una prueba de migración para comprobar que las funciones operan según lo previsto.

Configuración de la prueba de concepto recomendada

1. Configure la infraestructura de implementación:
 - Cree un grupo de entrega para sus pruebas de Android Enterprise.
 - Configure Android Enterprise en Citrix Endpoint Management.
2. Configure aplicaciones de usuario.
3. Configure las funciones de Android Enterprise.
4. Asigne directivas al grupo de entrega de Android Enterprise.
5. Pruebe las funciones y confírmelas.
6. Complete una guía de configuración de dispositivos para cada caso de uso.
7. Documente los pasos de configuración para los usuarios.

Implementación

Ahora puede implementar la configuración de Android Enterprise y preparar a sus usuarios para la migración.

Estrategia de implementación recomendada

La estrategia de implementación recomendada por Citrix consiste en probar todos los sistemas de producción para Android Enterprise y, más tarde, completar la migración de dispositivos.

- En este caso, los usuarios siguen utilizando dispositivos antiguos con su configuración actual. Configure nuevos dispositivos para la administración de Android Enterprise.
- Migre los dispositivos existentes solamente cuando sea necesario realizar una actualización o sustitución.
- Migre los dispositivos existentes a la administración de Android Enterprise al final de su ciclo de vida habitual. Si no, migre dichos dispositivos cuando deban reemplazarse si se pierden o se estropean.

Android Enterprise

December 13, 2023

Android Enterprise es un conjunto de herramientas y servicios proporcionados por Google como una solución de administración empresarial para dispositivos Android. Con Android Enterprise:

- Puede utilizar Citrix Endpoint Management para administrar dispositivos Android que sean propiedad de la empresa y dispositivos Android BYOD.
- Puede administrar todo el dispositivo o un perfil independiente en el dispositivo. Ese perfil independiente aísla las cuentas, las aplicaciones y los datos empresariales de las cuentas por un lado, y las aplicaciones y los datos personales por el otro.
- También puede administrar dispositivos dedicados a un solo uso, como la administración de inventario. Para obtener una descripción general de Google sobre lo que puede hacer Android Enterprise, consulte [Android Enterprise Management](#).

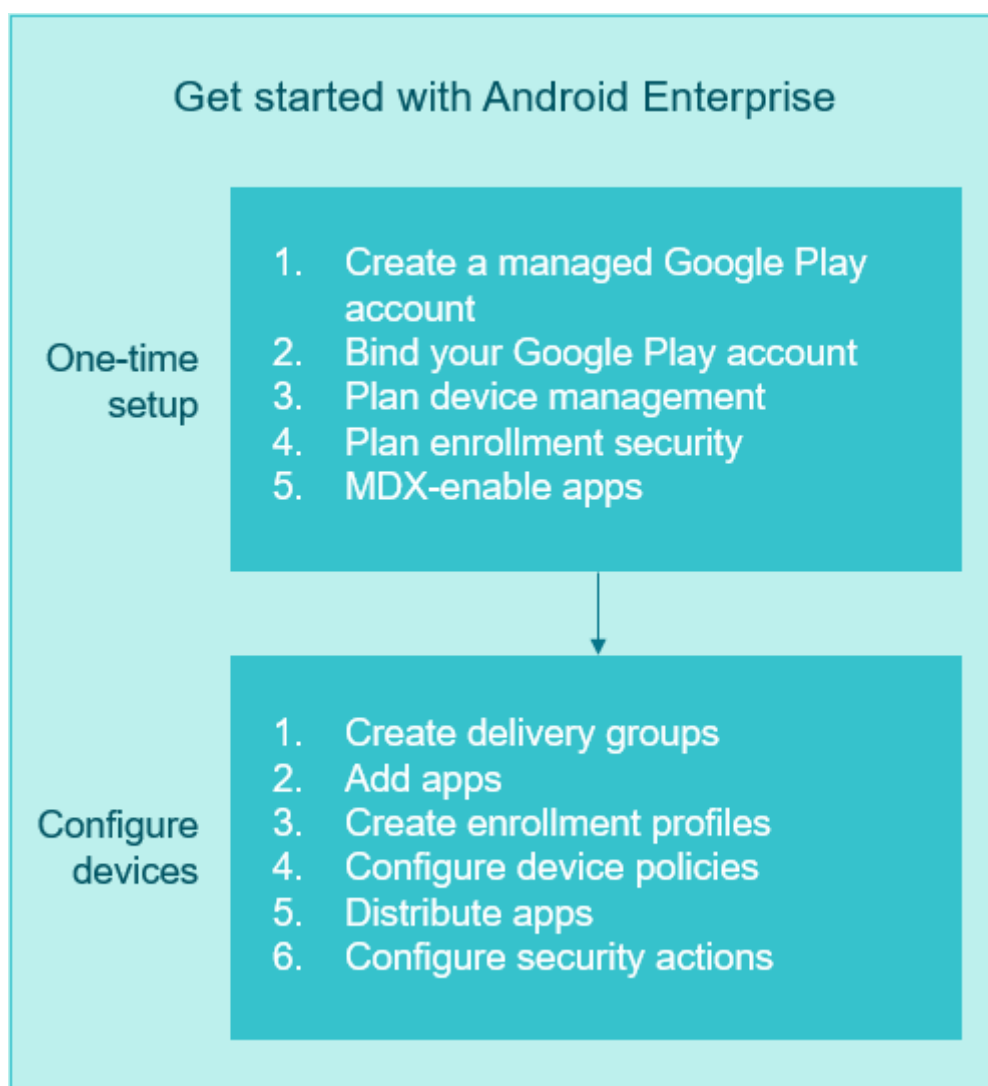
Recursos:

- Para obtener una lista de términos y definiciones relacionados con Android Enterprise, consulte [Android Enterprise terminology](#) en la guía para desarrolladores de Google 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 compatibles](#).
- Para obtener información sobre las conexiones salientes que se deben tener en cuenta al configurar entornos de red para Android Enterprise, consulte el artículo [Android Enterprise Network Requirements](#) de la asistencia técnica de Google.
- Para obtener información sobre cómo implementar Android Enterprise, consulte [Implementar recursos](#)).

Introducción a Android Enterprise

Importante:

Ya no se admite el modo de administración de dispositivos. Si los usuarios tienen dispositivos en el modo de administración de dispositivos, consulte [Migrar de la administración de dispositivos a Android Enterprise](#). Después de migrar los dispositivos a Android Enterprise, siga estos pasos para configurar dispositivos Android Enterprise.



Configuración de una sola vez

1. Cree una cuenta de Google Play administrado.

Consulte Usar Google Play administrado con Citrix Endpoint Management y Requisitos.

2. Vincule la cuenta de Google Play con Citrix Endpoint Management.

Consulte Conectar Citrix Endpoint Management a Google Play.

3. Decida cómo administrar los dispositivos.

Consulte Perfiles y casos de implementación de dispositivos.

4. Planifique la seguridad presente en la inscripción de los dispositivos de usuario.

Consulte Seguridad de la inscripción.

5. Prepare aplicaciones habilitadas para MDX para entregarlas.

Utilice el SDK de MAM para desarrollar las aplicaciones. O bien, si no lo tiene todo listo para realizar la transición al nuevo SDK, utilice el MDX Toolkit basado en línea de comandos para empaquetar las aplicaciones.

Consulte [Introducción al SDK de MAM](#).

Ahora lo tiene todo listo para configurar sus dispositivos Android Enterprise con directivas de aplicación y dispositivo, perfiles de inscripción y aplicaciones. Consulte la siguiente sección para obtener directrices.

Configurar dispositivos

1. Cree grupos de entrega.

Con ello, podrá decidir quién obtiene qué recursos y cuándo los obtienen. Consulte [Implementar recursos](#).

Dejaremos de ofrecer aplicaciones publicadas para la plataforma AD heredada a los dispositivos inscritos en Android Enterprise. Para los dispositivos Android Enterprise, debe publicar aplicaciones para la plataforma Android Enterprise. Para continuar publicando aplicaciones en modo AD heredado para dispositivos en modo AD, cree un grupo de entrega aparte para esas aplicaciones. Consulte [Elementos retirados](#).

2. Agregue aplicaciones. Puede aprobar las aplicaciones en Google Play directamente desde la consola de Citrix Endpoint Management.

Consulte el artículo de asistencia de Google [Manage apps in your organization](#).

3. Cree perfiles de inscripción.

Especifique las opciones de administración de dispositivos y aplicaciones que sean necesarias para la inscripción. Consulte [Perfiles y casos de implementación de dispositivos y Crear perfiles de inscripción](#).

- Cuando se implementa una aplicación de tienda pública de Android Enterprise al usuario de un dispositivo Android, ese usuario se inscribe automáticamente en Android Enterprise.
- La activación automática le permite configurar los dispositivos para que se inscriban automáticamente cuando se enciendan por primera vez. Consulte [Activación automática](#).

4. Configure las directivas de dispositivo y aplicación.

Equilibre la seguridad empresarial con la privacidad del usuario y la experiencia del usuario. Consulte [Configurar directivas de aplicaciones y de dispositivo para Android Enterprise](#).

5. Distribuya las aplicaciones.

Se utiliza Google Play administrado para agregar, comprar y aprobar aplicaciones para implementarlas en el espacio de trabajo de Android Enterprise del dispositivo. Los usuarios solo podrán instalarse las aplicaciones de Google Play administrado que usted haya puesto a su disposición.

Consulte:

- [Distribuir aplicaciones de Android Enterprise](#)
- [Directiva de configuraciones administradas](#)
- [Directiva de permisos de aplicación](#)

6. Configure acciones de seguridad para supervisar y ofrecer el cumplimiento de normas.

Consulte Acciones de seguridad.

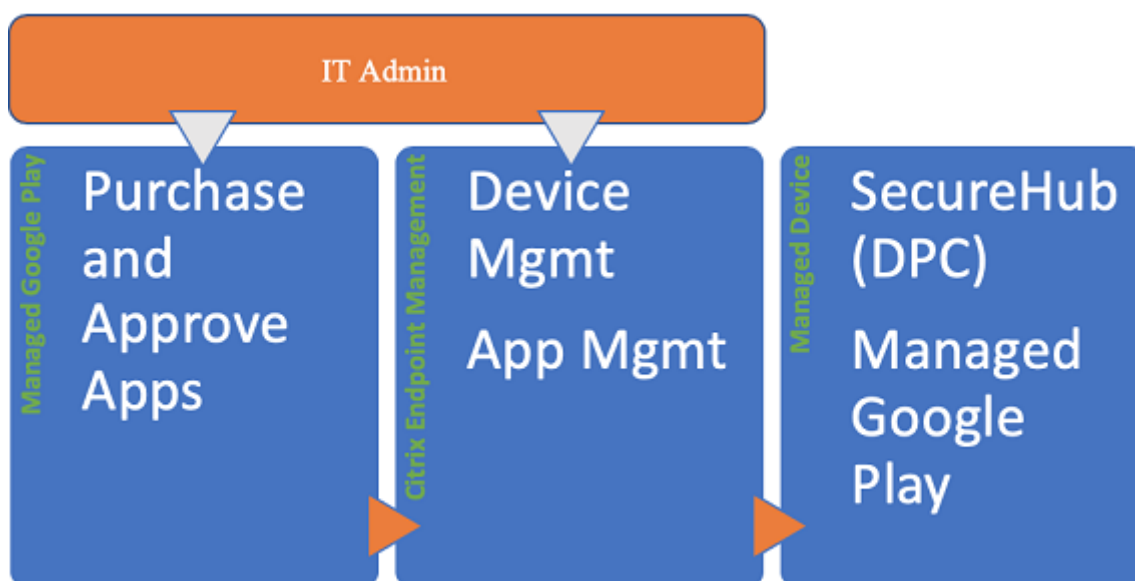
Usar Google Play administrado con Citrix Endpoint Management

Al integrar Citrix Endpoint Management en Google Play administrado para utilizar Android Enterprise, se crea una empresa. Google define una empresa como un vínculo entre la organización y la solución de administración móvil empresarial (EMM). Todos los usuarios y los dispositivos que la organización administra a través de esa solución pertenecen a la empresa.

Una empresa de Android Enterprise tiene tres componentes: una solución EMM, una aplicación de controlador de directivas de dispositivos (DPC) y una plataforma de aplicaciones de empresa de Google. Al integrar Citrix Endpoint Management en Android Enterprise, la solución completa tiene estos componentes:

- **Citrix Endpoint Management:** La administración de movilidad empresarial (EMM) de Citrix. Citrix Endpoint Management es la Citrix Endpoint Management unificada para un espacio de trabajo digital y seguro. Citrix Endpoint Management proporciona los medios para que los administradores de TI gestionen dispositivos y aplicaciones para sus organizaciones.
- **Citrix Secure Hub:** La aplicación DPC de Citrix. Citrix Secure Hub es el panel de inicio de Citrix Endpoint Management. Citrix Secure Hub aplica directivas en el dispositivo.
- **Google Play administrado:** Una plataforma de aplicaciones de empresa de Google que se integra en Citrix Endpoint Management. La API de EMM de Google Play establece directivas de aplicación y distribuye aplicaciones.

En esta ilustración se muestra cómo interactúan los administradores con estos componentes y cómo interactúan los componentes entre sí:

**Nota:**

Puede utilizar Google Play administrado o Google Workspace (antes denominado G Suite) para registrar Citrix como su proveedor EMM. En este artículo se analiza el uso de Android Enterprise con Google Play administrado. Si su organización usa Google Workspace para ofrecer acceso a las aplicaciones, puede utilizarlo con Android Enterprise. Consulte [Android Enterprise heredado para clientes de Google Workspace](#).

Al utilizar Google Play administrado, puede aprovisionar cuentas de Google Play administrado para dispositivos y usuarios finales. Las cuentas de Google Play administrado proporcionan acceso a Google Play administrado, lo que permite a los usuarios instalar y utilizar las aplicaciones que ponga a su disposición. Si su organización utiliza un servicio de identidad de terceros, puede vincular las cuentas de Google Play administrado a las cuentas de identidad existentes.

Puesto que las empresas de este tipo no están vinculadas a un dominio, puede crear más de una empresa para una sola organización. Por ejemplo, cada departamento o región 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 de usuario y las funciones de la tienda de aplicaciones de Google Play con un conjunto de funciones de gestión diseñadas para las empresas. Se utiliza Google Play administrado para agregar, comprar y aprobar aplicaciones para implementarlas en el espacio de trabajo de Android Enterprise del dispositivo. Se puede utilizar Google Play para implementar aplicaciones públicas, privadas y de terceros.

Para los usuarios de dispositivos administrados, Google Play administrado es la tienda de aplicaciones de empresa. Los usuarios pueden explorar aplicaciones, ver los detalles de la aplicación e

instalarlas. A diferencia de la versión pública de Google Play, los usuarios solo podrán instalar las aplicaciones de Google Play administrado que usted haya puesto a su disposición.

Perfiles y casos de implementación de dispositivos

Los casos de implementación de dispositivos se distinguen en función de a quién pertenecen los dispositivos que usted implementa y cómo los administra usted. En cambio, los perfiles de dispositivo se distinguen en función de cómo el DPC administra y aplica las directivas en los dispositivos.

Un perfil de trabajo aísla las cuentas, las aplicaciones y los datos de empresa por un lado, y las cuentas, las aplicaciones y los datos personales por el otro. Los perfiles de trabajo y los perfiles personales se separan a nivel de 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 actualicen a la versión 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 [Changes ahead for Android Enterprise’s Fully Managed with Work Profile](#). Para dispositivos con 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 profesional	No	No	Solo para dispositivos nuevos o de restablecimiento de fábrica. Consulte Aprovechar dispositivos Android Enterprise totalmente administrados.

Administración de dispositivos	Casos de uso	Perfil de trabajo	Perfil personal	Notas
Totalmente administrado con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa	Dispositivos propiedad de la empresa destinados al uso personal y profesional	Sí	Sí. En estos dispositivos, se ejecutan dos copias del DPC: Una administra el dispositivo en modo propietario del dispositivo y la otra administra el perfil de trabajo en modo propietario del perfil. Puede aplicar directivas independientes al dispositivo y al perfil de trabajo.	Consulte Aprovevisionar dispositivos Android Enterprise totalmente administrados con un perfil de trabajo o un perfil de trabajo en dispositivos propiedad de la empresa.
Dispositivos dedicados*	Dispositivos propiedad de la empresa configurados para un solo caso de uso, como la señalización digital o la impresión de tíquets	No	No	Consulte Aprovevisionar dispositivos Android Enterprise dedicados.

Administración de dispositivos	Casos de uso	Perfil de trabajo	Perfil personal	Notas
Perfil de trabajo BYOD**	Dispositivos personales inscritos en la administración del perfil de trabajo (también conocido como modo propietario del perfil)	Sí	Sí. DPC administra solo el perfil de trabajo, no todo el dispositivo.	Estos dispositivos no necesitan ser nuevos ni haberse restablecido a los valores de fábrica. Consulte Aprovechamiento de dispositivos de perfil de trabajo en 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 relacionado con la aplicación, no con el dispositivo.

** Citrix Endpoint Management no admite dispositivos Zebra en el modo 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 posibilidad de que los usuarios se excluyan de MDM.

Para obtener información sobre la especificación del nivel de seguridad y los pasos necesarios para la inscripción, consulte [Inscripción, roles y cuentas de usuario](#).

Citrix Endpoint Management admite los siguientes métodos de autenticación para dispositivos Android inscritos en MDM o MDM+MAM. Para obtener información, consulte estos artículos:

- [Autenticación de dominios o dominio y token de seguridad](#)
- [Autenticación con certificado de cliente o certificado y dominio](#)
- Proveedores de identidades:
 - [Autenticación con Azure Active Directory a través de Citrix Cloud](#) (Tech Preview)
 - [Autenticación con Okta a través de Citrix Cloud](#) (Tech Preview)

Otro método de autenticación que rara vez se utiliza es el certificado de cliente junto con el token de seguridad. Para obtener información, consulte <https://support.citrix.com/article/CTX215200>.

Requisitos

Antes de comenzar a usar Android Enterprise, necesita:

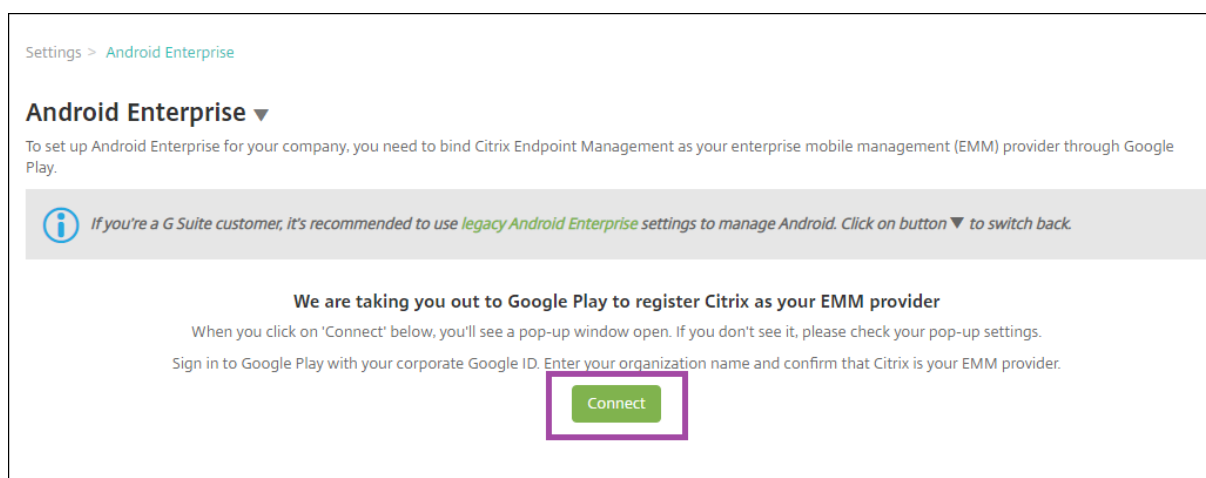
- Cuentas y credenciales:
 - Para configurar Android Enterprise con Google Play administrado, una cuenta corporativa de Google
 - Para descargar los archivos MDX más recientes, una cuenta de cliente de Citrix
- Firebase Cloud Messaging (FCM) y una directiva Programación de conexiones configurada para Citrix Endpoint Management. Consulte [Firebase Cloud Messaging](#) y [Directiva de programación de conexiones](#).

Conectar Citrix Endpoint Management a Google Play

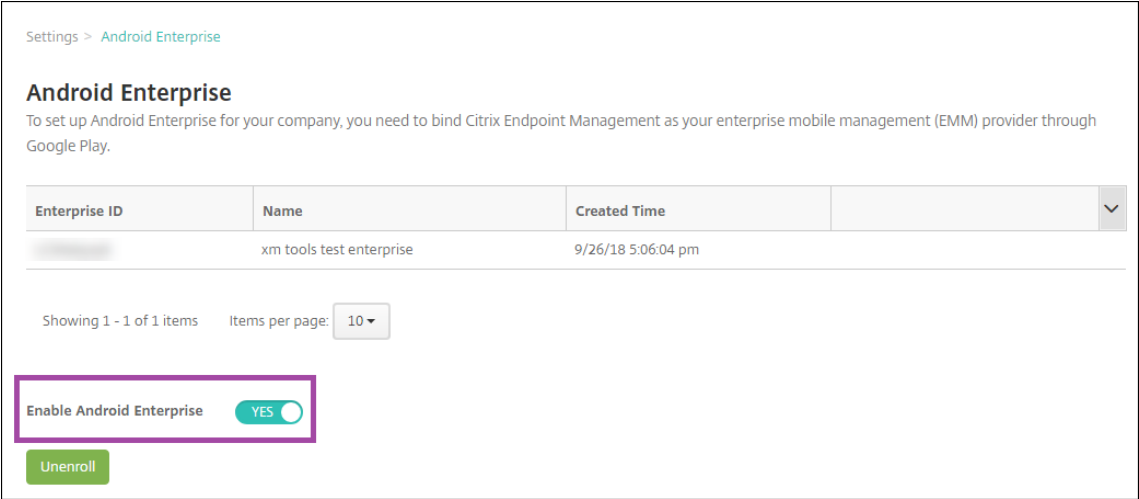
Para configurar Android Enterprise en su organización, registre Citrix como su proveedor de EMM a través de Google Play administrado. Esta configuración conecta Google Play administrado con Citrix Endpoint Management y crea una empresa para Android Enterprise en Citrix Endpoint Management.

Necesita una cuenta corporativa de Google para iniciar sesión en Google Play.

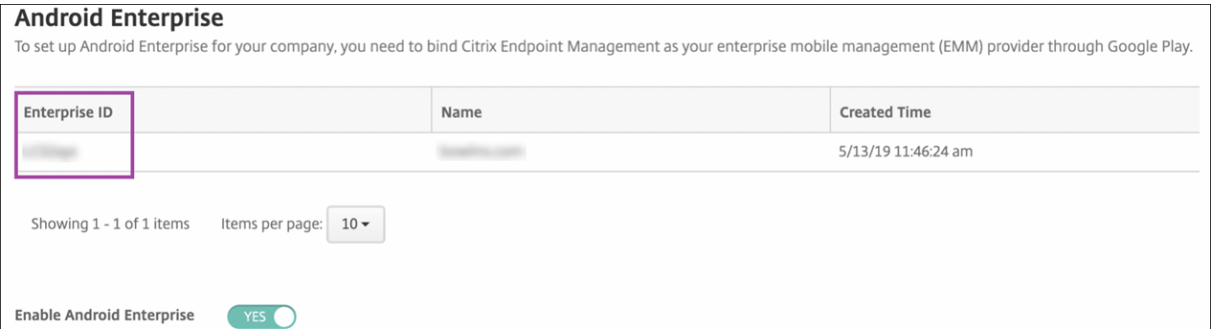
1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Android Enterprise**.
2. Haga clic en **Connect**. Se abre Google Play.



1. Inicia sesión en Google Play con las credenciales de su cuenta corporativa de Google. Introduzca el nombre de su organización y confirme que Citrix es su proveedor de EMM.
2. Se agrega una ID de empresa para Android Enterprise. Para habilitar Android Enterprise, ajuste **Habilitar Android Enterprise** en **Sí**.



El ID de Enterprise aparece en la consola de Citrix Endpoint Management.



Su entorno está conectado a Google y está listo para administrar los dispositivos. Ya puede proporcionar aplicaciones a los usuarios.

Citrix Endpoint Management puede ofrecer a los usuarios aplicaciones móviles de productividad de Citrix, aplicaciones MDX, aplicaciones de tiendas públicas, aplicaciones web y SaaS, aplicaciones de empresa y enlaces web. Para obtener más información sobre cómo proporcionar estos tipos de aplicaciones a los usuarios, consulte [Distribuir aplicaciones de Android Enterprise](#).

En esta sección se muestra cómo ofrecer aplicaciones de productividad móvil.

Proporcionar aplicaciones móviles de productividad de Citrix a usuarios de Android Enterprise

Para proporcionar aplicaciones móviles de productividad de Citrix a usuarios de Android Enterprise, debe seguir estos pasos.

1. Publique las aplicaciones como aplicaciones MDX. Consulte Configurar aplicaciones como aplicaciones MDX.
2. Configure las reglas para el desafío de seguridad que emplean los usuarios con el fin de acceder a los perfiles de trabajo de sus dispositivos. Consulte Configurar la directiva de desafío de seguridad.

Las aplicaciones que publique están disponibles para los dispositivos inscritos de su empresa de Android Enterprise.

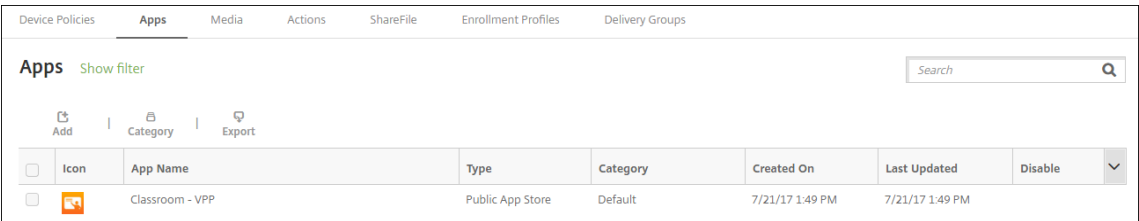
Nota:


Cuando implementa una aplicación de tienda pública de Android Enterprise en un usuario de dispositivo 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**.



Apps						
Show filter						
Search						
Add Category Export						
<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated
<input type="checkbox"/>		Classroom - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM

2. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the [MDX Service](#) to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: Secure Mail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

- Haga clic en **MDX**. Aparecerá la página **Información de la aplicación**.
- En el lado izquierdo de la página, seleccione **Android Enterprise** como plataforma.
- En la página **Información de la aplicación**, escriba la información siguiente:
 - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en **Nombre de la aplicación**, en la tabla **Aplicaciones**.
 - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
 - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte [Acerca de las categorías de aplicaciones](#).
- Haga clic en **Siguiente**. Aparecerá la página **Aplicación MDX para Android Enterprise**.
- Haga clic en **Cargar** y vaya a la ubicación de los archivos .mdx para la aplicación. Seleccione el archivo y haga clic en **Abrir**.
- La interfaz de usuario le notifica si la aplicación adjunta requiere la aprobación de Google Play Store administrado. Para aprobar la aplicación sin salir de la consola de Citrix Endpoint Management, haga clic en **Sí**.

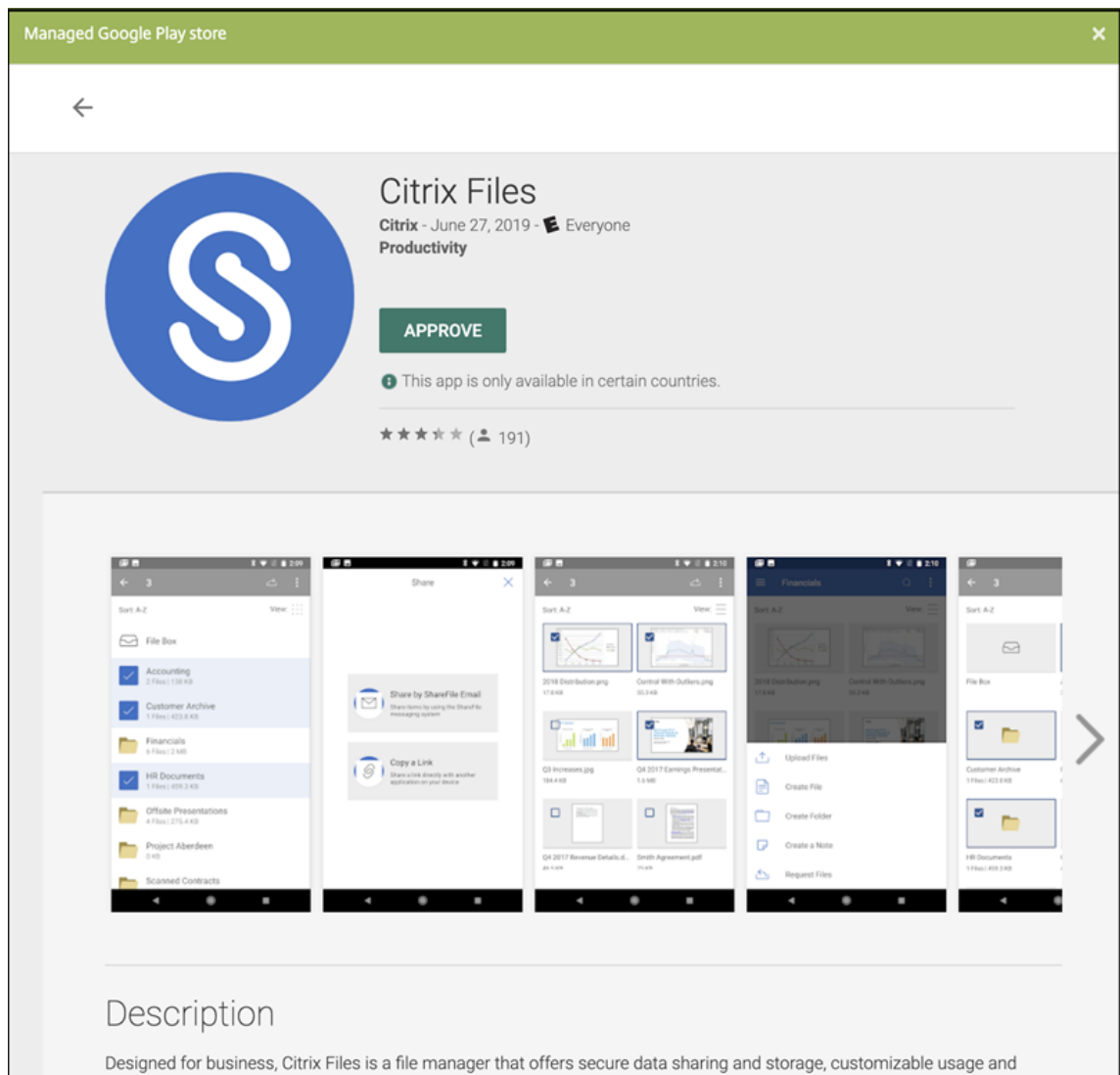
App is not approved

App is not approved on the managed Google Play store. You can approve the app now or later. Do you want to approve it now?

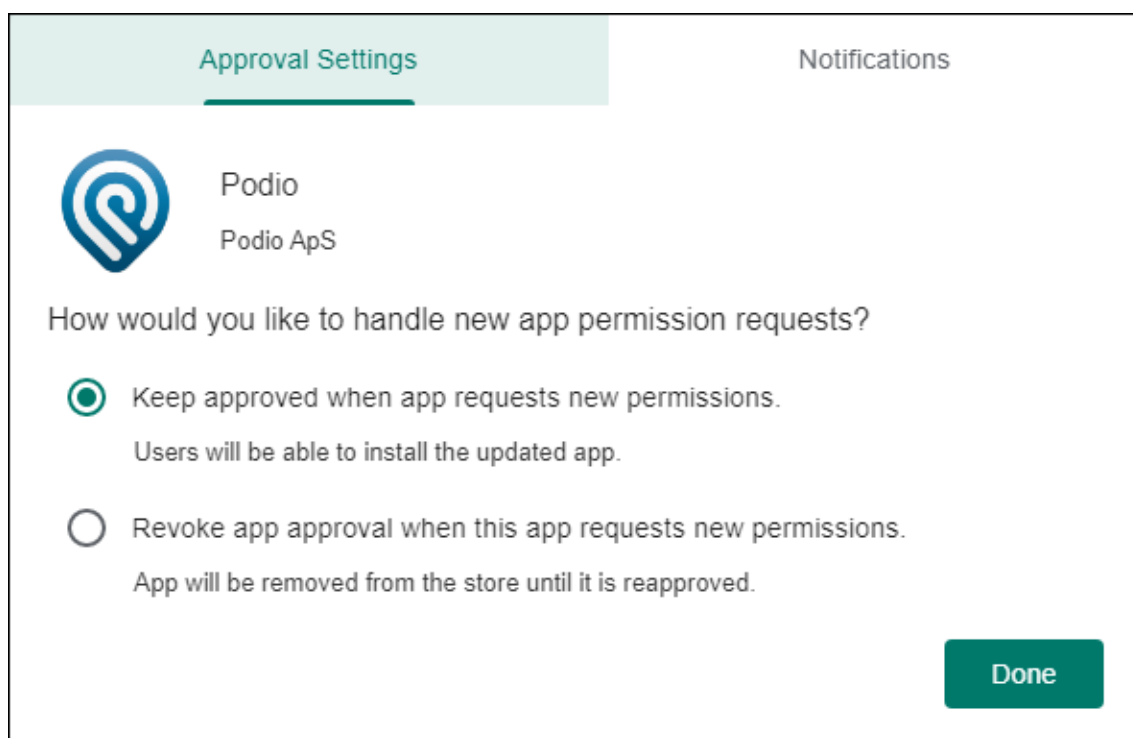
No

Yes

9. Cuando se abra la página de Google Play Store administrado, haga clic en **Approve**.




10. Vuelva a hacer clic en **Approve**.
11. Seleccione **Keep approved when app requests new permissions**. Haga clic en **Guardar**.



The screenshot shows the 'Approval Settings' tab for the 'Podio' app (Podio ApS). The question is 'How would you like to handle new app permission requests?'. There are two radio button options: 'Keep approved when app requests new permissions.' (selected) and 'Revoke app approval when this app requests new permissions.' A 'Done' button is at the bottom right.

Approval Settings

Notifications

 Podio
Podio ApS

How would you like to handle new app permission requests?

☒ Keep approved when app requests new permissions.
Users will be able to install the updated app.

☐ Revoke app approval when this app requests new permissions.
App will be removed from the store until it is reapproved.

Done

12. Cuando se aprueba y guarda la aplicación, aparecen más parámetros en la página. Configure estos parámetros:

- **Nombre de archivo:** Escriba el nombre del archivo asociado a la aplicación.
- **Descripción de la aplicación:** Escriba una descripción de la aplicación.
- **Seguimiento del producto:** Especifique qué tipo de seguimiento de producto quiere enviar a los dispositivos de usuario. Si tiene un seguimiento diseñado para prueba, puede seleccionarlo y asignárselo a sus usuarios. El valor predeterminado es Producción.
- **Versión de la aplicación:** Si quiere, escriba el número de versión de la aplicación.
- **ID del paquete:** La URL de la aplicación de Google Play Store.
- **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
- **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
- **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.

13. Configure las **directivas MDX**. Para obtener más información sobre directivas para aplicaciones MDX, consulte [Vista general de las directivas MDX](#) e [Introducción al SDK de MAM](#).
14. Configurar las reglas de implementación. Para obtener información, consulte [Implementar recursos](#).
15. Expanda **Configuración del almacén**. Este parámetro no se aplica a las aplicaciones de Android

Enterprise, que solo aparecen en Google Play administrado.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings ☒ ON

Allow app comments ☒ ON

Si quiere, puede agregar una sección de preguntas frecuentes sobre la aplicación o capturas de pantalla que aparecen en el almacén de aplicaciones. También puede definir si los usuarios pueden puntuar o comentar la aplicación.

- Configure estos parámetros:
 - **Preguntas frecuentes sobre aplicaciones:** Agregue una sección de preguntas frecuentes sobre la aplicación (junto con sus respuestas).
 - **Capturas de pantalla de aplicaciones:** Agregue capturas de pantalla para ayudar a clasificar la aplicación en el almacén de aplicaciones. El formato del gráfico que cargue debe ser PNG. No puede cargar imágenes en formato GIF o JPEG.
 - **Permitir puntuación de aplicaciones:** Seleccione si permitir a los usuarios puntuar la aplicación. Está **activado** de forma predeterminada.
 - **Permitir comentarios de aplicaciones:** Seleccione si permitir a los usuarios publicar comentarios referentes a la aplicación seleccionada. Está **activado** de forma predeterminada.

16. Haga clic en **Siguiente**. Aparecerá la página **Aprobaciones**.

Los flujos de trabajo se utilizan cuando se necesita aprobación para crear cuentas de usuario. Si no quiere establecer flujos de trabajo de aprobación, puede ir directamente al paso 15.

Configure estos parámetros para asignar o crear un flujo de trabajo:

- **Flujo de trabajo para usar:** En la lista, haga clic en un flujo de trabajo existente o haga clic en **Crear un flujo de trabajo**. El valor predeterminado es **Ninguno**.
- Si selecciona **Crear un flujo de trabajo** configure los siguientes parámetros: Para obtener más información, consulte [Crear y administrar flujos de trabajo](#).
- **Nombre:** Escriba un nombre único para el flujo de trabajo.
- **Descripción:** Si quiere, escriba una descripción del flujo de trabajo.
- **Plantillas de correo electrónico de aprobación:** En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar al flujo de trabajo. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.
- **Niveles de aprobación administrativa:** En la lista, seleccione la cantidad de niveles de aprobación administrativa necesarios para este flujo de trabajo. El valor predeterminado es 1 nivel. Las opciones posibles son:
 - No se necesita
 - 1 nivel
 - 2 niveles
 - 3 niveles
- **Seleccionar dominio de Active Directory:** En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
- **Buscar aprobadores adicionales requeridos:** Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Buscar**. Los nombres se originan en Active Directory.
- Cuando el nombre aparezca en el campo, marque la casilla situada al lado. El nombre y la dirección de correo electrónico aparecen en la lista **Aprobadores adicionales requeridos**

seleccionados.

- Para quitar a una persona de la lista **Aprobadores adicionales requeridos seleccionados**, 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 requeridos seleccionados** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla situada junto a cada nombre que quiera quitar.

17. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.

The screenshot displays the 'Delivery Group Assignments (optional)' configuration page. On the left, a sidebar shows the 'MDX' section with steps 1 through 4. Step 4, 'Delivery Group Assignments (optional)', is currently selected and highlighted in light blue. The main content area is titled 'Delivery Group Assignments (optional)' and includes a sub-header 'Assign this app to one or more delivery groups.' Below this, there is a 'Choose delivery groups' section with a search input field and a 'Search' button. A list of delivery groups is shown below the search field: 'AllUsers' (checked with a green checkbox) and 'OA DG for Mac users' (unchecked). To the right of this list, there is a box titled 'Delivery groups to receive app assignment' which currently contains 'AllUsers'. At the bottom of the main area, there is a 'Deployment Schedule' link with a help icon.

18. Junto a **Elegir grupos de entrega**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione un grupo o varios de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.

19. Expanda **Programación de implementación** y, a continuación, configure estos parámetros:

- Junto a **Implementar**, haga clic en **Sí** para programar la implementación, o bien, haga clic en **No** para cancelarla. Está **activado** de forma predeterminada.
- 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 de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Condición de implementación**, puede hacer clic en **En cada conexión** o en **Solo cuando haya fallado la implementación anterior**. La opción predeterminada es **En cada conexión**.

- Junto a **Implementar para conexiones permanentes**, asegúrese de que está seleccionado **No**. Está **desactivado** de forma predeterminada. Las conexiones permanentes no están disponibles para Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management a partir de la versión 10.18.19 o una posterior. No recomendamos las conexiones en el caso de clientes que comenzaron a utilizar Citrix Endpoint Management antes de la versión 10.18.19.

Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Parámetros > Propiedades de servidor**.

La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Implementar para conexiones permanentes**.

20. Haga clic en **Guardar**.

Repita los pasos para cada aplicación móvil de productividad.

Configurar la directiva de desafío de seguridad

La directiva de dispositivos de código de acceso de Citrix Endpoint Management configura las reglas de reto de seguridad. Los retos 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 acerca de la directiva Código de acceso, consulte [Directiva de código de acceso](#).

- Si la implementación de Android Enterprise incluye dispositivos BYOD, configure la directiva de código de acceso para el perfil de trabajo.
- Si la implementación incluye dispositivos totalmente administrados y propiedad de la empresa, configure la directiva de código de acceso para el propio dispositivo.
- Si la 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 ver el panel **Plataformas** de la directiva. En el panel **Plataformas** de la directiva, seleccione **Android Enterprise**.
4. Haga clic en **Código de acceso** en el panel derecho.

Device PoliciesAppsMediaActionsShareFileEnrollment Profiles

Policy PlatformClear All

☐ iOS10

☐ Windows Desktop/Tablet11

☐ Android11

☐ macOS8

☐ Windows Mobile/CE8

☐ Windows Phone9

☒ Android Enterprise17

Add a New PolicyHide filter

Policies most often used

Exchange

Location

Passcode

Restrictions

Scheduling

1. Introduzca un **nombre de directiva**. Haga clic en **Siguiente**.

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery

Passcode Policy

1 Policy Info

2 PlatformsClear All

☐ iOS

☐ macOS

☐ Android

☐ Samsung KNOX

☒ Android Enterprise

Policy Information

This policy creates a passcode policy based on the standards of your organization, such as the grace period before device lock.

Policy Name *

Passcode - AE

Description

2. Establezca la configuración para la directiva de código de acceso.
- **Active** la opción **Código de acceso de dispositivo obligatorio** para ver los parámetros disponibles de los desafíos de seguridad en el propio dispositivo.
 - Establezca **Desafío de seguridad de perfil de trabajo** en **Sí** para ver los parámetros

disponibles de los desafíos de seguridad de 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 la forma en que se inscriben los dispositivos Android si Android Enterprise está habilitado para la implementación de Citrix Endpoint Management. Cuando crea un perfil de inscripción para dispositivos Android Enterprise, puede configurarlo para inscribir los dispositivos nuevos y restablecidos a los valores de fábrica como:

- Dispositivos totalmente administrados
- Dispositivos dedicados
- Dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa

También puede configurar cada uno de estos perfiles de inscripción de Android Enterprise para inscribir dispositivos Android BYOD como dispositivos de perfil de trabajo.

Si Android Enterprise está habilitado para la implementación de Citrix Endpoint Management, todos los dispositivos Android recién inscritos (o que se han inscrito de nuevo) se inscriben como dispositivos Android Enterprise. De forma predeterminada, el perfil de inscripción global registra los dispositivos Android nuevos y de restablecimiento de fábrica como dispositivos totalmente administrados e inscribe los dispositivos BYOD Android como dispositivos propiedad de la empresa de perfil de trabajo.

Cuando crea los perfiles de inscripción, les asigna grupos de entrega. Si un usuario pertenece a varios grupos de entrega que tienen perfiles de inscripción diferentes, 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

De forma predeterminada, los dispositivos totalmente administrados se inscriben utilizando el perfil de inscripción global, pero se pueden crear otros perfiles 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 la cantidad de dispositivos que los miembros con este perfil pueden inscribir.
4. Seleccione **Android** en **Plataformas** o haga clic en **Siguiente**. Aparecerá la página Configuración de inscripción.
5. Establezca **Administración** en **Android Enterprise**.
6. Establezca **Modo propietario del dispositivo** en **Dispositivo propiedad de la empresa**.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	<p>Workspace integration ⓘ</p> <p>Enrollment through Workspace app <input type="checkbox"/> ⓘ</p> <p>Device management ⓘ</p> <p>Management <input checked="" type="radio"/> Android Enterprise ⓘ <input type="radio"/> Legacy device administration (not recommended) ⓘ <input type="radio"/> Do not manage devices ⓘ</p> <p>Device owner mode <input checked="" type="radio"/> Company-owned device ⓘ <input type="radio"/> Fully managed with work profile / Work profile on corporate-owned devices ⓘ <input type="radio"/> Dedicated device ⓘ <input type="radio"/> None ⓘ</p> <p>BYOD work profile <input checked="" type="checkbox"/> ⓘ</p> <p>Application management ⓘ</p> <p>Citrix MAM <input checked="" type="checkbox"/> ⓘ</p> <p>User consent</p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ⓘ</p>
Android	
iOS	
Windows	
3 Assignment (optional)	

7. El **perfil de trabajo BYOD** le permite configurar el perfil de inscripción para inscribir dispositivos BYOD como dispositivos de perfil de trabajo. Los dispositivos nuevos y restablecidos a los valores de fábrica se inscriben como dispositivos totalmente administrados. Establezca el **perfil de trabajo BYOD** en **Sí** para permitir la inscripción de dispositivos BYOD como dispositivos de perfil de trabajo. Establezca el **perfil de trabajo BYOD** en **No** para restringir la inscripción a los dispositivos totalmente administrados. De forma predeterminada, está **activado**.
8. Elija si quiere inscribir dispositivos en Citrix MAM.
9. Si establece el **perfil de trabajo BYOD** en **Sí**, configure el consentimiento del usuario. Si quiere que los usuarios de dispositivos de perfil de trabajo BYOD puedan rechazar la administración de dispositivos al inscribirlos, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Sí**.

Si el **perfil de trabajo BYOD** está **activado**, el valor predeterminado de **Permitir a los usuarios rechazar la administración de dispositivos** es **Sí**. Si el **perfil de trabajo BYOD** está estable-

cido en **No**, la opción **Permitir a los usuarios rechazar la administración de dispositivos** está desactivada.

10. Seleccione **Asignación (opciones)**. Aparecerá la pantalla Asignación de grupos de entrega.
11. Elija un grupo o varios grupos de entrega que contengan los administradores que inscriben los dispositivos totalmente administrados. A continuación, haga clic en **Guardar**.

La página “Perfil de inscripción” aparece con el perfil que agregó.

Agregar un perfil de inscripción de dispositivos dedicado

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 garantizar que estos administradores puedan inscribir todos los dispositivos necesarios, cree un perfil de inscripción para ellos con dispositivos ilimitados 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 **Sin límite** la cantidad de dispositivos que los miembros con este perfil pueden inscribir.
3. Seleccione **Android** en **Plataformas** o haga clic en **Siguiente**. Aparecerá la página Configuración de inscripción.
4. Establezca **Administración** en **Android Enterprise**.
5. Establezca **Modo propietario del dispositivo** en **Dispositivo dedicado**.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Workspace integration ⓘ Enrollment through Workspace app <input type="checkbox"/> ⓘ
Android	Device management ⓘ Management <input checked="" type="radio"/> Android Enterprise ⓘ <input type="radio"/> Legacy device administration (not recommended) ⓘ <input type="radio"/> Do not manage devices ⓘ Device owner mode <input type="radio"/> Company-owned device ⓘ <input type="radio"/> Fully managed with work profile / Work profile on corporate-owned devices ⓘ <input checked="" type="radio"/> Dedicated device ⓘ <input type="radio"/> None ⓘ BYOD work profile <input checked="" type="checkbox"/> ⓘ
iOS	Application management ⓘ Citrix MAM <input checked="" type="checkbox"/> ⓘ
Windows	User consent Allow users to decline device management <input checked="" type="checkbox"/> ⓘ
3 Assignment (optional)	

6. El **perfil de trabajo BYOD** le permite configurar el perfil de inscripción para inscribir dispositivos BYOD como dispositivos de perfil de trabajo. Los dispositivos nuevos y restablecidos a los valores de fábrica se inscriben como dispositivos dedicados. Establezca el **perfil de trabajo BYOD** en **Sí** para permitir la inscripción de dispositivos BYOD como dispositivos de perfil de trabajo. Establezca el **perfil de trabajo BYOD** en **No** para restringir la inscripción a los dispositivos propiedad de la empresa. De forma predeterminada, está **activado**.

7. Elija si quiere inscribir dispositivos en Citrix MAM.

8. Si establece el **perfil de trabajo BYOD** en **Sí**, configure el consentimiento del usuario. Si quiere que los usuarios de dispositivos de perfil de trabajo BYOD puedan rechazar la administración de dispositivos al inscribirlos, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Sí**.

Si el **perfil de trabajo BYOD** está **activado**, el valor predeterminado de **Permitir a los usuarios rechazar la administración de dispositivos** es **Sí**. Si el **perfil de trabajo BYOD** está establecido en **No**, la opción **Permitir a los usuarios rechazar la administración de dispositivos** está desactivada.

9. Seleccione **Asignación (opciones)**. Aparecerá la pantalla Asignación de grupos de entrega.

10. Elija un grupo o varios grupos de entrega que contengan los administradores que inscriben los dispositivos dedicados. A continuación, haga clic en **Guardar**.

La página “Perfil de inscripción” aparece con el perfil que agregó.

Agregar un perfil de inscripción para dispositivos totalmente administrados con un perfil de trabajo o un 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 la cantidad de dispositivos que los miembros con este perfil pueden inscribir.
4. Seleccione **Android** en **Plataformas** o haga clic en **Siguiente**. Aparecerá la página Configuración de inscripción.
5. Establezca **Administración** en **Android Enterprise**. Establezca **Modo propietario del dispositivo** en **Totalmente administrado con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa**.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	<p>Workspace integration ⓘ</p> <p>Enrollment through Workspace app <input type="checkbox"/> ⓘ</p> <p>Device management ⓘ</p> <p>Management <input checked="" type="radio"/> Android Enterprise ⓘ <input type="radio"/> Legacy device administration (not recommended) ⓘ <input type="radio"/> Do not manage devices ⓘ</p> <p>Device owner mode <input type="radio"/> Company-owned device ⓘ <input checked="" type="radio"/> Fully managed with work profile / Work profile on corporate-owned devices ⓘ <input type="radio"/> Dedicated device ⓘ <input type="radio"/> None ⓘ</p> <p>BYOD work profile <input checked="" type="checkbox"/> ⓘ</p> <p>Application management ⓘ</p> <p>Citrix MAM <input checked="" type="checkbox"/> ⓘ</p> <p>User consent</p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ⓘ</p>
Android	
iOS	
Windows	
3 Assignment (optional)	

6. El **perfil de trabajo BYOD** le permite configurar el perfil de inscripción para inscribir dispositivos BYOD como dispositivos de perfil de trabajo. Los dispositivos nuevos y restablecidos a los valores de fábrica se inscriben como dispositivos totalmente administrados con un perfil de trabajo. Establezca el **perfil de trabajo BYOD** en **Sí** para permitir la inscripción de dispositivos BYOD como dispositivos de perfil de trabajo. Establezca el **perfil de trabajo BYOD** en **No** para restringir la inscripción a los dispositivos dedicados. El valor predeterminado es **Desactivado**.
7. Elija si quiere inscribir dispositivos en Citrix MAM.
8. Si establece el **perfil de trabajo BYOD** en **Sí**, configure el consentimiento del usuario. Si quiere

que los usuarios de dispositivos de perfil de trabajo BYOD puedan rechazar la administración de dispositivos al inscribirlos, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Sí**.

Si el **perfil de trabajo BYOD** está **activado**, el valor predeterminado de **Permitir a los usuarios rechazar la administración de dispositivos** es **Sí**. Si el **perfil de trabajo BYOD** está establecido en **No**, la opción **Permitir a los usuarios rechazar la administración de dispositivos** está desactivada.

9. Seleccione **Asignación (opciones)**. Aparecerá la pantalla Asignación de grupos de entrega.
10. Elija un grupo o varios grupos de entrega que contengan los administradores que inscriben los dispositivos totalmente administrados con un perfil de trabajo. A continuación, haga clic en **Guardar**.

La página “Perfil de inscripción” aparece con el perfil que agregó.

Agregar un perfil de inscripción para dispositivos antiguos

Google ha retirado el modo de administrador de dispositivos de la administración de dispositivos. Google anima a los clientes a administrar todos los dispositivos Android en el modo propietario del dispositivo o en el modo propietario del perfil (consulte [Retirada del administrador de dispositivos](#) en las guías para desarrolladores de Google Android Enterprise).

Para habilitar este cambio:

- Citrix ha establecido Android Enterprise como opción de inscripción predeterminada para dispositivos Android.
- Si Android Enterprise está habilitado para la implementación de Citrix Endpoint Management, todos los dispositivos Android recién inscritos (o que se han inscrito de nuevo) se inscriben como dispositivos Android Enterprise.

Es posible que su organización no esté preparada para comenzar a administrar dispositivos Android antiguos mediante Android Enterprise. En ese caso, puede seguir administrándolos en el modo de administrador de dispositivos. En el caso de los dispositivos ya inscritos en el modo de administrador de dispositivos, Citrix Endpoint Management continúa administrándolos en el modo de administrador de dispositivos.

Cree un perfil de inscripción para dispositivos antiguos para permitir que las nuevas inscripciones de dispositivos Android utilicen el modo de administrador de dispositivos.

Para crear un perfil de inscripción para los dispositivos antiguos:

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 la cantidad de dispositivos que los miembros con este perfil pueden inscribir.
4. Seleccione **Android** en **Plataformas** o haga clic en **Siguiente**. Aparecerá la página Configuración de inscripción.
5. Establezca **Administración** en **Administración de dispositivos antigua (no se recomienda)**. Haga clic en **Siguiente**.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	<p>Workspace integration ?</p> <p>Enrollment through Workspace app <input type="checkbox"/> ?</p> <p>Device management ?</p> <p>Management <input type="radio"/> Android Enterprise ? <input checked="" type="radio"/> Legacy device administration (not recommended) ? <input type="radio"/> Do not manage devices ?</p> <p>Application management ?</p> <p>Citrix MAM <input checked="" type="checkbox"/> ?</p> <p>User consent</p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ?</p>
Android	
iOS	
Windows	
3 Assignment (optional)	

6. Elija si quiere inscribir dispositivos en Citrix MAM.
7. Si quiere que los usuarios puedan rechazar la administración de dispositivos al inscribirlos, establezca **Permitir a los usuarios rechazar la administración de dispositivos** en **Sí**. De forma predeterminada, está **activado**.
8. Seleccione **Asignación (opciones)**. Aparecerá la pantalla Asignación de grupos de entrega.
9. Elija un grupo o varios grupos de entrega que contengan los administradores que inscriben los dispositivos dedicados. A continuación, haga clic en **Guardar**.

La página “Perfil de inscripción” aparece con el perfil que agregó.

Para seguir administrando dispositivos antiguos en el modo de administrador de dispositivos, inscríbalos o vuelva a inscribirlos con este perfil. Para inscribir dispositivos de administrador de dispositivos similares a los dispositivos de perfil de trabajo, los usuarios deben descargar Citrix Secure Hub y proporcionar una URL de servidor de inscripción.

Aprovisionar dispositivos de perfil de trabajo en Android Enterprise

Los dispositivos de perfil de trabajo de Android Enterprise se inscriben en el modo propietario de perfil. Estos dispositivos no necesitan ser nuevos ni haberse restablecido a los valores de fábrica. Los dispositivos BYOD se inscriben como dispositivos de perfil de trabajo. La experiencia de inscripción es similar a la inscripción de Android en Citrix Endpoint Management. Los usuarios descargan Citrix Secure Hub desde Google Play e inscriben sus dispositivos.

De forma predeterminada, los parámetros de **depuración por USB y fuentes desconocidas** están inhabilitados en un dispositivo cuando se inscribe en Android Enterprise como dispositivo de perfil de trabajo.

Cuando inscriba dispositivos en Android Enterprise como dispositivos de perfil de trabajo, vaya siempre a Google Play. Desde allí, habilite Citrix Secure Hub para que aparezca en el perfil personal del usuario.

Aprovisionar dispositivos Android Enterprise totalmente administrados

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 el modo propietario del dispositivo. Solo los dispositivos nuevos o los restablecidos a los valores de fábrica se pueden inscribir en el modo propietario del dispositivo.

Puede inscribir dispositivos en el modo propietario del dispositivo mediante cualquiera de estos métodos de inscripción:

- **Token identificador DPC:** Con este método de inscripción, los usuarios escriben los caracteres `afw#xenmobile` al configurar el dispositivo. `afw#xenmobile` es el token identificador 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 identificador DPC de Citrix.
- **Conexión de transmisión de datos en proximidad (NFC):** El método de inscripción de la conexión NFC transfiere datos entre dos dispositivos por transmisión de datos en proximidad. Bluetooth, Wi-Fi y otros modos de comunicación están inhabilitados en un dispositivo nuevo o que ha sido restablecido a sus valores de fábrica. NFC es el único protocolo de comunicación que el dispositivo puede utilizar en ese estado. Consulte Inscribir dispositivos con una conexión NFC.
- **Código QR:** La inscripción con códigos QR se puede utilizar para inscribir una flota distribuida de dispositivos que no admiten NFC, como las tabletas. El método de inscripción por código QR define y configura el modo de perfil del dispositivo al escanear un código QR desde el asistente de configuración. Consulte Inscribir dispositivos con un código QR.

- **Zero Touch:** La activación automática le permite configurar los dispositivos para que se inscriban automáticamente cuando se enciendan por primera vez. La activación automática se admite en algunos dispositivos Android con Android 9.0 o versiones posteriores. Consulte Activación automática.
- **Cuentas de Google:** Los usuarios introducen sus credenciales de cuenta de Google para iniciar el proceso de aprovisionamiento. Esta opción es para empresas que utilizan Google Workspace.

Inscribir dispositivos mediante el token identificador DPC de Citrix

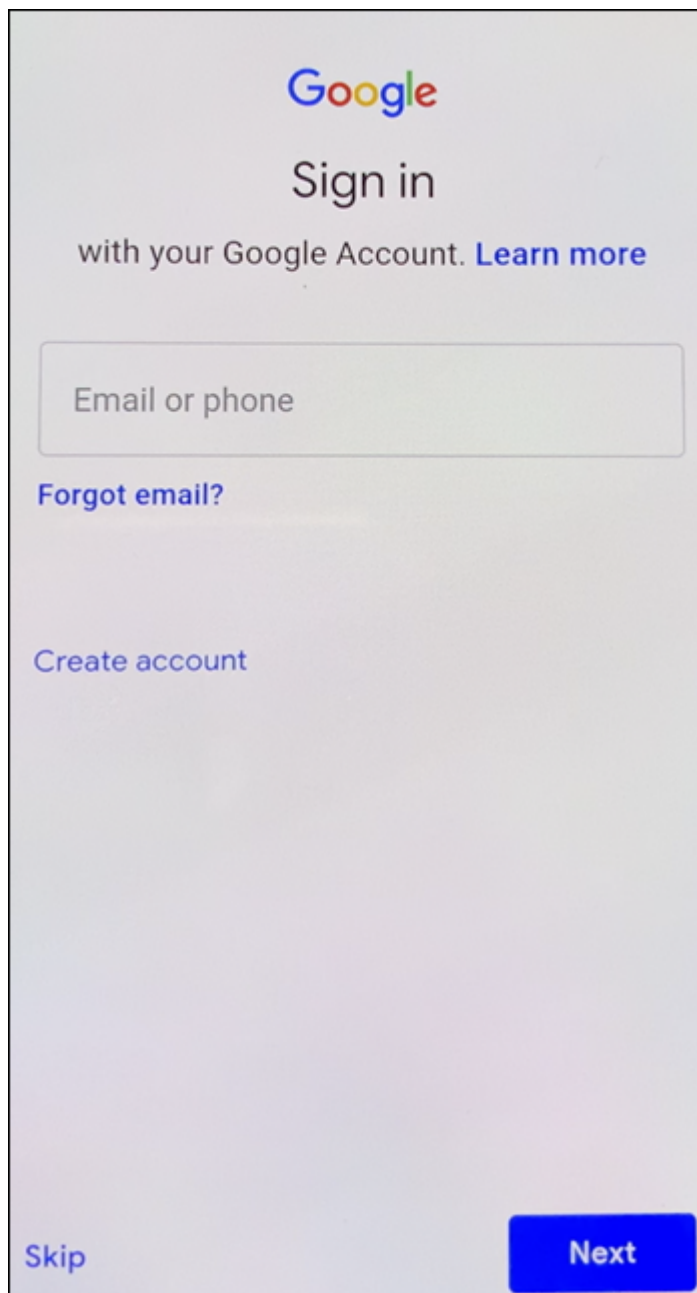
Los usuarios escriben `afw#xenmobile` cuando se les pide que introduzcan una cuenta de Google después de encender dispositivos nuevos o restablecidos a los valores de fábrica para la configuración inicial. Esta acción descarga e instala Citrix Secure Hub. Los usuarios siguen las indicaciones de configuración de Citrix Secure Hub para completar la inscripción.

Requisitos del sistema

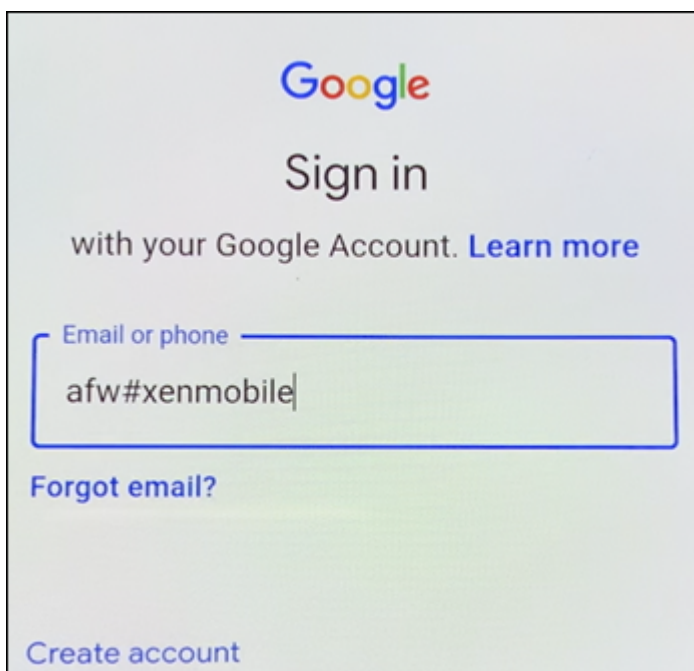
- Compatible con todos los dispositivos Android que ejecutan el sistema operativo Android.

Para inscribir el dispositivo

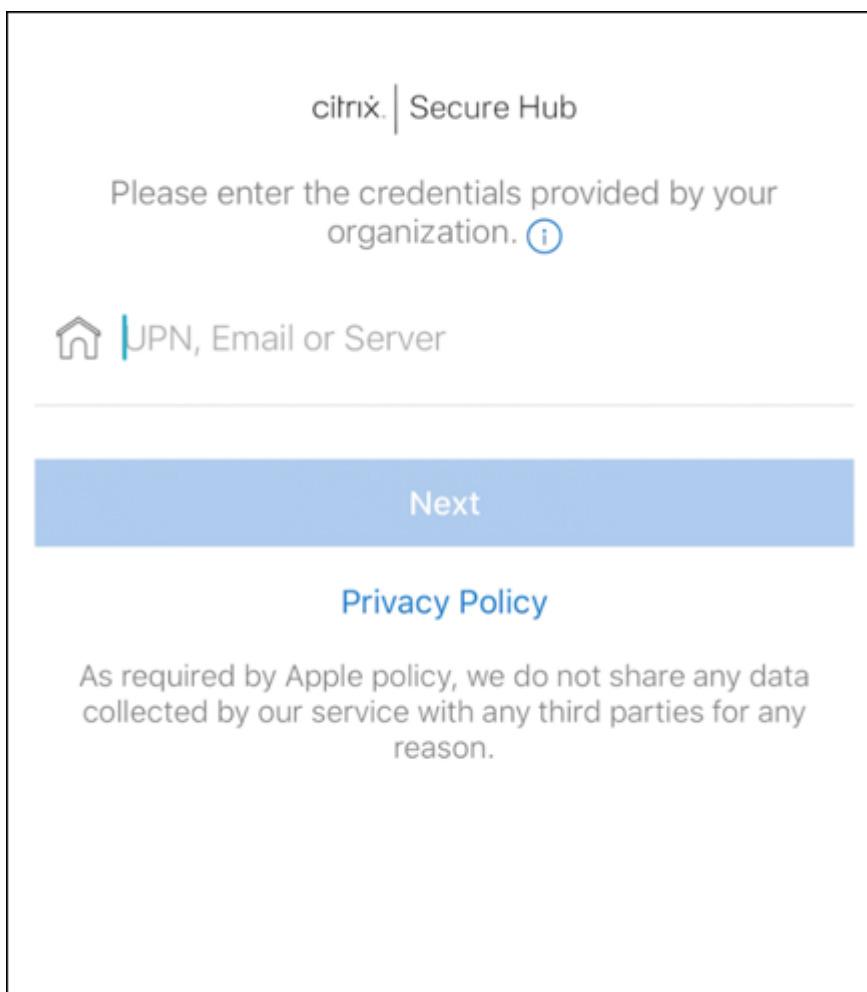
1. Encienda un dispositivo nuevo o restablecido a los valores de fábrica.
2. La configuración inicial del dispositivo se carga y solicita una cuenta de Google. Si el dispositivo carga la pantalla de inicio del dispositivo, compruebe que en la barra de notificaciones hay la notificación **Finalizar configuración**.



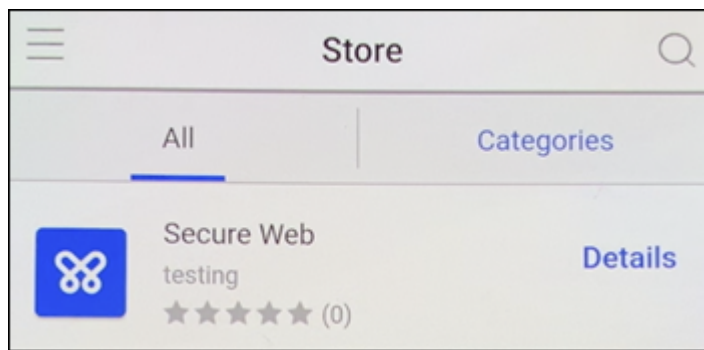
3. Escriba `afw#xenmobile` en el campo **Correo electrónico o Teléfono**.



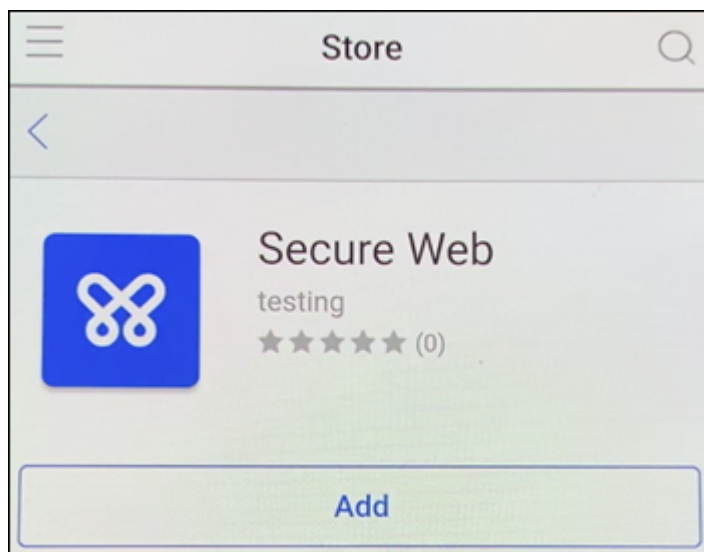
4. Toque **Instalar** en la pantalla de Android Enterprise que solicita la instalación de Citrix Secure Hub.
5. Toque **Instalar** en la pantalla del instalador de Citrix Secure Hub.
6. Toque **Permitir** para todas las solicitudes de permisos de la aplicación.
7. Toque **Aceptar y continuar** para instalar Citrix Secure Hub y permitirle que administre el dispositivo.
8. Citrix Secure Hub ya se ha instalado y se halla en la pantalla de inscripción predeterminada. En este ejemplo, la detección automática no está configurada. Si lo estuviera, el usuario puede introducir su nombre de usuario o su correo electrónico y se le encontraría un servidor. En lugar de seguir este método, introduzca la URL de inscripción del entorno y toque **Siguiente**.

The image shows a login screen for Citrix Secure Hub. At the top, the Citrix logo is followed by 'Secure Hub'. Below this, a message says 'Please enter the credentials provided by your organization.' with an information icon. There is a home icon followed by the text 'UPN, Email or Server'. A large blue button labeled 'Next' is centered below a horizontal line. Underneath the button, there is a link for 'Privacy Policy'. At the bottom, a disclaimer states: 'As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.'

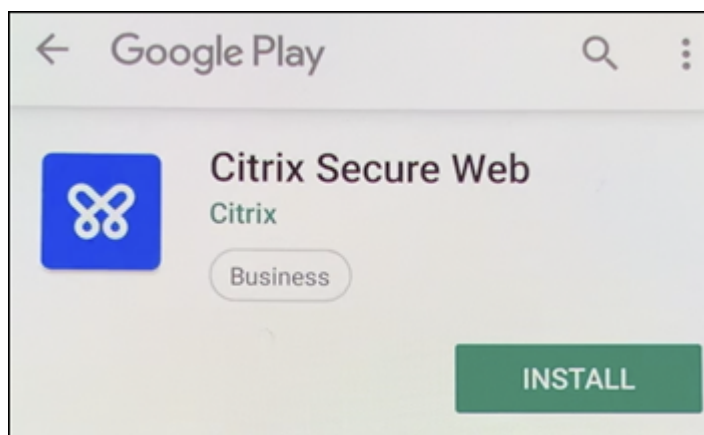
9. La configuración predeterminada de Citrix Endpoint Management permite a los usuarios elegir MAM o MDM+MAM. Si se le pide de esta manera, toque **Sí, inscribirlo** para elegir MDM+MAM.
10. Introduzca la dirección de correo electrónico y la contraseña del usuario y, a continuación, toque **Siguiente**.
11. Se pide al usuario que configure un código de acceso de dispositivo. Toque **Establecer** e introduzca un código de acceso.
12. Se solicita al usuario que configure un método de desbloqueo del perfil de trabajo. En este ejemplo, toque **Contraseña y PIN**, e introduzca un PIN.
13. El dispositivo se encuentra ahora en la pantalla de inicio de Citrix Secure Hub **Mis aplicaciones**. Toque **Agregar aplicaciones desde la tienda**.
14. Para agregar Citrix Secure Web, toque **Citrix Secure Web**.



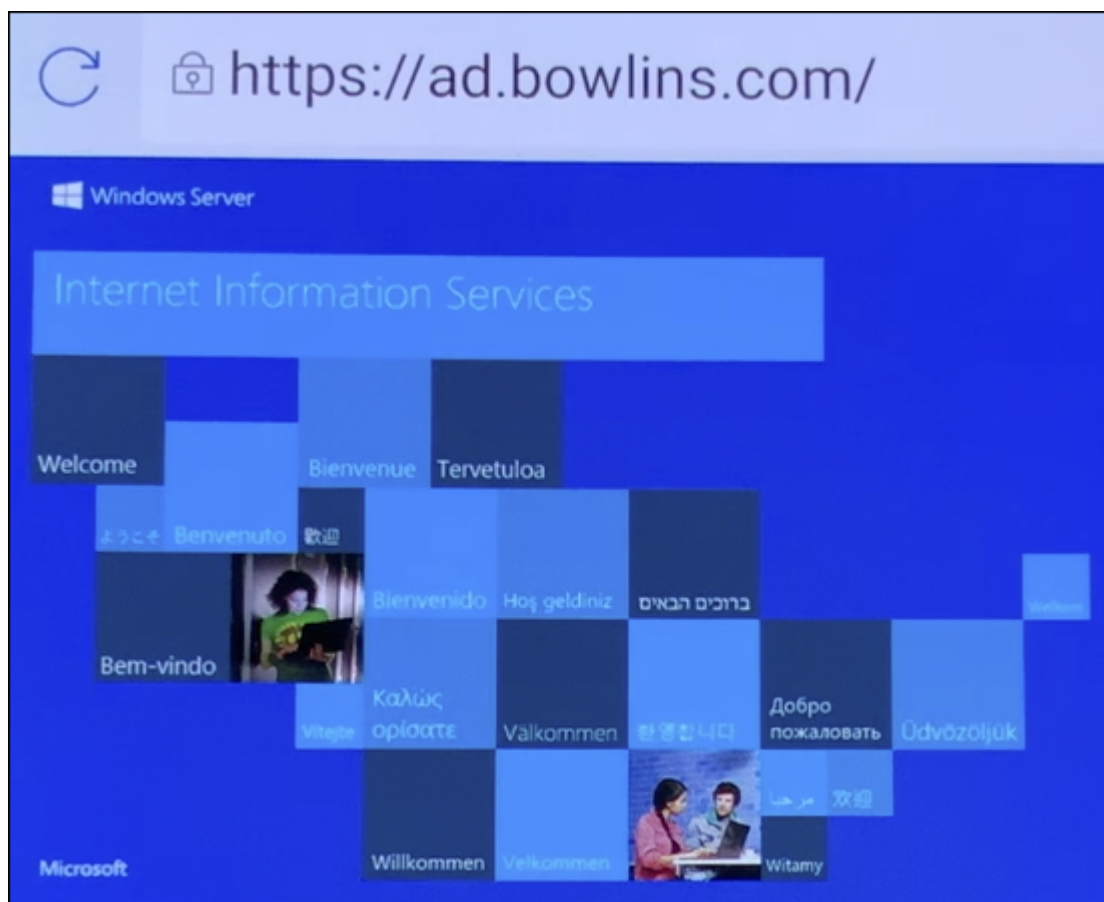
15. Toque **Agregar**.



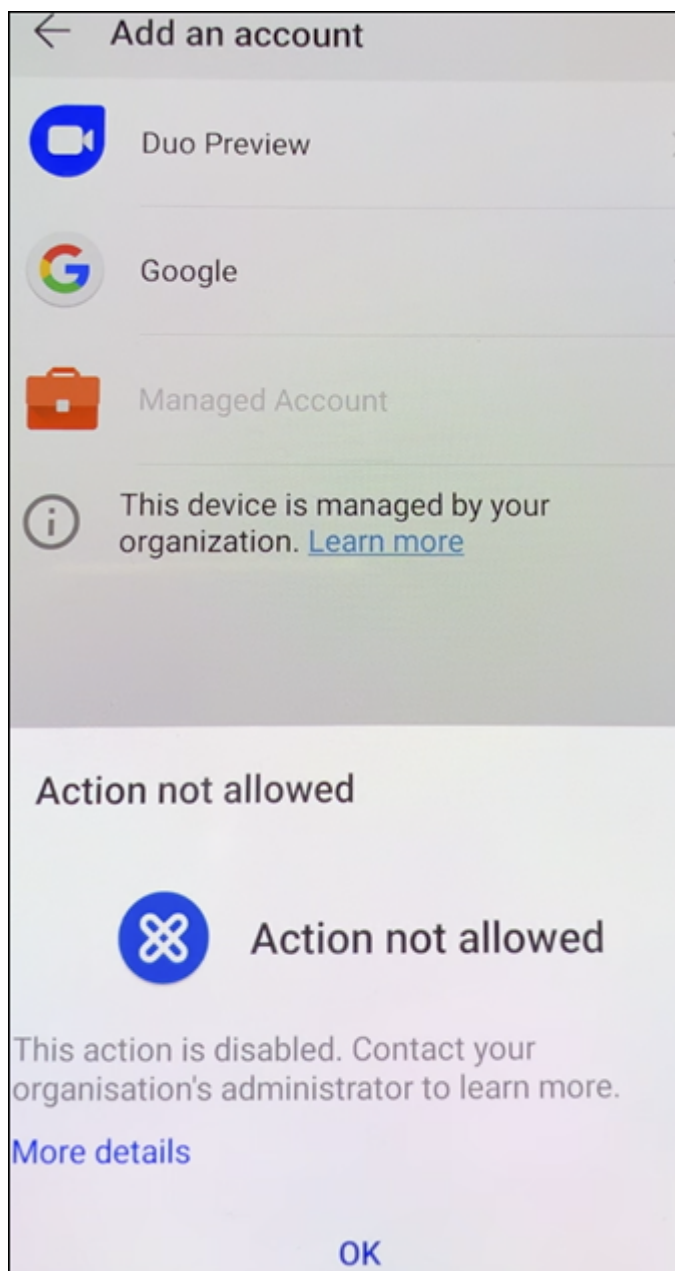
16. Citrix Secure Hub dirige al usuario a Google Play Store para instalar Citrix Secure Web. Toque **Instalar**.



17. Después de que Citrix Secure Web se instale, toque **Abrir**. Introduzca una dirección URL de un sitio interno en la barra de direcciones y compruebe que se carga la página.



18. Vaya a **Parámetros > Cuentas** en el dispositivo. Observe que la **cuenta administrada** no se puede modificar. Las opciones de desarrollador para compartir la pantalla o la depuración remota también están bloqueadas.



Inscribir dispositivos con una conexión NFC

Para inscribir un dispositivo como dispositivo totalmente administrado mediante conexiones NFC, se necesitan dos dispositivos: uno que se haya restablecido a sus valores de fábrica y otro con la herramienta Citrix Endpoint Management Provisioning Tool.

Requisitos del sistema y requisitos previos

- Dispositivos Android compatibles.

- Un dispositivo nuevo o restablecido a los valores de fábrica con la función de NFC, provisionado para Android Enterprise como un dispositivo totalmente administrado. Consulte la sección de [Aprovisionar dispositivos Android Enterprise totalmente administrados](#).
- Otro dispositivo con la función de NFC, que ejecuta la herramienta de aprovisionamiento configurada. La herramienta Provisioning Tool está disponible en Citrix Secure Hub o en la [página de descargas de Citrix](#).

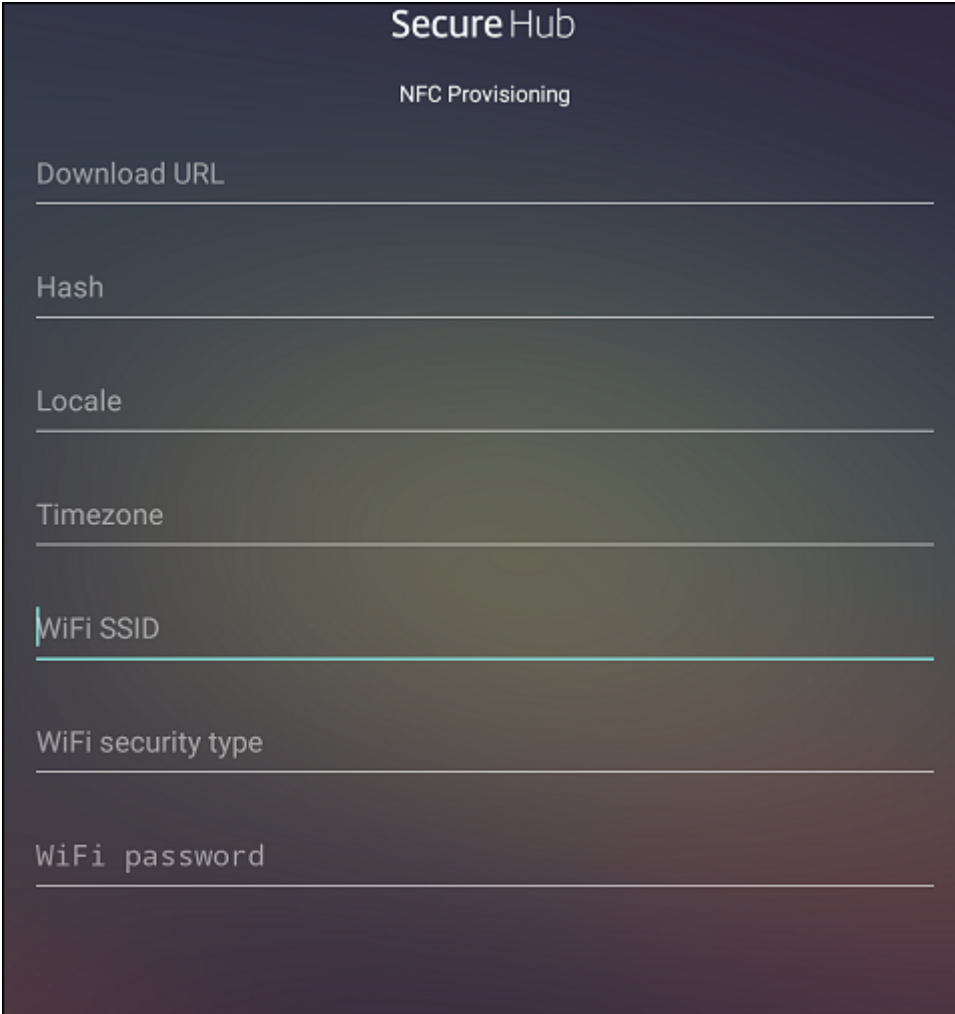
Un dispositivo solo puede tener un perfil Android Enterprise. En este caso, el perfil es para Citrix Secure Hub administrado. Al intentar agregar una segunda aplicación DPC, se quita la instancia instalada de Citrix Secure Hub.

Datos transferidos a través de la conexión NFC Para aprovisionar un dispositivo restablecido a sus valores de fábrica, debe enviar los siguientes datos vía una conexión NFC para inicializar Android Enterprise:

- Nombre del paquete de la aplicación DPC que actuará como propietaria del dispositivo (en este caso, Citrix Secure Hub).
- Ubicación de intranet o Internet desde donde el dispositivo puede descargar la aplicación DPC.
- Valor hash SHA-256 de la aplicación DPC para verificar si la descarga se ha realizado correctamente.
- Datos de la conexión Wi-Fi para que un dispositivo restablecido a sus valores de fábrica pueda conectarse y descargar la aplicación DPC. Nota: Android no admite 802.1x Wi-Fi para este paso.
- Zona horaria del dispositivo (opcional).
- Ubicación geográfica del dispositivo (opcional).

Cuando los dos dispositivos se conectan por NFC, los datos de la herramienta Provisioning Tool se envían al dispositivo restablecido a los valores de fábrica. Esos datos se utilizan para descargar Citrix Secure Hub con los parámetros del administrador. Si no introduce valores para la zona horaria y la ubicación geográfica, Android los configurará automáticamente en el nuevo dispositivo.

Configuración de la herramienta Citrix Endpoint Management Provisioning Tool Antes de una conexión NFC, es necesario configurar la herramienta Provisioning Tool. Esta configuración se transfiere, a continuación, al dispositivo restablecido a los valores de fábrica durante la conexión NFC.



The screenshot shows the 'Secure Hub' interface with the 'NFC Provisioning' section. It contains seven input fields, each with a label and a horizontal line for text entry. The labels are: 'Download URL', 'Hash', 'Locale', 'Timezone', 'WiFi SSID', 'WiFi security type', and 'WiFi password'. The 'WiFi SSID' field has a small blue cursor icon at the start of the line.

Puede introducir los datos en los campos requeridos o rellenar los campos mediante un archivo de texto. En los pasos del siguiente procedimiento, se describe cómo configurar un archivo de texto con descripciones para cada campo. La aplicación no guarda información una vez introducida esta, por lo que puede ser conveniente crear un archivo de texto para conservar esa información para el futuro.

Para configurar Provisioning Tool mediante un archivo de texto Nombre el archivo `nfcprovisioning.txt` y colóquelo en la carpeta `/sdcard/` de la tarjeta SD del dispositivo. La aplicación leerá el archivo de texto y rellenará los valores.

El archivo de texto debe contener estos datos:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION  
=<download_location>
```

Esta línea es la ubicación de intranet o Internet de la aplicación de proveedor EMM. Una vez que el dispositivo restablecido a los valores de fábrica se haya conectado a una red Wi-Fi por conexión NFC, el dispositivo debe tener acceso a esta ubicación para la descarga. La URL es una dirección URL normal,

sin formato especial.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256 hash>
```

Esta línea es la suma de comprobación de la aplicación de proveedor 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 del dispositivo conectado por Wi-Fi donde se está ejecutando la herramienta Provisioning Tool.

```
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 códigos de idioma y país. Los códigos de idioma son códigos de idioma ISO de dos letras minúsculas (por ejemplo, “es” para español), según se definen en [ISO 639-1](#). Los códigos de país son códigos de país de dos letras mayúsculas (por ejemplo, “ES” para España), según se definen en [ISO 3166-1](#). Por ejemplo, introduzca es_ES para el español hablado en España. Si no introduce ningún código, el país y el idioma se rellenan automáticamente.

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

La zona horaria en que se ejecuta el dispositivo. Escriba el [nombre de la base de datos del área o ubicación](#). Por ejemplo, **America/Los_Angeles** para la zona horaria del Pacífico en Estados Unidos. Si no introduce ningún nombre, la zona horaria se rellena automáticamente.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

Este dato no es necesario, porque el valor está codificado en la aplicación como “Citrix Secure Hub”. Se menciona aquí a título meramente informativo.

Si existe una red Wi-Fi protegida con WPA2, un archivo nfcprovisioning.txt completado puede 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=ga50TwdCmfdJ72LGR
\u003d
```

```
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 existe una red Wi-Fi no protegida, un archivo nfcprovisioning.txt completado puede 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=ga50TwdCmfdJ72LGR
\u003d
```

```
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: `qn7oZUtheu3JBainzZRrjCQv6L006Ll10jcxT3-yKM`. Para descargar un archivo APK destinado para 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** del componente Android SDK Build-Tools
- Línea de comandos de OpenSSL

Para obtener la suma de comprobación de una aplicación, siga estos pasos:

1. Descargue el archivo APK de la aplicación desde Google Play.
2. En la línea de comandos de OpenSSL, vaya a la herramienta **apksigner**: `android-sdk/build-tools/<version>/apksigner` y escriba lo siguiente:

```
1 apksigner verify -print-certs <apk_path> | perl -nle 'print $& if
   m{
2   (?<=SHA-256 digest:) .* }
```

```
3 ' | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
4 <!--NeedCopy-->
```

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:

```
1 {
2
3   "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.
4   zenprise/com.zenprise.configuration.AdminFunction",
5   "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "
6   qn7oZUtheu3JBainzZRrjCQv6L006Ll10jcxT3-yKM",
7   "android.app.extra.
8   PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://
9   play.google.com/managed/downloadManagingApp?identifier=xenmobile",
10  "android.app.extra.PROVISIONING_DEVICE_ADMIN_EXTRAS_BUNDLE": {
11    "serverURL": "https://supportability.xm.cloud.com"
12  }
13 }
14 <!--NeedCopy-->
```

Bibliotecas usadas La herramienta Provisioning Tool utiliza las bibliotecas siguientes en su código fuente:

- Biblioteca [appcompat](#) v7, biblioteca Design support y biblioteca Palette v7 de Google bajo la licencia de Apache 2.0

Para obtener información, consulte [Support Library Features Guide](#).

- [Butter Knife](#) de Jake Wharton bajo la licencia de Apache 2.0

Inscribir dispositivos con un código QR

Los usuarios pueden inscribir un dispositivo totalmente administrado mediante el código QR que genera para ellos.

Requisitos del sistema Dispositivos Android con Android 7.0 o una versión posterior.

Crear un código QR Para generar un código QR, especifique la información de inscripción que se necesite. Una vez generado el código QR, guárdelo localmente. Citrix Endpoint Management no lo guarda.

Settings > Android Enterprise QR Code

Android Enterprise QR Code

Input the required information and click the button below to generate QR code for Android Enterprise enrollment.

Server FQDN:

User name:

Password:

Skip encryption: ☐

Enable all system apps: ☐

Skip user consent: ☒

JSON output:

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "qn7oZUtheu3JBainzRrrjCQv6L006L10JcxT3-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
}
```

[Generate QR Code](#)

1. Vaya a **Ajustes > Código QR de Android Enterprise**.

2. Si es necesario, especifique esta información de inscripción:

- **FQDN del servidor:** Escriba el nombre de dominio completo (FQDN) del servidor de Citrix Endpoint Management (por ejemplo, [example.cem.cloud.com](#)). Este campo es opcional. Si la deja vacía, los usuarios deben rellenar esta información cuando se inscriban.
- **Nombre de usuario:** Escriba el nombre de usuario utilizado para inscribirse. Si piensa distribuir el código QR a más de un usuario, 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 deberán rellenar esta información cuando se inscriban.
- **Contraseña:** Escriba la contraseña asociada al nombre de usuario escrito. Si deja el campo vacío, los usuarios deberán rellenar esta información cuando se inscriban.
- **Omitir cifrado:** Si está **activada**, el dispositivo no se cifra durante la inscripción. El valor predeterminado es **Desactivado**.
- **Habilitar todas las aplicaciones del sistema:** Si está **activada**, permite acceder a todas las aplicaciones del sistema que hay en el dispositivo. El valor predeterminado es **Desac-**

tivado.

- **Omitir el consentimiento del usuario:** Si está **desactivada**, los usuarios pueden optar por no participar en la administración de dispositivos. El valor predeterminado es **Desactivado**.

El cuadro **Salida de JSON** muestra el contenido JSON que corresponde a la información especificada.

3. Para agregar más información sobre la inscripción, modifique el contenido JSON en el cuadro **Salida de JSON**.
4. Haga clic en **Generar código QR**. El código QR aparece a la derecha de la salida de JSON.
5. Haga clic con el botón secundario en la imagen del código QR y guárdela.
6. Envíe la imagen a los usuarios para la inscripción de dispositivos.

Un dispositivo con valores de fábrica restablecido escanea este código QR para inscribirse como un dispositivo totalmente administrado.

Para inscribir el dispositivo Después de encender un dispositivo nuevo o restablecido a los valores de fábrica:

1. Toque seis veces en la pantalla de bienvenida para iniciar la inscripción por código QR.
2. Cuando se le solicite, conéctese a la Wi-Fi. Se puede acceder a la ubicación de descarga que tenga establecido Citrix Secure Hub en el código QR a través de esta red Wi-Fi.

Una vez que el dispositivo se haya conectado a la red Wi-Fi, descarga un lector de códigos QR desde Google e inicia la cámara.

3. Apunte la cámara al código QR para escanear el código.

Android descarga Citrix Secure Hub de la ubicación de descarga del código QR, valida la firma del certificado de firma, instala Citrix Secure Hub y establece el modo 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.

Activación automática

La activación automática le permite configurar dispositivos para que se aprovisionen como dispositivos totalmente administrados cuando al encenderse por primera vez.

Su distribuidor de dispositivos creará una cuenta para usted en el portal de activación automática de Android, una herramienta en línea que le permite aplicar configuraciones a los dispositivos. Con

portal de activación automática de Android, cree una o más configuraciones de activación automática y aplique las configuraciones a los dispositivos asignados a su cuenta. Cuando los usuarios encienden estos dispositivos, los dispositivos se inscriben automáticamente en Citrix Endpoint Management. La configuración asignada al dispositivo define su proceso de inscripción automática.

Requisitos del sistema

- La activación automática se ofrece a partir de la versión Android 9.0.

Información de su distribuidor sobre dispositivos y cuentas

- Los dispositivos aptos para la activación automática se compran a un distribuidor empresarial o a un socio de Google. Para obtener una lista de los socios de activación automática de Android Enterprise, consulte el [sitio web de Android](#).
- Una cuenta de portal de activación automática de Android Enterprise, creada por su distribuidor.
- Datos de inicio de sesión de la cuenta de portal de activación automática de Android Enterprise, proporcionados por su distribuidor.

Crear una configuración de activación automática Cuando cree una configuración de activación automática, 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. Sustituya la URL de su servidor por “URL” en este ejemplo.

```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6              "serverURL": "URL"
7          }
8      }
9
10
11 <!--NeedCopy-->
```

Puede utilizar un JSON opcional con más parámetros para personalizar su configuración en mayor profundidad. En este ejemplo, se especifica el servidor de Citrix Endpoint Management y el nombre de usuario y la contraseña que utilizan los dispositivos que utilizan esta configuración para iniciar sesión en el servidor.

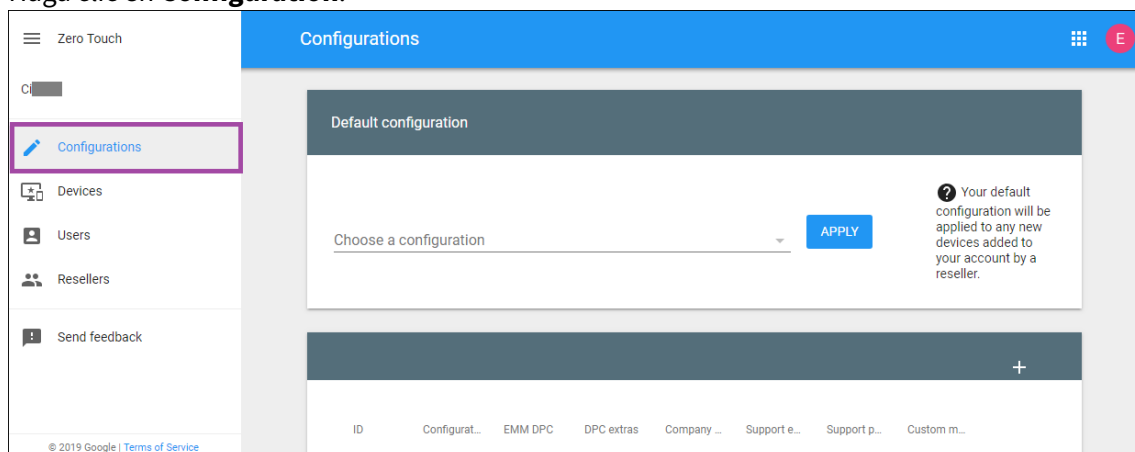
```
1      {
2
```

```
3      "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4      {
5
6          "serverURL": "URL",
7          "xm_username": "username",
8          "xm_password": "password"
9      }
10
11    }
12
13    <!--NeedCopy-->
```

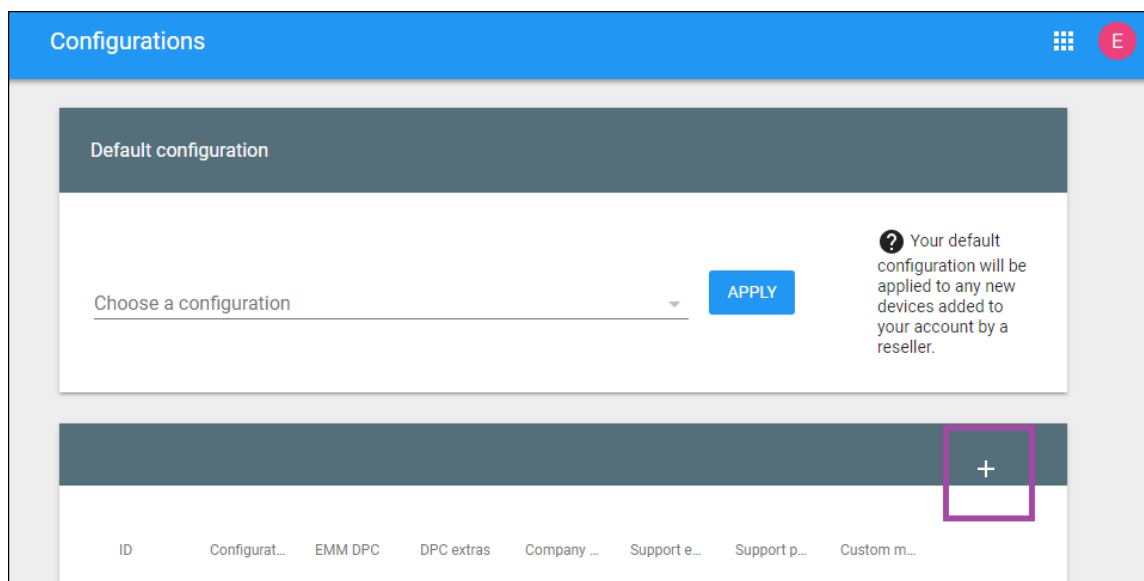
Importante:

Para inscribir dispositivos en el perfil de trabajo en el modo de dispositivos propiedad de la empresa, agregue { "desiredProvisioningMode": "managedProfile" } al JSON personalizado en PROVISIONING_ADMIN_EXTRAS_BUNDLE.

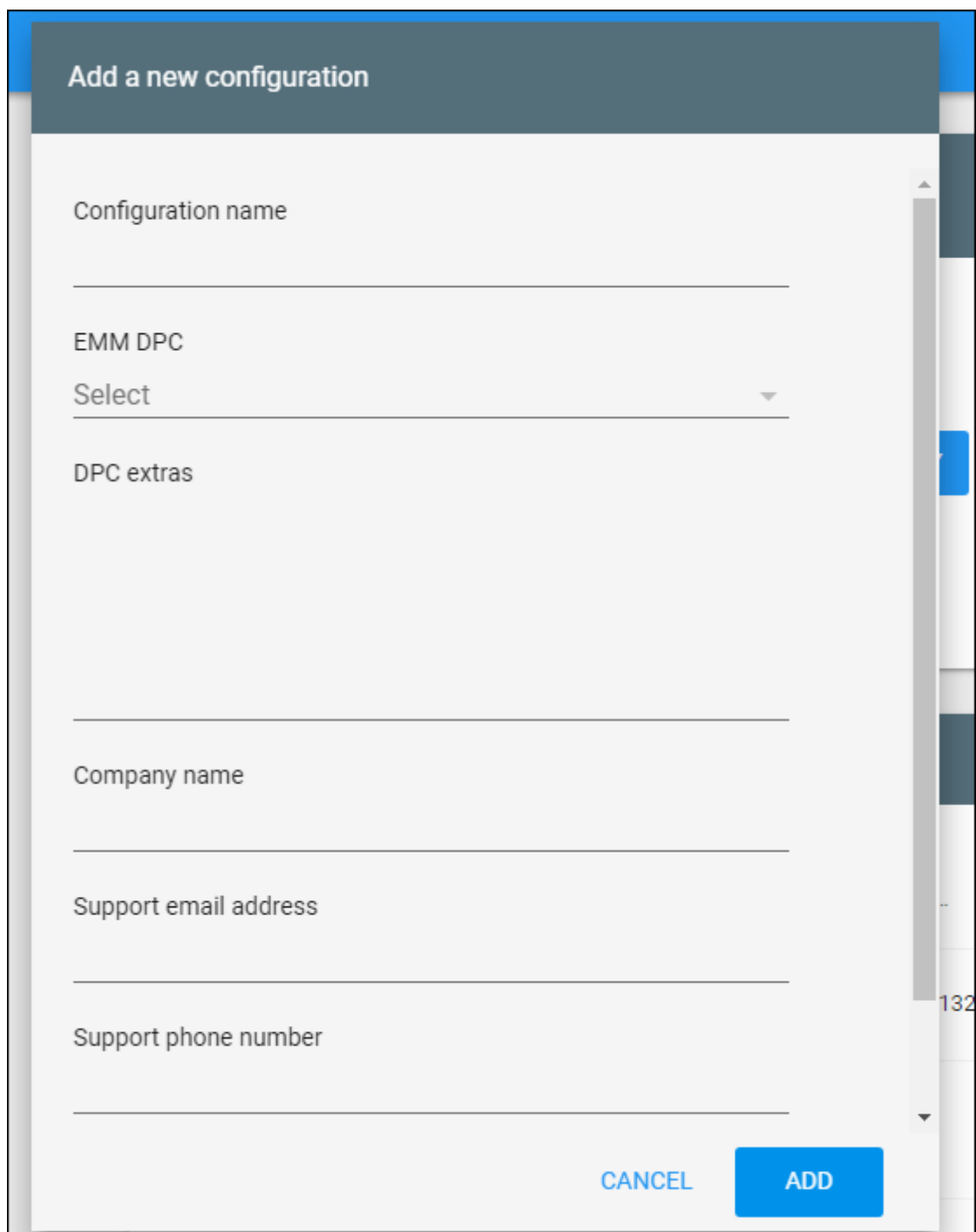
1. Vaya al portal de activación automática de Android en <https://partner.android.com/zerotouch>. Inicie sesión con la información de la cuenta de su distribuidor de dispositivos de activación automática.
2. Haga clic en **Configuration**.



3. Haga clic en + sobre la tabla de configuración.



4. Introduzca la información de configuración en la ventana de configuración que aparece.



Add a new configuration

Configuration name

EMM DPC

Select

DPC extras

Company name

Support email address

Support phone number

CANCEL ADD

- **Nombre de configuración:** Escriba el nombre que quiera para esta configuración.
- **Controlador de políticas de dispositivo de EMM:** Elija **Citrix Secure Hub**.
- **Información adicional de DPC:** Pegue el texto JSON personalizado en este campo.
- **Nombre de empresa:** Escriba el nombre que quiera que aparezca en sus dispositivos Android Enterprise de activación automática durante el aprovisionamiento del dispositivo.
- **Dirección de correo de electrónico de asistencia:** Escriba una dirección de correo elec-

trónico con la que los usuarios puedan ponerse en contacto para obtener ayuda. Esta dirección aparece en los dispositivos Android Enterprise de activación automática antes del aprovisionamiento de dispositivos.

- **Teléfono de asistencia:** Escriba un número de teléfono con el que los usuarios puedan ponerse en contacto para obtener ayuda. Este número de teléfono aparece en los dispositivos Android Enterprise de activación automática antes del aprovisionamiento de dispositivos.
- **Mensaje personalizado:** Si quiere, agregue una o dos frases para ayudar a los usuarios a ponerse en contacto con usted o para darles más detalles sobre lo que ocurre con su dispositivo. Este mensaje personalizado aparece en los dispositivos Android Enterprise de activación automática antes del aprovisionamiento de dispositivos.

5. Haga clic en **Agregar**.

6. Para crear más configuraciones, repita los pasos 2, 3 y 4.

7. Para aplicar una configuración a un dispositivo:

- a) En el portal de activación automática de Android, haga clic en **Dispositivos**.
- b) Busque el dispositivo en la lista de dispositivos y elija la configuración que quiera asignar.

IMEI or serial number	Configuration	Deregister
868160030116860	No config	DEREGISTER

- c) Haga clic en **Update**.

Puede aplicar una configuración a muchos dispositivos mediante un archivo CSV.

Para obtener información sobre cómo aplicar una configuración a muchos dispositivos, consulte [Ac-](#)

[tivación automática para administradores de TI](#). Esta sección de Android Enterprise tiene más información sobre cómo administrar configuraciones y aplicarlas a los dispositivos.

Aprovisionar dispositivos Android Enterprise dedicados

Los dispositivos Android Enterprise dedicados son dispositivos totalmente administrados que se destinan a cumplir un solo caso de uso. Así, restringe estos dispositivos a una aplicación o a un pequeño conjunto de aplicaciones que permitan realizar las tareas necesarias para este caso de uso. También 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 [Aprovisionar dispositivos Android Enterprise totalmente administrados](#). Aprovisionar dispositivos dedicados requiere una configuración adicional antes de inscribirlos.

Para aprovisionar dispositivos dedicados:

- Agregue un perfil de inscripción para los administradores de Citrix Endpoint Management a los que permite inscribir dispositivos dedicados en su implementación de Citrix Endpoint Management. Consulte [Crear perfiles de inscripción](#).
- Para habilitar un dispositivo dedicado de modo que pueda acceder a las aplicaciones, agréguelas a la lista de aplicaciones permitidas.
- Si quiere, configure la aplicación permitida para permitir el modo de bloqueo de tarea. Cuando una aplicación se encuentra en el modo de bloqueo de tarea, esa aplicación queda anclada a la pantalla del dispositivo cuando el usuario la abre. No aparece el botón Inicio y el botón Atrás está desactivado. 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 ha agregado.

Requisitos del sistema

- La inscripción de dispositivos Android dedicados comienza a ofrecerse a partir de Android 6.0.

Permitir aplicaciones y establecer el modo de bloqueo de tarea

Con la directiva Quiosco, puede permitir aplicaciones y establecer el modo de bloqueo de tarea. De forma predeterminada, los servicios Citrix Secure Hub y Google Play están en la lista de permitidos.

Para agregar la directiva de quiosco

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

- Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar nueva directiva**.
- Expanda **Más** y, a continuación, en “Seguridad”, haga clic en **Quiosco**. Aparecerá la página de asignación **Directiva de quiosco**.
- En Plataformas, seleccione **Android Enterprise**. Desmarque las demás plataformas.
- En el panel “Información de directiva”, escriba el **nombre de la directiva** y una **descripción** opcional.
- Haga clic en **Siguiente** y, a continuación, en **Agregar**.
- Para permitir una aplicación y permitir o denegar el modo de bloqueo de tarea para esa aplicación:

En la lista, seleccione la aplicación que quiere permitir.

Seleccione **Permitir** para que la aplicación quede anclada en la pantalla del dispositivo cuando el usuario la abra. Elija **Denegar** para que la aplicación no quede anclada. El valor predeterminado es **Permitir**.

The screenshot displays the 'Kiosk Policy' configuration interface. On the left, a sidebar contains three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Samsung SAFE' is unchecked and 'Android Enterprise' is checked. The main content area is titled 'Kiosk Policy' and includes a description: 'This policy lets you whitelist apps onto a Kiosk for Corporate Owned Single Use devices. If an app supports lock task mode and when lock task status of that app is set to allow, it will get pinned to the screen on the device.' Below this, there is a table for 'Allowed apps' with two columns: 'Apps to whitelist *' and 'Lock task status'. The 'Apps to whitelist *' column has a dropdown menu with 'Cosu App' selected. The 'Lock task status' column has two radio buttons: 'Allow' (selected) and 'Deny'. To the right of these radio buttons are 'Save' and 'Cancel' buttons. At the bottom of the main area, there is a section for 'Deployment Rules' with a right-pointing arrow. In the bottom right corner of the interface, there are 'Back' and 'Next >' buttons.

- Haga clic en **Guardar**.
- Para permitir otra aplicación y permitir o denegar el modo de bloqueo de tarea para esa aplicación, haga clic en **Agregar**.
- Configure las reglas de implementación y elija los grupos de entrega. Para obtener más información, consulte [Directivas de dispositivo](#).

Aprovisionar 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, los dispositivos se inscriben como “perfil de trabajo en dispositivos propiedad de la empresa”. Todos estos dispositivos son dispositivos propiedad de la empresa que se utilizan tanto para el trabajo como para fines 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:

- El propietario del dispositivo es “Empresa”.
- El tipo de instalación del dispositivo en Android Enterprise es “COPE (propiedad de la empresa con acceso privado)”.

Requisitos del sistema

- La inscripción de dispositivos totalmente administrados con perfiles de trabajo se admite a partir de la versión Android 9.0.

Para inscribir el dispositivo

Los dispositivos nuevos y restablecidos a los valores de fábrica se inscriben como dispositivos totalmente administrados con un perfil de trabajo. Estos dispositivos emplean uno de los métodos de inscripción utilizados para otros dispositivos totalmente administrados, como se describe en Aprovisionar 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 con el código QR o los métodos de activación automática descritos en esa sección.

Importante:

Al inscribir dispositivos en el modo de perfil de trabajo en dispositivos propiedad de la empresa con el método de código QR, agregue esto a la salida de JSON, encima del campo `serverURL`:
`"desiredProvisioningMode": "managedProfile",`

JSON output

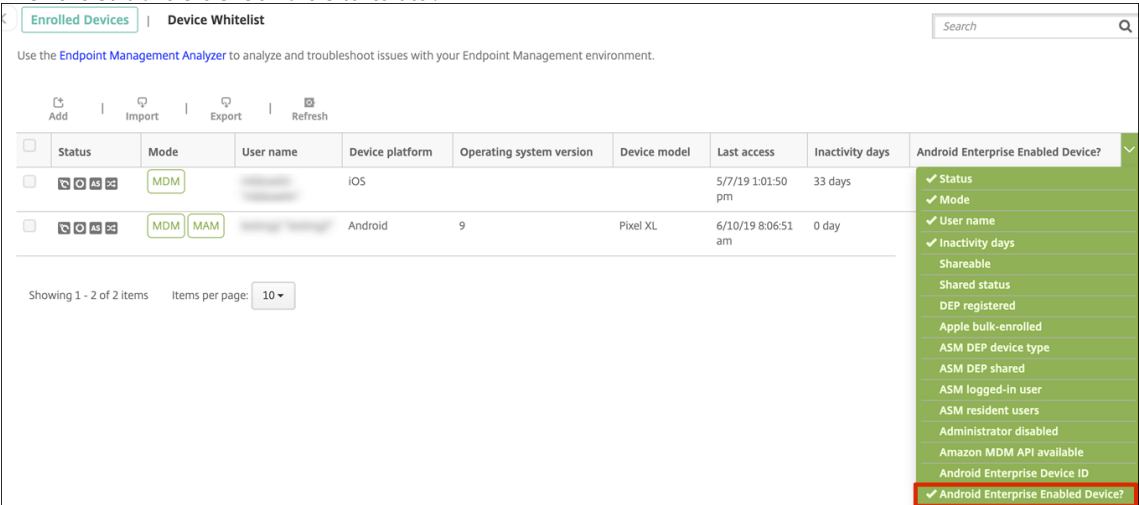
```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
  "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
  "qn7oZUtheu3JBainzZRrjCQv6LOO6LL10jcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
  "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 restablecidos a los valores de fábrica se inscriben como dispositivos de perfil de trabajo como se describe en [Aprovisionar dispositivos de perfil de trabajo en Android Enterprise](#).

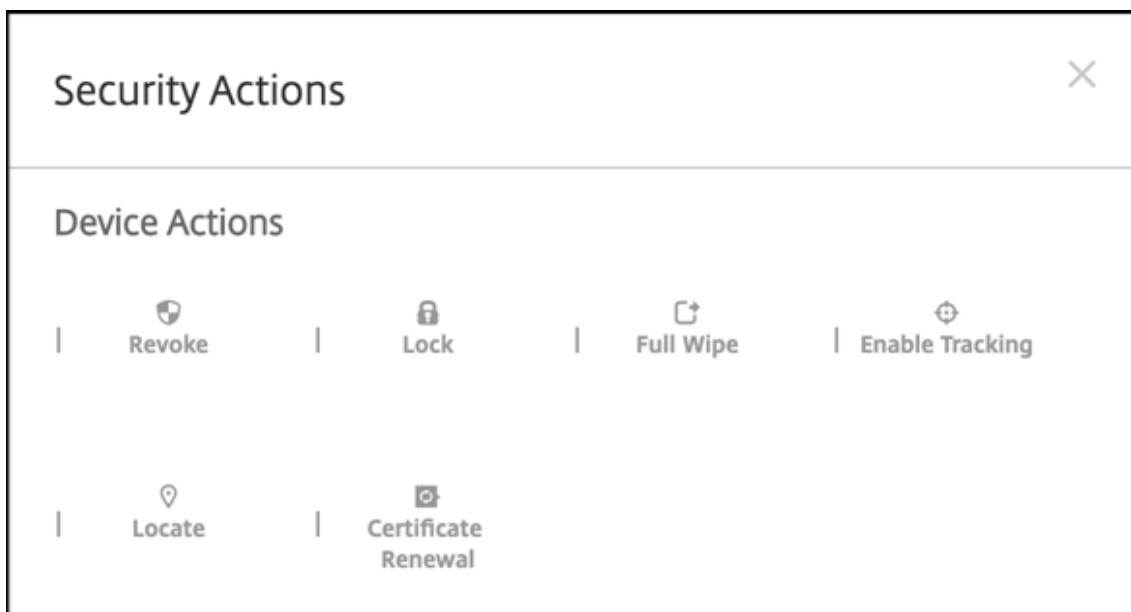
Ver dispositivos Android Enterprise en la consola de Citrix Endpoint Management

Para ver los dispositivos Android Enterprise totalmente administrados, dedicados y totalmente administrados con un perfil de trabajo:

- 1. En la consola de Citrix Endpoint Management, vaya a **Administrar > Dispositivos**.
- 2. Para agregar la columna **¿Dispositivo habilitado para Android Enterprise?**, haga 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. Esta diferencia se debe a que el dispositivo solo permite aplicaciones de Google Play Store administrado. No hay una opción para que el usuario instale aplicaciones desde la tienda pública. Su organización administra todo el contenido del dispositivo.



Configurar directivas de aplicaciones y de dispositivo para Android Enterprise

Para obtener información general de las directivas controladas tanto a nivel de dispositivo como de aplicación, consulte [Directivas MDX y directivas de dispositivo compatibles con Android Enterprise](#).

Qué debe saber sobre las directivas:

- **Restricciones a dispositivos:** Docenas de restricciones para los dispositivos le permiten controlar funciones como:
 - El uso de la cámara del dispositivo
 - Copiar y pegar contenido entre perfiles personales y de trabajo
- **VPN por aplicación:** Utilice la directiva Configuraciones administradas para configurar perfiles de VPN para Android Enterprise.
- **Directiva de correo electrónico:** Se recomienda utilizar la directiva Configuraciones administradas para configurar aplicaciones.

Directivas de dispositivo

En esta tabla se indican todas las directivas de dispositivo disponibles para dispositivos Android Enterprise.

Importante:

Para los dispositivos que se inscriben en Android Enterprise y utilizan aplicaciones MDX, puede controlar algunos parámetros a través de MDX y Android Enterprise. Utilice la configuración de directiva menos restrictiva para MDX y controle la directiva a través de Android Enterprise.

Permisos de aplicación	Inventario de aplicaciones	Desinstalación de aplicaciones
Actualizar automáticamente aplicaciones administradas	Programación de conexiones	Credenciales
XML personalizado	Opciones de Citrix Endpoint Management	Files
Administración de Keyguard	Quiosco	Configuración de Launcher
Ubicación	Configuraciones administradas	Red
Actualización de SO	Código de acceso	Restricciones

Directivas de dispositivo para los dispositivos totalmente administrados con un perfil de trabajo (dispositivos COPE)

En el caso de los dispositivos totalmente administrados con perfiles de trabajo, puede usar algunas directivas de dispositivo para aplicar configuraciones diferentes a todo el dispositivo y al perfil de trabajo. También puede usar otras directivas de dispositivo para aplicar una configuración solo a todo el dispositivo o solo al perfil de trabajo. En el caso de dispositivos inscritos en el modo de perfil de trabajo en dispositivos propiedad de la empresa, las directivas solo se aplican al perfil de trabajo, no a todo el dispositivo.

Directiva	Aplicable a
Permisos de aplicación	Perfil de trabajo
Inventario de aplicaciones	Perfil de trabajo
Desinstalación de aplicaciones	Perfil de trabajo
Actualizar automáticamente 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
Files	Perfil de trabajo
Administración de Keyguard	Dispositivo y perfil de trabajo
Quiosco	N/D
Configuración de Launcher	Dispositivo y perfil de trabajo
Ubicación	Dispositivo (solo modo de ubicación)
Configuraciones administradas	Perfil de trabajo
Red	Dispositivo
Actualización de SO	N/D
Código de acceso	Dispositivo y perfil de trabajo
Restricciones	Dispositivo y perfil de trabajo (crear directivas separadas para el dispositivo y el perfil de trabajo)
VPN	N/D

Consulte también [Directivas MDX y directivas de dispositivo compatibles con Android Enterprise](#) e [Introducción al SDK de MAM](#).

Acciones de seguridad

Android Enterprise admite las siguientes acciones de seguridad. Para ver una descripción de cada acción de seguridad, consulte [Acciones de seguridad](#).

Acciones de seguridad	Perfil de trabajo	Totalmente administrado
Renovación de certificados	Sí	Sí
Borrado completo	Sí (después de un borrado selectivo)	Sí
Localizar	Sí	Sí
Bloquear	Sí	Sí
Bloqueo y restablecimiento de contraseña	No	Sí
Notificar (Hacer sonar)	Sí	Sí
Revocar	Sí	Sí
Borrado selectivo	Sí	Sí

Notas de acciones de seguridad

- La acción de seguridad “Localizar” falla, a menos que la directiva Localización establezca el modo de ubicación para el dispositivo en **Alta precisión** o **Ahorro de batería**. Consulte [Directiva de ubicación](#).
- En dispositivos de perfil de trabajo con versiones de Android anteriores a Android 9.0:
 - La acción de bloqueo y restablecimiento de contraseña no es compatible.
- En dispositivos de perfil de trabajo con la versión de Android 9.0 o posterior:
 - El código de acceso enviado bloquea el perfil de trabajo. El dispositivo en sí no se bloquea.
 - Si no hay un código de acceso establecido en el perfil de trabajo:
 - ★ Si no se envía ningún código de acceso o el código enviado no cumple los requisitos de código de acceso, el dispositivo se bloquea.
 - Si hay un código de acceso establecido en el perfil de trabajo:
 - ★ Si no se envía ningún código de acceso o el código enviado no cumple los requisitos de código de acceso, el perfil de trabajo se bloquea, pero el dispositivo no se bloquea.

Desinscribir una empresa de Android Enterprise

Si ya no quiere utilizar su empresa de Android Enterprise, puede desinscribirla.

Advertencia:

Una vez que desinscriba una empresa, las aplicaciones de Android Enterprise en dispositivos ya inscritos a través de ella se restablecen a sus estados predeterminados. Google ya no administra los dispositivos. Si se inscribe en una nueva empresa de Android Enterprise, deberá aprobar aplicaciones para la nueva organización desde Google Play administrado. A continuación, puede actualizar las aplicaciones desde la consola de Citrix Endpoint Management.

Después de que la empresa Android Enterprise se ha desinscrito:

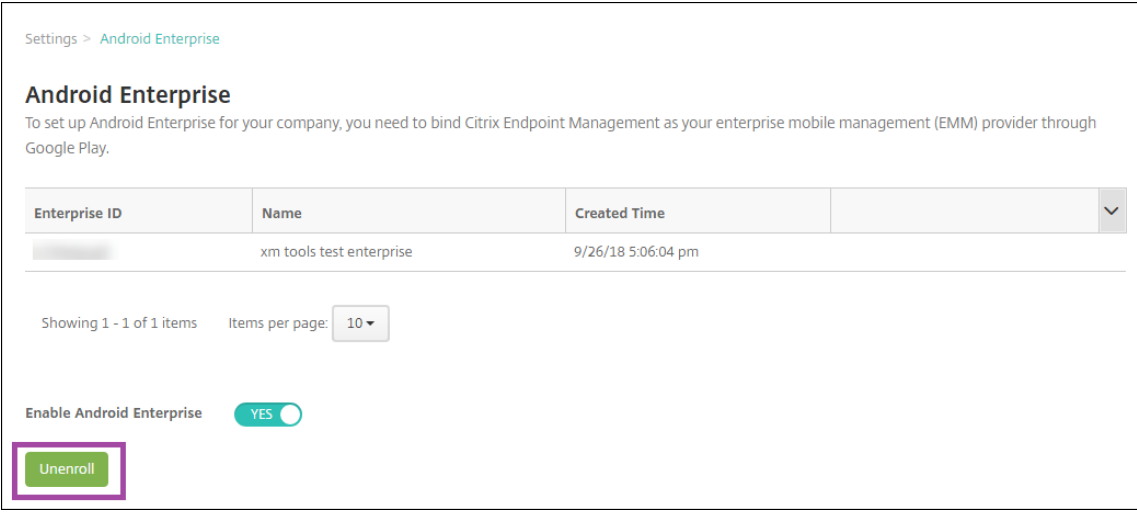
- En los dispositivos y los usuarios inscritos a través de la empresa, las aplicaciones de Android Enterprise se restablecen a sus estados predeterminados. Las directivas Configuraciones administradas que se hayan aplicado ya no afectan a las operaciones.
- Citrix Endpoint Management administra los dispositivos inscritos a través de la empresa. Desde el punto de vista de Google, esos dispositivos no están administrados. No puede agregar nuevas aplicaciones de Android Enterprise. No se pueden aplicar directivas Configuraciones administradas. Se pueden aplicar otras directivas, tales 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.

Desinscriba una empresa de Android Enterprise mediante la consola del servidor de Citrix Endpoint Management y las herramientas de Citrix Endpoint Management Tools.

Cuando realiza esta tarea, Citrix Endpoint Management abre una ventana emergente para las herramientas. Antes de comenzar, asegúrese de que el explorador tenga permiso para abrir ventanas emergentes. Algunos exploradores web, como Google Chrome, requieren que se inhabilite el bloqueo de ventanas emergentes y se agregue la dirección del sitio de Citrix Endpoint Management a la lista de permitidos del bloqueo de ventanas emergentes.

Para desinscribir una empresa de Android Enterprise

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En la página **Parámetros**, haga clic en **Android Enterprise**.
3. Haga clic en **Desinscribir**.



Distribuir aplicaciones de Android Enterprise

November 29, 2023

Citrix Endpoint Management administra las aplicaciones implementadas en los dispositivos. Puede organizar e implementar los siguientes tipos de aplicaciones de Android Enterprise.

- **Aplicaciones de la tienda de aplicaciones administrada:** 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 MDX Toolkit. Estas aplicaciones incluyen directivas MDX. Las aplicaciones MDX se obtienen de fuentes internas y tiendas públicas. Implemente aplicaciones móviles de productividad de Citrix como aplicaciones MDX.
- **Aplicaciones de empresa:** Aplicaciones privadas que usted desarrolla u obtiene de otra fuente. Estas aplicaciones se ofrecen a los usuarios a través de Google Play Store administrado. Google Play Store administrado es la tienda de aplicaciones de empresa de Google.
- **Aplicaciones privadas habilitadas para MDX:** Aplicaciones de empresa preparadas con el SDK de MAM o empaquetadas con MDX Toolkit.

Puede agregar aplicaciones de empresa y aplicaciones privadas habilitadas para MDX de dos formas diferentes.

- Agregue las aplicaciones a la consola de Citrix Endpoint Management como aplicaciones de empresa, tal y como se describe en las secciones Aplicaciones de empresa y Aplicaciones privadas habilitadas para MDX de este artículo.
- Publique las aplicaciones directamente en Google Play Store administrado con la cuenta de desarrollador de Google. A continuación, agregue las aplicaciones a la consola de Citrix Endpoint

Management como aplicaciones administradas de la tienda de aplicaciones. Consulte [Aplicaciones administradas de la tienda de aplicaciones](#).

Si publica aplicaciones con la cuenta de desarrollador de Google y, a continuación, pasa a utilizar la consola de Citrix Endpoint Management, cambiará el propietario de las aplicaciones. En este caso, deberá administrar las aplicaciones en ambas ubicaciones. Citrix recomienda agregar las aplicaciones siguiendo un método u otro, no los dos.

Si necesita quitar aplicaciones autoadministradas de Google Play Store administrado, abra un tíquet con Google. Los desarrolladores pueden inhabilitar, pero no eliminar, aplicaciones de Google Play Store administrado.

En las secciones siguientes, se ofrece información más detallada sobre la configuración de aplicaciones Android Enterprise. Para obtener información sobre cómo distribuir aplicaciones, consulte [Agregar aplicaciones](#). Este artículo contiene:

- Flujos de trabajo generales para agregar aplicaciones web y SaaS o enlaces web
- El flujo de trabajo para aplicaciones obligatorias de empresa y de tienda pública
- Cómo entregar aplicaciones empresariales desde la red de entrega de contenido (CDN) de Citrix Content Delivery para las aplicaciones empresariales.

Aplicaciones administradas de la tienda de aplicaciones

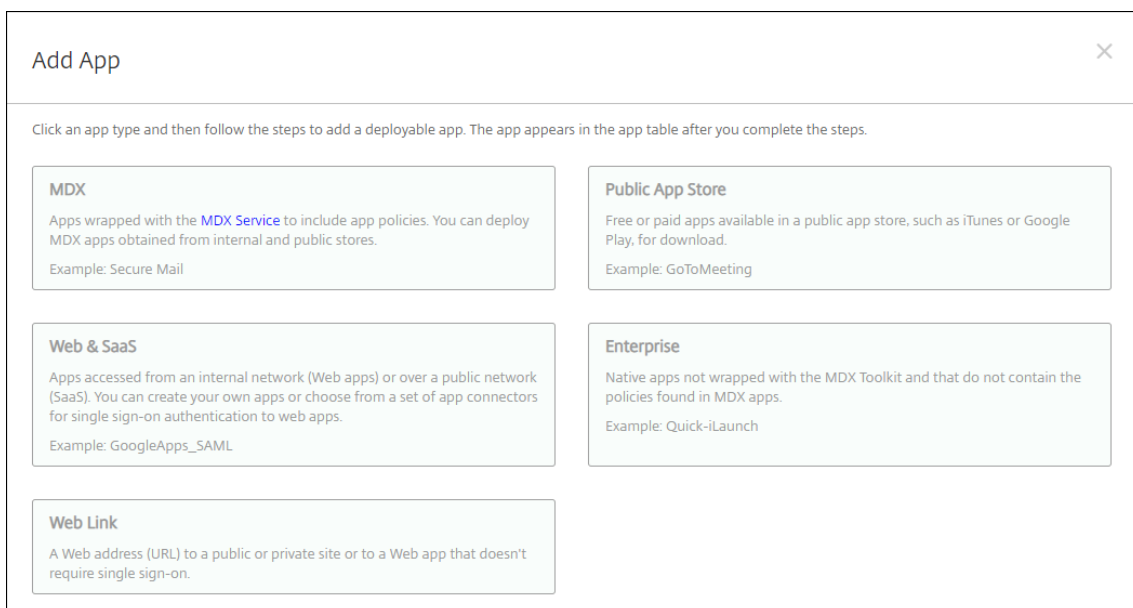
Puede agregar, a Citrix Endpoint Management, aplicaciones gratuitas disponibles en Google Play Store administrado.

Nota:

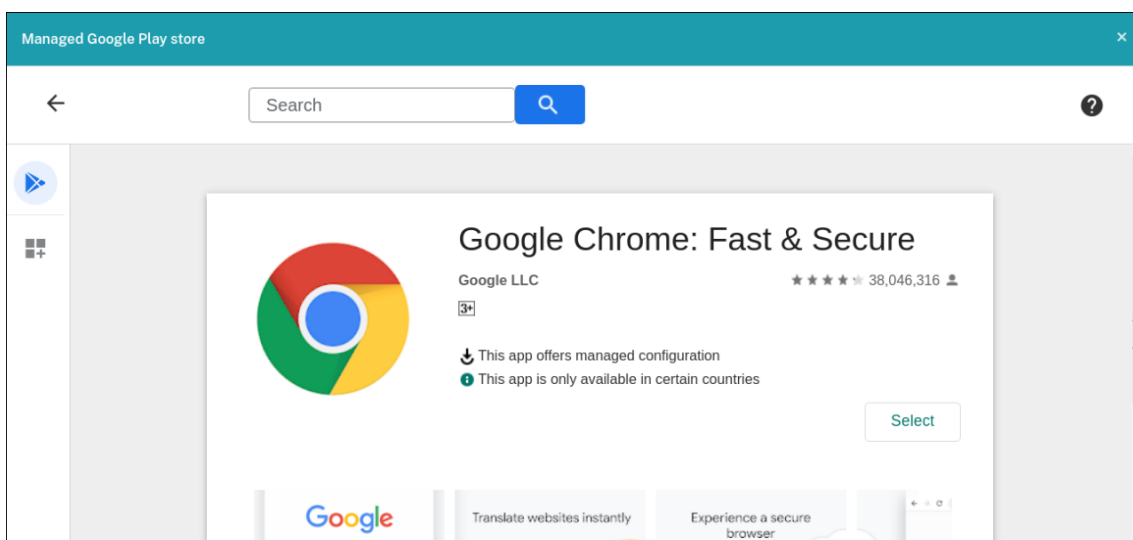
Para que todas las aplicaciones de Google Play Store sean accesibles desde Google Play administrado, utilice la propiedad de servidor **Acceder a todas las aplicaciones en Google Play Store**. Consulte [Propiedades de servidor](#). Al establecer esta propiedad en **true**, todos los usuarios de Android Enterprise pueden acceder a aplicaciones de la tienda pública de Google Play. A continuación, puede usar la [directiva 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 pública de aplicaciones**.



3. En el panel **Información de la aplicación**, escriba la información siguiente:
 - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en **Nombre de la aplicación**, en la tabla **Aplicaciones**.
 - **Descripción:** Escriba, si quiere, una descripción 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 encontrar el ID de paquete en Google Play Store. El ID se encuentra en la dirección URL de la aplicación. Por ejemplo, **com.Slack** es el ID de paquete en https://play.google.com/store/apps/details?id=com.Slack&hl=en_US.
6. Aparecerán las aplicaciones que coincidan con los criterios de búsqueda. Haga clic en la aplicación deseada y luego haga clic en **Seleccionar**.



7. Haga clic en **Seleccionar** de nuevo.
8. Haga clic en el icono de la aplicación y defina el **nombre** y la **descripción** de la aplicación.

Public App Store

- 1 App Information
- 2 Platform Clear All
 - ☐ iPhone
 - ☐ iPad
 - ☐ Android (legacy DA)
 - ☒ **Android Enterprise**
 - ☐ Windows Desktop/Tablet
 - ☐ Windows Phone
- 3 Approvals (optional)
- 4 Delivery Group Assignments (optional)

Managed Google Play
Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

com.podio Search

Search results for com.podio in Managed Google Play

Podio
Podio ApS

Didn't find the app you were looking for?

App Details

Name * Podio

Description * The flexible way to manage projects, anywhere.

Product track Production - 20.9.0

Version 20.9.0

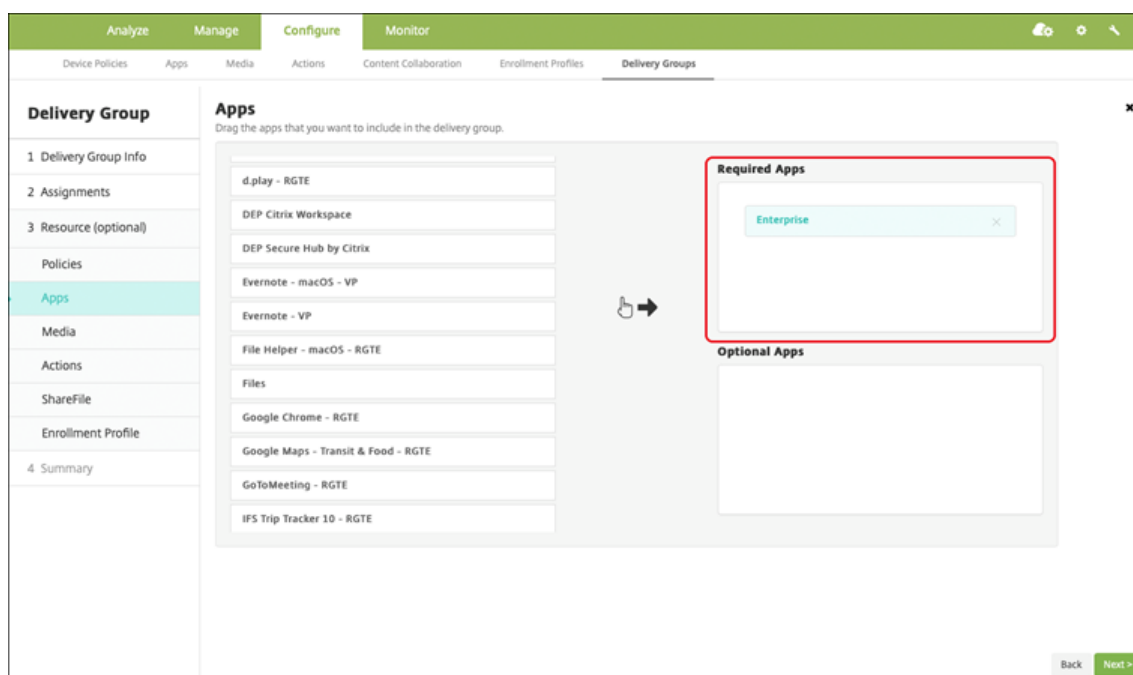
Package ID com.podio

Image

9. Asigne los grupos de entrega que quiera a la aplicación y haga clic en **Guardar**. Para obtener 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 **Edit**.
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 los archivos MDX a Citrix Endpoint Management y configure los detalles de la aplicación, además de las configuraciones de las directivas que se aplicarán a ella. Si quiere configurar las aplicaciones móviles de productividad de Citrix para Android Enterprise, agréguelas como aplicaciones MDX. Para obtener información sobre las directivas de aplicaciones que están disponibles para cada tipo de plataforma de dispositivos, consulte:

- [Introducción al SDK de MAM](#)
- [Vista general de las directivas MDX](#)

Paso 1: Agregar y configurar aplicaciones

1. Para las aplicaciones móviles de productividad de Citrix, descargue los archivos MDX de tienda pública; es decir, vaya a <https://www.citrix.com/downloads>. Vaya a **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.

Para otros tipos de aplicaciones MDX, debe obtener 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**.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the **MDX Service** to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: Secure Mail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Haga clic en **MDX**. Aparecerá la página **Información de la aplicación MDX**. En el panel **Información de la aplicación**, escriba la información siguiente:

- **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en **Nombre de la aplicación**, en la tabla **Aplicaciones**.
- **Descripción:** Escriba, si quiere, una descripción 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 la aprobación de Google Play Store administrado. Para aprobar la aplicación sin salir de la consola de Citrix Endpoint Management, haga clic en **Sí**.

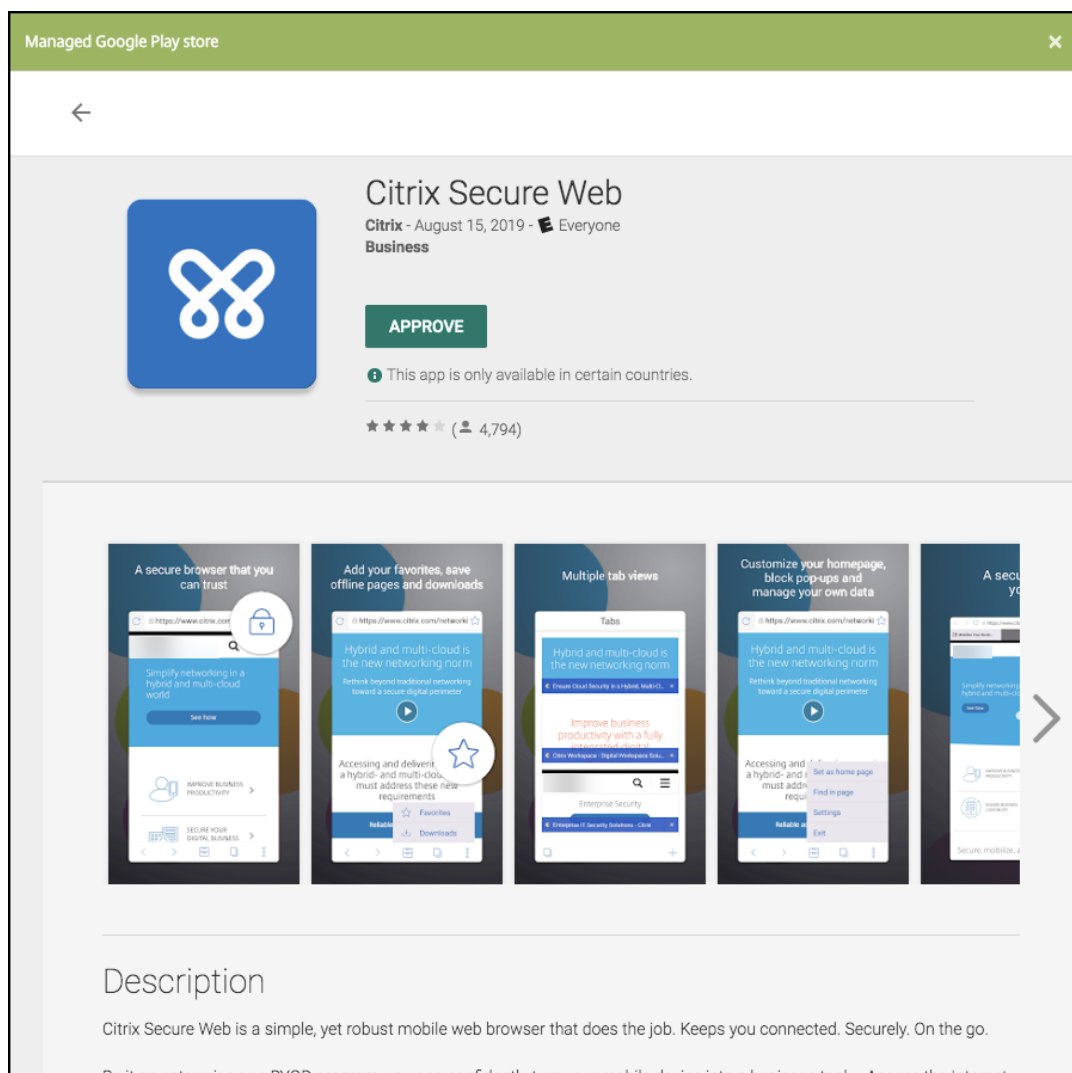
App is not approved

App is not approved on the managed Google Play store. You can approve the app now or later. Do you want to approve it now?

No

Yes

Una vez abierto Google Play Store administrado, siga las instrucciones para aprobar y guardar la aplicación.



Al agregarse correctamente la aplicación, aparece la página **Detalles de la aplicación**.

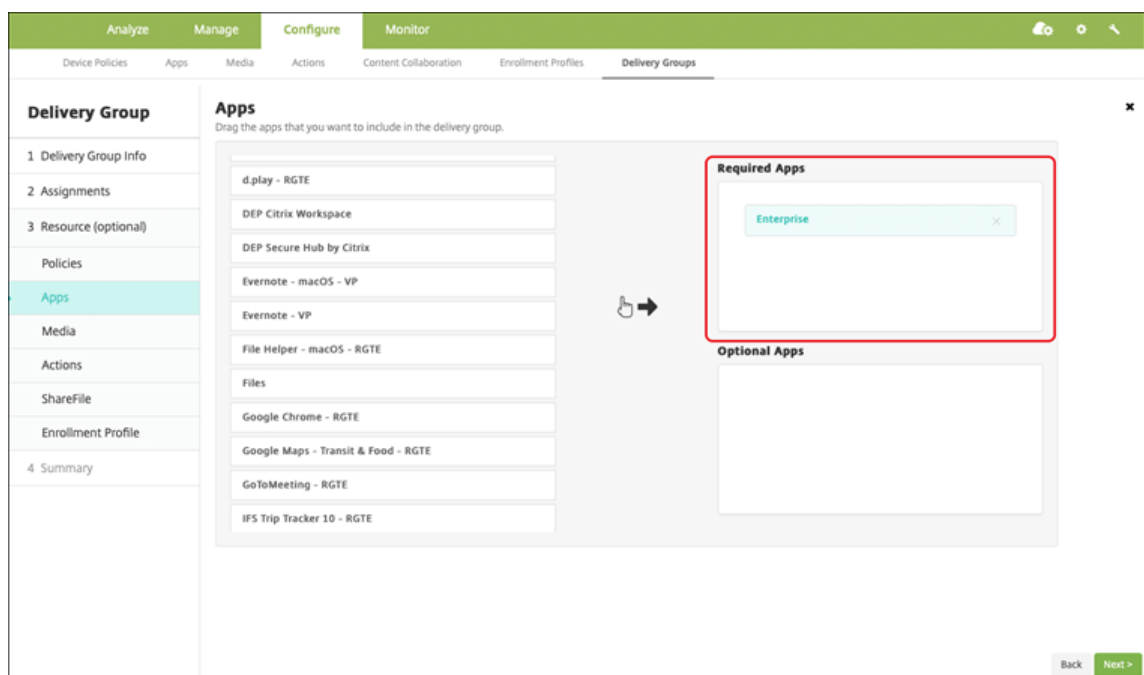
6. Configure estos parámetros:

- **Nombre de archivo:** Escriba el nombre del archivo asociado a la aplicación.
- **Descripción de la aplicación:** Escriba una descripción de la aplicación.
- **Versión de la aplicación:** Si quiere, 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 de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
- **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
- **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.

- Configure las **directivas MDX**. Las directivas MDX varían según la plataforma. Además, estas directivas incluyen opciones para tales áreas de directiva como autenticación, seguridad de los dispositivos y restricciones a aplicaciones. En la consola, se ofrece información descriptiva sobre cada una de las directivas. Para obtener información sobre las directivas de aplicaciones que están disponibles para cada tipo de plataforma de dispositivos, consulte:
 - [Introducción al SDK de MAM](#)
 - [Vista general de las directivas MDX](#)
- Configure las reglas de implementación y los parámetros del almacén.
- Asigne los grupos de entrega que quiera a la aplicación y haga clic en **Guardar**. Para obtener información, consulte [Implementar recursos](#).

Paso 2: Configurar la implementación de aplicaciones

- Vaya a **Configurar > Grupos de entrega** y seleccione el grupo de entrega que configuró. Haga clic en **Edit**.
- En la sección **Aplicaciones**, arrastre las aplicaciones deseadas al cuadro **Aplicaciones obligatorias**.



- En la página **Resumen**, haga clic en **Guardar**.
- En la página **Grupos de entrega**, seleccione el grupo de entrega y haga clic en **Implementar**.

Aplicaciones de empresa

Las aplicaciones empresariales representan aplicaciones privadas que no están preparadas con el SDK de MAM o MDX Toolkit. Se trata de aplicaciones desarrolladas internamente o se han obtenido directamente de otras fuentes. Para agregar una aplicación de empresa, se necesita el archivo APK asociado a ella. Debe seguir las [Prácticas recomendadas de aplicaciones privadas](#) de Google.

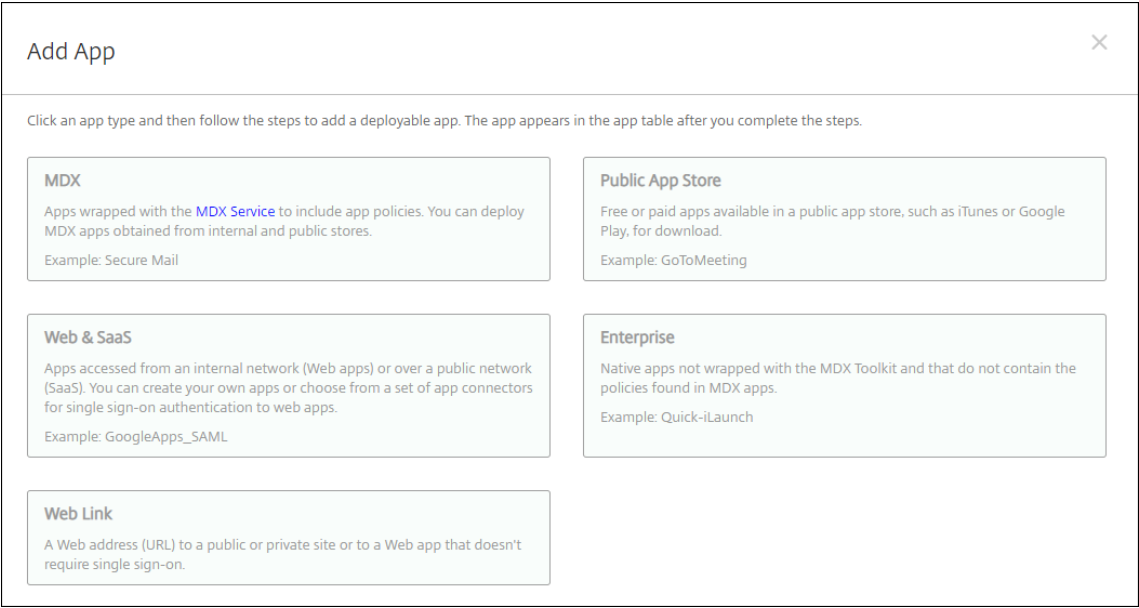
Vea este vídeo para obtener más información:



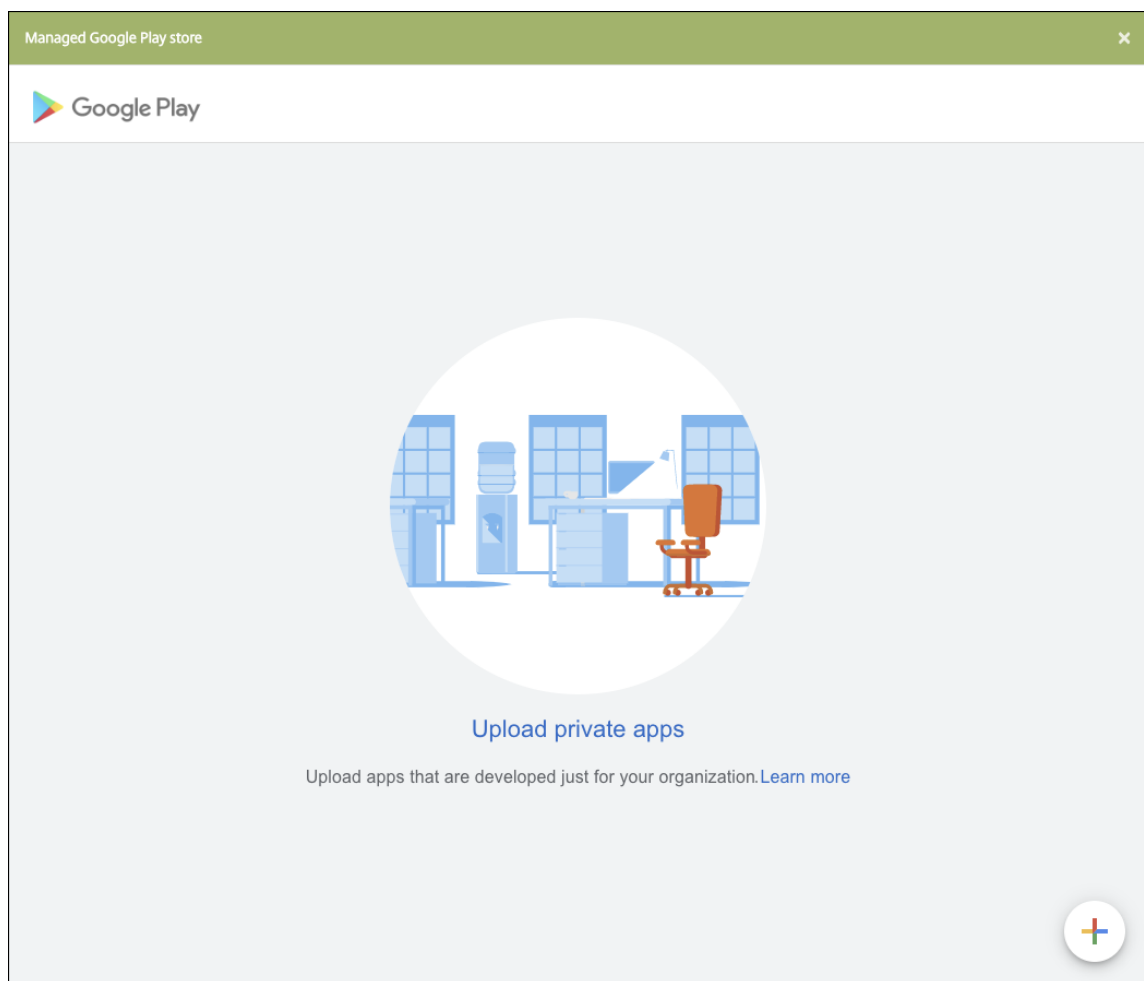
Paso 1: Agregar y configurar aplicaciones

Agregue la aplicación de una de dos maneras:

- Publique la aplicación directamente en Google Play Store administrado y agréguela a la consola de Citrix Endpoint Management como una aplicación de Google Play Store administrado. Siga las indicaciones de la documentación de Google sobre cómo [publicar aplicaciones privadas](#) y, a continuación, siga los pasos descritos en la sección Aplicaciones administradas de la tienda de aplicaciones.
- Agregue la aplicación a la consola de Citrix Endpoint Management como una aplicación de empresa. Siga estos pasos:
 1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones**. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.



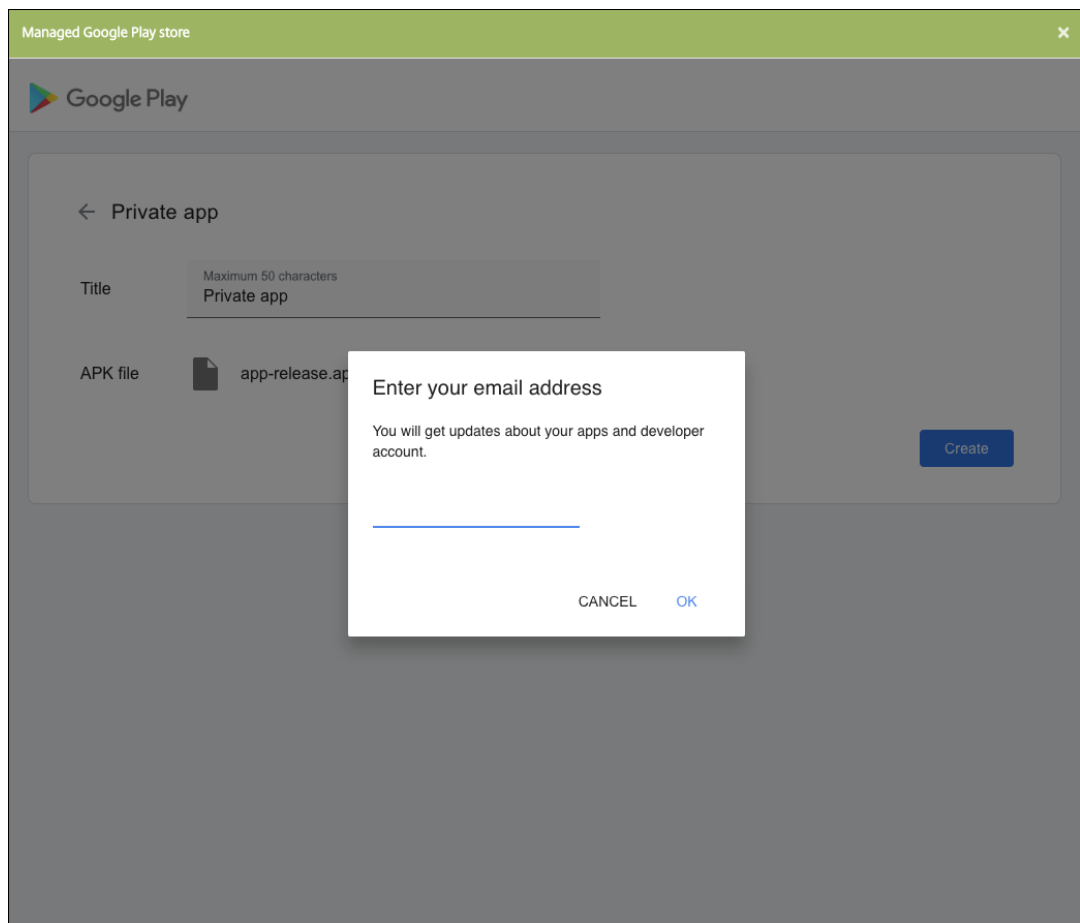
- Haga clic en **Empresa**. En el panel **Información de la aplicación**, escriba la información siguiente:
 - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en “Nombre de la aplicación”, en la tabla “Aplicaciones”.
 - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
- Seleccione **Android Enterprise** como plataforma.
- El botón **Cargar** abre Google Play Store administrado. No es necesario registrarse con una cuenta de desarrollador para publicar una aplicación privada. Haga clic en el icono **Más** situado en la esquina inferior derecha para continuar.



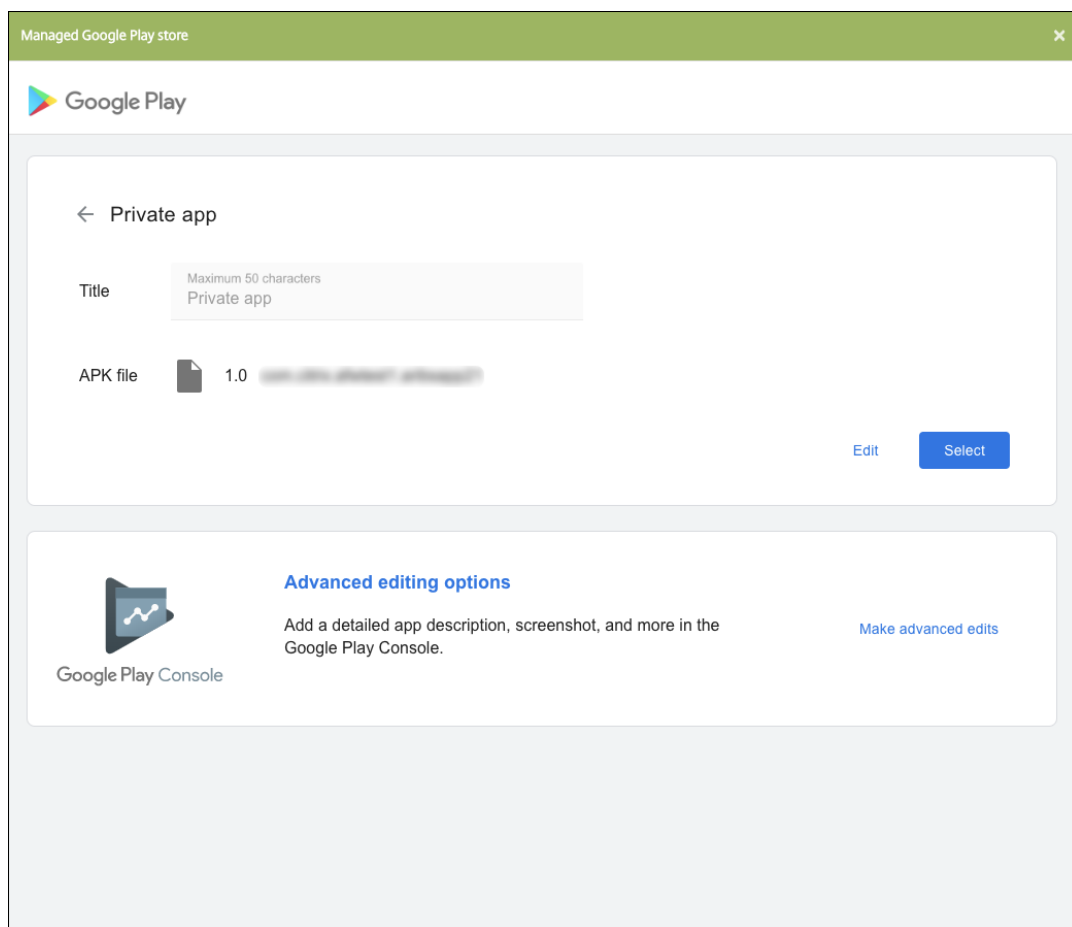
- a) Introduzca el nombre de la aplicación y cargue el archivo APK. Cuando haya terminado, haga clic en **Crear**. La aplicación privada puede tardar hasta 10 minutos en publicarse.

The screenshot shows a window titled "Managed Google Play store" with a close button (X) in the top right corner. Below the title bar is the Google Play logo. The main content area is titled "← Private app". It contains a "Title" label followed by a text input field with a placeholder "Maximum 50 characters". Below this is an "APK file" label followed by a blue button labeled "Upload APK". In the bottom right corner of the form area is a grey button labeled "Create".

- b) Introduzca una dirección de correo electrónico para obtener actualizaciones sobre sus aplicaciones.



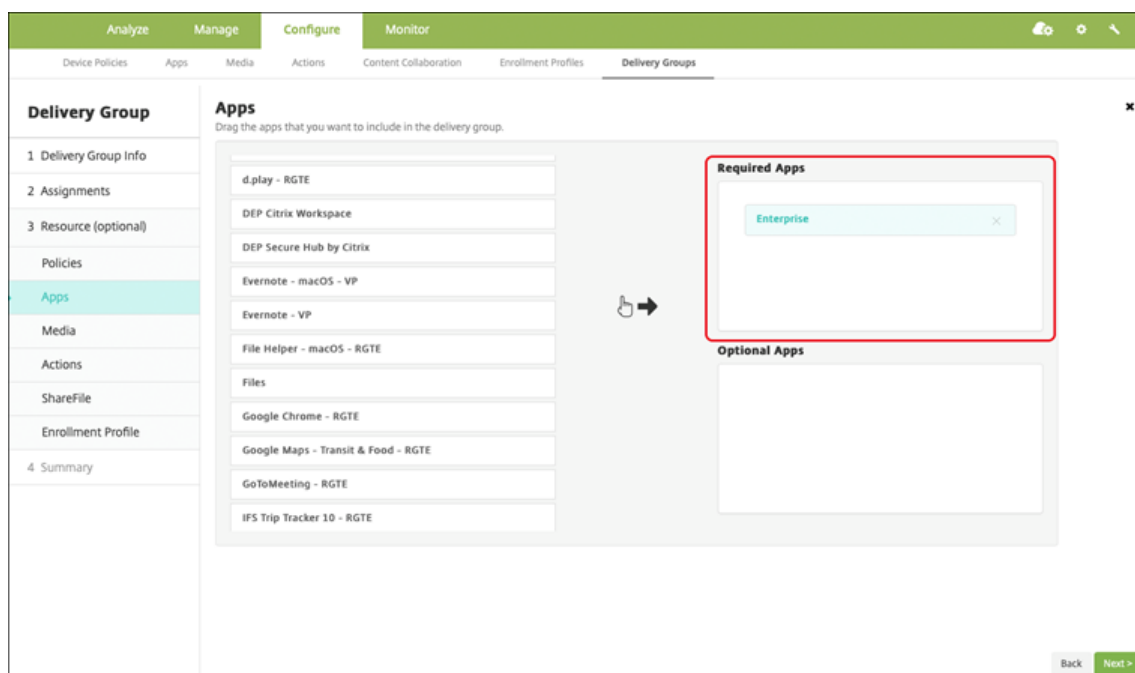
- c) Después de publicar la aplicación, haga clic en el icono de la aplicación privada. Si quiere agregar una descripción de la aplicación, cambiar el icono de esta o realizar otras acciones, haga clic en la opción para **realizar modificaciones avanzadas**. De lo contrario, haga clic en **Seleccionar** para abrir la página de información de la aplicación.



5. Haga clic en **Siguiente**. Aparecerá la página de información referente a la aplicación para la plataforma pertinente.
6. Configure los parámetros para el tipo de plataforma, como:
 - **Nombre de archivo:** Si quiere, escriba un nuevo nombre para la aplicación.
 - **Descripción de la aplicación:** Si quiere, indique una nueva descripción de la aplicación.
 - **Versión de la aplicación:** Este campo no se puede cambiar.
 - **ID del paquete:** Identificador único de la aplicación.
 - **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
 - **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
 - **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
7. Configure las reglas de implementación y los parámetros del almacén.
8. Asigne los grupos de entrega que quiera a la aplicación y haga clic en **Guardar**. Para obtener 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 **Edit**.
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 privadas habilitadas para MDX

Para agregar aplicaciones de Android Enterprise como aplicaciones de empresa habilitadas para MDX:

1. Cree una aplicación privada de Android Enterprise y habilítela para MDX.
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 aplicación de empresa.
3. Agregue el archivo MDX a Citrix Endpoint Management.

Si decide alojar y publicar aplicaciones a través de Google Play Store, no elija la firma de certificados de Google. Firme la aplicación con el mismo certificado utilizado para habilitar la aplicación para

MDX. Para obtener más información sobre la publicación de aplicaciones, consulte la documentación de Google en [Cómo publicar tu app](#) y [Firma tu app](#). El SDK de MAM no empaqueta aplicaciones, por lo que no requiere un certificado distinto del utilizado para desarrollar la aplicación.

Para obtener más información sobre cómo publicar aplicaciones privadas a través de la consola de Google Play, consulte [Publicar aplicaciones privadas desde Play Console](#) en la documentación de Google.

Para publicar una aplicación a través de Citrix Endpoint Management, consulte las secciones siguientes.

Preparar una aplicación de Android Enterprise

Al crear una aplicación de Android Enterprise, debe seguir [las prácticas recomendadas de aplicaciones privadas](#) de Google.

Después de crear una aplicación de Android Enterprise, integre el SDK de MAM en la aplicación o empaquete la aplicación con MDX Toolkit. A continuación, agregue los archivos resultantes a XenMobile.

Puede actualizar la aplicación cargando un archivo APK actualizado. Los pasos siguientes cubren el empaquetado de aplicaciones con MDX Toolkit.

1. Cree la aplicación de Android Enterprise y genere un archivo APK firmado.
2. El siguiente archivo de ejemplo contiene todas las directivas conocidas. Es posible que algunas de ellas no se puedan aplicar a su entorno. Se ignoran todas las configuraciones que no se puedan utilizar. Cree un archivo XML con los siguientes parámetros:

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <MobileAppPolicies>
3   <PolicySchemaVersion>
4     1.0
5   </PolicySchemaVersion>
6   <Policies>
7     <DevicePasscode>false</DevicePasscode>
8     <AppPasscode>false</AppPasscode>
9     <MaxOfflinePeriod>72</MaxOfflinePeriod>
10    <SetupAuthAddress/>
11    <RequireUserEntropy>false</RequireUserEntropy>
12    <BlockRootedDevices>true</BlockRootedDevices>
13    <BlockDebuggerAccess>false</BlockDebuggerAccess>
14    <RequireDeviceLock>false</RequireDeviceLock>
15    <NonCompliantDeviceBehavior>AllowAppAfterWarning</NonCompliantDeviceBehavior>
16    <WifiOnly>false</WifiOnly>
17    <RequireInternalNetwork>false</RequireInternalNetwork>
18    <InternalWifiNetworks/>
19    <AllowedWifiNetworks/>
20    <UpgradeGracePeriod>168</UpgradeGracePeriod>
```

```

21      <WipeDataOnAppLock>false</WipeDataOnAppLock>
22      <ActivePollPeriod>60</ActivePollPeriod>
23      <PublicFileAccessLimitsList/>
24      <CutAndCopy>Unrestricted</CutAndCopy>
25      <Paste>Unrestricted</Paste>
26      <DocumentExchange>Unrestricted</DocumentExchange>
27      <OpenInExclusionList/>
28      <InboundDocumentExchange>Unrestricted</
        InboundDocumentExchange>
29      <InboundDocumentExchangeWhitelist/>
30      <connectionSecurityLevel>TLS</connectionSecurityLevel>
31      <DisableCamera>false</DisableCamera>
32      <DisableGallery>false</DisableGallery>
33      <DisableMicrophone>false</DisableMicrophone>
34      <DisableLocation>false</DisableLocation>
35      <DisableSms>false</DisableSms>
36      <DisableScreenCapture>false</DisableScreenCapture>
37      <DisableSensor>false</DisableSensor>
38      <DisableNFC>false</DisableNFC>
39      <BlockLogs>false</BlockLogs>
40      <DisablePrinting>false</DisablePrinting>
41      <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
        MvpnNetworkAccess>
42      <MvpnSessionRequired>False</MvpnSessionRequired>
43      <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>
44      <DisableLocalhostConnections>false</
        DisableLocalhostConnections>
45      <CertificateLabel/>
46      <DefaultLoggerOutput>file,console</DefaultLoggerOutput>
47      <DefaultLoggerLevel>15</DefaultLoggerLevel>
48      <MaxLogFiles>2</MaxLogFiles>
49      <MaxLogFileSize>2</MaxLogFileSize>
50      <RedirectSystemLogs>false</RedirectSystemLogs>
51      <EncryptLogs>false</EncryptLogs>
52      <GeofenceLongitude>0</GeofenceLongitude>
53      <GeofenceLatitude>0</GeofenceLatitude>
54      <GeofenceRadius>0</GeofenceRadius>
55      <EnableGoogleAnalytics>false</EnableGoogleAnalytics>
56      <Authentication>OfflineAccessOnly</Authentication>
57      <ReauthenticationPeriod>480</ReauthenticationPeriod>
58      <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
59    </Policies>
60  </MobileAppPolicies>
61  <!--NeedCopy-->

```

3. Empaquete la aplicación con MDX Toolkit. Para obtener información sobre cómo usar MDX Toolkit, consulte [Empaquetar 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 aplicaciones, establezca el parámetro **storeURL** en la URL de la tienda. Una vez publicada la aplicación, los usuarios pueden descargarla desde la URL de la

tienda.

Aquí se muestra un ejemplo de un comando de MDX Toolkit utilizado para empaquetar una aplicación llamada SampleAEapp:

```
1  ```\n2  java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -\n    Duser.variant\n3  -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap\n4  -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk\n5  -out ~/Desktop/AEAppFiles/SampleAEApp.mdx\n6  -MinPlatform 5.0\n7  -keystore /MyKeystore\n8  -storepass mystorepwd123\n9  -keyalias key0\n10 -keypass mykeypwd123\n11 -storeURL "https://play.google.com/store/apps/details?id=\n    SampleAEAppPackage"\n12 -appType Premium\n13 -premiumMdxPolicies <Path to Premium policy XML>\n14 <!--NeedCopy--> ```\n
```

Al empaquetar la aplicación, se genera un archivo APK empaquetado y un archivo MDX.

Agregar el archivo APK empaquetado

Agregue la aplicación de una de dos maneras:

- Publique la aplicación directamente en Google Play Store administrado y agréguela a la consola de Citrix Endpoint Management como una aplicación de Google Play Store administrado. Siga las indicaciones de la documentación de Google sobre cómo [publicar aplicaciones privadas](#) y, a continuación, siga los pasos descritos en la sección Aplicaciones administradas de la tienda de aplicaciones.
- Agregue la aplicación a la consola de Citrix Endpoint Management como una aplicación de empresa. 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**.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the [MDX Service](#) to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: Secure Mail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Haga clic en **Empresa**. En el panel **Información de la aplicación**, escriba la información siguiente:

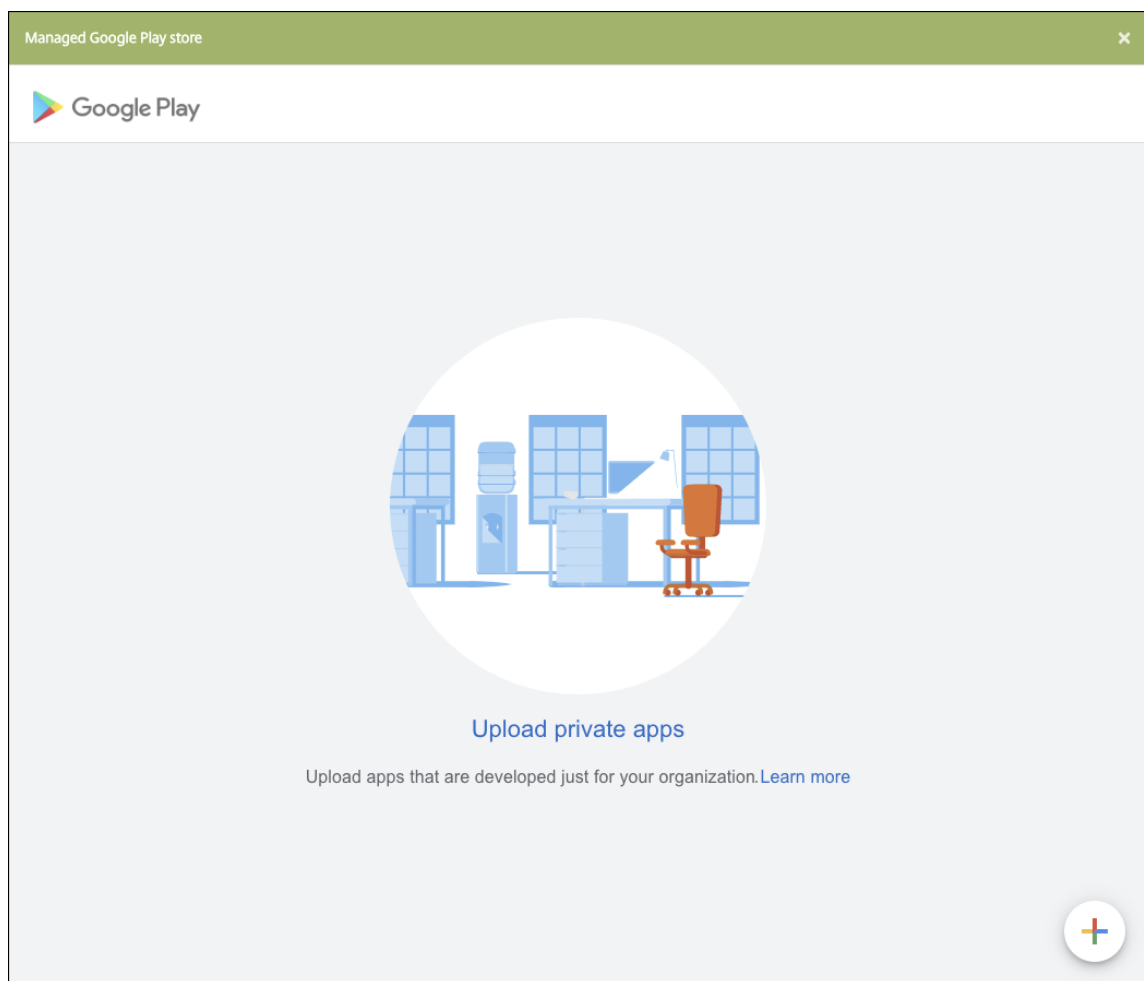
- **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en “Nombre de la aplicación”, en la tabla “Aplicaciones”.
- **Descripción:** Escriba, si quiere, una descripción de la aplicación.

4. Seleccione **Android Enterprise** como plataforma.

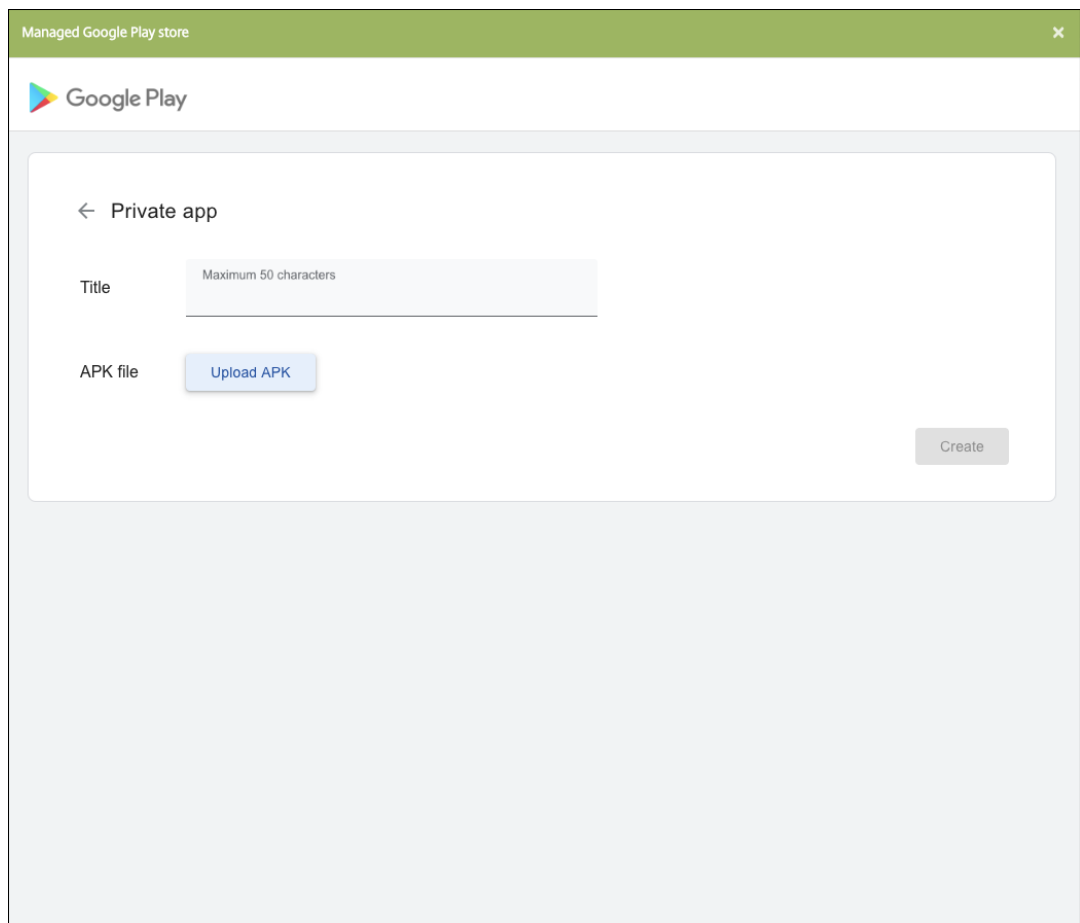
5. El botón **Cargar** abre Google Play Store administrado. No es necesario registrarse con una cuenta de desarrollador para publicar una aplicación privada. Haga clic en el icono **Más** situado en la esquina inferior derecha para continuar.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

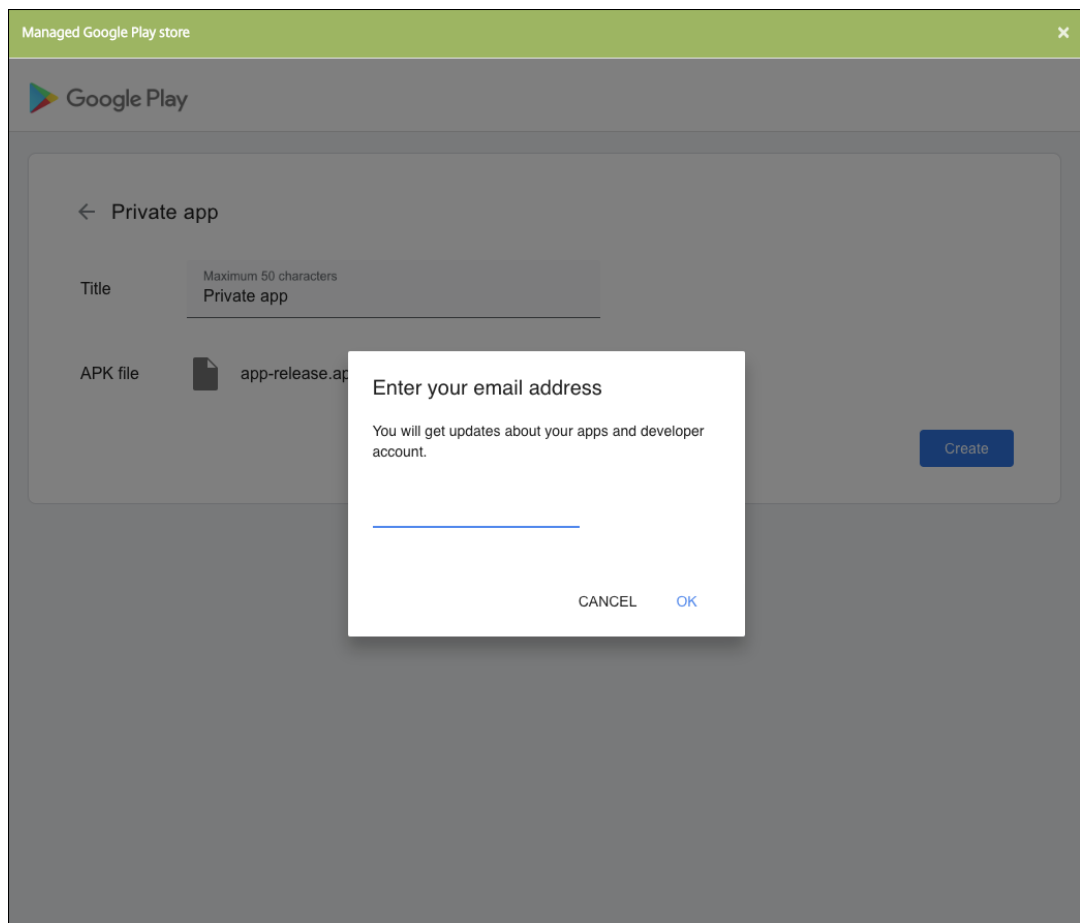
431



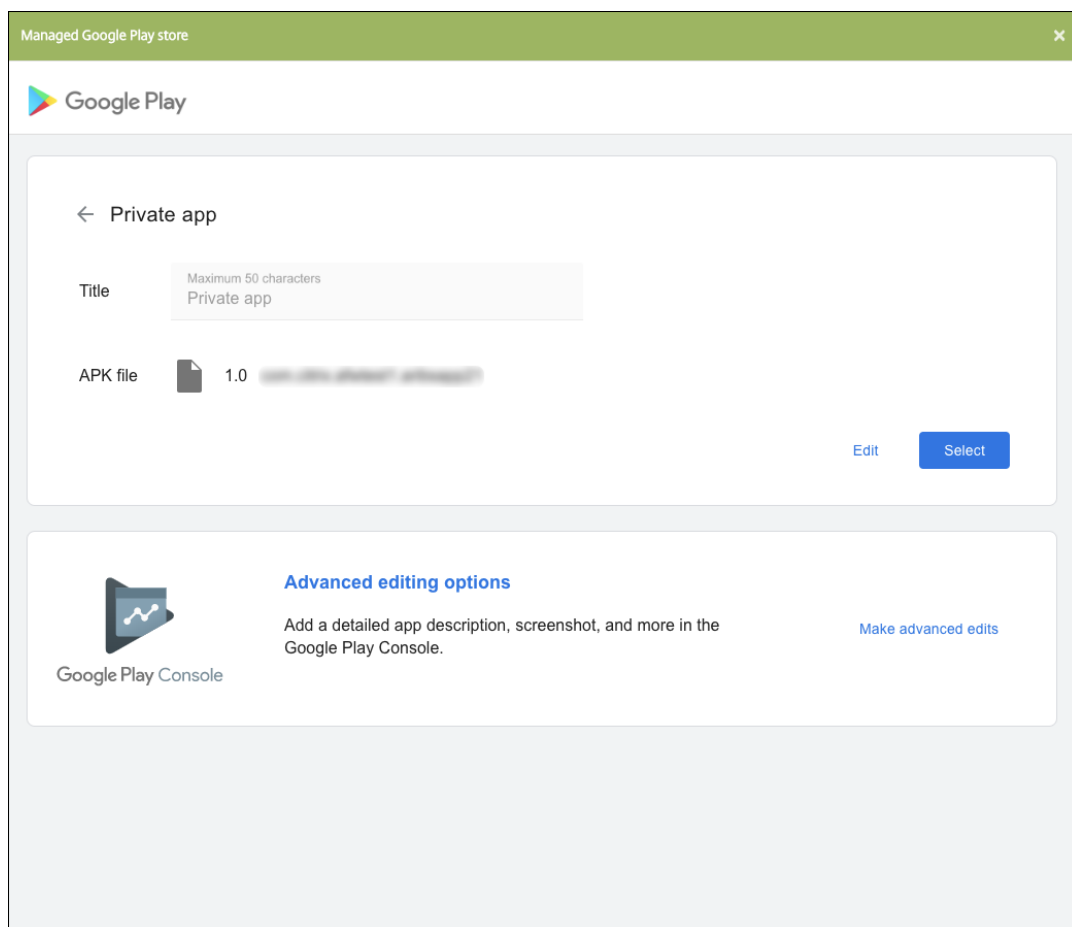
- a) Introduzca el nombre de la aplicación y cargue el archivo APK. Cuando haya terminado, haga clic en **Crear**. La aplicación privada puede tardar hasta 10 minutos en publicarse.



- b) Introduzca una dirección de correo electrónico para obtener 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 referente a la aplicación para la plataforma pertinente.
7. Configure los parámetros para el tipo de plataforma, como:
 - **Nombre de archivo:** Si quiere, escriba un nuevo nombre para la aplicación.
 - **Descripción de la aplicación:** Si quiere, indique una nueva descripción de la aplicación.
 - **Versión de la aplicación:** Este campo no se puede cambiar.
 - **ID del paquete:** Identificador único de la aplicación.
 - **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
 - **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
 - **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
8. Configure las reglas de implementación y los parámetros del almacén.
9. En la página **Aplicación de empresa**, haga clic en **Siguiente**. Aparecerá la página **Aprobaciones**.

Para utilizar flujos de trabajo que requieran aprobación antes de permitir que los usuarios accedan a la aplicación, consulte [Aplicar flujos de trabajo](#). Si no necesita flujos de trabajo de aprobación, puede ir directamente al paso 13.

10. Haga clic en **Siguiente**.
11. Aparecerá la página **Asignación de grupos de entrega**. No es necesario realizar ninguna acción en esta página. Los grupos de entrega y la programación de implementación de esta aplicación se configuran al agregar el archivo MDX. Haga clic en **Guardar**.

Opcional: Agregar o cambiar la dirección URL de la tienda

Si no sabía cuál era la dirección URL de la tienda al empaquetar la aplicación, puede agregarla ahora.

1. Seleccione la aplicación en Google Play Store administrado. Al seleccionar la aplicación, la URL de la tienda aparece en la barra de direcciones del explorador. Copie el nombre del paquete de la aplicación desde el formulario de la URL. Por ejemplo: <https://play.google.com/store/apps/details?id=SampleAEappPackage>. Puede que la URL que copie empiece por <https://play.google.com/work/>. Debe cambiar **work** a **store**.
2. Con MDX Toolkit, agregue la URL del almacén al archivo MDX:

```
1 java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \  
2 setinfo \  
3 -in ~/Desktop/SampleApps/Sample.mdx \  
4 -out ~/Desktop/SampleApps/wrapped/Sample.mdx \  
5 -storeURL "https://play.google.com/store/apps/details?id=  
SampleAEappPackage"  
6 <!--NeedCopy-->
```

Agregar el archivo MDX

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones**. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX
Apps wrapped with the **MDX Service** to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: Secure Mail

Public App Store
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

Enterprise
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

2. Haga clic en **MDX**. Aparecerá la página **Información de la aplicación MDX**. En el panel **Información de la aplicación**, escriba la información siguiente:

- **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en **Nombre de la aplicación**, en la tabla **Aplicaciones**.
- **Descripción:** Escriba, si quiere, una descripción 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 MDX Toolkit.

- La interfaz de usuario le notifica si la aplicación adjunta requiere la aprobación de Google Play Store administrado. Para aprobar la aplicación sin salir de la consola de Citrix Endpoint Management, haga clic en **Sí**.

App is not approved

App is not approved on the managed Google Play store. You can approve the app now or later. Do you want to approve it now?

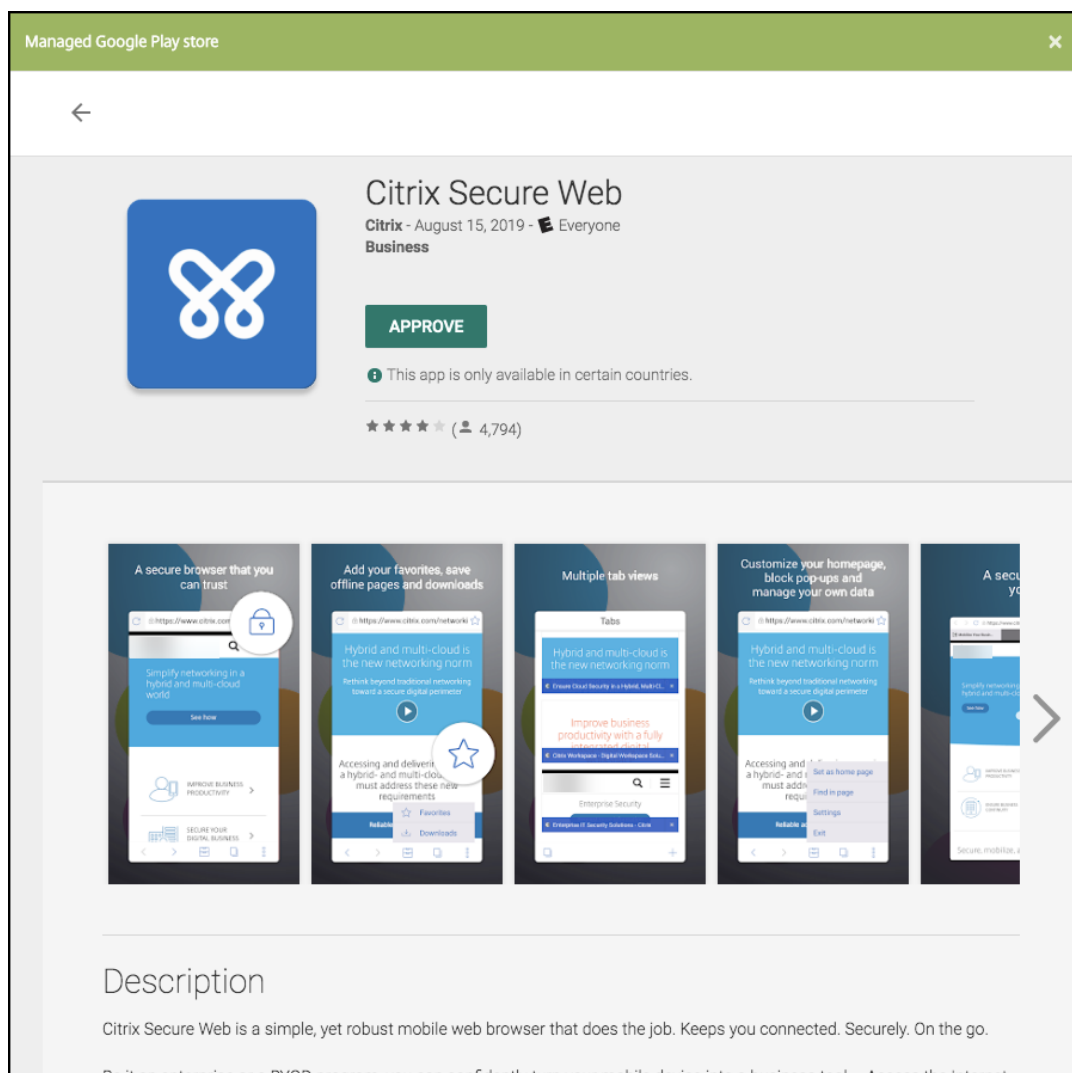
No

Yes

Una vez abierto Google Play Store administrado, siga las instrucciones para aprobar y guardar la aplicación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

437



Al agregarse correctamente la aplicación, aparece la página **Detalles de la aplicación**.

5. Configure estos parámetros:

- **Nombre de archivo:** Escriba el nombre del archivo asociado a la aplicación.
- **Descripción de la aplicación:** Escriba una descripción de la aplicación.
- **Versión de la aplicación:** Si quiere, 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 de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
- **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
- **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.

6. Configure las **directivas MDX**. Las directivas MDX varían según la plataforma. Además, estas directivas incluyen opciones para tales áreas de directiva como autenticación, seguridad de los dispositivos y restricciones a aplicaciones. En la consola, se ofrece información descriptiva sobre cada una de las directivas. Para obtener información sobre las directivas de aplicaciones que están disponibles para cada tipo de plataforma de dispositivos, consulte:

- [Introducción al SDK de MAM](#)
- [Vista general de las directivas de aplicaciones MDX de terceros](#)

7. Configure las reglas de implementación y los parámetros del almacén.

La opción **Implementar para conexiones permanentes** se aplica una vez configurada la clave de implementación en segundo plano para la programación en **Parámetros > Propiedades de servidor**.

La opción permanente:

- No está disponible para dispositivos iOS
- No está disponible para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management a partir de la versión 10.18.19 o una posterior
- No se recomienda para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19

La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Implementar para conexiones permanentes**.

8. Asigne los grupos de entrega que quiera 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 con el SDK de MAM o MDX Toolkit.
2. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones**. Se abrirá la página **Aplicaciones**.

Add App

×

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the **MDX Service** to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: Secure Mail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

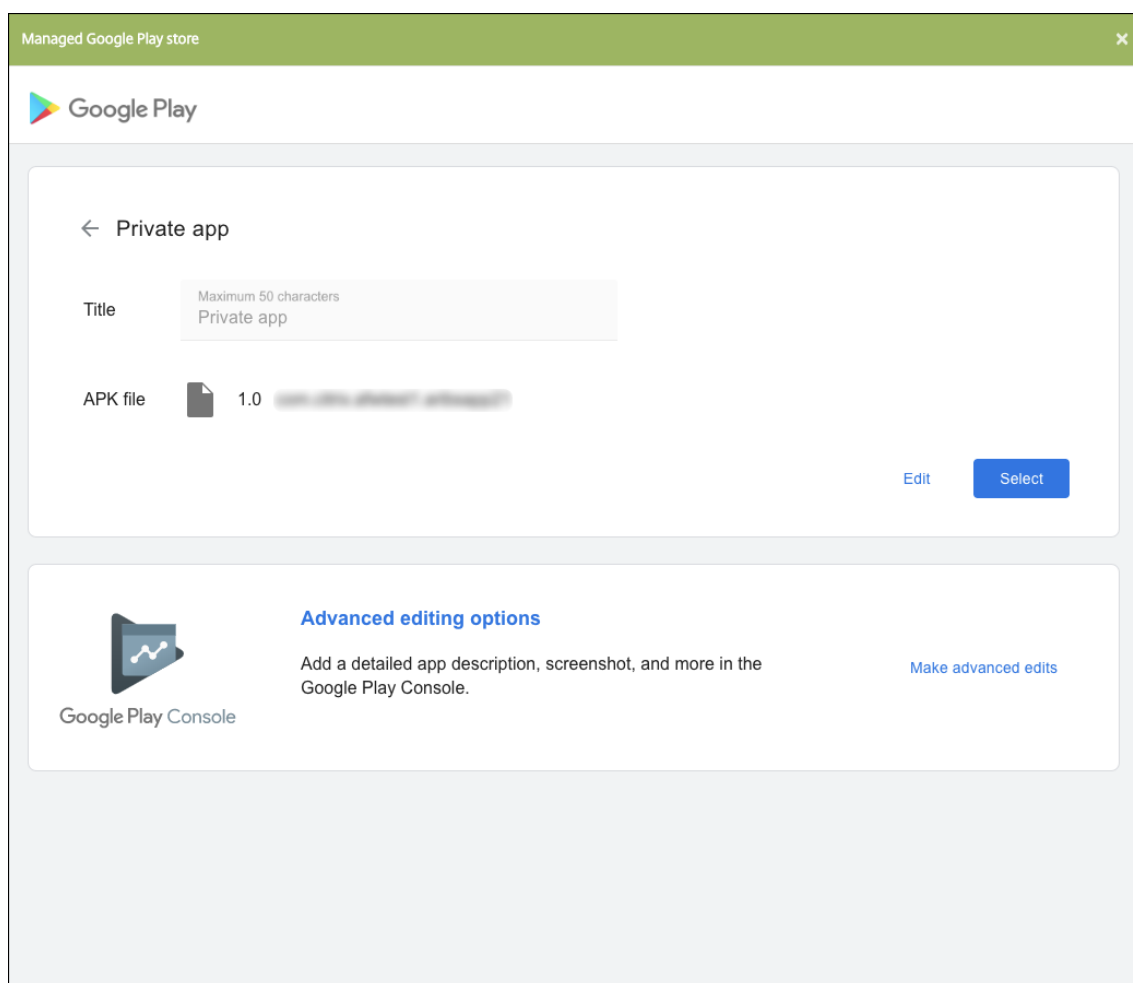
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Haga clic en **Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.
4. Haga clic en **Empresa**. En el panel **Información de la aplicación**, escriba la información siguiente:
 - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en “Nombre de la aplicación”, en la tabla “Aplicaciones”.
 - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
5. Seleccione **Android Enterprise** como plataforma.
6. Haga clic en **Siguiente**. Aparecerá la página **Aplicación de empresa**.
7. Haga clic en **Cargar**.
8. En la página de Google Play Store administrado, seleccione la aplicación que quiera actualizar.
9. En la página de información de la aplicación, haga clic en la opción **Modificar** situada junto al nombre del archivo APK.



10. Vaya al nuevo archivo APK y cárguelo.

11. En la página de Google Play Store administrado, haga clic en **Guardar**.

Android Enterprise heredado para clientes de Google Workspace (anteriormente G Suite)

November 29, 2023

Los clientes de Google Workspace deben usar los parámetros de Android Enterprise heredado para configurar Android Enterprise heredado. Google ha cambiado recientemente el nombre de G Suite a Google Workspace.

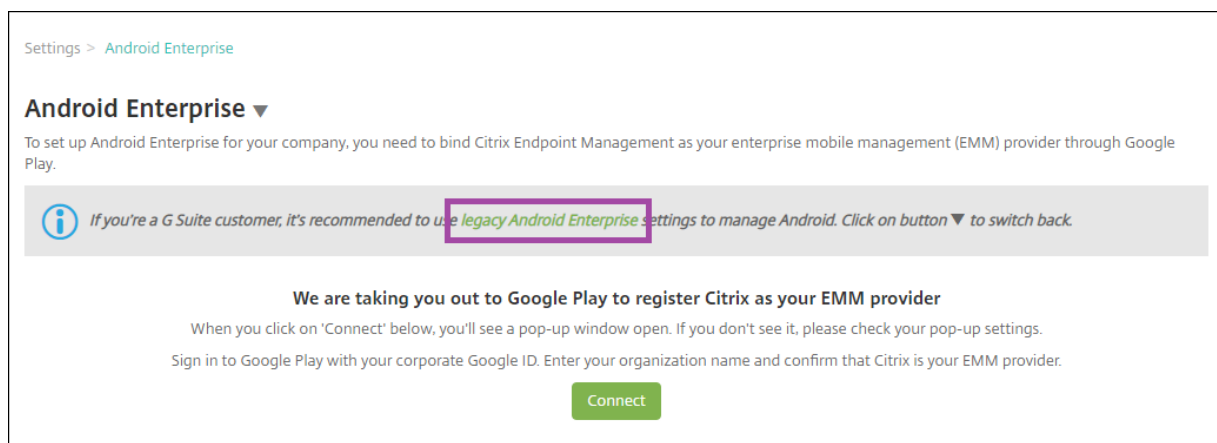
Si su organización ya utiliza Google Workspace para proporcionar a los usuarios acceso a las aplicaciones de Google, puede utilizar Google Workspace para registrar Citrix como EMM. Si su organización utiliza Google Workspace, entonces tiene un ID de empresa existente y cuentas de Google existentes

para los usuarios. Para utilizar Citrix Endpoint Management con Google Workspace, sincronice con su directorio LDAP y recupere la información de la cuenta de Google procedente de Google mediante la API de Google Directory. Dado que este tipo de empresa está vinculado 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 accesible públicamente
- Una cuenta de administrador de Google
- Dispositivos Android que admiten el perfil administrado
- Una cuenta de Google que tenga Google Play instalado
- Un perfil de Work instalado en el dispositivo

Para empezar a configurar Android Enterprise heredado, haga clic en **Legacy Android Enterprise** en la página **Android Enterprise** en los parámetros de Citrix Endpoint Management.





Crear una cuenta de Android Enterprise

Para poder configurar una cuenta de Android Enterprise, antes debe verificar el nombre de dominio en Google.

Si ya ha verificado el nombre de su dominio en Google, puede pasar a 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>.

Aparece la siguiente página, donde puede introducir información sobre el administrador y la empresa.



Bring Android to your office

Sign up to use Android devices at your company.

① About you

Name

First Name

Last Name

Current work email Doesn't have to be an official business email.

e.g. john@mydomain.com

Phone

+1

2. Introduzca la información del usuario administrador.

① About you

Name

Justa ✓

User ✓

Current work email Doesn't have to be an official business email.

justa.user@gmail.com ✓

Phone

+15551234567 ✓

3. Escriba la información de la empresa, además de la información de su cuenta de administrador.

2

About your business

Business name

EXAMPLE CORP

✓

Business domain address

example.com

✓

You'll need to verify that you own this domain.

Number of employees

1 employee

Country/Region

United States

3

Your Google admin account

Why do I need this?

Username

justa.user

✓

@

example.com

Create an account to manage Android for Work

Create a password

8-character minimum; case sensitive

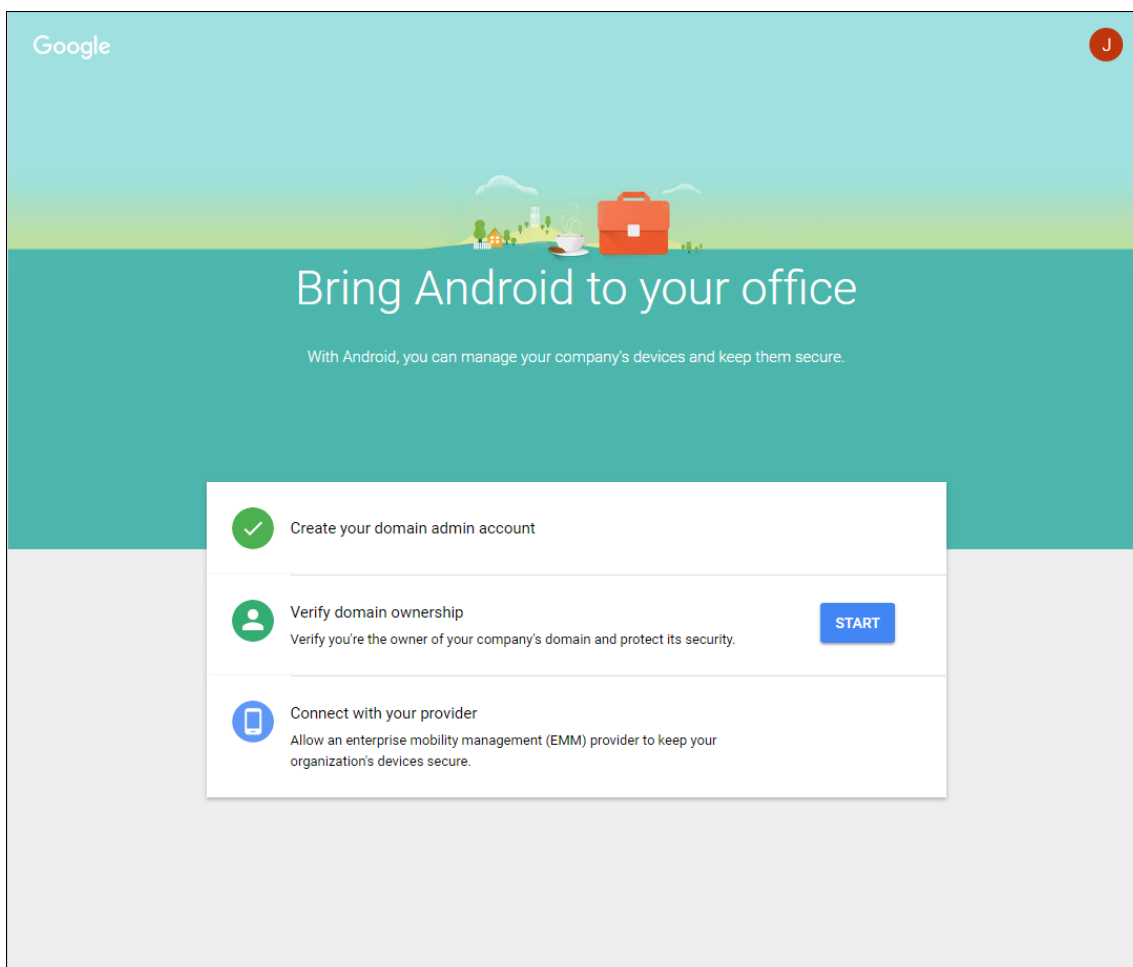
.....

✓

.....

✓

Una vez completado el primer paso, verá la página siguiente.



Verificación de la propiedad del dominio


Permita a Google verificar el dominio de alguna de las siguientes maneras:

- Agregue un registro TXT o CNAME al sitio web de su host de dominio.
- Cargue un archivo HTML en el servidor web del dominio.
- Agregue una etiqueta `<meta>` a la página de inicio. Google recomienda el primer método. Los pasos para comprobar que usted es el propietario del dominio no se describen en este artículo, pero puede encontrar esta información aquí: <https://support.google.com/a/answer/6248925>.

1. Haga clic en **Comenzar** para iniciar la verificación de su dominio.

Verá la página **Verificar propiedad de dominio**. Siga las instrucciones de esta página para verificar su dominio.

2. Haga clic en **Verificar**.



Verify domain ownership


Before you can use Google Apps with domain **example.com**, we need to contact your domain host to verify that you own it. Doing this helps ensure that no one can pose as you on Google Apps and send email from your domain. [Learn more](#)


After your domain is verified, we will set up Google Apps email for your users on **example.com**. This will automatically re-route your emails to Google Apps. [Learn more](#)

We have detected that **example.com** is hosted at **GoDaddy.com**. If you're having trouble, try to [verify your domain here](#).

Note: Before you route email to Google Apps, make sure that you create a user on Google Apps for each person receiving mail at **example.com**.

VERIFY

 Need help? Search the [Help Center](#) or call 844-390-7627 and provide your unique PIN **12345678**





Verify domain ownership


Verification checklist


Follow these steps to help Google verify that you own the domain **example.com**.

[Learn more](#)

 I have successfully logged in.

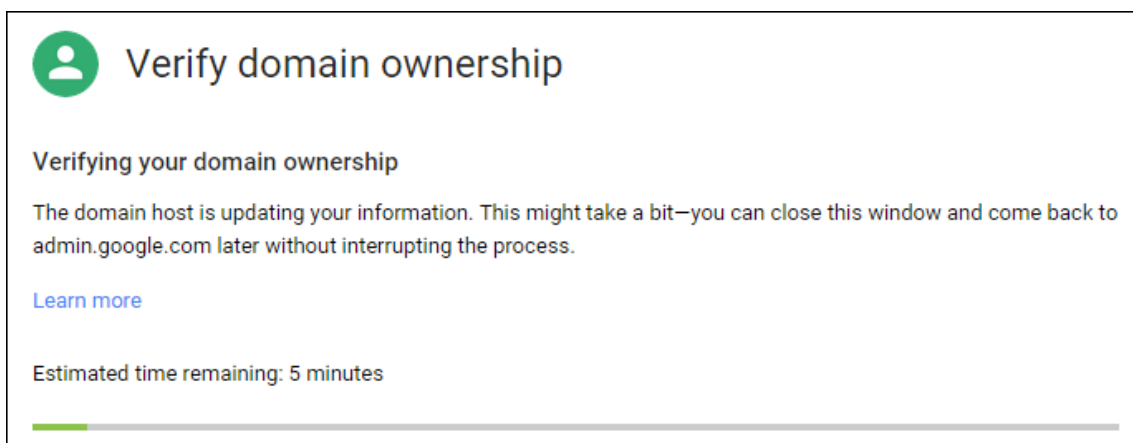
 I have opened the control panel for my domain.

 I have created the CNAME record.

 I have saved the CNAME record.

VERIFY

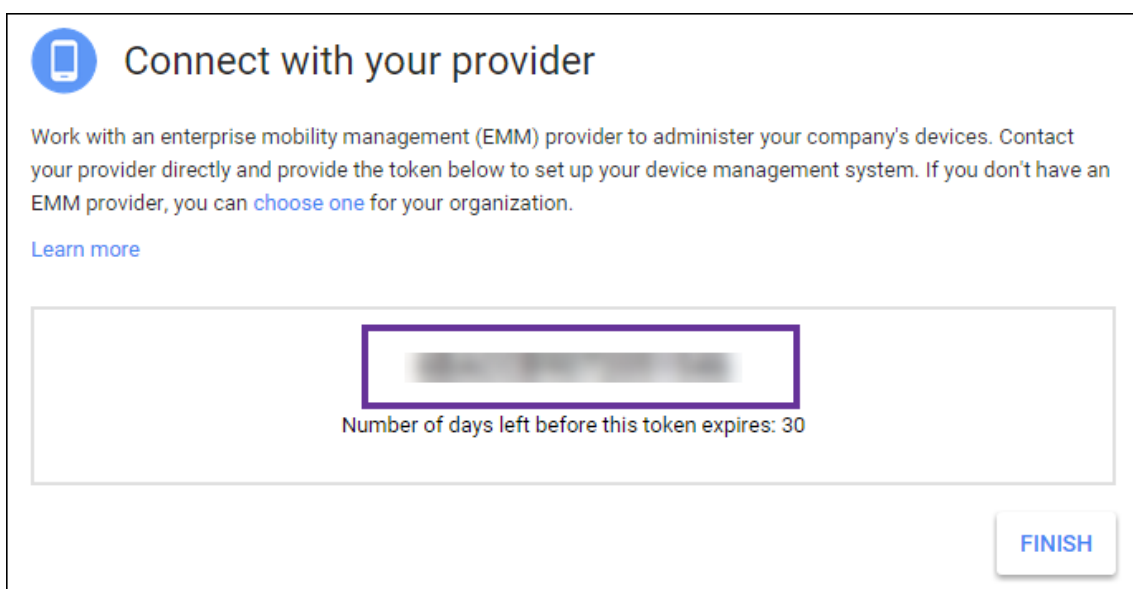
3. Google verifica que usted posee el dominio.



4. Aparecerá la siguiente página tras una verificación correcta. Haga clic en **Continuar**.



5. Google crea un token de vinculación de EMM que usted debe suministrar a Citrix y usarlo para configurar los parámetros de Android Enterprise. Copie y guarde el token, porque lo necesitará más adelante durante el procedimiento de configuración.



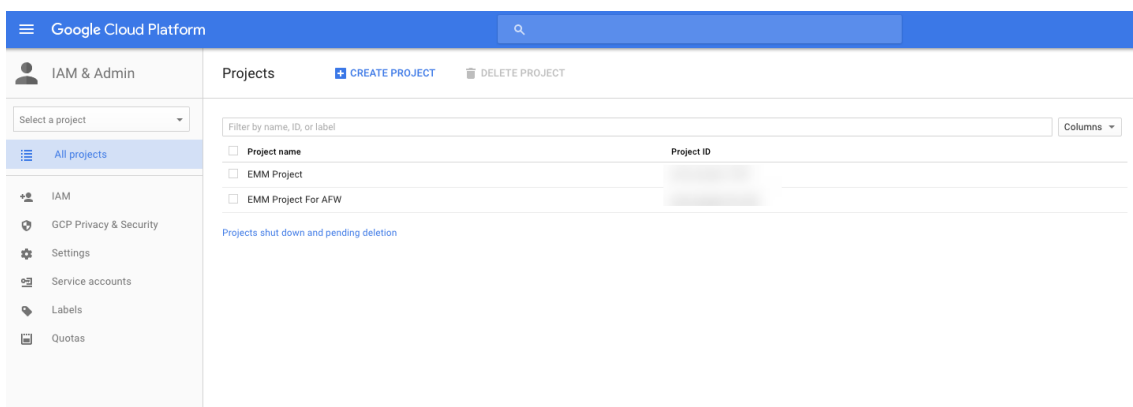
6. Haga clic en **Finalizar** para completar la configuración de Android Enterprise. Aparecerá una página que indicará que el dominio se ha verificado correctamente.

Después de crear una cuenta de servicio de Android Enterprise, puede iniciar sesión en la consola de administración de Google para administrar sus opciones de movilidad.

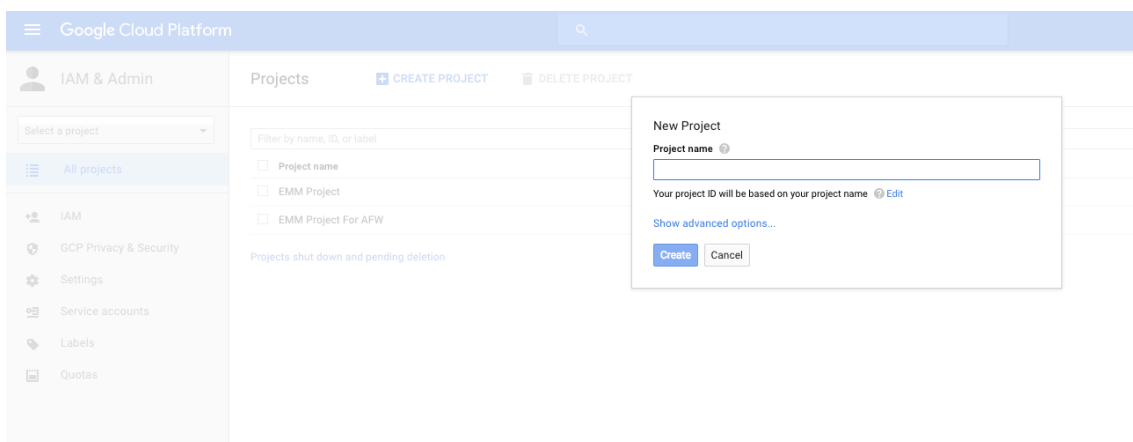
Configuración de una cuenta de servicio de Android Enterprise y descarga de un certificado de Android Enterprise

Para permitir que Citrix Endpoint Management establezca contacto con los servicios de Google Play y Google Directorio, debe crear una cuenta de servicio en 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 está utilizando, vaya a <https://developers.google.com/identity/protocols/OAuth2ServiceAccount>.

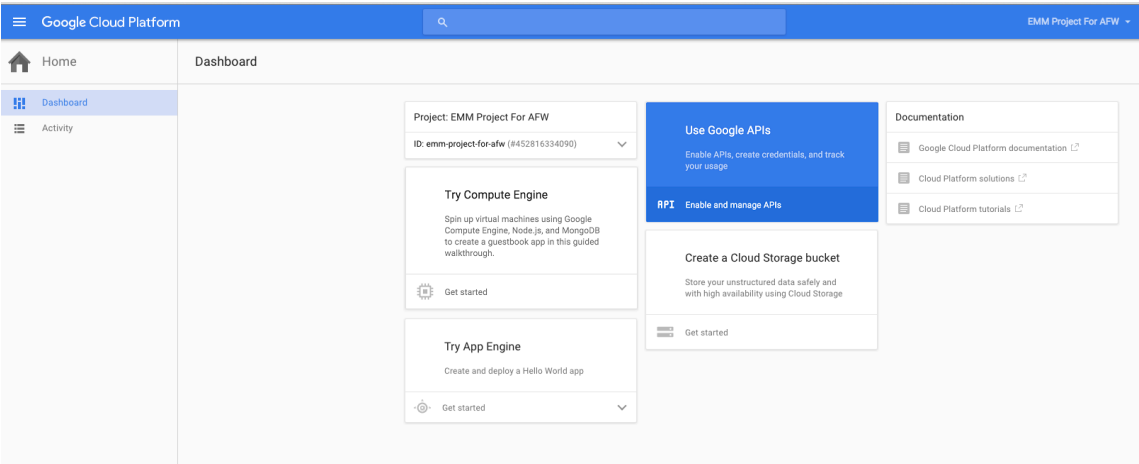
1. En un explorador web, vaya a <https://console.cloud.google.com/project> e inicie sesión con las credenciales de administrador de Google.
2. En la lista **Projects**, haga clic en **Create Project**.



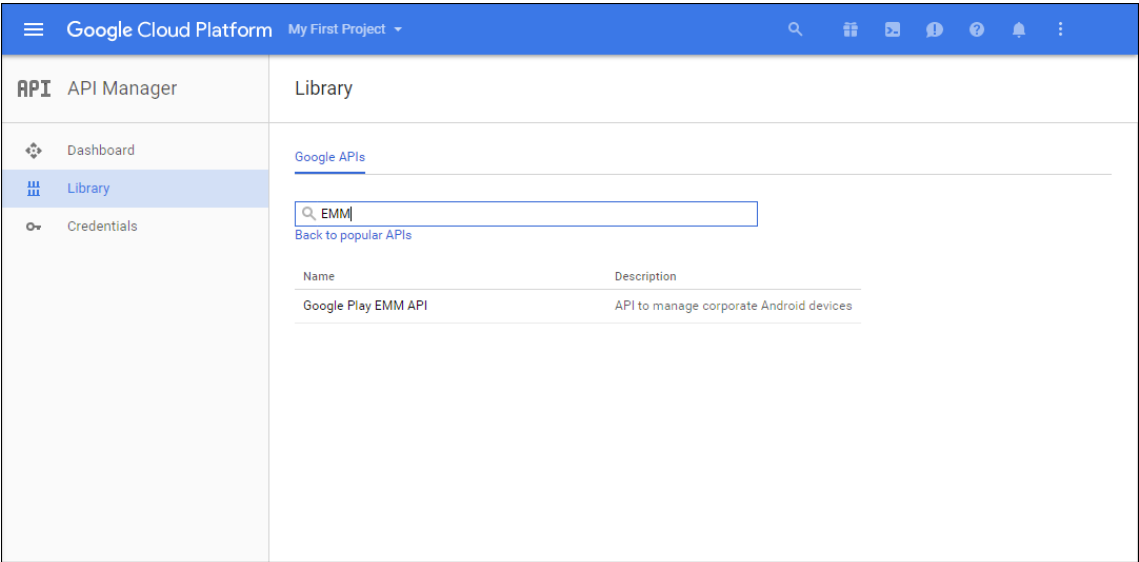
3. En **Project name**, introduzca un nombre para el proyecto.



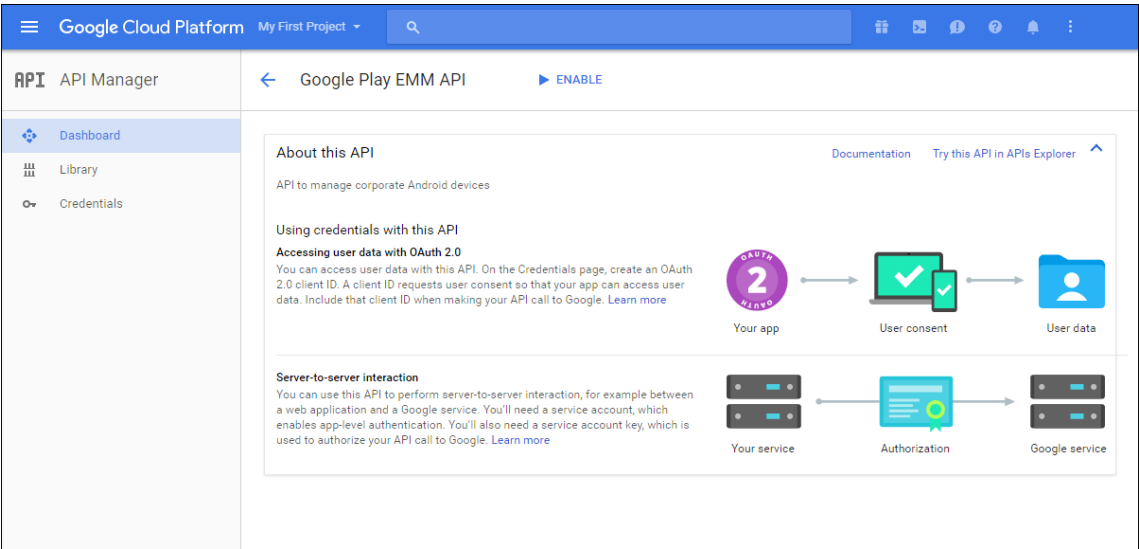
4. En el panel de mandos, haga clic en **Use Google APIs**.



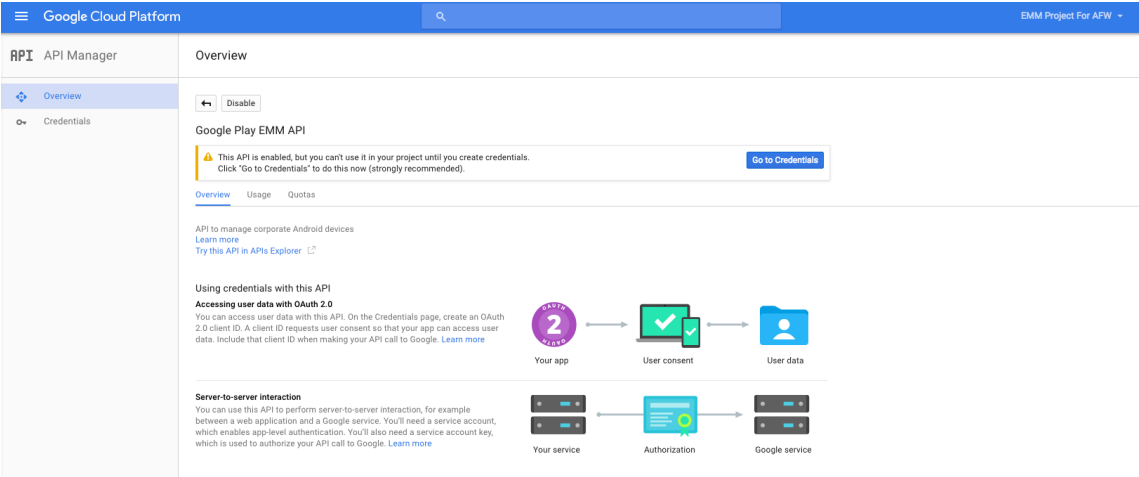
5. Haga clic en **Library** y, en **Search**, escriba **EMM**. A continuación, haga clic en el resultado de la búsqueda.



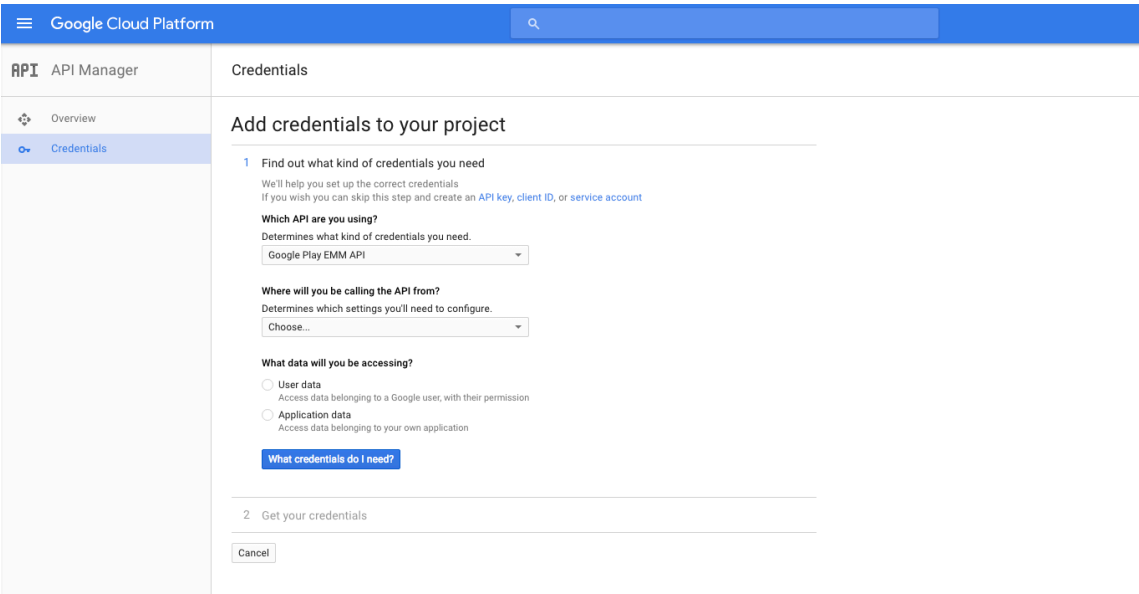
6. En la página **Overview**, haga clic en **Enable**.



7. Junto a **Google Play EMM API**, haga clic en **Go to Credentials**.

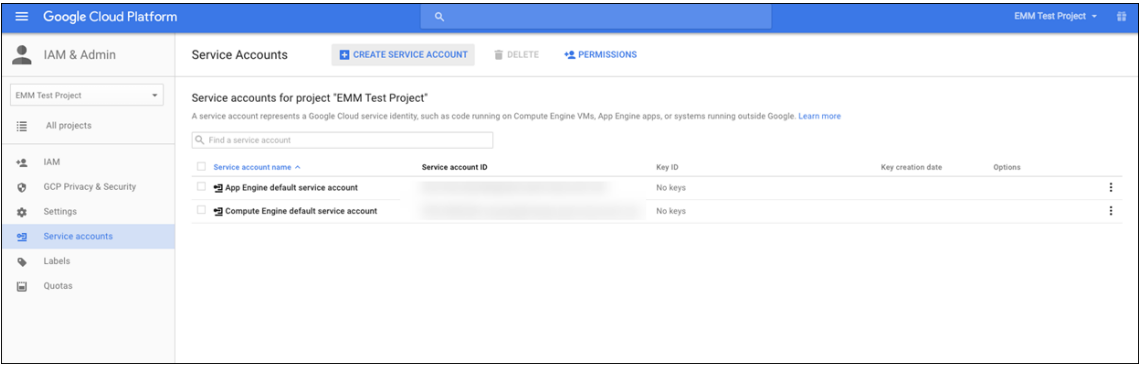


8. En la lista **Add credentials to our project**, en el paso 1, haga clic en **service account**.



The screenshot shows the Google Cloud Platform API Manager interface. The left sidebar has 'API Manager' selected, with 'Overview' and 'Credentials' as sub-options. The main area is titled 'Credentials' and 'Add credentials to your project'. It contains a multi-step wizard. Step 1, 'Find out what kind of credentials you need', includes instructions, a dropdown for 'Which API are you using?' (set to 'Google Play EMM API'), a dropdown for 'Where will you be calling the API from?' (set to 'Choose...'), and radio buttons for 'What data will you be accessing?' (with 'User data' selected). A 'What credentials do I need?' button is at the bottom. Step 2, 'Get your credentials', is partially visible. A 'Cancel' button is at the bottom left.

9. En la página **Service Accounts**, haga clic en **Create Service Account**.



The screenshot shows the Google Cloud Platform IAM & Admin 'Service Accounts' page for the 'EMM Test Project'. The left sidebar has 'IAM & Admin' selected, with 'Service accounts' as a sub-option. The main area has a 'CREATE SERVICE ACCOUNT' button and a table of existing service accounts. The table has columns for 'Service account name', 'Service account ID', 'Key ID', 'Key creation date', and 'Options'. It lists three accounts: 'App Engine default service account' and 'Compute Engine default service account', both with 'No keys'.

Service account name	Service account ID	Key ID	Key creation date	Options
App Engine default service account		No keys		
Compute Engine default service account		No keys		

10. En **Create service account**, establezca un nombre para la cuenta y marque la casilla **Furnish a new private key**. Haga clic en **P12**, marque la casilla **Enable Google Apps Domain-wide Delegation** y haga clic en **Create**.

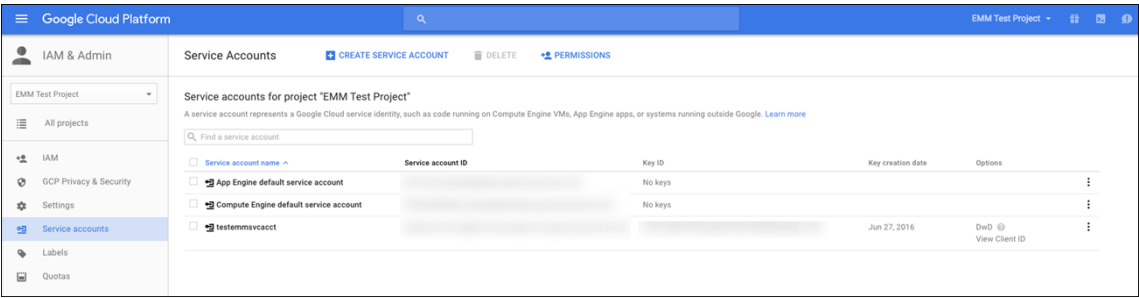
The screenshot shows the 'Create service account' dialog. The 'Service account name' field contains 'testemmsvcacct'. The 'Service account ID' field also contains 'testemmsvcacct'. The 'Furnish a new private key' checkbox is checked, with a note: 'Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.' Under 'Key type', the 'P12' radio button is selected, with a note: 'For backward compatibility with code using the P12 format'. The 'Enable Google Apps Domain-wide Delegation' checkbox is also checked, with a note: 'Grants a client access to all users' data on a Google Apps domain without manual authorization on their part. Below this is a warning box: 'To change settings for Google Apps domain, product name for the OAuth consent screen must be configured. Assign the product name below or configure the OAuth consent screen.' The 'Product name for the consent screen' field contains 'anynamewilldo'. At the bottom are three buttons: 'Create' (highlighted in blue), 'Configure consent screen', and 'Cancel'.

El archivo de certificado (P12) se descargará en su equipo. Guarde el certificado en una ubicación segura.

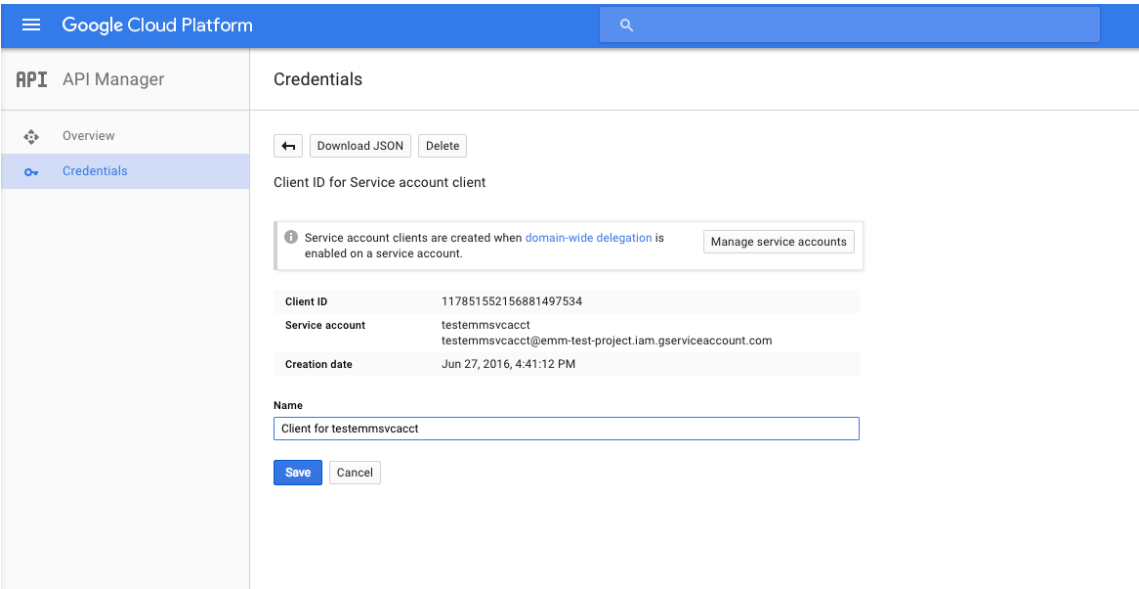
11. En la pantalla de confirmación **Service account created**, haga clic en **Close**.

The screenshot shows the 'Service account created' confirmation dialog. It states: 'The service account "testemmsvcacct" was given editor permission for the project.' It then says: 'The account's private key [redacted] has been saved on your computer. This is the only copy of the key, so store it securely.' Below this, it says: 'This is the private key's password. It will not be shown again. You must present this password to use the private key. Learn more'. The password field contains 'notasecret'. At the bottom is a blue 'Close' button.

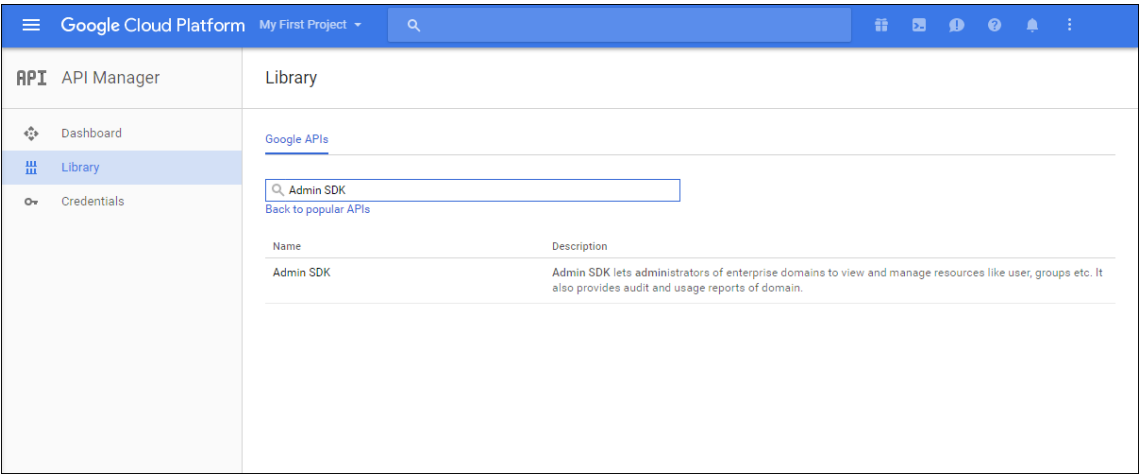
12. En **Permissions**, haga clic en **Service accounts** y, en **Options** para su cuenta de servicio, haga clic en **View Client ID**.



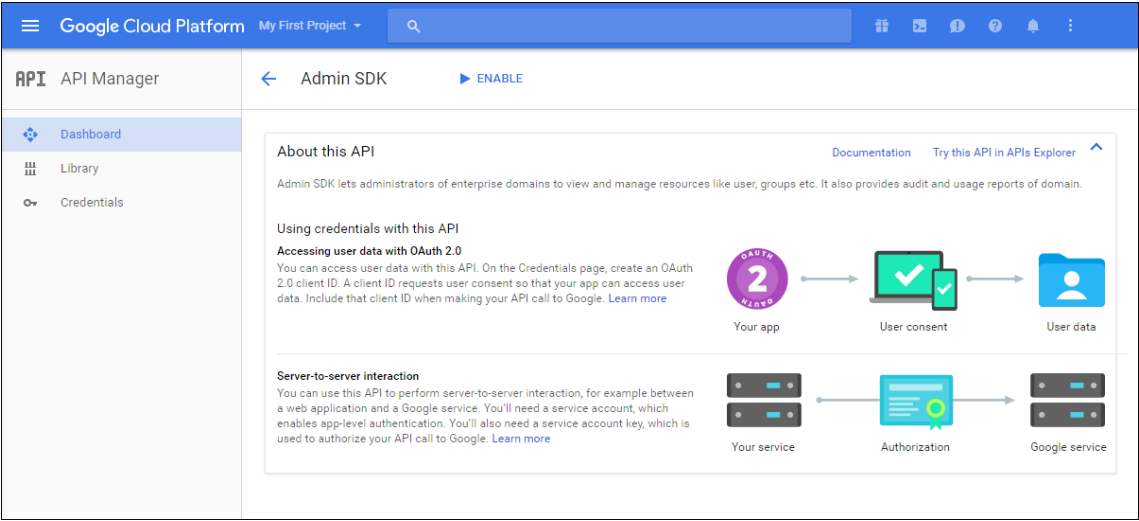
13. Aparecerán los datos requeridos para la autorización de cuentas en la consola de administración de Google. Copie el **ID del cliente** y el **ID de la cuenta de servicio** a una ubicación donde pueda recuperar la información más adelante. Necesita esta información, junto con el nombre de dominio, para enviarla a Citrix para su inclusión en una lista de permitidos.



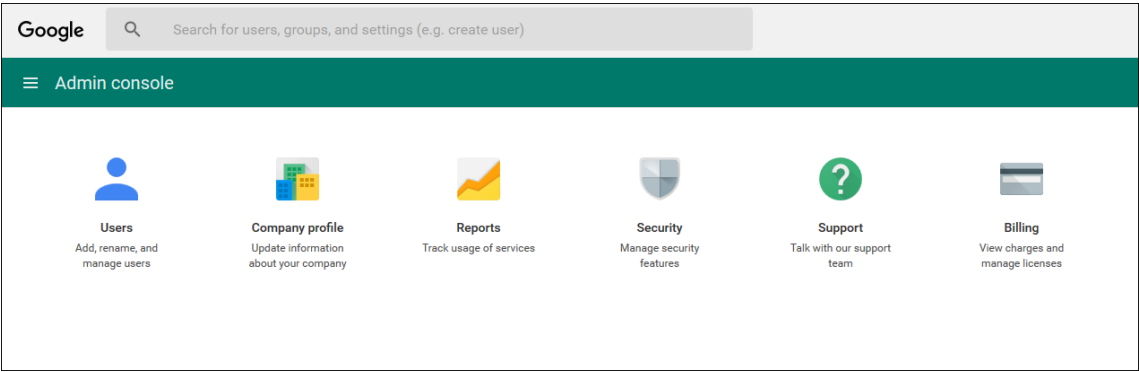
14. En la página **Library**, busque **Admin SDK** y haga clic en el resultado de búsqueda.



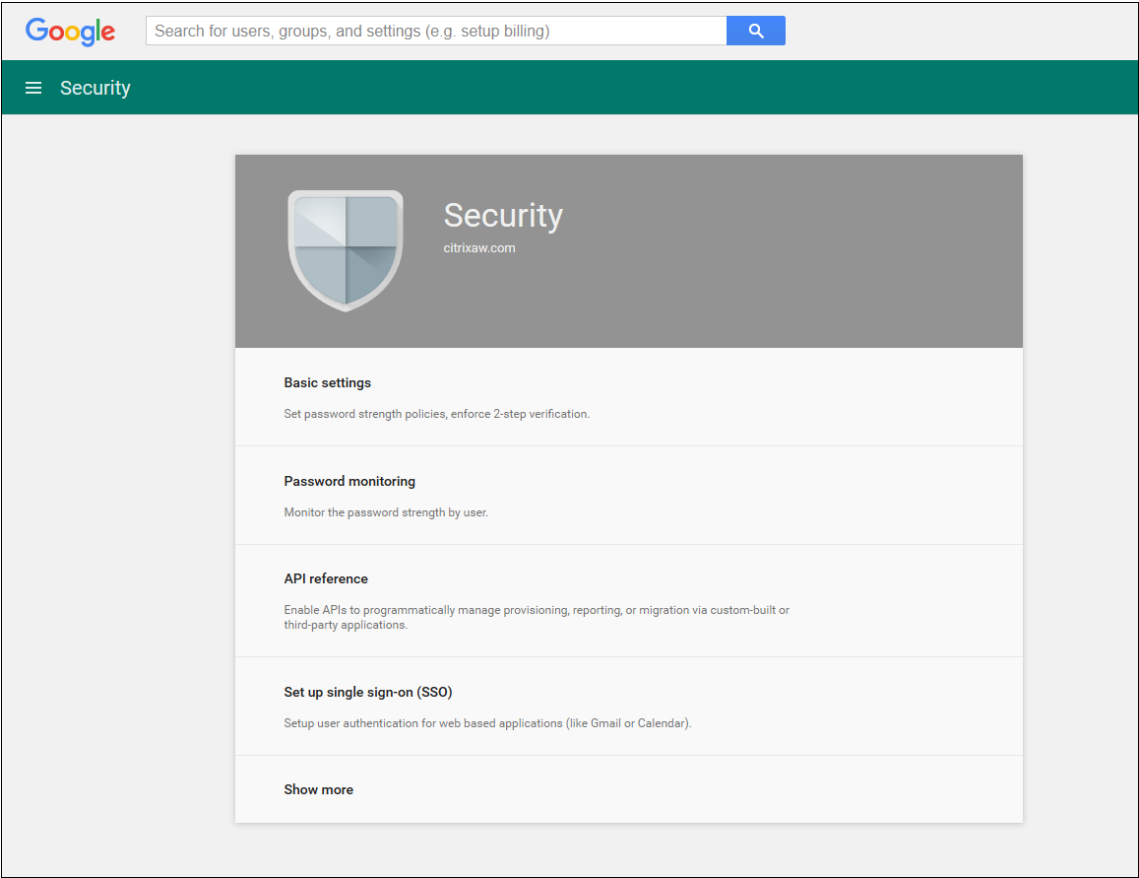
15. En la página **Overview**, haga clic en **Enable**.

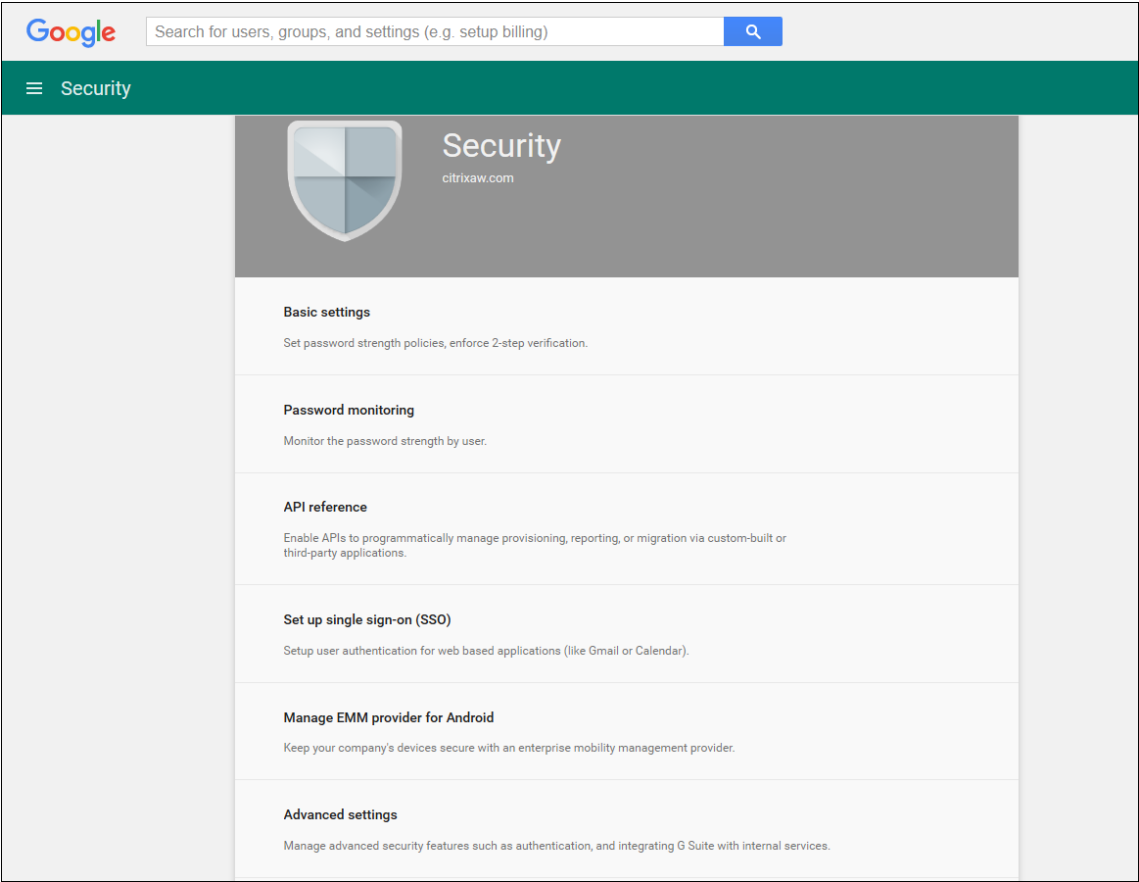


16. Abra la consola de administración de Google para su dominio y haga clic en **Seguridad**.

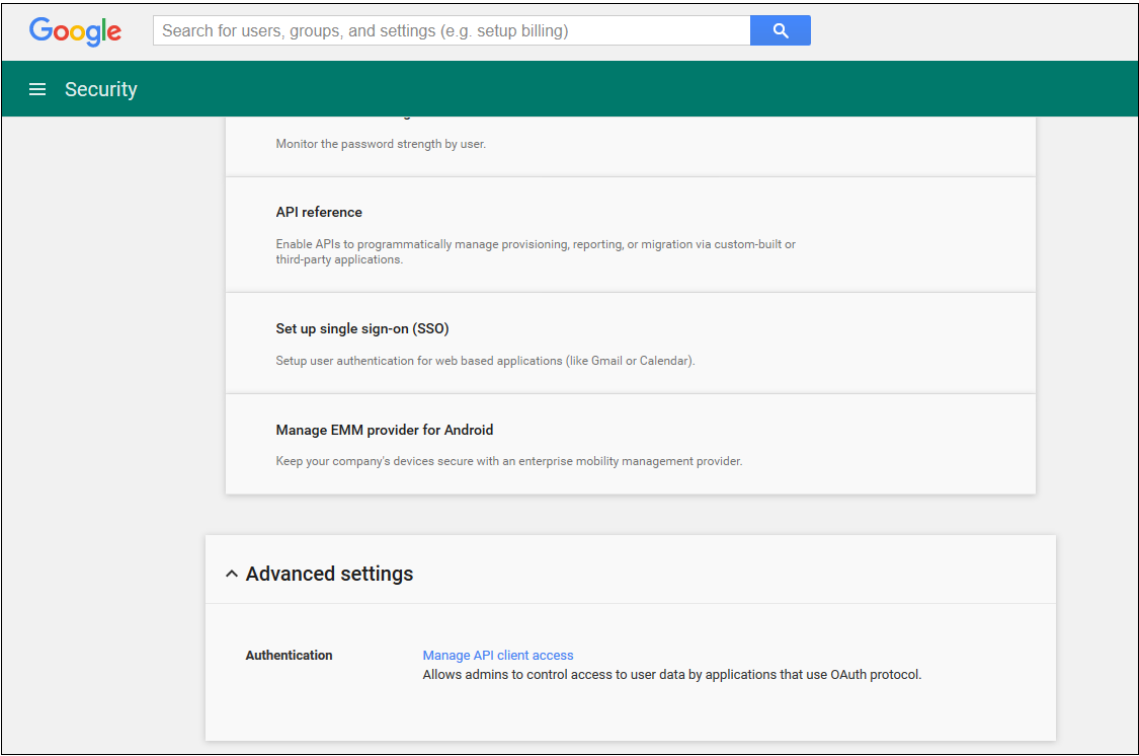


17. En la página **Ajustes**, haga clic en **Mostrar más** y en **Configuración avanzada**.

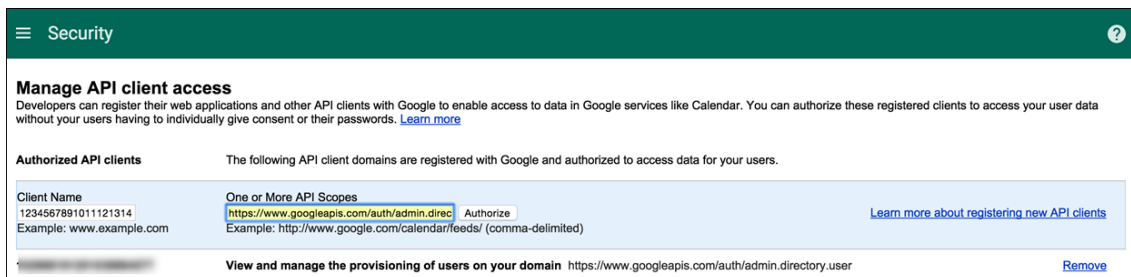




18. Haga clic en **Administrar el acceso de cliente API**.



19. En **Nombre de cliente**, introduzca el ID de cliente que guardó previamente, en **Uno o más ámbitos API**, introduzca `https://www.googleapis.com/auth/admin.directory.user` y haga clic en **Autorizar**.



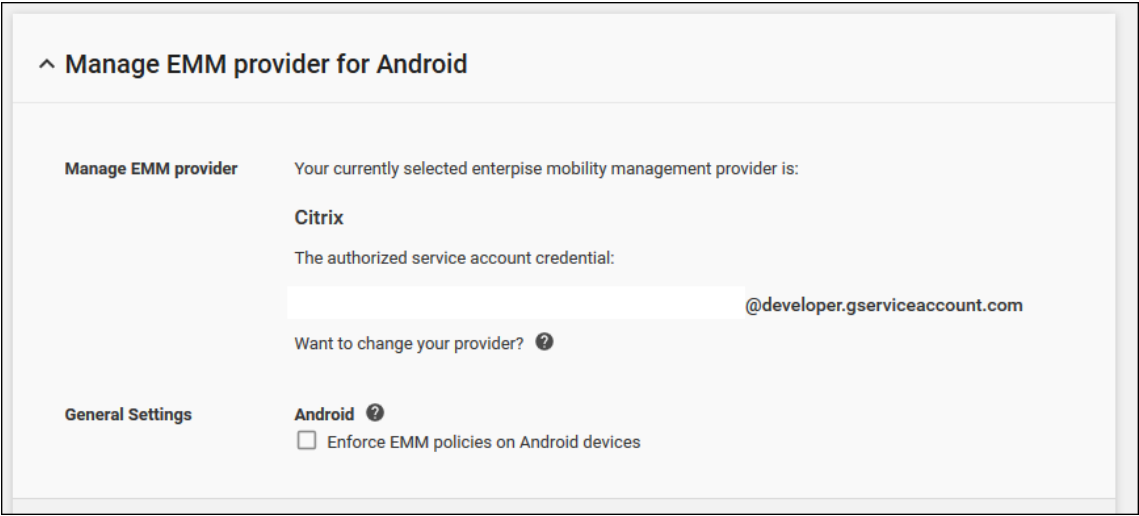
Vincular a EMM

Para poder utilizar Citrix Endpoint Management para administrar los dispositivos Android, debe ponerse en contacto con el servicio de asistencia técnica de Citrix y proporcionarles su nombre de dominio, cuenta de servicio y token de vinculación. Citrix enlaza el token con Citrix Endpoint Management como su proveedor de administración de movilidad empresarial (EMM). Para obtener la información de contacto de la asistencia técnica de Citrix, consulte [Asistencia técnica de Citrix](#).

1. Para confirmar la vinculación, inicie sesión en el portal de administración de Google y haga clic en **Seguridad**.
2. Haga clic en **Administrar proveedor de EMM de Android**.

Verá que su cuenta de Google Android Enterprise aparece vinculada a Citrix como su proveedor EMM.

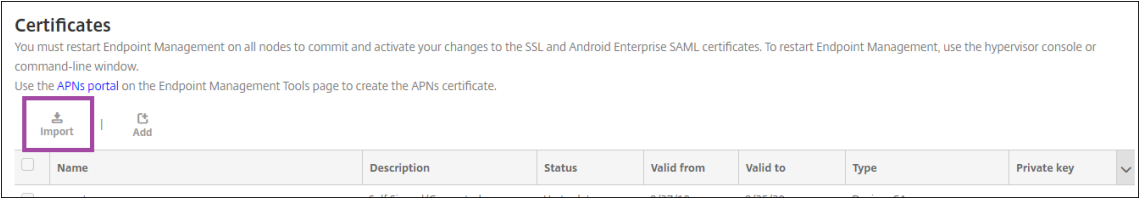
Después de confirmar la vinculación con el token, ya puede empezar a usar la consola de Citrix Endpoint Management para administrar sus dispositivos Android. Importe el certificado P12 generado en el paso 14. Configure los parámetros del servidor de Android Enterprise, habilite el inicio de sesión Single Sign-On basado en SAML y defina al menos una directiva de dispositivo para Android Enterprise.



Importar el certificado P12

Siga estos pasos para importar el certificado P12 de Android Enterprise:

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. A continuación, abra la página **Parámetros** y haga clic en **Certificados**. Aparecerá la página **Certificados**.



2. Haga clic en **Importar**. Aparecerá el cuadro de diálogo **Importar**.

Import ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import Keystore

Keystore type PKCS#12

Use as Server

Keystore file* A 4d... Browse

Password*

Description

Cancel Import

Configure los siguientes parámetros:

- **Importar:** Seleccione **Almacén de claves** en la lista.
- **Tipo de almacén de claves:** Seleccione **PKCS#12** en la lista.
- **Usar como:** Seleccione **Servidor** en la lista.
- **Archivo de almacén de claves:** Haga clic en **Examinar** y vaya al certificado P12.
- **Contraseña:** Escriba la contraseña del certificado. Esta es la contraseña de clave privada que creó al configurar su cuenta de Android Enterprise.
- **Descripción:** Escriba una descripción opcional del certificado.

3. Haga clic en **Importar**.

Configurar los parámetros de servidor de Android Enterprise

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Parámetros**.
2. En **Plataformas**, haga clic en **Android Enterprise**. Aparecerá la página **Android Enterprise**.

Settings > Android Enterprise

Legacy Android Enterprise ▼

Provide Android Enterprise configuration parameters.

Domain Name * ?

Domain Admin Account * ?

Service Account ID * ?

Client ID * ?

Enable Android Enterprise ☐ NO

Cancel Save

Configure estos parámetros y haga clic en **Guardar**.

- **Nombre de dominio:** Introduzca el nombre del dominio de Android Enterprise. Por ejemplo: dominio.com
- **Cuenta de administrador de dominio:** Introduzca el nombre de usuario del administrador del dominio; por ejemplo, la cuenta de correo electrónico utilizada en el portal Google Developer Portal.
- **ID de cuenta de servicio:** Introduzca el ID de la cuenta de servicio. Por ejemplo, el correo electrónico asociado a la cuenta de servicio de Google (`serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com`).
- **ID de cliente:** Escriba el ID numérico del cliente correspondiente a su cuenta de servicio de Google.
- **Habilitar Android Enterprise:** Seleccione para habilitar o inhabilitar Android Enterprise.

Habilitar Single Sign-On basado en SAML

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. Haga clic en **Certificados**. Aparecerá la página **Certificados**.

Settings > Certificates

Certificates

You must restart Endpoint Management on all nodes to commit and activate your changes to the SSL and Android Enterprise SAML certificates. To restart Endpoint Management, use the hypervisor console or command-line window.

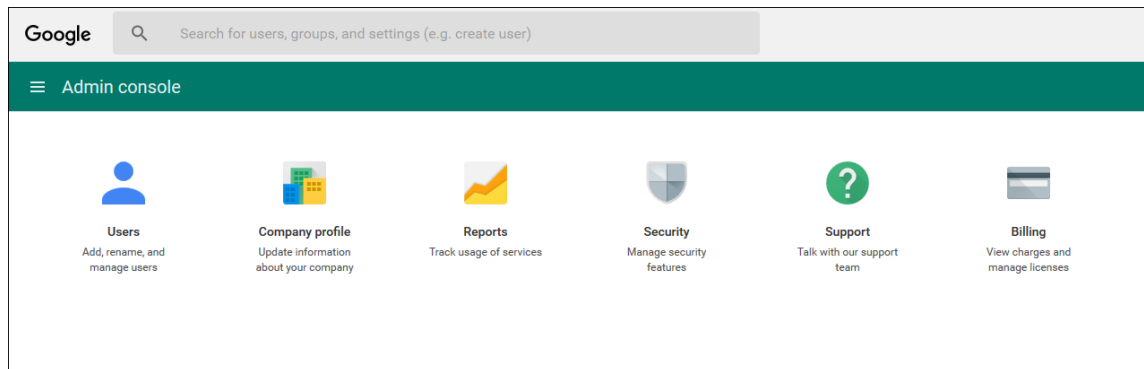
Use the [APNs portal](#) on the Endpoint Management Tools page to create the APNs certificate.

Import | Add | Detail | **Export**

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key
<input checked="" type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	8/27/18	8/25/38	Devices CA	

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 Google Admin con las credenciales de administrador de Android Enterprise. Para acceder al portal, consulte [portal Google Admin](#).
6. Haga clic en **Seguridad**.



7. En **Seguridad**, haga clic en **Configurar inicio de sesión único (SSO)** y configure los parámetros siguientes:

^ Set up single sign-on (SSO)

SAML-based Single Sign-On allows you to authenticate accounts for web based applications (like Gmail or Calendar). With SSO, users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop applications (or POP access to Gmail), users must sign in directly with the username and password set up via the Admin console. ?

☒ Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL	<input type="text" value="https://example.com/aw/saml/signin"/>
	URL for signing in to your system and Google Apps
Sign-out page URL	<input type="text" value="https://example.com/aw/saml/signout"/>
	URL for redirecting users to when they sign out
Change password URL	<input type="text" value="https://example.com/aw/saml/changepassword"/>
	URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled
Verification certificate	<input type="button" value="CHOOSE FILE"/> <input type="button" value="UPLOAD"/>
	The certificate file must contain the public key for Google to verify sign-in requests. ?
<input type="checkbox"/> Use a domain specific issuer ?	
Network masks	<input type="text"/>
	Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

DISCARD CHANGES [SAVE CHANGES](#)

- **URL de la página de inicio de sesión:** Introduzca la URL para que los usuarios inicien sesiones en el sistema y Google Apps. Por ejemplo: <https://<Xenmobile-FQDN>/aw/saml/signin>.
- **URL de la página de cierre de sesión:** Introduzca la URL a la que se redirige a los usuarios cuando cierran la sesión. Por ejemplo: <https://<Xenmobile-FQDN>/aw/saml/signout>.
- **Cambiar URL de contraseña:** Introduzca la URL para permitir que los usuarios cambien su contraseña en el sistema. Por ejemplo: <https://<Xenmobile-FQDN>/aw/saml/changepassword>. Si se define este campo, los usuarios verán esta solicitud incluso cuando SSO no esté disponible.
- **Certificado de verificación:** Haga clic en **ELEGIR ARCHIVO** y busque el certificado SAML exportado desde Citrix Endpoint Management.

8. Haga clic en **Guardar cambios**.

Configurar una directiva de dispositivo para Android Enterprise

Configure una directiva de códigos de acceso para requerir que los usuarios definan un código de acceso en sus dispositivos la primera vez que los inscriban.

Device Policies Apps Media Actions ShareFile Enrollment Profiles Delivery Groups

Passcode Policy ×

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

1 Policy Info

2 Platforms Clear All

- ☒ iOS
- ☒ macOS
- ☒ Android
- ☒ Samsung KNOX
- ☒ **Android Enterprise**
- ☒ Windows Phone
- ☒ Windows Desktop/Tablet

3 Assignment

Device passcode required ON

Passcode requirements for device passcode

Minimum length 6

Biometric recognition OFF

Required characters No restriction

Advanced rules OFF A 3.0+

Passcode security for device passcode

Maximum failed sign-on attempts Not defined ⓘ

Lock device after (minutes of inactivity) (0-999) None

Passcode expiration in days (1-730) 0

Previous passwords saved (0-50) 0 ⓘ

Work profile security challenge required OFF A 7.0+

Back Next >

Estos son los pasos básicos para configurar una directiva de dispositivo:

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Directivas de dispositivo**.
2. Haga clic en **Agregar** y seleccione la directiva que quiere agregar en el cuadro de diálogo **Agregar nueva directiva**. Para este ejemplo, haga clic en **Código de acceso**.
3. Complete la página **Información de directiva**.
4. Haga clic en **Android Enterprise** y defina las configuraciones de la directiva.
5. Asigne la directiva a un grupo de entrega.

Configurar parámetros de cuenta para Android Enterprise

En Citrix Endpoint Management, antes de empezar a administrar aplicaciones y directivas Android en los dispositivos, debe configurar la información de la cuenta y del dominio de Android Enterprise.

Primero, debe completar las tareas de configuración de Android Enterprise en Google para definir un administrador de dominio y obtener un ID de cuenta de servicio, así como un token de vinculación.

1. En la consola web de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En **Plataformas**, haga clic en **Android Enterprise**. Aparecerá la página de configuración **Android Enterprise**.

The screenshot shows the 'Legacy Android Enterprise' configuration page. At the top, it says 'Settings > Android Enterprise'. Below that is the title 'Legacy Android Enterprise' with a dropdown arrow. A subtitle reads 'Provide Android Enterprise configuration parameters.' There are four input fields, each with a red asterisk and a help icon: 'Domain Name', 'Domain Admin Account', 'Service Account ID', and 'Client ID'. Below these is a toggle switch for 'Enable Android Enterprise' currently set to 'NO'. At the bottom right are 'Cancel' and 'Save' buttons.

1. En la página **Android Enterprise**, configure los siguientes parámetros:
 - **Nombre de dominio:** Introduzca el nombre de dominio.
 - **Cuenta de administrador de dominio:** Escriba el nombre de usuario del administrador de dominio.
 - **ID de cuenta de servicio:** Escriba el ID de la cuenta de servicio de Google.
 - **ID de cliente:** Escriba el ID del cliente correspondiente a su cuenta de servicio de Google.
 - **Habilitar Android Enterprise:** Seleccione si habilitar o no Android Enterprise.
2. Haga clic en **Guardar**.

Configurar el acceso de socio de Google Workspace para Citrix Endpoint Management

Algunas funciones de Citrix Endpoint Management que ofrece Chrome usan las API de socios de Google para la comunicación entre Citrix Endpoint Management y el dominio de Google Workspace. Por ejemplo, Citrix Endpoint Management requiere las API para las directivas de dispositivo que administran las funciones de Chrome (como el modo incógnito y el modo invitado).

Para habilitar las API de socios, configure su dominio de Google Workspace en la consola de Citrix Endpoint Management y, a continuación, configure su cuenta de Google Workspace.

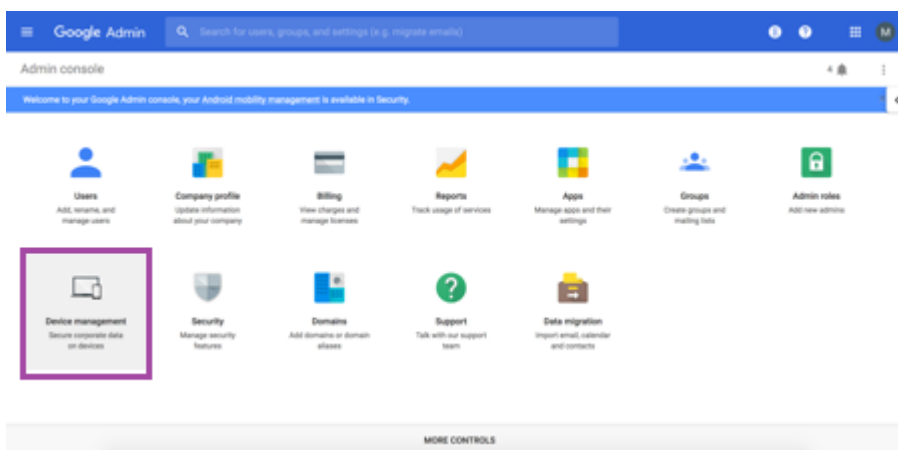
Configurar el dominio de Google Workspace en Citrix Endpoint Management

Para permitir que Citrix Endpoint Management se comunice con las API en su dominio de Google Workspace, vaya a **Parámetros > Configuración de Google Chrome** y defina estos parámetros.

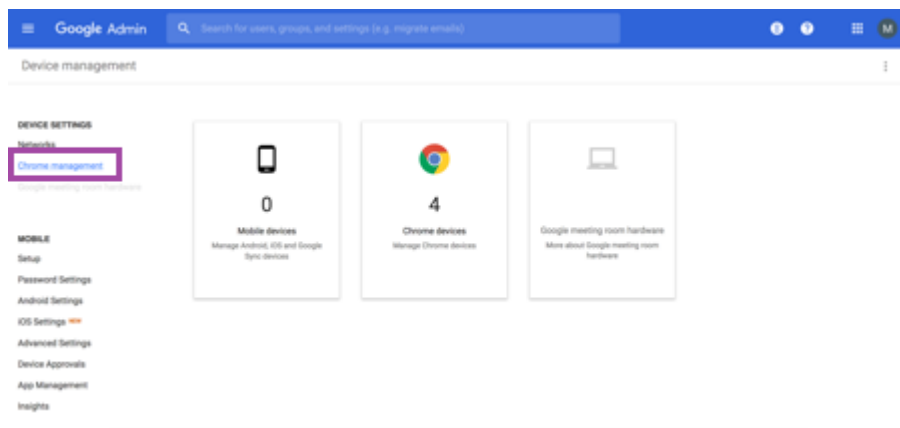
- **Dominio de Google Workspace:** El dominio de Google Workspace que aloja las API que necesita Citrix Endpoint Management.
- **Cuenta de administrador de Google Workspace:** La cuenta de administrador del dominio de Google Workspace.
- **ID de cliente de Google Workspace:** El ID de cliente para Citrix. 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 la cuenta, rellenado desde su cuenta empresarial de Google.

Habilitar el acceso de socios para dispositivos y usuarios en su dominio de Google Workspace

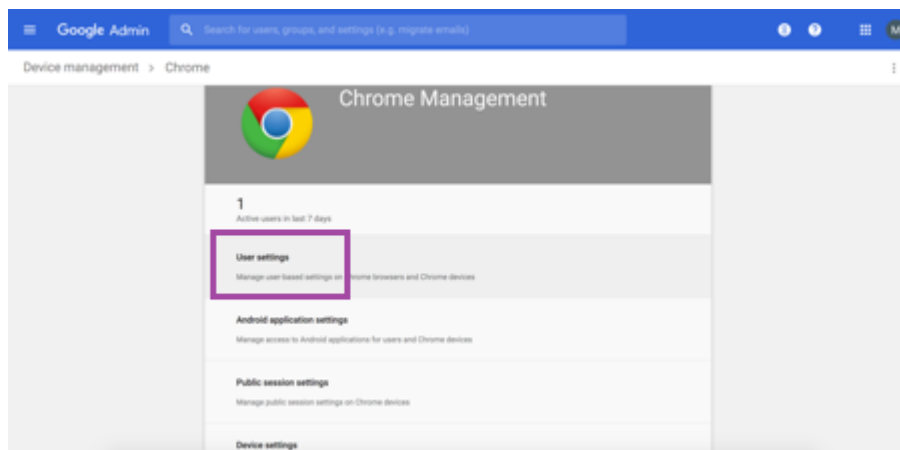
1. Inicie sesión en la Consola de administración de Google: <https://admin.google.com>.
2. Haga clic en **Administración de dispositivos**.



3. Haga clic en **Administración de Chrome**.



4. Haga clic en **Configuración de usuario**.



5. Busque **Administración de Chrome - Acceso de partners**.

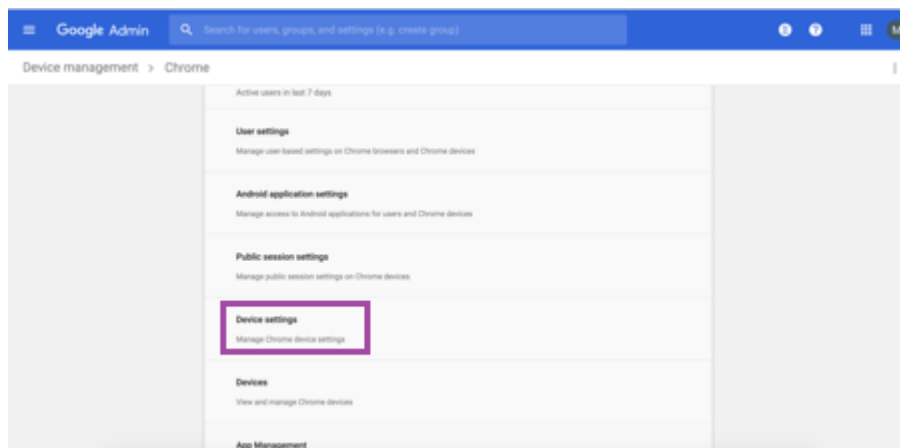


6. Marque la casilla **Habilitar Administración de Chrome - Acceso de partners**.

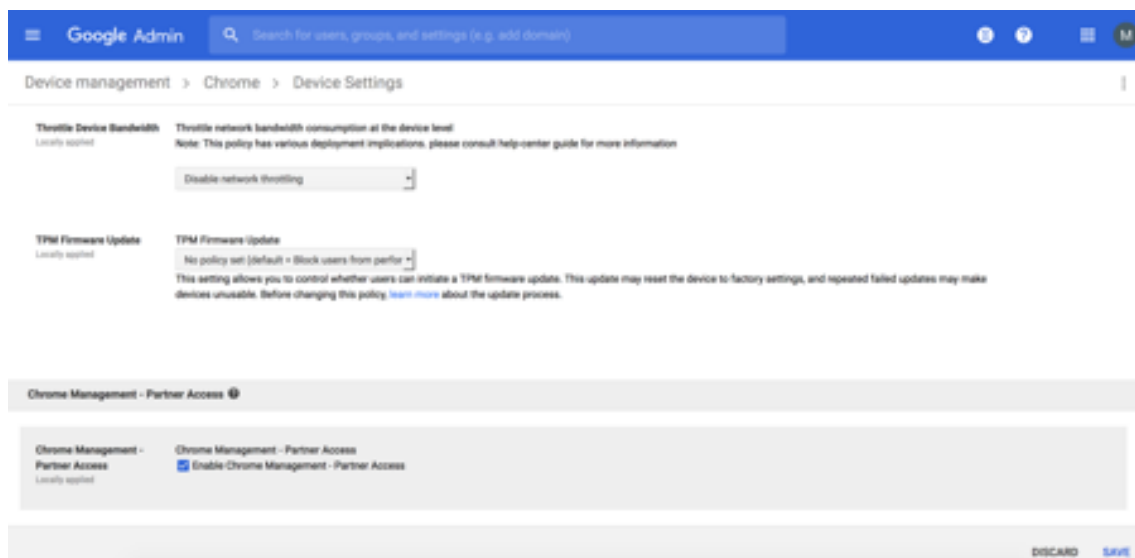
7. Acepte el indicador de que comprende y quiere habilitar el acceso de socios. Haga clic en

Guardar.

8. En la página de administración de Chrome, haga clic en **Configuración del dispositivo**.



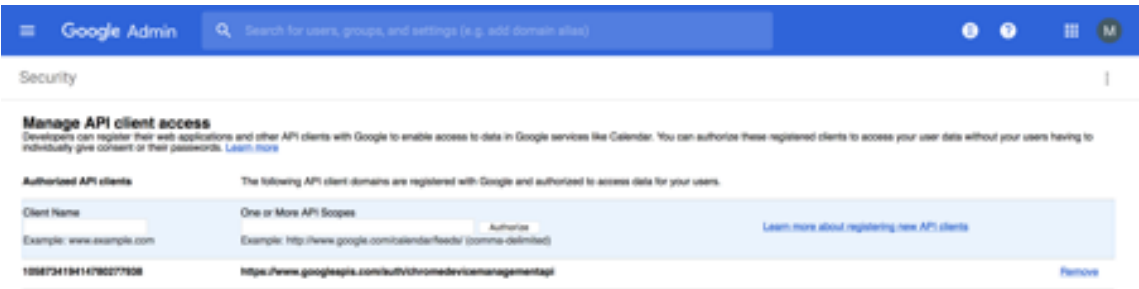
9. Busque **Administración de Chrome - Acceso de partners**.



10. Marque la casilla **Habilitar Administración de Chrome - Acceso de partners**.
11. Acepte el indicador de que comprende y quiere habilitar el acceso de socios. Haga clic en **Guardar**.
12. Vaya a la página **Seguridad** y haga clic en **Configuración avanzada**.



13. Haga clic en **Administrar el acceso de cliente 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 el acceso de cliente API** y pegue el valor copiado en el campo **Nombre de cliente**.
15. En **Uno o más ámbitos API**, agregue la URL: <https://www.googleapis.com/auth/chromedevicemanagementapi>



16. Haga clic en **Autorizar**.
Aparece el mensaje de configuración guardada.

Inscribir dispositivos Android Enterprise

Si el proceso de inscripción de dispositivos requiere que los usuarios introduzcan un ID o un nombre de usuario, el formato aceptado depende de cómo esté configurado el servidor de Citrix Endpoint Management para buscar usuarios (por nombre principal de usuario [UPN] o por nombre de cuenta SAM).

Si el servidor de Citrix Endpoint Management está configurado para buscar usuarios por nombre UPN, los usuarios deben introducir un nombre UPN en el formato:

- *nombre de usuario@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:

- *nombre de usuario@dominio*
- *dominio\nombre de usuario*

Para determinar para qué tipo de nombre de usuario está configurado su servidor de Citrix Endpoint Management:

1. En la consola del servidor de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. Haga clic en **LDAP** para ver la configuración de la conexión LDAP.
3. En la parte inferior de la página, verá el campo **Buscar usuarios por**:
 - Si está establecido en **userPrincipalName**, el servidor de Citrix Endpoint Management está configurado para buscar usuarios por nombre UPN.
 - Si está establecido en **sAMAccountName**, el servidor de Citrix Endpoint Management está configurado para buscar usuarios por cuenta SAM.

Desinscribir una empresa de Android Enterprise

Puede desinscribir una empresa de Android Enterprise mediante la consola del servidor de Citrix Endpoint Management y las herramientas de Citrix Endpoint Management Tools.

Cuando realiza esta tarea, el servidor de Citrix Endpoint Management abre una ventana emergente para Citrix Endpoint Management Tools. Antes de comenzar, asegúrese de que el servidor de Citrix Endpoint Management tenga permiso para abrir ventanas emergentes en el explorador web que esté mediante. Algunos exploradores web, como Google Chrome, requieren que se inhabilite el bloqueo de ventanas emergentes y se agregue la dirección del sitio de Citrix Endpoint Management a la lista de permitidos del bloqueo de ventanas emergentes.

Advertencia:

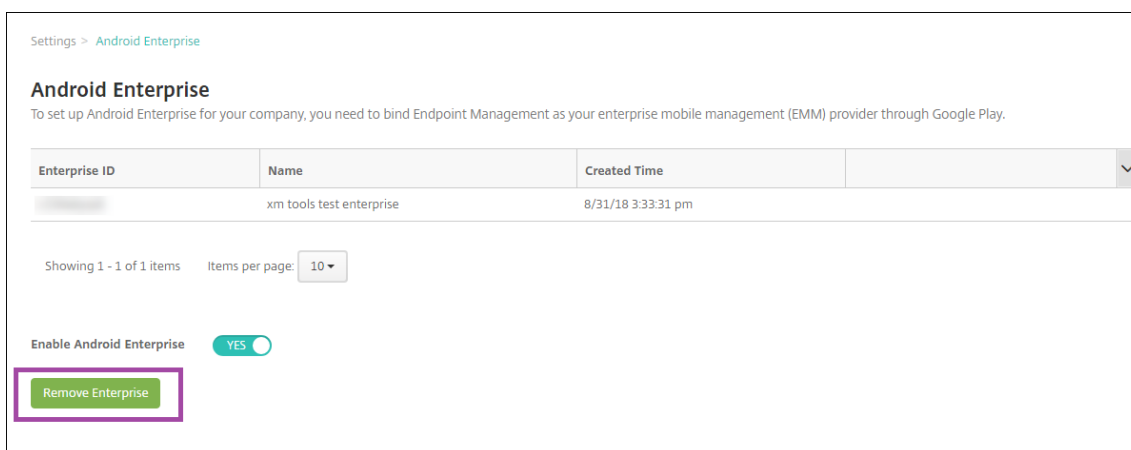
Una vez que se haya desinscrito una empresa, las aplicaciones Android Enterprise en dispositivos ya inscritos a través de ella se restablecen a sus estados predeterminados. Google ya no administrará los dispositivos. Volver a inscribirlos en una empresa de Android Enterprise podría requerir una configuración adicional para restaurar la funcionalidad anterior.

Después de que la empresa Android Enterprise se ha desinscrito:

- En los dispositivos y los usuarios inscritos a través de la empresa, las aplicaciones de Android Enterprise se restablecen a sus estados predeterminados. Las directivas Permisos de aplicación y Configuraciones administradas que se hayan aplicado previamente ya no tienen efecto.
- Citrix Endpoint Management administra los dispositivos inscritos a través de la empresa, pero se consideran no administrados desde el punto de vista de Google. No se pueden agregar nuevas aplicaciones Android Enterprise. No se pueden aplicar las directivas Permisos de aplicación ni Configuraciones administradas. Sin embargo, aún se pueden aplicar otras directivas, tales 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.

Para desinscribir una empresa de Android Enterprise

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En la página **Parámetros**, haga clic en **Android Enterprise**.
3. Haga clic en **Quitar empresa**.



4. Especifique una contraseña. La necesitará en el próximo paso para completar la desinscripción. Haga clic en **Desinscribir**.

Settings > Android Enterprise

Android Enterprise

To set up Android Enterprise for your company, you need to bind Endpoint Management as your enterprise mobile management (EMM) provider through Google Play.

Enterprise ID	Name	Created Time	
	xm tools test enterprise	8/31/18 3:33:31 pm	▼

Showing 1 - 1 of 1 items Items per page: 10 ▼

Enable Android Enterprise ☒

Specify a password then press Unenroll to initiate the process to remove the enterprise. You will need to provide this password in the next step. Please disable any popup blockers as this step requires opening Endpoint Management Tools in a new tab.

New password: *

Confirm password: *

5. Cuando se abra la página de Citrix Endpoint Management Tools, introduzca la contraseña que creó en el paso anterior.

⚠ Warning: After this enterprise is unenrolled, Android Enterprise apps on devices enrolled in it are reset to their default states. The devices will no longer be managed by Google. Re-enrolling them in an Android Enterprise enterprise may not restore previous functionality without further configuration.

1

Enter password and press Next to continue unenrollment process.

Password must be least 4 characters.

2

Enter the email address of any administrator for the enterprise and press Unenroll to complete unenrollment.

3

Complete Steps 1 and 2.

6. Haga clic en **Desinscribir**.

⚠ Warning: After this enterprise is unenrolled, Android Enterprise apps on devices enrolled in it are reset to their default states. The devices will no longer be managed by Google. Re-enrolling them in an Android Enterprise enterprise may not restore previous functionality without further configuration.

1

Enter password and press Next to continue unenrollment process.

Password must be least 4 characters.

Next

2

Enter the email address of any administrator for the enterprise and press Unenroll to complete unenrollment.

xm tools test enterprise
LC04akyvpk

Unenroll

3

Complete Steps 1 and 2.

Aprovisionar dispositivos totalmente administrados en Android Enterprise

Solo los dispositivos propiedad de la empresa pueden ser dispositivos totalmente administrados en Android Enterprise. En 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 de trabajo.

Citrix Endpoint Management admite estos métodos de inscripción para los dispositivos totalmente administrados:

- **afw#xenmobile:** Con este método de inscripción, el usuario escribe 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 de códigos QR es una forma fácil de aprovisionar una flota distribuida de dispositivos que no admiten NFC, como las tabletas. Puede usar el método de inscripción por código QR en flotas de dispositivos que se han restablecido a sus valores de fábrica. El método de inscripción por código QR instala y configura dispositivos totalmente administrados mediante el escaneo de un código QR desde el asistente de configuración.
- **Conexión Near Field Communication (NFC):** Puede usar el método de inscripción por conexión NFC en flotas de dispositivos que se han restablecido a sus valores de fábrica. Una conexión NFC transfiere datos entre dos dispositivos por transmisión de datos en proximidad. Bluetooth, Wi-Fi y otros modos de comunicación están inhabilitados en un dispositivo que ha sido restablecido a sus valores de fábrica. NFC es el único protocolo de comunicación que el dispositivo

puede utilizar en ese estado.

afw#xenmobile

El método de inscripción se usa después de encender un dispositivo nuevo o restablecido a los valores de fábrica para la configuración inicial. Los usuarios escriben **afw#xenmobile** cuando se les pide que introduzcan una cuenta de Google. Esta acción descarga e instala Citrix Secure Hub. Los usuarios siguen las indicaciones de configuración de Citrix Secure Hub para completar la inscripción.

Se recomienda este método de inscripción para la mayoría de los clientes porque la versión más reciente de Citrix Secure Hub se descarga desde Google Play Store. A diferencia de otros métodos de inscripción, no es necesario proporcionar Citrix Secure Hub para descargarlo desde el servidor de Citrix Endpoint Management.

Requisitos previos:

- Compatible con todos los dispositivos Android que ejecutan el sistema operativo Android.

Código QR

Para inscribir un dispositivo en el modo de dispositivo mediante un código QR, debe generar un código QR. Para ello, cree un JSON y conviértalo en un código QR. La cámara del dispositivo escanea el código QR para inscribir el dispositivo.

Requisitos previos:

- Se admite en todos los dispositivos con 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: qn7oZUtheu3JBainzZRrjCQv6LOO6LL1OjcxT3-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:** Indique los códigos de idioma y país.

Los códigos de idioma son códigos de idioma ISO de dos letras minúsculas (por ejemplo, “es” para español), según se definen en [ISO 639-1](#). Los códigos de país son códigos de país de dos letras mayúsculas (por ejemplo, “ES” para España), según se definen en [ISO 3166-1](#). Por ejemplo, introduzca es_ES para el español hablado en España.

- **android.app.extra.PROVISIONING_TIME_ZONE:** La zona horaria en que se ejecuta el dispositivo.

Escriba el [nombre de la base de datos del área o ubicación](#). Por ejemplo, **America/Los_Angeles** para la zona horaria del Pacífico en Estados Unidos. Si no introduce ningún nombre, la zona horaria se rellena automáticamente.

- **android.app.extra.PROVISIONING_LOCAL_TIME:** Tiempo en milisegundos desde epoch.

El epoch de Unix (o la hora de Unix, la hora de POSIX o la marca de hora de Unix) es la cantidad de segundos que hayan transcurridos desde el 1 de enero de 1970 (medianoche UTC/GMT). En este tiempo no se cuentan los segundos intercalares (en ISO 8601: 1970-01-01T00:00:00Z).

- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** Establézcalo en **true** para omitir el cifrado durante la creación del perfil. Establezca esta opción en **false** para forzar el cifrado durante la creación del perfil.

Un archivo JSON típico es similar al siguiente:

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.citrix.endpoint.management.device",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "12345678901234567890123456789012",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://example.com/download",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

Valide el archivo JSON que se cree mediante una herramienta de validación JSON, como <https://jsonlint.com>. Convierta esa cadena JSON en un código QR con cualquier generador de códigos QR en línea.

Este código QR se escanea con un dispositivo restablecido a los valores de fábrica para inscribirlo como dispositivo totalmente administrado.

Para inscribir el dispositivo

Para inscribir un dispositivo como un dispositivo totalmente administrado, el dispositivo debe haberse restablecido a los valores de fábrica.

1. Toque seis veces en la pantalla de bienvenida para iniciar la inscripción por código QR.
2. Cuando se le solicite, conéctese a la Wi-Fi. Se puede acceder a la ubicación de descarga que tenga establecido Citrix Secure Hub en el código QR (codificado en JSON) a través de esta red Wi-Fi.

Una vez que el dispositivo se haya conectado a la red Wi-Fi, descarga un lector de códigos QR desde 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 establecida en el código QR, valida la firma del certificado de firma, instala Citrix Secure Hub y establece el modo de propietario del dispositivo.

Para obtener más información sobre el aprovisionamiento de dispositivos mediante el método de código QR, consulte la [documentación de API de Google para desarrolladores de Android EMM](#).

Conexión NFC

Para inscribir un dispositivo como dispositivo totalmente administrado mediante conexiones NFC, se necesitan dos dispositivos: uno que se haya restablecido a sus valores de fábrica y otro con la herramienta Citrix Endpoint Management Provisioning Tool.

Requisitos previos:

- Dispositivos Android compatibles
- Citrix Endpoint Management habilitado para Android Enterprise
- Un dispositivo nuevo o restablecido a los valores de fábrica, aprovisionado para Android Enterprise como un dispositivo totalmente administrado. Dispone de los pasos necesarios para completar este requisito previo más adelante en este artículo.
- Otro dispositivo con capacidades de comunicación NFC, que ejecuta la herramienta Provisioning Tool configurada. La herramienta Provisioning Tool 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 para la administración de movilidad empresarial (EMM). En Citrix Endpoint Management, Citrix Secure Hub es la aplicación EMM. Solo se permite un perfil por dispositivo. Si intenta agregar una segunda aplicación EMM, se eliminará la primera.

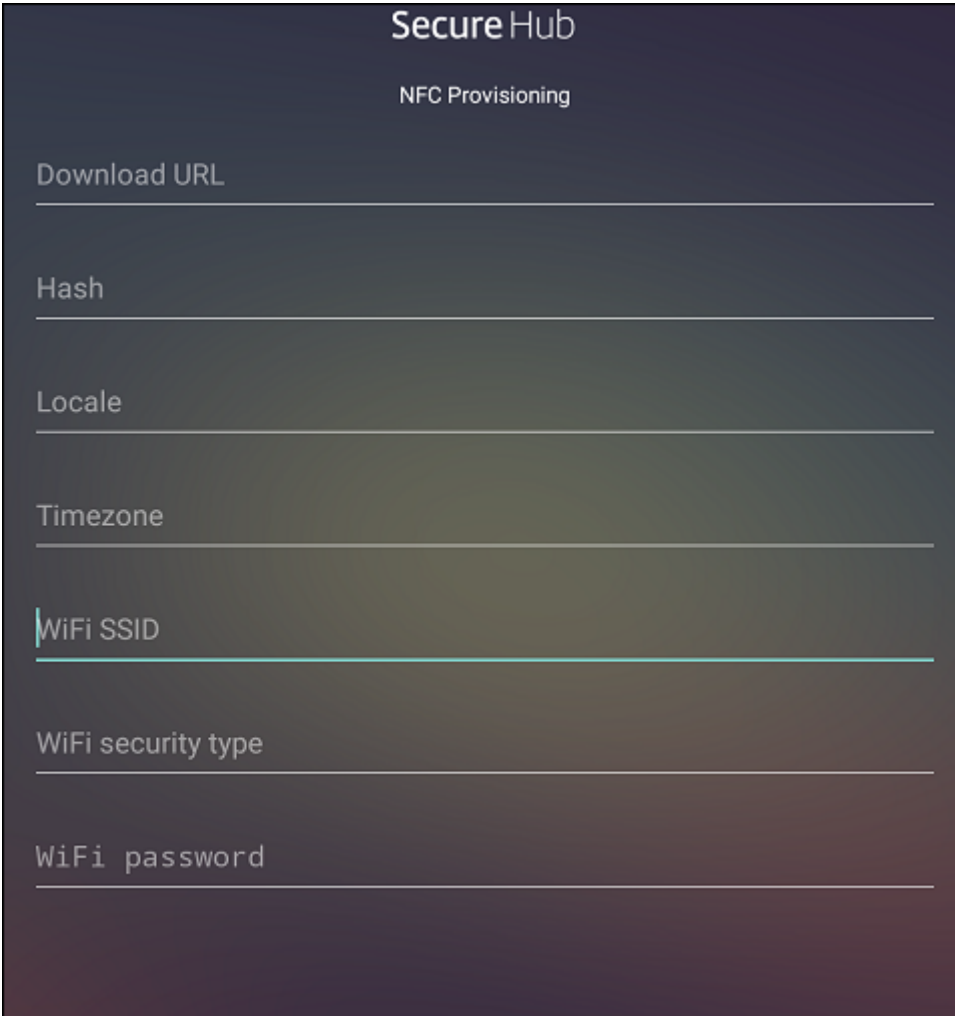
Datos transferidos a través de la conexión NFC Para aprovisionar un dispositivo restablecido a sus valores de fábrica, debe enviar los siguientes datos vía una conexión NFC para inicializar Android Enterprise:

- Nombre del paquete de la aplicación de proveedor EMM que actuará como propietario del dispositivo (en este caso, Citrix Secure Hub).
- Ubicación de intranet o Internet desde donde el dispositivo puede descargar la aplicación de proveedor EMM.
- Valor hash SHA-256 de la aplicación de proveedor EMM para verificar si la descarga fue correcta.

- Datos de la conexión Wi-Fi para que un dispositivo restablecido a sus valores de fábrica pueda conectarse y descargar la aplicación de proveedor EMM. Nota: Android no admite 802.1x Wi-Fi para este paso.
- Zona horaria del dispositivo (opcional).
- Ubicación geográfica del dispositivo (opcional).

Cuando los dos dispositivos se conectan por NFC, los datos de la herramienta Provisioning Tool se envían al dispositivo restablecido a los valores de fábrica. Esos datos se utilizan para descargar Citrix Secure Hub con los parámetros del administrador. Si no introduce valores para la zona horaria y la ubicación geográfica, Android los configurará automáticamente en el nuevo dispositivo.

Configuración de la herramienta Citrix Endpoint Management Provisioning Tool Antes de una conexión NFC, es necesario configurar la herramienta Provisioning Tool. Esta configuración se transfiere, a continuación, al dispositivo restablecido a los valores de fábrica durante la conexión NFC.



The image shows a dark-themed configuration screen for 'Secure Hub' with the subtitle 'NFC Provisioning'. It contains several input fields for provisioning data:

- Download URL
- Hash
- Locale
- Timezone
- WiFi SSID (highlighted with a green bar)
- WiFi security type
- WiFi password

Puede introducir los datos en los campos requeridos o rellenar los campos mediante un archivo de

texto. En los pasos del siguiente procedimiento, se describe cómo configurar un archivo de texto que contenga descripciones para cada campo. La aplicación no guarda información una vez introducida esta, por lo que puede ser conveniente crear un archivo de texto para conservar esa información para el futuro.

Para configurar Provisioning Tool mediante un archivo de texto Nombre el archivo `nfcprovisioning.txt` y colóquelo en la tarjeta SD del dispositivo (en la carpeta `/sdcard/`). La aplicación leerá el archivo de texto y rellenará los valores.

El archivo de texto debe contener los datos siguientes:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION
=<download_location>
```

Esta línea es la ubicación de intranet o Internet de la aplicación de proveedor EMM. Una vez que el dispositivo restablecido a los valores de fábrica se haya conectado a una red Wi-Fi por conexión NFC, el dispositivo debe tener acceso a esta ubicación para la descarga. La URL es una dirección URL normal, sin formato especial.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA-256
hash>
```

Esta línea es la suma de comprobación de la aplicación de proveedor 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 del dispositivo conectado por Wi-Fi donde se está ejecutando la herramienta Provisioning Tool.

```
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 códigos de idioma y país. Los códigos de idioma son códigos de idioma ISO de dos letras minúsculas (por ejemplo, “es” para español), según se definen en [ISO 639-1](#). Los códigos de país son códigos de país de dos letras mayúsculas (por ejemplo, “ES” para España), según se definen en [ISO 3166-1](#). Por ejemplo, introduzca `es_ES` para el español hablado en España. Si no introduce ningún código, el país y el idioma se rellenan automáticamente.

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

La zona horaria en que se ejecuta el dispositivo. Escriba el [nombre de la base de datos del área o ubicación](#). Por ejemplo, **America/Los_Angeles** para la zona horaria del Pacífico en Estados Unidos. Si no introduce ningún nombre, la zona horaria se rellena automáticamente.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

Este dato no es necesario, porque el valor está codificado en la aplicación como “Citrix Secure Hub”. Se menciona aquí a título meramente informativo.

Si existe una red Wi-Fi protegida con WPA2, un archivo nfcprovisioning.txt completado puede 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=ga50TwdCmfdJ72LGR
\u003d
```

```
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 existe una red Wi-Fi no protegida, un archivo nfcprovisioning.txt completado puede 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=ga50TwdCmfdJ72LGR
\u003d
```

```
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: `qn7oZUtheu3JBaInzZRrrjCQv6L006Ll10jcxT3-yKM`. Para descargar un archivo APK destinado para 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** del componente Android SDK Build-Tools
- Línea de comandos de OpenSSL

Para obtener la suma de comprobación de una aplicación, siga estos pasos:

1. Descargue el archivo APK de la aplicación desde Google Play.
2. En la línea de comandos de OpenSSL, vaya a la herramienta **apksigner**: `android-sdk/build-tools/<version>/apksigner` y escriba lo siguiente:

```
1 apksigner verify -print-certs <apk_path> | perl -nle 'print $& if
   m{
2   (?<=SHA-256 digest:) .* }
3   ' | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
4   <!--NeedCopy-->
```

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:

```
1 {
2
3   "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.
   zenprise/com.zenprise.configuration.AdminFunction",
4   "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "
   qn7oZUtheu3JBainzZRrjCQv6L006Ll10jcxT3-yKM",
5   "android.app.extra.
   PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://
   play.google.com/managed/downloadManagingApp?identifier=xenmobile",
6   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
7
8     "serverURL": "https://supportability.xm.cloud.com"
9   }
10
11 }
12
13 <!--NeedCopy-->
```

Bibliotecas utilizadas La herramienta Provisioning Tool utiliza las bibliotecas siguientes en su código fuente:

- Biblioteca `appcompat` v7, biblioteca Design support y biblioteca Palette v7

Para obtener información, busque Support Library Features Guide en la [documentación para desarrolladores de Android](#).

- `Butter Knife` de Jake Wharton bajo la licencia de Apache 2.0

Aprovisionar dispositivos de perfil de trabajo en Android Enterprise

En los dispositivos de perfil de trabajo de Android Enterprise, las áreas corporativas y personales de un dispositivo se separan de forma segura. Por ejemplo, los dispositivos BYOD pueden ser dispositivos de perfil de trabajo. La experiencia de inscripción para los dispositivos de perfil de trabajo es similar a la inscripción de Android en Citrix Endpoint Management. Los usuarios descargan Citrix Secure Hub desde Google Play e inscriben sus dispositivos.

De forma predeterminada, los parámetros de depuración por USB y fuentes desconocidas están inhabilitados en un dispositivo cuando se inscribe en Android Enterprise como un modo de perfil de trabajo.

Sugerencia:

Cuando inscriba dispositivos en Android Enterprise como dispositivos de perfil de trabajo, vaya siempre a Google Play. Desde allí, habilite Citrix Secure Hub para que aparezca en el perfil personal del usuario.

Sistema operativo Android

November 29, 2023

Nota:

Este artículo no se aplica a dispositivos administrados con Android Enterprise. Para obtener información acerca de esos dispositivos, consulte otros artículos de esta sección.

Citrix Endpoint Management también admite dispositivos con sistema operativo Android que no se administran a través de un programa empresarial de Android o Samsung. Utilice Firebase Cloud Messaging (FCM) para controlar cómo y cuándo los dispositivos Android se conectan al servicio Citrix Endpoint Management. 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 posibilidad de que los usuarios se excluyan de MDM. Citrix Endpoint Management admite los siguientes tipos de autenticación para dispositivos Android en MDM+MAM. Para obtener información, consulte estos artículos:

- [Autenticación de dominios o dominio y token de seguridad](#)
- [Autenticación con certificado de cliente o certificado y 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 que rara vez se utiliza es el certificado de cliente junto con el 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 [Incorporarse como usuario y configurar 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. Configure directivas de dispositivo para Android.
4. Inscriba los dispositivos Android.
5. Configure las acciones de seguridad para los dispositivos y las aplicaciones. Consulte [Acciones de seguridad](#).

Para conocer los sistemas operativos admitidos, consulte [Sistemas operativos admitidos](#).

Métodos de inscripción admitidos







En la siguiente tabla se indican los métodos de inscripción que Citrix Endpoint Management admite para dispositivos Android:

Método	Compatible
Inscripción en bloque	No
Inscripción manual	Sí
Invitaciones de inscripción	Sí

Agregar manualmente un dispositivo Android

Si quiere agregar manualmente un dispositivo Android o iOS (por ejemplo, para probarlo), siga estos pasos.

1. En la consola de Citrix Endpoint Management, haga clic en **Administrar > Dispositivos**. Aparecerá la página **Dispositivos**.

Devices Users Enrollment Invitations					
Devices Show filter					
Add Import Export Refresh					
<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version
<input type="checkbox"/>	  	MDM MAM	[Redacted]	Android	5.0.2
<input type="checkbox"/>	  	MDM MAM	[Redacted]	iOS	8.4.1

2. Haga clic en **Agregar**. Aparecerá la página **Agregar dispositivo**.

Devices Users Enrollment Invitations	
Details	<div>Add Device ×</div> <div>Select Platform <input checked="" type="radio"/> iOS <input type="radio"/> Android</div> <div>Serial Number* <input type="text"/></div>

3. Configure estos parámetros:

- **Seleccione la 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**. La tabla **Dispositivos** aparecerá con el dispositivo agregado al final de la lista. Seleccione el dispositivo agregado y, a continuación, en el menú que aparecerá, haga clic en **Modificar** para ver y confirmar los detalles del dispositivo.

Nota:

Cuando se marca la casilla situada junto a un dispositivo, el menú de opciones aparece encima de la lista de dispositivos. Si hace clic en cualquier lugar de la lista, el menú de opciones aparece a la derecha de la lista.

- LDAP configurado
- Si utiliza grupos y usuarios locales:
 - Uno o varios grupos locales.
 - Usuarios locales asignados a grupos locales.
 - Los grupos de entrega se asocian con grupos locales.
- Si usa Active Directory:
 - Los grupos de entrega se asocian con grupos de Active Directory.

5. En la página **General** se muestra una lista de los **identificadores** de dispositivo, como el número de serie y otra información en función del tipo de plataforma. Para **Propietario del dispositivo**, seleccione **Empresa** o **BYOD**.

Asimismo, la página **General** muestra una lista de las propiedades de **Seguridad** de que está dotado el dispositivo (como el ID seguro, el bloqueo del dispositivo y la omisión del bloqueo de activación), así como otra información en función del tipo de plataforma. El campo **Borrado completo del dispositivo** contiene el código PIN del usuario. El usuario debe introducir ese código después de que se haya borrado el dispositivo. Si el usuario no consigue recordar el código, usted puede buscarlo en “Detalles del dispositivo”.

6. La página **Propiedades** muestra una lista de las propiedades de dispositivo que aprovisionará Citrix Endpoint Management. La lista contiene todas las propiedades de 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 saber cuáles son los valores válidos para cada propiedad, consulte el PDF [Valores y nombres de propiedades de dispositivo](#).

Cuando se agrega una propiedad, esta aparece inicialmente en la categoría donde se haya agregado. Después de hacer clic en **Siguiente** y volver a la página **Propiedades**, la propiedad aparece en la lista apropiada.

Para eliminar una propiedad, coloque el cursor sobre ella y, a continuación, haga clic en el aspa (X) situada en el lado derecho. Citrix Endpoint Management elimina inmediatamente el elemento.

7. Las secciones restantes de **Detalles del dispositivo** contienen información resumida acerca del

dispositivo.

- **Propiedades de usuario:** Muestra los roles de RBAC, los miembros del grupo, las cuentas de Google Play administrado y las propiedades del usuario. Puede retirar una cuenta de Google Play administrada desde esta página.
- **Directivas asignadas:** Muestra la cantidad de directivas implementadas, pendientes y fallidas. También muestra el nombre, el tipo e información de última implementación de cada directiva. Permite restablecer el estado de implementación como pendiente y volver a implementar directivas que el usuario eliminó.
- **Aplicaciones:** Muestra la cantidad de implementaciones de aplicaciones instaladas, pendientes y erróneas según el último inventario. Indica el nombre de la aplicación, el identificador y el tipo, entre otros datos. Para obtener una descripción de las claves de inventario de iOS y macOS, como **HasUpdateAvailable**, consulte [Mobile Device Management \(MDM\) Protocol](#).
- **Multimedia:** Muestra la cantidad de implementaciones de archivos multimedia instalados, pendientes y erróneos según el último inventario.
- **Acciones:** Muestra la cantidad de acciones implementadas, pendientes y erróneas. Indica el nombre de la acción y la hora de la última implementación.
- **Grupos de entrega:** Muestra la cantidad de grupos de entrega en estado correcto, pendiente y fallido. Indica el nombre del grupo de entrega y la hora de cada implementación. Seleccione un grupo de entrega para ver información más detallada (como el estado, la acción, el canal o el usuario).
- **Perfiles iOS:** Muestra el último inventario de perfiles iOS, que incluye el nombre, el tipo, la organización y la descripción.
- **Perfiles de datos de iOS:** Muestra información acerca del perfil de datos utilizado por la empresa para la distribución (como el UUID, la fecha de caducidad y si se administra o no).
- **Certificados:** Muestra la cantidad de certificados válidos, caducados o revocados, incluida la información sobre el tipo, el proveedor, el emisor, el número de serie y los días que quedan hasta la caducidad.
- **Conexiones:** Muestra los estados de la primera y la última conexión. Para cada conexión, aparecen el nombre de usuario, así como la hora de las dos últimas autenticaciones (la penúltima y la última).
- **Estado de MDM:** Muestra información como el estado MDM, la hora del último envío push y la hora de la última respuesta del dispositivo.

Configurar directivas de dispositivo para Android

Use estas directivas para configurar cómo interactúa Citrix Endpoint Management con los dispositivos Android. En esta tabla se indican todas las directivas de dispositivo disponibles para dispositivos Android.

|||

|—|—|—|

[[APN]](/es-es/citrix-endpoint-management/policies/apn-policy.html#android-settings) |[Acceso a aplicaciones]](/es-es/citrix-endpoint-management/policies/app-access-policy.html) |[Inventario de aplicaciones]](/es-es/citrix-endpoint-management/policies/app-inventory-policy.html) |
[[Bloqueo de aplicaciones]](/es-es/citrix-endpoint-management/policies/app-lock-policy.html#android-legacy-da-settings) |[Desinstalación de aplicaciones]](/es-es/citrix-endpoint-management/policies/app-uninstall-policy.html) |[Credenciales]](/es-es/citrix-endpoint-management/policies/credentials-policy.html#android-settings) |
[[Opciones de Citrix Endpoint Management]](/es-es/citrix-endpoint-management/policies/options-policy.html) |[Desinstalación de Citrix Endpoint Management]](/es-es/citrix-endpoint-management/policies/uninstall-policy.html) |[Archivos]](/es-es/citrix-endpoint-management/policies/files-policy.html) |
[[Configuración de Launcher]](/es-es/citrix-endpoint-management/policies/launcher-configuration-policy.html) |[Ubicación]](/es-es/citrix-endpoint-management/policies/location-policy.html#android-legacy-da-settings) |[Red]](/es-es/citrix-endpoint-management/policies/network-policy.html#android-legacy-da-settings)|
[[Código de acceso]](/es-es/citrix-endpoint-management/policies/passcode-policy.html#android-legacy-da-settings) |[Restricciones]](/es-es/citrix-endpoint-management/policies/restrictions-policy.html#android-settings) |[Programación]](/es-es/citrix-endpoint-management/policies/connection-scheduling-policy.html) |
[[Almacén]](/es-es/citrix-endpoint-management/policies/store-policy.html) |[Términos y condiciones]](/es-es/citrix-endpoint-management/policies/terms-and-conditions-policy.html) |[Túnel]](/es-es/citrix-endpoint-management/policies/tunnel-policy.html)|
[VPN](#) | [Clip web](#) |

Inscribir dispositivos Android

1. Vaya a Google Play Store en el dispositivo Android, descargue la aplicación Citrix Secure Hub y toque la aplicación para abrirla.
2. Cuando se le solicite la instalación de la aplicación, haga clic en **Siguiente** y, a continuación, haga clic en **Instalar**.
3. Después de que Citrix Secure Hub se instale, toque **Abrir**.
4. Para dispositivos con Android 6.0 o posterior, conceda los permisos necesarios:
 - ¿Permitir que Citrix Secure Hub realice y administre las llamadas telefónicas? (obligatorio)
 - ¿Permitir que Citrix Secure Hub acceda a fotos, contenido multimedia y archivos que haya en el dispositivo? (obligatorio)
 - ¿Permitir que Citrix Secure Hub acceda a la ubicación del dispositivo? (opcional)

5. Introduzca las credenciales de empresa, como el nombre del servidor de Citrix Endpoint Management de su empresa, el nombre principal de usuario (UPN) o su dirección de correo electrónico. A continuación, haga clic en **Siguiente**.
6. Elija cómo inscribir el dispositivo:
 - Para inscribir en MDM+MAM, toque **Sí, inscribirlo**.
 - Para inscribir en MAM, toque **No**.
7. En la pantalla **Activate device administrator**, toque **Activate**.
8. Escriba la contraseña de empresa y, a continuación, toque **Iniciar sesión**.
9. Es posible que tenga que crear un PIN de Citrix (según la configuración de Citrix Endpoint Management). 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. Deberá introducir su PIN de Citrix dos veces. En la pantalla **Crear PIN de Citrix**, introduzca un PIN.
10. Vuelva a escribir el PIN. Se abrirá Citrix Secure Hub. En ese momento, puede acceder al almacén de aplicaciones para ver las aplicaciones que puede instalar en el dispositivo Android.
11. Si ha configurado Citrix Endpoint Management de manera que las aplicaciones se envíen automáticamente a los dispositivos de los usuarios después de la inscripción, los usuarios verán mensajes con solicitudes de instalación de las aplicaciones. Además, las directivas que configure en Citrix Endpoint Management se implementan en el dispositivo. Toque **Instalar** para instalar las aplicaciones.

Para inscribir y reinscribir un dispositivo Android

Los usuarios pueden desinscribirse una vez dentro de Citrix Secure Hub. Cuando los usuarios se desinscriben con el siguiente procedimiento, el dispositivo sigue apareciendo en el inventario de dispositivos en la consola de Citrix Endpoint Management. No obstante, no es posible realizar acciones en el dispositivo. Por ejemplo, no puede realizar un seguimiento del dispositivo ni supervisar su estado de cumplimiento.

1. Toque Citrix Secure Hub para abrir la aplicación.
2. Dependiendo de si dispone de un teléfono o una tableta, lleve a cabo lo siguiente:

En un teléfono:

- Deslice desde la izquierda de la pantalla para abrir un panel de configuración.
- Toque **Preferencias** > **Cuentas**. A continuación, toque **Eliminar cuenta**.

En una tableta:

- Toque la flecha situada junto a su dirección de correo electrónico en la esquina superior derecha.
 - Toque **Preferencias > Cuentas**. A continuación, toque **Eliminar cuenta**.
3. En la ventana **¿Quiere eliminar la cuenta?**, toque **Sí, eliminar**.
Citrix Secure Hub anula la inscripción del dispositivo. Siga las instrucciones que aparecen en la pantalla para reinscribir el dispositivo.

Acciones de seguridad

Android admite las siguientes acciones de seguridad. Para ver una descripción de cada acción de seguridad, consulte [Acciones de seguridad](#).

Bloqueo de aplicaciones	Borrado de aplicaciones	Renovación de certificados
Borrado completo	Localizar	Bloquear
Bloqueo y restablecimiento de contraseña	Notify	Revocar
Borrado selectivo		

Nota:

Para dispositivos que ejecutan Android 6.0 o posterior, la acción de seguridad “Localizar” requiere que el usuario conceda permisos de localización durante la inscripción. El usuario puede optar por no conceder permisos de localización. Si el usuario no concede el permiso durante la inscripción, Citrix Endpoint Management vuelve a solicitarlo cuando envía el comando de localización.

Firestore Cloud Messaging

November 29, 2023

Nota:

Firestore Cloud Messaging (FCM) se conocía anteriormente como Google Cloud Messaging (GCM).

Algunas etiquetas y mensajes de la consola de Citrix Endpoint Management aún se refieren a GCM.

Citrix le recomienda que utilice Firebase Cloud Messaging (FCM) para controlar cómo y cuándo los dispositivos Android se conectan a Citrix Endpoint Management. Citrix Endpoint Management, cuando se configura para FCM, envía notificaciones de conexión a dispositivos Android habilitados para FCM. Así, toda acción de seguridad o comando de implementación desencadena una notificación push para pedir al usuario que se reconecte al servidor de Citrix Endpoint Management.

Después de completar los pasos de configuración indicados en este artículo y después de que un dispositivo comience a usarse, este dispositivo se registrará en el servicio FCM de Citrix Endpoint Management. Esa conexión permite la comunicación casi en tiempo real entre el servicio de Citrix Endpoint Management y el dispositivo mediante FCM. El registro de FCM funciona para inscripciones de nuevos dispositivos y dispositivos previamente inscritos.

Cuando Citrix Endpoint Management necesita iniciar una conexión con el dispositivo, se conecta al servicio FCM. Entonces, el servicio FCM notifica al dispositivo que se conecte. Este tipo de conexión es similar a lo que Apple utiliza para su servicio de notificaciones push.

Requisitos previos

- Cliente más reciente de Citrix Secure Hub
- Credenciales de cuenta de Google para desarrolladores
- Servicios de Google Play instalados en dispositivos Android habilitados para FCM

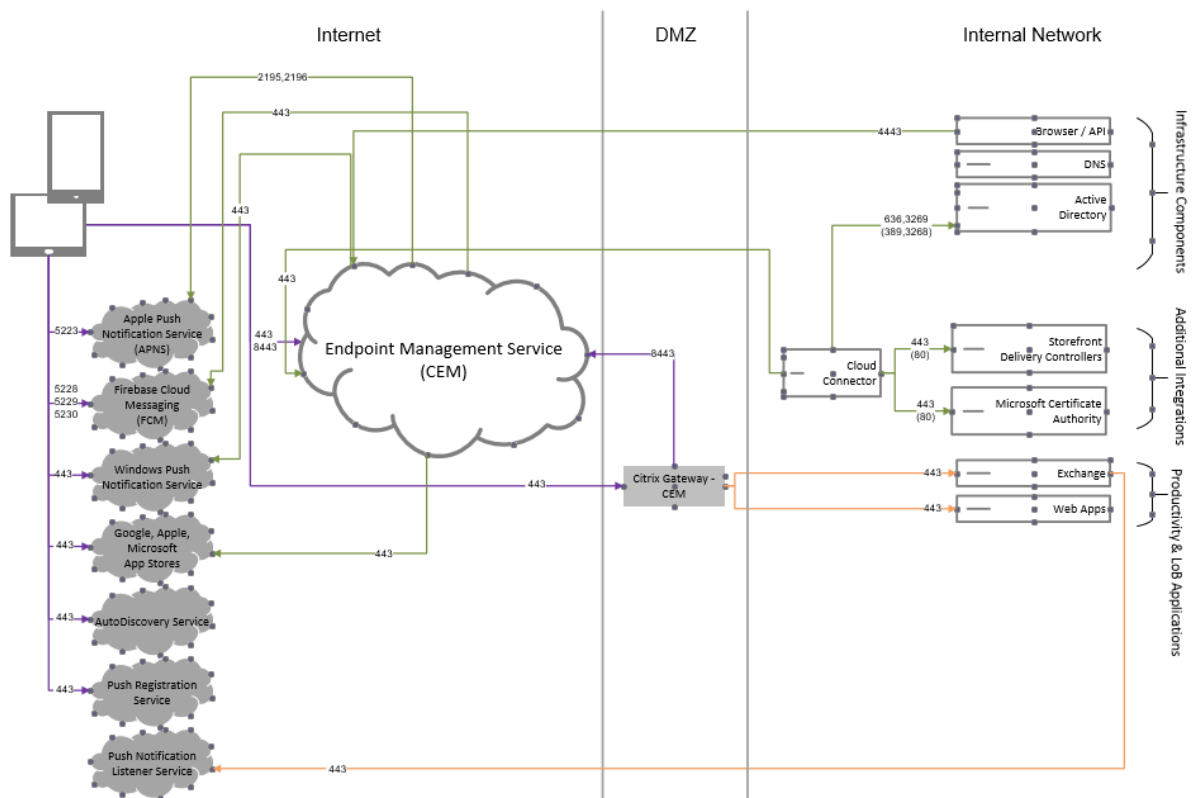
Puertos de firewall

- Abra el puerto 443 en Citrix Endpoint Management para fcm.googleapis.com y [Google.com](https://google.com).
- Abra una comunicación saliente por Internet para la red Wi-Fi de dispositivos en los puertos 5228, 5229 y 5230.
- Para permitir las conexiones salientes, FCM recomienda incluir en la lista de permitidos los puertos 5228, 5229 y 5230 sin restricciones de IP. Sin embargo, si necesita restricciones de IP, FCM recomienda incluir todas las direcciones IP de los bloques IPv4 e IPv6 en la lista de IP permitidas. Esos bloques se muestran en [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 de FCM en la red interna y externa.

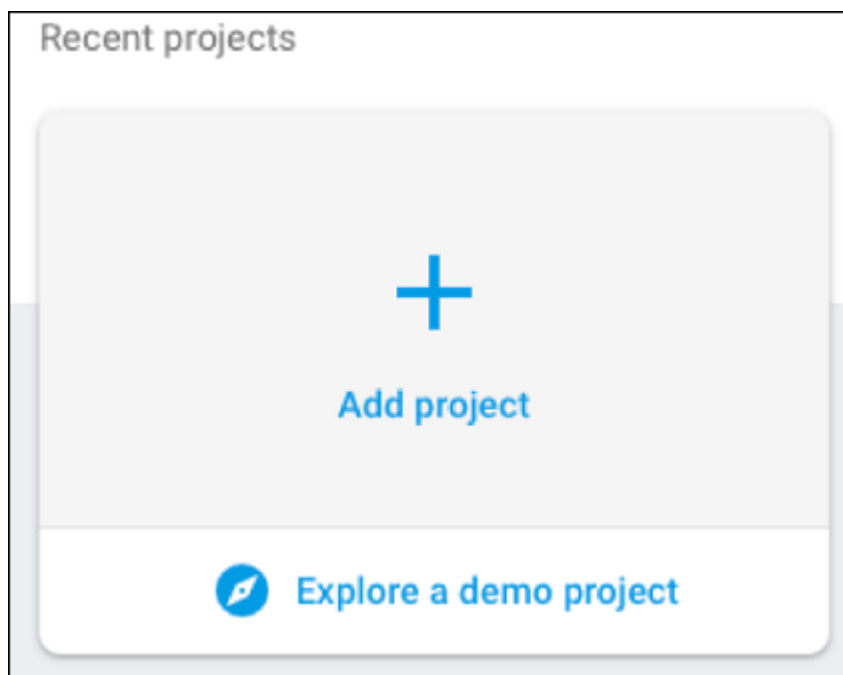


Para configurar su cuenta de Google para FCM

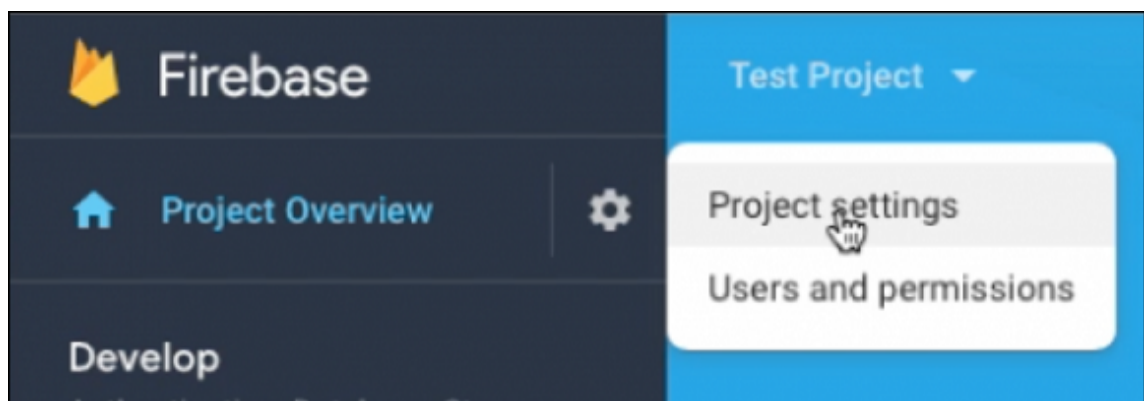
1. Inicie sesión en la siguiente URL con las credenciales de la cuenta de Google para desarrolladores:

<https://console.firebase.google.com/>

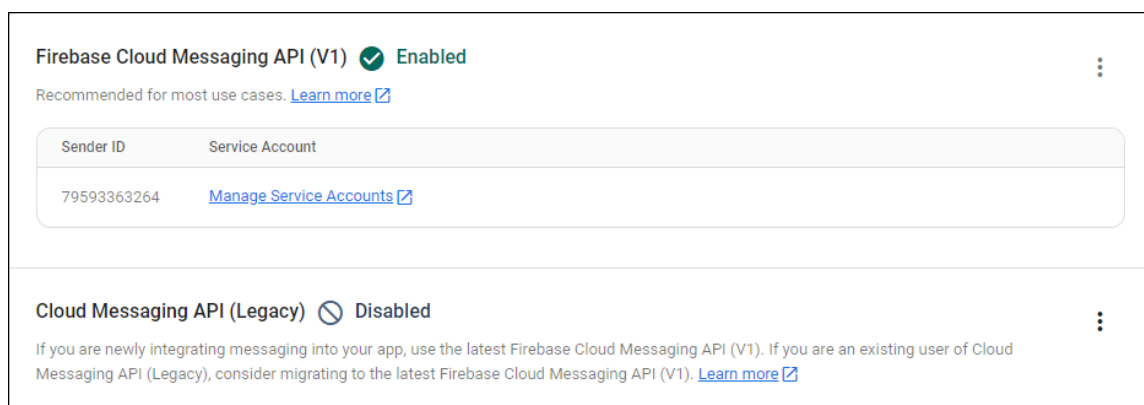
2. Haga clic en **Add project**.



3. Después de crear el proyecto, haga clic en **Project settings**.



4. Haga clic en la ficha **Cloud Messaging**. Compruebe que la API de Firebase Cloud Messaging esté habilitada y haga clic en **Manage Service Accounts**.



5. Copie los valores de los campos **Key** y **OAuth 2 Client ID**. Si no tiene ninguna clave en la lista, haga clic en los puntos suspensivos de **Actions** para agregar una nueva clave.

Filter Enter property name or value								
<input type="checkbox"/>	Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
<input type="checkbox"/>	firebase-adminsdk-2lmzm2@test-79ca2.iam.gserviceaccount.com	●	firebase-adminsdk	Firebase Admin SDK Service Agent	7d63fbdf1d81eaaad1ef9aec401043a926f92e7	Jul 14, 2022	104212590725511261742	⋮

Para ver los pasos necesarios 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 **Parámetros > Firebase Cloud Messaging**.

- Modifique el campo **API Key** y escriba la **clave** de Firebase Cloud Messaging que copió en el último paso de la configuración de Firebase Cloud Messaging.
- Modifique el campo **Sender ID** y escriba el valor de **OAuth 2 Client ID** que copió en el procedimiento anterior.

Settings > Firebase Cloud Messaging

Firebase Cloud Messaging

Configure Firebase Cloud Messaging (FCM) in order to send connection notifications to Android devices that are enabled for FCM. For steps to set up a FCM client app on Android, see the Google Developers Cloud Messaging documentation.

API key

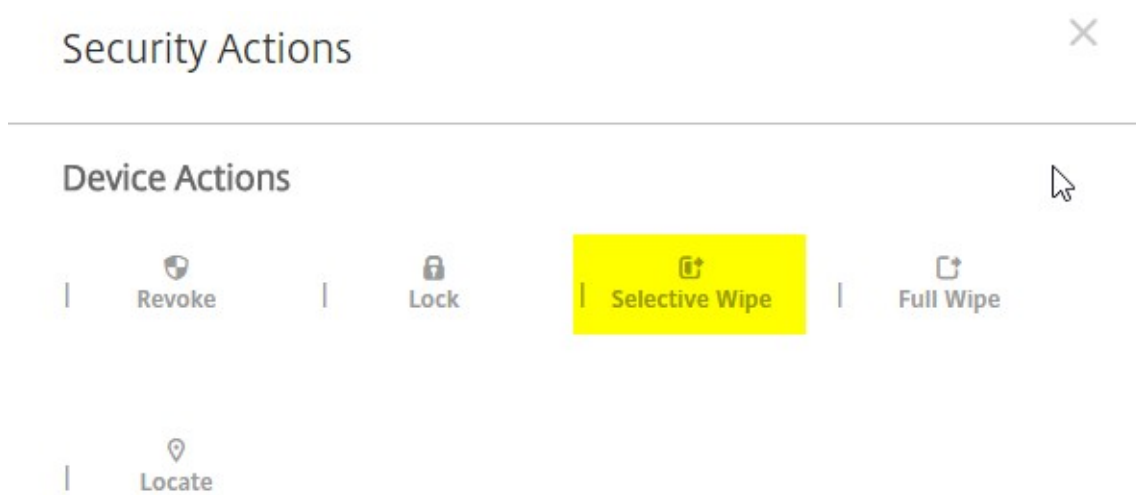
Sender ID

Para probar la configuración

1. Inscriba un dispositivo Android.
2. Deje el dispositivo inactivo durante algún tiempo, de forma 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**.

Devices Users Enrollment Invitations										
Devices Show filter										
<div> Add Edit Secure Notify Delete Import Export Refresh </div>										
<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP registered	Activation
<input checked="" type="checkbox"/>		MDM MAM		Android	6.0.1	Nexus 9	07/27/2016 06:05:25 pm	2 days	No	

4. En **Acciones de dispositivo**, haga clic en **Borrado selectivo**.



Si la configuración es correcta, se lleva a cabo el borrado selectivo en el dispositivo.

Android SafetyNet

November 29, 2023

Puede usar la funcionalidad Android SafetyNet para evaluar la compatibilidad y la seguridad de los dispositivos Android que tienen Citrix Secure Hub instalado. Android SafetyNet no está disponible para implementaciones de MAM.

Cuando esta función está habilitada, la API de SafetyNet Attestation examina la información sobre software y hardware en un dispositivo para crear un perfil de ese dispositivo. La API a continuación busca el mismo perfil dentro de una lista de modelos de dispositivo que hayan pasado la prueba de compatibilidad de Android. La API también usa esta información para determinar si Citrix Secure Hub ha sido modificado por una fuente desconocida.

Cuando la función Android SafetyNet está habilitada, Citrix Secure Hub envía la solicitud de la API de SafetyNet Attestation a los servicios de Google Play y el resultado se devuelve a Citrix Endpoint Management. Citrix Endpoint Management luego actualiza la información del dispositivo con los resultados de la atestación. Puede configurar acciones automatizadas que utilicen los resultados de la atestación para desencadenar acciones en el dispositivo.

Para obtener más información sobre cómo funciona la API de SafetyNet Attestation, consulte la [documentación para desarrolladores de Android](#).

Calcular cuántas solicitudes de la API de SafetyNet Attestation necesita

Las solicitudes de la API de SafetyNet Attestation se envían:

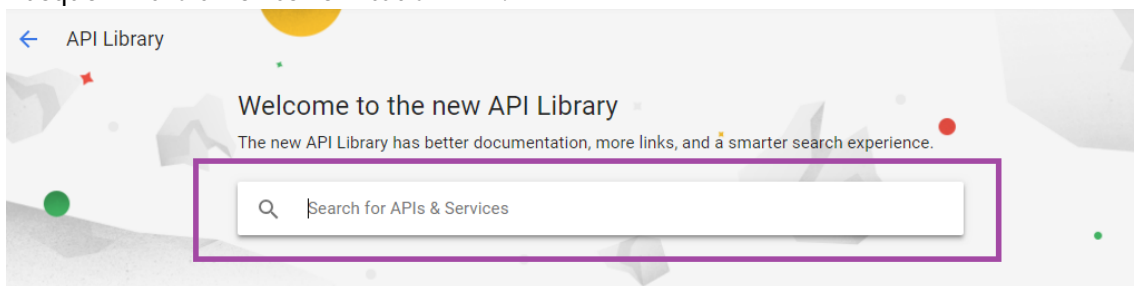
- Cuando un dispositivo se inscribe en Citrix Endpoint Management.
- Cuando se produce una autenticación en línea de Citrix Secure Hub. La autenticación en línea se produce cuando una sesión del servidor caduca o cuando un usuario cierra sesión en el servidor y luego vuelve a iniciarla. Citrix Secure Hub solicita al usuario que proporcione credenciales para autenticarse en el servidor.
- Cuando se reinicia un dispositivo.
- En un intervalo de tiempo recurrente que usted configure, entre 24 y 1000 horas.

Si su implementación de Citrix Endpoint Management hará más de 10 000 solicitudes al día, [rellene este formulario de solicitud de cuota](#).

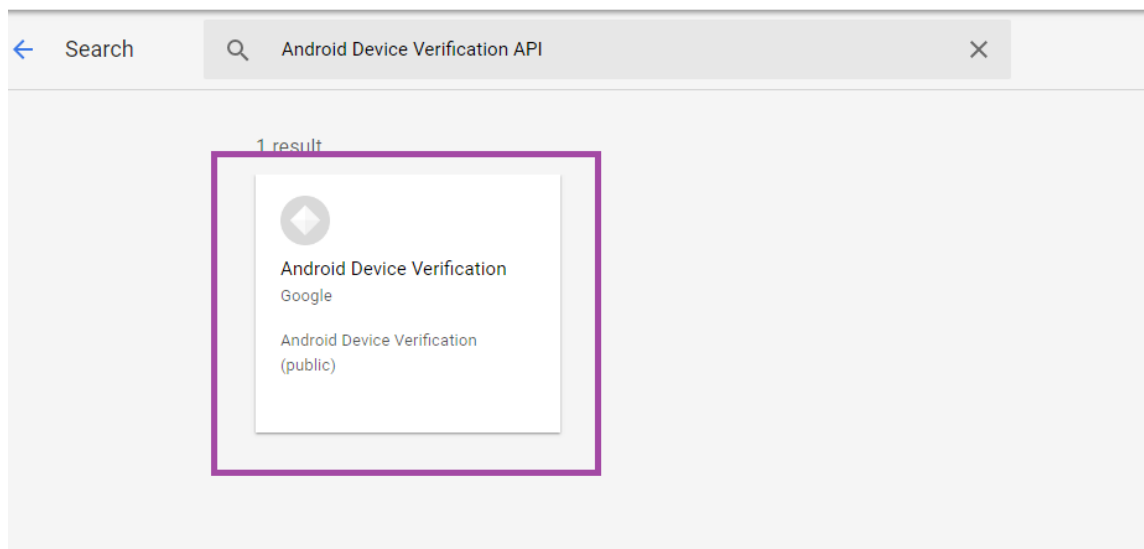
Obtener la clave de la API SafetyNet

Para habilitar Android SafetyNet en Citrix Endpoint Management, necesita la clave de la API SafetyNet.

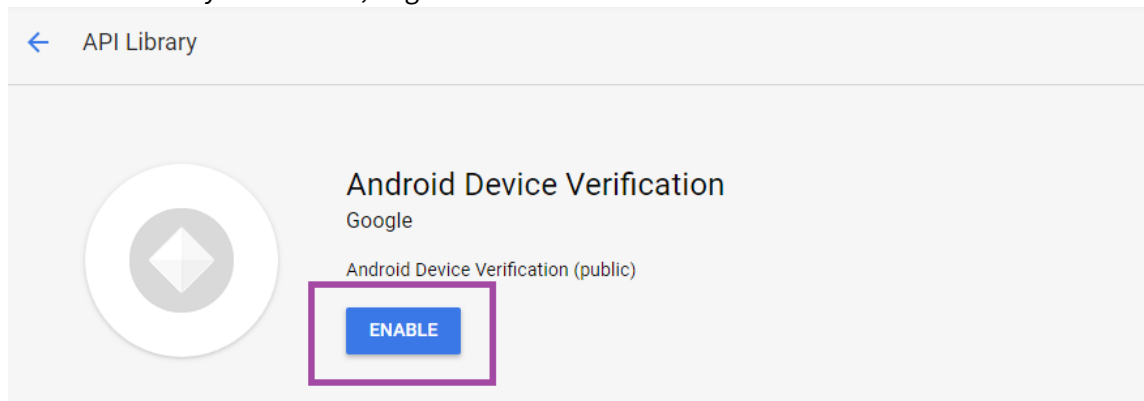
1. Inicie sesión en la consola API de Google con las credenciales de su cuenta de administrador de Google.
2. Vaya a la página Biblioteca.
3. Busque “Android Device Verification API”.



4. Haga clic en **Android Device Verification API**.

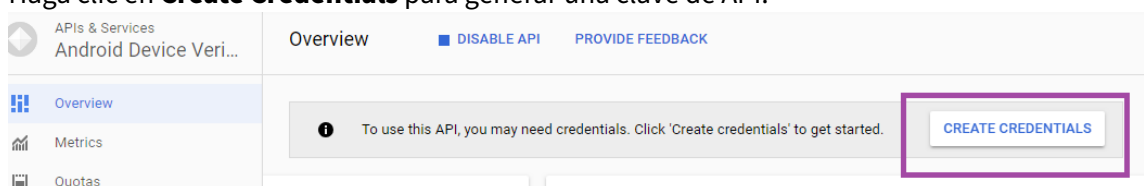


5. Si la API no está ya habilitada, haga clic en **Enable**.

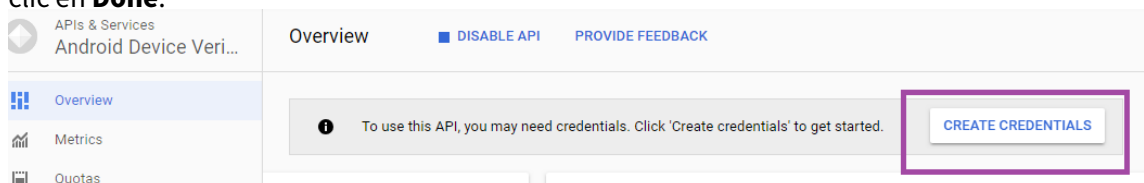


6. Haga clic en **Administrar**.

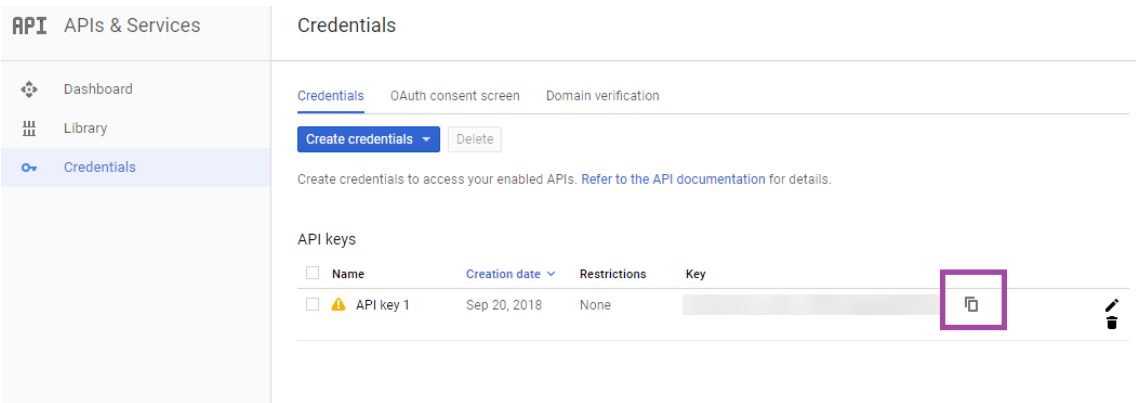
7. Haga clic en **Create Credentials** para generar una clave de API.



8. Seleccione **Android Device Verification** y haga clic en **What credentials to I need**. Luego haga clic en **Done**.



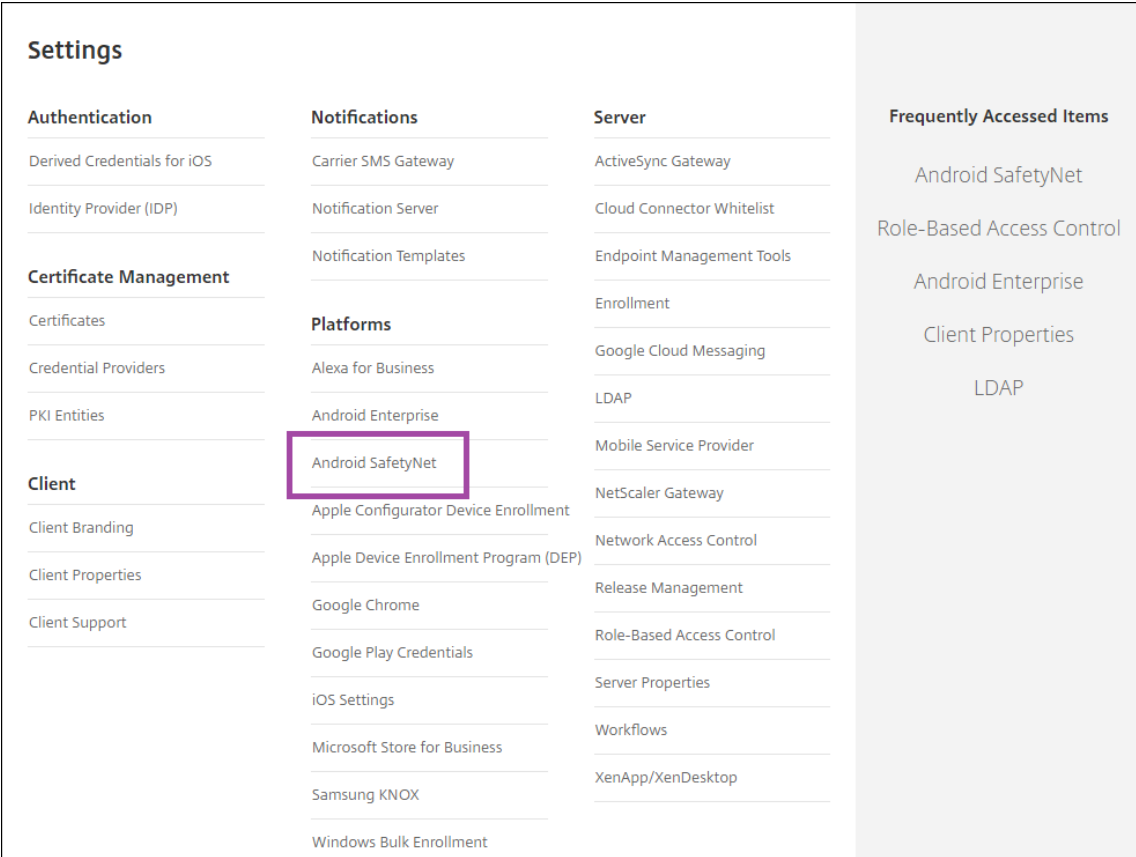
9. En la página **Credentials**, haga clic en el icono de copiar que hay junto a la clave para copiar la clave.



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 con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En la página **Parámetros**, haga clic en **Android SafetyNet**.



3. Configure estos parámetros:

- **Clave de API.** Pegue la clave de la API SafetyNet que obtuvo de la consola de la API de Google.
- **Programa de atestación en horas.** Introduzca el intervalo en horas en el que la API de SafetyNet Attestation evalúa sus dispositivos Android. El valor mínimo es 24 horas. El valor máximo es 1000 horas. El valor por defecto es 24 horas.

Settings > Android SafetyNet

Android SafetyNet

Configure Android SafetyNet, to enable Secure Hub to perform SafetyNet Attestation

Api key *

Attestation schedule in Hours *

4. Haga clic en **Guardar**.

Ver resultados de Android SafetyNet

Para ver los resultados de la evaluación de la API de SafetyNet Attestation para un dispositivo:

1. En la consola de Citrix Endpoint Management, haga clic en **Administrar > Dispositivos**.
2. Seleccione dispositivos Android para ver los resultados de la API de SafetyNet Attestation. Luego haga clic en **Mostrar más**.
3. En la página **Device details**, seleccione **Properties**.
4. Los resultados aparecen en la sección **Security**.

Security information		Add
Administrator disabled	Yes	
External storage encrypted	No	
Internal storage encrypted	No	
Jailbroken/Rooted	Yes	
Kiosk mode	False	
Out of Compliance	False	
Passcode compliant	Yes	
SafetyNet CTS Profile match	False	
SafetyNet basic integrity	False	
SafetyNet last known status	RESTORE_TO_FACTORY_ROM	

La API de SafetyNet Attestation devuelve estos estados para cada dispositivo:

- **SafetyNet CTS profile match:** Si este valor está en **True**, el dispositivo tiene un perfil que coincide con el que ha pasado la prueba Android Compatibility Test Suite (CTS). Si este valor está en **False**, el dispositivo no tiene un perfil que coincide con el que ha pasado la prueba Android CTS.
- **SafetyNet basic integrity:** Si este valor está en **True**, la API de SafetyNet Attestation no encontró pruebas de que Citrix Secure Hub en el dispositivo haya sido modificado por una fuente desconocida. Si este valor está en **False**, Citrix Secure Hub en el dispositivo ha sido modificado por una fuente desconocida.
- **SafetyNet last known status:** Este valor muestra el último estado SafetyNet conocido del dispositivo:
 - **Success:** La API de SafetyNet Attestation no encontró pruebas de que Citrix Secure Hub en el dispositivo haya sido modificado por una fuente desconocida.
 - **LOCK_BOOTLOADER:** El usuario debe bloquear el gestor de arranque del dispositivo. Citrix Secure Hub en el dispositivo ha sido modificado por una fuente desconocida.
 - **RESTORE_TO_FACTORY_ROM:** El usuario debe restaurar el dispositivo con una memoria ROM vacía de fábrica. Citrix Secure Hub en el dispositivo ha sido modificado por una fuente desconocida.

API Play Integrity

November 29, 2023

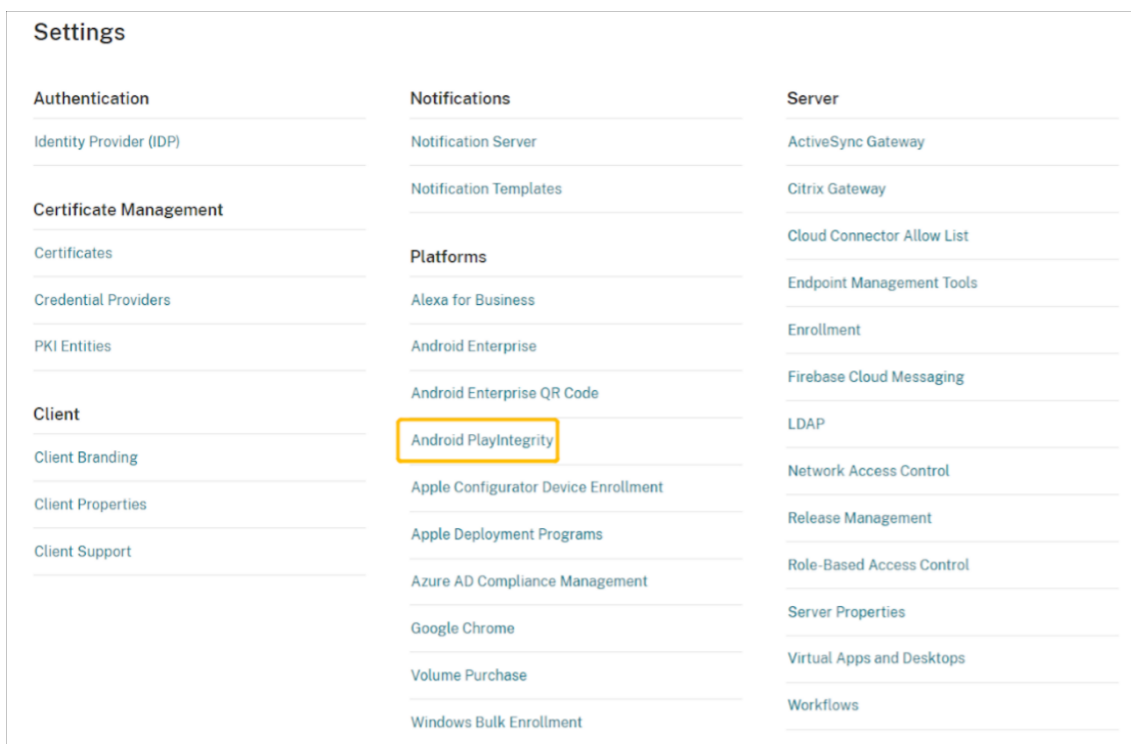
La API de Play Integrity ayuda a proteger sus aplicaciones y juegos de interacciones potencialmente arriesgadas y fraudulentas, como trampas en juegos y accesos no autorizados, lo que le permite responder con medidas adecuadas para evitar ataques y reducir el abuso. Para obtener más información, consulte [Play Integrity API](#).

Habilitar la API de Play Integrity

Siga estos pasos para cambiar a la API de Play Integrity.

1. Active *afw.safetynet.attestation.api*. Marca de función retirada para el servidor de Citrix Endpoint Management especificado.

2. En la consola de Citrix Endpoint Management, seleccione **Android Play Integrity** en la página **Parámetros**.



3. Introduzca un valor en el campo Calendario de atestación por horas. Es el intervalo de tiempo en el que la API de atestación de Play Integrity evalúa su dispositivo. El valor mínimo es de 24 horas y el valor máximo es de 1000 horas. El valor por defecto es 24 horas. Haga clic en **Guardar**.
4. Actualice Citrix Secure Hub para Android a la versión 23.7.0. Cierre la sesión en el dispositivo e inicie sesión en Citrix Secure Hub para activar la autenticación mediante 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 quiere 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**.

Devices	Users	Enrollment Invitations
<div>Device details</div> <div>1 General</div> <div>2 Properties</div> <div>3 User Properties</div> <div>4 Assigned Policies</div> <div>5 Apps</div> <div>6 Media</div>		
<div>– Security information</div> <div>Administrator disabledNo</div> <div>Has a containerNo</div> <div>Internal storage encryptedYes</div> <div>Jailbroken/RootedNo</div> <div>Passcode compliantYes</div> <div>Passcode presentNo</div> <div>PlayIntegrity Device Recognition Verdict["MEETS_BASIC_INTEGRITY"]</div> <div>PlayIntegrity last known statusSuccess</div>		

4. La atestación de la API de Play Integrity devuelve estos estados:

- Si el campo **Play Integrity Device Recognition Verdict** contiene **“MEETS_BASIC_INTEGRITY”**, significa que la instancia de Citrix Secure Hub que se ejecuta en el dispositivo supera al menos la integridad básica del sistema.
- Si el campo **Play Integrity Device Recognition Verdict** no contiene **“MEETS_BASIC_INTEGRITY”**, significa que es posible que la instancia de Citrix Secure Hub del dispositivo esté ejecutándose en una versión de Android no reconocida, que tenga un cargador de arranque desbloqueado o que no se haya certificado por el fabricante.
- Si el campo **Play Integrity last known status** contiene **Success**, significa que la atestación de la API de PlayIntegrity se ha ejecutado correctamente.
- Si el campo **Play Integrity last known status** contiene **Failure**, significa que la atestación de la API de PlayIntegrity no se pudo ejecutar.

Nota:

El administrador puede borrar la marca de función que le permite a usted usar SafetyNet antes de que se retire definitivamente SafetyNet Attestation a finales de noviembre de 2023.

Limitaciones

1. Los dispositivos COSU y DO recién inscritos se marcan como no conformes aunque sí lo sean.

La API de Play Integrity se muestra vacía tras la primera vez atestación durante la inscripción de DO, lo que hace que el dispositivo parezca no cumplir con los requisitos. Se trata de un problema conocido de Google. Se publicó DPC Support Lib 20230418 para solucionarlo.

La corrección está disponible en la versión 23.9.0. Hasta entonces, siga estos pasos como solución temporal:

- Borre la marca de función y siga utilizando la API de SafetyNet para continuar utilizando la API de SafetyNet Attestation.
- Cierre la sesión e iníciela de nuevo para activar una atestación después de la inscripción. También puede esperar a la siguiente atestación periódica, que son las 24 horas predeterminadas.

Este problema solo ocurre durante la inscripción. La API de Play Integrity funciona bien después de la inscripción.

2. Los dispositivos WPCOD recién inscritos se marcan como no conformes aunque los dispositivos sí estén conformes. Google está revisando este problema.

Samsung

November 29, 2023

Samsung ofrece varias soluciones compatibles con Citrix Endpoint Management.

Utilice Firebase Cloud Messaging (FCM) para controlar cómo y cuándo los dispositivos Android se conectan al servicio Citrix Endpoint Management. 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 posibilidad de que los usuarios se excluyan de MDM. Citrix Endpoint Management admite los siguientes tipos de autenticación para dispositivos Android inscritos en MDM+MAM. Para obtener información, consulte estos artículos:

- [Autenticación de dominios o dominio y token de seguridad](#)
- [Autenticación con certificado de cliente o certificado y 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 que rara vez se utiliza es el certificado de cliente junto con el 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 [Incorporarse como usuario y configurar 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. Implemente las claves de licencia de Samsung.

4. Configure las directivas de dispositivo para Samsung.
5. Configure las acciones de seguridad para los dispositivos y las aplicaciones. Consulte Acciones de seguridad.

Para conocer los sistemas operativos admitidos, consulte [Sistemas operativos admitidos](#).

Métodos de inscripción admitidos

En la siguiente tabla se indican los métodos de inscripción que Citrix Endpoint Management admite para dispositivos Android:

Método	Compatible
Inscripción manual	Sí
Invitaciones de inscripción	Sí

Para obtener información acerca de la inscripción de dispositivos, consulte [Inscribir dispositivos Android](#).

Implementar las claves de licencia de Samsung

Samsung tiene claves de Enterprise License Management (ELM). Las licencias de Samsung se adquieren en Samsung.

Configurar las directivas de dispositivo para Samsung

Directivas de dispositivo:

—	—	—
[Restricciones de aplicaciones](/en-us/citrix-endpoint-management/policies/app-restrictions-policy.html)	[Desinstalación de aplicaciones](/es-es/citrix-endpoint-management/policies/app-uninstall-policy.html)	[Explorador web](/es-es/citrix-endpoint-management/policies/browser-policy.html)
[Copiar aplicaciones al contenedor de Samsung](/es-es/citrix-endpoint-management/policies/copy-apps-to-samsung-container-policy.html)	[Exchange](/es-es/citrix-endpoint-management/policies/exchange-policy.html)	[Código de acceso](/es-es/citrix-endpoint-management/policies/passcode-policy.html)
[Restricciones](#) |[VPN](#)|

Acciones de seguridad

Android admite las siguientes acciones de seguridad. Para ver una descripción de cada acción de seguridad, consulte [Acciones de seguridad](#).

Bloqueo de aplicaciones	Borrado de aplicaciones	Renovación de certificados
Borrado completo	Localizar	Bloquear
Bloqueo y restablecimiento de contraseña	Notify	Revocar
Borrado selectivo		

Nota:

Para dispositivos que ejecutan Android 6.0 o posterior, la acción de seguridad “Localizar” requiere que el usuario conceda permisos de localización durante la inscripción. El usuario puede optar por no conceder permisos de localización. Si el usuario no concede los permisos durante la inscripción, Citrix Endpoint Management vuelve a solicitarlos cuando envía el comando de localización.

Control de acceso de red

March 1, 2024

Puede utilizar la solución de control de acceso de red (NAC) para ampliar la evaluación de seguridad que ofrece Citrix Endpoint Management para dispositivos Android y Apple. La solución NAC usa la evaluación de seguridad de Citrix Endpoint Management para facilitar y gestionar las decisiones de autenticación. Después de configurar el dispositivo NAC, se aplican las directivas de dispositivo y los filtros NAC que configure en Citrix Endpoint Management.

El uso de Citrix Endpoint Management con una solución NAC agrega QoS y un control más detallado sobre los dispositivos internos de la red. Para obtener un resumen de las ventajas de integrar NAC en Citrix Endpoint Management, consulte [Control de acceso](#).

Citrix admite estas soluciones para la integración en Citrix Endpoint Management:

- NetScaler Gateway
- ForeScout

Citrix no garantiza la integración de otras soluciones NAC.

Con un dispositivo NAC en la red:

- Citrix Endpoint Management admite NAC como una función de seguridad para dispositivos de punto final que sean iOS, Android Enterprise y Android.
- Puede habilitar filtros en Citrix Endpoint Management para establecer dispositivos como conformes o no conformes con NAC, en función de una serie de reglas o propiedades. Por ejemplo:
 - Si un dispositivo administrado en Citrix Endpoint Management no cumple los criterios especificados, Citrix Endpoint Management lo marca como no conforme. Un dispositivo NAC bloquea dispositivos no conformes que haya presentes en su red.
 - Si un dispositivo administrado en Citrix Endpoint Management tiene instaladas aplicaciones no conformes, un filtro NAC puede bloquear la conexión VPN. Como resultado, un dispositivo de usuario no conforme no puede acceder a aplicaciones ni sitios web a través de la VPN.
 - Si utiliza NetScaler Gateway para NAC, puede habilitar el túnel dividido para evitar que el plug-in de NetScaler Gateway envíe tráfico de red innecesario a NetScaler Gateway. Para obtener más información sobre los túneles divididos, consulte [Configurar el túnel dividido](#).

Filtros de conformidad con NAC admitidos

Citrix Endpoint Management admite los siguientes filtros de conformidad para 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 reconectar.

Aplicaciones prohibidas: Comprueba si un dispositivo tiene aplicaciones prohibidas, según se definen en la directiva Acceso a aplicaciones. Para obtener más información acerca de esa directiva, consulte [Directivas de acceso a aplicaciones](#).

Dispositivos inactivos: Comprueba si un dispositivo está inactivo según se define en el parámetro **Umbral de días de inactividad** en **Propiedades de servidor**. Para obtener más información, consulte [Propiedades del servidor](#).

Aplicaciones obligatorias que faltan: Comprueba si en un dispositivo falta alguna aplicación obligatoria, según se definen en la directiva Acceso a aplicaciones.

Aplicaciones no sugeridas: Comprueba si un dispositivo tiene aplicaciones no sugeridas, según se definen en la directiva Acceso a aplicaciones.

Contraseña no conforme: Comprueba si la contraseña del usuario cumple los requisitos de conformidad. En dispositivos iOS y Android, Citrix Endpoint Management puede determinar si la contraseña actual del dispositivo cumple los requisitos de conformidad con la directiva Código de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para definir una contraseña si Citrix Endpoint Management envía una directiva Código de acceso al dispositivo. Antes de que el usuario defina la contraseña, el código de acceso podría no cumplir los requisitos de conformidad.

Dispositivos no conformes: Comprueba si un dispositivo ya no es conforme, según lo definido en la propiedad de dispositivo No conforme. Por regla general, las acciones automatizadas o el uso que terceros hacen de las API de Citrix Endpoint Management modifican esa propiedad.

Estado revocado: Comprueba si el certificado del dispositivo se ha revocado. Un dispositivo revocado no se puede volver a inscribir hasta que se autorice de nuevo.

Dispositivos Android o iOS liberados por root/jailbreak: Comprueba si un dispositivo iOS está liberado por jailbreak o un dispositivo Android está liberado por rooting.

Dispositivos no administrados: Comprueba si Citrix Endpoint Management administra un dispositivo. Por ejemplo, un dispositivo inscrito en MAM o que se haya desinscrito no es un dispositivo administrado.

Nota:

El filtro “Conformidad/No conformidad implícita” establece el valor predeterminado solo en los dispositivos que administra Citrix Endpoint Management. Por ejemplo, los dispositivos que tengan instalada una aplicación bloqueada o que no estén inscritos se marcan como no conformes. El dispositivo NAC bloquea dichos dispositivos en la red.

Introducción a la configuración

Se recomienda configurar los componentes de NAC en el orden indicado.

1. Configure directivas de dispositivo para admitir NAC:

Para dispositivos iOS: Consulte [Configurar la directiva de VPN para admitir NAC](#).

Para dispositivos Android Enterprise: Consulte [Crear una configuración administrada por Android Enterprise para Citrix SSO](#).

Para dispositivos Android: Consulte [Configurar el protocolo Citrix SSO para Android](#).

2. Habilite filtros NAC en Citrix Endpoint Management.

3. Configure una solución NAC:

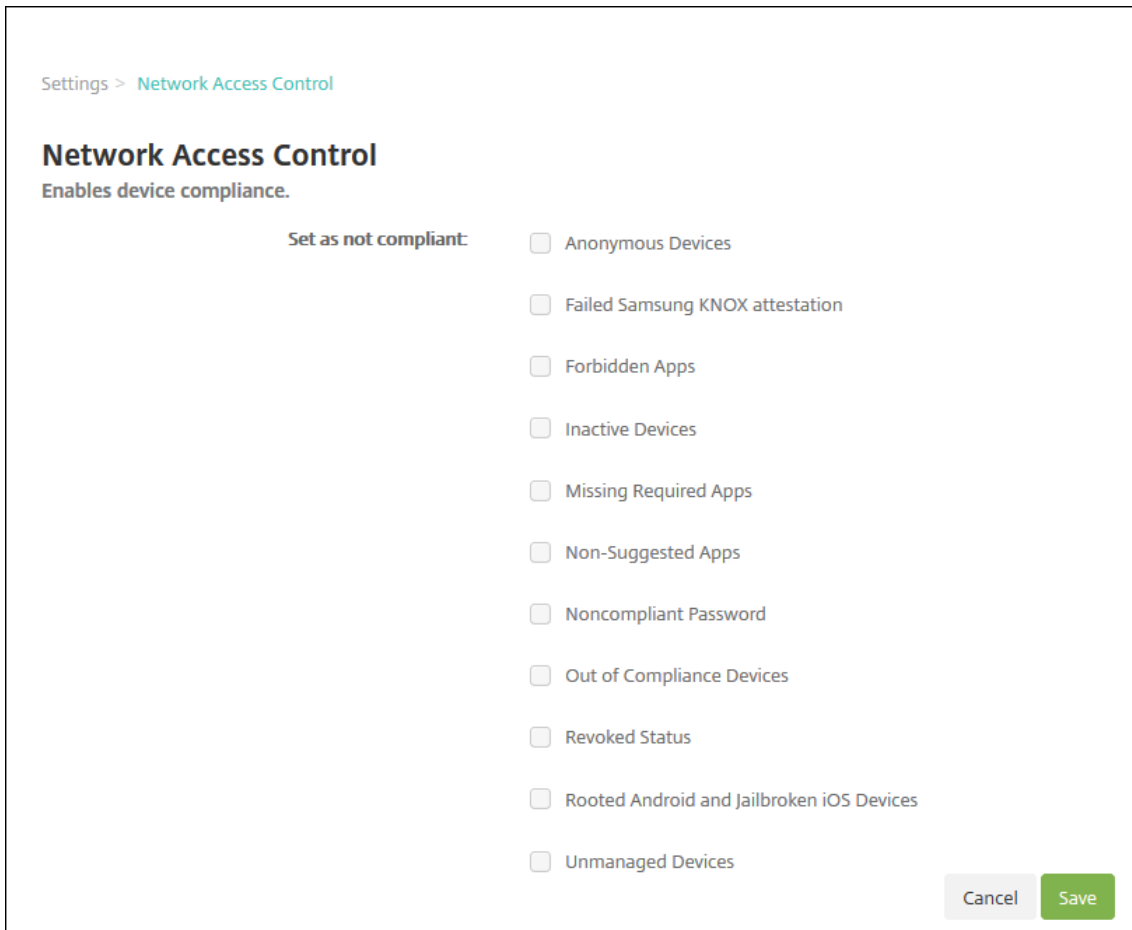
- NetScaler Gateway, detallado en [Actualizar las directivas de NetScaler Gateway para admitir NAC](#)

Requiere instalar 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 de red**.



Settings > Network Access Control

Network Access Control

Enables device compliance.

Set as not compliant:

- ☐ Anonymous Devices
- ☐ Failed Samsung KNOX attestation
- ☐ Forbidden Apps
- ☐ Inactive Devices
- ☐ Missing Required Apps
- ☐ Non-Suggested Apps
- ☐ Noncompliant Password
- ☐ Out of Compliance Devices
- ☐ Revoked Status
- ☐ Rooted Android and Jailbroken iOS Devices
- ☐ Unmanaged Devices

Cancel Save

2. Marque las casillas de los filtros **Establecer como no conforme** 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 de sesiones VPN en el servidor virtual de su VPN.

Estos pasos actualizan un dispositivo NetScaler Gateway con cualquiera de estas características:

- Está integrado en Citrix Endpoint Management.
- O bien, está configurado para VPN, no forma parte del entorno de Citrix Endpoint Management, y puede establecer contacto con Citrix Endpoint Management.

En su servidor de VPN virtual desde una ventana de consola, haga lo siguiente. Las direcciones IP y los FQDN de los comandos y los ejemplos son ficticios.

1. Elimine y desenlace todas las directivas clásicas si las utiliza en su servidor de VPN virtual. Para verificar, escriba:

```
show vpn vservlet <VPN_VServer>
```

Elimine todos los resultados que contengan 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 vservlet <VPN_VServer> -policy <policy_name>
```

2. Cree la directiva de sesión avanzada correspondiente. Para ello, escriba 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. Enlace la directiva a su servidor de VPN virtual. Para ello, escriba lo siguiente.

```
bind vpn vservlet _XM_EndpointManagement -policy vpn_nac -priority 100
```

4. Cree un servidor virtual de autenticación. Para ello, escriba lo siguiente.

```
add authentication vservlet <authentication vservlet name> <service type> <ip address>
```

Por ejemplo: `add authentication vservlet authvs SSL 0.0.0.0`

En el ejemplo, 0.0.0.0 significa que el servidor virtual de autenticación no es público.

5. Enlace un certificado SSL con el servidor virtual. Para ello, escriba lo siguiente.

```
bind ssl vservlet <authentication vservlet name> -certkeyName <Webserver certificate>
```

Por ejemplo: `bind ssl vservlet authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. Asocie un perfil de autenticación al servidor virtual de autenticación desde el servidor de VPN virtual. Primero, cree el perfil de autenticación. Para ello, escriba lo siguiente.

```
add authentication authnProfile <profile name> -authnVsName <authentication vservlet name>
```

Por ejemplo:

```
add authentication authnProfile xm_nac_prof -authnVsName authvs
```

7. Asocie el perfil de autenticación al servidor de VPN virtual. Para ello, escriba 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 desde NetScaler Gateway a un dispositivo. Para ello, escriba 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.

```
1 HTTP/1.1 200 OK
2 < Server: Apache-Coyote/1.1
3 < X-Citrix-Device-State: Non Compliant
4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
5 <!--NeedCopy-->
```

9. Si el paso anterior da el resultado correcto, cree la acción de autenticación web en Citrix Endpoint Management. Primero, cree una expresión de directiva para extraer el ID del dispositivo desde el 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. Para ello, escriba 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\")"
```

El resultado correcto para NAC de Citrix Endpoint Management es `HTTP status 200 OK`. El encabezado `X-Citrix-Device-State` debe tener el valor `Compliant`.

11. Cree una directiva Autenticación con la que asociar la acción. Para ello, escriba 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 de LDAP existente en una directiva avanzada. Para ello, escriba 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 de LDAP. Para ello, escriba lo siguiente.

```
add authentication policylabel <policy_label_name>
```

Por ejemplo: `add authentication policylabel ldap_pol_label`

14. Asocie la directiva de LDAP a la etiqueta de directiva. Para ello, escriba lo siguiente.

```
bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
```

15. Conecte un dispositivo conforme para hacer 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 a asociar con el servidor virtual de autenticación. Escriba el siguiente comando para recuperar la identificación del dispositivo.

```
add authentication loginSchemaPolicy <schema policy> -rule <rule> -action lschema_single_factor_deviceid
```

17. Enlace el servidor virtual de autenticación. Para ello, escriba lo siguiente.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority 100 -gotoPriorityExpression END
```

18. Cree una directiva de LDAP avanzada de autenticación para permitir la conexión 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
```

iOS

November 29, 2023

Para administrar dispositivos iOS en Citrix Endpoint Management, configure un certificado del servicio de notificaciones push de Apple (APNs) proveniente de Apple. Para obtener información, consulte [Certificados APNs](#).

Los perfiles de inscripción determinan si los dispositivos iOS se inscriben en MDM+MAM, con la posibilidad de que los usuarios se excluyan de 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 estos artículos:

- [Autenticación de dominios o dominio y token de seguridad](#)
- [Autenticación con certificado de cliente o certificado y 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 certificados de servidor TLS. Verifique que todos los certificados cumplen los nuevos requisitos de Apple. Consulte la publicación de Apple: <https://support.apple.com/en-us/HT210176>. Para obtener ayuda sobre 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 [Incorporarse como usuario y configurar 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. Configure directivas de dispositivo iOS.
4. Inscribir dispositivos iOS.
5. Configure las acciones de seguridad para los dispositivos y las aplicaciones. Consulte [Acciones de seguridad](#).

Para conocer los sistemas operativos admitidos, consulte [Sistemas operativos admitidos](#).

Compatibilidad con iOS 14

Citrix Endpoint Management y las aplicaciones móviles de Citrix son compatibles con iOS 14, pero no son compatibles actualmente con las nuevas funcionalidades de iOS 14.

En el caso de los dispositivos iOS supervisados, puede demorar las actualizaciones de software hasta 90 días. En la directiva de restricciones para iOS, use estos parámetros:

- **Forzar demora de actualizaciones de software**
- **Demora forzosa para actualizaciones de software**

Consulte [Parámetros de iOS](#). Esos parámetros no están disponibles para dispositivos en modo de inscripción de usuarios ni en modo no supervisado (MDM completo).

Nombres de host de Apple que deben permanecer abiertos

Algunos nombres de host de Apple deben permanecer abiertos para garantizar el correcto funcionamiento de iOS, macOS y el App Store. Bloquear dichos nombres de host puede afectar a la instalación, la actualización y el funcionamiento correcto de iOS, aplicaciones iOS, el funcionamiento de MDM y la inscripción de dispositivos y aplicaciones. Para obtener más información, consulte <https://support.apple.com/en-us/HT201999>.

Métodos de inscripción admitidos

La manera de administrar los dispositivos iOS se especifica en los perfiles de inscripción. Puede elegir entre estos parámetros de inscripción:

- **Inscripción de usuarios de Apple:** Para dispositivos BYOD, ofrece un equilibrio entre la privacidad de datos personales y la seguridad de datos corporativos. Este modo de inscripción está disponible en versión Tech Preview pública. Para habilitar esta función, póngase en contacto con su equipo de asistencia.
- **Inscripción de dispositivos Apple:** Para dispositivos iOS supervisados, con perfiles personales y corporativos por separado en el dispositivo.
- **No administrar dispositivos:** Excluya estos dispositivos de MDM si quiere administrar aplicaciones solamente.

Para obtener más información sobre la creación de perfiles de inscripción, consulte [Perfiles de inscripción](#).

Citrix Endpoint Management admite estos 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 empresas y Apple School Manager (ASM) para centros educativos. Para obtener más información, consulte [Implementar dispositivos mediante los Programas de implementación de Apple](#).

Apple School Manager es un tipo de Programa de implementación de Apple Educación. Consulte [Integrar en funciones de Apple Educación](#).

Use los Programas de implementación de Apple para inscribir en bloque dispositivos iOS, iPadOS y macOS. Puede comprar esos dispositivos directamente de Apple, un distribuidor autorizado de Apple o un operador. Puede usar Apple Configurator para inscribir dispositivos iOS tanto si los adquirió directamente de Apple como si no. Consulte [Inscribir dispositivos Apple en bloque](#).

ID de Apple administrados

La inscripción de usuarios se integra estrechamente en los ID de Apple administrados. Puede crear un ID de Apple administrado de forma manual mediante ABM/ASM o de forma dinámica con Azure Active Directory (AAD).

Para la autenticación no federada, cree ID de Apple administrados mediante ABM/ASM para agregar una cuenta. Para obtener información sobre cómo agregar una cuenta en ABM/ASM, consulte la documentación de Apple en <https://support.apple.com/guide/apple-business-manager/welcome/web> y de ASM en <https://support.apple.com/guide/apple-school-manager/welcome/web>. Se recomienda lo siguiente para evitar pasos adicionales cuando los usuarios se inscriban:

- Al crear un ID de Apple administrado, use una dirección de correo que coincida con la dirección de correo corporativa.
- Establezca el rol del usuario en **Staff**.
- Haga que los usuarios cambien manualmente su contraseña antes de inscribirse. Informe a los usuarios de que recomendamos que usen la misma contraseña que la cuenta corporativa.

Para crear ID de Apple administrados de forma dinámica, configure Citrix Cloud para usar AAD como su proveedor de identidades. Para obtener más información sobre la configuración de Citrix Cloud

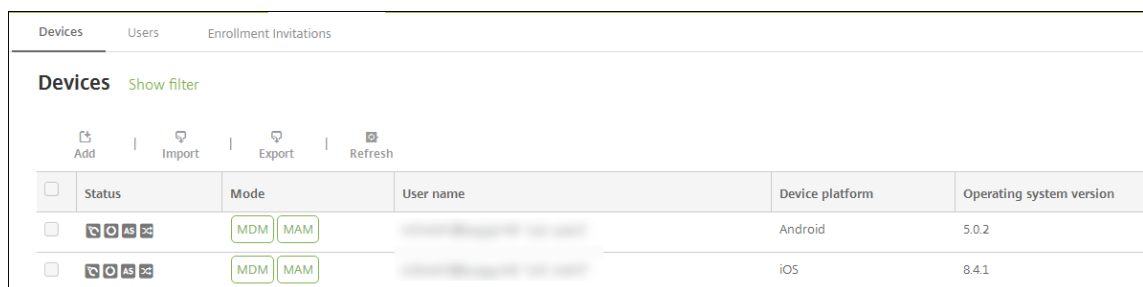
para usar AAD, consulte [Autenticación con Azure Active Directory a través de Citrix Cloud](#). Configure igualmente la autenticación federada en ABM/ASM. Para obtener más información sobre cómo configurar la autenticación federada en ABM o ASM, consulte el [Manual de uso de Apple Business Manager](#) y el [Manual de uso de Apple School Manager](#).

Al crear manualmente los ID de Apple administrados, puede configurar un dominio personalizado para usarlo en lugar del dominio predeterminado. El dominio personalizado que configure reemplaza el dominio existente. Por ejemplo, sus direcciones de correo electrónico corporativas siguen el formato `first.last@company.com`, pero, en su lugar, usted quiere usar `mycompany.website.com` como el dominio del ID de Apple administrado. Al crear el ID de Apple administrado en ABM/ASM, la dirección de correo electrónico pasa a ser `first.last@mycompany.website.com`.

Agregar manualmente un dispositivo iOS

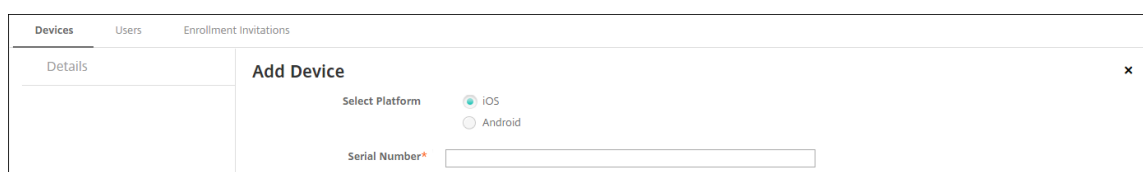
Si quiere agregar manualmente un dispositivo iOS (por ejemplo, para probarlo), siga estos pasos.

1. En la consola de Citrix Endpoint Management, haga clic en **Administrar > Dispositivos**. Aparecerá la página **Dispositivos**.



Status	Mode	User name	Device platform	Operating system version
	MDM MAM	[Redacted]	Android	5.0.2
	MDM MAM	[Redacted]	iOS	8.4.1

2. Haga clic en **Agregar**. Aparecerá la página **Agregar dispositivo**.



3. Configure estos parámetros:
 - **Seleccione la plataforma:** Haga clic en **iOS**.
 - **Número de serie:** Escriba el número de serie del dispositivo.
4. Haga clic en **Agregar**. La tabla **Dispositivos** aparecerá con el dispositivo agregado al final de la lista. Seleccione el dispositivo agregado y, a continuación, en el menú que aparecerá, haga clic en **Modificar** para ver y confirmar los detalles del dispositivo.

Nota:

Cuando se marca la casilla situada junto a un dispositivo, el menú de opciones aparece encima de la lista de dispositivos. Si hace clic en cualquier lugar de la lista, el menú de opciones aparece a la derecha de la lista.

- LDAP configurado
- Si utiliza grupos y usuarios locales:
 - Uno o varios grupos locales.
 - Usuarios locales asignados a grupos locales.
 - Los grupos de entrega se asocian con grupos locales.
- Si usa Active Directory:
 - Los grupos de entrega se asocian con grupos de Active Directory.

Devices	Users	Enrollment Invitations
Device details <div> <div> 1 General 2 Properties 3 User Properties 4 Assigned Policies 5 Apps 6 Media 7 Actions 8 Delivery Groups 9 iOS Profiles 10 iOS Provisioning Profiles 11 Certificates 12 Connections 13 MDM Status </div> <div> <div> <div>Serial Number</div> <div>IMEI/MEID</div> <div>ActiveSync ID</div> <div>WiFi MAC Address</div> <div>Bluetooth MAC Address</div> <div>Device Ownership</div> </div> <div> <div>Strong ID</div> <div>Full Wipe of Device</div> <div>Selective Wipe of Device</div> <div>Lock Device</div> <div>Device Unlock</div> </div> </div> </div>		

5. En la página **General** se muestra una lista de los **identificadores** de dispositivo, como el número de serie y otra información en función del tipo de plataforma. Para **Propietario del dispositivo**, seleccione **Empresa** o **BYOD**.

Asimismo, la página **General** muestra una lista de las propiedades de **Seguridad** de que está dotado el dispositivo (como el ID seguro, el bloqueo del dispositivo y la omisión del bloqueo de activación), así como otra información en función del tipo de plataforma. El campo **Borrado completo del dispositivo** contiene el código PIN del usuario. El usuario debe introducir ese código después de que se haya borrado el dispositivo. Si el usuario no consigue recordar el código, usted puede buscarlo en “Detalles del dispositivo”.

6. La página **Propiedades** muestra una lista de las propiedades de dispositivo que aprovisiona Citrix Endpoint Management. La lista contiene todas las propiedades de 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 saber cuáles son los valores válidos para cada propiedad, consulte el PDF [Valores y nombres de propiedades de dispositivo](#).

Cuando se agrega una propiedad, esta aparece inicialmente en la categoría donde se haya agregado. Después de hacer clic en **Siguiente** y volver a la página **Propiedades**, la propiedad aparece en la lista apropiada.

Para eliminar una propiedad, coloque el cursor sobre ella y, a continuación, haga clic en el aspa (X) situada en el lado derecho. Citrix Endpoint Management elimina inmediatamente el elemento.

7. Las secciones restantes de **Detalles del dispositivo** contienen información resumida del dispositivo.
- **Propiedades de usuario:** Muestra los roles de RBAC, los miembros del grupo, las cuentas de compras por volumen y las propiedades del usuario. Puede retirar una cuenta de compras por volumen desde esta página.
 - **Directivas asignadas:** Muestra la cantidad de directivas implementadas, pendientes y fallidas. También muestra el nombre, el tipo e información de última implementación de cada directiva. Permite restablecer el estado de implementación como pendiente y volver a implementar directivas que el usuario eliminó.
 - **Aplicaciones:** Muestra la cantidad de implementaciones de aplicaciones instaladas, pendientes y erróneas según el último inventario. Indica el nombre de la aplicación, el identificador y el tipo, entre otros datos. Para obtener una descripción de las claves de inventario de iOS y macOS, como **HasUpdateAvailable**, consulte [Mobile Device Management \(MDM\) Protocol](#).
 - **Multimedia:** Muestra la cantidad de implementaciones de archivos multimedia instalados, pendientes y erróneos según el último inventario.
 - **Acciones:** Muestra la cantidad de acciones implementadas, pendientes y erróneas. Indica el nombre de la acción y la hora de la última implementación.
 - **Grupos de entrega:** Muestra la cantidad de grupos de entrega en estado correcto, pendiente y fallido. Indica el nombre del grupo de entrega y la hora de cada implementación. Seleccione un grupo de entrega para ver información más detallada (como el estado, la acción, el canal o el usuario).
 - **Perfiles iOS:** Muestra el último inventario de perfiles iOS, que incluye el nombre, el tipo, la organización y la descripción.
 - **Perfiles de datos de iOS:** Muestra información acerca del perfil de datos utilizado por la empresa para la distribución (como el UUID, la fecha de caducidad y si se administra o no).

- **Certificados:** Muestra la cantidad de certificados válidos, caducados o revocados, incluida la información sobre el tipo, el proveedor, el emisor, el número de serie y los días que quedan hasta la caducidad.
- **Conexiones:** Muestra los estados de la primera y la última conexión. Para cada conexión, aparecen el nombre de usuario, así como la hora de las dos últimas autenticaciones (la penúltima y la última).
- **Estado de MDM:** Muestra información como el estado MDM, la hora del último envío push y la hora de la última respuesta del dispositivo.

Configurar directivas para dispositivos iOS

Use estas directivas para configurar cómo interactúa Citrix Endpoint Management con los dispositivos iOS o iPadOS. En esta tabla se indican todas las directivas de dispositivo disponibles para dispositivos iOS y iPadOS.

— — —	
[[Duplicación AirPlay]](/es-es/citrix-endpoint-management/policies/airplay-mirroring-ios-policy.html)	
[[AirPrint]](/es-es/citrix-endpoint-management/policies/airprint-ios-policy.html)	[[APN]](/es-es/citrix-endpoint-management/policies/apn-policy.html#ios-settings)
[[Acceso a aplicaciones]](/es-es/citrix-endpoint-management/policies/app-access-policy.html)	
[[Atributos de aplicación]](/es-es/citrix-endpoint-management/policies/app-attributes-policy.html)	
[[Configuración de aplicaciones]](/es-es/citrix-endpoint-management/policies/app-configuration-policy.html#ios-settings)	
[[Inventario de aplicaciones]](/es-es/citrix-endpoint-management/policies/app-inventory-policy.html)	
[[Bloqueo de aplicaciones]](/es-es/citrix-endpoint-management/policies/app-lock-policy.html#ios-settings)	[[Desinstalación de aplicaciones]](/es-es/citrix-endpoint-management/policies/app-uninstall-policy.html#ios-and-macos-settings)
[[Notificaciones de aplicaciones]](/es-es/citrix-endpoint-management/policies/apps-notifications-policy.html)	[[Bluetooth]](/es-es/citrix-endpoint-management/policies/bluetooth-policy.html)
[[Calendario (CalDAV)]](/es-es/citrix-endpoint-management/policies/calendar-caldav-ios-policy.html)	
[[Telefonía móvil]](/es-es/citrix-endpoint-management/policies/cellular-policy.html)	[[Contactos (CardDAV)]](/es-es/citrix-endpoint-management/policies/contacts-carddav-ios-policy.html)
	[[Credenciales]](/es-es/citrix-endpoint-management/policies/credentials-policy.html#ios-settings)
[[Nombre del dispositivo]](/es-es/citrix-endpoint-management/policies/device-name-policy.html)	
[[Configuración de la educación]](/es-es/citrix-endpoint-management/policies/education-configuration-policy.html)	[[Exchange]](/es-es/citrix-endpoint-management/policies/exchange-policy.html#ios-settings)
[[Fuente]](/es-es/citrix-endpoint-management/policies/font-policy.html)	[[Diseño de pantalla inicial]](/es-es/citrix-endpoint-management/policies/home-screen-layout-policy.html)
	[[Importar

perfil de iOS y macOS](/es-es/citrix-endpoint-management/policies/import-ios-mac-os-x-profile-policy.html)

[[LDAP](/es-es/citrix-endpoint-management/policies/ldap-policy.html) [[Ubicación](/es-es/citrix-endpoint-management/policies/location-policy.html) [[Mensaje de la pantalla bloqueada](/es-es/citrix-endpoint-management/policies/lock-screen-message-policy.html)

[[Correo](/es-es/citrix-endpoint-management/policies/mail-policy.html) [[Dominios administrados](/es-es/citrix-endpoint-management/policies/managed-domains-policy.html) [[Máximo de usuarios residentes](/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 la red](/es-es/citrix-endpoint-management/policies/network-usage-policy.html)

[[Información sobre la organización](/es-es/citrix-endpoint-management/policies/organization-info-policy.html) [[Actualización de 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 de código de acceso](/es-es/citrix-endpoint-management/policies/passcode-lock-grace-period.html) [[Hotspot personal](/es-es/citrix-endpoint-management/policies/personal-hotspot-policy.html) [[Eliminación de perfiles](/es-es/citrix-endpoint-management/policies/profile-removal-policy.html)

[[Perfil de datos](/es-es/citrix-endpoint-management/policies/provisioning-profile-policy.html)

[[Eliminación de perfiles de datos](/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/policies/restrictions-policy.html#ios-settings)

[[Itinerancia](/es-es/citrix-endpoint-management/policies/roaming-policy.html) [[SCEP](/es-es/citrix-endpoint-management/policies/scep-policy.html)

[[Cuenta SSO](/es-es/citrix-endpoint-management/policies/sso-account-policy.html) [[Almacén](/es-es/citrix-endpoint-management/policies/store-policy.html) [[Calendarios suscritos](/es-es/citrix-endpoint-management/policies/subscribed-calendars-policy.html)

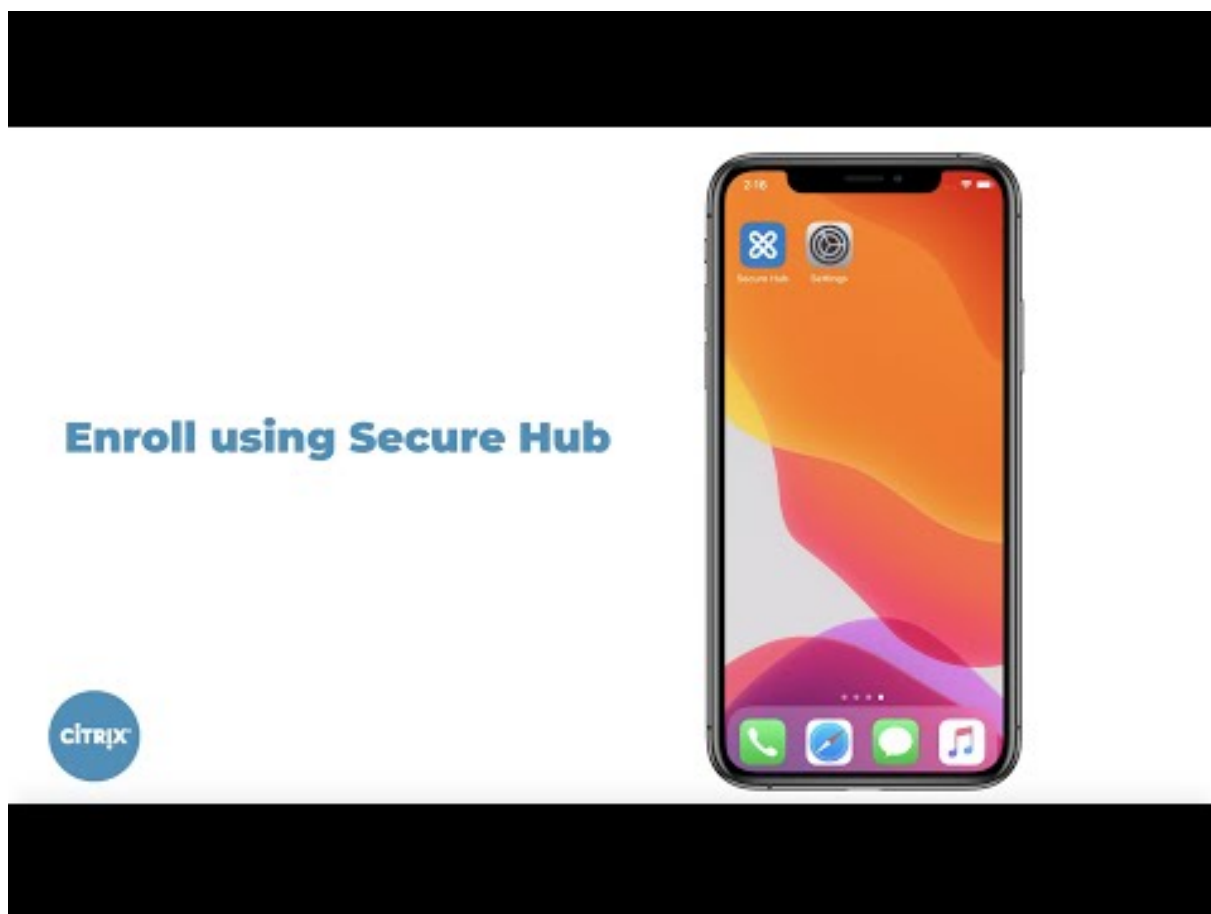
[[Términos y condiciones](/es-es/citrix-endpoint-management/policies/terms-and-conditions-policy.html) [[VPN](/es-es/citrix-endpoint-management/policies/vpn-policy.html#ios-settings)

[[Fondo de pantalla](/es-es/citrix-endpoint-management/policies/wallpaper-policy.html)

[Filtro de contenido web](#) | [Clip web](#) | |

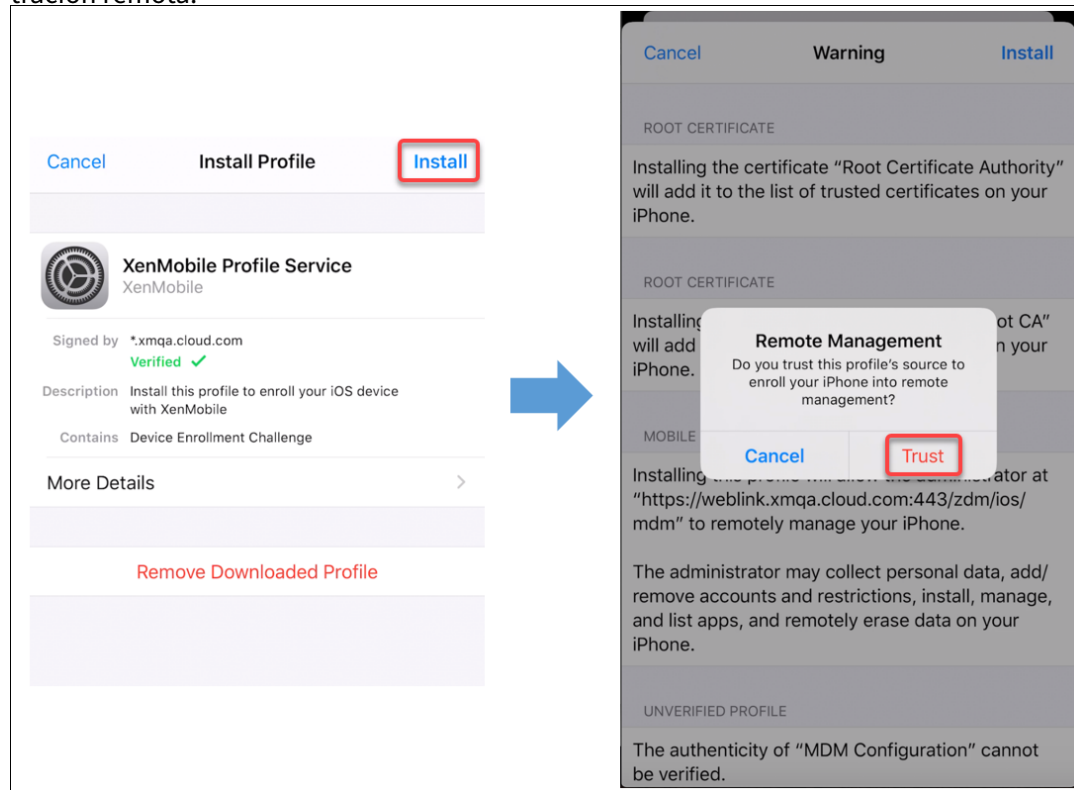
Inscribir dispositivos iOS

En esta sección se muestra cómo los usuarios inscriben dispositivos iOS (12.2 o una versión posterior) en Citrix Endpoint Management. Para obtener más información sobre la inscripción en iOS, consulte este vídeo:



1. Vaya a la tienda Apple en su dispositivo iOS, descargue la aplicación Citrix Secure Hub y, a continuación, toque la aplicación.
2. Cuando se le pida instalar la aplicación, toque **Siguiente** y, a continuación, toque **Instalar**.
3. Después de que Citrix Secure Hub se instale, toque **Abrir**.
4. Introduzca las credenciales de empresa, como el nombre del servidor de Citrix Endpoint Management de su empresa, el nombre principal de usuario (UPN) o su dirección de correo electrónico. A continuación, haga clic en **Siguiente**.
5. Toque **Sí, inscribirlo** para inscribir el dispositivo iOS.
6. Aparecerá una lista de los datos que Citrix Endpoint Management recopila. Haga clic en **Siguiente**. Aparecerá una explicación del modo en que una organización utiliza esos datos. Haga clic en **Siguiente**.
7. Después de escribir las credenciales, toque **Permitir** cuando se le pida para descargar el perfil de configuración. Después de descargar el perfil de configuración, toque **Cerrar**.
8. En la configuración del dispositivo, instale el perfil de XenMobile.
 - Vaya a **Configuración > General > Perfil > XenMobile Profile Service** y toque **Instalar** para agregar el perfil.
 - En la ventana de notificaciones, toque **Confiar** para inscribir el dispositivo en la adminis-

tración remota.



9. Una vez hecha correctamente la inscripción, abra Citrix Secure Hub. Si inscribe dispositivos en MDM+MAM: Una vez que se hayan validado las credenciales, cree el PIN de Citrix y confírmelo cuando se le solicite.
10. Una vez completado el flujo de trabajo, el dispositivo está inscrito. Ahora, puede acceder al almacén de aplicaciones para ver las aplicaciones que puede instalar en el dispositivo iOS.

Acciones de seguridad

La inscripción de dispositivos para iOS permite estas acciones de seguridad. Para ver una descripción de cada acción de seguridad, consulte [Acciones de seguridad](#).

- Omisión del bloqueo de activación
- Bloqueo de aplicaciones
- Borrado de aplicaciones
- Bloqueo de activación de ASM
- Renovación de certificados
- Desactivar restricciones
- Habilitar o inhabilitar el modo perdido
- Habilitar o inhabilitar el seguimiento
- Borrado completo

- Localizar
- Bloquear
- Hacer sonar
- Solicitar o detener la duplicación AirPlay
- Reiniciar o apagar
- Revocar o autorizar
- Borrado selectivo
- Desbloquear

La inscripción de usuarios para iOS permite estas acciones de seguridad:

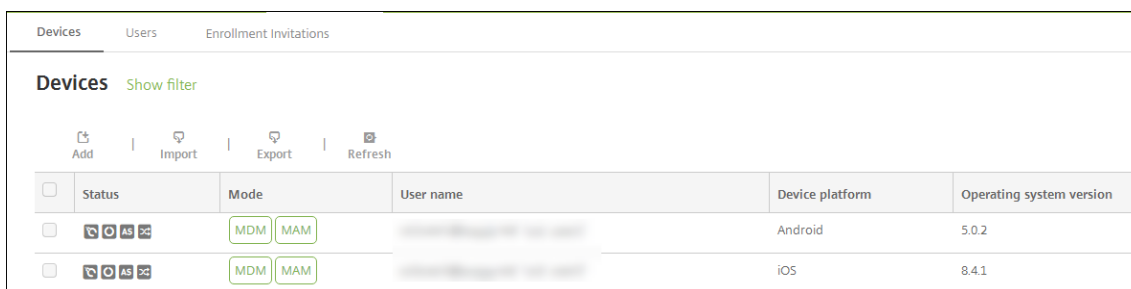
- Revocar
- Bloquear
- Borrado selectivo
- Renovación de certificados

Bloquear dispositivos iOS

Puede bloquear un dispositivo iOS perdido y mostrar un mensaje y un número de teléfono en la pantalla de bloqueo.

Para que se muestren un mensaje y un teléfono en un dispositivo bloqueado, establezca la directiva [Código de acceso](#) en **true** en la consola de Citrix Endpoint Management. En vez de ello, los usuarios pueden habilitar manualmente el código de acceso en el dispositivo.

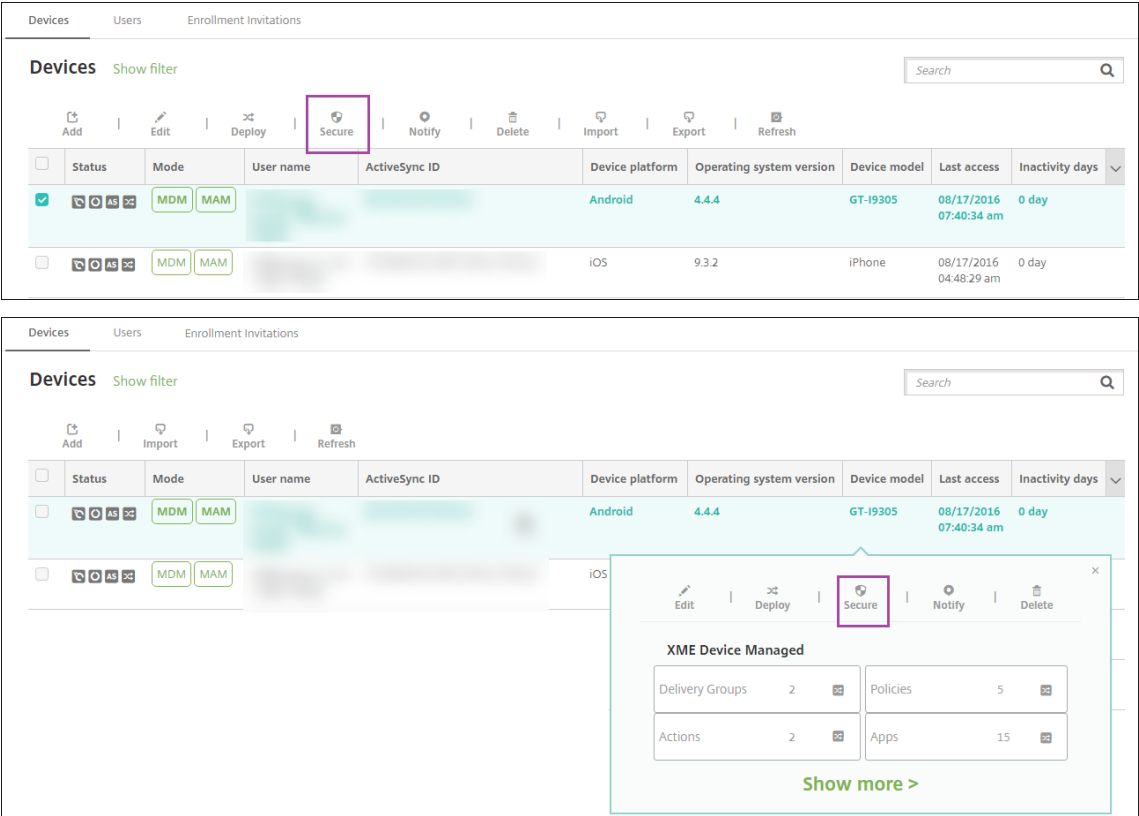
1. Haga clic en **Administrar > Dispositivos**. Aparecerá la página **Dispositivos**.



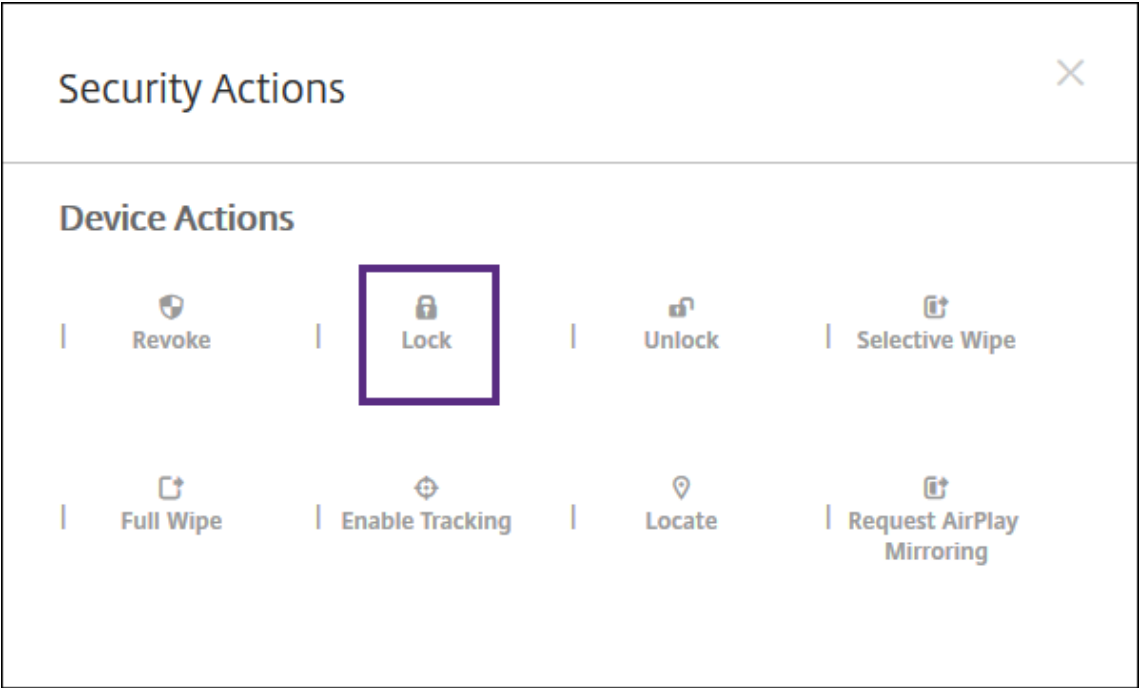
	Status	Mode	User name	Device platform	Operating system version
<input type="checkbox"/>		MDM MAM	[Redacted]	Android	5.0.2
<input type="checkbox"/>		MDM MAM	[Redacted]	iOS	8.4.1

2. Seleccione el dispositivo iOS que quiere bloquear.

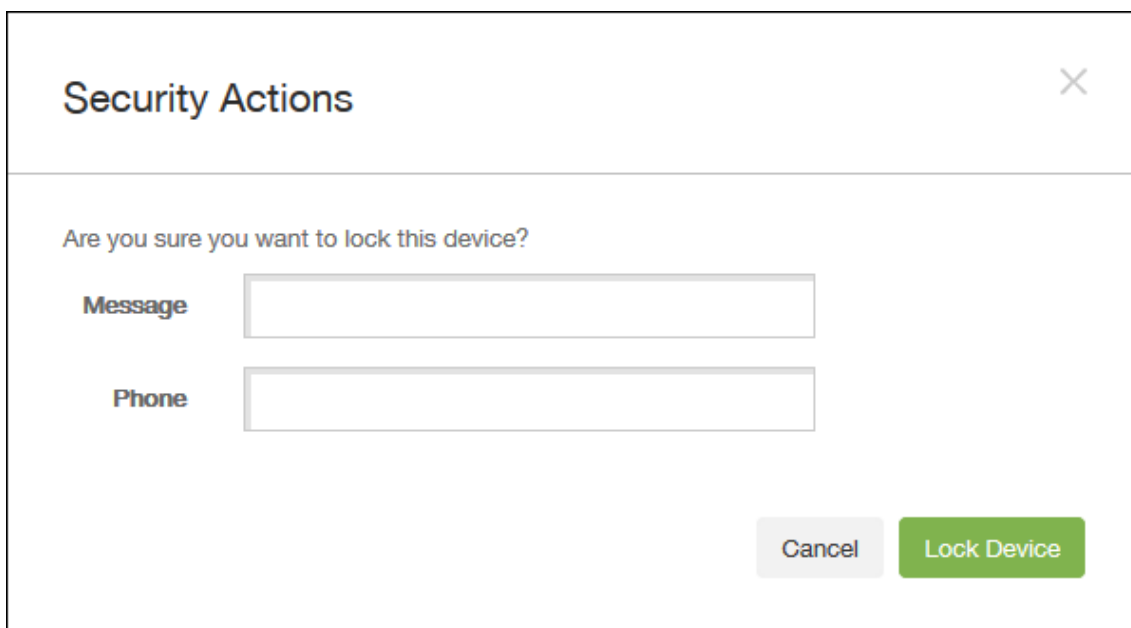
Marque la casilla situada junto a un dispositivo para que el menú de opciones aparezca encima de la lista de dispositivos. Haga clic en cualquier lugar de la lista para que el menú de opciones aparezca a la derecha de la lista.



3. En el menú de opciones, seleccione **Proteger**. Aparecerá el cuadro de diálogo **Acciones de seguridad**.



4. Haga clic en **Bloquear**. Aparecerá el cuadro de confirmación **Acciones de seguridad**.



Security Actions ✕

Are you sure you want to lock this device?

Message

Phone

Cancel Lock Device

5. Si lo prefiere, puede introducir el mensaje y el número de teléfono que aparecerán en la pantalla de bloqueo del dispositivo.

iOS agrega 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 mostrará un mensaje del tipo “Llamar al propietario” en la pantalla de bloqueo del dispositivo.

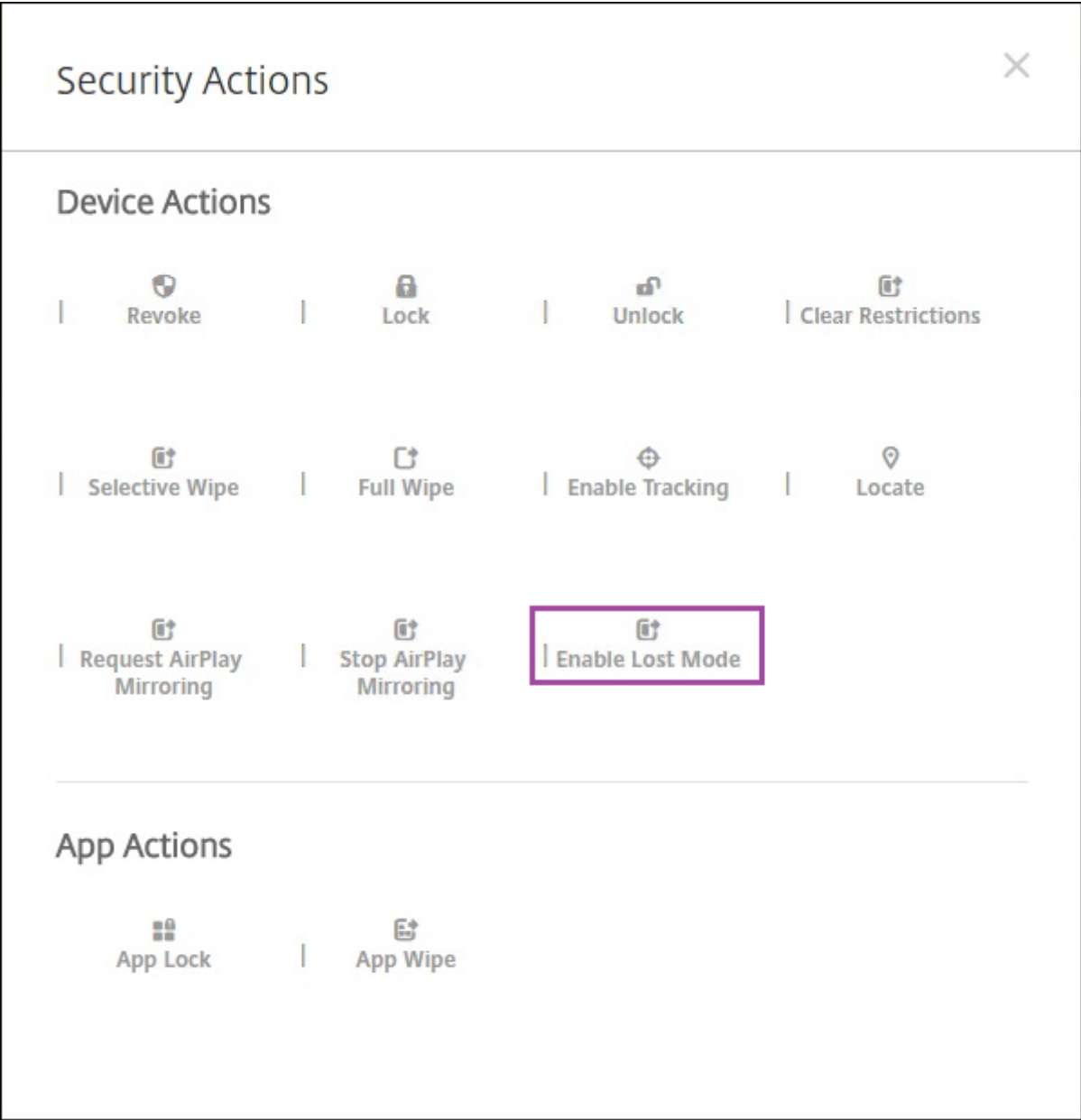
6. Haga clic en **Bloquear dispositivo**.

Colocar dispositivos iOS en modo perdido

La propiedad de dispositivo “modo perdido” de Citrix Endpoint Management coloca un dispositivo iOS en el modo Perdido (de Apple). A diferencia del modo Perdido gestionado de Apple, el modo perdido de Citrix Endpoint Management no requiere que el usuario configure **Buscar mi iPhone o iPad** ni habilite los servicios de localización geográfica de Citrix Secure Hub para permitir la localización de su dispositivo.

En el modo Perdido de Citrix Endpoint Management, solo Citrix Endpoint Management puede desbloquear el dispositivo (en cambio, si usa la funcionalidad de bloqueo del dispositivo de Citrix Endpoint Management, los usuarios pueden desbloquear el dispositivo directamente con un código PIN que proporcione).

Para habilitar o inhabilitar el modo perdido, vaya a **Administrar > Dispositivos**, elija un dispositivo iOS supervisado y 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 el modo perdido.

Security Actions

Are you sure you want to enable the lost mode for this device?

Message ?

Phone number ?

Footnote ?

Cancel Enable Lost Mode

App Actions

App Lock | App Wipe

Para comprobar el estado del modo perdido, utilice cualquiera de los siguientes métodos:

- En la ventana **Acciones de seguridad**, compruebe si el botón es **Inhabilitar modo perdido**.
- Desde **Administrar > Dispositivos**, en la ficha **General**, en **Seguridad**, consulte la última acción de “Habilitar modo perdido” o “Inhabilitar modo perdido”.

Devices	Users	Enrollment Invitations
<div>Device details</div> <div><div>1 General</div><div>2 Properties</div><div>3 User Properties</div><div>4 Assigned Policies</div><div>5 Apps</div><div>6 Actions</div><div>7 Delivery Groups</div><div>8 iOS Profiles</div><div>9 iOS Provisioning Profiles</div><div>10 Certificates</div><div>11 Connections</div><div>12 MDM Status</div></div>		
		<div>Device Shutdown</div> <div>No device shutdown.</div>
		<div>Device locate</div> <div>No device locate .</div>
		<div>Device Enable Tracking</div> <div>No device enable tracking.</div>
		<div>Device Disown</div> <div>No device disown.</div>
		<div>DEP Activation Lock</div> <div>No DEP device activation lock.</div>
		<div>Activation Lock Bypass</div> <div>No device activation lock bypass.</div>
		<div>Device Clear Restrictions</div> <div>No Clear Restrictions.</div>
		<div>Device App Wipe</div> <div>No device App Wipe.</div>
		<div>Device App Lock</div> <div>No device App Lock.</div>
		<div>Request AirPlay Mirroring</div> <div>No request AirPlay mirroring.</div>
		<div>Stop AirPlay Mirroring</div> <div>No stop AirPlay mirroring.</div>
		<div>Enable Lost Mode</div> <div>No lost mode enabled.</div>
		<div>Disable Lost Mode</div> <div>No lost mode disabled.</div>
		<div>Next ></div>

- Desde **Administrar > Dispositivos**, en la ficha **Propiedades**, compruebe que el valor del parámetro **Modo perdido de MDM habilitado** es correcto.

Devices	Users	Enrollment Invitations
<div>Device details</div> <div><div>1 General</div><div>2 Properties</div><div>3 User Properties</div><div>4 Assigned Policies</div><div>5 Apps</div><div>6 Actions</div><div>7 Delivery Groups</div><div>8 iOS Profiles</div><div>9 iOS Provisioning Profiles</div><div>10 Certificates</div><div>11 Connections</div><div>12 MDM Status</div></div>		
		<div>Activation lock enabled</div> <div>No</div>
		<div>Hardware encryption capabilities</div> <div>Block and file levels encryption</div>
		<div>Internal storage encrypted</div> <div>No</div>
		<div>Jailbroken/Rooted</div> <div>No</div>
		<div>MDM lost mode enabled</div> <div>No</div>
		<div>Passcode compliant</div> <div>Yes</div>
		<div>Passcode compliant with configuration</div> <div>Yes</div>
		<div>Passcode present</div> <div>No</div>
		<div>Supervised</div> <div>No</div>
		<div>– Storage space</div> <div>Add</div>
		<div>Available storage space</div> <div>10.92 GB</div>
		<div>Total storage space</div> <div>12.28 GB</div> <div>×</div>
		<div>– System information</div> <div>Add</div>
		<div>Active iTunes account</div> <div>Yes</div>
		<div>Cloud backup enabled</div> <div>No</div>
		<div>Back</div> <div>Next ></div>

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 **Acciones** no incluye las siguientes acciones automatizadas: **Revocar el dispositivo**, **Borrar datos selectivamente del dispositivo** ni **Borrar datos completamente del dispositivo**.
- En **Administrar > Dispositivos**, la lista **Acciones de seguridad** ya no incluye las acciones de dispositivo **Revocar** ni **Borrado selectivo**. En cambio, puede llevar a cabo un **Borrado completo**, si fuera necesario.

iOS agrega las palabras “iPad perdido” a lo que escriba en el campo **Mensaje** de la pantalla **Acciones de seguridad**.

Si deja el campo **Mensaje** vacío y proporciona un número de teléfono, Apple mostrará un mensaje del tipo “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 o iPad que evita la reactivación de un dispositivo supervisado que se haya perdido o haya sido robado. El bloqueo de activación requiere el ID de Apple del usuario y la contraseña para desactivar Buscar mi iPhone o iPad, borrar el dispositivo o volver a activarlo. Para los dispositivos propiedad de la organización, es necesario omitir un bloqueo de activación para, por ejemplo, restablecer o reasignar dispositivos.

Para habilitar el bloqueo de activación, debe configurar e implementar la directiva 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 en un bloqueo de activación, debe emitir la acción de seguridad “Omisión del bloqueo de activación” desde la consola de Citrix Endpoint Management.

Por ejemplo, si un usuario devuelve un teléfono perdido o si usted quiere configurar uno antes o después de un borrado completo, cuando el teléfono le solicite las credenciales de la cuenta del App Store de Apple, omita ese paso mediante la acción de seguridad Omisión del bloqueo de activación.

Requisitos del dispositivo para la omisión del bloqueo de activación

- Supervisado a través de Apple Configurator o del Programa de implementación de Apple
- Configurado con una cuenta de iCloud
- Buscar mi iPhone o iPad habilitado
- Inscrito en Citrix Endpoint Management
- La directiva de opciones de MDM, con el bloqueo de activación habilitado, implementada en los dispositivos

Para omitir un bloqueo de activación antes de emitir el borrado completo de un dispositivo:

1. Vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Proteger** y, a continuación, haga clic en **Omisión del bloqueo de activación**.

2. Borre los datos del dispositivo. La pantalla del bloqueo de activación no aparece durante la configuración del dispositivo.

Para omitir un bloqueo de activación después de emitir el borrado completo de un dispositivo:

1. Borre los datos del dispositivo o restablézcalo. La pantalla del 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 **Omisión del bloqueo de activación**.
3. Toque el botón Atrás del dispositivo. Aparecerá la pantalla de inicio.

Tenga en cuenta lo siguiente:

- Recomiende a los usuarios que no desactiven Buscar mi iPhone o iPad. No realice ningún borrado completo desde el dispositivo. En cualquiera de estos casos, se pide al usuario que escriba la contraseña de la cuenta de iCloud. Tras validar la cuenta, el usuario no verá la pantalla “Activar iPhone o iPad” después de borrar todo el contenido y toda la configuración.
- Para un dispositivo con un código de omisión del bloqueo de activación generado y con el bloqueo de activación habilitado: si no puede omitir la página “Activar iPhone o iPad” después de un borrado completo, no necesita eliminar el dispositivo de Citrix Endpoint Management. Usted o el usuario pueden ponerse en contacto con la asistencia técnica de Apple para desbloquear el dispositivo directamente.
- Durante un inventario de hardware, Citrix Endpoint Management busca en el dispositivo un código de omisión del bloqueo de activación. Si hay disponible un código de omisión, el dispositivo lo envía a Citrix Endpoint Management. A continuación, para quitar ese código de omisión del dispositivo, envíe la acción de seguridad “Omisión del bloqueo de activación” desde la consola de Citrix Endpoint Management. En ese momento, Citrix Endpoint Management y Apple tienen el código de omisión requerido para desbloquear el dispositivo.
- La acción de seguridad “Omisión del bloqueo de activación” necesita la disponibilidad de un servicio de Apple. Si la acción no funciona, puede desbloquear un dispositivo de una de estas maneras:
 - En el dispositivo, debe introducir manualmente las credenciales de la cuenta iCloud.
 - Deje en blanco el campo del nombre de usuario y escriba el código de omisión en el campo de la contraseña. Para buscar el código de omisión, vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Modificar > Propiedades**. El **Código de omisión del bloqueo de activación** se encuentra en el apartado **Información de seguridad**.

macOS

November 29, 2023

Para administrar dispositivos macOS en Citrix Endpoint Management, configure un certificado del servicio de notificaciones push de Apple (APNs) proveniente de Apple. Para obtener información, consulte [Certificados APNs](#).

Citrix Endpoint Management inscribe los dispositivos macOS en MDM. Citrix Endpoint Management admite los siguientes tipos de autenticación de inscripción para dispositivos macOS en MDM.

- Dominio
- Dominio y contraseña de un solo uso
- URL de invitación y contraseña de un solo uso

Requisitos para certificados de confianza en macOS 15:

Apple tiene nuevos requisitos para certificados de servidor TLS. Verifique que todos los certificados cumplen los nuevos requisitos de Apple. Consulte la publicación de Apple: <https://support.apple.com/en-us/HT210176>. Para obtener ayuda sobre 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 [Incorporarse como usuario y configurar 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. Configure directivas de dispositivo macOS.
4. Inscriba los dispositivos macOS.
5. Configure las acciones de seguridad para los dispositivos y las aplicaciones. Consulte [Acciones de seguridad](#).

Para conocer los sistemas operativos admitidos, consulte [Sistemas operativos admitidos](#).

Nombres de host de Apple que deben permanecer abiertos

Algunos nombres de host de Apple deben permanecer abiertos para garantizar el correcto funcionamiento de iOS, macOS y el App Store. Bloquear dichos nombres de host puede afectar a la instalación, la actualización y el funcionamiento correcto de iOS, aplicaciones iOS, el funcionamiento de MDM y la inscripción de dispositivos y aplicaciones. Para obtener más información, consulte <https://support.apple.com/en-us/HT201999>.

Métodos de inscripción admitidos

En la siguiente tabla se indican los métodos de inscripción que Citrix Endpoint Management admite para los dispositivos macOS:

Método	Compatible
Programa de implementación de Apple	Sí
Apple School Manager	Sí
Apple Configurator	No
Inscripción manual	Sí
Invitaciones de inscripción	Sí

Apple dispone de programas de inscripción de dispositivos para las cuentas Empresas y Educación. Para las cuentas Business, debe inscribirse en el Programa de implementación de Apple con el fin de usarlo para inscribir y administrar dispositivos en Citrix Endpoint Management. Ese programa está pensado para dispositivos iOS, macOS y Apple TV. Consulte [Implementar dispositivos mediante el Programa de implementación de Apple](#).

Para las cuentas Educación, cree una cuenta de Apple School Manager. Apple School Manager unifica el programa de implementación y las compras por volumen. Apple School Manager es un tipo de Programa de implementación de Apple Educación. Consulte [Integrar en funciones de Apple Educación](#).

Puede utilizar el Programa de implementación de Apple para inscribir en bloque dispositivos iOS, macOS y Apple TV. Puede comprar esos dispositivos directamente de Apple, un distribuidor autorizado de Apple o un proveedor.

Configurar directivas de dispositivo macOS

Use estas directivas para configurar cómo interactúa Citrix Endpoint Management con los dispositivos macOS. En esta tabla se indican todas las directivas de dispositivo disponibles para dispositivos macOS.

Duplicación AirPlay	Inventario de aplicaciones	Desinstalación de aplicaciones
Calendario (CalDAV)	Contactos (CardDAV)	Credenciales
Nombre del dispositivo	Exchange	FileVault

Firewall	Fuente	Importar perfil de iOS y macOS
LDAP	Correo	Red
Actualización de 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 y directamente desde sus dispositivos.

- **Enviar una invitación de inscripción a los usuarios:** Este método de inscripción permite definir uno de estos modos de seguridad de inscripción para dispositivos macOS:
 - Nombre de usuario y contraseña
 - Nombre de usuario y PIN
 - Autenticación de dos factores

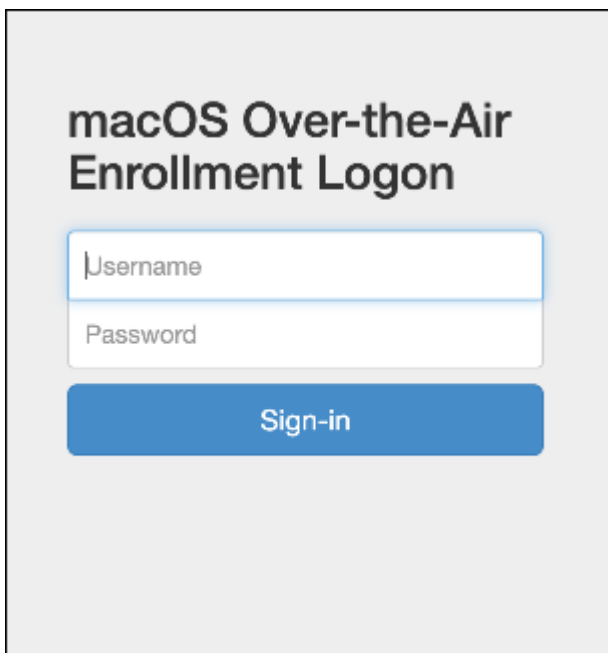
Cuando el usuario siga las instrucciones de la invitación a la inscripción, aparecerá una pantalla de inicio de sesión con el nombre de usuario ya rellenado.

- **Enviar un enlace de inscripción a los usuarios:** Este método de inscripción para dispositivos macOS envía a los usuarios un enlace de inscripción, que pueden abrir en los exploradores Safari o Chrome. A continuación, el usuario se inscribe suministrando su nombre de usuario y contraseña.

Para impedir que se use un enlace de inscripción para dispositivos macOS, defina la propiedad de servidor **Enable macOS OTAE** en **False**. Como resultado, los usuarios de macOS solo podrán inscribirse mediante una invitación de inscripción.

Enviar una invitación de inscripción a los usuarios macOS

1. Agregue una invitación para la inscripción de usuarios de macOS. Consulte [Invitaciones de inscripción](#).
2. Cuando los usuarios reciban la invitación y hagan clic en el enlace, aparecerá la siguiente pantalla en el explorador Safari. Citrix Endpoint Management rellena el nombre de usuario. Si eligió **Dos factores** como modo de seguridad de inscripción, aparecerá un campo adicional.

The image shows a login screen for macOS Over-the-Air Enrollment. It has a light gray background. At the top, the text "macOS Over-the-Air Enrollment Logon" is displayed in a bold, dark font. Below this, there are two input fields: the first is labeled "Username" and the second is labeled "Password". Both fields are white with a light blue border. Below the password field is a blue button with the text "Sign-in" in white.

3. Los usuarios deben instalar certificados según sea necesario. La solicitud a los usuarios para instalar certificados depende de si se ha configurado un certificado SSL público de confianza y un certificado de firma digital público de confianza para macOS. Para obtener información acerca de los certificados, consulte [Certificados y autenticación](#).
4. Los usuarios proporcionan las credenciales solicitadas.

Se instalan las directivas de dispositivos Mac. Ahora ya puede iniciar la administración de dispositivos macOS con Citrix Endpoint Management del mismo modo en que administra dispositivos móviles.

Enviar un enlace de inscripción a los usuarios macOS

1. Envíe el enlace de inscripción <https://serverFQDN:8443/instanceName/macOS/ota>, que los usuarios abrirán en los exploradores web Safari o Chrome.
 - **serverFQDN** es el nombre de dominio completo del servidor que ejecuta Citrix Endpoint Management.
 - El puerto **8443** es el puerto seguro predeterminado. Si ha configurado otro puerto, indique ese puerto, en lugar de 8443.
 - El elemento **instanceName** a menudo se muestra como **zdm** y es el nombre que se especificó durante la instalación del servidor.

Para obtener más información acerca del envío de enlaces de instalación, consulte [Para enviar un enlace de instalación](#).

2. Los usuarios deben instalar certificados según sea necesario. Si ha configurado un certificado SSL público de confianza y un certificado de firma digital público de confianza para iOS y macOS, los usuarios verán el mensaje que pide instalar los certificados. Para obtener información acerca de los certificados, consulte [Certificados y autenticación](#).
3. Los usuarios inician sesión en su Mac.

Se instalan las directivas de dispositivos Mac. Ahora ya puede iniciar la administración de dispositivos macOS con Citrix Endpoint Management del mismo modo en que administra dispositivos móviles.

Acciones de seguridad

macOS admite las siguientes acciones de seguridad. Para ver una descripción de cada acción de seguridad, consulte [Acciones de seguridad](#).

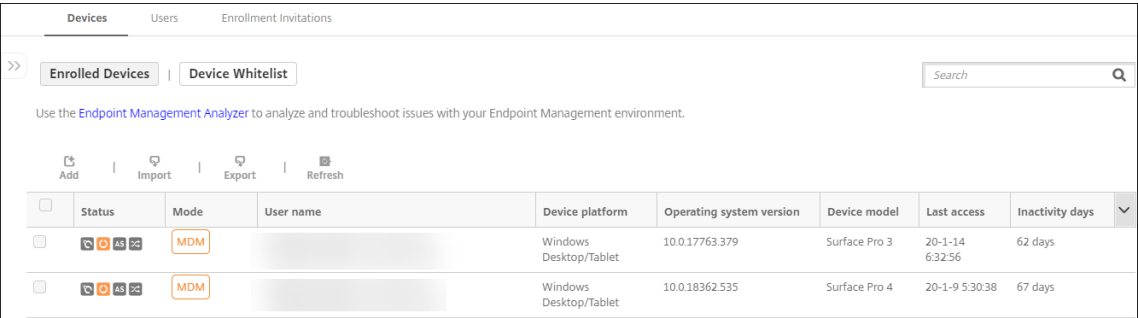
Revocar	Bloquear	Borrado selectivo
Borrado completo	Renovación de certificados	Rotar clave personal de recuperación

Bloquear dispositivos macOS

Puede bloquear de forma remota dispositivos macOS perdidos. Citrix Endpoint Management bloquea el dispositivo. A continuación, genera un código PIN y lo establece en el dispositivo. Para acceder al dispositivo, el usuario deberá teclear ese código PIN. Use el comando **Cancelar bloqueo de dispositivo** para quitar el bloqueo desde la consola de Citrix Endpoint Management.

Puede utilizar la directiva [Código de acceso](#) para configurar más parámetros asociados al código PIN. Para obtener más información, consulte [Parámetros de macOS](#).

1. Haga clic en **Administrar > Dispositivos**. Aparecerá la página **Dispositivos**.



2. Seleccione el dispositivo macOS que quiere bloquear.

Marque la casilla situada junto a un dispositivo para que el menú de opciones aparezca encima de la lista de dispositivos. También puede hacer clic en cualquier otro elemento de la lista para mostrar el menú de opciones en el lado derecho de la lista.

DevicesUsersEnrollment Invitations

>>Enrolled DevicesDevice Whitelist

Search

Use the [Endpoint Management Analyzer](#) to analyze and troubleshoot issues with your Endpoint Management environment.

Add

Edit

Secure

Notify

Delete

Import

Export

Refresh

<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	
<input type="checkbox"/>		MDM		Windows Desktop/Tablet	10.0.17763.379	Surface Pro 3	20-1-14 6:32:56	62 days	
<input type="checkbox"/>		MDM		Windows Desktop/Tablet	10.0.18362.535	Surface Pro 4	20-1-9 5:30:38	67 days	

DevicesUsersEnrollment Invitations

>>Enrolled DevicesDevice Whitelist

Search

Use the [Endpoint Management Analyzer](#) to analyze and troubleshoot issues with your Endpoint Management environment.

Add

Import

Export

Refresh

<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	
<input type="checkbox"/>		MDM		Windows Desktop/Tablet	10.0.17763.379	Surface Pro 3	20-1-14 6:32:56	62 days	
<input type="checkbox"/>		MDM		Windows Desktop/Tablet	10.0.18362.535	Surface Pro 4	20-1-9 5:30:38	67 days	
<input type="checkbox"/>		MDM		Windows Desktop/Tablet	10.0.17134.1365	HVM domU	20-3-16 15:38:19	0 day	
<input type="checkbox"/>		MDM		Android	10	SM-G970F	20-2-11 19:36:49	34 days	
<input type="checkbox"/>		MDM		macOS	10.12.3	MacBook Air	20-2-11 20:15:18	33 days	
<input type="checkbox"/>		MDM		Android					
<input type="checkbox"/>		WEM		Windows Desktop/Tablet					
<input type="checkbox"/>		MDM WEM		Windows Desktop/Tablet					

Showing 1 - 8 of 8 itemsItems per page: 10

Edit

Secure

Notify

Delete

Device Unmanaged

Delivery Groups0

Policies0

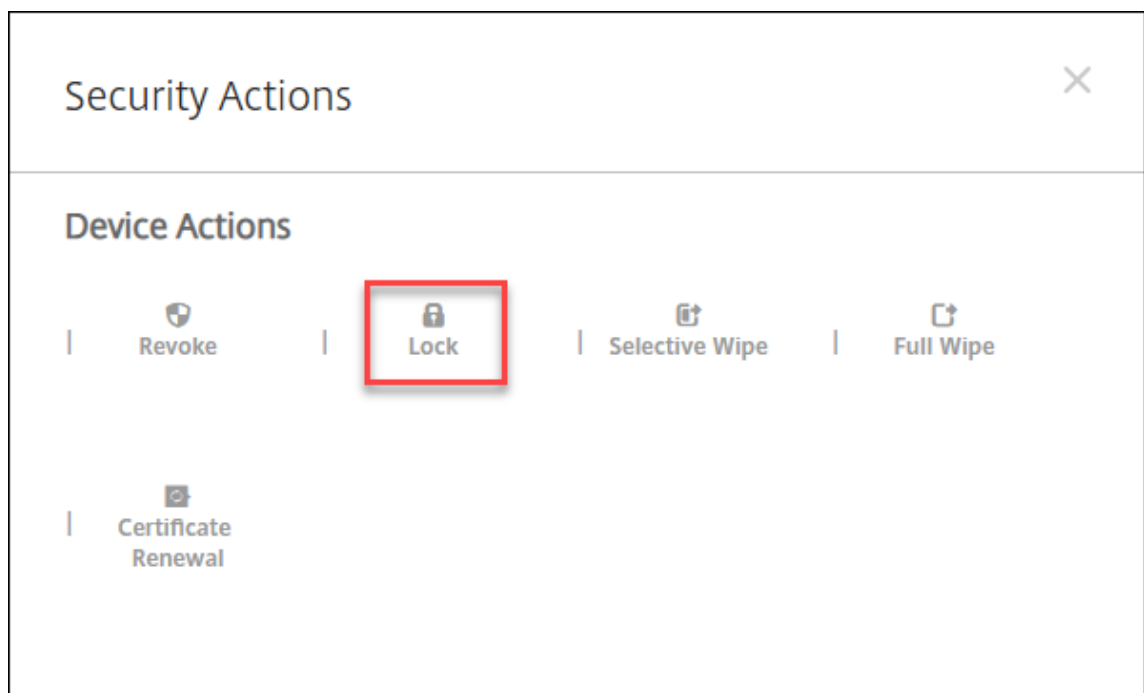
Actions0

Apps0

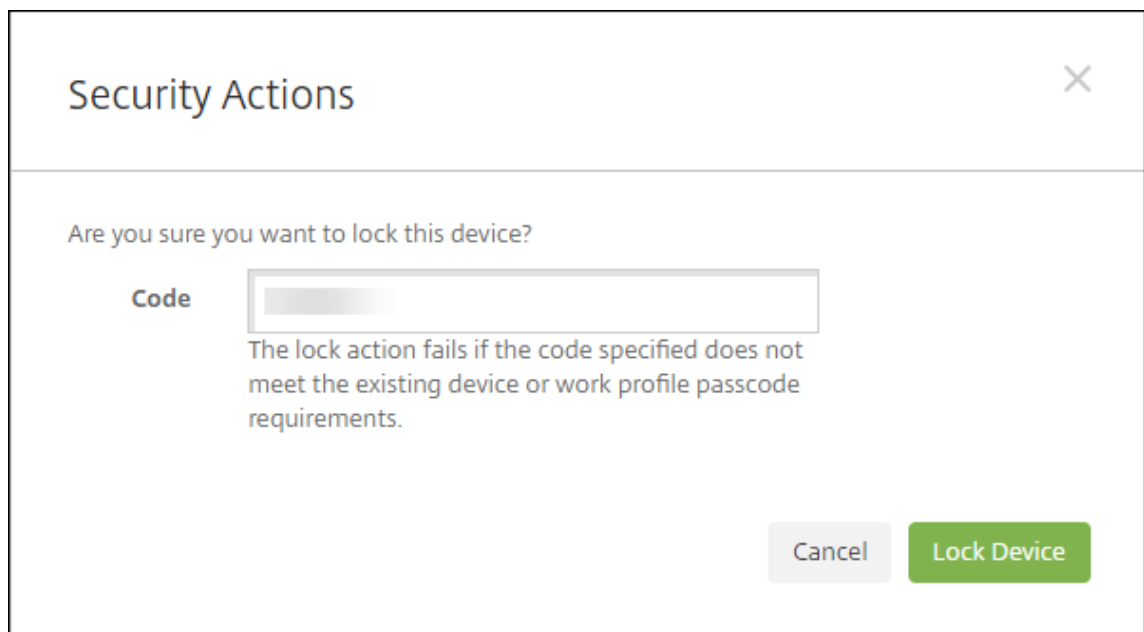
Media0

Show more >

3. En el menú de opciones, seleccione **Proteger**. Aparecerá el cuadro de diálogo **Acciones de seguridad**.



4. Haga clic en **Bloquear**. Aparecerá el cuadro de confirmación **Acciones de seguridad**.



5. Haga clic en **Bloquear dispositivo**.

Importante:

También puede especificar un código de acceso en lugar de utilizar 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.

Identificador de arranque

Un identificador de arranque ayuda a otorgar el atributo SecureToken de macOS a las cuentas cuando usted inicia sesión en un dispositivo macOS. SecureToken pasa de una cuenta de confianza a otra. Las cuentas con SecureToken habilitado pueden realizar operaciones criptográficas en el dispositivo. Sin el identificador de arranque, debe seguir complejos flujos de trabajo para crear cuentas en ese dispositivo antes de agregar cuentas de usuario individuales.

Citrix Endpoint Management admite la custodia de identificadores de arranque para dispositivos macOS inscritos a través del Programa de implementación de Apple. El Programa de implementación de Apple se utiliza para inscribir dispositivos macOS adquiridos directamente de Apple, de un distribuidor autorizado de Apple o de un operador. Para obtener información sobre cómo inscribirse en el Programa de implementación de Apple, consulte [Implementar dispositivos mediante el Programa de implementación de Apple](#).

Los identificadores de arranque se generan durante el flujo de trabajo del Asistente de configuración. Concretamente, se generan durante la creación de cuentas de usuario local. El Asistente de configuración se ejecuta la primera vez que los usuarios inician sus dispositivos. Los identificadores se guardan en la base de datos de Citrix Endpoint Management y no resultan visibles ni para usted ni para los usuarios finales. Al eliminar los dispositivos del sitio de Citrix Endpoint Management, se eliminan los identificadores. Restablecer los valores de fábrica de los dispositivos tampoco los elimina.

Requisitos previos:

- macOS 11.0 o una versión posterior
- Dispositivos macOS que tienen el chip de seguridad T2 de Apple
- Dispositivos macOS inscritos a través del Programa de implementación de Apple

Una de las ventajas de la custodia de identificadores de arranque con Citrix Endpoint Management es que las cuentas remotas se pueden habilitar para FileVault y se puede desbloquear el volumen de FileVault. Para obtener información sobre FileVault, consulte [Directiva de FileVault](#).

Implementar dispositivos mediante los Programas de implementación de Apple

March 1, 2024

Los Programas de implementación de Apple (ADP) permiten inscribir automáticamente dispositivos Apple en Citrix Endpoint Management sin tener que tocar ni preparar los dispositivos antes de que los usuarios los obtengan. Cuando el usuario haya desempaqueado y activado el dispositivo, el dispositi-

tivo se inscribe automáticamente en Citrix Endpoint Management, y todos los parámetros de administración, las aplicaciones y los libros están listos para el usuario.

Los ADP incluyen Apple Business Manager (ABM) para empresas y Apple School Manager (ASM) para centros educativos. ABM y ASM están disponibles para dispositivos iOS, iPadOS y macOS. Para obtener más información sobre la elegibilidad de los dispositivos, consulte el [Manual de uso de Apple Business Manager](#) y el [Manual de uso de Apple School Manager](#).

Nota:

ABM y ASM combinan los antiguos programas de inscripción de dispositivos y de compras por volumen de Apple.

En este artículo se describe el flujo de trabajo general de la implementación con ABM o ASM:

1. [Inscríbase en ABM o ASM](#)
2. [Conectar su cuenta de ABM o ASM a Citrix Endpoint Management](#)
3. [Ordenar dispositivos](#)
4. [Asignar dispositivos a Citrix Endpoint Management](#)
5. [Comprar contenidos por volumen y sincronizarlos con Citrix Endpoint Management](#)
6. [Configurar reglas de implementación para aplicaciones y directivas de dispositivos](#)
7. Agregar grupos de entrega que contengan usuarios y recursos asignados a ellos

Después de completar este proceso de implementación, los dispositivos ya pueden desempaquetarse y activarse para una inscripción automatizada del dispositivo.

Requisitos previos

Abra los puertos necesarios para la conectividad entre Citrix Endpoint Management y Apple. Para obtener más información, consulte [Requisitos de puertos](#).

Inscríbase en ABM o ASM

Para empezar a implementar dispositivos en Apple, inscríbase en ABM o ASM.

ABM y ASM están disponibles para organizaciones, no para usuarios individuales. Debe proporcionar mucha información sobre la organización para crear una cuenta. Es posible que tarde un tiempo en solicitar y recibir aprobación para la cuenta.

Inscribirse en ABM

Para inscribirse en ABM, vaya a business.apple.com. Haga clic en **Enroll now** para solicitar una nueva cuenta.

Se recomienda usar una dirección de correo electrónico asociada a su organización, como deployment@company.com. El proceso de inscripción puede tardar unos días. Después de recibir las credenciales de inicio de sesión, siga los pasos que se indican en ABM para crear una cuenta.

Inscribirse en ASM

Para crear la cuenta de ASM, vaya a [Apple School Manager](#) y siga las instrucciones ahí indicadas para inscribirse. La primera vez que inicia 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 el [Manual de uso de Apple School Manager](#).
- Al configurar una cuenta de usuario de ASM, use un nombre de dominio diferente del nombre de dominio de Active Directory. Por ejemplo, puede anteponer un prefijo de tipo `appleid` al nombre de dominio de ASM.
- Cuando se conecta a ASM para ver los datos de la lista del aula, ASM crea ID de Apple administrados para profesores y alumnos. La lista contiene datos de profesores, alumnos y clases. Para obtener información sobre cómo agregar datos de listas a ASM, consulte el Manual del usuario de Apple School Manager, vinculado más arriba en esta lista.
- Puede personalizar el formato del ID de Apple administrado para que se ajuste a su institución como se describe en el Manual del usuario de Apple School Manager, vinculado más arriba en esta lista.

Importante:

No cambie los ID de Apple administrados una vez que haya importado la información de ASM en Citrix Endpoint Management.

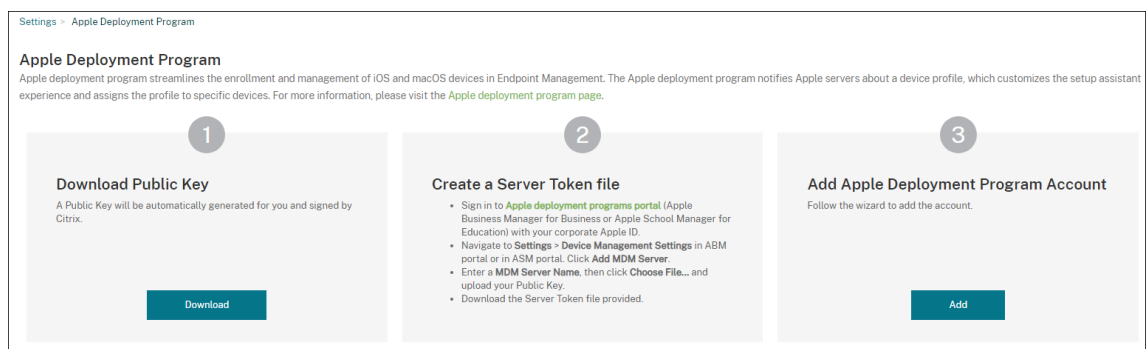
- Si ha adquirido los dispositivos por medio de distribuidores y operadores, vincule esos dispositivos a ASM. Para obtener más información, consulte el Manual del usuario de Apple School Manager, vinculado más arriba en esta lista.

Conectar su cuenta de ABM o ASM a Citrix Endpoint Management

Después de crear su cuenta de ABM o ASM, conéctela al servidor de implementación de Citrix Endpoint Management.

Paso 1: Descargue una clave pública desde el servidor de Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Programas de implementación de Apple**.



2. En **Descargar clave pública**, haga clic en **Descargar**.

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 administrador 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 el parámetro **MDM Server Name**, escriba un nombre para el servidor de Citrix Endpoint Management. El nombre del servidor que escriba le servirá de referencia. No es la URL o 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 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 del token aparece en la consola de Citrix Endpoint Management una vez importado el archivo de token.

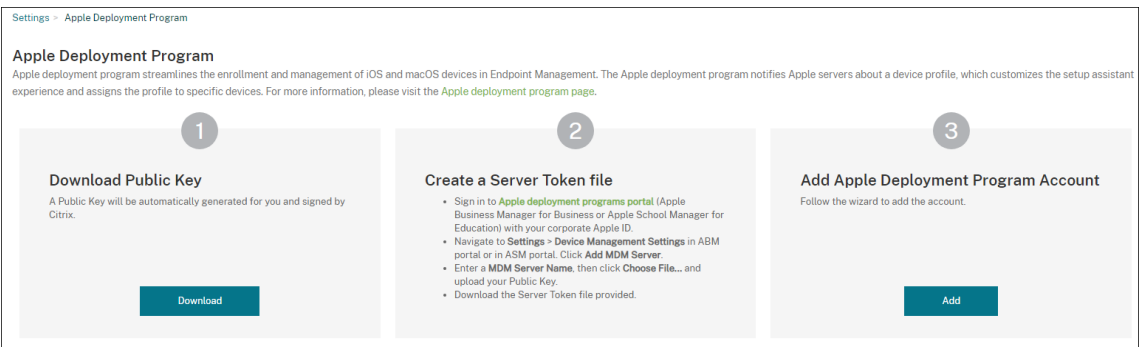
6. En **Default Device Assignment**, haga clic en **Change**. Elija cómo quiere asignar los dispositivos y, a continuación, proporcione la información solicitada. Para obtener más información, consulte el [Manual de uso de ABM](#) o el [Manual de uso de Apple School Manager](#).

Paso 3: Agregue su cuenta a Citrix Endpoint Management

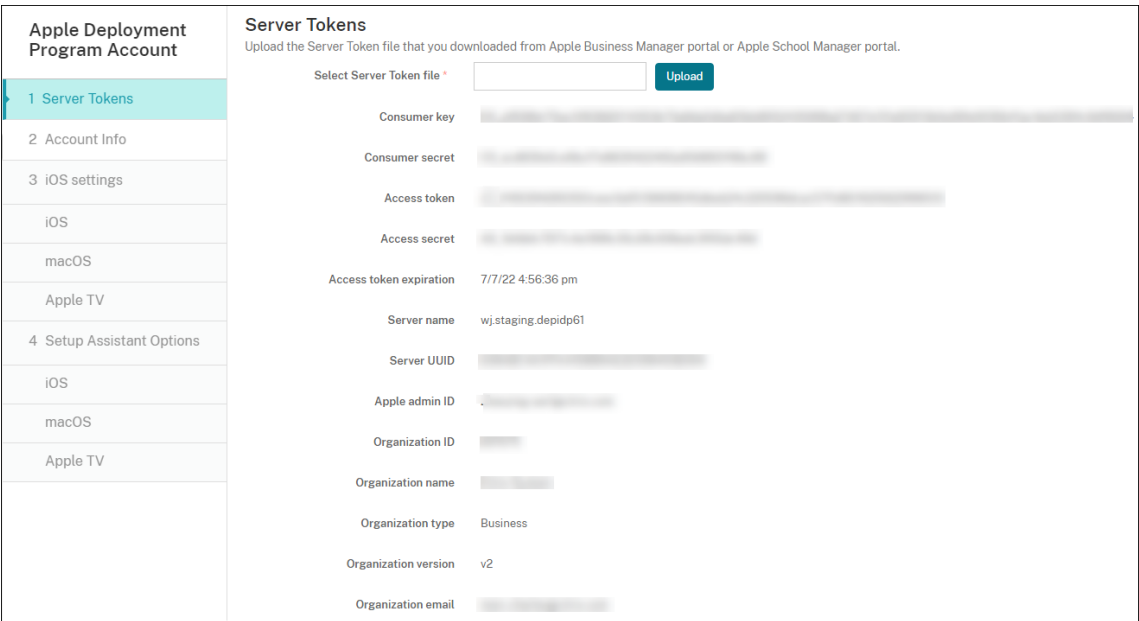
Puede agregar varias cuentas de ABM o ASM a Citrix Endpoint Management. Esta función permite utilizar distintos parámetros de inscripción y opciones del asistente de instalación según el país y el departamento, entre otros. A continuación, puede asociar las cuentas de ABM o ASM a distintas directivas de dispositivo.

Por ejemplo, puede centralizar todas las cuentas de ABM o ASM de diferentes países en el mismo servidor de Citrix Endpoint Management para importar y supervisar todos los dispositivos de ABM o ASM. Primero se personalizan los parámetros de inscripción y las opciones del asistente de instalación por departamento, jerarquía organizativa u otra estructura. A continuación, se configuran directivas para proporcionar la funcionalidad adecuada en toda la organización y permitir que los usuarios reciban la asistencia pertinente.

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Programa de implementación de Apple** y, en **Agregar cuenta del Programa de implementación de Apple**, haga clic en **Agregar**.



2. En la página **Tokens de servidor**, especifique su archivo de token de servidor y, a continuación, haga clic en **Cargar**.



Aparecerá la información del token de servidor.

3. En la página **Información de cuenta**, especifique los siguientes parámetros:

Apple Deployment Program Account	Account Info
1 Server Tokens	Specify your Apple deployment program account information.
2 Account Info	Apple deployment program account name *
3 iOS settings	Business/Education unit *
iOS	Unique service ID
macOS	Support phone number *
Apple TV	Support email address
4 Setup Assistant Options	
iOS	
macOS	
Apple TV	

- **Nombre de la cuenta de Programas de implementación de Apple:** Un nombre descriptivo único para esta cuenta de ADP que identifica cómo quiere organizar las cuentas de ADP (por ejemplo, por país o jerarquía organizativa).
- **Unidad de negocio/educación:** El departamento o la unidad de negocio a la que se asigna el dispositivo. Este campo es obligatorio.
- **ID único de servicio:** Un ID exclusivo optativo para ayudarlo a identificar la cuenta.
- **Número de teléfono de asistencia:** Un número de teléfono al que puedan llamar los usuarios para obtener ayuda durante la instalación. Este campo es obligatorio.
- **Dirección de correo electrónico de asistencia:** Una dirección opcional de correo electrónico de asistencia disponible para los usuarios finales.
- **Sufijo de educación:** Para las cuentas ASM. Escriba el sufijo asignado a los dispositivos inscritos a través de esta cuenta.

4. En **Parámetros de iOS**, especifique los siguientes parámetros:

Settings > Apple Deployment Program > Edit Apple Deployment Program Account

Apple Deployment Program Account

- 1 Server Tokens
- 2 Account Info
- 3 iOS settings
- iOS**
- macOS
- Apple TV
- 4 Setup Assistant Options
- iOS
- macOS
- Apple TV

iOS settings

Specify the settings to define the enrollment process and the mode of iOS Automatic Device Enrollment devices.

Enrollment settings

- Require device enrollment ☒ ⓘ
- Require credentials for device enrollment ☒ ⓘ iOS 7.1+
- Enroll using Citrix Identity Provider ☒ ⓘ iOS 13.0+
- Wait for configuration to complete setup ☒ ⓘ iOS 9.0+

Device settings

- Supervised mode ☒ ⓘ
- Shared mode ☐ ⓘ
- Allow enrollment profile removal ☒ ⓘ
- Allow device pairing ☒ ⓘ

Parámetros de inscripción:

- **Requerir inscripción del dispositivo:** Puede requerir a los usuarios que inscriban sus dispositivos. El valor predeterminado es **Activado**.
- **Requerir credenciales para inscripción de dispositivos:** Puede pedir a los usuarios que indiquen sus credenciales durante la configuración de ABM o ASM. Recomendamos que solicite a todos los usuarios que introduzcan sus credenciales durante la inscripción de dispositivos, lo que permitiría solamente a los usuarios autorizados inscribir dispositivos. El valor predeterminado es **Activado**.

Si habilita ABM o ASM antes de la primera configuración y no selecciona esta opción, Citrix Endpoint Management crea los componentes de ABM o ASM. Este proceso de creación incluye componentes como usuario, Citrix Secure Hub, inventario de software y grupo de implementación. Si selecciona esta opción, Citrix Endpoint Management no crea los componentes. Como resultado, si posteriormente desactiva esta opción, los usuarios que no hayan introducido sus credenciales no podrán realizar la inscripción en ABM o ASM porque esos componentes no existen. Para agregar componentes de ABM o ASM, en ese caso es necesario inhabilitar y habilitar la cuenta de ABM o ASM.

- **Inscribirse mediante el proveedor de identidades de Citrix:** Si se inscribe mediante el proveedor de identidades de Citrix. Este parámetro solo está disponible para cuentas de ABM. Si está **activado**, los dispositivos iOS habilitados para ADP se inscriben únicamente mediante el proveedor de identidades de Citrix. El valor predeterminado es **Desactivado**.

Para activar el parámetro, primero debe configurar el proveedor de identidades de Citrix como su proveedor de identidades. Vaya a **Parámetros > Proveedor de identidades (IDP)**, haga clic en **Agregar** y seleccione **Proveedor de identidades de Citrix**.

Si este parámetro está **activado**, tenga en cuenta lo siguiente:

- No puede eliminar la configuración del proveedor de identidades de Citrix correspondiente en la página **Parámetros > Proveedor de identidades (IDP)**.
- Al modificar la configuración del proveedor de identidades de Citrix correspondiente, no puede cambiar de proveedor de identidades.
- **Esperar a que se complete la configuración:** Puede requerir que los dispositivos de los usuarios permanezcan en el modo de asistente de instalación hasta implementar todos los recursos de MDM en ellos. Esta opción está disponible para dispositivos en modo supervisado. El valor predeterminado es **Desactivado**.
- En la documentación de Apple consta que los comandos siguientes pueden no funcionar mientras un dispositivo esté en modo de asistente de instalación:
 - InviteToProgram
 - InstallApplication
 - ApplyRedemptionCode
 - InstallMedia
 - RequestMirroring
 - DeviceLock

Parámetros del dispositivo:

- **Modo supervisado: Actívelo** si usa el Apple Configurator para administrar los dispositivos inscritos o si está habilitada la opción **Esperar a que se complete la configuración**. El valor predeterminado es **Activado**. Para obtener información detallada sobre cómo colocar un dispositivo iOS en modo supervisado, consulte [Implementar dispositivos con Apple Configurator 2](#).
- **Permitir quitar el perfil de inscripción:** Puede permitir que los dispositivos usen un perfil que se pueda quitar de forma remota. El valor predeterminado es **Desactivado**.
- **Permitir emparejamiento de dispositivos:** Si puede administrar dispositivos inscritos mediante Apple Music y Apple Configurator. El valor predeterminado es **Desactivado**.

Identidades de supervisión

Si utiliza la herramienta GroundControl, puede agregar un certificado para hacer lo siguiente:

- Anular las restricciones de emparejamiento para evitar el mensaje “Confiar en este host”.
- Ampliar las acciones del dispositivo administrado por USB para que se puedan realizar acciones (como instalar perfiles sin interacción del usuario). Eso permite que GroundControl habilite el modo de aplicación única y el bloqueo del dispositivo hasta desprotegerlo.
- Restaurar una copia de seguridad en los dispositivos de ABM o ASM.

Para obtener más información sobre GroundControl, consulte [el sitio web de GroundControl](#).

5. En **Parámetros de macOS**, especifique los siguientes parámetros:

Settings > Apple Deployment Program > Edit Apple Deployment Program Account

Apple Deployment Program Account

macOS Settings
Specify the settings to define the enrollment process of macOS Automatic Device Enrollment devices.

Enrollment settings

- Require device enrollment ☒ ⓘ
- Enroll using Citrix Identity Provider ☒ ⓘ macOS 10.15+
- Wait for configuration to complete setup ☒ ⓘ macOS 10.11+

Device settings

- Allow enrollment profile removal ☒ ⓘ

Parámetros de inscripción:

- **Requerir inscripción del dispositivo:** Puede requerir a los usuarios que inscriban sus dispositivos. El valor predeterminado es **Activado**.
- **Inscribirse mediante el proveedor de identidades de Citrix:** Si se inscribe mediante el proveedor de identidades de Citrix. Este parámetro solo está disponible para cuentas de ABM. Si está **activado**, los dispositivos macOS habilitados para ADP se inscriben únicamente mediante el proveedor de identidades de Citrix. El valor predeterminado es **Desactivado**.

Para activar el parámetro, primero debe configurar el proveedor de identidades de Citrix como su proveedor de identidades. Vaya a **Parámetros > Proveedor de identidades (IDP)**, haga clic en **Agregar** y seleccione **Proveedor de identidades de Citrix**.

Si este parámetro está **activado**, tenga en cuenta lo siguiente:

- No puede eliminar la configuración del proveedor de identidades de Citrix correspondiente en la página **Parámetros > Proveedor de identidades (IDP)**.
- Al modificar la configuración del proveedor de identidades de Citrix correspondiente, no puede cambiar de proveedor de identidades.
- **Esperar a que se complete la configuración:** Si está **activado**, el dispositivo macOS no continúa con el Asistente de instalación hasta que el código de acceso a recursos MDM se implementa en el dispositivo. Esa implementación ocurre antes de la creación de la cuenta local. Esta configuración está disponible para macOS 10.11 y versiones posteriores. El valor predeterminado es **Desactivado**.

Parámetros del dispositivo:

- **Permitir quitar el perfil de inscripción:** Puede permitir que los dispositivos usen un perfil que se pueda quitar de forma remota. El valor predeterminado es **Desactivado**.

6. En **Parámetros de Apple TV**, especifique estos parámetros:

- **Requerir inscripción del dispositivo:** Impide que los usuarios omitan la inscripción.
- **Requerir credenciales para inscripción de dispositivos:** Pide credenciales durante la inscripción. Cuando este parámetro está desactivado, Apple TV se inscribe como “usuario predeterminado de Device Enrollment Program”.
- **Esperar a que se complete la configuración:** El dispositivo espera en la pantalla del **asistente de configuración** hasta que todos los recursos se implementen.
- **Modo supervisado:** Concede más capacidades al administrador en la configuración de restricciones.
- **Permitir quitar el perfil de inscripción:** Permite a los usuarios eliminar los perfiles de inscripción.
- **Permitir emparejamiento de dispositivos:** Permite que los dispositivos inscritos a través del programa de inscripción de dispositivos DEP (Device Enrollment Program) se administren mediante herramientas de Apple (como App Store y Apple Configurator).

Apple Deployment Program Account	Apple TV Settings Specify the settings to define the enrollment process of Apple TV Automatic Device Enrollment devices.
1 Server Tokens	Enrollment settings
2 Account Info	
3 iOS settings	
iOS	Device settings
macOS	
Apple TV	
4 Setup Assistant Options	
iOS	
macOS	
Apple TV	

Require device enrollment	<input checked="" type="checkbox"/>	?
Require credentials for device enrollment	<input checked="" type="checkbox"/>	?
Wait for configuration to complete setup	<input type="checkbox"/>	x ?
Supervised mode	<input checked="" type="checkbox"/>	?
Allow enrollment profile removal	<input type="checkbox"/>	x ?
Allow device pairing	<input type="checkbox"/>	x ?

7. En **Opciones del asistente de configuración de iOS**, seleccione los pasos a omitir del Asistente de configuración de iOS cuando los usuarios inicien 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 finalizada la instalación, a menos que restrinja el acceso a esas funciones por completo. Para obtener más información sobre cómo restringir el acceso a funciones, consulte [Directiva de restricciones](#). Se borra el valor predeterminado de todos los elementos. Las siguientes descripciones explican lo que ocurre cuando se

selecciona un parámetro.

Apple Deployment Program Account	iOS Setup Assistant Options
1 Server Tokens	Select the Setup Assistant items that users won't see when they start their iOS Automatic Device Enrollment devices for the first time.
2 Account Info	<input type="checkbox"/> Skip setup
3 iOS settings	<input type="checkbox"/> Location services
iOS	<input type="checkbox"/> Touch ID iOS 8.0+
macOS	<input checked="" type="checkbox"/> Passcode lock
Apple TV	<input type="checkbox"/> Set up as new or restore
4 Setup Assistant Options	<input type="checkbox"/> Move from Android iOS 9.0+
iOS	<input checked="" type="checkbox"/> Apple ID
macOS	<input type="checkbox"/> Terms and conditions
Apple TV	<input checked="" type="checkbox"/> Apple Pay iOS 8.0+
	<input checked="" type="checkbox"/> Siri
	<input checked="" type="checkbox"/> App analytics
	<input checked="" type="checkbox"/> Display zoom iOS 8.0+
	<input checked="" type="checkbox"/> True Tone iOS 10.0+
	<input checked="" type="checkbox"/> Home button iOS 10.0+
	<input checked="" type="checkbox"/> New feature highlights iOS 11.0+
	<input checked="" type="checkbox"/> Privacy iOS 11.3+
	<input checked="" type="checkbox"/> Software update iOS 12.0+
	<input type="checkbox"/> Screen Time iOS 12.0+
	<input checked="" type="checkbox"/> SIM setup iOS 12.0+
	<input checked="" type="checkbox"/> iMessage & FaceTime iOS 12.0+
	<input type="checkbox"/> Appearance iOS 13.0+
	<input type="checkbox"/> Welcome iOS 13.0+
	<input checked="" type="checkbox"/> Restore completed iOS 14.0+

- **Servicios de localización:** Impide a los usuarios configurar el servicio de localización en el dispositivo.
- **Touch ID:** Impide que los usuarios configuren Touch ID o Face ID en dispositivos iOS.
- **Bloqueo de código de acceso:** Impide que los usuarios establezcan un código de acceso para el dispositivo. Si no existe ningún código, los usuarios no pueden usar Touch ID o Apple Pay.
- **Definir como nuevo o Restaurar:** Impide que los usuarios configuren el dispositivo como nuevo o a partir de una copia de seguridad de iCloud o del App Store de Apple.
- **Mover desde Android:** Impide que los usuarios transfieran datos de un dispositivo Android a un dispositivo iOS. Esta opción solo está disponible cuando la opción **Definir como nuevo o Restaurar** está seleccionada (es decir, se omite el paso).
- **ID de Apple:** Impide que los usuarios establezcan una cuenta de ID de Apple gestionado para el dispositivo.
- **Términos y condiciones:** Impide que los usuarios lean y acepten los términos y condiciones de uso del dispositivo.
- **Apple Pay:** Impide que los usuarios configuren Apple Pay. Si se desactiva esta opción, los usuarios deben configurar Touch ID y Apple ID. Compruebe que esos parámetros estén desactivados.
- **Siri:** Impide que el usuario configure Siri.
- **App Analytics:** Impide a los usuarios configurar si se pueden compartir los datos de fallos y estadísticas de uso con Apple.

- **Zoom de presentación:** Impide a los usuarios configurar la resolución de la pantalla (estándar o ampliada) en los dispositivos iOS.
- **True Tone:** Impide que los usuarios establezcan sensores de cuatro canales para ajustar dinámicamente el balance de blancos de la pantalla.
- **Botón de inicio:** Impide que los usuarios establezcan el estilo de retroalimentación del botón de inicio.
- **Nuevas funciones destacadas:** Impide que los usuarios vean las pantallas que muestran información sobre las nuevas funciones del software Apple.
- **Privacidad:** Impide que los usuarios vean el panel de datos y privacidad. Para iOS 11.3 y versiones posteriores.
- **Actualización de software:** Impide que los usuarios actualicen iOS a la versión más reciente. Para iOS 12.0 y versiones posteriores.
- **Screen Time:** Impide que los usuarios activen Screen Time. Para iOS 12.0 y versiones posteriores.
- **Configuración de SIM:** Impide que los usuarios configuren un plan de datos móviles. Para iOS 12.0 y versiones posteriores.
- **iMessage y FaceTime:** Impide que el usuario vea la pantalla iMessage y FaceTime. Para iOS 12.0 y versiones posteriores.
- **Apariencia:** Impide que los usuarios seleccionen el modo de apariencia. Para iOS 13.0 y versiones posteriores.
- **Bienvenida:** Impide que el usuario vea la pantalla **Cómo empezar**. Para iOS 13.0 y versiones posteriores.
- **Restauración completada:** Impide que los usuarios vean si una restauración se completa durante la instalación. Para iOS 14.0 y versiones posteriores.
- **Actualización completada:** Impide que los usuarios vean si una actualización de software se completa durante la instalación. Para iOS 14.0 y versiones posteriores.
- **App Store:** Impide que los usuarios configuren el App Store. Para iOS 11.1 y versiones posteriores.

La cuenta aparece en **Parámetros > Programa de implementación de Apple**.

8. En **Opciones del asistente de configuración de macOS**, seleccione los pasos a omitir del Asistente de configuración de macOS cuando los usuarios inicien 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 finalizada la instalación, a menos que restrinja el acceso a esas funciones por completo. Para obtener más información sobre cómo restringir el acceso a funciones, consulte [Directiva de restricciones](#). Se borra el valor predeterminado de todos los elementos. Las siguientes descripciones explican lo que ocurre cuando se selecciona un parámetro.

Apple Deployment Program Account	macOS Setup Assistant Options
1 Server Tokens	Select the Setup Assistant items that users won't see when they start their macOS Automatic Device Enrollment devices for the first time.
2 Account Info	
3 iOS settings	
iOS	
macOS	
Apple TV	
4 Setup Assistant Options	
iOS	
macOS	<div> <div>Skip setup</div> <div> <input type="checkbox"/> Set up as new or restore <input type="checkbox"/> Location services macOS 10.11+ <input type="checkbox"/> Apple ID <input type="checkbox"/> Terms and conditions <input type="checkbox"/> Siri macOS 10.12+ <input type="checkbox"/> FileVault macOS 10.10+ ⓘ <input type="checkbox"/> App analytics <input type="checkbox"/> Privacy macOS 10.13+ <input type="checkbox"/> iCloud Analytics macOS 10.13+ <input type="checkbox"/> iCloud Documents and Desktop macOS 10.13+ <input type="checkbox"/> Appearance macOS 10.14+ <input type="checkbox"/> Accessibility macOS 11+ <input type="checkbox"/> Biometric macOS 10.12.4+ <input type="checkbox"/> True Tone macOS 10.13.6+ <input type="checkbox"/> Apple Pay macOS 10.12.4+ <input type="checkbox"/> Screen Time macOS 10.15+ </div> </div>
Apple TV	
	<div> <div>Local account setup options</div> <div> <input type="checkbox"/> Create primary account as a standard user macOS 10.11+ </div> </div> <div> <div>Admin full name</div> <input type="text"/> ⓘ </div> <div> <div>Admin short name</div> <input type="text" value="localadmin"/> </div>

- **Definir como nuevo o Restaurar:** Impide que los usuarios configuren el dispositivo como nuevo o a partir de una copia de seguridad de Time Machine o migren el sistema.
- **Servicios de localización:** Impide a los usuarios configurar el servicio de localización en el dispositivo. Para macOS 10.11 y versiones posteriores.
- **ID de Apple:** Impide que los usuarios establezcan una cuenta de ID de Apple gestionado para el dispositivo.
- **Términos y condiciones:** Impide que los usuarios lean y acepten los términos y condiciones de uso del dispositivo.
- **Siri:** Impide que el usuario configure Siri. Para macOS 10.12 y versiones posteriores:
- **FileVault:** Usar FileVault para cifrar el disco de arranque. Citrix Endpoint Management solo aplica el parámetro FileVault si el sistema tiene una única cuenta de usuario local y esa cuenta se ha registrado en iCloud.

Puede usar la funcionalidad de cifrado de disco FileVault en macOS para proteger el volumen del sistema mediante el cifrado de su contenido (<https://support.apple.com/en-us/HT204837>). Si ejecuta el Asistente de configuración en un modelo reciente de portátil Mac donde FileVault está desactivado, puede que le aparezca una solicitud para que habilite esta función. El mensaje aparece tanto en sistemas nuevos como en sistemas actualizados a OS X 10.10 o 10.11, pero solo si el sistema tiene una sola cuenta de administrador local y esa cuenta está registrada en iCloud.

- **App Analytics:** Impide a los usuarios configurar si se pueden compartir los datos de fallos

y estadísticas de uso con Apple.

- **Privacidad:** Impide que los usuarios vean el panel Datos y privacidad. Para macOS 10.13 y versiones posteriores.
- **Análisis de iCloud:** Impide que los usuarios elijan si enviar o no datos de diagnóstico de iCloud a Apple. Para macOS 10.13 y versiones posteriores.
- **Escritorio y documentos de iCloud:** Impide que los usuarios configuren el escritorio y los documentos de iCloud. Para macOS 10.13 y versiones posteriores.
- **Apariencia:** Impide que los usuarios seleccionen el modo de apariencia. Para macOS 10.14 y versiones posteriores.
- **Accesibilidad:** Impide que el usuario escuche VoiceOver automáticamente. Solo está disponible si el dispositivo está conectado a Ethernet. Para macOS 11 y versiones posteriores.
- **Biometría:** Impide que el usuario configure Touch ID y Face ID. Para macOS 10.12.4 y versiones posteriores:
- **True Tone:** Impide que los usuarios establezcan 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 se desactiva esta opción, los usuarios deben configurar Touch ID y Apple ID. Asegúrese de que los parámetros **ID de Apple** y **Biometría** estén desactivados.
- **Screen Time:** Impide que los usuarios activen Screen Time. Para macOS 10.15 y versiones posteriores:
- **App Store:** Impide que el usuario configure el App Store. Para macOS 11.1 y versiones posteriores.
- **Desbloquear con el Apple Watch:** Impide que los usuarios desbloqueen su Mac con un Apple Watch. Para macOS 12 y versiones posteriores.
- **Opciones de configuración de cuenta local:** Especifique los parámetros para crear una cuenta en el dispositivo. Primero, Citrix Endpoint Management crea la cuenta de administrador local mediante la información que especifique aquí. Cuando los usuarios activan su dispositivo, se crea una cuenta de usuario como la cuenta principal. La opción **Crear cuenta principal como usuario estándar** determina si la cuenta principal tiene privilegios de administrador.

Importante:

Solo puede seleccionar la opción **Crear cuenta principal como usuario estándar**

después de **activar** la opción **Esperar a que se complete la configuración** en la página **Parámetros de macOS**.

- **Crear cuenta principal como usuario estándar:** Al seleccionarse, Citrix Endpoint Management crea el usuario con permisos estándar en lugar de conceder a este usuario privilegios de administrador de usuarios en el dispositivo. Omita esta opción si quiere conceder privilegios de administrador de usuarios en el dispositivo. De forma predeterminada, esta opción no está seleccionada.
- **Nombre completo del administrador:** Escriba el nombre que mostrará el sistema para la cuenta de administrador.
- **Nombre corto del administrador** Escriba el nombre que mostrará el dispositivo para la carpeta particular y en el shell.
- **Contraseña del administrador:** Introduzca una contraseña segura para la cuenta de administrador.
- **Mostrar la cuenta de administrador en Usuarios y grupos:** Si no está marcada, 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 opción para ocultar la cuenta de administrador que Citrix Endpoint Management crea en primer lugar.

Para mejorar la seguridad, Citrix Endpoint Management comprueba si se debe rotar diariamente la contraseña de la cuenta de administrador. De forma predeterminada, Citrix Endpoint Management rota la contraseña cada 7 días. Para cambiar el valor predeterminado, actualice la propiedad `mac.dep.admin.passwd.rotate` del servidor. Para obtener información, consulte [Propiedades de servidor](#).

Para aumentar la seguridad, Citrix Endpoint Management genera las contraseñas de la siguiente manera:

- 12 caracteres de largo
- 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 el dispositivo en cuestión, haga clic en **Mostrar más** y, a continuación, consulte la página **Detalles del dispositivo > General**. La sección **Seguridad** muestra lo siguiente:

- **Antigua contraseña de administrador:** Permite ver la contraseña anterior. Citrix Endpoint Management muestra solamente la última contraseña. Haga clic en **Mostrar contraseña** para ver la contraseña.
- **Actual contraseña de administrador:** Permite ver la contraseña actual.

- **Cambiar contraseña de administrador:** Permite ver el estado del cambio de contraseña. Es posible que aparezca esta información en función del estado:
 - Solicitud de cambio de contraseña: < valor de tiempo específico >.
 - Cambio de contraseña: < valor de tiempo específico >.
 - Error al intentar cambiar la contraseña: < valor de tiempo específico >.
 - La contraseña aún no se ha cambiado.

9. En **Opciones del asistente de configuración de Apple TV**, seleccione los pasos que omitir del asistente de configuración de Apple TV (es decir, los pasos que los usuarios no tienen que llevar a cabo) cuando inicien sus dispositivos por primera vez. Se borra el valor predeterminado de todos los elementos. Guarde los cambios.

Apple Deployment Program Account

1 Server Tokens

2 Account Info

3 iOS settings

iOS

macOS

Apple TV

4 Setup Assistant Options

iOS

macOS

Apple TV

Apple TV Setup Assistant Options

Select the Setup Assistant items that users won't see when they start their Apple TV Automatic Device Enrollment devices for the first time.

Skip setup

☒

Siri and Dictation

☒

Apple ID

☒

Sync TV Home Screen Layout

☒

Set Up Your Apple TV

☒

Sign In to Your TV Provider

☒

Location services

☒

See the World

☒

App analytics

☒

Terms and conditions

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**.

Settings > Apple Deployment Program

Apple Deployment Program

Apple deployment program streamlines the enrollment and management of iOS and macOS devices in Endpoint Management. The Apple deployment program notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. For more information, please visit the [Apple deployment program page](#).

1

Download Public Key

A Public Key will be automatically generated for you and signed by Citrix.

Download

2

Create a Server Token file

- Sign in to [Apple deployment programs portal](#) (Apple Business Manager for Business or Apple School Manager for Education) with your corporate Apple ID.
- Navigate to [Settings > Device Management Settings](#) in ABM portal or in ASM portal. Click [Add MDM Server](#).
- Enter a [MDM Server Name](#), then click [Choose File...](#) and upload your Public Key.
- Download the Server Token file provided.

3

Add Apple Deployment Program Account

Follow the wizard to add the account.

Add

☐

Apple deployment program account name

☐

Business/Education unit

☐

Status

☐

Organization type

☐

Organization email

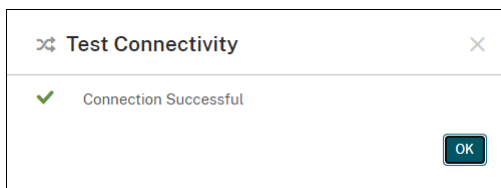
☐

Created on

☐

Server token expires on

Aparecerá un mensaje de estado.



Ordenar dispositivos

Puede adquirir dispositivos directamente desde estos canales:

- Apple. Proporcione sus números de cliente de Apple al vendedor.
- Distribuidores u operadores participantes autorizados de Apple. Proporcione el ID de su organización al vendedor y obtenga su ID de distribuidor.

Para obtener más información sobre la administración de proveedores de dispositivos, consulte el [Manual de uso de Apple Business Manager](#) o el [Manual de uso de Apple School Manager](#).

Una vez que se haya enviado el pedido, los dispositivos Apple que haya adquirido 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 úselo para asignar dispositivos de este pedido a 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 adquirieron los dispositivos.

Para obtener más información, consulte el [Manual de uso de Apple Business Manager](#) o el [Manual de uso de Apple School Manager](#).

Comprar contenidos por volumen y sincronizarlos con Citrix Endpoint Management

ABM y ASM le permiten comprar, distribuir y administrar licencias de aplicaciones y libros por volumen a partir de una única cuenta de organización. Para permitir que Citrix Endpoint Management se comuniquen con ABM o ASM para obtener la información de las licencias para su distribución, siga estos pasos:

1. En el portal de ABM o ASM, compre aplicaciones y libros públicos en **Apps and Books** y compre aplicaciones personalizadas desarrolladas para Citrix Endpoint Management en **Custom Apps**.
2. En el portal de ABM o ASM, descargue el token de contenidos asignado a Citrix Endpoint Management.

Para obtener más información sobre los pasos 1 y 2, consulte el [Manual de uso de Apple Business Manager](#) o el [Manual de uso de Apple School Manager](#).

3. En la consola de Citrix Endpoint Management, cree una cuenta de compras por volumen basada en el token de contenidos que descargó.

Para obtener más información, consulte [Agregar aplicaciones a través de las compras por volumen de Apple](#).

Una vez creada la cuenta de compras por volumen, las aplicaciones y los libros que haya adquirido aparecen en **Administrar > Aplicaciones**, y los dispositivos asignados al servidor de Citrix Endpoint Management aparecen en **Administrar > Dispositivos**.

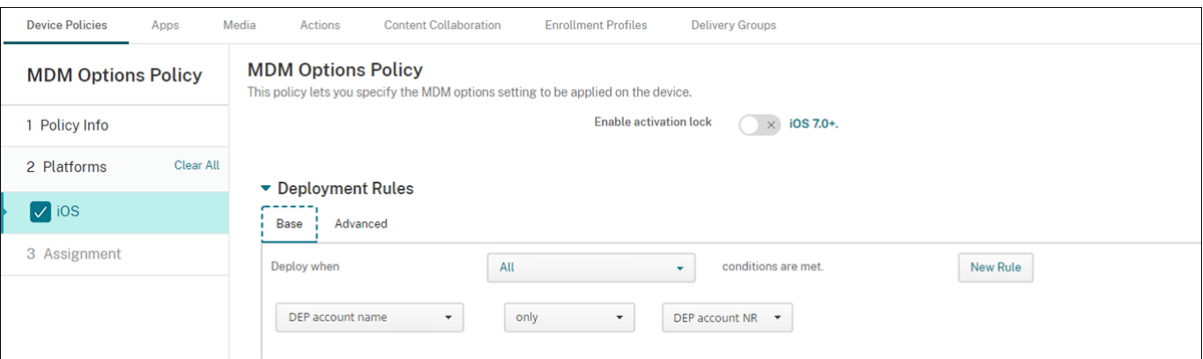
Configurar reglas de implementación para aplicaciones y directivas de dispositivos

Puede asociar cuentas de ABM o ASM a aplicaciones y directivas de dispositivo diferentes al configurar aplicaciones y directivas de dispositivo.

1. En las páginas **Configurar > Directivas de dispositivo** y **Configurar > Aplicaciones**, expanda **Reglas de implementación**.
2. Especifique que se implemente una directiva o una aplicación para una cuenta de ABM concreta o para todas las cuentas de ABM excepto la seleccionada.

La lista de cuentas de ABM incluye solo aquellas cuentas que tengan el estado habilitado o inhabilitado. Si la cuenta de ABM está inhabilitada, el dispositivo de ABM no pertenece a esta cuenta. Por lo tanto, Citrix Endpoint Management no implementa la aplicación o la directiva en el dispositivo.

En este ejemplo, una directiva de dispositivos se implementa solo en dispositivos cuyo nombre de cuenta de ABM sea “ABM Account NR”.



Inscribir dispositivos Apple en bloque

March 1, 2024

En Citrix Endpoint Management, puede inscribir una gran cantidad de dispositivos iOS, iPadOS y macOS de dos formas:

- Utilice los Programas de implementación de Apple (ADP) para inscribir dispositivos Apple adquiridos directamente de Apple, de un distribuidor autorizado de Apple o de un operador.

Para obtener más información sobre la implementación de dispositivos habilitados para ADP, consulte [Implementar dispositivos mediante los Programas de implementación de Apple](#). En este artículo se describe cómo los usuarios inscriben dispositivos habilitados para ADP y cómo reinscribir los dispositivos.

- Use Apple Configurator 2 para inscribir dispositivos iOS, independientemente de si los compra directamente de Apple.

En este artículo se describe cómo implementar dispositivos en bloque a través de Apple Configurator 2.

Acerca de la inscripción en bloque

Los ADP incluyen Apple Business Manager (ABM) para empresas y Apple School Manager (ASM) para la educación. La inscripción en bloque a través de los ADP ofrece lo siguiente:

- No tiene que tocar ni preparar los dispositivos.
- Después de completar los parámetros de implementación en Citrix Endpoint Management, puede entregar los dispositivos a los usuarios, y estos pueden comenzar a usarlos inmediatamente.
- Puede simplificar el proceso de configuración para los usuarios al eliminar algunos de los pasos del asistente de configuración.
- Para obtener más información sobre la configuración de ABM y ASM, consulte la documentación disponible de [Apple Business Manager](#) y [Apple School Manager](#).

La inscripción en bloque a través de Apple Configurator 2 ofrece lo siguiente:

- Conecte los dispositivos iOS a un Mac con macOS 10.7.2 o una versión posterior y la aplicación Apple Configurator 2. Debe preparar los dispositivos iOS y configurar las directivas a través de Apple Configurator 2.
- Los dispositivos se inscriben automáticamente Citrix Endpoint Management durante el proceso de configuración. Una vez completada la configuración, Citrix Endpoint Management envía las directivas, las aplicaciones y otros recursos a los dispositivos. A partir de ahí puede empezar a administrar los dispositivos.
- Para obtener más información sobre cómo usar Apple Configurator 2, consulte la [ayuda de Apple Configurator](#).

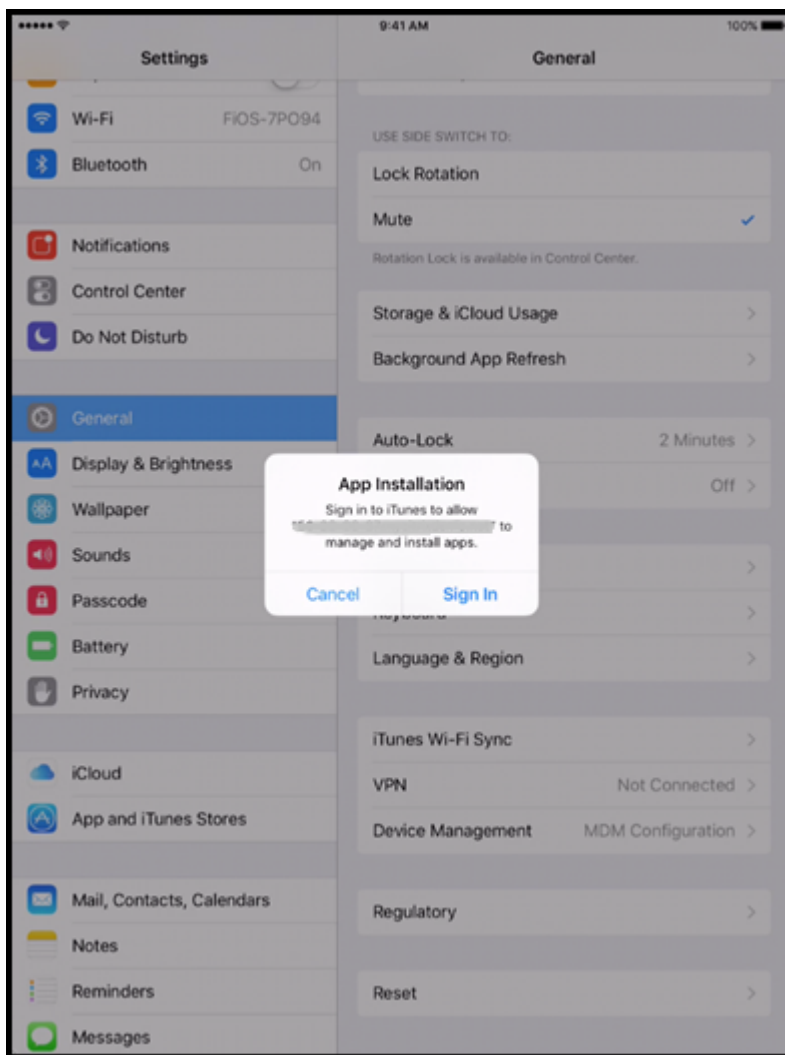
Cómo los usuarios inscriben dispositivos habilitados para ADP

Los usuarios inscriben sus dispositivos en Citrix Endpoint Management de esta manera:

1. Los usuarios inician su dispositivo.
2. Citrix Endpoint Management entrega al dispositivo los parámetros de ADP configurados en la página **Parámetros > Programas de implementación de Apple**.
3. Los usuarios configuran los parámetros iniciales en el dispositivo.
4. El dispositivo inicia automáticamente el proceso de inscripción de dispositivo de Citrix Endpoint Management.
5. Los usuarios siguen configurando otros parámetros iniciales en el dispositivo.
6. En la pantalla de inicio, puede que se pida a los usuarios que inicien sesión en el App Store de Apple para 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 compras por volumen para cada dispositivo. En este caso, no es necesario crear una cuenta de App Store ni utilizar una cuenta existente.



7. Los usuarios abren Citrix Secure Hub y escriben sus credenciales. Si hay una directiva que lo requiera, puede que se pida a los usuarios que creen y confirmen un PIN de Citrix.

Citrix Endpoint Management implementa las aplicaciones obligatorias restantes en el dispositivo.

Reinscribir los dispositivos habilitados para ADP

Los dispositivos habilitados para ADP se inscriben a partir de los valores restablecidos de fábrica. Para reinscribir un dispositivo habilitado para ADP, primero debe borrar el dispositivo por completo para desinscribirlo. Estos son los pasos detallados:

1. En la página **Administrar > Dispositivos**, seleccione el dispositivo.
2. Haga clic en **Seguridad**.
3. Haga clic en **Borrado completo** para desinscribir el dispositivo y devolverlo a los valores restablecidos de fábrica.

4. Inicie el dispositivo.

Importante:

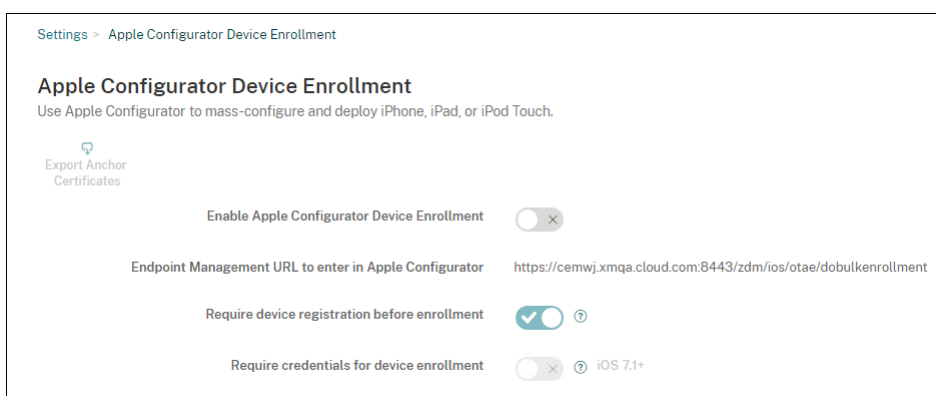
No use el **borrado selectivo** para desinscribir un dispositivo habilitado para ADP porque la inscripción de ADP requiere el dispositivo en sus valores restablecidos de fábrica.

Implementar dispositivos mediante Apple Configurator 2

Puede usar Apple Configurator 2 para implementar una gran cantidad de dispositivos con parámetros, aplicaciones y datos, e inscribir estos dispositivos en Citrix Endpoint Management.

Paso 1: Configure los parámetros en Citrix Endpoint Management

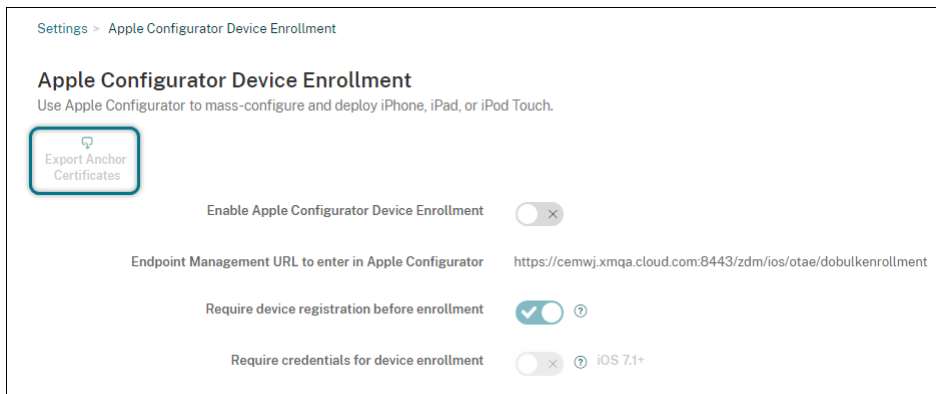
1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Apple Configurator Device Enrollment**.



2. Establezca **Permitir inscripción de dispositivos en Apple Configurator** en **Sí**.
3. Copie el parámetro **URL de inscripción que introducir en Apple Configurator** y pegue esta URL cuando configure los parámetros en Apple Configurator 2. Este parámetro 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), como `mdm.server.url.com`, o la dirección IP del servidor de Citrix Endpoint Management.
4. Para evitar que se inscriban dispositivos desconocidos, **active** el parámetro **Requerir registro del dispositivo antes de inscribirlo**. Nota: Si este parámetro está **activado**, debe agregar manualmente los dispositivos configurados a **Administrar > Dispositivos** en Citrix Endpoint Management o a través de un archivo CSV antes de la inscripción.
5. Para obligar a los usuarios de los dispositivos iOS que introduzcan sus credenciales cuando se inscriban, **active** el parámetro **Requerir credenciales para inscripción de dispositivos**. De forma predeterminada, está **desactivado**.

Nota:

Si el servidor de Citrix Endpoint Management está usando 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: Configure los ajustes en Apple Configurator 2**

1. Prepare un Mac con macOS 10.7.2 o una versión posterior y con Apple Configurator 2 instalado.
2. Use un cable de conector a USB de Dock para conectar los dispositivos Apple al Mac. Puede configurar hasta 30 dispositivos conectados simultáneamente. Si no dispone de un conector de Dock, use varios concentradores USB 2.0 de alta velocidad para conectar los dispositivos.
3. Inicie Apple Configurator 2. El configurador muestra todos los dispositivos que puede preparar para supervisión.
4. Para preparar un dispositivo para supervisión:
 - Si quiere mantener el control del dispositivo aplicando periódicamente una configuración, seleccione **Supervise devices**. Haga clic en **Siguiente**.

Importante:

Colocar un dispositivo en el modo supervisado instala la versión seleccionada de iOS en el dispositivo. Con este proceso, se borran del dispositivo todos los datos de usuario o aplicaciones almacenados previamente.

- En iOS, haga clic en **Latest** para ver la versión más reciente de iOS que quiera instalar.
5. En **Enroll in MDM Server**, elija un servidor MDM. Para agregar un servidor, haga clic en **Next**.
 6. En **Define an MDM server**, proporcione un nombre para el servidor y pegue la dirección URL del servidor MDM desde la consola de Citrix Endpoint Management.

7. En **Assign to organization**, elija una organización para supervisar el dispositivo.
Para obtener más información sobre la preparación de dispositivos con Apple Configurator 2, consulte la página de ayuda [Preparar dispositivos Apple Configurator](#).
8. A medida que prepare cada dispositivo, enciéndalo para iniciar el asistente de configuración de iOS, que prepara el dispositivo para su primer uso.

Agregar dispositivos a ABM o ASM mediante Apple Configurator 2

Puede agregar dispositivos iPhone, iPad y Apple TV a su cuenta de ABM o ASM mediante Apple Configurator 2, independientemente de dónde se hayan adquirido los dispositivos.

Una vez agregados los dispositivos, estos aparecen en la sección **Devices**. Estos dispositivos ya no incluyen la configuración de inscripción asignada a través de Apple Configurator 2. Para obtener más información, consulte el [Manual de uso de Apple Business Manager](#) o el [Manual de uso de Apple School Manager](#).

Renovar el token de ADP

Citrix Endpoint Management muestra una advertencia de caducidad de licencia cuando el token de ADP caduca. Reemplace el token desde ASM o ABM.

Paso 1: Descargue una clave pública desde el 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: Cree y descargue un archivo de token de servidor desde su cuenta de Apple

1. Inicie sesión en ABM para descargar el token.
2. Abra **Settings** y seleccione el servidor del que necesita un token. Haga clic en **Edit**.
3. En **MDM Server Settings**, cargue la nueva clave pública que descargó de Citrix Endpoint Management y guarde los cambios.
4. Haga clic en **Download Token** para descargar el nuevo token.

Paso 3: Cargue un archivo de token del servidor en Citrix Endpoint Management

1. En Citrix Endpoint Management, vaya a **Parámetros > 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.

Integración en funciones de Apple Educación

March 1, 2024

Puede usar Citrix Endpoint Management como solución de Administración de dispositivos móviles (MDM) en un entorno que usa Apple Educación. Citrix Endpoint Management admite Apple School Manager (ASM) y la aplicación Aula para iPad. La directiva de configuración de la educación de Citrix Endpoint Management define los dispositivos de profesores y alumnos que van a usarse con Apple Educación.

En el marco de Apple Educación, ofrece iPads preconfigurados y supervisados a profesores y alumnos. Esa configuración incluye la inscripción de ASM en Citrix Endpoint Management, una cuenta administrada de ID de Apple configurada con una contraseña nueva y los iBooks y aplicaciones de compras por volumen obligatorios.

Para obtener más información acerca de las funciones de Apple Educación, consulte el sitio [Educación de Apple](#) y la guía de implantación para el sector educativo en el mismo sitio.

Apple School Manager

Siga estos pasos generales para integrar Citrix Endpoint Management en ASM.

1. Cree una cuenta para su institución en ASM con el fin de inscribir su institución en ASM.
2. Configure una cuenta de compras por volumen de Educación 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 profesor y alumno.
6. Después de ello, puede ofrecer los dispositivos preconfigurados a profesores y alumnos.
7. Administrar datos de profesores, alumnos y clases
8. Si un dispositivo se pierde o alguien lo roba, puede bloquearlo y localizarlo.

Para obtener información sobre cómo inscribirse en ASM y conectar su cuenta con Citrix Endpoint Management, consulte [Implementar dispositivos mediante el Programa de implementación de Apple](#).

Requisitos previos

- NetScaler Gateway
- Perfil de inscripción configurado para MDM+MAM.
- Apple iPad de 3.ª generación (versión mínima) o iPad Mini, con iOS 9.3 (versión mínima)

Nota:

Citrix Endpoint Management no valida cuentas de usuario de ASM en LDAP o Active Directory. Sin embargo, puede conectar Citrix Endpoint Management a LDAP o Active Directory para administrar usuarios y dispositivos no relacionados con profesores y alumnos de ASM. Por ejemplo, puede usar Active Directory para proporcionar Citrix Secure Mail y Citrix Secure Web a otros miembros de ASM, como gestores y administradores de TI.

Como los alumnos y los profesores de ASM son usuarios locales, no es necesario implementar Citrix Secure Hub en sus dispositivos.

No se admiten usuarios locales (solo usuarios de Active Directory) en la inscripción MAM que incluye la autenticación de NetScaler Gateway. Por lo tanto, Citrix Endpoint Management solo implementa los iBooks y las aplicaciones de compras por volumen obligatorios en los dispositivos de profesores y alumnos.

Aplicación Aula para iPad

La aplicación Aula para iPad permite a los profesores conectarse a los dispositivos de los alumnos y administrarlos. Puede ver las pantallas de los iPads, abrir aplicaciones en ellos, abrir y compartir enlaces Web, así como presentar la pantalla de un alumno en Apple TV.

Aula es una aplicación gratuita disponible en el App Store. Usted carga la aplicación en la consola de Citrix Endpoint Management. Luego, se configura a través de la directiva de configuración de la educación, que se implementará a posteriori en los dispositivos de los profesores.

Para obtener más información sobre cómo implementar la aplicación Aula, consulte [Distribuir aplicaciones de Apple](#).

Para obtener más información sobre los requisitos, la instalación y las funciones de la aplicación Aula, consulte el [Manual de uso de Aula](#) del sitio de soporte de Apple.

Agregar contraseñas para los usuarios de Apple School Manager

Después de agregar una cuenta de ASM, Citrix Endpoint Management importa las clases y los usuarios desde ASM. Citrix Endpoint Management trata las clases como grupos locales y, en la consola, se usa el término “grupo” para ellas. Si una clase ya tiene un nombre de grupo en ASM, Citrix Endpoint

Management asigna ese nombre de grupo a la clase. De lo contrario, Citrix Endpoint Management utiliza el ID del sistema de origen para formar el nombre del grupo. Citrix Endpoint Management no utiliza el nombre del curso para nombrar la clase debido a que los nombres de los cursos en ASM no son únicos.

Citrix Endpoint Management utiliza los ID de Apple administrados para crear usuarios locales con el tipo de usuario **ASM**. Los usuarios son locales porque ASM crea las credenciales independientemente de todos los orígenes de datos externos. Por eso, Citrix Endpoint Management no utiliza un servidor de directorio para autenticar a estos usuarios nuevos.

ASM no envía contraseñas de usuario temporales a Citrix Endpoint Management. Puede importarlas desde un archivo CSV o agregarlas manualmente. Para importar contraseñas de usuario temporales:

1. Obtenga el archivo CSV generado por ASM cuando cree las contraseñas temporales de los ID de Apple administrados.
2. Modifique ese archivo CSV, cambie las contraseñas temporales por las contraseñas nuevas que los usuarios deberán proporcionar para inscribirse en Citrix Endpoint Management. No hay ninguna restricción en el tipo de contraseña que se puede utilizar para este propósito.

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**. Aparecerá la página **Usuarios**.

En la siguiente página de ejemplo **Administrar > Usuarios** se muestra una lista de los usuarios importados desde ASM. En la lista **Usuarios**:

- El **Nombre de usuario** es el ID de Apple administrado.
- El tipo de usuario es **ASM**, para indicar que la cuenta proviene de ASM.
- En **Grupos** se muestran las clases.

Devices

Users

Enrollment Invitations

Filters

Local groups

Clear

Role

Clear

Domain

Clear

Education title

Clear

Instructor

7

Student

25

Other

0

Users

Hide filter

Add Local User

Import Local Users

Manage Local Groups

Export

	User name	First name	Last name	User type	Roles	Groups	Domain	Created
<input type="checkbox"/>		Julia	Romero	ASM	USER	SAMPLE-CLASS-1013 - H5.SAMPLE-CLASS-1014 - H5	local	21/07/2017 14:43:00
<input type="checkbox"/>		Kaelyn	Lazzara	ASM	USER	SAMPLE-CLASS-1013 - H5.SAMPLE-CLASS-1014 - H5	local	21/07/2017 14:43:00
<input type="checkbox"/>		Brooklyn	Bailly	ASM	USER	SAMPLE-CLASS-1010 - H5.SAMPLE-CLASS-1014 - H5	local	21/07/2017 14:43:00

4. Haga clic en **Importar usuarios locales**. Aparece el cuadro de diálogo **Importar archivo de aprovisionamiento**.
5. En “Formato”, elija **Usuario ASM**, vaya al archivo CSV que ha preparado en el paso 2 y, a continuación, haga clic en **Importar**.

Import Provisioning File

Format

☐ User ?

☒ ASM user ?

☐ User property ?

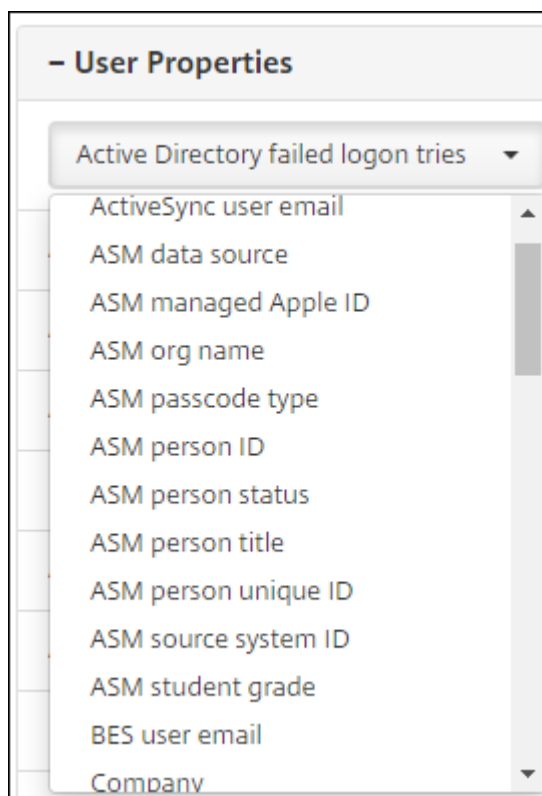
File*

Browse

Cancel

Import

6. Para ver las propiedades de un usuario local, selecciónelo y haga clic en **Modificar**.



Además de las propiedades de nombre, están disponibles estas propiedades de ASM:

- **Origen de datos de ASM:** El origen de los datos de la clase, como **CSV** o **SFTP**.
- **ID de Apple administrado por ASM:** Un ID de Apple administrado puede incluir el nombre de la institución y **appleid**. Por ejemplo, el ID puede ser del tipo **el-sagomez@appleid.micolegio.edu**. Citrix Endpoint Management requiere un ID de Apple administrado para la autenticación.
- **Nombre de la organización de ASM:** El nombre que dio a la cuenta en Citrix Endpoint Management.
- **Tipo de código de acceso de ASM:** La directiva Contraseña de la persona: **complejo** (una contraseña de no alumno con ocho o varios números y letras), **cuatro** (dígitos) o **seis** (dígitos).
- **ID personal único de ASM:** Un identificador del usuario.
- **Estado personal de ASM:** Especifica si el ID de Apple administrado está **Activo** o **Inactivo**. Este estado se activa después de que el usuario proporcione la nueva contraseña de la cuenta de ID de Apple administrado.
- **Título personal de ASM:** Puede ser profesor, alumno u otro.
- **ID personal único de ASM:** Un identificador único para el usuario.
- **ID del sistema de origen de ASM:** Identificador del origen del sistema.
- **Curso del alumno de ASM:** Información del curso del alumno (los profesores no usan esta opción).

Planificar y agregar recursos y grupos de entrega a Citrix Endpoint Management

Con un grupo de entrega, se especifican los recursos que se van a implementar en categorías de usuarios. Por ejemplo, puede crear un grupo de entrega para profesores y alumnos. También puede optar por crear varios grupos de entrega para personalizar las aplicaciones, el contenido multimedia y las directivas que se enviarán a los diferentes profesores o alumnos. Asimismo, puede crear uno o varios grupos de entrega por clase. También puede crear uno o varios grupos de entrega para los administradores (otro personal existente en el centro educativo).

Los recursos que implemente en los dispositivos de usuario incluyen directivas de dispositivo, aplicaciones de compras por volumen y libros de iBooks.

- Directivas de dispositivo:

Si los profesores utilizan la aplicación Aula, se necesita la directiva de configuración de la educación. No olvide consultar otras directivas de dispositivo para determinar cómo configurar y restringir los iPads de profesores y alumnos.

- Aplicaciones de compras por volumen:

Citrix Endpoint Management requiere que implemente las aplicaciones de compras por volumen como aplicaciones obligatorias para los usuarios de Educación. Citrix Endpoint Management no admite la implementación de esas aplicaciones de compras por volumen como opcionales.

Si usa la aplicación Aula de Apple, impleméntela solamente en los dispositivos de los profesores.

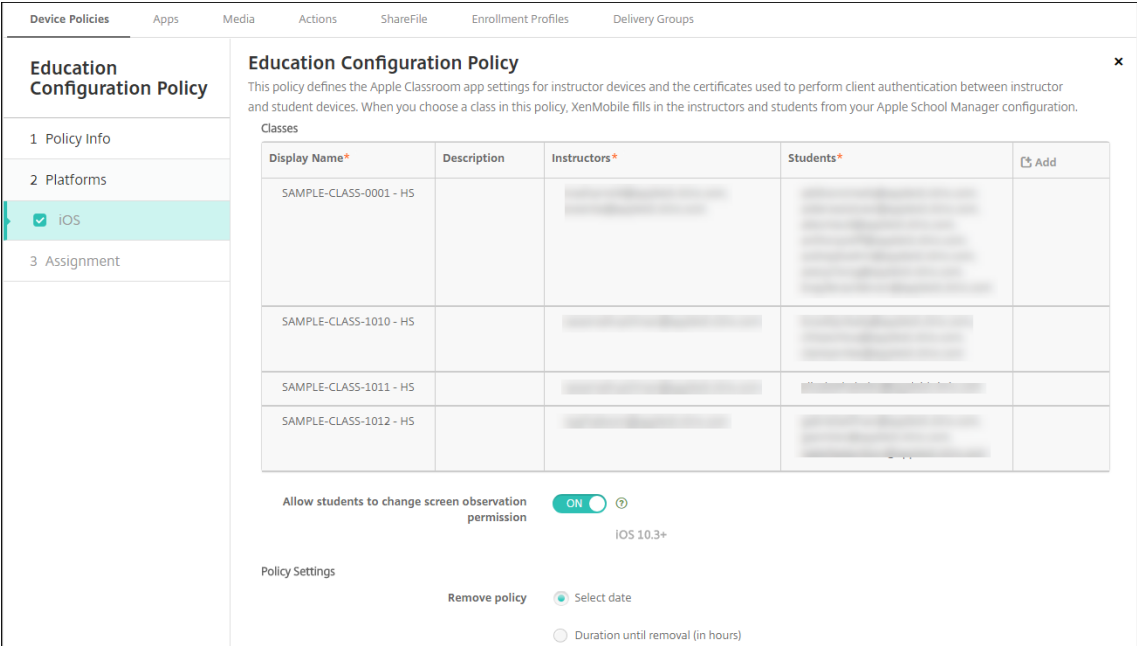
Implemente las demás aplicaciones que quiera proporcionar a profesores o alumnos. Esta solución no usa la aplicación Citrix Secure Hub, de modo que no es necesario implementarla a profesores o alumnos.

- iBooks de compras por volumen:

Una vez que Citrix Endpoint Management se haya conectado a su cuenta de ASM, los libros de iBooks que haya adquirido aparecen en la consola de Citrix Endpoint Management, en **Configurar > Multimedia**. Los libros de iBooks que figuran en dicha página están disponibles para agregarlos a grupos de entrega. Citrix Endpoint Management solo admite que se agreguen libros de iBooks como contenido multimedia obligatorio.

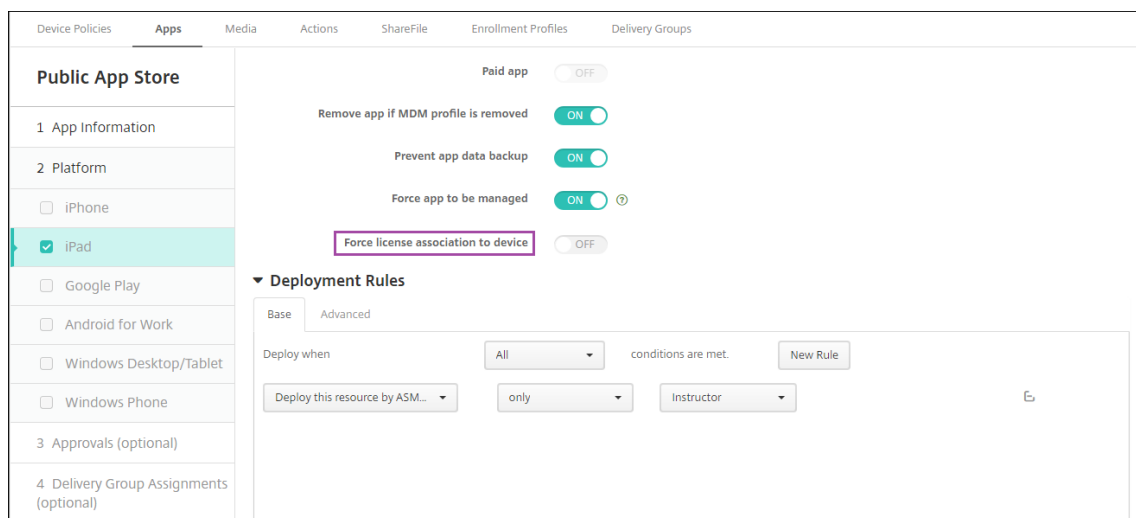
Tras determinar los recursos y los grupos de entrega correspondientes a profesores y alumnos, puede crear esos elementos en la consola de Citrix Endpoint Management.

1. Cree las directivas de dispositivo que quiera implementar en los dispositivos de profesores o alumnos. Para obtener información acerca de la directiva de dispositivo “Configuración de la educación”, consulte [Directiva de configuración de la educación](#).



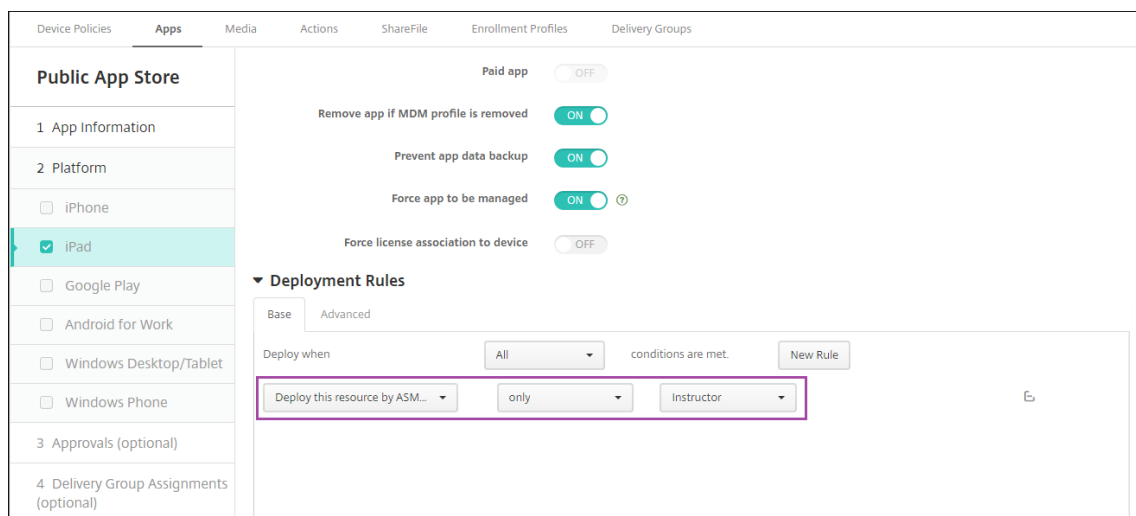
Para obtener más información acerca de las directivas de dispositivo, consulte [Directivas de dispositivo](#) y los artículos concretos de directiva.

2. Configure aplicaciones (**Configurar > Aplicaciones**) y iBooks (**Configurar > Multimedia**):
- De forma predeterminada, Citrix Endpoint Management asigna aplicaciones y libros de iBooks por usuario. Durante la primera implementación, tanto profesores como alumnos reciben una solicitud para registrarse en ASM. Después de aceptar la invitación, los usuarios reciben sus aplicaciones y sus libros de iBooks de ASM durante la siguiente implementación (en las seis horas siguientes). Citrix recomienda forzar la implementación de aplicaciones y libros de iBooks a usuarios nuevos de ASM. Para ello, seleccione el grupo de entrega y haga clic en **Implementar**.
- Puede asignar aplicaciones (pero no libros de iBooks) por dispositivo. Para ello, **active** el parámetro **Forzar asociación de licencia con el dispositivo**. Cuando se asignan aplicaciones a nivel de dispositivo, los usuarios no reciben una invitación para participar en el Programa de compras por volumen.

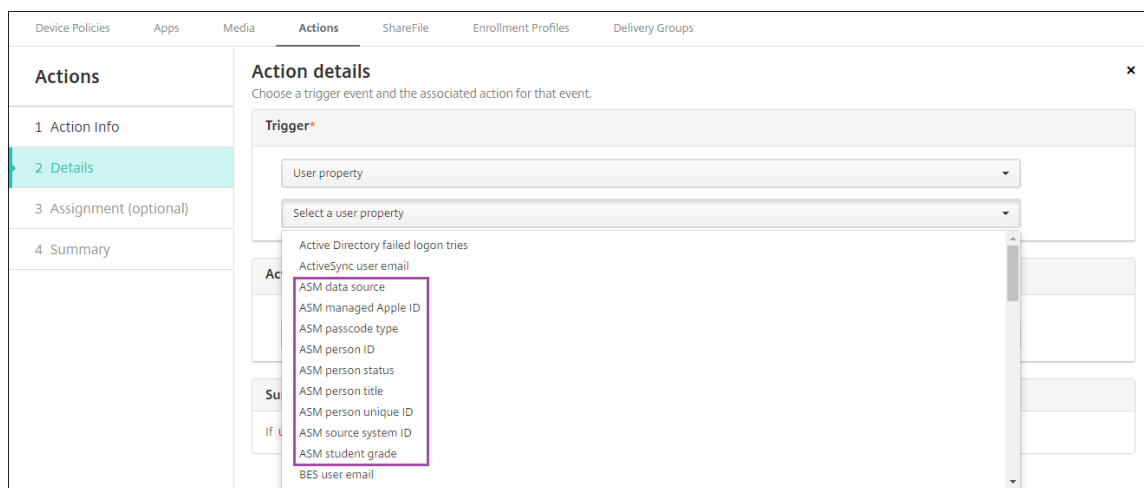


- Para implementar una aplicación solo a profesores, seleccione un grupo de entrega que incluya solo profesores o use la siguiente regla de implementación:

```
1 Deploy this resource by ASM device type
2 only
3 Instructor
4 <!--NeedCopy-->
```



- Si quiere obtener ayuda para agregar aplicaciones de compras por volumen, consulte [Agregar una aplicación de tienda 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 alumno cuando se instale una nueva aplicación en ellos. También puede optar por crear una acción que se active con una propiedad de usuario determinada, como se muestra en el siguiente ejemplo.



Para crear una acción, vaya a **Configurar > Acciones**. Para obtener información detallada sobre cómo configurar las acciones, consulte [Acciones automatizadas](#).

4. En **Configurar > Grupos de entrega**, cree grupos de entrega para profesores y para alumnos. Elija las clases que se importaron desde ASM. Asimismo, cree una regla de implementación para profesores y alumnos.

Por ejemplo, las siguientes asignaciones de usuario son para profesores. La regla de implementación es:

```
1 Limit by user property
2 ASM person title
3 is equal to
4 Instructor
5 <!--NeedCopy-->
```

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

Delivery Group

1 Delivery Group Info

2 User

3 Resource (optional)

Policies

Apps

Media

Actions

ShareFile

Enrollment Profile

4 Summary

User Assignments

Select domain

local

Include user groups

sample

Search

☒ local\SAMPLE-CLASS-0001 - HS

☒ local\SAMPLE-CLASS-1010 - HS

☒ local\SAMPLE-CLASS-1011 - HS

☒ local\SAMPLE-CLASS-1012 - HS

☒ local\SAMPLE-CLASS-1013 - HS

Selected user groups:

local

SAMPLE-CLASS-1013 - HS

SAMPLE-CLASS-1014 - HS

b8d22143-e8c8-4c30-92db-d0f497151137 - HS

SAMPLE-CLASS-1010 - HS

SAMPLE-CLASS-0001 - HS

SAMPLE-CLASS-1012 - HS

MSP

SAMPLE-CLASS-1011 - HS

☒ Or ☐ And

Deploy to anonymous user

OFF

Deployment Rules

Base

Advanced

Limit by user property

ASM person title

is equal to

Instructor

+

⌵

AND

OR

NOT

EDIT

New Rule

Delete

En cambio, las siguientes asignaciones de usuario son para los alumnos. La regla de implementación es:

```
1 Limit by user property
2 ASM person title
3 is equal to
4 Student
5 <!--NeedCopy-->
```

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

Delivery Group

1 Delivery Group Info

2 User

3 Resource (optional)

Policies

Apps

Media

Actions

ShareFile

Enrollment Profile

4 Summary

User Assignments

Select domain

local

Include user groups

sample

Search

local\SAMPLE-CLASS-0001 - H5

local\SAMPLE-CLASS-1010 - H5

local\SAMPLE-CLASS-1011 - H5

local\SAMPLE-CLASS-1012 - H5

local\SAMPLE-CLASS-1013 - H5

Selected user groups:

local

SAMPLE-CLASS-1013 - H5

SAMPLE-CLASS-1014 - H5

b8d22143-e8c8-4c30-92db-d0f497151137 - H5

SAMPLE-CLASS-1010 - H5

SAMPLE-CLASS-0001 - H5

SAMPLE-CLASS-1012 - H5

MSP

SAMPLE-CLASS-1011 - H5

Or

And

Deploy to anonymous user

OFF

Deployment Rules

Base

Advanced

Limit by user property

ASM person title

is equal to

Student

+

-

AND

OR

NOT

EDIT

New Rule

Delete

También puede filtrar un grupo de entrega mediante una regla de implementación basada en el nombre de organización de ASM.

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

Delivery Group

1 Delivery Group Info

2 Assignments

3 Resource (optional)

Policies

Apps

Media

Actions

ShareFile

Enrollment Profile

4 Summary

Or

And

Deploy to anonymous user

OFF

Deployment Rules

Base

Advanced

Deploy when

All

conditions are met.

New Rule

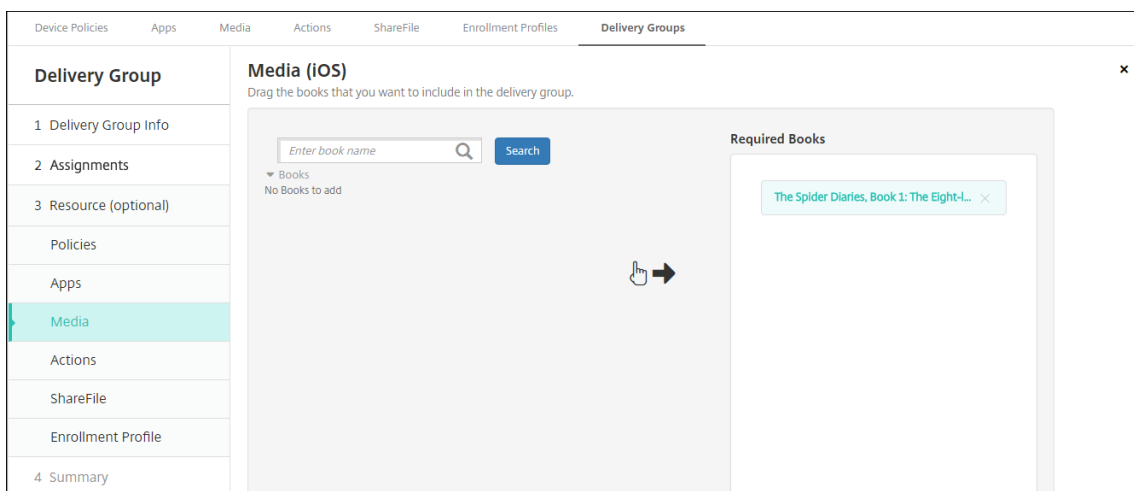
ASM org name

only

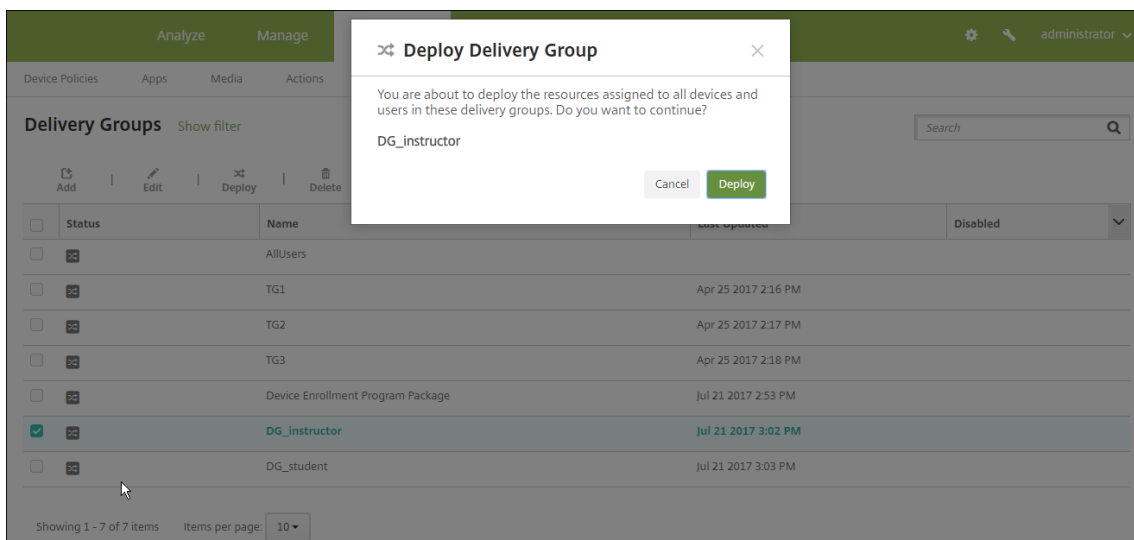
ASM

-

5. Asigne los recursos a los grupos de entrega. En el siguiente ejemplo se muestra un libro de iBook que contiene un grupo de entrega.



En el siguiente ejemplo se muestra el cuadro de confirmación que aparece cuando se selecciona un grupo de entrega y se hace 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 profesor y alumno

Puede inscribir dispositivos mediante uno de los siguientes métodos:

- Un administrador de centro educativo puede inscribir dispositivos de profesores y alumnos con la contraseña de usuario que se estableció en la consola de Citrix Endpoint Management. Por lo tanto, puede facilitar a los usuarios dispositivos que ya están configurados con las aplicaciones y el contenido multimedia pertinente.
- Tras recibir los dispositivos, los usuarios pueden inscribirse con la contraseña de usuario que

se les haya dado. 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, use los dispositivos del Programa de implementación de Apple que están vinculados a ASM.

1. Si los dispositivos no están vinculados a ASM, borre el contenido y los parámetros de estos. Para ello, restablezca el disco duro a los valores de fábrica.
2. Inscriba un dispositivo de ASM con un profesor. A continuación, inscriba un dispositivo de ASM con un alumno.
3. En la página **Administrar > Dispositivos**, compruebe que ambos dispositivos de ASM se inscribieron en modo de solo MDM.

Puede filtrar la página **Dispositivos** por el estado del dispositivo de ASM: **Registrado en ASM**, **Compartido en ASM**, **Profesor** y **Alumno**.

Status	Mode	User name	Serial number	IMEI/MEID	Operating system version	Device model	Last access	Inactivity days	ASM
	MDM				10.3.2	iPad	06/22/2017 07:00:03 pm	0 day	Instru

4. Para verificar que los recursos MDM se hayan implementado correctamente en el dispositivo: seleccione cada dispositivo, haga clic en **Modificar** y revise la información de las distintas páginas.

DevicesUsersEnrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Assigned Policies

5 Apps

6 Media

7 Actions

8 Delivery Groups

9 iOS Profiles

10 iOS Provisioning Profiles

11 Certificates

12 Connections

13 MDM Status

XXXXXXXXXXXX@company.com | iPad

Delivery Groups

Success (1)Pending (0)Failed (0)

Delivery Groups	Time
DG_instructor	31/07/2017 09:00:11

Showing 1 - 1 of 1 items

- Details

Status	Action	Channel/User	Date
Success	Installation result : The Spider Diaries, Book 1: The Eight-legged Monster (Book already installed)		31/07/2017 09:00:11
Success	Installation result : MY LITTLE PONY: Magic Princess Quests - VPP (No need to install)		31/07/2017 09:00:11
Success	Mobileconfig response : EDU (Profile already installed)		31/07/2017 09:00:11
Success	Installation result : Classroom - VPP (No need to install)		31/07/2017 09:00:11
Success	Installation result : The Spider Diaries, Book 1: The Eight-legged Monster (Book already installed)		31/07/2017 03:00:11

Distribuir dispositivos

Apple recomienda organizar un evento para poder distribuir dispositivos a profesores y alumnos.

Si no va a distribuir dispositivos preinscritos, también deberá dar lo siguiente a los usuarios:

- Contraseñas de Citrix Endpoint Management para la inscripción
- Contraseñas temporales de ASM para los ID de Apple administrados.

A continuación, se expone la primera experiencia que tendrá el usuario.

1. La primera vez que un usuario inicia su dispositivo después de un restablecimiento completo, Citrix Endpoint Management le solicita que inscriba el dispositivo en la pantalla de inscripción.
2. El usuario proporciona su ID de Apple administrado y la contraseña de Citrix Endpoint Management que se usa para autenticarse en Citrix Endpoint Management.
3. En el paso de configuración del ID de Apple, el dispositivo pide al usuario que introduzca su ID de Apple administrado y su contraseña temporal de ASM. Esos elementos autentican al usuario en los servicios de Apple.
4. El dispositivo pide al usuario que cree una contraseña para su ID de Apple administrado. Esa contraseña se va a utilizar para proteger sus datos en iCloud.
5. Al final del Asistente de configuración, Citrix Endpoint Management empieza a instalar las directivas, las aplicaciones y el contenido multimedia en el dispositivo. En cuanto a las aplicaciones y los libros de iBooks asignados a cada usuario, el asistente pide a profesores y alumnos que se registren en compras por volumen. Después de aceptar la invitación, los usuarios reciben

sus aplicaciones y sus libros de iBooks de compras por volumen durante la siguiente implementación (en las seis horas siguientes).

Administrar datos de profesores, alumnos y clases

Cuando administre datos de profesores, alumnos y clases, tenga en cuenta lo siguiente:

- No cambie los ID de Apple administrados una vez que haya importado la información de ASM en Citrix Endpoint Management. Citrix Endpoint Management también utiliza identificadores de usuario de ASM para identificar a los usuarios.
- Si agrega o modifica los datos de clase en ASM después de crear una o varias directivas “Configuración de la educación”: modifique las directivas y, a continuación, vuelva a implementarlas.
- Si una clase cambia de profesor después de que haya implementado la directiva de configuración de la educación, revise la directiva para comprobar que se haya actualizado 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 “Título personal de ASM”(alumno, profesor u otro) de la misma forma que recibe las demás propiedades. Por lo tanto, si cambia el “Título personal 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 el curso del alumno y borre el curso del profesor.
2. Si cambia una cuenta de alumno a una cuenta de profesor, quite al usuario de la lista de alumnos que corresponda a la clase. A continuación, agregue el usuario a la lista de profesores de la misma clase u otra.

Si cambia una cuenta de profesor a una cuenta de alumno, quite al usuario de la clase. A continuación, agregue el usuario a la lista de alumnos en la misma clase o en otra. Sus actualizaciones aparecerán en la consola de Citrix Endpoint Management tras la siguiente sincronización (cada cinco minutos de forma predeterminada) o la siguiente obtención de datos (cada 24 horas de forma predeterminada).

3. Modifique la directiva de configuración de la educación para aplicar el cambio y vuelva a implementarla.
 - Si elimina a un usuario en el portal de ASM, Citrix Endpoint Management también eliminará a ese usuario de la consola de Citrix Endpoint Management después de una obtención de datos.

Puede reducir el intervalo entre dos puntos de referencia. Para ello, cambie este valor de propiedad de 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 que solo contenga a ese alumno e implemente los recursos en el dispositivo de ese alumno.
- Si un alumno o profesor pierde su contraseña temporal, deberá ponerse en contacto con el administrador de ASM. El administrador puede proporcionar una contraseña temporal o generar una nueva.

Administrar un dispositivo perdido o robado

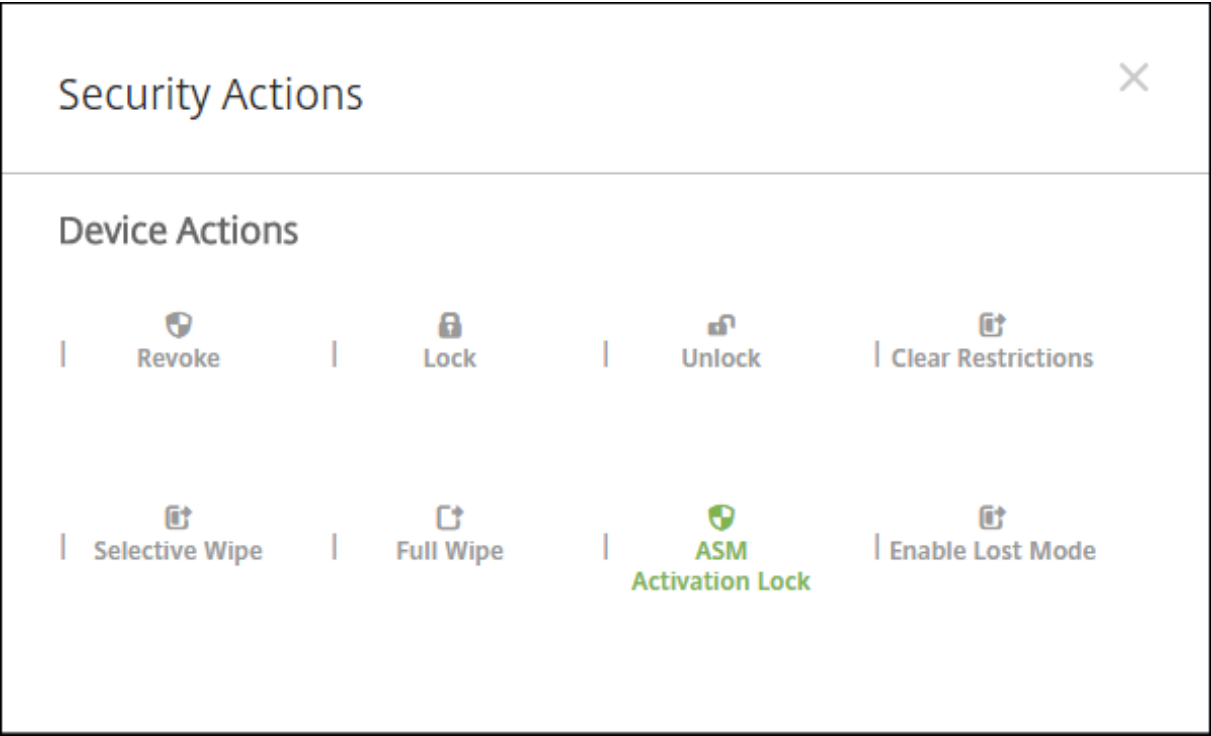
El servicio “Buscar Mi iPhone” o “Buscar Mi iPad” de Apple incluye la función “Bloqueo de activación”. El “Bloqueo de activación” impide que usuarios no autorizados usen o revendan un dispositivo perdido o robado que está inscrito en el Programa de implementación de Apple.

Citrix Endpoint Management incluye la acción de seguridad **Bloqueo de activación de ASM**, que permite enviar un código de bloqueo a un dispositivo inscrito en el Programa de implementación de Apple de ASM.

Cuando se usa la acción de seguridad **Bloqueo de activación de ASM**, Citrix Endpoint Management puede localizar dispositivos sin que los usuarios habiliten el servicio “Buscar Mi iPhone” o “Buscar Mi iPad”. Si un dispositivo de ASM se restablece a los valores de fábrica o se borran todos los datos que contiene, el usuario debe proporcionar su ID de Apple administrado y la contraseña para desbloquear el dispositivo.

Para quitar el bloqueo desde la consola, haga clic en la acción de seguridad **Omisión del 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 en blanco el inicio de sesión y escribir el **Código de anulación del bloqueo de activación de ASM** en el lugar de la contraseña. Esa información está disponible en **Detalles del dispositivo**, en la ficha **Propiedades**.

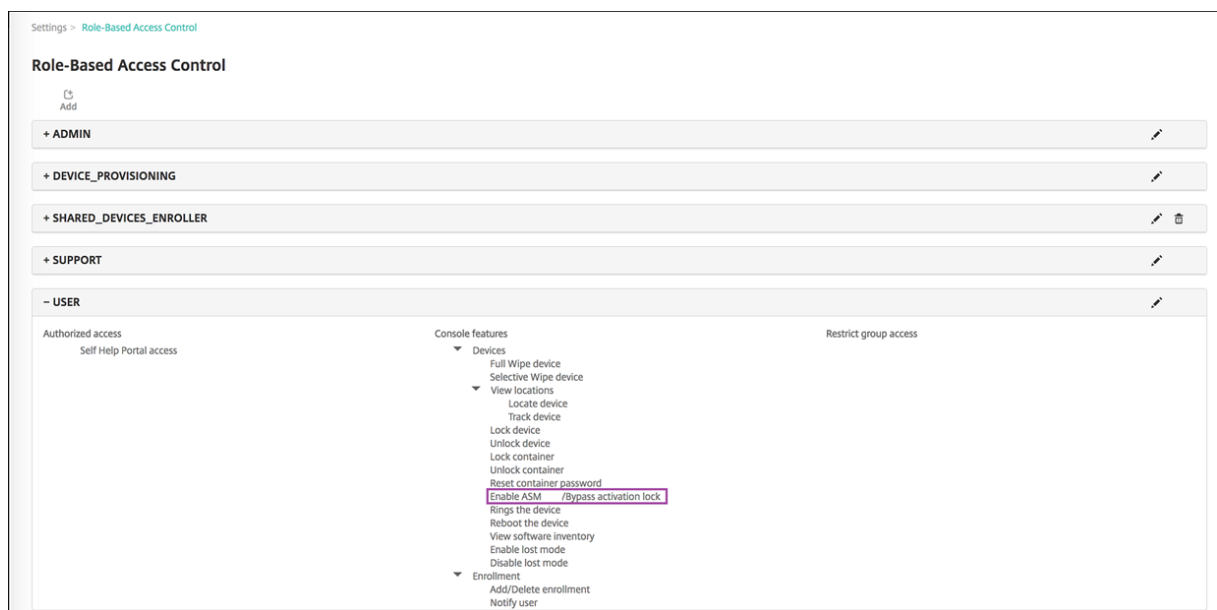
Para establecer el bloqueo de activación, vaya a **Administrar > Dispositivos**, seleccione el dispositivo, haga clic en **Seguridad** y, a continuación, haga clic en **Bloqueo de activación de ASM**.



Las propiedades **Clave de custodia de ASM** y **Código de anulación del bloqueo de activación de ASM** aparecen en **Detalles del dispositivo**.

Devices	Users	Enrollment Invitations
<div>Device details</div> <div><div>1 General</div><div>2 Properties</div><div>3 User Properties</div><div>4 Assigned Policies</div><div>5 Apps</div><div>6 Media</div><div>7 Actions</div><div>8 Delivery Groups</div><div>9 iOS Profiles</div><div>10 iOS Provisioning Profiles</div><div>11 Certificates</div><div>12 Connections</div><div>13 MDM Status</div></div>		
		<div><div>– Security information</div><div>Add</div><div>ASM Automated Device Enrollment escrow key</div><div>ASM Automated Device Enrollment activation lock bypass code</div><div>Activation lock bypass code</div><div>Activation lock enabled</div><div>No</div><div>Hardware encryption capabilities</div><div>Block and file levels encryption</div><div>Internal storage encrypted</div><div>No</div><div>Jailbroken/Rooted</div><div>No</div><div>MDM lost mode enabled</div><div>No</div><div>Passcode compliant</div><div>Yes</div><div>Passcode compliant with configuration</div><div>Yes</div><div>Passcode present</div><div>No</div><div>Supervised</div><div>Yes</div></div>
		<div><div>– Storage space</div><div>Add</div><div>Available storage space</div><div>25.58 GB</div><div>Total storage space</div><div>27.05 GB</div></div>

El permiso de RBAC para un bloqueo de activación ASM se encuentra en **Dispositivos > Habilitar omisión de bloqueo de activación de ASM**.



iPads compartidos

November 29, 2023

La función iPad compartido permite a varios usuarios usar un iPad. La experiencia de cada usuario se puede personalizar aunque los dispositivos se compartan. Puede usar iPads compartidos con fines educativos o comerciales. Apple School Manager (ASM) ofrece los roles de profesor y alumno, además de los roles que ofrece Apple Business Manager (ABM).

Requisitos previos para iPads compartidos

- Apple School Manager o Apple Business Manager
- Citrix Endpoint Management
- Cualquier iPad Pro, iPad de 5.^a generación, iPad Air 2 o posterior y iPad mini 4 o posterior
- Al menos 32 GB de almacenamiento
- Dispositivos supervisados

Configurar iPads compartidos

Varios alumnos o empleados pueden compartir un iPad para distintos fines.

O usted o los propietarios de los dispositivos inscriben los iPads compartidos y luego implementan directivas de dispositivo, aplicaciones y archivos multimedia en ellos. A continuación, los usuarios

proporcionan sus credenciales administradas de ID de Apple para iniciar sesión en un iPad compartido. Si implementó anteriormente una directiva de configuración de la educación en los dispositivos de los alumnos, no es necesario que inicien sesión como “Otro usuario” para compartir esos dispositivos.

Citrix Endpoint Management utiliza dos canales de comunicación para iPads compartidos: el canal del sistema para el propietario del dispositivo (profesor o supervisor) y el canal del usuario para el usuario residente actual (alumno o empleado). Citrix Endpoint Management utiliza esos canales para enviar los comandos MDM apropiados para los recursos que admite Apple.

A continuación, dispone de los recursos que se implementan a través del canal del sistema:

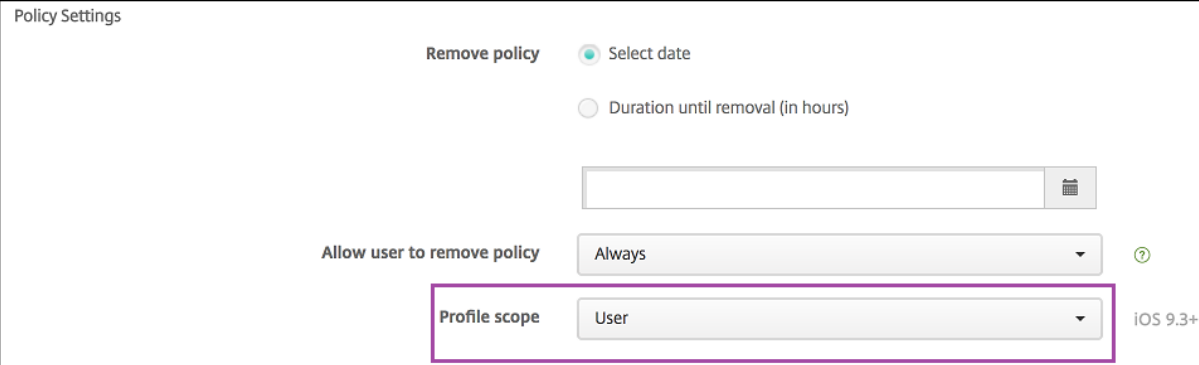
- Directivas de dispositivo: [Configuración de la educación](#), [Mensaje de la pantalla bloqueada](#), [Máximo de usuarios residentes](#) y [Período de gracia de bloqueo de código de acceso](#).
- Aplicaciones de compras por volumen basadas en dispositivos
Apple no admite aplicaciones de empresa ni aplicaciones de compras por volumen basadas en usuarios en iPads compartidos. Las aplicaciones instaladas en un iPad compartido son para todo el dispositivo; no se pueden utilizar por usuario.
- iBooks de compras por volumen basada en usuarios
Apple admite la asignación de iBooks de compras por volumen basados en usuarios en iPads compartidos.

A continuación, dispone de los recursos que se implementan a través del canal del usuario:

- Directivas de dispositivo: Notificaciones de aplicaciones, Diseño de pantalla inicial, Restricciones y Clip Web.

Citrix Endpoint Management solo admite estas directivas por el canal del usuario.

El canal de implementación se especifica cuando se configuran las directivas de dispositivo, en el parámetro **Ámbito del perfil**.



Policy Settings

Remove policy ☒ Select date ☐ Duration until removal (in hours)

Allow user to remove policy Always ⓘ

Profile scope User ⓘ iOS 9.3+

Para eliminar las directivas de dispositivo que implementó por el canal del usuario, debe elegir el **Ámbito de implementación** llamado **Usuario** para la directiva “Eliminación de perfiles”.

Flujo de trabajo general de las tareas

Por lo general, usted distribuye iPads compartidos, preconfigurados y supervisados a los propietarios de dispositivos. A continuación, esas personas distribuyen los dispositivos a los alumnos o a los empleados. Si no distribuye iPads compartidos preinscritos, deberá suministrar a los propietarios de dispositivos sus contraseñas del servidor de Citrix Endpoint Management para que puedan inscribir sus dispositivos.

A continuación, dispone del flujo de trabajo general de las tareas necesarias para configurar e inscribir los iPads compartidos.

1. Utilice la consola de Citrix Endpoint Management Server para agregar cuentas de ASM o ABM (**Parámetros > Programa de implementación de Apple**) con el **Modo compartido** habilitado. Para obtener más información, consulte “Administrar cuentas para iPads compartidos” más adelante.
2. Tal y como se describe en esa sección, debe agregar las directivas, las aplicaciones y los archivos multimedia necesarios a Citrix Endpoint Management. Asigne esos recursos a los grupos de entrega.
3. Pida a los propietarios de dispositivos que realicen un restablecimiento de hardware de los iPads compartidos. Aparece la pantalla de administración remota para la inscripción.
4. Los propietarios de dispositivos inscriben los iPads compartidos.
Citrix Endpoint Management implementa los recursos configurados en cada iPad compartido que se haya inscrito. Tras un reinicio automático, los propietarios de 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 administrado y su contraseña de ASM temporal.
El iPad compartido se autentica en ASM y solicita al usuario que cree una contraseña de ASM. La próxima vez que el usuario del dispositivo inicie sesión en el iPad compartido, dicho usuario proporciona la nueva contraseña de ASM.
6. Otro usuario del dispositivo que comparte el iPad puede, a continuación, repetir el paso anterior e iniciar sesión.

Administrar cuentas para iPads compartidos

Si ya usa Citrix Endpoint Management con Apple Educación o Apple Business, tiene una cuenta de ASM/ABM configurada en Citrix Endpoint Management para dispositivos que no se comparten, como los dispositivos que utilizan los propietarios de dispositivos. Puede usar la misma cuenta de ASM/ABM y el mismo servidor de Citrix Endpoint Management para dispositivos compartidos y no compartidos.

Organizar iPads compartidos en grupos de dispositivos

ASM/ABM permite agrupar dispositivos. Para ello, debe crear varios servidores MDM. Al asignar iPads compartidos a un servidor MDM, cree un grupo de dispositivos para cada grupo de iPads compartidos:

- Grupo de iPads compartidos 1 > Grupo de dispositivos 1 del servidor MDM
- Grupo de iPads compartidos 2 > Grupo de dispositivos 2 del servidor MDM
- Grupo de iPads compartidos N > Grupo de dispositivos N del servidor MDM

Agregar cuentas de ASM a cada grupo de dispositivos

Al crear varias cuentas de ASM/ABM desde la consola del servidor de Citrix Endpoint Management, importa automáticamente los grupos de iPads compartidos:

- Grupo de dispositivos 1 del servidor MDM > Grupo de dispositivos 1 de la cuenta
- Grupo de dispositivos 2 del servidor MDM > Grupo de dispositivos 2 de la cuenta
- Grupo de dispositivos N del servidor MDM > Grupo de dispositivos N de la cuenta

A continuación, dispone de los requisitos específicos para iPads compartidos:

- Una cuenta de ASM/ABM para cada grupo de dispositivos con estos parámetros habilitados:
 - **Requerir inscripción del dispositivo**
 - **Modo supervisado**
 - **Modo compartido**
- Para una organización educativa determinada, debe usar el mismo **Sufijo de educación** para todas las cuentas de ASM.

Aplicaciones para iPads compartidos

iPads compartidos admite la asignación de aplicaciones de compras por volumen basadas en el dispositivo. Antes de implementar una aplicación en un iPad compartido, Citrix Endpoint Management envía una solicitud al servidor de compras por volumen de Apple para asignar licencias de compras por volumen a los dispositivos. Para consultar las asignaciones de compras por volumen, vaya a **Configurar > Aplicaciones > iPad** y expanda **Compras por volumen**.

Multimedia para iPads compartidos

iPads compartidos admite la asignación de iBooks de compras por volumen basada en el usuario. Antes de implementar iBooks en un iPad compartido, Citrix Endpoint Management envía una solicitud

al servidor de compras por volumen de Apple para asignar licencias de compras por volumen a los usuarios. Para consultar las asignaciones de compras por volumen, vaya a **Configurar > Multimedia > iPad** y expanda **Compras por volumen**.

Deployment Rules

Base Advanced

Deploy when: All conditions are met. New Rule

Deploy this resource by device model: only iPad

Device operating system version: is greater than or equal to 9.3

Supervised: True

Apple Deployment Program account name: only ASM Automated Device Enrollment

Volume Purchase

Volume purchase License: Use Volume purchase company token

Volume purchase Account: test

Volume purchase ID Assignment

License ID	Usage Status	Associated User
7545903139	Used	
7545903138	Used	

License Usage: 2 of 5

Back Next >

Reglas de implementación para iPads compartidos

Para la implementación de iPads compartidos, las reglas a nivel de grupo de entrega no se aplican porque están relacionadas con propiedades de usuario. Para filtrar las directivas, las aplicaciones y los archivos multimedia por grupo de dispositivos, agregue una regla de implementación para los recursos según el nombre de la cuenta. Por ejemplo:

- Para la cuenta del grupo de dispositivos 1, configure esta regla de implementación:

```
1 Apple Deployment Program account name
2 Only
3 Device Group 1 account
4
5 <!--NeedCopy-->
```

- Para la cuenta del grupo de dispositivos 2, configure esta regla de implementación:

```
1 Apple Deployment Program account name
2 Only
3 Device Group 2 account
4
5 <!--NeedCopy-->
```

- Para la cuenta del grupo de dispositivos N, configure esta regla de implementación:

```
1 Apple Deployment Program account name
2 Only
3 Device Group N account
4
5 <!--NeedCopy-->
```

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

Apps Notifications Policy

1 Policy Info

2 Platforms

IOS

3 Assignment

Calendar	True	True	True	True	True	True	None	
Mail	True	True	True	True	True	True	None	
Maps	True	True	True	True	True	True	None	
Wallet	True	True	True	True	True	True	None	

Policy Settings

Remove policy

Select date

Duration until removal (in hours)

Allow user to remove policy

Always

Profile scope

User

IOS 9.3+

Deployment Rules

Base

Advanced

Deploy when

All

conditions are met.

New Rule

Deploy this resource by device model

only

iPad

Device operating system version

is greater than or equal to

9.3

Supervised

True

Apple Deployment Program account name

only

ASM Automated Device Enrollment

Back

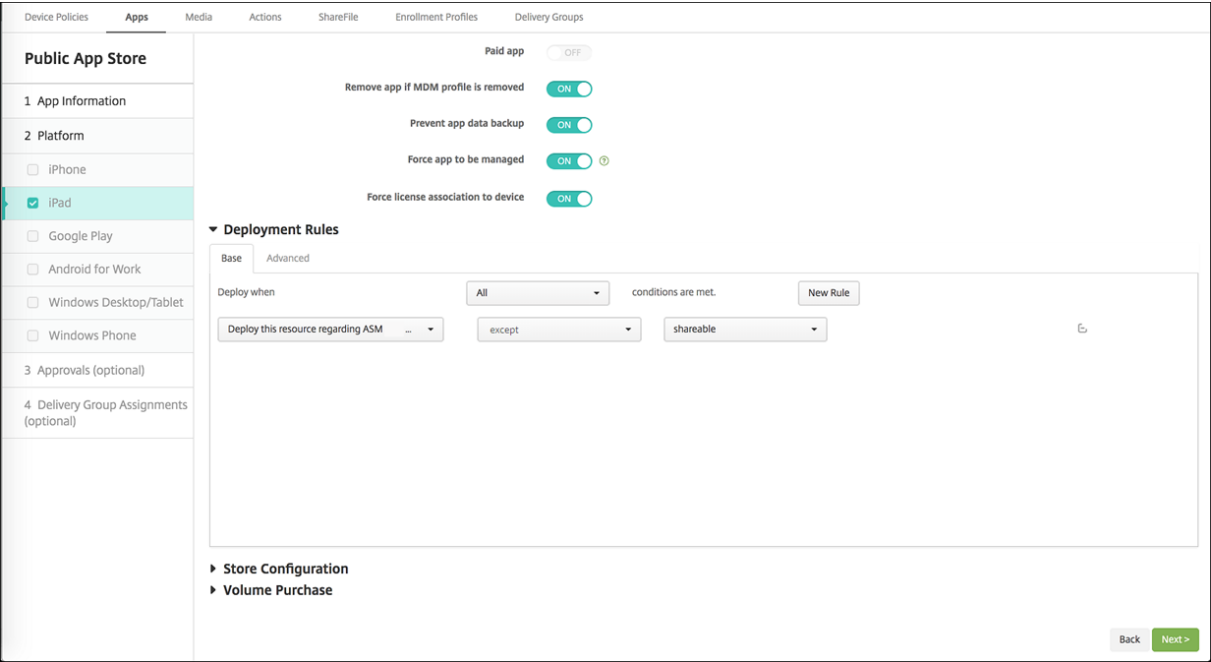
Next >

Para implementar la aplicación Aula de Apple solo a los propietarios de dispositivos (que utilizan iPads no compartidos), filtre los recursos por estado compartido en ASM con estas reglas de implementación:

```
1 Deploy this resource regarding ASM/ABM shared mode
2 only
3 unshared
4
5 <!--NeedCopy-->
```

O bien:

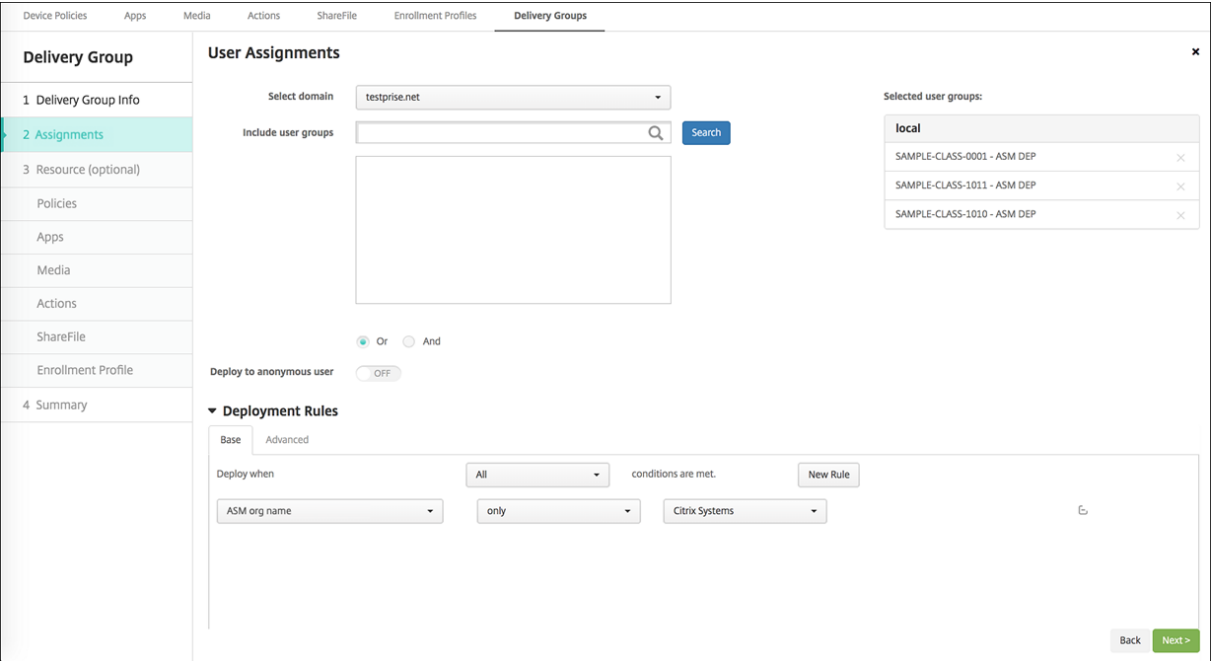
```
1 Deploy this resource regarding ASM/ABM shared mode
2 except
3 shareable
4
5 <!--NeedCopy-->
```



Grupos de entrega para iPads compartidos

Para el grupo de dispositivos:

- Configure un grupo de entrega. Para los profesores, asigne todas las clases definidas en la directiva Configuración de la educación.



- Ese grupo de entrega debe incluir estos recursos de MDM:

- Directivas de dispositivo:
 - ★ Configuración de la educación (para ASM)
 - ★ Mensaje de la pantalla bloqueada
 - ★ Notificaciones de aplicaciones
 - ★ Diseño de pantalla inicial
 - ★ Restricciones
 - ★ Máximo de usuarios residentes
 - ★ Período de gracia de bloqueo de código de acceso
- Aplicaciones de compras por volumen requeridas
- iBooks de compras por volumen requeridos

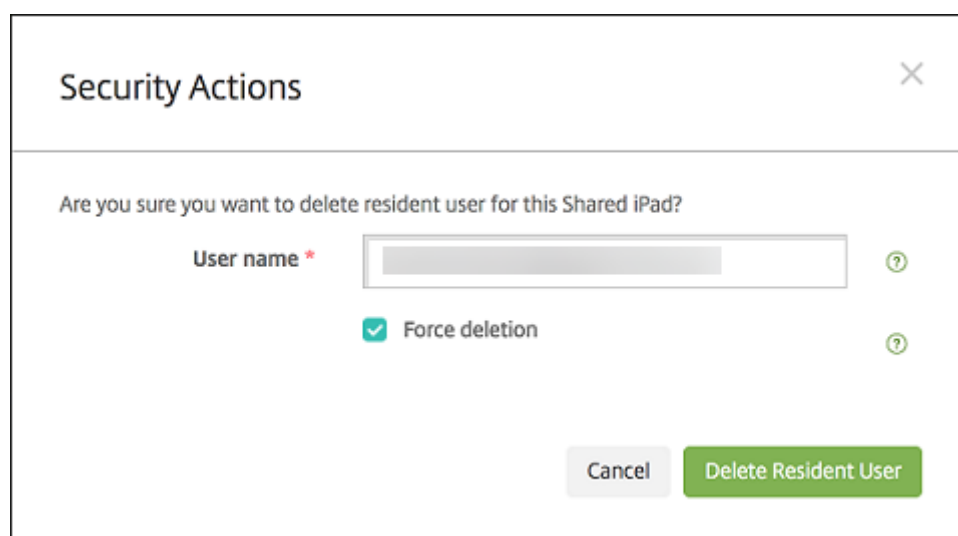
Acciones de seguridad para iPads compartidos

Además de las acciones de seguridad existentes, puede usar estas acciones de seguridad para iPads compartidos:

- **Obtener usuarios residentes:** Ofrece una lista de 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:** Obliga al cierre de sesión del usuario actual.
- **Eliminar usuario residente:** Elimina la sesión actual de un usuario específico. El usuario puede volver a iniciar sesión.
- **Eliminar todos los usuarios:** Elimina todos los usuarios del dispositivo.



Después de hacer clic en **Eliminar usuario residente**, puede especificar el nombre del 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

Dispone de información específica de iPads compartidos en la página **Administrar > Dispositivos**:

- Puede ver:
 - Si un dispositivo se comparte (**Compartido en ASM/ABM**)
 - Quién está conectado al dispositivo compartido (**Usuario conectado de ASM/ABM**)
 - Todos los usuarios asignados al dispositivo compartido (**Usuarios residentes de ASM**)

Devices									
Device Whitelist Users Enrollment Invitations									
<div>Search</div>									
Refresh									
	Serial number	Device platform	Operating system version	Device model	ASM device type	ASM shared	ASM logged-in user	ASM resident users	
eid.citrix.com eid.citrix.com*		iOS	11.2.2	iPad	Instructor	Yes			

- Puede filtrar la lista de dispositivos por el **Estado del dispositivo ASM/ABM**:

Devices									
Device Whitelist Users Enrollment Invitations									
<div>Search</div>									
<div>Device Status Clear</div>									
<div>Device Ownership Clear</div>									
<div>Shared Status Clear</div>									
<div>Inactive Time Clear</div>									
<div>User Location Clear</div>									
<div>App Restrictions Clear</div>									
<div>ASM Device Status Clear</div>									
<div>ASM registered 2</div>									
<div>ASM shared 1</div>									
platform	Operating system version	Device model	ASM device type	ASM shared	ASM logged-in user	ASM resident users			
	11.2.2	iPad	Instructor	Yes					

- Puede consultar datos sobre el usuario que inició sesión en un iPad compartido desde la página **Administrar > Dispositivos > Propiedades del usuario conectado**.

DevicesUsersEnrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Logged-in User Properties

5 Assigned Policies

6 Apps

7 Media

8 Actions

9 Delivery Groups

10 iOS Profiles

11 iOS Provisioning Profiles

12 Certificates

13 Connections

14 MDM Status

| iPad

User Properties

User name

Enter new password

Role *
USER

Membership

local\Android Default Group

local\Android SD Enroller Group

local\Android SD Group

local\Apple Configurator Group

local\CWC_GRP

Manage Groups

VPP Accounts

ASM VPP

Retire

Back

Next >

DevicesUsersEnrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Logged-in User Properties

5 Assigned Policies

6 Apps

7 Media

8 Actions

9 Delivery Groups

10 iOS Profiles

11 iOS Provisioning Profiles

12 Certificates

13 Connections

14 MDM Status

- User Properties

Add

ASM DEP org name	Citrix Systems
ASM person title	Student
ASM person unique ID	
Name	Brayden Anderson
ASM source system ID	S25-008
ASM person status	Active
First name	Brayden
ASM person ID	SAMPLE-STUDENT-0008
ASM managed Apple ID	
Surname	Anderson
ASM student grade	4
ASM passcode type	four
ASM data source	SFTP

Back

Next >

- Puede ver el canal utilizado para implementar recursos a los propietarios de dispositivos y los usuarios en un grupo de entrega desde la página **Administrar > Dispositivos > Grupos de entrega**. La columna **Canal/usuario** muestra el tipo (**Sistema** o **Usuario**) y el destinatario.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

585

Devices

Users

Enrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Logged-in User Properties

5 Assigned Policies

6 Apps

7 Media

8 Actions

9 Delivery Groups

10 iOS Profiles

11 iOS Provisioning Profiles

12 Certificates

13 Connections

14 MDM Status

Connections

First connection

8/30/17 12:42:38 pm

Status

Active

Last connection

11/30/17 5:48:04 pm

User name	Penultimate authentication	Last authentication	Has data to sync	Data quota	Data used	Is logged-in
	10/12/17 10:15:34 am	10/12/17 10:19:00 am				
	11/23/17 3:45:28 pm	11/23/17 3:45:29 pm				
	11/23/17 5:48:03 pm	11/23/17 5:48:03 pm				
	11/30/17 5:48:03 pm	11/30/17 5:48:04 pm				
	11/30/17 5:48:03 pm	11/30/17 5:48:04 pm	Yes			Yes
	11/29/17 7:02:32 pm	11/29/17 7:02:32 pm	No		120.82 MB	No

Showing 1 - 6 of 6 items

Back

Next >

- Puede ver el estado de envío por ambos canales.

Devices

Device Whitelist

Users

Enrollment Invitations

Device details

2 Properties

3 User Properties

4 Logged-in User Properties

5 Assigned Policies

6 Apps

7 Media

8 Actions

9 Delivery Groups

10 iOS Profiles

11 iOS Provisioning Profiles

12 Certificates

13 Connections

14 MDM Status

System channel

Push status

Active

Last push initiation

1/24/18 1:00:03 pm

Last notification completion

1/24/18 1:00:03 pm

Last reply time

1/24/18 1:00:03 pm

User channel

Push status

Active

Last push initiation

1/24/18 1:00:03 pm

Last notification completion

1/24/18 1:00:03 pm

Last reply time

1/24/18 1:00:03 pm

Refresh

Back

Save

Distribuir aplicaciones de Apple

November 29, 2023

Citrix Endpoint Management administra las aplicaciones implementadas en los dispositivos. Puede

organizar e implementar los siguientes tipos de aplicaciones iOS, iPadOS y macOS.

- **Tienda pública de aplicaciones (solo para iOS/iPadOS):** Este grupo contiene las aplicaciones, gratuitas o de pago, disponibles en una tienda pública de aplicaciones, como App Store de Apple o Google Play. Por ejemplo, GoToMeeting.
- **Empresarial (para iOS, iPadOS y macOS):** Aplicaciones nativas que no están habilitadas para MDX y no contienen las directivas asociadas a aplicaciones MDX.
- **MDX (solo para iOS/iPadOS):** Aplicaciones preparadas con el SDK de MAM o empaquetadas con MDX Toolkit. Estas aplicaciones incluyen directivas MDX. Las aplicaciones MDX se obtienen de fuentes internas y tiendas públicas.
- **Compras por volumen (para iOS, iPadOS y macOS):** Aplicaciones con licencias administradas a través del Programa de compras por volumen de Apple.
- **Aplicaciones iOS personalizadas (solo para iOS/iPadOS):** Aplicaciones propietarias B2B desarrolladas por equipos internos o externos.

Para obtener más información sobre diferentes tipos de aplicaciones, consulte [Agregar aplicaciones](#).

Algunas implementaciones requieren una cuenta de Apple Business Management (ABM) o de Apple School Management (ASM). Para obtener más información, consulte las secciones siguientes.

Para cada tipo de aplicación y método de distribución, Citrix recomienda una serie de directrices de configuración. Para obtener información sobre la distribución de aplicaciones para otras plataformas, consulte [Agregar aplicaciones](#). Las secciones siguientes proporcionan información más detallada sobre 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 tienda pública de aplicaciones, incluidas las aplicaciones de movilidad de Citrix	No aplicable	En Citrix Endpoint Management: Configurar > Aplicaciones , agregue aplicaciones de Tienda pública de aplicaciones para iPhone o iPad. Configure las aplicaciones y asígnelas a grupos de entrega.	En Citrix Endpoint Management: Configure e implemente aplicaciones mediante grupos de entrega.
Aplicaciones de tienda pública de aplicaciones entregadas con las compras por volumen de Apple, incluidas las aplicaciones de movilidad de Citrix	Inscríbase en un Programa de implementación de Apple. En Citrix Endpoint Management: Vaya a Parámetros > Compras por volumen para agregar su cuenta de compras 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 grupos de entrega.	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 empresa	No aplicable	En Citrix Endpoint Management: Vaya a Configurar > Aplicaciones . Haga clic en Agregar y, a continuación, en Empresarial . Cargue el archivo IPA. Configure las aplicaciones y asígneles a grupos de entrega.	En Citrix Endpoint Management: Configure e implemente aplicaciones mediante grupos de entrega.
Aplicaciones MDX	No aplicable	En Citrix Endpoint Management: Vaya a Configurar > Aplicaciones . Haga clic en Agregar y, a continuación, en MDX . Asegúrese de seleccionar iPad/iPhone para la plataforma. Cargue el archivo MDX. Configure las aplicaciones y asígneles a grupos de entrega.	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 MDX distribuidas mediante compras por volumen de Apple	Inscríbase en un Programa de implementación de Apple. En Citrix Endpoint Management: Vaya a Parámetros > Compras por volumen para agregar su cuenta de compras por volumen.	En ABM: Compre y agregue aplicaciones MDX desde Aplicaciones y Libros. Vincule la aplicación con su cuenta de ABM. En Citrix Endpoint Management: Vaya a Configurar > Aplicaciones , configure las aplicaciones y asígnelas a grupos de entrega.	En Citrix Endpoint Management: Configure e implemente aplicaciones mediante grupos de entrega.
Aplicaciones personalizadas	Inscríbase en un Programa de implementación de Apple. En Citrix Endpoint Management: Vaya a Parámetros > Compras por volumen para agregar su cuenta de compras por volumen.	En ABM: Agregue su aplicación al App Store como aplicación privada. Vincúlela con su cuenta de ABM. En Citrix Endpoint Management: Vaya a Configurar > Aplicaciones , configure las aplicaciones y asígnelas a grupos de entrega.	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 personalizadas que se han habilitado para MDX	Inscríbase en un Programa de implementación de Apple. En Citrix Endpoint Management: Vaya a Parámetros > Compras por volumen para agregar su cuenta de compras por volumen.	En ABM: Agregue su aplicación al App Store como aplicación privada. Vincúlela con su cuenta de ABM. En Citrix Endpoint Management: Vaya a Configurar > Aplicaciones y cargue el archivo MDX. Configure las aplicaciones y asígneles a grupos de entrega.	En Citrix Endpoint Management: Configure e implemente aplicaciones mediante grupos de entrega.

Aplicaciones de la tienda pública de aplicaciones

Puede agregar a Citrix Endpoint Management aplicaciones gratuitas y de pago disponibles en el App Store.

Disponibilidad de funciones

Se necesita la 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 pública de aplicaciones**.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX
Apps wrapped with the **MDX Service** to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: Secure Mail

Public App Store
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

Enterprise
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Seleccione **iPhone** o **iPad** como plataformas.
4. Introduzca el nombre de la aplicación en el cuadro de búsqueda y haga clic en **Buscar**.

Device Policies
Apps
Media
Actions
ShareFile
Enrollment Profiles
Delivery Groups

Public App Store
1 App Information
2 Platform Clear All
☒ iPhone
☒ iPad
☐ Google Play
☐ Android Enterprise
☐ Windows Desktop/Tablet
☐ Windows Phone
3 Approvals (optional)
4 Delivery Group Assignments (optional)

iPhone App Settings
Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.
 Search
Search results for podio in iPhone apps

Podio Podio

Pódio das Frutas Mais Agência Web LT...

TodayPodio Angelo Vallauri

Todo Cross Dequo

Spokn: Big Ideas in m... PODIO.XYZ, INC.

Didn't find the app you were looking for?

5. Aparecerán las aplicaciones que coincidan con los criterios de búsqueda. Haga clic en la aplicación correspondiente.
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 quiera configurar y haga clic en **Modificar**.
3. Citrix recomienda habilitar la función **Forzar 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 obliga-**

torias.

Delivery Group

1 Delivery Group Info

2 Assignments

3 Resource (optional)

Policies

Apps

Media

Actions

ShareFile

Enrollment Profile

4 Summary

Apps

Drag the apps that you want to include in the delivery group. Apple User Enrollment does not support public app store apps unless deployed through volume purchase.

twitter

Search

Apps

Required Apps

twitter

Optional Apps

- 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 la aplicación se instala en segundo plano después de que los usuarios la hayan aceptado.



Aplicaciones del tienda pública de aplicaciones entregadas con las compras por volumen de Apple

Puede administrar licencias de aplicaciones iOS/iPadOS a través del Programa de compras por volumen de Apple. Siga estos pasos para agregar a Citrix Endpoint Management aplicaciones de compras por volumen.

Disponibilidad de funciones

Se necesita la 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 inscríbese en Apple Business Manager (ABM) o en 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 compras por volumen, consulte [Compras por volumen de Apple](#).
3. Al agregar su cuenta de compras por volumen, habilite **Actualización automática de aplicaciones**. Este parámetro garantiza que las aplicaciones de los dispositivos de usuario se actualicen automáticamente cuando aparece una actualización en el Apple Store. Si una aplicación tiene habilitado el parámetro **Forzar administración de la aplicación**, esta se actualiza sin avisar al usuario. La actualización se produce independientemente de si la aplicación es obligatoria u opcional.

Para usar los parámetros **Forzar administración de la aplicación** y **Actualización automática de aplicaciones**, habilite la propiedad `apple.app.force.managed` del servidor. Consulte [Propiedades de servidor](#).

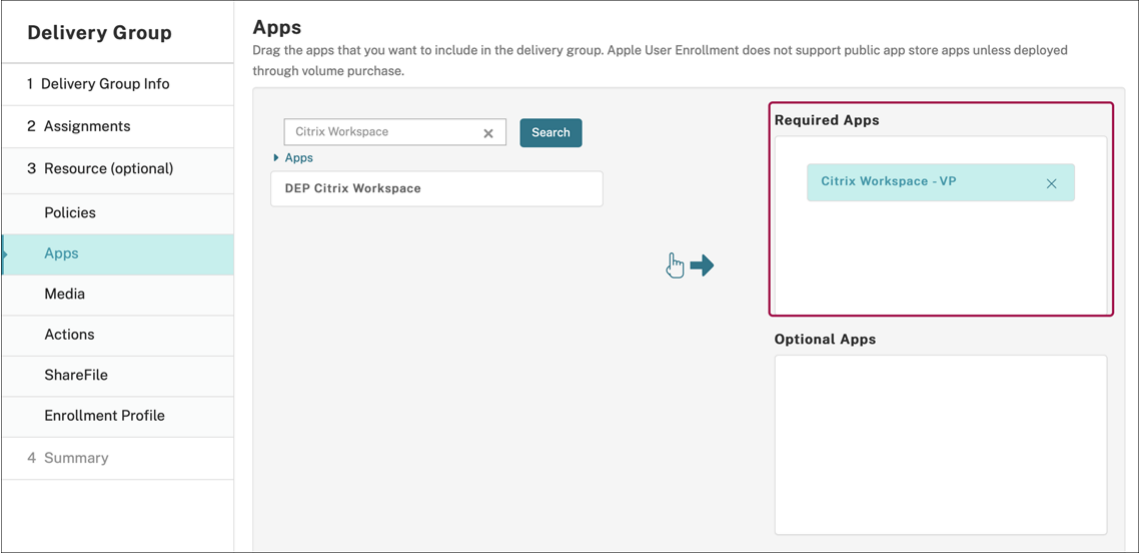
Paso 2: Obtener aplicaciones y licencias de Apple

Compre 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 las que son gratuitas. Una vez que adquiere licencias en ABM/ASM, Citrix Endpoint Management muestra la aplicación automáticamente.

Para obtener información sobre cómo poner 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 compras por volumen que quiera configurar y haga clic en **Modificar**.
3. Seleccione las plataformas: **iPhone, iPad o macOS**.
4. Citrix recomienda habilitar la función **Forzar administración de la aplicación** (solo para 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 obligatorias**.



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 la aplicación se instala en segundo plano después de que los usuarios la hayan aceptado.



Aplicaciones de empresa

También puede agregar aplicaciones nativas que no tengan asociada ninguna directiva MDX. Siga estos pasos para agregar aplicaciones que no existen en el App Store.

Disponibilidad de funciones

Se necesita la supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	Sí
SO	iOS/iPadOS/macOS

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 **Empresa**.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX
Apps wrapped with the **MDX Service** to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: Secure Mail

Public App Store
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

Enterprise
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. En la página **Información de la aplicación**, configure lo siguiente:

- **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en Nombre de la aplicación, en la tabla Aplicaciones.
- **Descripción:** Escriba, si quiere, una descripción de la aplicación.
- **Categoría de la aplicación:** Si quiere, en la lista, haga clic en la categoría a la que se agregará la aplicación.

4. Haga clic en **Siguiente**. Aparecerá la página de las **plataformas de la aplicación**.

5. Seleccione las plataformas: **iPhone**, **iPad** o **macOS**.

6. Cargar el archivo IPA (para iOS y iPadOS) o cargar el archivo PKG (para macOS)

7. Haga clic en **Siguiente**. Aparecerá la página de **Detalles de la aplicación**.

8. Configure estos parámetros:

- **Nombre de archivo:** Si quiere, escriba un nuevo nombre para la aplicación.
- **Descripción de la aplicación:** Si quiere, indique una nueva descripción de la aplicación.
- **Versión de la aplicación:** Este campo no se puede cambiar.
- **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
- **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
- **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
- **Quitar aplicación si se quita el perfil MDM:** Seleccione si quiere quitar la aplicación de un dispositivo cuando se quite el perfil de MDM. El valor predeterminado es Sí. (solo iOS/i-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

598

PadOS)

- **Impedir copia de seguridad de datos de la aplicación:** Seleccione si quiere impedir que la aplicación realice copias de seguridad de los datos. El valor predeterminado es Sí. (solo iOS/iPadOS)
- **Forzar administración de la aplicación:** Si instala una aplicación no administrada, **active** esta opción para que los usuarios de dispositivos no supervisados vean un mensaje en que se les solicita permiso para administrarla. Si el usuario acepta la solicitud, la aplicación se administrará. Si una aplicación tiene habilitado el parámetro **Forzar administración de la aplicación**, esta se actualiza sin avisar al usuario. La actualización se produce independientemente de si la aplicación es obligatoria u opcional (solo para iOS/iPadOS).

Para usar los parámetros **Forzar administración de la aplicación** y **Actualización automática de aplicaciones**, habilite la propiedad `apple.app.force.managed` del servidor. Consulte [Propiedades de servidor](#).

Enterprise	iOS Enterprise App
1 App Information	Upload an .ipa file <input type="button" value="Upload"/>
2 Platform	<div> <div> <input checked="" type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Android (legacy DA) <input type="checkbox"/> Samsung KNOX <input type="checkbox"/> Android Enterprise <input type="checkbox"/> Windows Phone <input type="checkbox"/> Windows Desktop/Tablet <input type="checkbox"/> Workspace Hub </div> <div> App name * <input type="text" value="Hello Cordova"/> Description * <input type="text" value="Hello Cordova"/> App version <input type="text" value="2.0.0"/> Minimum OS version <input type="text" value="8.0"/> Maximum OS version <input type="text"/> Excluded devices <input type="text" value="example: manufacturer or model, ..."/> Package ID <input type="text" value="com.citrix.hellocordova"/> </div> </div>
3 Approvals (optional)	Remove app if MDM profile is removed <input checked="" type="checkbox"/>

9. 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 > Grupos de entrega**. Seleccione el grupo de entrega que quiera configurar y haga clic en la página **Aplicaciones**.
2. Arrastre las aplicaciones deseadas al cuadro **Aplicaciones obligatorias**.

Delivery Group	Apps
1 Delivery Group Info	Drag the apps that you want to include in the delivery group. Apple User Enrollment does not support public app store apps unless deployed through volume purchase.
2 Assignments	<div><input type="text" value="B2B"/> × Search</div> <div><div>Apps</div><div>SecureMail B2B - RGTE</div><div>SecureMail B2B - VP</div></div> <div>➡</div>
3 Resource (optional)	<div>Required Apps</div> <div><div>B2B</div>×</div> <div>Optional Apps</div> <div></div>
Policies	
Apps	
Media	
Actions	
ShareFile	
Enrollment Profile	
4 Summary	

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 la aplicación se instala en segundo plano después de que los usuarios la hayan aceptado.



Aplicaciones MDX

Para usar las directivas MDX y las funciones de seguridad, agregue aplicaciones que estén habilitadas para el SDK de MAM o empaquetadas con MDX. Puede implementar aplicaciones MDX mediante las compras por volumen o sin ellas.

Disponibilidad de funciones

Se necesita la 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 pública de aplicaciones, siga los pasos descritos en Aplicaciones de la tienda pública de aplicaciones y, a continuación, siga los pasos que se indican en 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**.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Service to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: Secure Mail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

- 3. Seleccione **iPhone o iPad** como plataformas.
- 4. Cargue el archivo MDX.

5. Configure los detalles de la aplicación. **Desactive Aplicación implementada mediante las compras por volumen.** Citrix también recomienda habilitar la función **Forzar administración de la aplicación.**

Use the [MDX Service](#) on Citrix Cloud to wrap an app for delivery.

File name *	Secure Mail
App Description *	Managed Enterprise Application
App version	19.3.5
Package ID	XGFUKY3NSP.com.citrix.mail.ios
Minimum OS version	10.0
Maximum OS version	
Excluded devices	example: manufacturer or model ...
Remove app if MDM profile is removed	ON
Prevent app data backup	ON
Force app to be managed	ON ⓘ
App deployed via Volume purchase	OFF ⓘ
▼ MDX Policies	
Authentication	
Device passcode	OFF ⓘ

6. Configure las directivas MDX. **Active** la opción **Inhabilitar actualización obligatoria.**

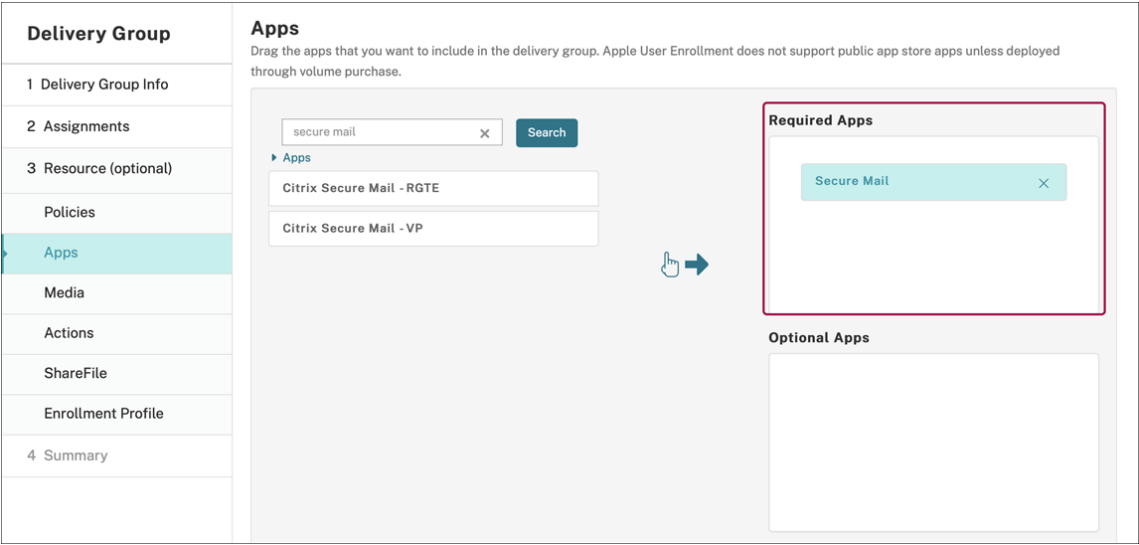
The screenshot displays the configuration interface for Citrix Endpoint Management, organized into three main sections: Miscellaneous Access, Encryption, and App Interaction. Each section contains several settings with corresponding input fields or toggle switches, and each setting has a green help icon (a question mark inside a circle) to its right.

- Miscellaneous Access**
 - Disable required upgrade**: A toggle switch set to **ON**.
 - App update grace period (hours)**: A text input field containing the value **168**.
 - Erase app data on lock**: A toggle switch set to **OFF**.
 - Active poll period (minutes)**: A text input field containing the value **60**.
- Encryption**
 - Enable encryption**: A dropdown menu currently showing **On**.
 - Database encryption exclusions**: An empty text input field.
 - File encryption exclusions**: An empty text input field.
- App Interaction**
 - Cut and copy**: A dropdown menu currently showing **Restricted**.
 - Paste**: A dropdown menu currently showing **Unrestricted**.

7. 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 > Grupos de entrega** y haga clic en **Agregar**.
2. En la sección **Aplicaciones**, 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 la aplicación se instala en segundo plano después de que los usuarios la hayan aceptado.



Aplicaciones MDX distribuidas mediante compras por volumen de Apple

Para usar las directivas MDX y las funciones de seguridad, agregue aplicaciones que estén habilitadas para el SDK de MAM o empaquetadas con MDX. Para implementar aplicaciones mediante las compras por volumen, las aplicaciones deben existir en la tienda de aplicaciones.

Disponibilidad de funciones

Se necesita la supervisión del dispositivo	No
Disponible para el modo de inscripción de usuarios	Sí
Disponible en	iOS/iPadOS

Paso 1: Vincular cuentas

1. Configure e inscríbase en Apple Business Manager (ABM) o en 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 compras por volumen, consulte [Compras por volumen de Apple](#).
3. Al agregar su cuenta de compras por volumen, habilite **Actualización automática de aplicaciones**. Este parámetro garantiza que las aplicaciones de los dispositivos de usuario se actualicen automáticamente cuando aparece una actualización en el Apple Store. Si una aplicación tiene habilitado el parámetro **Forzar administración de la aplicación**, esta se actualiza sin avisar al usuario. La actualización se produce independientemente de si la aplicación es obligatoria u opcional.

Para usar los parámetros **Forzar administración de la aplicación** y **Actualización automática de aplicaciones**, habilite la propiedad `apple.app.force.managed` del servidor. Consulte [Propiedades de servidor](#).

Paso 2: Obtener aplicaciones y licencias de Apple

Compre 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 las que son gratuitas. Una vez que adquiere licencias en ABM/ASM, Citrix Endpoint Management muestra la aplicación automáticamente.

Para obtener información sobre cómo poner 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**.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the [MDX Service](#) to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: Secure Mail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Seleccione **iPhone** o **iPad** como plataformas.
4. Cargue el archivo MDX.
5. Configure los detalles de la aplicación. **Active Aplicación implementada mediante las compras por volumen**. Citrix también recomienda habilitar la función **Forzar administración de la aplicación**.

File name *

Secure Mail

App Description *

Managed Enterprise Application

App version

19.3.5

Package ID

XGFKY3NSP.com.citrix.mail.ios

Minimum OS version

10.0

Maximum OS version

Excluded devices

example: manufacturer or model, ...

Remove app if MDM profile is removed

ON

Prevent app data backup

ON

Force app to be managed

ON

App deployed via Volume purchase

ON

▼ MAM SDK Policies

Authentication

Device passcode

OFF

6. Configure las directivas MDX. **Active** la opción **Inhabilitar actualización obligatoria**.

Miscellaneous Access

Disable required upgrade

ON

?

App update grace period (hours)

168

?

Erase app data on lock

OFF

?

Active poll period (minutes)

60

?

Encryption

Enable encryption

On

?

Database encryption exclusions

?

File encryption exclusions

?

App Interaction

Cut and copy

Restricted

?

Paste

Unrestricted

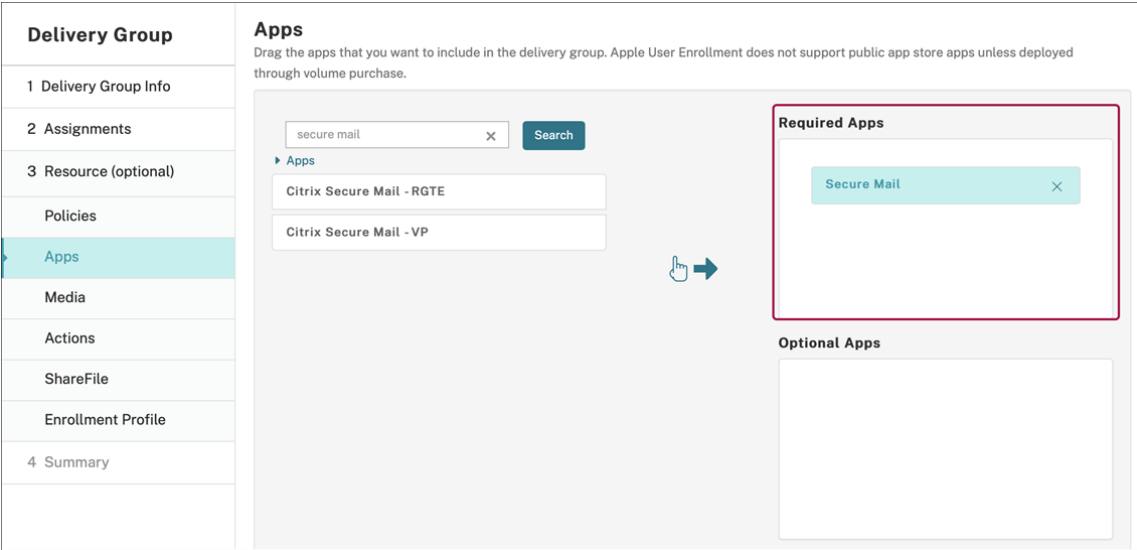
?

7. Asigne un grupo de entrega a la aplicación para cada plataforma y haga clic en **Guardar**.

Esta configuración genera dos entradas para esta aplicación en la lista de aplicaciones. Al seleccionar una aplicación que quiera configurar, seleccione la aplicación con **Tipo MDX**.

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 MDX 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 la aplicación se instala en segundo plano después de que los usuarios la hayan aceptado.



Aplicaciones personalizadas

Las aplicaciones personalizadas son aplicaciones propietarias B2B. Puede utilizar Citrix Endpoint Management y las compras por volumen de Apple para distribuir aplicaciones propietarias de forma privada y segura. Puede distribuir las aplicaciones a socios, clientes, franquiciados y empleados internos específicos.

Disponibilidad de funciones

Se necesita la 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 compras por volumen de Apple (requiere dispositivos con iOS 7 o una versión posterior)
- Inscriba dispositivos en Citrix Endpoint Management mediante 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 las compras por volumen, vincule su cuenta de compras por volumen con Citrix Endpoint Management.

1. Configure e insíbase 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 compras por volumen, consulte [Compras por volumen de Apple](#).
3. Al agregar su cuenta de compras por volumen, habilite **Actualización automática de aplicaciones**. Este parámetro garantiza que las aplicaciones de los dispositivos de usuario se actualicen automáticamente cuando aparece una actualización en el Apple Store. Si una aplicación tiene habilitado el parámetro **Forzar administración de la aplicación**, esta se actualiza sin

avisar al usuario. La actualización se produce independientemente de si la aplicación es obligatoria u opcional.

Para usar los parámetros **Forzar administración de la aplicación** y **Actualización automática de aplicaciones**, habilite la propiedad `apple.app.force.managed` del servidor. Consulte [Propiedades de servidor](#).

Paso 2: Configurar aplicaciones en ABM

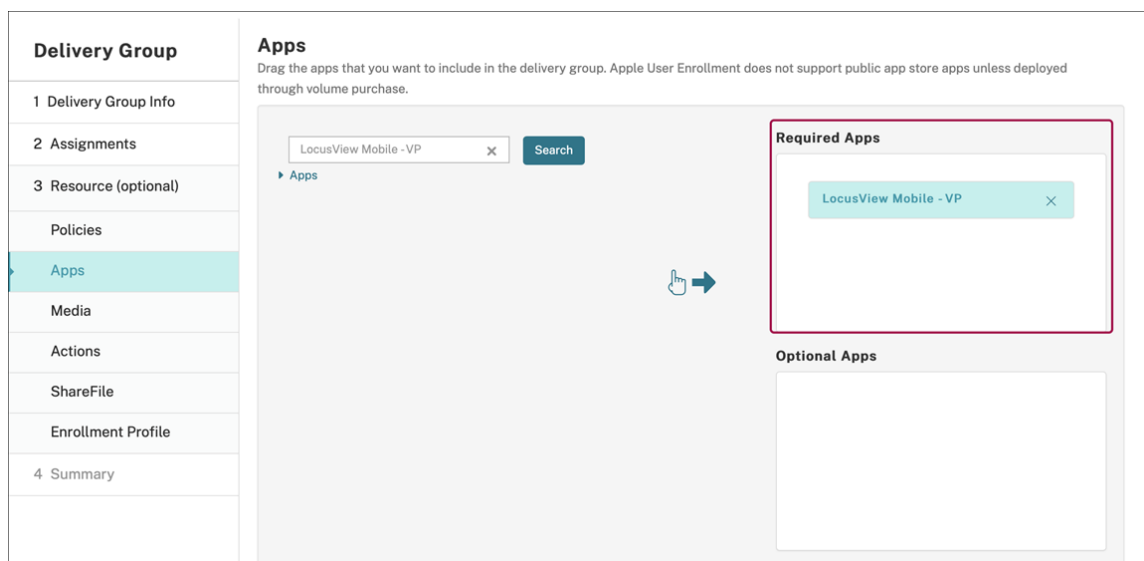
Agregue aplicaciones a su cuenta de ABM. Puede cargar y distribuir sus propias aplicaciones personalizadas o comprar licencias para aplicaciones personalizadas de otras organizaciones. Para obtener más información sobre cómo agregar y habilitar aplicaciones personalizadas en ABM, consulte la [documentación 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 compras por volumen aparecen en la lista de aplicaciones.
2. Seleccione la aplicación que quiere configurar. Haga clic en **Edit**.
3. Seleccione las plataformas: **iPhone**, **iPad** o **macOS**.
4. Elija los grupos de entrega a los que quiere 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 obligatorias**.



3. Vuelva a **Configurar > Grupos de entrega**.
4. Seleccione el grupo de entrega que quiere implementar y haga clic en **Implementar**.
5. Los usuarios recibirán una solicitud para implementar aplicaciones. Las aplicaciones se instalan en segundo plano una vez que los usuarios las hayan aceptado.



Aplicaciones personalizadas que se han habilitado para MDX

Para usar las directivas MDX y las funciones de seguridad, agregue aplicaciones personalizadas que estén habilitadas para el SDK de MAM o empaquetadas con MDX.

Disponibilidad de funciones

Se necesita la 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 las compras por volumen, vincule su cuenta de compras por volumen con 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 compras por volumen, consulte [Compras por volumen de Apple](#).
3. Al agregar su cuenta de compras por volumen, habilite **Actualización automática de aplicaciones**. Este parámetro garantiza que las aplicaciones de los dispositivos de usuario se actualicen automáticamente cuando aparece una actualización en el Apple Store. Si una aplicación tiene habilitado el parámetro **Forzar administración de la aplicación**, esta se actualiza sin avisar al usuario. La actualización se produce independientemente de si la aplicación es obligatoria u opcional.

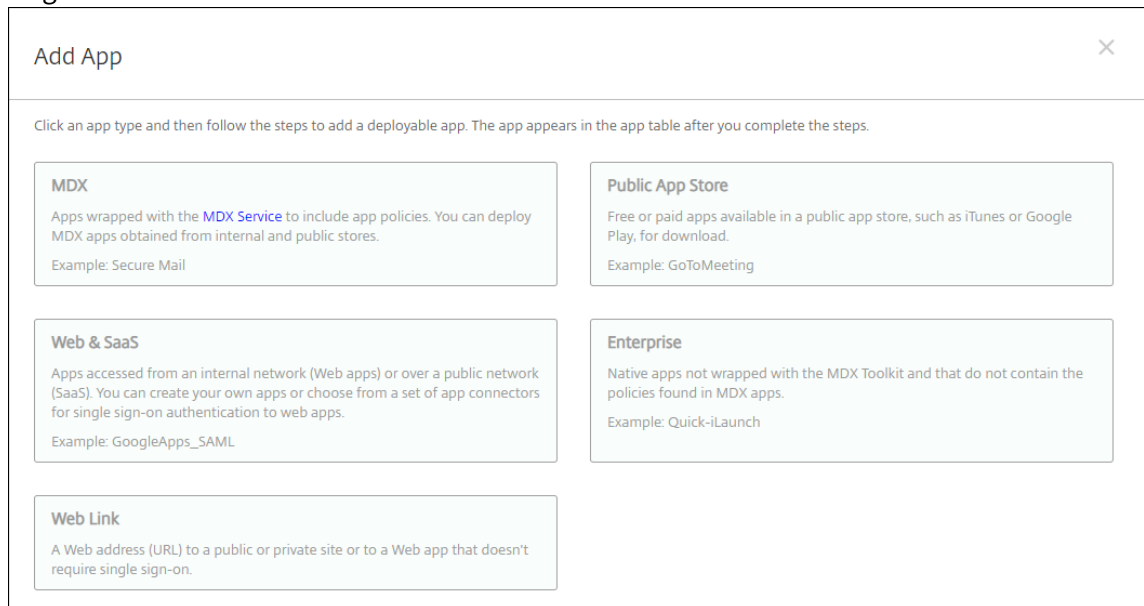
Para usar los parámetros **Forzar administración de la aplicación** y **Actualización automática de aplicaciones**, habilite la propiedad `apple.app.force.managed` del servidor. Consulte [Propiedades de servidor](#).

Paso 2: Configurar aplicaciones en ABM

Agregue aplicaciones a 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**.



Add App ×

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX Apps wrapped with the MDX Service to include app policies. You can deploy MDX apps obtained from internal and public stores. Example: Secure Mail	Public App Store Free or paid apps available in a public app store, such as iTunes or Google Play, for download. Example: GoToMeeting
Web & SaaS Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps. Example: GoogleApps_SAML	Enterprise Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps. Example: Quick-iLaunch
Web Link A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.	

3. Seleccione las plataformas **iPhone o iPad**.
4. Cargue el archivo MDX para la aplicación que quiera agregar.
5. Configure los detalles de la aplicación. **Active Aplicación implementada mediante las compras por volumen**. Citrix también recomienda habilitar la función **Forzar administración de la aplicación**.

File name *

Secure Mail

App Description *

Managed Enterprise Application

App version

19.3.5

Package ID

XGFKY3NSP.com.citrix.mail.ios

Minimum OS version

10.0

Maximum OS version

Excluded devices

example: manufacturer or model, ...

Remove app if MDM profile is removed

ON

Prevent app data backup

ON

Force app to be managed

ON

App deployed via Volume purchase

ON

▼ MAM SDK Policies

Authentication

Device passcode

OFF

6. Configure las directivas MDX. **Active** la opción **Inhabilitar actualización obligatoria**.

Miscellaneous Access

Disable required upgrade ☒ ON ?

App update grace period (hours) ?

Erase app data on lock ☐ OFF ?

Active poll period (minutes) ?

Encryption

Enable encryption ?

Database encryption exclusions ?

File encryption exclusions ?

App Interaction

Cut and copy ?

Paste ?

7. Asigne un grupo de entrega a la aplicación y haga clic en **Guardar**.

Esta configuración genera dos entradas para esta aplicación en la lista de aplicaciones. Al seleccionar una aplicación que quiera configurar, seleccione la aplicación con **Tipo MDX**.

Paso 4: Configurar la implementación de aplicaciones

1. En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones**. Las aplicaciones de compras por volumen aparecen en la lista de aplicaciones.
2. Seleccione la aplicación que quiere configurar. Haga clic en **Edit**.
3. Elija los grupos de entrega a los que quiere distribuir 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.

Delivery Group

1 Delivery Group Info

2 Assignments

3 Resource (optional)

Policies

Apps

Media

Actions

ShareFile

Enrollment Profile

4 Summary

Apps

Drag the apps that you want to include in the delivery group. Apple User Enrollment does not support public app store apps unless deployed through volume purchase.

LocusView Mobile - VP

Search

Apps

Required Apps

LocusView Mobile

Optional Apps

- 6. Vuelva a **Configurar > Grupos de entrega**.
- 7. Seleccione el grupo de entrega que quiere implementar y haga clic en **Implementar**.
- 8. Los usuarios recibirán una solicitud para implementar aplicaciones. Las aplicaciones se instalan en segundo plano una vez aceptadas.

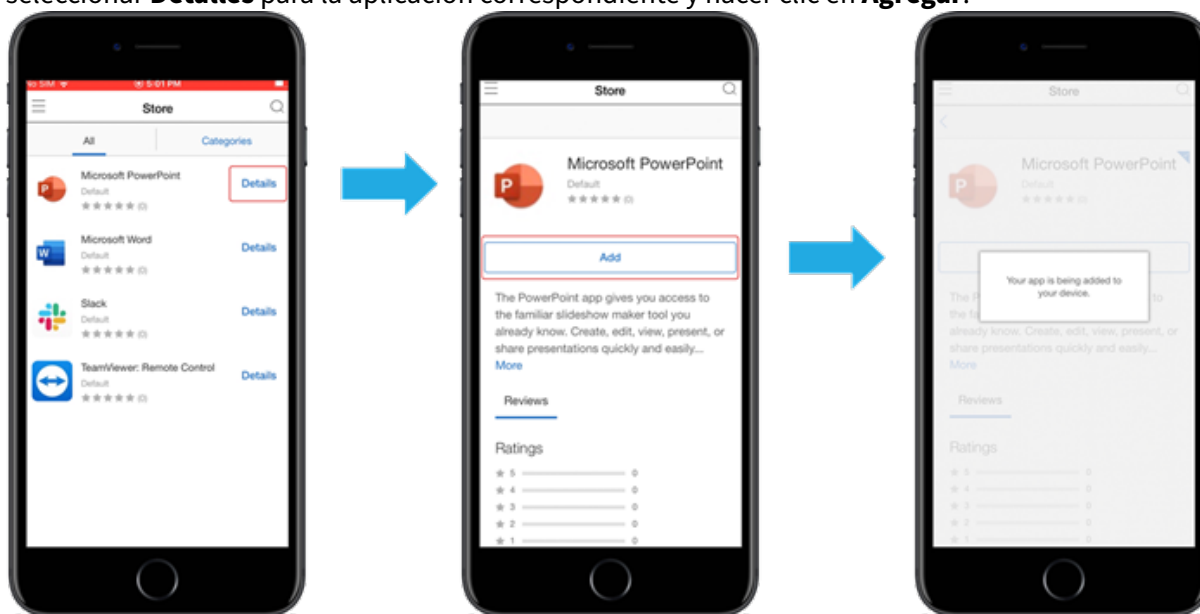


Aplicaciones opcionales (solo iOS/iPadOS)

Citrix recomienda implementar aplicaciones con la opción **Requerido**. Las aplicaciones necesarias se instalan silenciosamente en los dispositivos del usuario, lo que minimiza la interacción con ellas. 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 correspondiente y hacer clic en **Agregar**.



Control de acceso de red

March 1, 2024

Puede utilizar la solución de control de acceso de red (NAC) para ampliar la evaluación de seguridad que ofrece Citrix Endpoint Management para dispositivos Android y Apple. La solución NAC usa la evaluación de seguridad de Citrix Endpoint Management para facilitar y gestionar las decisiones de autenticación. Después de configurar el dispositivo NAC, se aplican las directivas de dispositivo y los filtros NAC que configure en Citrix Endpoint Management.

El uso de Citrix Endpoint Management con una solución NAC agrega QoS y un control más detallado sobre los dispositivos internos de la red. Para obtener un resumen de las ventajas de integrar NAC en Citrix Endpoint Management, consulte [Control de acceso](#).

Citrix admite estas soluciones para la integración en Citrix Endpoint Management:

- NetScaler Gateway
- ForeScout

Citrix no garantiza la integración de otras soluciones NAC.

Con un dispositivo NAC en la red:

- Citrix Endpoint Management admite NAC como una función de seguridad para dispositivos de punto final que sean iOS, Android Enterprise y Android.
- Puede habilitar filtros en Citrix Endpoint Management para establecer dispositivos como conformes o no conformes con NAC, en función de una serie de reglas o propiedades. Por ejemplo:
 - Si un dispositivo administrado en Citrix Endpoint Management no cumple los criterios especificados, Citrix Endpoint Management lo marca como no conforme. Un dispositivo NAC bloquea dispositivos no conformes que haya presentes en su red.
 - Si un dispositivo administrado en Citrix Endpoint Management tiene instaladas aplicaciones no conformes, un filtro NAC puede bloquear la conexión VPN. Como resultado, un dispositivo de usuario no conforme no puede acceder a aplicaciones ni sitios web a través de la VPN.
 - Si utiliza NetScaler Gateway para NAC, puede habilitar el túnel dividido para evitar que el plug-in de NetScaler Gateway envíe tráfico de red innecesario a NetScaler Gateway. Para obtener más información sobre los túneles divididos, consulte [Configurar el túnel dividido](#).

Filtros de conformidad con NAC admitidos

Citrix Endpoint Management admite los siguientes filtros de conformidad para 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 reconectar.

Aplicaciones prohibidas: Comprueba si un dispositivo tiene aplicaciones prohibidas, según se definen en la directiva Acceso a aplicaciones. Para obtener más información acerca de esa directiva, consulte [Directivas de acceso a aplicaciones](#).

Dispositivos inactivos: Comprueba si un dispositivo está inactivo según se define en el parámetro **Umbral de días de inactividad** en **Propiedades de servidor**. Para obtener más información, consulte [Propiedades del servidor](#).

Aplicaciones obligatorias que faltan: Comprueba si en un dispositivo falta alguna aplicación obligatoria, según se definen en la directiva Acceso a aplicaciones.

Aplicaciones no sugeridas: Comprueba si un dispositivo tiene aplicaciones no sugeridas, según se definen en la directiva Acceso a aplicaciones.

Contraseña no conforme: Comprueba si la contraseña del usuario cumple los requisitos de conformidad. En dispositivos iOS y Android, Citrix Endpoint Management puede determinar si la contraseña actual del dispositivo cumple los requisitos de conformidad con la directiva Código de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para definir una contraseña si Citrix Endpoint Management envía una directiva Código de acceso al dispositivo. Antes de que el usuario defina la contraseña, el código de acceso podría no cumplir los requisitos de conformidad.

Dispositivos no conformes: Comprueba si un dispositivo ya no es conforme, según lo definido en la propiedad de dispositivo No conforme. Por regla general, las acciones automatizadas o el uso que terceros hacen de las API de Citrix Endpoint Management modifican esa propiedad.

Estado revocado: Comprueba si el certificado del dispositivo se ha revocado. Un dispositivo revocado no se puede volver a inscribir hasta que se autorice de nuevo.

Dispositivos Android o iOS liberados por root/jailbreak: Comprueba si un dispositivo iOS está liberado por jailbreak o un dispositivo Android está liberado por rooting.

Dispositivos no administrados: Comprueba si Citrix Endpoint Management administra un dispositivo. Por ejemplo, un dispositivo inscrito en MAM o que se haya desinscrito no es un dispositivo administrado.

Nota:

El filtro “Conformidad/No conformidad implícita” establece el valor predeterminado solo en los dispositivos que administra Citrix Endpoint Management. Por ejemplo, los dispositivos que tengan instalada una aplicación bloqueada o que no estén inscritos se marcan como no conformes. El dispositivo NAC bloquea dichos dispositivos en la red.

Introducción a la configuración

Se recomienda configurar los componentes de NAC en el orden indicado.

1. Configure directivas de dispositivo para admitir NAC:

Para dispositivos iOS: Consulte [Configurar la directiva de VPN para admitir NAC](#).

Para dispositivos Android Enterprise: Consulte [Crear una configuración administrada por Android Enterprise para Citrix SSO](#).

Para dispositivos Android: Consulte [Configurar el protocolo Citrix SSO para Android](#).

2. Habilite filtros NAC en Citrix Endpoint Management.
3. Configure una solución NAC:

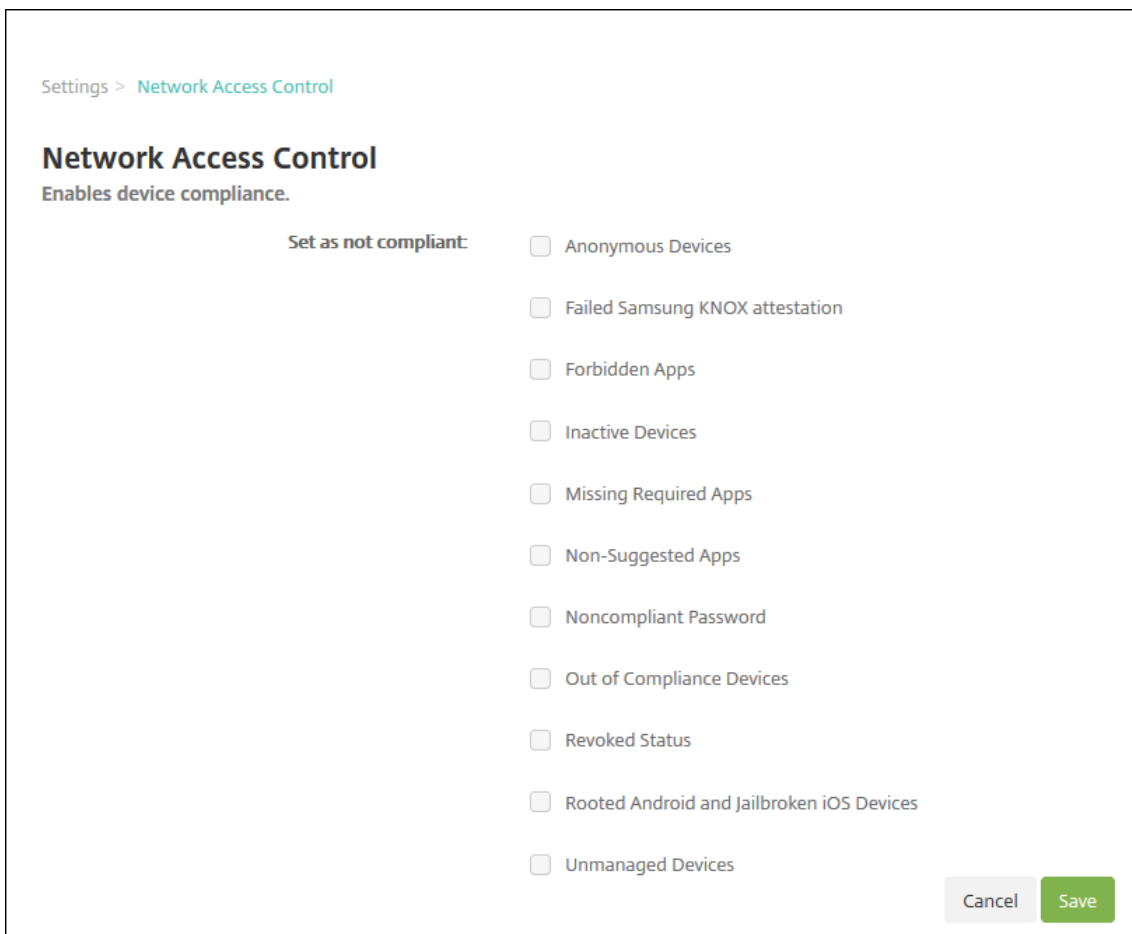
- NetScaler Gateway, detallado en [Actualizar las directivas de NetScaler Gateway para admitir NAC](#)

Requiere instalar 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 de red**.



Settings > Network Access Control

Network Access Control

Enables device compliance.

Set as not compliant:

- ☐ Anonymous Devices
- ☐ Failed Samsung KNOX attestation
- ☐ Forbidden Apps
- ☐ Inactive Devices
- ☐ Missing Required Apps
- ☐ Non-Suggested Apps
- ☐ Noncompliant Password
- ☐ Out of Compliance Devices
- ☐ Revoked Status
- ☐ Rooted Android and Jailbroken iOS Devices
- ☐ Unmanaged Devices

Cancel Save

2. Marque las casillas de los filtros **Establecer como no conforme** 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 de sesiones VPN en el servidor virtual de su VPN.

Estos pasos actualizan un dispositivo NetScaler Gateway con cualquiera de estas características:

- Está integrado en Citrix Endpoint Management.
- O bien, está configurado para VPN, no forma parte del entorno de Citrix Endpoint Management, y puede establecer contacto con Citrix Endpoint Management.

En su servidor de VPN virtual desde una ventana de consola, haga lo siguiente. Las direcciones IP y los FQDN de los comandos y los ejemplos son ficticios.

1. Elimine y desenlace todas las directivas clásicas si las utiliza en su servidor de VPN virtual. Para verificar, escriba:

```
show vpn vserver <VPN_VServer>
```

Elimine todos los resultados que contengan 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. Para ello, escriba 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. Enlace la directiva a su servidor de VPN virtual. Para ello, escriba lo siguiente.

```
bind vpn vserver _XM_EndpointManagement -policy vpn_nac -priority 100
```

4. Cree un servidor virtual de autenticación. Para ello, escriba 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 es público.

5. Enlace un certificado SSL con el servidor virtual. Para ello, escriba 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 de VPN virtual. Primero, cree el perfil de autenticación. Para ello, escriba 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 al servidor de VPN virtual. Para ello, escriba 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 desde NetScaler Gateway a un dispositivo. Para ello, escriba 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.

```
1 HTTP/1.1 200 OK
2 < Server: Apache-Coyote/1.1
3 < X-Citrix-Device-State: Non Compliant
4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
5 <!--NeedCopy-->
```

9. Si el paso anterior da el resultado correcto, cree la acción de autenticación web en Citrix Endpoint Management. Primero, cree una expresión de directiva para extraer el ID del dispositivo desde el 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. Para ello, escriba 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\")"
```

El resultado correcto para NAC de Citrix Endpoint Management es `HTTP status 200 OK`. El encabezado `X-Citrix-Device-State` debe tener el valor `Compliant`.

11. Cree una directiva Autenticación con la que asociar la acción. Para ello, escriba 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 de LDAP existente en una directiva avanzada. Para ello, escriba 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 de LDAP. Para ello, escriba lo siguiente.

```
add authentication policylabel <policy_label_name>
```

Por ejemplo: `add authentication policylabel ldap_pol_label`

14. Asocie la directiva de LDAP a la etiqueta de directiva. Para ello, escriba lo siguiente.

```
bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT
```

15. Conecte un dispositivo conforme para hacer 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 a asociar con el servidor virtual de autenticación. Escriba el siguiente comando para recuperar la identificación del dispositivo.

```
add authentication loginSchemaPolicy <schema policy> -rule <rule> -action lschema_single_factor_deviceid
```

17. Enlace el servidor virtual de autenticación. Para ello, escriba lo siguiente.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority 100 -gotoPriorityExpression END
```

18. Cree una directiva de LDAP avanzada de autenticación para permitir la conexión 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
```

Tableta y escritorio Windows

December 13, 2023

Citrix Endpoint Management inscribe los dispositivos con Windows 10 o Windows 11 en MDM. Citrix Endpoint Management admite los siguientes tipos de autenticación para dispositivos con Windows 10 o Windows 11 inscritos en MDM.

- Autenticación basada en dominios
 - Active Directory
 - Azure Active Directory
- Proveedores de identidades:
 - Azure Active Directory
 - Proveedor de identidades Citrix

Para obtener más información acerca de los tipos de autenticación admitidos, consulte [Certificados y autenticación](#).

Un flujo de trabajo general para iniciar la administración de dispositivos con Windows 10 o Windows 11 es el siguiente:

1. Complete el proceso de incorporación. Consulte [Incorporarse como usuario y configurar recursos](#) y [Preparar la inscripción de dispositivos y la entrega de recursos](#).

Si tiene pensado inscribir dispositivos Windows con el servicio de detección automática, primero debe configurar el servicio de detección automática de Citrix. Póngase en contacto con la asistencia técnica de Citrix para obtener ayuda. Para obtener más información, consulte [Solicitar detección automática para dispositivos Windows](#).
2. Elija y configure un método de inscripción. Consulte Métodos de inscripción admitidos.
3. Configure directivas de dispositivo para escritorios y tabletas Windows.
4. Los usuarios inscriben dispositivos con Windows 10 o Windows 11.

5. Configure las acciones de seguridad para los dispositivos y las aplicaciones. Consulte Acciones de seguridad.

Para conocer los sistemas operativos admitidos, consulte [Sistemas operativos admitidos](#).

Métodos de inscripción admitidos

La manera de administrar los dispositivos con Windows 10 o Windows 11 se especifica en los perfiles de inscripción. Hay dos opciones disponibles:

- Totalmente administrado (inscripción en MDM)
- No administrar dispositivos (sin inscripción en MDM)

Para configurar los parámetros de inscripción de dispositivos con Windows 10 o Windows 11, vaya a **Configurar > Perfiles de inscripción > Windows**. Para obtener más información sobre los perfiles de inscripción, consulte [Perfiles de inscripción](#).

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	
Android	
iOS	
Windows	<div>Device management ⓘ Management <input checked="" type="radio"/> Fully managed ⓘ <input type="radio"/> Do not manage devices ⓘ</div> <div>User consent Allow users to decline device management <input checked="" type="checkbox"/> On ⓘ</div> <div>Workspace integration ⓘ Enrollment through Workspace app <input type="checkbox"/> Off ⓘ</div>
3 Assignment (optional)	

En la siguiente tabla se indican los métodos de inscripción que Citrix Endpoint Management admite para dispositivos con Windows 10 o Windows 11:

Método	Compatible
Inscripción a través de Azure Active Directory	Sí
Inscripción en el servicio de detección automática	Sí
Inscripción en bloque de Windows	Sí
Inscripción manual	Sí

Método	Compatible
Invitaciones de inscripción	No

Nota:

- En la inscripción manual, los usuarios deben introducir el nombre de dominio completo (FQDN) del servidor de Citrix Endpoint Management. No se recomienda el uso de la inscripción manual. En su lugar, utilice otros métodos a fin de simplificar el proceso de inscripción para los usuarios.
- No puede enviar invitaciones de inscripción a los dispositivos Windows. Los usuarios de Windows se inscriben directamente a través de sus dispositivos.

Configurar directivas de dispositivo para escritorios y tabletas Windows

Use estas directivas para configurar cómo interactúa Citrix Endpoint Management con escritorios y tabletas con Windows 10 o Windows 11. En esta tabla se indican todas las directivas de dispositivo disponibles para escritorios y tabletas Windows.

— — —	
[[Configuración de aplicaciones]](/es-es/citrix-endpoint-management/policies/app-configuration-policy.html#windows-desktoptablet-settings) [[Inventario de aplicaciones]](/es-es/citrix-endpoint-management/policies/app-inventory-policy.html) [[Bloqueo de aplicaciones]](/es-es/citrix-endpoint-management/policies/app-lock-policy.html#windows-desktop-and-tablet-settings)	
[[Desinstalación de aplicaciones]](/es-es/citrix-endpoint-management/policies/app-uninstall-policy.html) [[Protección de aplicaciones]](/es-es/citrix-endpoint-management/policies/application-guard-policy.html) [[BitLocker]](/es-es/citrix-endpoint-management/policies/bitlocker-policy.html#windows-desktop-and-tablet-settings)	
[[Credenciales]](/es-es/citrix-endpoint-management/policies/credentials-policy.html#windows-desktoptablet-settings) [[XML personalizado]](/es-es/citrix-endpoint-management/policies/custom-xml-policy.html) [[Defender]](/es-es/citrix-endpoint-management/policies/defender-policy.html)	
[[Device Guard]](/es-es/citrix-endpoint-management/policies/device-guard-policy.html) [[Atestación de mantenimiento de dispositivos]](/es-es/citrix-endpoint-management/policies/device-health-attestation-policy.html) [[Exchange]](/es-es/citrix-endpoint-management/policies/exchange-policy.html#windows-desktoptablet-settings)	
[[Firewall]](/es-es/citrix-endpoint-management/policies/firewall-device-policy.html#windows-desktop-and-tablet-settings) [[Quiosco]](/es-es/citrix-endpoint-management/policies/kiosk-policy.html#windows-desktop-and-tablet-settings)[[Red]](/es-es/citrix-endpoint-management/policies/network-policy.html#windows-desktoptablet-settings)	

[[Office]](/es-es/citrix-endpoint-management/policies/office-policy.html) | [[Actualización de SO]](/es-es/citrix-endpoint-management/policies/control-os-updates.html#windows-desktop-and-tablet-settings) | [[Código de acceso]](/es-es/citrix-endpoint-management/policies/passcode-policy.html#windows-desktop-tablet-settings) |

[[Restricciones]](/es-es/citrix-endpoint-management/policies/restrictions-policy.html#windows-desktop-tablet-settings) | [[Store]](/es-es/citrix-endpoint-management/policies/store-policy.html) |

[[Términos y condiciones]](/es-es/citrix-endpoint-management/policies/terms-and-conditions-policy.html#windows-tablet-settings) |

[[VPN]](/es-es/citrix-endpoint-management/policies/vpn-policy.html#windows-desktop-tablet-settings) | [[Clip web]](/es-es/citrix-endpoint-management/policies/webclip-policy.html#windows-desktop-tablet-settings) | [[Agente Windows]](/es-es/citrix-endpoint-management/policies/windows-agent-policy.html)|

| [Configuración de GPO de Windows](#)|[Windows Hello para empresas](#) |

Inscribir dispositivos con Windows 10 o Windows 11 a través de Azure Active Directory

Importante:

Antes de que los usuarios puedan inscribirse, debe configurar los parámetros de Azure Active Directory (AD) en Azure y, a continuación, configurar Citrix Endpoint Management. Para obtener información detallada, consulte [Conectar Citrix Endpoint Management a Azure AD](#).

Los dispositivos con Windows 10 o Windows 11 pueden inscribirse con Azure como método federado de autenticación de AD. Este método de inscripción requiere una suscripción a Azure AD Premium.

Puede unir dispositivos con Windows 10 o Windows 11 a Microsoft Azure AD con cualquiera de los métodos siguientes:

- Para dispositivos propiedad de la empresa:
 - Inscribirse en MDM al unir los dispositivos a Azure AD la primera vez que los encienda. En este caso, los usuarios completan la inscripción como se describe en el siguiente artículo: <https://docs.microsoft.com/en-us/azure/active-directory/devices/azuread-joined-devices-frx>.

Para los dispositivos Windows que inscriba con este método, puede usar Windows AutoPilot para instalar y preconfigurar los dispositivos. Para obtener más información, consulte [Usar Windows AutoPilot para instalar y configurar dispositivos](#).
 - Inscribirse en MDM al unir el dispositivo a Azure AD desde la página **Configuración** de Windows una vez que el dispositivo se haya configurado. En este caso, los usuarios completan la inscripción como se describe en [Inscribirse en MDM al unirse a Azure AD después de configurar dispositivos](#).

- Para dispositivos personales (BYOD o dispositivos móviles):
 - Inscribirse en MDM al registrarse en Azure AD mientras se agrega la cuenta de trabajo de Microsoft a Windows. En este caso, los usuarios completan la inscripción como se describe en Inscribirse en MDM al registrarse en Azure AD.

Inscribirse en MDM al unirse a Azure AD después de configurar dispositivos

1. En el menú Inicio de un dispositivo, vaya a **Configuración > Cuentas > Obtener acceso 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 **Hecho** para completar el proceso de inscripción.

Inscribirse en MDM al registrarse en Azure AD

1. En el menú Inicio de un dispositivo, vaya a **Configuración > Cuentas > Obtener acceso 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 **Información** en la cuenta.
4. Haga clic en **Unirse** para continuar con el proceso de inscripción.
5. Haga clic en **Hecho** para completar el proceso de inscripción.

Inscribir dispositivos Windows mediante el servicio de detección automática

Para configurar el servicio de detección automática para dispositivos Windows, solicite ayuda a la asistencia técnica de Citrix. Para obtener más información, consulte [Solicitar detección automática para dispositivos Windows](#).

Nota:

Para que los dispositivos Windows se puedan inscribir, el certificado SSL de escucha debe ser un certificado público. La inscripción falla si se cargan certificados SSL autofirmados.

Los usuarios siguen estos pasos para completar la inscripción:

1. En el menú Inicio de un dispositivo, vaya a **Configuración > Cuentas > Obtener acceso a trabajo o escuela** y haga clic en **Inscribirse 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 un usuario local, introduzca una dirección de correo electrónico que no exista y un nombre de dominio correcto (por ejemplo, `foo\@mydomain.com`). Ese paso permite a un usuario omitir una limitación conocida de Microsoft donde la administración de dispositivos integrada de Windows realiza la inscripción. En el cuadro de diálogo **Conectando con un servicio**, escriba el nombre de usuario y la contraseña asociados al usuario local. A continuación, el dispositivo detecta el servidor de Citrix Endpoint Management y se inicia el proceso de inscripción.

3. Introduzca las credenciales y haga clic en **Continuar**.
4. En el cuadro de diálogo **Condiciones de uso**, acepte que el dispositivo sea administrado y, a continuación, haga clic en **Aceptar**.

El proceso de inscribir dispositivos Windows unidos a un dominio a través del servicio de detección automática falla si la directiva de dominio inhabilita la inscripción MDM. Los usuarios pueden utilizar, en su lugar, cualquiera de los métodos siguientes:

- Quitar los dispositivos del dominio, inscribir y volverlos a unir.
- Introducir el nombre de dominio completo FQDN del servidor de Citrix Endpoint Management para continuar.

Inscripción en bloque de Windows

Con la inscripción en bloque de Windows, puede configurar varios dispositivos para que un servidor MDM los administre sin necesidad de restablecer la imagen inicial de los dispositivos. Puede usar un paquete de aprovisionamiento para la inscripción en bloque de escritorios y portátiles con Windows 10 o Windows 11. Para obtener información, consulte [Inscribir dispositivos Windows en bloque](#).

Acciones de seguridad

Los dispositivos con Windows 10 o Windows 11 permiten estas acciones de seguridad. Para ver 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 con Windows 10 o Windows 11 pueden inscribirse en Azure. Los usuarios creados en Azure AD pueden acceder a los dispositivos. Citrix Endpoint Management se implementa en Microsoft Azure como 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 AD, vaya a **Azure Active Directory > Movilidad (MDM y MAM) > Agregar aplicación** y haga clic en **Configuración de la aplicación MDM local**.
2. Proporcione un nombre para la aplicación y haga clic en **Agregar**.
3. (Opcional) Azure no permite el uso de dominios no verificados, como cloud.com, para la configuración de IDP. Si el FQDN de inscripción de Citrix Endpoint Management incluye cloud.com, contacte con Citrix Support y envíeles el registro TXT de Azure. Citrix Support verifica el subdominio, lo que le permite continuar con la configuración. Si su FQDN pertenece a su propio dominio, puede verificarlo como siempre en Azure.
4. Seleccione la aplicación que creó, configure lo siguiente y, a continuación, haga clic en **Guardar**.
 - **Ámbito de usuario de MDM**. Seleccione **Todo**.
 - **URL de condiciones de uso MDM**. Introduzca en el formato `https://<Citrix Endpoint Management Enrollment FQDN>:8443/zdm/wpe/tou`.
 - **URL de detección MDM**. Introduzca en 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 puede volver a usar en ninguna otra aplicación.

- En el panel **Permisos necesarios**, 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 su uso posterior. Necesitará la clave en el paso 7.
6. En la consola de Citrix Endpoint Management, vaya a **Parámetros > 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**. Escriba un nombre único para identificar la conexión del proveedor de identidades que va a crear.
 - **Tipo de IDP**. Seleccione **Azure Active Directory**.
 - **ID de arrendatario**. El **ID del directorio** en Azure. Lo verá cuando vaya a **Azure Active Directory > Propiedades** en Azure.
 8. En la página **Información sobre MDM con Windows**, configure lo siguiente y haga clic en **Siguiente**.
 - **URI de ID de la aplicación**. El valor de URI de ID de aplicación que escribió en Azure.
 - **ID de cliente**. El ID de aplicación que aparece 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 IDP**, configure lo siguiente y haga clic en **Siguiente**:
 - **Tipo de identificador del usuario**. Seleccione **userPrincipalName**.
 - **Cadena de identificador del usuario**. Escriba `${ 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 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

No es posible implementar MDM únicamente con Workspace Environment Management (WEM). Si utiliza únicamente Citrix Endpoint Management, se le limita a administrar dispositivos con Windows 10 o Windows 11. Al integrar ambos, WEM puede acceder a funciones de MDM, y usted puede administrar un espectro más amplio de sistemas operativos Windows a través de Citrix Endpoint Management. Esa administración adopta la forma de configurar objetos de directivas de grupo de Windows. Actualmente, los administradores importan un archivo ADMX a Citrix Endpoint Management y lo envían a

escritorios y tabletas con Windows 10 o Windows 11 para configurar aplicaciones específicas. Mediante la directiva de configuración de objetos de directiva de grupo de Windows, puede configurar los objetos de directiva de grupo e insertar cambios en el servicio WEM. A continuación, el agente de WEM aplica los objetos de directiva de grupo (GPO) a los dispositivos y sus aplicaciones.

La administración de MDM no es un requisito para la integración de WEM. Se pueden enviar configuraciones de GPO a cualquier dispositivo compatible con WEM, incluso si Citrix Endpoint Management no admite ese dispositivo de forma nativa.

Para ver una lista de los dispositivos admitidos, consulte [Requisitos del sistema operativo](#).

Los dispositivos que reciben la directiva de configuración de GPO de Windows se ejecutan en un nuevo modo de Citrix Endpoint Management denominado WEM. En la lista **Administrar > Dispositivos** de dispositivos inscritos, la columna **Modo** para dispositivos administrados por WEM muestra **WEM**.

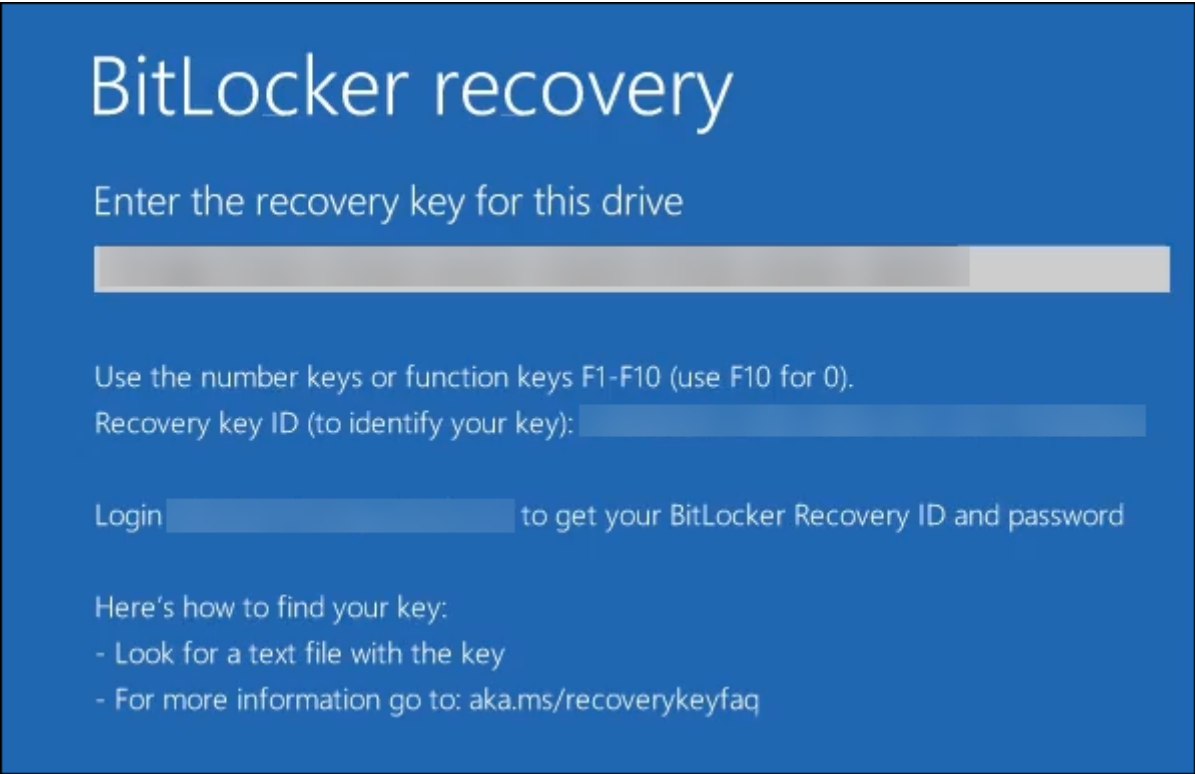
Para obtener más información, consulte [Directiva de configuración de GPO de Windows](#).

Clave de recuperación de BitLocker

El cifrado de discos mediante BitLocker es una útil función de seguridad. Sin embargo, desbloquear dispositivos puede ser complicado si el usuario pierde su clave de recuperación de BitLocker. Ahora, Citrix Endpoint Management puede guardar automáticamente y de forma segura las claves de recuperación de BitLocker de los usuarios. Los usuarios pueden encontrar su clave de recuperación de BitLocker en Self Help Portal. Para habilitar y buscar la clave de recuperación de BitLocker:

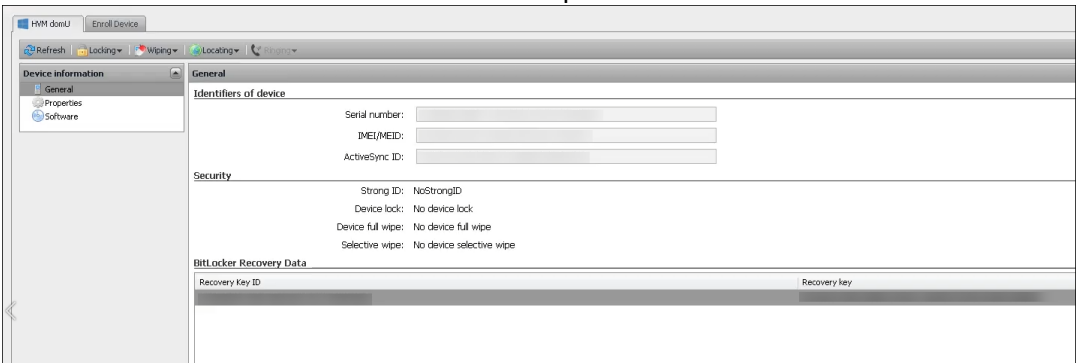
1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Propiedades del servidor**.
2. Busque `shp` y habilite la función `shp.console.enable`. Asegúrese de que `enable.new.shp` permanece inhabilitado. Para obtener más información sobre cómo habilitar Self Help Portal, consulte [Configurar modos de seguridad de inscripción](#).
3. Vaya a **Configurar > Directivas de dispositivo**. Busque la directiva de BitLocker o cree una y habilite **Recuperación de seguridad de BitLocker en Citrix Endpoint Management**.

Al desbloquear su dispositivo, los usuarios finales pueden ver un mensaje en el que se les pide que introduzcan su clave. El mensaje muestra también el ID de clave de recuperación.



Para encontrar su clave de recuperación de BitLocker, los usuarios se dirigen a Self Help Portal.

1. En los detalles de **General**, consulte **Datos de recuperación de BitLocker**.
 - **ID de la 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 indicado en el mensaje anterior.
 - **Clave de recuperación:** La clave que el usuario debe introducir para desbloquear el disco. Introduzca esta tecla en la solicitud de desbloqueo.



Para obtener más información sobre la directiva de dispositivo BitLocker, consulte [Directiva BitLocker](#).

Inscribir dispositivos Windows en bloque

November 29, 2023

Citrix Endpoint Management admite la inscripción en bloque de dispositivos de escritorio y tabletas con Windows 10 o Windows 11. Con la inscripción en bloque, puede configurar múltiples dispositivos para que Citrix Endpoint Management los administre sin restablecer la imagen inicial de los dispositivos. Utilice el paquete de aprovisionamiento para la inscripción en bloque.

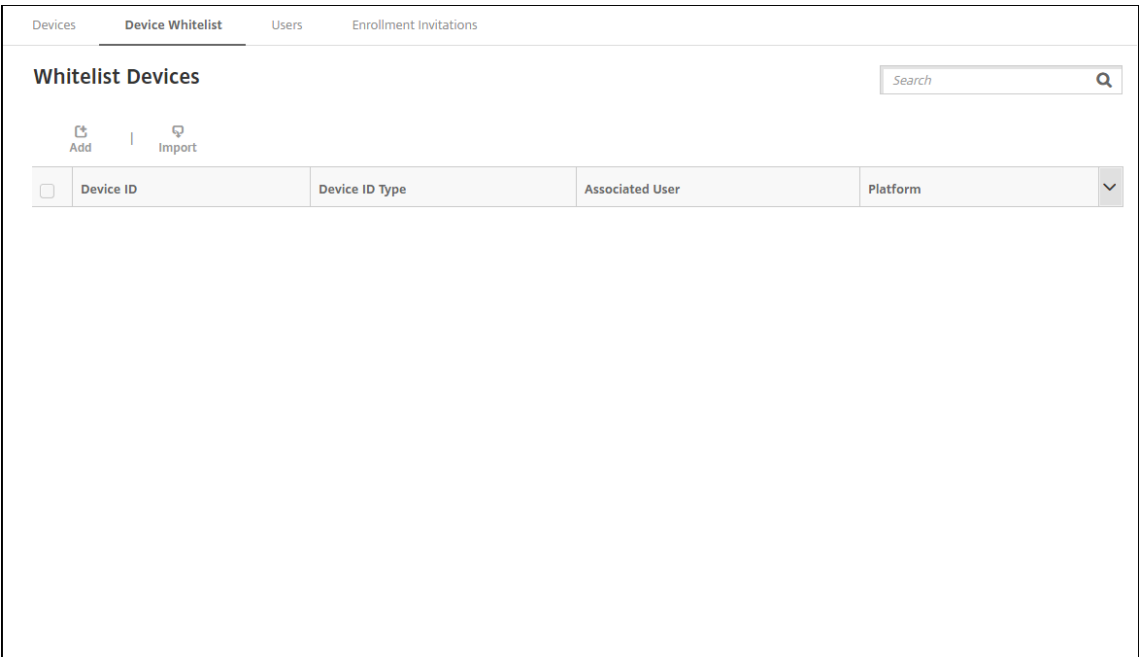
A continuación, se muestra un flujo de trabajo general para inscribir en bloque dispositivos con Windows 10 o Windows 11:

1. Asigne dispositivos. Puede asignar dispositivos uno por uno o en bloque.
2. Configure la inscripción en bloque.
3. Cree un paquete de aprovisionamiento y aplíquelo a cada dispositivo.

Antes de ejecutar la inscripción en bloque, compruebe que todos los dispositivos estén asignados a los usuarios correctos. Para realizar la asignación, agregue los dispositivos uno por uno o en bloque.

Asignar dispositivos uno por uno

1. En la consola de Citrix Endpoint Management, vaya a **Administrar > Dispositivos > Lista de dispositivos permitidos**.



2. Para agregar cada dispositivo, haga clic en **Agregar**.

The screenshot shows the 'Add Whitelist Device' form in the Citrix Endpoint Management console. The form is titled 'Add Whitelist Device' and has three tabs: 'Devices', 'Users', and 'Enrollment Invitations'. The 'Devices' tab is selected. The form contains the following fields:

- Device platform ***: A dropdown menu with '-- Select --'.
- Device ID Type ***: A dropdown menu with '-- Select --' and a green help icon.
- Device ID ***: A text input field with a green help icon.
- Associated User**: A text input field.
- Select domain ***: A dropdown menu.
- Search for user ***: A text input field with a magnifying glass icon and a blue 'Search' button.

At the bottom right of the form, there are two buttons: 'Cancel' and 'Save'.

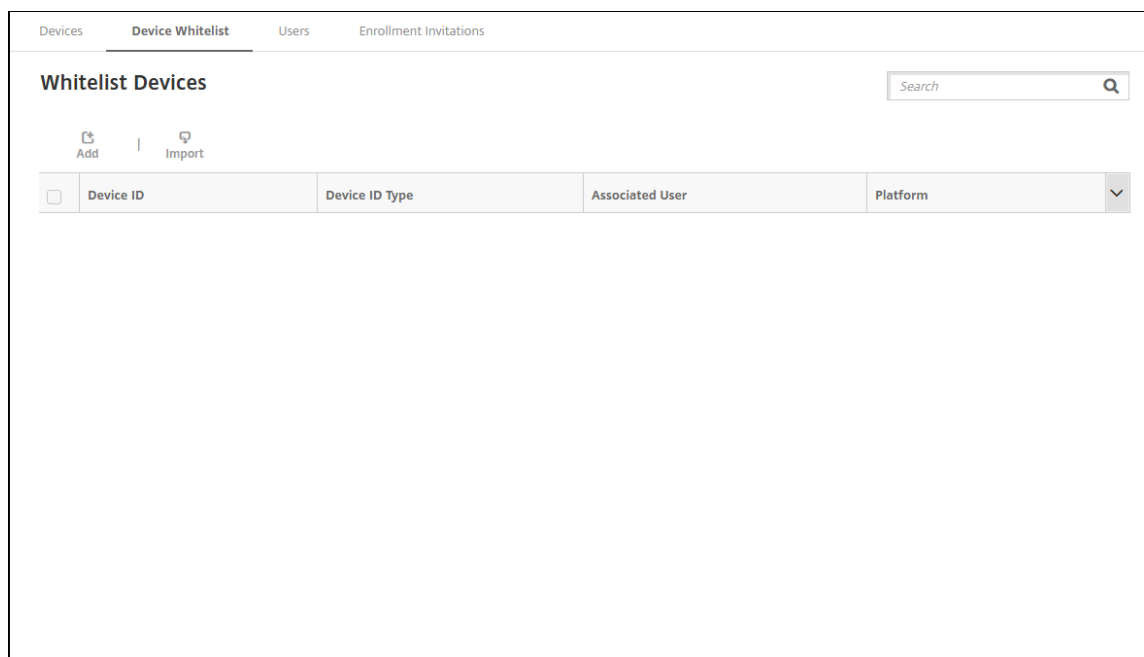
3. Escriba la siguiente información:

- **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 anteriormente para el dispositivo.
- **Usuario asociado:** Muestra al usuario asociado de este dispositivo. Este campo se rellena automáticamente con el usuario seleccionado.
- **Seleccionar dominio:** Seleccione el dominio en el que quiere buscar un usuario asociado.
- **Buscar usuario** Introduzca un nombre de usuario completo o parcial en este campo y haga clic en **Buscar** para encontrar un usuario y asociarlo con este dispositivo.

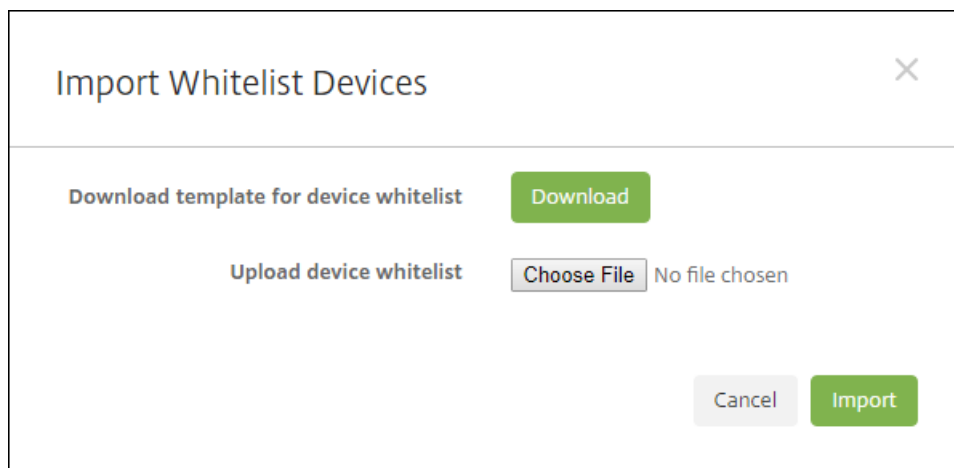
4. Haga clic en **Guardar**.

Agregar dispositivos en bloque

1. En la consola de Citrix Endpoint Management, vaya a **Administrar > Dispositivos > Lista de dispositivos permitidos**.



2. Haga clic en **Importar**.

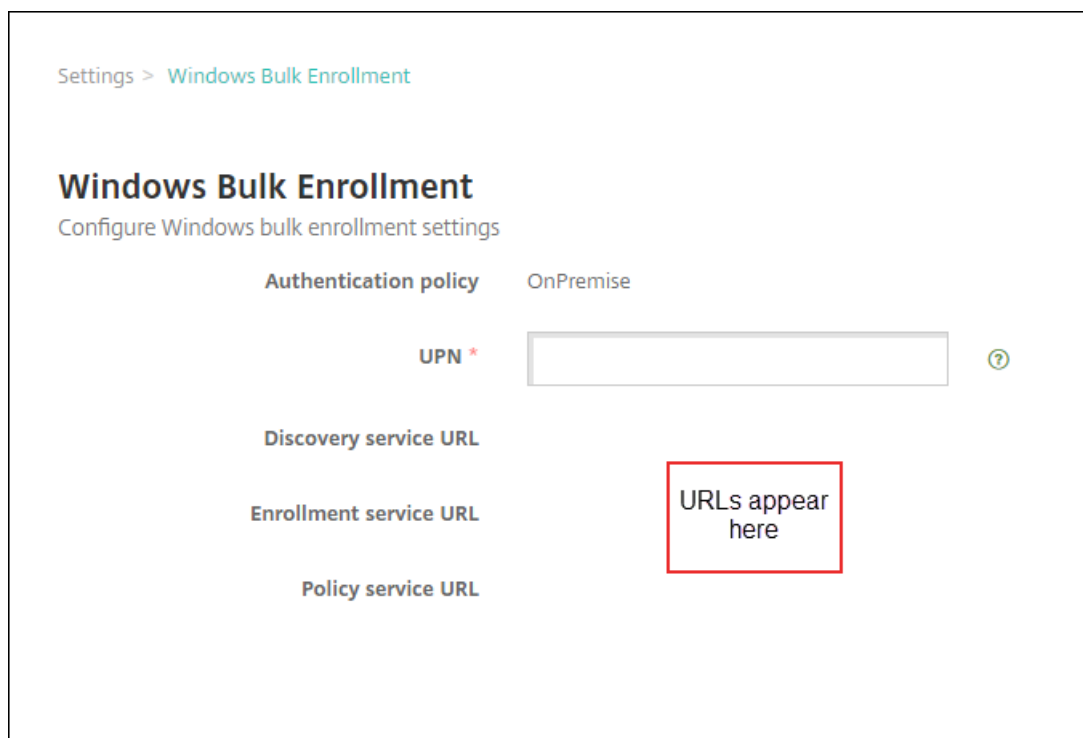


3. Haga clic en **Descargar** para descargar una plantilla (hoja de cálculo) para la lista de dispositivos permitidos. Rellene esa hoja de cálculo y, a continuación, cárguela con **Elegir archivo e importar**.

Configurar la inscripción en bloque

1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Inscripción en bloque 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 de Citrix Endpoint Management que tenga permisos

de inscripción. Puede proporcionar un UPN diferente del usuario asociado que seleccionó anteriormente.



Settings > Windows Bulk Enrollment

Windows Bulk Enrollment

Configure Windows bulk enrollment settings

Authentication policy OnPremise

UPN * ?

Discovery service URL

Enrollment service URL

Policy service URL

URLs appear here

Necesitará 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 en bloque, descargue el Diseñador de configuración de Windows desde la Tienda Microsoft. El Diseñador de configuración de Windows crea paquetes de aprovisionamiento que se utilizan para crear imágenes de dispositivos. En estos paquetes, puede incluir la configuración de la inscripción en bloque de Citrix Endpoint Management para que los dispositivos aprovisionados se inscriban automáticamente en Citrix Endpoint Management.

Para obtener información sobre el uso de un paquete de aprovisionamiento, consulte <https://docs.microsoft.com/en-us/windows/client-management/mdm/bulk-enrollment-using-windows-provisioning-tool>. Siga los pasos que se describen en la sección *Create and apply a provisioning package for on-premises authentication* de ese documento. Siga estos pasos para incluir las siguientes opciones de configuración de inscripción en bloque de Citrix Endpoint Management y para aplicar el paquete a cada uno de los dispositivos.

- **URL del servicio de detección.**

- **URL del servicio de inscripción.**
- **URL del servicio de directivas.**
- **Secreto.** Contraseña del UPN. Anteriormente, introdujo el nombre de usuario en el campo UPN.

Inscripción en bloque de dispositivos de forma inmediata

Citrix Endpoint Management admite la inscripción en bloque de dispositivos Windows de manera inmediata. Siga estos pasos para configurar y realizar la inscripción en bloque:

1. Utilice la consola de Citrix Endpoint Management para agregar dispositivos (uno por uno o en bloque) y configurar la inscripción en bloque. Para obtener más información, consulte [Agregar dispositivos en bloque](#) y [Configurar la inscripción en bloque](#).
2. Cree un paquete de aprovisionamiento como se describe en [Crear y aplicar un paquete de aprovisionamiento](#).

Nota:

Deberá configurar el nombre de 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 que especifique para cada dispositivo debe coincidir con el nombre utilizado al importar dispositivos de la lista de permitidos.

3. Coloque ese paquete de aprovisionamiento en un dispositivo de memoria USB.
4. Introduzca la memoria USB en el dispositivo de destino la primera vez que el usuario lo encienda.

El dispositivo Windows detecta automáticamente el paquete de aprovisionamiento (.ppkg) incluido 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.

En dispositivos con Windows 10 (versión 2004 o una posterior) o Windows 11, puede simplificar el proceso de inscripción mediante la creación de un solo paquete de aprovisionamiento. El paquete puede aplicarse a todos los dispositivos. Así, no necesitará crear un paquete de aprovisionamiento por cada dispositivo.

Para simplificar el proceso de inscripción, siga estos pasos al crear un paquete de aprovisionamiento:

1. Para ello, en el Diseñador de configuración de Windows, 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.

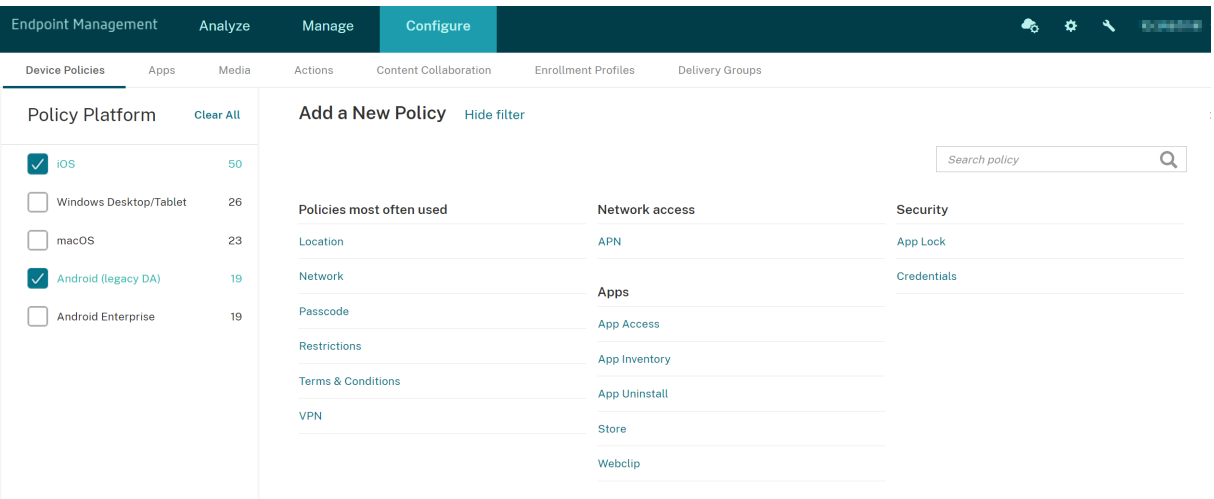
Directivas de dispositivo

March 1, 2024

Puede configurar la interacción entre Citrix Endpoint Management y los dispositivos mediante directivas. Aunque muchas directivas sean las mismas para todos los dispositivos, cada dispositivo tiene un conjunto específico de directivas para su sistema operativo. En consecuencia, se pueden encontrar muchas diferencias entre plataformas e incluso entre dispositivos Android de diferentes fabricantes.

Para ver las directivas que están 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 del panel **Plataforma de directiva**. 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 una descripción resumida de cada directiva de dispositivo, consulte Directivas de dispositivo resumidas en este artículo.

Nota:

Si el 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 que esté presente en uno o varios dispositivos inscritos entra en conflicto, tiene prioridad la directiva que concuerde con el GPO.

Para ver las directivas que admite el contenedor de Android Enterprise, consulte [Android Enterprise](#).

Requisitos previos

- Cree los grupos de entrega que va a utilizar.
- Instalar los certificados de CA necesarios.

Agregar una directiva de dispositivo

A continuación, se presentan los pasos básicos necesarios para crear una directiva de dispositivo:

1. Especificar el nombre y la descripción de la directiva.

Importante:

No utilice barras diagonales (/) en un nombre de directiva. Si lo hace, puede producirse un error al modificar la directiva más adelante.

2. Configurar la directiva para una o varias plataformas.
3. Crear las reglas de implementación (opcional).
4. Asignar la directiva a grupos de entrega.
5. Configurar la programación de las implementaciones (opcional).

Para crear y administrar directivas de dispositivo, vaya a **Configurar > Directivas de dispositivo**.

Device Policies

AppsMediaActionsShareFileEnrollment ProfilesDelivery Groups

Device Policies

Show filter

Search

Add

Export

<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status	▼
<input type="checkbox"/>	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM		
<input type="checkbox"/>	K--AppInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM		
<input type="checkbox"/>	K--Webclip	Mdm Weblink	8/12/17 6:46 AM	8/12/17 6:46 AM		
<input type="checkbox"/>	K--Passcode	Password	8/12/17 6:47 AM	8/12/17 6:47 AM		
<input type="checkbox"/>	K--Wifi	Wifi	8/12/17 6:47 AM	8/12/17 6:47 AM		
<input type="checkbox"/>	K--T&C	Terms Conditions	8/12/17 6:48 AM	8/12/17 6:48 AM		

Para agregar una directiva:

1. En la página **Directivas de dispositivo**, haga clic en **Agregar**. Aparecerá la página **Agregar nueva directiva**.

Endpoint Management

AnalyzeManageConfigure

Device PoliciesAppsMediaActionsContent CollaborationEnrollment ProfilesDelivery Groups

Policy Platform

Clear All

☐ iOS50

☐ Windows Desktop/Tablet26

☐ macOS23

☐ Android (legacy DA)19

☐ Android Enterprise19

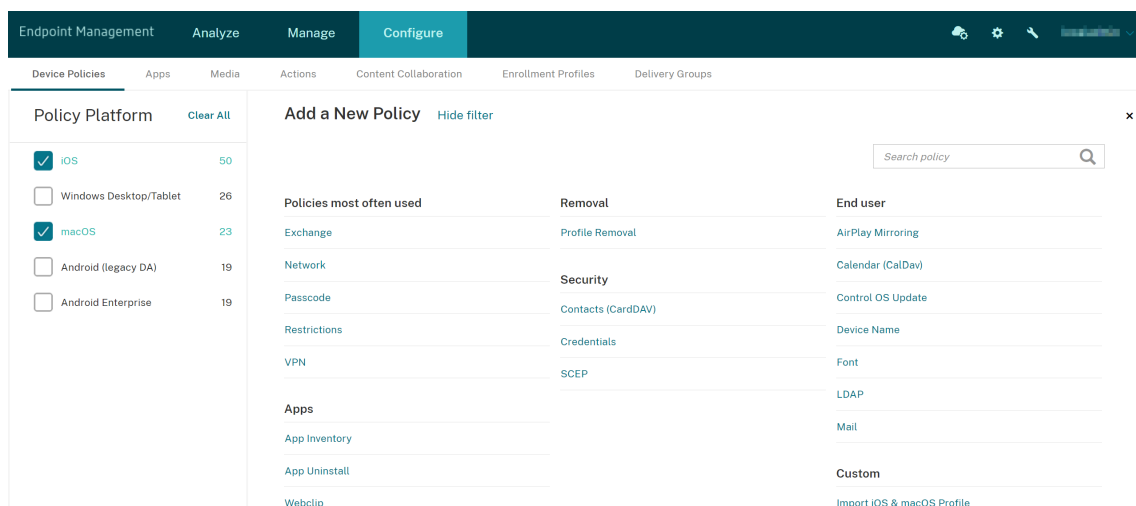
Add a New Policy

Hide filter

Search policy

Policies most often used	Removal	End user
Exchange	Profile Removal	AirPlay Mirroring
Location	Provisioning Profile Removal	AirPrint
Network		Bluetooth
Passcode	Security	Calendar (CalDav)
Restrictions	App Lock	Control OS Update
Scheduling	App Permissions	Device Name
Terms & Conditions	Application Guard	Font
VPN	BitLocker	Home Screen Layout
Network access	Contacts (CardDAV)	LDAP
	Credentials	Lock screen message

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 la directiva para continuar y agregar la directiva.



También puede escribir el nombre de la directiva en el cuadro de búsqueda. Cuando escriba, aparecerán posibles coincidencias. Si la directiva está en la lista, haga clic en ella. Solo permanecerá en los resultados la directiva que seleccione. Haga clic en la directiva para abrir la página **Información de directiva** referente a ella.

3. Seleccione las plataformas a incluir en la directiva. Las páginas de configuración referentes a las plataformas seleccionadas aparecerán en el paso 5.
4. Complete los datos de la página **Información de directiva** y haga clic en **Siguiente**. La página **Información de directiva** recopila información (como el nombre de la directiva) para ayudarle a identificar sus directivas y realizar un seguimiento de ellas. Esta página es similar para todas las directivas.
5. Complete las páginas de plataformas. Aparecerán páginas de cada plataforma que haya seleccionado en el paso 3. Estas páginas son distintas para cada directiva. Una directiva puede ser diferente en función de las plataformas. No todas las directivas se aplican a todas las plataformas.

Algunas páginas contienen tablas de elementos. Para eliminar un elemento existente, coloque el cursor sobre la línea que lo contiene y, a continuación, haga clic en el icono de papelera situado a la derecha. En el cuadro de diálogo de confirmación, haga clic en **Eliminar**.

Para modificar un elemento existente, coloque el cursor sobre la línea que lo contiene y haga clic en el icono de lápiz situado a la derecha.

Para configurar reglas de implementación, asignaciones y programación

Para obtener más información sobre cómo configurar las reglas de implementación, consulte [Implementación de recursos](#).

1. En la página de una 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 diferentes opciones para especificar las condiciones de implementación. Puede optar por implementar la directiva cuando se cumplan todas las condiciones o cuando se cumpla cualquiera de ellas. La opción predeterminada es **All**.
 - Haga clic en **Nueva regla** para definir las condiciones.
 - En las listas, haga clic en las condiciones (por ejemplo, **Propietario del dispositivo y BYOD**).
 - Si quiere agregar más condiciones, haga clic en **Nueva regla** de nuevo. Puede agregar cuantas condiciones quiera.
2. Haga clic en la ficha **Avanzado** para combinar las reglas con opciones booleanas. Las condiciones que haya elegido aparecerán en la ficha **Base**.
3. Puede usar lógica booleana más avanzada para combinar, modificar o agregar reglas.
 - Haga clic en **AND**, **OR** o **NOT**.
 - En la lista, seleccione las condiciones que quiere agregar a la regla. A continuación, haga clic en el signo más (+) situado en el lado derecho para agregar la condición a la regla.

En cualquier momento, puede seleccionar una condición y, a continuación, hacer clic en **Modificar** o en **Eliminar**.
 - Haga clic en **Nueva regla** para agregar otra condición.
4. Haga clic en **Siguiente** para ir a la página de la siguiente plataforma o, cuando haya completado todas las páginas de plataforma, para ir a la página **Asignaciones**.
5. En la página **Asignaciones**, seleccione los grupos de entrega a los que se aplicará la directiva. Al hacer clic en un grupo de entrega, el grupo aparecerá en el cuadro **Grupos de entrega a recibir asignaciones de aplicaciones**.

El cuadro **Grupos de entrega a recibir asignaciones de aplicaciones** no aparecerá hasta que seleccione un grupo de entrega.

Passcode Policy ✕

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Choose delivery groups

Type to search 🔍 Search

- ☒ AllUsers
- ☐ sales

Delivery groups to receive app assignment

- AllUsers

6. En la página **Asignaciones**, expanda **Programación de implementación** y, a continuación, configure los siguientes parámetros:

- Junto a **Implementar**, haga clic en **Sí** para programar la implementación, o bien, haga clic en **No** para cancelarla. De forma predeterminada, está **activado**.
- Junto a **Programación de implementación**, haga clic en **Ahora** o en **Más tarde**. La opción predeterminada es **Now**.
- Si hace clic en **Más tarde**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.
- Junto a **Condición de implementación**, puede hacer clic en **En cada conexión** o en **Solo cuando haya fallado la implementación anterior**. La opción predeterminada es **En cada conexión**.
- Junto a **Implementar para conexiones permanentes**, haga clic en **Sí** o **No**. De forma predeterminada, está **desactivado**.

Nota:

Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Parámetros > Propiedades de servidor**.

La opción permanente:

- No está disponible para dispositivos iOS
- No está disponible para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management a partir de la versión 10.18.19 o una posterior
- No se recomienda para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19

La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Implementar para conexiones permanentes**.

The screenshot shows a configuration panel for 'Deployment Schedule'. At the top, there is a dropdown menu set to 'Deploy' with an 'ON' toggle switch. Below this, there are two radio button options for 'Deployment Schedule': 'Now' (selected) and 'Later'. Underneath, there are two radio button options for 'Deployment condition': 'On every connection' (selected) and 'Only when previous deployment has failed'. At the bottom, there is a toggle switch for 'Deploy for always-on connections' which is currently 'OFF'.

7. Haga clic en **Guardar**.

La directiva aparecerá en la tabla **Directivas de dispositivo**.

Eliminar una directiva de un dispositivo

Los pasos para eliminar una directiva de dispositivo que hubiera en un dispositivo dependen de la plataforma.

- Android

Para eliminar una directiva de un dispositivo Android, use la directiva Desinstalar Citrix Endpoint Management. Para obtener más información, consulte [Directiva de desinstalación de Citrix Endpoint Management](#).

- iOS y macOS

Para eliminar una directiva de dispositivo que hubiera en un dispositivo iOS o macOS, use la directiva Eliminación de perfiles. En dispositivos iOS y macOS, todas las directivas forman parte del perfil MDM. Por lo tanto, puede crear una directiva Eliminación de perfiles solo para la directiva que quiere eliminar. El resto de las directivas y el perfil se conservan en el dispositivo. Para obtener más información, consulte [Directiva de eliminación de perfiles](#).

- Windows 10 y Windows 11

No puede quitar directamente una directiva de dispositivo que haya en un dispositivo de escritorio o tableta Windows. Sin embargo, puede utilizar cualquiera de los siguientes métodos:

- Anule la inscripción del dispositivo y envíe un nuevo conjunto de directivas a este. Los usuarios deben volver a inscribirse para continuar.
- Envíe una acción de seguridad para borrar selectivamente el dispositivo específico. Esta acción elimina todos los datos de empresa y todas las aplicaciones empresariales que hu-

biera en el dispositivo. A continuación, elimine la directiva de dispositivo que hubiera en el grupo de entrega que contiene solo ese dispositivo y envíe el grupo de entrega al dispositivo. Los usuarios deben volver a inscribirse para continuar.

Modificar una directiva de dispositivo

Para modificar una directiva de dispositivo, marque la casilla situada junto a dicha directiva. El menú de opciones aparece sobre la lista de directivas. O bien, haga clic en una directiva de la lista para mostrar más controles.

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery Groups

<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status	
<input type="checkbox"/>	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM		
<input checked="" type="checkbox"/>	K--AppInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM		
<input type="checkbox"/>	K--Webclip	Mdm Weblink				
<input type="checkbox"/>	K--Passcode	Password				
<input type="checkbox"/>	K--Wifi	Wifi				
<input type="checkbox"/>	K--T&C	Terms Conditions				
<input type="checkbox"/>	K--Location	Locationservices				
<input type="checkbox"/>	K--EAS	Exchange				
<input type="checkbox"/>	K--AppLock	Applock				

EditDelete

Deployment

0

Installed

0

Pending

0

Failed

Show more >

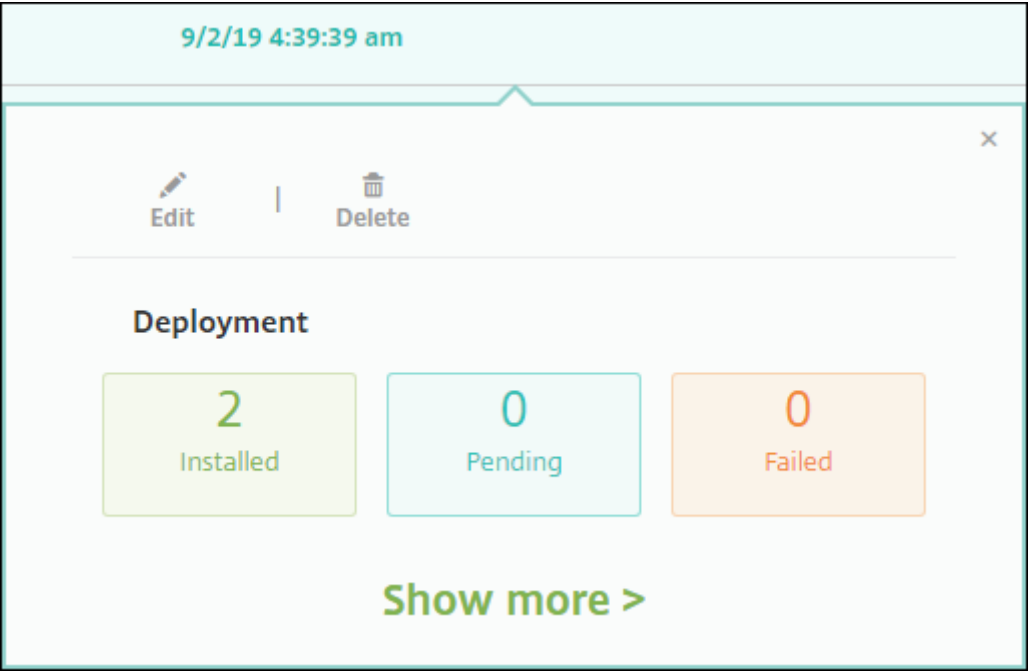
Para ver los detalles de la directiva, haga clic en **Mostrar más**.

Para modificar toda la configuración de una directiva de dispositivo, haga clic en **Modificar**.

Aparecerá un cuadro de diálogo de confirmación si hace clic en **Eliminar**. Haga clic en **Eliminar** de nuevo para eliminar la directiva.

Consultar el estado de implementación de directivas

En la página **Configurar > Directivas de dispositivo**, haga clic en la fila de una directiva para consultar el estado de su implementación.



Cuando está pendiente la implementación de una directiva, los usuarios pueden actualizar la directiva desde Citrix Secure Hub. Para ello, deben tocar **Preferencias > Información del dispositivo > Actualizar directiva**.

Filtrar la lista de las directivas de dispositivo agregadas

Puede filtrar la lista de las directivas agregadas por tipos de directivas, plataformas y grupos de entrega asociados. En la página **Configurar > Directivas de dispositivo**, haga clic en **Mostrar filtro**. En la lista, marque las casillas de los elementos que quiere ver.

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

Filters

Clear All

Policy Type

Clear

Policy Platform

Clear

☐

iOS

14

☐

macOS

5

☐

Android

13

☐

Samsung KNOX

3

☐

Android for Work

1

Show more

Associated Delivery Group

Clear

Device Policies

Hide filter

Search

Q

Add

Export

<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status	▼
<input type="checkbox"/>	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM		
<input type="checkbox"/>	K--ApplInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM		
<input type="checkbox"/>	K--Webclip	Mdm Weblink	8/12/17 6:46 AM	8/12/17 6:46 AM		
<input type="checkbox"/>	K--Passcode	Password	8/12/17 6:47 AM	8/12/17 6:47 AM		
<input type="checkbox"/>	K--Wifi	Wifi	8/12/17 6:47 AM	8/12/17 6:47 AM		
<input type="checkbox"/>	K--T&C	Terms Conditions	8/12/17 6:48 AM	8/12/17 6:48 AM		

Haga clic en **GUARDAR ESTA VISTA** para guardar un filtro. Entonces, el nombre del filtro aparecerá en el botón situado debajo del botón **GUARDAR ESTA VISTA**.

Directivas de dispositivo resumidas

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Duplicación AirPlay	Agrega dispositivos AirPlay específicos (tales como Apple TV u otro equipo Mac) a dispositivos iOS. También puede agregar dispositivos a una lista de permitidos para dispositivos supervisados. Esa opción limitará a los usuarios a solamente dispositivos AirPlay en la lista de permitidos.
AirPrint	Agrega impresoras AirPrint a la lista de impresoras AirPrint que aparece en los dispositivos iOS. Esta directiva facilita los entornos en los que las impresoras y los dispositivos están en subredes diferentes.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
APN	Determina los parámetros utilizados para conectar sus dispositivos al servicio GPRS (General Packet Radio Service) de un operador de teléfonos concreto. Esta configuración ya está definida en la mayoría de los teléfonos recientes. Use esta directiva si su organización no usa 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 prohibidas en el dispositivo. Luego, puede crear una acción automatizada como reacción al cumplimiento del dispositivo con los requisitos de dicha lista de aplicaciones.
Atributos de aplicación	Especifica atributos (por ejemplo, un ID de paquete de aplicación administrada o un identificador de red VPN por aplicación) para dispositivos iOS.
Configuración de aplicaciones	Permite configurar de forma remota varias opciones y comportamientos de las aplicaciones que admiten la configuración administrada. Para ello, debe implementar un archivo de configuración XML (llamado lista de propiedades o plist) en dispositivos iOS. O bien puede implementar pares de clave y valor en escritorios o tabletas con Windows 10.
Inventario de aplicaciones	Permite realizar un inventario de las aplicaciones presentes en los dispositivos administrados. Una vez realizado el inventario, Citrix Endpoint Management lo coteja con las directivas de acceso a aplicaciones que se hayan implementado en esos dispositivos. De esta forma, puede detectar aplicaciones que se encuentren en una lista de permitidos o en una lista de bloqueados (para acceder a ellas o no) y actuar correctamente.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Bloqueo de aplicaciones	Permite definir una lista de las aplicaciones que los usuarios pueden ejecutar o no en dispositivos iOS o en determinados dispositivos Android. Puede convertir un iPad en un quiosco.
Permisos de aplicación	Configura cómo gestionan las solicitudes a aplicaciones Android Enterprise incluidas en los perfiles de trabajo lo que Google considera permisos “peligrosos”.
Desinstalación de aplicaciones	Permite quitar aplicaciones de los dispositivos de usuario.
Restricciones de desinstalación de aplicaciones	Permite especificar las aplicaciones que los usuarios pueden o no pueden desinstalar.
Protección de aplicaciones	Pensada solo para el explorador Microsoft Edge, esta directiva especifica la configuración de la Protección de aplicaciones de Windows Defender. La configuración incluye si debe bloquearse, o no, contenido externo en sitios de empresa.
Notificaciones de aplicaciones	Controla cómo reciben los usuarios de iOS las notificaciones provenientes de aplicaciones concretas.
Actualizar automáticamente aplicaciones administradas	Controla cómo se actualizan en dispositivos Android Enterprise las aplicaciones administradas instaladas.
BitLocker	Permite configurar los parámetros disponibles en la interfaz de BitLocker en dispositivos con Windows 10 o Windows 11.
Bluetooth	Habilita o inhabilita el Bluetooth en dispositivos iOS.
Explorador web	Permite definir si los dispositivos de los usuarios pueden usar el explorador web o limitar las funciones de explorador web que se puedan usar.
Calendario (CalDAV)	Permite agregar una cuenta de calendario (CalDAV) a dispositivos iOS o macOS. La cuenta de CalDAV permite a los usuarios sincronizar datos de programación con cualquier servidor compatible con CalDAV.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Telefonía móvil	Permite configurar las opciones de red móvil.
Programación de conexiones	Es necesaria para que los dispositivos Android se conecten de vuelta a Citrix Endpoint Management para la administración MDM, el envío de aplicaciones y la implementación de directivas. Si no envía esta directiva y no habilita Google FCM, el dispositivo no podrá volver a conectarse al servidor.
Contactos (CardDAV)	Permite agregar una cuenta de contacto de iOS (CardDAV) a dispositivos iOS o macOS. La cuenta de CardDAV permite a los usuarios sincronizar datos de contacto con cualquier servidor compatible con CardDAV.
Credenciales	Permite la autenticación integrada con la configuración de PKI en Citrix Endpoint Management. Por ejemplo, con una entidad de PKI, un almacén de claves, un proveedor de credenciales o un certificado de servidor.
XML personalizado	Permite personalizar funciones tales como el aprovisionamiento de dispositivos, la habilitación de las funciones de los dispositivos, la configuración de dispositivos y la administración de fallos.
Defender	Permite configurar Windows Defender para tabletas y escritorios con Windows 10 o Windows 11.
Device Guard	Permite habilitar funciones de seguridad, tales como el arranque seguro, el bloqueo UEFI y la virtualización.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Atestación de mantenimiento de dispositivos	Requiere que los dispositivos con Windows 10 o Windows 11 informen de su estado. Para ello, deben enviar datos concretos e información del tiempo de ejecución al servicio Health Attestation Service (HAS) para el análisis. El servicio 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, según el contenido de éste, puede implementar las acciones automatizadas que haya configurado.
Nombre del dispositivo	Permite definir los nombres de los dispositivos iOS y macOS de forma que pueda identificarlos. Puede usar macros, texto o una combinación de ambos para definir el nombre del dispositivo.
Configuración de la educación	Permite configurar los dispositivos de profesores y alumnos para que se usen con Educación de Apple. Si los profesores utilizan la aplicación Aula, se necesita la directiva de configuración de la educación. Compatible con dispositivos iOS (iPadOS).
Opciones de Citrix Endpoint Management	Permite configurar el comportamiento de Citrix Secure Hub al conectarse a Citrix Endpoint Management desde dispositivos Android.
Desinstalación de Citrix Endpoint Management	Permite desinstalar Citrix Endpoint Management de dispositivos Android. Cuando se implementa, esta directiva elimina Citrix Endpoint Management de todos los dispositivos que contenga el grupo de implementación.
Exchange	Permite habilitar el correo electrónico de ActiveSync para el cliente de correo electrónico nativo en el dispositivo.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Archivos	Permite agregar a Citrix Endpoint Management archivos de script que realizan determinadas funciones para los usuarios. También puede agregar archivos de documento a los que quiere que los usuarios de dispositivos Android tengan acceso en sus dispositivos. Al agregar el archivo, también puede especificar el directorio donde se almacenará el archivo en ese dispositivo.
FileVault	Esta directiva le permite habilitar el cifrado de dispositivos FileVault en los dispositivos macOS inscritos. También puede controlar cuántas veces puede omitir un usuario la configuración de FileVault durante el inicio de sesión. Disponible para macOS 10.7 o versiones posteriores.
Firewall	Permite configurar los parámetros de firewall. Puede proporcionar las direcciones IP, los puertos y los nombres de host a los que quiera permitir o bloquear el acceso de los dispositivos. También puede configurar el proxy y las opciones de redirección de este.
Fuente	Permite agregar fuentes a dispositivos iOS y macOS. Las fuentes deben tener el formato TrueType (TTF) u OpenType (OFT). Citrix Endpoint Management no admite colecciones de fuentes (TTC, OTC).
Diseño de pantalla inicial	Permite especificar la distribución de aplicaciones y carpetas en la pantalla de inicio de iOS de los dispositivos supervisados.
Importar perfil de iOS y macOS	Permite importar en Citrix Endpoint Management archivos XML de configuración de dispositivos iOS y macOS. El archivo contiene las restricciones y las directivas seguridad de los dispositivos que se preparan con Apple Configurator.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Administración de Keyguard	Permite especificar las funciones disponibles para los usuarios antes de que desbloqueen el Keyguard del dispositivo y el Keyguard de Work Challenge. En el caso de dispositivos totalmente administrados y dedicados, también permite controlar funciones de Keyguard del dispositivo. Por ejemplo, es posible inhabilitar funciones de la pantalla de bloqueo, como desbloqueo mediante huella digital, agentes de confianza y notificaciones.
Configuración de Launcher	Especifica la configuración de Citrix Launcher en dispositivos Android, como las aplicaciones permitidas y una imagen de logotipo personalizado para el icono de Launcher.
LDAP	En dispositivos iOS, esta directiva permite proporcionar información sobre el servidor LDAP a utilizar, incluida la información de cuenta necesaria (como el nombre de host del servidor LDAP). La directiva también ofrece un conjunto de directivas de búsquedas LDAP a usar cuando se consulta el servidor LDAP.
Ubicación	Permite ubicar geográficamente los dispositivos en un mapa, siempre que el dispositivo tenga habilitado GPS para Citrix Secure Hub. Después de implementar esta directiva en el dispositivo, puede enviar el comando “locate” desde Citrix Endpoint Management. El dispositivo responde con sus coordenadas de ubicación. Citrix Endpoint Management también admite directivas de geocerca y seguimiento geográfico.
Mensaje de la pantalla bloqueada	Permite establecer los mensajes que aparecerán, en caso de pérdida, en la ventana de inicio de sesión de un iPad compartido y la pantalla de bloqueo de un dispositivo iOS supervisado.
Mail	Permite configurar una cuenta de correo electrónico en dispositivos iOS o macOS.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Configuraciones administradas	Controla diversas opciones de configuración y restricciones de aplicaciones para dispositivos Android Enterprise.
Dominios administrados	Permite definir los dominios administrados que se aplicarán al correo electrónico y al explorador web Safari. Los dominios administrados ayudan a proteger la información empresarial porque gestionan las aplicaciones que pueden abrir los documentos descargados desde dominios mediante Safari. Así, puede especificar las direcciones URL o los subdominios para controlar la forma en que los usuarios pueden abrir documentos, datos adjuntos y archivos descargados del explorador web en dispositivos iOS supervisados.
Máximo de usuarios residentes	Permite especificar la cantidad máxima de usuarios que puede tener un iPad compartido. Compatible con dispositivos iOS e iPadOS.
Opciones de MDM	Permite administrar la función Bloqueo de activación de Buscar mi iPhone o iPad en teléfonos iOS supervisados.
Red	Permite a los administradores implementar datos del enrutador Wi-Fi en los dispositivos administrados. Los datos de enrutador son: el SSID, los datos de autenticación y los datos de configuración.
Uso de la red	Permite definir reglas de uso de la red para especificar la forma en que las aplicaciones administradas deben usar, por ejemplo, redes de datos móviles en dispositivos iOS. Las reglas solo se aplican a aplicaciones administradas. Las aplicaciones administradas son aquellas que se implementan en los dispositivos de los usuarios por medio de Citrix Endpoint Management.
Office	Implemente aplicaciones de Microsoft Office en cualquier dispositivo con Windows 10 (versión 1709 o una posterior) o Windows 11.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Información sobre la organización	Permite especificar la información de la organización para los mensajes de alertas que Citrix Endpoint Management implementa en los dispositivos iOS.
Actualización de SO	Implementa las últimas actualizaciones del sistema operativo en dispositivos compatibles y supervisados.
Código de acceso	Permite imponer un código de acceso (PIN o contraseña) en un dispositivo administrado. Además, puede definir la complejidad y el tiempo de espera del código de acceso en el dispositivo.
Período de gracia de bloqueo de código de acceso	Permite especificar la cantidad de minutos que una pantalla de iPad compartido permanece bloqueada antes de que el usuario deba escribir un código de acceso para desbloquearla. Compatible con dispositivos iOS e iPadOS.
Hotspot personal	Permite a los usuarios conectarse a Internet cuando no tienen una red Wi-Fi al alcance. Los usuarios se conectan a través de una conexión de datos móviles en su dispositivo iOS con la funcionalidad de hotspot personal.
Eliminación de perfiles	Permite eliminar el perfil de aplicación que haya presente en los dispositivos macOS.
Perfil de datos	Permite indicar un perfil de datos de distribución empresarial que se envía a los dispositivos. Cuando desarrolla y firma el código de una aplicación iOS de empresa, generalmente incluye un perfil de datos. Apple requiere ese perfil para que la aplicación se pueda ejecutar en un dispositivo iOS. Si falta o ha caducado un perfil de datos, la aplicación se bloquea cuando un usuario toca en ella para abrirla.
Eliminación de perfiles de datos	Permite eliminar perfiles de datos de iOS.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Proxy	Permite especificar la configuración global de proxy HTTP en dispositivos iOS. Puede implementar solamente una directiva global de proxy HTTP por dispositivo.
Restricciones	Ofrece numerosas opciones para bloquear y controlar funciones y funcionalidades en los dispositivos administrados. Ejemplos de opciones de restricción: inhabilitar la cámara o el micrófono, aplicar reglas de itinerancia o pedir el acceso a servicios externos, como almacenes de aplicaciones.
Itinerancia	Permite configurar si se permite la itinerancia de voz y de datos en los dispositivos iOS. Si se inhabilita la itinerancia de voz, la itinerancia de datos se inhabilita 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 admite el servicio Enterprise Firmware-Over-The-Air (E-FOTA) de Samsung.
SCEP	Permite configurar dispositivos iOS y macOS para obtener un certificado desde un servidor SCEP externo. También puede entregar un certificado al dispositivo mediante SCEP de una PKI que está conectada a Citrix Endpoint Management. Para ello, cree un proveedor de PKI y una entidad de PKI en el modo distribuido.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Cuenta de inicio Single Sign-On (SSO)	Permite crear cuentas SSO para que los usuarios solo deban iniciar sesión una vez para acceder a Citrix Endpoint Management y a los recursos internos de la empresa. Así, no es necesario que los usuarios almacenen credenciales en el dispositivo. Citrix Endpoint Management utiliza las credenciales del usuario de empresa de una cuenta SSO para varias aplicaciones, incluidas las aplicaciones del App Store de Apple. Esta directiva es compatible con la autenticación Kerberos. Disponible para iOS.
Cifrado de almacenamiento	Permite cifrar el almacenamiento interno y el externo. En algunos dispositivos, esta directiva impide que los usuarios usen una tarjeta de almacenamiento en sus dispositivos.
Almacén	Permite especificar si aparecerá un clip web del almacén de aplicaciones en la pantalla de inicio de los dispositivos de usuario.
Calendarios suscritos	Permite agregar un calendario suscrito a la lista de calendarios en dispositivos iOS. Debe haberse suscrito a un calendario para poder agregarlo a la lista de calendarios suscritos ubicada en los dispositivos de los usuarios.
Términos y condiciones	Permite requerir que los usuarios acepten las directivas específicas de la empresa que regulan las conexiones a la red corporativa. Cuando los usuarios inscriban sus dispositivos en Citrix Endpoint Management, deberán aceptar los términos y las condiciones para llevar a cabo la inscripción. Si rechazan dichos términos y condiciones, se cancelará el proceso de inscripción.
Túnel	Defina parámetros de proxy entre el componente del cliente de cualquier aplicación del dispositivo móvil y el componente del servidor de aplicaciones.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
VPN	Permite acceder a sistemas back-end que utilizan tecnología antigua de puerta de enlace VPN. Esta directiva ofrece datos de conexión de puerta de enlace VPN que se pueden implementar en los dispositivos. Citrix Endpoint Management es compatible con varios proveedores de VPN, como Cisco AnyConnect, Juniper y Citrix VPN. También es posible vincular esta directiva a una entidad de certificación (CA) y habilitar VPN a demanda (siempre que la puerta de enlace VPN admita esta opción).
Fondo de pantalla	Permite agregar un archivo JPG o PNG para establecer el fondo de escritorio en un dispositivo iOS para la pantalla de bloqueo, la pantalla de inicio o ambas pantallas. Para usar fondos de pantalla diferentes en iPads y iPhones, debe crear varias directivas de fondo de escritorio y aplicarlas a los usuarios correspondientes.
Clip web	Permite colocar accesos directos (o clips web) que acceden a sitios web de forma 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	Permite filtrar el contenido web en dispositivos iOS. Citrix Endpoint Management utiliza la función Autofiltro de Apple y los sitios que usted agregue a las listas de permitidos y a las listas de bloqueados. Disponible solamente para dispositivos iOS supervisados.
Agente Windows	Habilite esta directiva para ejecutar los scripts de PowerShell cargados en escritorios y tabletas Windows.

Nombre de directiva de dispositivo	Descripción de directiva de dispositivo
Configuración del objeto de directiva de grupo Windows	Configure objetos de directiva de grupo (GPO) para cualquier dispositivo Windows admitido por Citrix Workspace Environment Management.
Windows Hello para empresas	Permite habilitar esa función Windows de modo que los usuarios puedan aprovisionar Windows Hello para empresas en sus dispositivos. La directiva también permite configurar limitaciones de códigos de acceso y otras funciones de seguridad.

Directivas de dispositivo por plataforma

Directiva	iOS	macOS	Android Enterprise	Android (AD heredado)	Escritorio o tableta	Otros
					Windows	
Directiva de duplicación	X	X				
AirPlay						
Directiva de AirPrint	X					
Directiva de APN	X			X		
Directiva de acceso a aplicaciones	X			X		
Directiva de atributos de aplicación	X					
Directiva de configuración de aplicaciones	X				X	

Directiva	iOS	macOS	Android Enterprise	Android (AD heredado)	Escritorio o tableta	
					Windows	Otros
Directiva de inventario de aplicaciones	X	X	X	X	X	
Directiva de bloqueo de aplicaciones	X			X	X	
Directiva de permisos de aplicación			X			
Directiva de desinstalación de aplicaciones	X	X	X	X		
Directiva de restricciones de desinstalación de aplicaciones						X
Directiva de protección de aplicaciones					X	
Directiva de notificaciones de aplicaciones	X					

Directiva	iOS	macOS	Android Enterprise	Android (AD heredado)	Escritorio o tableta	
					Windows	Otros
Actualizar automáticamente aplicaciones administradas			X			
Directiva de BitLocker					X	
Directiva de Bluetooth	X					
Directiva de explorador web						X
Directiva de calendario (CalDAV)	X	X				
Directiva de red de telefonía móvil	X					
Directiva de programación de conexiones			X	X		
Directiva de contactos (CardDAV)	X	X				
Directiva de copia de aplicaciones al contenedor de Samsung						X

Directiva	iOS	macOS	Android Enterprise	Android (AD heredado)	Escritorio o tableta	
					Windows	Otros
Directiva de Creden- ciales	X	X	X	X	X	
Directiva de XML person- alizado			X		X	
Directiva de Defender					X	
Directiva de Device Guard					X	
Directiva de Device Health Attestation					X	
Directiva de nombre de dispositivo	X	X				
Directiva de configu- ración de la educación	X					
Directiva de opciones de Citrix Endpoint Manage- ment			X	X		
Directiva de desinsta- lación de Citrix Endpoint Manage- ment				X		
Directiva de Exchange	X	X	X	X	X	

Directiva	iOS	macOS	Android Enterprise	Android (AD heredado)	Escritorio o tableta	
					Windows	Otros
Directiva de archivos			X	X		
Directiva de FileVault		X				
Directiva de firewall		X			X	
Directiva de fuentes	X	X				
Directiva de diseño de pantalla de inicio	X					
Directiva de im- portación de configu- ración del dispositivo						X
Directiva de im- portación de perfiles de iOS y macOS	X	X				
Directiva de dispositivos de adminis- tración de Keyguard			X			
Directiva de quiosco			X		X	
Directiva de configu- ración del Launcher			X	X		

Directiva	iOS	macOS	Android Enterprise	Android (AD heredado)	Escritorio o tableta	
					Windows	Otros
Directiva de LDAP	X	X				
Directiva de localización geográfica	X		X	X		
Directiva de mensaje de pantalla bloqueada	X					
Directiva de correo	X	X				
directiva de configuraciones administradas			X			
Directiva de dominios administrados	X					
Directiva de máximo de usuarios residentes	X					
Directiva de opciones de MDM	X					
Directiva de redes	X		X	X		
Directiva de uso de red	X					
Directiva de Office					X	

Directiva	iOS	macOS	Android Enterprise	Android (AD heredado)	Escritorio o tableta	
					Windows	Otros
Directiva de informa- ción de la organi- zación	X					
Directiva de actual- ización del SO	X	X	X		X	
Directiva de código de acceso	X	X	X	X	X	
Directiva de período de gracia de bloqueo de código de acceso	X					
Directiva de hotspot personal	X					
Directiva de eliminación de perfiles	X	X				
Directiva de perfil de datos	X					
Directiva de eliminación de perfiles de datos	X					
Directiva de proxy	X					
Directiva de restric- ciones	X	X		X	X	

Directiva	iOS	macOS	Android Enterprise	Android (AD heredado)	Escritorio o tableta	
					Windows	Otros
Directiva de itinerancia	X					
Directiva de clave de licencia			X			
MDM de Samsung						
Directiva de SCEP	X	X				
Directivas de Siri y dictado	X					
Directiva de cuenta SSO	X					
Directiva de cifrado de almacenamiento						
Directiva de tiendas	X			X	X	
Directiva de calendarios suscritos	X					
Directiva de términos y condiciones	X			X	X	
Directiva de túnel				X		
Directiva de VPN	X	X		X	X	
Directiva de fondo de pantalla	X					
Directiva de clip web	X	X		X	X	

					Escritorio o tableta	
Directiva	iOS	macOS	Android Enterprise	Android (AD heredado)	Windows	Otros
Directiva de filtro de contenido web	X					
Directiva de Agente de Windows					X	
Directiva de configuración de GPO de Windows					X	
Directiva de Hello para empresas					X	

Directiva de duplicación AirPlay

November 29, 2023

La función AirPlay de Apple permite a los usuarios reproducir contenido de un dispositivo iOS en una pantalla de TV de forma inalámbrica y a través de Apple TV. También permite replicar de forma exacta lo que aparece en la pantalla de un dispositivo en la pantalla de una TV o de otro equipo Mac.

En Citrix Endpoint Management, puede agregar una directiva de dispositivo para agregar dispositivos AirPlay específicos (como Apple TV u otro equipo Mac) a los dispositivos iOS. También tiene la opción de agregar dispositivos a una lista de dispositivos supervisados permitidos, lo que limita a los usuarios a esos dispositivos AirPlay únicamente. Para obtener información sobre cómo colocar un dispositivo en modo supervisado, consulte [Implementar dispositivos mediante Apple Configurator 2](#).

Nota:

Antes de continuar, compruebe que dispone de los ID de los dispositivos pertinentes, así como de las contraseñas de todos los dispositivos que quiera agregar.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Contraseña de AirPlay:** Para agregar cada dispositivo, haga clic en **Agregar** y lleve a cabo lo siguiente:
 - **Nombre del dispositivo:** Escriba la dirección de hardware (dirección MAC) en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
 - **Contraseña:** Escriba una contraseña opcional para el dispositivo.
 - Haga clic en **Agregar** para agregar el dispositivo, o bien haga clic en **Cancelar** para no agregarlo.
- **ID de la lista de permitidos:** Esta lista se omite en caso de dispositivos no supervisados. Los ID de dispositivo de esta lista pertenecen a los únicos dispositivos AirPlay que se encuentran a disposición de los dispositivos de usuarios. Para agregar cada dispositivo AirPlay a la lista, haga clic en **Agregar** y lleve a cabo lo siguiente:
 - **ID del dispositivo:** Escriba el ID del dispositivo en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
 - Haga clic en **Agregar** para agregar el dispositivo, o bien haga clic en **Cancelar** para no agregarlo.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.

Parámetros de macOS

AirPlay mirroring policy

This policy lets you configure specific AirPlay devices to add to iOS and macOS devices. For supervised devices, you can also add a list of allowed AirPlay devices.

AirPlay password

Device name * Password * Add

Allow list ID

Device ID * Add

Policy Settings

Remove policy ☒ Select date ☐ Duration until removal (in hours)

Allow user to remove policy Always ⓘ

Profile scope User macOS 10.7+

Back Next >

- **Contraseña de AirPlay:** Para agregar cada dispositivo, haga clic en **Agregar** y lleve a cabo lo siguiente:
 - **Nombre del dispositivo:** Escriba la dirección de hardware (dirección MAC) en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
 - **Contraseña:** Escriba una contraseña opcional para el dispositivo.
 - Haga clic en **Agregar** para agregar el dispositivo, o bien haga clic en **Cancelar** para no agregarlo.
- **ID de la lista de permitidos:** Esta lista se omite en caso de dispositivos no supervisados. Los ID de dispositivo de esta lista pertenecen a los únicos dispositivos AirPlay que se encuentran a disposición de los dispositivos de usuarios. Para agregar cada dispositivo AirPlay a la lista, haga clic en **Agregar** y lleve a cabo lo siguiente:
 - **ID del dispositivo:** Escriba el ID del dispositivo en el formato xx:xx:xx:xx:xx:xx. Este campo no distingue entre mayúsculas y minúsculas.
 - Haga clic en **Agregar** para agregar el dispositivo, o bien haga clic en **Cancelar** para no agregarlo.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar 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**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Directiva de AirPrint

December 6, 2021

La directiva AirPrint permite agregar impresoras AirPrint a la lista de impresoras AirPrint que aparecen en los dispositivos iOS. Esta directiva facilita los entornos en los que las impresoras y los dispositivos están en subredes diferentes.

Nota:

Para configurar la directiva 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 agregar cada destino de AirPrint, haga clic en **Agregar** y lleve a cabo lo siguiente:
 - **Dirección IP:** Escriba la dirección IP de la impresora AirPrint.
 - **Ruta del recurso:** Escriba la ruta del recurso asociada a la impresora. Este valor corresponde al parámetro del registro Bonjour de `_ipps.tcp`. Por ejemplo, `printers/Canon_MG5300_series` o `printers/Xerox_Phaser_7600`.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.

- ★ **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Solo disponible para iOS 6.0 o versiones posteriores.

Directiva de permisos de aplicación

March 1, 2024

Para las aplicaciones de Android Enterprise que se hallan en perfiles de trabajo: Puede definir cómo las solicitudes a estas aplicaciones gestionan lo que Google considera permisos “peligrosos”. Usted controla si solicitar a los usuarios que concedan o denieguen una solicitud de permiso por parte de las aplicaciones. Esta función se aplica a dispositivos que ejecutan Android 7.0 y versiones posteriores.

Google define como peligrosos aquellos permisos que:

- Otorgan a una aplicación acceso a datos o recursos que implican una información privada del usuario.
- O bien pueden afectar los datos almacenados del usuario o el funcionamiento de otras aplicaciones. Por ejemplo, la capacidad de leer contactos de usuario es un permiso peligroso.

Puede configurar un estado global para controlar el comportamiento de todas las solicitudes de permisos peligrosos. El ámbito de este parámetro son las aplicaciones de Android Enterprise que se encuentran en los perfiles de trabajo. También puede controlar el comportamiento de la solicitud de permisos peligrosos para grupos de permisos individuales, según lo definido por Google, para cada aplicación. Esas configuraciones individuales prevalecen sobre el estado global.

Para obtener información sobre cómo define Google los grupos de permisos, consulte la [Guía de desarrolladores de Android](#).

De forma predeterminada, se solicitará 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 [Directivas de dispositivo](#).

Parámetros de Android Enterprise

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

Android Enterprise App Permissions

1 Policy Info

2 Platforms Clear All

Android Enterprise

3 Assignment

Android Enterprise App Permissions

This policy lets you specify the behavior when Android Enterprise apps request dangerous permissions.

Global State *

Prompt

Calendar

App *	Grant Status	<div>+ Add</div>
Gmail	Deny	

Camera

App *	Grant Status	<div>+ Add</div>
com.sec.android.gallery3d	Deny	

Contacts

App *	Grant Status	<div>+ Add</div>
com.sec.android.gallery3d	Deny	

Location

App *	Grant Status	<div>+ Add</div>
-------	--------------	------------------

Microphone

App *	Grant Status	<div>+ Add</div>
-------	--------------	------------------

Phone

App *	Grant Status	<div>+ Add</div>
-------	--------------	------------------

Sensors

App *	Grant Status	<div>+ Add</div>
-------	--------------	------------------

Back

Next >

- **Estado global:** Controla el comportamiento de todas las solicitudes de permisos peligrosos. En la lista, haga clic en **Preguntar**, **Conceder** o **Denegar**.
 - **Preguntar:** Se solicita a los usuarios que concedan o denieguen las solicitudes de permisos peligrosos.
 - **Conceder:** Se conceden todas las solicitudes de permisos peligrosos. No se pregunta al usuario.
 - **Denegar:** Se deniegan todas las solicitudes de permisos peligrosos. No se pregunta al usuario.

El valor predeterminado es **Preguntar**.

- Puede configurar un comportamiento individual de cada grupo de permisos para cada aplicación. Para configurar el comportamiento de un grupo de permisos, haga clic en **Agregar** y, a continuación, en **Aplicación**, elija una aplicación de la lista. Si configura las aplicaciones del sistema Android Enterprise, haga clic en **Agregar** e indique el nombre del paquete de aplicaciones que habilitó en la directiva de restricciones. En “Estado de acceso”, elija **Preguntar**, **Conceder** o **Denegar**. Este estado de acceso prevalece sobre el estado global.
 - **Preguntar:** Se solicita a los usuarios que concedan o denieguen las solicitudes de permisos peligrosos de este grupo para esta aplicación.
 - **Conceder:** Se conceden las solicitudes de permisos peligrosos de este grupo para esta aplicación. No se pregunta al usuario.

Nota:

Para los dispositivos inscritos en el modo **Propietario de perfil**, el permiso **Conceder** no se aplica a la cámara, a la ubicación, al micrófono ni al sensor si el dispositivo emplea Android 12 o una versión posterior.

- **Denegar:** Se rechazan las solicitudes de permisos peligrosos de este grupo para esta aplicación. No se pregunta al usuario.

El valor predeterminado es **Preguntar**.

- Haga clic en **Guardar**, situado junto a la aplicación y el estado de acceso.
- 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 acceso** de todos los grupos de permisos pertinentes, haga clic en **Siguiente**.

Directiva de APN

December 6, 2021

Puede agregar una directiva de nombre de punto de acceso (APN) de dispositivo para dispositivos iOS y Android. Use esta directiva si su organización no usa un APN de consumidor para conectarse a Internet desde un dispositivo móvil. Una directiva de nombres APN determina la configuración utilizada para conectar sus dispositivos al servicio GPRS de un operador concreto. 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](#).

Parámetros de iOS

APN Policy
✕

This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.

APN *

User name

Password

Server proxy address

Server proxy port

Policy Settings

Remove policy

☒ Select date

☐ Duration until removal (in hours)

📅

Back

Next >

- **APN:** Introduzca el nombre del punto de acceso. El nombre debe coincidir con un nombre APN de iOS aceptado o, si no, la directiva no funciona.
- **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 de perfil.
- **Contraseña:** La contraseña del usuario para este APN. Por motivos de seguridad, la contraseña se cifra. Si no está presente en la carga, el dispositivo solicitará la contraseña durante la instalación de perfil.
- **Dirección del servidor proxy:** La dirección IP o dirección URL del proxy de APN.
- **Puerto del servidor proxy:** El número de puerto del proxy de APN. El número de puerto es necesario si especificó la dirección de un servidor proxy.
- En **Configuraciones de directivas**, junto a **Quitar directiva**, haga clic en **Seleccionar fecha** o **Demora hasta la eliminación (en horas)**.
 - Para la opción **Seleccionar fecha**, haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - Para la opción **Se requiere contraseña**, escriba la contraseña.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Solo disponible para iOS 6.0 o versiones posteriores.

Parámetros de Android

APN Policy ✕

This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.

APN *	<input type="text"/>
User name	<input type="text" value="administrator"/>
Password	<input type="password" value="*****"/>
Server	<input type="text"/>
APN type	<input type="text"/>
Authentication type	<input type="text" value="None"/>
Server proxy address	<input type="text"/>
Server proxy port	<input type="text"/>
MMSC	<input type="text"/>

Back Next >

- **APN:** Introduzca el nombre del punto de acceso. El nombre debe coincidir con un nombre APN de Android aceptado o, si no, la directiva no funciona.
- **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 de perfil.
- **Contraseña:** La contraseña del usuario para este APN. Por motivos de seguridad, la contraseña se cifra. Si no está presente en la carga, el dispositivo solicitará la contraseña durante la instalación de perfil.
- **Servidor:** Este parámetro es anterior a los smartphones y normalmente queda vacío. Hace referencia a un servidor de puerta de enlace para protocolos de aplicación inalámbrica (WAP), destinado a teléfonos que no pueden acceder a sitios web estándar o mostrarlos.
- **Tipo de APN:** Este parámetro debe coincidir con el uso previsto del operador para el punto de acceso. Es una cadena separada por comas que contiene especificadores del servicio APN, y debe coincidir con las definiciones publicadas del operador inalámbrico. Por ejemplo:
 - *: Todo el tráfico de red pasa por este punto de acceso.
 - **mms**: El tráfico multimedia pasa por este punto de acceso.
 - **default**: Todo el tráfico de red, incluido el multimedia, pasa por este punto de acceso.
 - **supl**: El protocolo Secure User Plane Location está asociado al GPS asistido.
 - **dun**: El acceso telefónico a redes (Dial Up Networking) se ha retirado y no se usa a menudo.
 - **hipri**: Redes de alta prioridad.
 - **fota**: El firmware over-the-air se usa para recibir actualizaciones de firmware.
- **Tipo de autenticación:** En la lista, haga clic en el tipo de autenticación que se va a usar. El valor predeterminado es “Ninguna”.
- **Dirección del servidor proxy:** La dirección IP o dirección URL del proxy HTTP de APN del oper-

ador.

- **Puerto del servidor proxy:** El número de puerto del proxy de APN. El puerto es necesario si especificó la dirección de un servidor proxy.
- **MMSC:** La dirección del servidor de puerta de enlace MMS suministrada por el operador.
- **Dirección del proxy de MMS:** La dirección del servidor de MMS para el tráfico de mensajes multimedia. Los mensajes MMS sustituyeron a los mensajes SMS para enviar mensajes más largos con contenido multimedia, como imágenes o vídeos. Estos servidores requieren protocolos específicos (como MM1 y similares hasta MM11).
- **Puerto MMS:** El puerto utilizado para el proxy MMS.

Directiva de acceso a aplicaciones

November 29, 2023

La directiva de acceso a aplicaciones le permite definir una lista de aplicaciones que deben instalarse, que pueden instalarse o que 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 el cumplimiento de esta directiva de dicho dispositivo.

Importante:

La directiva de acceso a aplicaciones no impide que un usuario instale aplicaciones prohibidas o desinstale aplicaciones requeridas.

Solo puede configurar un tipo de directiva de acceso en un momento dado. Cada directiva contiene una lista de aplicaciones obligatorias, 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, nombre cada directiva de manera explícita para saber qué directiva se aplica exactamente a qué lista de aplicaciones concreta.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS y Android (AD heredado)

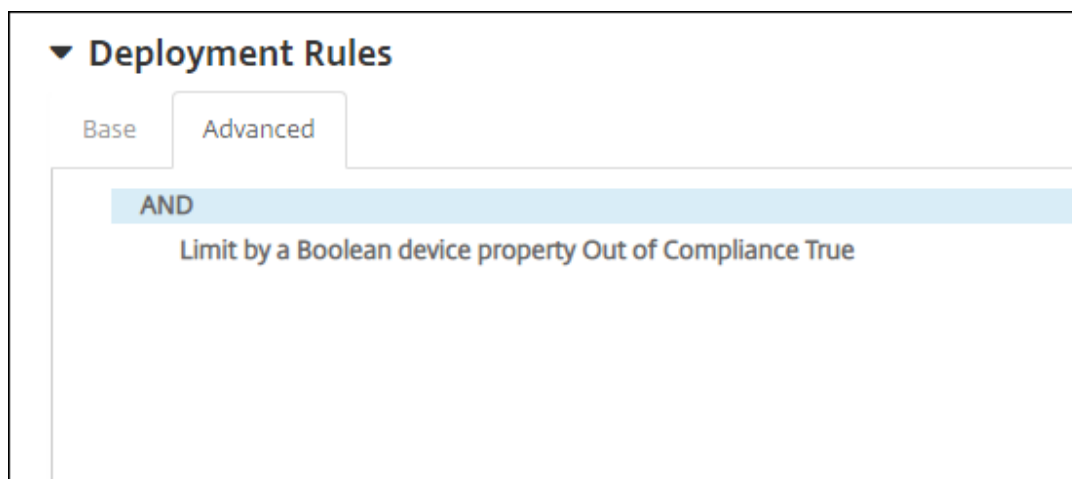
- **Directiva de acceso:** Seleccione el tipo de lista que quiere configurar para esta directiva.
 - **Requerido:** La aplicación debe existir en el dispositivo. Si la aplicación no existe, el dispositivo se marca como no conforme. **Requerido** es la opción predeterminada.

- **Prohibido:** La aplicación no debe existir en el dispositivo. Si la aplicación existe, el dispositivo se marca como no conforme.
- Para agregar aplicaciones a la lista:
 1. Haga clic en **Agregar** y, a continuación, configure lo siguiente:
 - **Nombre de la aplicación:** Escriba el nombre de la aplicación.
 - **Identificador de la aplicación:** Escriba un identificador opcional de la aplicación.
 2. Haga clic en **Guardar**.
 3. Repita estos pasos para cada aplicación que quiera agregar.

Configurar acciones automatizadas en función del cumplimiento del acceso a las aplicaciones

1. Agregue una directiva de acceso a aplicaciones para que se necesiten o se prohíban aplicaciones.
2. Configure dos acciones automatizadas según si las aplicaciones en cuestión sean necesarias o estén prohibidas:
 - Si son necesarias
 - Marca un dispositivo como no conforme si en el dispositivo no existe una aplicación que se necesita.
 - Marca un dispositivo como conforme una vez instalada la aplicación que se necesita.
 - Si están prohibidas
 - Marca un dispositivo como no conforme si en el dispositivo existe una aplicación prohibida.
 - Marca un dispositivo como conforme cuando la aplicación prohibida ya no esté instalada.

Para obtener información sobre la configuración de acciones automatizadas, consulte [Acciones automatizadas](#).
3. Cree una directiva de restricciones con los parámetros que quiera implementar en dispositivos no conformes.
 - a) Como parte de la directiva de restricciones, agregue una regla de implementación avanzada con las opciones **Limitar por propiedad booleana de dispositivo**, **No conforme** y **True**. Consulte [Directiva de restricciones](#).



4. Cree una directiva de eliminación de perfiles para quitar la directiva de restricciones una vez que el dispositivo haya vuelto a cumplir la normativa.
5. Agregue una regla de implementación avanzada con las opciones **Limitar por propiedad booleana de dispositivo, No conforme** y **False**. Consulte [Directiva de eliminación de perfiles](#).

Directiva de atributos de aplicación

November 29, 2023

La directiva **Atributos de aplicación** le permite especificar atributos para aplicaciones en dispositivos iOS. Al configurar este tipo de directiva, puede lograr lo siguiente:

- Asignar redes VPN por aplicación a las aplicaciones.
- Impedir que los usuarios desinstalen aplicaciones esenciales. Se aplica a iOS 14 y versiones posteriores.
- Si la función Dominios asociados está habilitada, especifique los dominios asociados que quiere agregar 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 la aplicación, de modo que pueda compartir credenciales o proporcionar funciones en la aplicación desde

los sitios web. Por ejemplo, con esta función habilitada, puede compartir datos y credenciales de inicio de sesión entre las aplicaciones y los sitios web de su organización.

Para obtener más información sobre cómo habilitar esta función, consulte [Supporting Associated Domains](#) en el sitio web de Apple.

Parámetros de iOS

The screenshot shows the 'App attributes' configuration page in the Citrix Endpoint Management console. The page is divided into several sections: 'Policy Info', 'Platforms' (with 'iOS' selected), and 'Assignment'. The 'App attributes' section contains the following fields and options:

- Managed app bundle ID:** A dropdown menu with the option 'Make a selection'.
- Per-app VPN identifier:** A dropdown menu with the option 'None'.
- Removable app:** A toggle switch that is currently turned on.
- Enable associated domain direct download:** A toggle switch that is currently turned on.
- Associated Domains:** A table with one entry, 'example.com', and an 'Add' button.

- **ID de paquete de apps administradas:** Especifique una aplicación de las siguientes maneras:
 - Seleccione el ID del paquete de aplicación. Las opciones están disponibles solo después de habilitar la directiva **Inventario de aplicaciones**, que recopila un inventario de aplicaciones en dispositivos administrados.
 - Seleccione **Agregar** y, a continuación, escriba el ID del paquete de aplicación. Para encontrar un ID de paquete de aplicación, consulte [Buscar el ID de paquete de una aplicación en el 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 se configuraron en la página **Directivas de dispositivo > Directiva VPN**. Para obtener más información, consulte [Configurar una VPN por aplicación](#).
- **Aplicación eliminable:** (Opcional) Especifique si los usuarios pueden quitar esta aplicación cuando se trata de una aplicación administrada. Para evitar que los usuarios desinstalen esta aplicación, **desactive** esta opción. El valor predeterminado es **Activado**.
- **Habilitar la descarga directa de dominios asociados:** (Opcional) De forma predeterminada, está **activada**, lo que indica que esta aplicación verifica la asociación de sitios comprobados directamente en el dominio, en lugar de hacerlo en los servidores de Apple. **Active** esta opción para dominios que no pueden acceder a Internet.
- **Dominios asociados:** (Opcional) Para agregar un dominio asociado para 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 el App Store

1. Busque la aplicación en el App Store y copie el número que aparece al final de la URL. Por ejemplo, 363501921 es el ID de la aplicación Citrix Workspace.
2. Vaya a <https://itunes.apple.com/lookup?id=> y pegue el número después de esa URL. Se descarga automáticamente un archivo TXT en el equipo.
3. En el archivo TXT, busque `bundleId` y obtenga el ID de paquete de la aplicación. Por ejemplo: El ID de paquete de la aplicación Citrix Workspace es `com.citrix.ReceiveriPad`.

Directiva de configuración de aplicaciones

March 1, 2024

Puede configurar, de forma remota, aplicaciones que admitan la configuración administrada. Para ello, debe implementar:

- Un archivo de configuración XML (también denominado lista de propiedades o `.plist`) en los dispositivos iOS.
- Pares de clave y valor en escritorios, tabletas o teléfonos con Windows 10 o Windows 11.

La configuración permite especificar varios parámetros y comportamientos de la aplicación. Citrix Endpoint Management envía la configuración a los dispositivos cuando los usuarios instalan la aplicación. Los parámetros y los comportamientos que se puedan configurar dependen de la aplicación y no forman parte del ámbito de este artículo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Nota:

Las variables de configuración de la aplicación las definen los respectivos propietarios de la aplicación.

Por ejemplo, Chrome administra y mantiene las variables de configuración de aplicaciones para Chrome. Para obtener más información, consulte [Variables de configuración de la aplicación Chrome](#).

Parámetros de iOS

- **Identificador:** En la lista, haga clic en la aplicación que quiera configurar, o bien 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 bien copie y pegue la información de configuración de la lista de propiedades XML (.plist).
- Haga clic en **Diccionario de comprobación**. Citrix Endpoint Management verifica el XML. Si no hay errores, verá **XML válido** bajo el cuadro de contenido. Si apareciera algún error de sintaxis bajo el cuadro de contenido, deberá corregirlo antes de continuar.

Parámetros de escritorios y tabletas Windows

Puede configurar aplicaciones de Plataforma universal de Windows (UWP) o aplicaciones Win32. Para importar los parámetros de la directiva de la plantilla administrativa de Microsoft (ADMX), configure las aplicaciones Win32.

Nota:

La directiva Configuración de aplicaciones admite archivos ADMX de terceros para aplicaciones de terceros (como Office). Por el contrario, no se admiten las plantillas de Microsoft ADMX para Windows que se proporcionan como directivas de grupo del sistema operativo disponibles en `%SystemRoot%\PolicyDefinitions<!--NeedCopy-->`.

- Si elige **Aplicación UWP**: En la lista **Seleccionar**, haga clic en la aplicación que quiera configurar, o bien haga clic en **Agregar nuevo** para agregar una aplicación a la lista.

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

App Configuration Policy

1 Policy Info

2 Platforms Clear All

☒ iOS

☒ Windows Phone

☒ Windows Desktop/Tablet

☒ Workspace Hub

3 Assignment

App Configuration Policy

This policy lets you specify key/value configuration parameters for an app. XenMobile pushes the app configuration to the device when the app gets installed. Please note that Win32 App configuration in the dropdown below holds good only for RS2 and above devices.

Application Type

UWP App

Make a selection

Parameter name

Value

Add

Deployment Rules

- Si hace clic en **Agregar nuevo**, escriba el nombre de familia del paquete en el campo que aparece.
- Haga clic en **Agregar** para agregar cada parámetro de configuración y lleve a cabo lo siguiente:
 - * **Nombre del parámetro:** Escriba el nombre clave de un parámetro de aplicación para el dispositivo Windows. Para obtener más información acerca de los parámetros de aplicación de Windows, consulte la documentación de Microsoft.
 - * **Valor:** Escriba el valor del parámetro especificado.
 - * Haga clic en **Agregar** para agregar el parámetro, o bien haga clic en **Cancelar** para no agregarlo.
- Si elige **Aplicación Win32:** Haga clic en **Examinar** y vaya al archivo ADMX que quiere usar para configurar la directiva.

App configuration

1 Policy Info

2 Platforms Clear All

☒ iOS

☒ Windows Phone

☒ Windows Desktop/Tablet

☒ Workspace Hub

3 Assignment

App configuration

This policy lets you specify key/value configuration parameters for an app. Endpoint Management pushes the app configuration to the device when the app gets installed. For Win32, the policy applies only to devices running RS2+.

Application type

Win32 app

ADMX file *

Browse

Add

Delete

admxmlname

Click 'Add' to add new Configuration

- Haga clic en **Agregar**. Las opciones de configuración del archivo ADMX aparecen en el lado derecho de la página.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

684

- Seleccione una ruta para la directiva. Si elige la misma ruta más de una vez, se aplica la configuración asociada a la versión más reciente seleccionada.
- **Active** la opción **Habilitar**.
- En la lista, introduzca los valores de los elementos como pares clave-valor. Use la cadena de texto **** para separar cada par clave-valor, y el valor y la clave dentro del par.
- Los valores de elementos que contienen un número decimal pueden requerir valores dentro de un rango concreto.

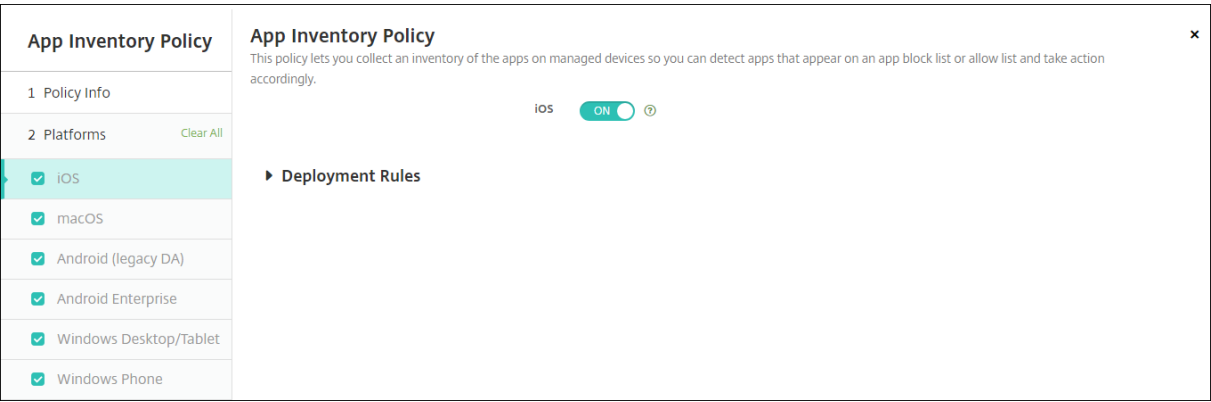
Directiva de inventario de aplicaciones

November 29, 2023

La directiva “Inventario de aplicaciones” permite realizar un inventario de las aplicaciones presentes en los dispositivos administrados. Una vez realizado el inventario, Citrix Endpoint Management puede cotejarlo con las directivas de acceso a aplicaciones que se hayan implementado en esos dispositivos. De esta manera, puede detectar aplicaciones que aparecen en una lista de aplicaciones permitidas o en una lista de aplicaciones bloqueadas y actuar en consecuencia. Utilice una directiva Acceso a aplicaciones para definir listas de aplicaciones 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 (AD heredado), Android Enterprise, escritorios Windows y tabletas Windows



- Para cada plataforma que seleccione, deje el valor predeterminado o **desactive** la opción. El valor predeterminado es **Activado**.

Inventario y eliminación de aplicaciones Win32

Puede determinar si las aplicaciones Win32 presentes en los dispositivos de usuario cumplen la directiva “Acceso a aplicaciones”. Para ver un inventario de las aplicaciones Win32 que están presentes en dispositivos administrados de tabletas y escritorios con Windows 10 o Windows 11:

1. Vaya a **Configurar > Directivas de dispositivo** y agregue una directiva “Inventario de aplicaciones” para la plataforma **Escritorio/tableta Windows**. Implemente la directiva.
2. Vaya a **Administrar > Dispositivos**, seleccione el dispositivo con Windows 10 o Windows 11 que quiere ver, haga clic en **Modificar** y, a continuación, haga clic en la ficha **Aplicaciones**.

Se muestran los resultados del inventario.

Nota:

Si configura un dispositivo con Windows 11, debe esperar hasta 24 horas para obtener resultados de inventario precisos, tal y como fue diseñado por Microsoft.

Devices

Users

Enrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Assigned Policies

5 Apps

6 Media

7 Actions

8 Delivery Groups

9 Certificates

10 Connections

Apps

Last inventory: 11/13/17 4:26:56 am

Installed (55)

Pending (0)

Failed (0)

Name	Ownership	Version	Author	Size	Installed	Identifier	Type
Microsoft.BingNews	Personal	4.21.2212.0			11/13/17 4:21:50 am	Microsoft.BingNews_8wekyb3d8bbwe	
Microsoft.BingWeather	Personal	4.21.2212.0			11/13/17 4:21:50 am	Microsoft.BingWeather_8wekyb3d8bbwe	
Microsoft.DesktopAppInstaller	Personal	1.0.10332.0			11/13/17 4:21:50 am	Microsoft.DesktopAppInstaller_8wekyb3d8bbwe	
Microsoft.Getstarted	Personal	5.12.2691.0			11/13/17 4:21:50 am	Microsoft.Getstarted_8wekyb3d8bbwe	
Microsoft.MSPaint	Personal	3.1710.30027.0			11/13/17 4:21:50 am	Microsoft.MSPaint_8wekyb3d8bbwe	
Microsoft.Messaging	Personal	3.34.25004.0			11/13/17 4:21:50 am	Microsoft.Messaging_8wekyb3d8bbwe	
Microsoft.Microsoft3DViewer	Personal	2.1710.12012.0			11/13/17 4:21:50 am	Microsoft.Microsoft3DViewer_8wekyb3d8bbwe	
Microsoft.MicrosoftOfficeHub	Personal	17.8809.7600.0			11/13/17 4:21:50 am	Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe	

- Compare el inventario de aplicaciones con la directiva “Acceso a aplicaciones”. Si el dispositivo tiene aplicaciones instaladas que están en la lista de aplicaciones bloqueadas, puede eliminarlas de los dispositivos.

Problemas de instalación y desinstalación de aplicaciones causados por un código de producto incorrecto

Si una aplicación Win32 se configura con un código de producto incorrecto, al principio la aplicación se instala, pero Microsoft no devuelve el estado de la aplicación a Citrix Endpoint Management. Como resultado de ello:

- La directiva “Desinstalación de aplicaciones” no desinstala la aplicación.
- Citrix Endpoint Management sigue implementando la aplicación porque no tiene confirmación de que está instalada. 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 del producto:

- Quite manualmente la aplicación del dispositivo.
- En la consola de Citrix Endpoint Management, vaya a **Configurar > Aplicaciones** y corrija el código del producto de la aplicación Win32.
- Implemente la aplicación Win32.

Directiva de protección de aplicaciones

October 11, 2021

La directiva “Protección de aplicaciones” indica la configuración de la Protección de aplicaciones de Windows Defender. La configuración incluye si habilitar o no la Protección de aplicaciones y controla el comportamiento del portapapeles.

La Protección de aplicaciones de Windows Defender protege su entorno de los sitios que su organización no ha definido como sitios de confianza. Cuando los usuarios visitan sitios que no figuran en su límite de red aislada, 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 un reinicio del dispositivo para instalar la Protección de aplicaciones de Windows Defender.
- Explorador Microsoft Edge

Parámetros de tabletas y escritorios Windows

The screenshot displays the 'Application Guard policy' configuration page in the Citrix Endpoint Management console. The left sidebar shows the navigation menu with 'Device Policies' selected. Under '1 Policy Info', 'Application Guard policy' is highlighted. The main content area shows the policy details and configuration options.

Application Guard policy

This policy lets you enable Windows Defender Application Guard and configure clipboard controls. Use this policy to protect your environment from sites not trusted by Microsoft Edge. When users visit untrusted sites, the sites open in a Hyper-V virtual browsing session. Enterprise cloud resources define trusted sites. This policy is available to devices running Windows 10 Enterprise (64-bit) version 1709 or later. To install Windows Defender Application Guard, the device must restart.

Application guard ☐ [?](#)

Clipboard behavior No restriction [?](#)

Block external content on enterprise sites ☐ [?](#)

Retain user-generated browser data ☐ [?](#)

Deployment Rules

[Back](#) [Next >](#)

- **Protección de aplicaciones:** Habilita la Protección de aplicaciones. Está **desactivado** de forma predeterminada.
 - **Recursos de nube empresarial:** Una lista de dominios empresariales en la nube, separados por comas.

- **Comportamiento del portapapeles:** Controla en qué direcciones se puede copiar y pegar contenido. Opciones disponibles:
 - **No configurado**
 - **Permitir copiar y pegar contenido solo del explorador web al PC:** Permite a los usuarios copiar y pegar contenido solo desde el explorador web al PC.
 - **Permitir copiar y pegar contenido solo del PC al explorador web:** Permite a los usuarios copiar y pegar contenido solo desde el PC al explorador web.
 - **Permitir copiar y pegar entre el PC y el explorador web:** Permite a los usuarios copiar y pegar contenido libremente entre su PC y el explorador web.
 - **Bloquear operaciones de copiar y pegar entre el PC y el explorador web:** No permite a los usuarios copiar ni pegar contenido entre su PC y el explorador web.
- **Contenido del portapapeles:** Controla el contenido que pueden copiar y pegar los usuarios. Opciones disponibles:
 - **No hay 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 texto e imágenes.
- **Bloquear contenido externo en sitios de la empresa:** Si está **activado**, la Protección de aplicaciones de Windows Defender impide que el contenido de sitios no aprobados se cargue en sitios de la empresa. Está **desactivado** de forma predeterminada.
- **Retener datos del explorador generados por el usuario:** Si está **activado**, permite guardar los datos del usuario creados durante una sesión de navegación virtual de la Protección de aplicaciones. Estos datos incluyen elementos como contraseñas, favoritos y cookies. Está **desactivado** de forma predeterminada.

Directiva de bloqueo de aplicaciones

November 29, 2023

La directiva “Bloqueo de aplicaciones” define una lista de aplicaciones:

- Cuya ejecución se permite en un dispositivo.
- Cuya ejecución se bloquea en un dispositivo.

El funcionamiento preciso de la directiva depende de la plataforma admitida. Por ejemplo, no se pueden bloquear múltiples aplicaciones en un dispositivo iOS.

Además, en dispositivos iOS, solo se puede seleccionar una aplicación iOS en cada directiva. Los usuarios solo pueden usar su dispositivo para ejecutar una aplicación. Por tanto, no pueden realizar ninguna otra actividad en el dispositivo, excepto las opciones que usted permita específicamente cuando aplique la directiva Bloqueo de aplicaciones.

Además, los dispositivos iOS deben estar supervisados para poder enviarles las directivas de bloqueo de aplicaciones.

Aunque la directiva funcione en la mayoría de dispositivos Android L y M, el bloqueo de aplicaciones no funciona en dispositivos Android N ni versiones posteriores. Esto se debe a que Google ha dejado de respaldar la API necesaria.

En tabletas y escritorios Windows administrados, puede crear una directiva Bloqueo de aplicaciones que defina la lista de aplicaciones en las listas de aplicaciones permitidas y bloqueadas. Puede permitir o bloquear ejecutables, instaladores MSI, aplicaciones de almacén, DLL y scripts.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

App lock	
1 Policy Info	App lock This policy lets you define allowed or blocked apps on a managed device. For Windows Desktop and Tablets: You can allow or block executables, MSI installers, store apps, DLLs, and scripts. First, you configure rules in the Local Security Policy App on the Windows Desktop and export the XML configuration file. Then, use this policy to upload the XML file to Endpoint Management.
2 Platforms Clear All	<div>App bundle ID * Make a selection</div> <div>Options<div><div>Disable touch screen</div><div>ON</div><div>IOS 6.0+</div></div><div><div>Disable device rotation sensing</div><div>OFF</div><div>IOS 6.0+</div></div><div><div>Disable volume buttons</div><div>OFF</div><div>IOS 6.0+</div></div><div><div>Disable ringer switch</div><div>OFF</div><div>IOS 6.0+</div></div><div><div>Disable sleep/wake button</div><div>OFF</div><div>IOS 6.0+</div></div><div><div>Disable auto-lock</div><div>OFF</div><div>IOS 6.0+</div></div><div><div>Enable VoiceOver</div><div>OFF</div><div>IOS 6.0+</div></div><div><div>Enable zoom</div><div>OFF</div><div>IOS 6.0+</div></div></div>

- **ID de paquete de la aplicación:** En la lista, haga clic en la aplicación a la que se aplica esta directiva, o bien haga clic en **Agregar nuevo** para agregar una aplicación a la lista. Si hace clic en **Agregar nuevo**, escriba el nombre de la aplicación en el campo que aparece.
- **Opciones:** Todas ellas están **desactivadas** de forma predeterminada, excepto **Inhabilitar pantalla táctil**, que está **activada** de forma predeterminada.
 - Inhabilitar pantalla táctil

- Inhabilitar detección de rotación de dispositivo
- Inhabilitar botones de volumen
- Inhabilitar botón de timbre

Si **Inhabilitar botón de timbre** está **activado**, los tonos dependen de la posición que tenía el modificador cuando se inhabilitó.

- Inhabilitar botón de reposo/activación
- Inhabilitar bloqueo automático
- Inhabilitar VoiceOver
- Habilitar zoom
- Habilitar la inversión de colores
- Habilitar AssistiveTouch
- Habilitar Leer selección
- Habilitar Audio mono
- Habilitar control de voz

- **Opciones habilitadas por el usuario:** De forma predeterminada está **desactivado** para cada opción.

- Permitir ajuste de VoiceOver
- Permitir ajuste de zoom
- Permitir ajuste de inversión de colores
- Permitir ajuste de AssistiveTouch
- Permitir ajuste de control de voz

- **Configuraciones de directivas**

- **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Solo disponible para iOS 6.0 o versiones posteriores.

Configurar un iPad como un quiosco

Puede utilizar la directiva de bloqueo de aplicaciones para utilizar un iPad supervisado como quiosco. Apple se refiere a esta funcionalidad como modo de aplicación única. Para obtener más información sobre esta función, consulte la [documentación de Apple](#). Asegúrese de implementar la aplicación que quiere 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, opcionalmente, una **Descripción**.
4. Seleccione solo la plataforma **iOS**.
5. Para **ID de paquete de apps**, seleccione la aplicación que quiera ejecutar en el iPad.
6. Configure las opciones que quiera, como se describió anteriormente, y guarde la directiva.
7. Agregue la directiva al mismo grupo de entrega que su iPad e implemente la directiva.

Parámetros de Android (AD heredado)

Nota:

No puede bloquear la aplicación Ajustes de Android mediante la directiva Bloqueo de aplicaciones.

App lock

This policy lets you define allowed or blocked apps on a managed device. For Windows Desktop and Tablets: You can allow or block executables, MSI installers, store apps, DLLs, and scripts. First, you configure rules in the Local Security Policy App on the Windows Desktop and export the XML configuration file. Then, use this policy to upload the XML file to Endpoint Management.

App lock parameters

Lock message:

Unlock password:

Prevent uninstall: ☐ OFF

Lock screen: **Browse**

Enforce: ☒ Block list ☐ Allow list

Apps

App name *	
	Add

• Parámetros de la directiva Bloqueo de aplicaciones

- **Mensaje de bloqueo:** Escriba el mensaje que verán los usuarios cuando intenten abrir una aplicación bloqueada.
- **Contraseña de desbloqueo:** Escriba la contraseña para desbloquear la aplicación.
- **Impedir desinstalación:** Seleccione si permitir a los usuarios desinstalar aplicaciones. El valor predeterminado es **Desactivado**.
- **Pantalla de bloqueo:** Seleccione la imagen que aparecerá en la pantalla de bloqueo del dispositivo. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.
- **Aplicar:** Haga clic en **Lista de bloqueados** para crear una lista de aplicaciones que no pueden ejecutarse en los dispositivos, o bien 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 lleve a cabo lo siguiente:

- **Nombre de la aplicación:** En la lista, haga clic en el nombre de la aplicación que se va a agregar a la lista de aplicaciones permitidas o a la lista de aplicaciones prohibidas. También puede hacer clic en **Agregar nuevo** para agregar una aplicación a la lista de aplicaciones disponibles.
- Si hace clic en **Agregar nuevo**, escriba el nombre de la aplicación en el campo que aparece.
- Haga clic en **Guardar** o **Cancelar**.
- Repita estos pasos para cada aplicación que quiera agregar a las listas de aplicaciones permitidas o prohibidas.

Parámetros de tabletas y escritorios Windows

App lock	App lock This policy lets you define allowed or blocked apps on a managed device. For Windows Desktop and Tablets: You can allow or block executables, MSI installers, store apps, DLLs, and scripts. First, you configure rules in the Local Security Policy App on the Windows Desktop and export the XML configuration file. Then, use this policy to upload the XML file to Endpoint Management.
1 Policy Info	
2 Platforms Clear All	AppLocker policy file <input type="text"/> Browse ?
<input checked="" type="checkbox"/> iOS	
<input checked="" type="checkbox"/> Android (legacy DA)	► Deployment Rules
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	

Requisitos previos para bloquear aplicaciones

- En Windows, configure las reglas en el editor de la directiva de seguridad local en un escritorio con Windows 10 o Windows 11.
- Exporte el archivo XML de la directiva. Citrix recomienda que cree 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 Bloqueo de aplicaciones. Para obtener más información sobre la creación de reglas, consulte este artículo de Microsoft: <https://docs.microsoft.com/en-us/windows/security/threat-protection/applocker/applocker-overview>

Para configurar y exportar el archivo XML de la directiva desde Windows

Importante:

Cuando configure el archivo XML de la directiva desde el editor de directivas de Windows, use el modo solo auditoría.

1. En el equipo Windows, inicie el editor de la **directiva de seguridad local**. Haga clic en **Inicio**, escriba **directiva de seguridad local** y luego 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, 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 el valor predeterminado.
5. Haga clic con el botón secundario en **AppLocker**, haga clic en **Exportar directiva** y guarde el archivo XML.

Nota:

Puede crear **reglas ejecutables**, **reglas de Windows Installer**, **reglas de script** y **reglas de aplicaciones empaquetadas**. Para hacerlo, haga clic con el botón secundario en la carpeta y haga clic en **Crear nueva regla**.

Para importar el archivo XML de la directiva en Citrix Endpoint Management

Cree una directiva Bloqueo de aplicaciones. Haga clic en **Examinar**, situado en el lado opuesto del parámetro del **archivo de la directiva Bloqueo de aplicaciones** y vaya al archivo XML.

Para dejar de aplicar una directiva de bloqueo de aplicaciones

Puede dejar de aplicar una directiva Bloqueo de aplicaciones después de implementarla en Citrix Endpoint Management. Para ello, debe crear un archivo XML vacío. A continuación, cree otra directiva de bloqueo de aplicaciones, cargue el archivo e impleméntela. Los dispositivos que tienen un bloqueo de aplicaciones habilitado no se ven afectados. Los dispositivos que reciben la directiva por primera vez no tienen implementada la directiva de bloqueo de aplicaciones.

Directiva de notificaciones de aplicaciones

December 6, 2021

La directiva de notificaciones de aplicaciones permite controlar cómo reciben los usuarios de iOS las notificaciones provenientes de las aplicaciones especificadas. Esta directiva solo está disponible para dispositivos supervisados con iOS 9.3 o una versión posterior.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Identificador de paquete de apps:** Especifique la aplicación donde quiere administrar los parámetros de notificación:
 - Seleccione el ID del paquete de aplicación. Las opciones están disponibles solo después de habilitar la directiva **Inventario de aplicaciones**, que recopila un inventario de aplicaciones en dispositivos administrados.
 - Seleccione **Agregar** y, a continuación, escriba el ID del paquete de aplicación. Para encontrar un ID de paquete de aplicación, consulte [Buscar el ID de paquete de una aplicación en el App Store](#).
- **Permitir notificaciones:** Debe **activar** esta opción para permitir las notificaciones.
- **Mostrar en el centro de notificaciones:** Debe **activar** esta opción para mostrar notificaciones en el Centro de notificaciones de los dispositivos de usuario.
- **Globos en los iconos:** Debe **activar** esta opción para que aparezca un globo en el icono de la aplicación con las notificaciones.
- **Sonidos:** Debe **activar** esta opción para incluir sonidos en las notificaciones.
- **Ver en la pantalla bloqueada:** Debe **activar** esta opción para mostrar notificaciones en la pantalla de bloqueo de los dispositivos de usuario.
- **Mostrar en CarPlay:** **Actívela** para mostrar notificaciones en Apple CarPlay. Se aplica a iOS 12 y versiones posteriores. De forma predeterminada, está **activado**.
- **Habilitar alerta crítica:** **Actívela** para que una aplicación pueda marcar una notificación como crítica que ignore los ajustes de No molestar y de tono. Se aplica a iOS 12 y versiones posteriores. Está **desactivado** de forma predeterminada.
- **Estilo de alerta en desbloqueo:** Seleccione **Ninguno**, **Pancarta** o **Alertas** para configurar la apariencia de las alertas mientras el dispositivo está desbloqueado.
- **Vista previa:** Seleccione el modo en que los dispositivos muestran las vistas previas de las notificaciones de la aplicación. Se aplica a iOS 14 y versiones posteriores.
 - **Siempre:** Para mostrar vistas previas de notificaciones cuando el dispositivo esté bloqueado o desbloqueado.
 - **Al desbloquearse:** Para mostrar vistas previas de notificaciones solo cuando el dispositivo está desbloqueado.

- **Nunca:** Para desactivar las vistas previas de notificaciones en el dispositivo.
- **Agrupación:** Seleccione el modo en que los dispositivos agrupan notificaciones en la aplicación. Se aplica a dispositivos con iOS 12 y versiones posteriores.
 - **Automático:** Para agrupar notificaciones en grupos especificados por la aplicación.
 - **Por aplicación:** Para agrupar notificaciones de la aplicación en un solo grupo.
 - **Desactivado:** Para desactivar la agrupación de notificaciones de la aplicación. Los dispositivos muestran todas las notificaciones, una detrás de otra.
- **Configuraciones de directivas**
 - **Quitar directiva:** Seleccione un método para programar la eliminación de directivas. Las opciones incluyen lo siguiente:
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Se aplica a iOS 6.0 y versiones posteriores.
 - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Se aplica a iOS 9.3 y versiones posteriores.

Directiva de desinstalación de aplicaciones

November 29, 2023

La directiva de desinstalación de aplicaciones permite eliminar aplicaciones de los dispositivos de usuario. Puede quitar una aplicación si ya no quiere admitirla o si quiere reemplazarla por una aplicación similar de otro proveedor.

Cuando esta directiva se implementa en los dispositivos de los usuarios, los usuarios reciben un mensaje para desinstalar la aplicación y, a continuación, la aplicación se quita.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS y macOS

App uninstall

This policy lets you specify which apps to uninstall. You can perform silent removal only on Samsung Knox devices. If you don't find the app in the list, use the package name.

Managed app bundle ID *

Add new

com.skype.skype

► Deployment Rules

Back Next > ?

- **ID de paquete de la aplicación administrada:** En la lista, selecciona una aplicación administrada existente o haga clic en **Agregar nuevo**. Si no hay aplicaciones configuradas para esta plataforma, la lista está vacía y debe agregar una nueva aplicación administrada. Al seleccionar **Agregar nuevo**, aparece un campo en el que puede escribir el nombre de una aplicación administrada. Disponible para iOS 5.0 y versiones posteriores y macOS 11.0 y versiones posteriores.

Parámetros de Android (AD heredado), Android Enterprise y escritorios y tabletas Windows

- **Aplicaciones que desinstalar:** Haga clic en **Agregar** y lleve a cabo lo siguiente para cada aplicación que quiera agregar:
 - **Nombre de la aplicación:** En la lista, haga clic en una aplicación existente, o bien haga clic en **Agregar nuevo** para introducir un nuevo nombre de aplicación. Si no hay ninguna aplicación configurada para esta plataforma, la lista está vacía y se deben agregar aplicaciones nuevas.
 - Haga clic en **Agregar** para agregar la aplicación, o bien haga clic en **Cancelar** para no agregarla.

Para las aplicaciones Android Enterprise, habilite también la Directiva de inventario de aplicaciones. Consulte [Directiva de inventario de aplicaciones](#).

Desinstalación automática de una aplicación empresarial después de instalarse la aplicación correspondiente de la tienda pública

Puede configurar Citrix Endpoint Management para que quite la versión de empresa de las aplicaciones Citrix cuando se instale la versión correspondiente desde una tienda pública de aplicaciones. Esta función impide que los dispositivos de usuario muestren dos iconos de aplicación idénticos después de instalar la versión de la tienda pública de aplicaciones.

Una condición de implementación para la directiva Desinstalación de aplicaciones hace que Citrix Endpoint Management quite de los dispositivos la versión antigua de una aplicación cuando se instala la versión nueva. Esta función solo está disponible para dispositivos iOS administrados conectados a un servidor Citrix Endpoint Management en modo Enterprise (XME).

Para configurar una regla de implementación mediante como condición el nombre de la aplicación instalada:

- Especifique el **ID de paquete de la aplicación administrada** para la aplicación empresarial.
- Para agregar una regla, haga clic en **Nueva regla** y, a continuación, como se muestra en el ejemplo, elija **Nombre de la aplicación instalada** y **es igual que**. Escriba el ID del paquete de la aplicación de tienda pública de aplicaciones.

En el ejemplo, cuando la aplicación de la tienda pública (com.citrix.mail.ios) se instala en un dispositivo de los grupos de entrega especificados, Citrix Endpoint Management quita la versión de empresa de esa aplicación (com.citrix.mail).

Directiva de restricciones de desinstalación de aplicaciones

July 7, 2022

Puede especificar las aplicaciones que los usuarios pueden o no pueden desinstalar en dispositivos Amazon.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de Amazon

- **Parámetros de restricción a la desinstalación de aplicaciones.** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada regla:
 - **Nombre de la aplicación:** En la lista, haga clic en una aplicación, o bien haga clic en **Agregar nuevo** para agregar una nueva aplicación.

- **Regla:** Seleccione si los usuarios pueden desinstalar la aplicación. El valor predeterminado es permitir la desinstalación.
- Haga clic en **Guardar** o **Cancelar**.

Directiva de dispositivo para actualizar automáticamente aplicaciones administradas

May 4, 2022

Esta directiva controla cómo se actualizan en dispositivos Android Enterprise las aplicaciones administradas instaladas. Se puede restringir la capacidad de los usuarios de permitir la actualización automática de aplicaciones en sus dispositivos. Si permite que los usuarios controlen la actualización automática de aplicaciones en sus dispositivos, ellos establecen las directivas de actualización automática de aplicaciones en la tienda Google Play administrada.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Automatically Update Managed Apps Policy	Automatically Update Managed Apps Policy This policy automatically updates the installed managed apps on the device.	
1 Policy Info	Automatically update managed apps Always	
2 Platforms Clear All	App update priority On	
<input checked="" type="checkbox"/> Android Enterprise	Set priority for updating apps	
3 Assignment	Available apps *	App auto update priority Add
	Deployment Rules	

• Actualizar automáticamente aplicaciones administradas

- **Siempre:** Habilita la actualización automática de aplicaciones. **Siempre** es el valor predeterminado.
 - **Permitir que el usuario configure la directiva:** Permite que el usuario configure la directiva de actualización automática de aplicaciones para el dispositivo en la tienda Google Play administrada.
 - **Nunca:** Inhabilita la actualización automática de aplicaciones.
 - **Solo cuando el dispositivo está conectado a una red Wi-Fi:** Permite la actualización automática de aplicaciones solo cuando el dispositivo está conectado a una red Wi-Fi.
- **Prioridad de actualización de las aplicaciones:** Si está **activada**, puede configurar un nivel de prioridad de actualización para cada aplicación administrada.

- **Establezca prioridad para la actualización de aplicaciones:** Haga clic en **Agregar** para configurar la prioridad de actualización de una aplicación.

Available apps *	App auto update priority
<div>Make a selection</div>	<div><input checked="" type="radio"/> Auto update low priority</div> <div><input type="radio"/> Auto update high priority</div> <div><input type="radio"/> Auto update postponed</div>

Save Cancel

- **Aplicaciones disponibles:** Seleccione una aplicación en el menú para configurar la prioridad de la actualización.
- **Prioridad de actualización automática de las aplicaciones:** Seleccione una prioridad de actualización entre las siguientes:
 - * **Prioridad baja para la actualización automática:** La aplicación se actualiza cuando el dispositivo se está cargando, no se está usando de forma activa y está conectado a una red de uso no medido.
 - * **Prioridad alta para la actualización automática:** 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 aparecido una nueva versión. Pasados los 90 días, la aplicación se actualiza automáticamente con prioridad baja. Después de actualizarse la aplicación, la aplicación no se actualiza automáticamente durante otros 90 días. El usuario puede actualizar la aplicación manualmente en cualquier momento.
- Haga clic en **Guardar** cuando haya terminado. Para modificar una configuración, haga clic en el icono del lápiz. Para eliminar la configuración, haga clic en el icono de la papelera.

Directiva de BitLocker

November 29, 2023

Windows 10 y Windows 11 incluyen una función de cifrado de disco llamada BitLocker, que proporciona protección adicional a archivos y al sistema frente al acceso no autorizado en un dispositivo Windows extraviado o robado. Para obtener una mayor protección, puede usar BitLocker con chips del Módulo de plataforma segura (TPM), versión 1.2 o posterior. Un chip TPM gestiona las operaciones de cifrado. Asimismo, genera, almacena y limita el uso de claves de cifrado.

A partir de Windows 10, compilación 1703, se puede controlar BitLocker mediante las directivas MDM. En Citrix Endpoint Management, puede usar la directiva de BitLocker para configurar los parámetros

disponibles en el asistente de BitLocker en dispositivos con Windows 10 o Windows 11. Por ejemplo, en un dispositivo con BitLocker habilitado, BitLocker pide a los usuarios varias opciones:

- Cómo desbloquear sus dispositivos tras el arranque
- Cómo crear copias de seguridad de su clave de recuperación
- Cómo desbloquear una unidad fija.

Con la directiva de BitLocker, también se puede configurar si:

- Habilitar BitLocker en dispositivos que no tienen chip TPM.
- Mostrar opciones de recuperación en la interfaz de BitLocker.
- Denegar el acceso de escritura en una unidad fija o extraíble cuando BitLocker no está habilitado.
- Guardar de forma segura una clave de recuperación cifrada de BitLocker para que los usuarios accedan en caso de que la olviden o pierdan. Esta clave se puede encontrar en Self Help Portal.

Nota

Una vez que el cifrado de BitLocker se haya iniciado en un dispositivo, no puede cambiar la configuración de BitLocker con la implementación de una directiva de BitLocker actualizada.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Requisitos

- La directiva de BitLocker requiere las ediciones Windows 10 Enterprise o Windows 11 Enterprise.
- Antes de implementar la directiva de BitLocker, prepare el entorno para BitLocker. Para obtener información detallada de Microsoft, incluidos la configuración y los requisitos del sistema para BitLocker, consulte los artículos en [BitLocker](#).

Parámetros de tabletas y escritorios Windows

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

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](#)

ON

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

Customize preboot recovery message and URL

ON

Preboot recovery message and URL

Use default recovery message and URL

Fixed drive recovery settings

Save recovery info to Active Directory Domain Services

ON

Allow certificate based data recovery agent

ON

48-bit recovery password

Allow 48-bit password

256-bit recovery password

Allow 256-bit recovery key

Hide fixed drive recovery options

ON

Save fixed drive 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

Fixed drive settings

Block write access to fixed drives not using BitLocker

ON

Removable drive settings

Block write access to removable drives not using BitLocker

ON

Block write access to other organization device

ON

Other drive settings

Prompt for other disk encryption

ON

Deployment Rules

- **Parámetros de BitLocker**

- **Requerir cifrado del dispositivo:** Determina si solicitar a los usuarios que habiliten el cifrado de BitLocker en escritorios y tabletas Windows. Si tiene el valor **Sí**, los dispositivos muestran un mensaje, una vez finalizada la inscripción, que indica que la empresa requiere el cifrado del dispositivo. Si tiene el valor **No**, el usuario no ve solicitudes y BitLocker usa los parámetros de la directiva. Está **desactivado** de forma predeterminada.

- **Parámetros de cifrado**

- **Configurar métodos de cifrado:** Determina los métodos de cifrado que se utilizarán para los tipos concretos de unidades. Si tiene el valor **No**, el Asistente de BitLocker pregunta al usuario del dispositivo qué método de cifrado se utilizará para el tipo de unidad. El método predeterminado para el cifrado de todas las unidades es XTS-AES de 128 bits. El método predeterminado para el cifrado de las unidades extraíbles es AES-CBC de 128 bits. Si se **activa**, BitLocker utiliza el método de cifrado especificado en la directiva. Asimismo, si se **activa**, aparecen los parámetros adicionales **Unidad del sistema operativo**, **Unidad fija** y **Unidad extraíble**. Elija el método predeterminado para el cifrado de cada tipo de unidad. Está **desactivado** de forma predeterminada.

- **Parámetros de unidad de SO**

- **Requerir autenticación adicional al inicio:** Especifica la autenticación adicional necesaria durante el inicio del dispositivo. También especifica si permitir que BitLocker esté presente en dispositivos que no tienen chip TPM. Si tiene el valor **No**, los dispositivos sin TPM no pueden utilizar el cifrado de BitLocker. Para obtener información acerca de TPM, consulte el artículo de Microsoft [Información general sobre la tecnología del Módulo de plataforma segura](#). Si tiene el valor **Sí**, aparecen los siguientes parámetros adicionales. Está **desactivado** de forma predeterminada.
- **Bloquear BitLocker en dispositivos sin 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 de iniciarlo. La contraseña de desbloqueo contiene un mínimo de ocho caracteres. Está **desactivado** de forma predeterminada.
- **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 este modo, las claves de cifrado se almacenan en el chip TPM. Este modo no requiere que el usuario facilite más datos de desbloqueo. El dispositivo del usuario se desbloquea automáticamente durante el reinicio con la clave de cifrado obtenida del chip TPM. El valor predeterminado es **Permitir TPM**.

- **PIN de inicio de TPM:** Este parámetro es el modo de desbloqueo TPM + PIN. Un PIN puede contener un máximo de 20 dígitos. Use el parámetro **Longitud mínima del PIN** para especificar la longitud mínima del PIN. El usuario configura un PIN durante la configuración de BitLocker y facilita ese PIN durante el inicio del dispositivo.
- **Clave de inicio de TPM:** Este parámetro 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 de iniciarlo.
- **PIN y clave de inicio de TPM:** Este parámetro es el modo de desbloqueo TPM + PIN + clave. Si el desbloqueo se realiza correctamente, el sistema operativo empieza a cargarse. De lo contrario, el dispositivo entra en modo de recuperación.

- **Longitud del PIN**

- **Longitud mínima del PIN:** La longitud mínima que debe tener el PIN para el inicio de TPM. El valor predeterminado es **6**.

- **Parámetros de recuperación de contraseña de BitLocker**

- **Recuperación de seguridad 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 Self Help Portal. 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](#).

- **Parámetros de recuperación de la unidad de SO:** Configura las opciones de recuperación que tienen los usuarios para una unidad de sistema operativo cifrada con BitLocker.

- **Habilitar la recuperación de la unidad de disco del OS:** Si se produce un error en el paso de desbloqueo, BitLocker pide al usuario la clave de recuperación configurada. Este parámetro configura las opciones de recuperación de unidades 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 permitir un agente de recuperación de datos basado en certificados. Agregue un agente de recuperación de datos desde las directivas de clave pública, ubicado en la Consola de administración de directivas de grupo (GPMC) o en el Editor de directivas de grupo local. Para obtener más información acerca de los agentes de recuperación de datos, consulte el artículo de Microsoft [BitLocker Group Policy settings](#). El valor predeterminado es **Desactivado**.

- **Contraseña de recuperación de 48 bits:** Especifica si permitir o exigir que los usuarios usen una contraseña de recuperación. BitLocker genera la contraseña y la guarda en un archivo o una cuenta de Microsoft Cloud. El valor predeterminado es **Permitir contraseña de 48 bits**.
- **Clave de recuperación de 256 bits:** Especifica si permitir o exigir que los usuarios usen una clave de recuperación. Una clave de recuperación es un archivo BEK, almacenado en una unidad USB. El valor predeterminado es **Permitir clave de recuperación de 256 bits**.
- **Ocultar opciones de recuperación de unidad de SO:** Especifica si mostrar u ocultar las opciones de recuperación en la interfaz de BitLocker. Si se **activa**, no aparecen opciones de recuperación en la interfaz de BitLocker. En ese caso, registre los dispositivos en Active Directory, guarde las opciones de recuperación en Active Directory y **active** la opción **Guardar información de recuperación en AD DS**. El valor predeterminado es **Desactivado**.
- **Guardar información de recuperación en Active Directory Domain Services:** Especifica si guardar las opciones de recuperación en Active Directory Domain Services. El valor predeterminado es **Desactivado**.
- **Información de recuperación guardada en Active Directory Domain Services:** Especifica si almacenar la contraseña de recuperación de BitLocker o el paquete de claves y la contraseña de recuperación en Active Directory Domain Services. Si almacena el paquete de claves, se admite la recuperación de datos desde una unidad que se haya dañado de físicamente. El valor predeterminado es **Contraseña de recuperación de copia de seguridad**.
- **Habilitar BitLocker después de almacenar información de recuperación en Active Directory Domain Services:** Especifica si impedir que los usuarios habiliten BitLocker a menos que el dispositivo esté conectado por dominio y la copia de seguridad de la información de recuperación de BitLocker en Active Directory se haya realizado correctamente. Si se **activa**, el dispositivo debe estar unido a un dominio antes de iniciar BitLocker. El valor predeterminado es **Desactivado**.
- **Mensaje y URL de recuperación de preinicio:** Especifica si BitLocker muestra un mensaje y una dirección URL personalizados en la pantalla de recuperación. Si se **activa**, aparecen los siguientes parámetros 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 URL y mensaje de recuperación de Citrix Endpoint Management**. Si se **desactiva**, aparece la URL y el mensaje de recuperación predeterminados. El valor predeterminado es **Desactivado**.
- **Parámetros de recuperación de unidades fijas:** Configura las opciones de recuperación que tienen los usuarios para unidades fijas cifradas con BitLocker. BitLocker no muestra mensajes

a los usuarios acerca del cifrado de la unidad fija. Para desbloquear una unidad durante el inicio, un usuario suministra una contraseña o una tarjeta inteligente. Los parámetros de desbloqueo de inicio (no incluidos en esta directiva), aparecen en la interfaz de BitLocker cuando un usuario habilita el cifrado de BitLocker en una unidad fija. Para obtener información sobre los parámetros relacionados, consulte la opción **Configurar la recuperación de la unidad del SO**, ya mencionada en esta lista. El valor predeterminado es **Desactivado**.

- **Parámetros de unidad fija**

- **Bloquear acceso de escritura en unidades fijas que no usen BitLocker:** Si se **activa**, los usuarios solo pueden escribir en las unidades fijas cuando están cifradas con BitLocker. El valor predeterminado es **Desactivado**.

- **Parámetros de unidad extraíble**

- **Bloquear acceso de escritura en unidades extraíbles que no usen BitLocker:** Si se **activa**, los usuarios solo pueden escribir en las unidades extraíbles cuando están cifradas con BitLocker. Configure este parámetro de acuerdo con el acceso de escritura que permite la organización en otras unidades extraíbles de la organización. El valor predeterminado es **Desactivado**.

- **Bloquear acceso de escritura en otros dispositivos de la organización:** Si se **activa**, los usuarios no pueden escribir en otros dispositivos de su organización, como una unidad de red.

- **Otros parámetros de unidad**

- **Pedir otro cifrado de disco:** Permite inhabilitar el diálogo de advertencia para otro cifrado de disco en los dispositivos. Está **desactivado** de forma predeterminada.

Directiva de dispositivos Bluetooth

December 6, 2021

Puede configurar una directiva de Bluetooth en dispositivos iOS supervisados para habilitar o inhabilitar Bluetooth.

Esta configuración requiere el derecho de acceso a la información de red, no admite la inscripción de usuarios y está disponible a partir de iOS 11.3.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

The screenshot shows the Citrix Endpoint Management console interface. At the top, there is a navigation bar with tabs: Device Policies, Apps, Media, Actions, Content Collaboration, Enrollment Profiles, and Delivery Groups. Below this, the 'Bluetooth' policy is selected. The left sidebar shows a list of policy steps: 1 Policy Info, 2 Platforms (with a 'Clear All' link), 3 Assignment, and 4 Deployment Rules. The 'iOS' platform is selected under step 2. The main content area displays the 'Bluetooth' policy details, including a description: 'This policy lets you enable or disable a personal hotspot on a device. This setting requires the Network Information access right, doesn't support User Enrollment, supervised only and is available in iOS 11.3 and later.' Below the description, there is a toggle switch for 'Disable bluetooth' which is currently turned off, and a version requirement 'iOS 11.0+'. At the bottom right of the console, there are 'Back' and 'Next >' buttons, along with a help icon.

- **Inhabilitar Bluetooth:** Le permite inhabilitar o habilitar Bluetooth en el dispositivo supervisado.

Directiva de calendario (CalDAV)

November 29, 2023

En Citrix Endpoint Management, puede agregar una directiva para agregar una cuenta de calendario (CalDAV) a los dispositivos iOS o macOS de los usuarios. De esta manera, los usuarios podrán sincronizar los datos de eventos programados con cualquier servidor que admita CalDAV.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Descripción de la cuenta:** Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Nombre de host:** Escriba la dirección del servidor CalDAV. Este campo es obligatorio.
- **Puerto:** Especifique el puerto por el que conectarse al servidor CalDAV. Este campo es obligatorio. El valor predeterminado es **8443**.

- **URL principal:** Indique la URL base de acceso al calendario del usuario.
- **Nombre de usuario:** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Escriba una contraseña opcional de usuario.
- **Usar SSL:** Seleccione si utilizar una conexión de Secure Sockets Layer (SSL) para el servidor CalDAV. El valor predeterminado es **Activado**.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Solo disponible para iOS 6.0 o versiones posteriores.

Parámetros de macOS

- **Descripción de la cuenta:** Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Nombre de host:** Escriba la dirección del servidor CalDAV. Este campo es obligatorio.
- **Puerto:** Especifique el puerto por el que conectarse al servidor CalDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **URL principal:** Indique la URL base de acceso al calendario del usuario.
- **Nombre de usuario:** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Escriba una contraseña opcional de usuario.
- **Usar SSL:** Seleccione si utilizar una conexión de Secure Sockets Layer (SSL) para el servidor CalDAV. El valor predeterminado es **Activado**.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar 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**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Directiva de red de telefonía móvil

November 29, 2023

Esta directiva permite configurar parámetros de redes de telefonía móvil en un dispositivo iOS.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

Puede usar macros en campos que no sean cadenas, como **Puerto del servidor proxy**.

Por ejemplo, ahora puede usar la macro `${ device.xyz }` o `${ setting.xyz }`, que se expande en un número entero. También puede usar las macros en un archivo XML de configuración de dispositivos que importe en Citrix Endpoint Management mediante la directiva “Importar perfil de iOS y macOS”.

• Asociar APN

- **Nombre:** Escriba un nombre para esta configuración.
- **Tipo de autenticación:** En la lista, haga clic en el Protocolo de autenticación por desafío mutuo (**CHAP**) o el Protocolo de autenticación por contraseña (**PAP**). El valor predeterminado es **PAP**.
- En **Nombre de usuario** y **Contraseña**, introduzca el nombre de usuario y la contraseña para la autenticación.

• APN

- **Nombre:** Escriba un nombre para la configuración del nombre de punto de acceso (APN).
- **Tipo de autenticación:** En la lista, haga clic en **CHAP** o **PAP**. El valor predeterminado es **PAP**.
- En **Nombre de usuario** y **Contraseña**, introduzca el nombre de usuario y la contraseña para la autenticación.

- **Servidor proxy:** Escriba la dirección de red del servidor proxy.
- **Puerto del servidor proxy:** Escriba el puerto del servidor proxy.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.

Directiva de programación de conexiones

November 29, 2023

Importante:

Citrix recomienda usar Firebase Cloud Messaging (FCM) para controlar las conexiones desde dispositivos Android y Android Enterprise a Citrix Endpoint Management. Para obtener más información sobre el uso de FCM, consulte [Firebase Cloud Messaging](#).

Si opta por no usar FCM, puede crear directivas de programación de conexiones para controlar cómo y cuándo se conectan los dispositivos de usuario a Citrix Endpoint Management. Si opta por usar FCM, debe crear también 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](#).

Parámetros de Android y Android Enterprise

- **Requerir la conexión de los dispositivos:** Haga clic en la opción que quiera establecer para esta programación.
 - **Nunca:** Se conecta manualmente. Los usuarios deben iniciar la conexión desde la instancia de Citrix Endpoint Management presente en sus dispositivos. Citrix no recomienda esta opción para las implementaciones de producción, ya que le impide implementar directivas de seguridad en los dispositivos; por lo tanto, los usuarios no recibirán nunca aplicaciones ni directivas nuevas. La opción **Nunca** está habilitada de forma predeterminada.

- **Cada:** Se conecta en el intervalo predeterminado. Cuando esta opción está activa y usted envía una directiva de seguridad, como un bloqueo o un borrado, Citrix Endpoint Management procesa la acción en el dispositivo la próxima vez que el dispositivo se conecta. Si se selecciona esta opción, aparece el campo **Conectar cada N minutos**. En él, debe introducir la cantidad de minutos tras los que el dispositivo debe volver a conectarse. El valor predeterminado y mínimo es **120**.
- **Definir programación:** La instancia de Citrix Endpoint Management presente en el dispositivo del usuario intenta volver a conectarse al servidor Citrix Endpoint Management después de perder la conexión de red. Citrix Endpoint Management supervisa la conexión transmitiendo paquetes de control a intervalos periódicos durante la franja de tiempo que usted indique. Consulte “Definir un período de tiempo de conexión” para configurar un período de tiempo de conexión.
 - * **Requerir una conexión dentro de cada uno de estos intervalos:** Los dispositivos de usuario deben conectarse al menos una vez durante uno de los períodos de tiempo definidos.
 - * **Usar la hora local del dispositivo en lugar de UTC:** Sincroniza 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

Cuando se habilitan las siguientes opciones, aparece una escala de tiempo en la que puede definir los períodos de tiempo pertinentes. Es posible habilitar una de las dos opciones o ambas: mantener una conexión permanente durante horas específicas o requerir una conexión dentro de períodos de tiempo determinados. Cada cuadrado de la escala de tiempo representa 1 hora. Si quiere una conexión entre las 8:00 y las 9:00 todos los días de la semana, haga clic en el cuadrado ubicado entre 8 a. m. y 9 a. m. todos los días de la semana.

Por ejemplo, las dos escalas de tiempo en la siguiente imagen requieren:

- Una conexión permanente entre las 8:00 y las 10:00 todos los días laborables de la semana
- Una conexión permanente entre la 1:00 del sábado y las 2:00 del domingo
- Al menos una conexión cada día laborable entre las 5:00 y las 8:00 o entre las 10:00 y las 12:00

☒ Define schedule

Maintain permanent connection during these hours ☒

	1 AM	2 AM	3 AM	4 AM	5 AM	6 AM	7 AM	8 AM	9 AM	10 AM	11 AM	12 PM	1 PM	2 PM	3 PM	4 PM	5 PM	6 PM	7 PM	8 PM	9 PM	10 PM	11 PM	12 AM
Mon																								
Tue																								
Wed																								
Thu																								
Fri																								
Sat																								
Sun																								

Require a connection within each of these ranges ☒

	1 AM	2 AM	3 AM	4 AM	5 AM	6 AM	7 AM	8 AM	9 AM	10 AM	11 AM	12 PM	1 PM	2 PM	3 PM	4 PM	5 PM	6 PM	7 PM	8 PM	9 PM	10 PM	11 PM	12 AM
Mon																								
Tue																								
Wed																								
Thu																								
Fri																								
Sat																								
Sun																								

Use local device time rather than UTC ☐

Directiva de contactos (CardDAV)

November 29, 2023

En Citrix Endpoint Management, puede agregar una directiva para agregar una cuenta de contactos iOS (CardDAV) a los dispositivos iOS o macOS de los usuarios. De esta manera, los usuarios podrán sincronizar los datos de contacto con cualquier servidor que admita CardDAV.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Descripción de la cuenta:** Escriba la descripción de la cuenta. Este campo es obligatorio.

- **Nombre de host:** Escriba la dirección del servidor CardDAV. Este campo es obligatorio.
- **Puerto:** Especifique el puerto por el que conectarse al servidor CardDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **URL principal:** Indique la URL base de acceso al calendario del usuario.
- **Nombre de usuario:** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Escriba una contraseña opcional de usuario.
- **Usar SSL:** Seleccione si utilizar una conexión de Secure Sockets Layer (SSL) para el servidor CardDAV. El valor predeterminado es **Activado**.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.

Parámetros de macOS

- **Descripción de la cuenta:** Escriba la descripción de la cuenta. Este campo es obligatorio.
- **Nombre de host:** Escriba la dirección del servidor CardDAV. Este campo es obligatorio.
- **Puerto:** Especifique el puerto por el que conectarse al servidor CardDAV. Este campo es obligatorio. El valor predeterminado es **8443**.
- **URL principal:** Indique la URL base de acceso al calendario del usuario.
- **Nombre de usuario:** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña:** Escriba una contraseña opcional de usuario.
- **Usar SSL:** Seleccione si utilizar una conexión de Secure Sockets Layer (SSL) para el servidor CardDAV. El valor predeterminado es **Activado**.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.

- ★ **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar 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**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Directiva de XML personalizado

November 29, 2023

En Citrix Endpoint Management, puede crear directivas de XML personalizado para adaptar las siguientes funciones en dispositivos Windows compatibles:

- El aprovisionamiento, que incluye la configuración del dispositivo y la habilitación o inhabilitación de las funciones.
- La configuración de dispositivos, que incluye la capacidad para permitir a los usuarios cambiar la configuración y los parámetros de sus dispositivos.
- Las actualizaciones de software, que incluyen la capacidad para proporcionar software nuevo o correcciones de errores para cargarlos en el dispositivo, incluidas las aplicaciones y el software del sistema.
- Los errores de administración, que incluye la recepción de informes de error y de estado del dispositivo.

Nota:

Al crear contenido XML, use el símbolo % con precaución. El símbolo % es un carácter XML reservado que solo se utiliza para escapar caracteres XML especiales. Para usar % en un nombre, codifíquelo como %25.

Para dispositivos Windows: Puede crear su propia configuración XML personalizada mediante la API de Open Mobile Alliance Device Management (OMA DM) en Windows. La creación de contenido XML personalizado con la API de OMA DM no se cubre en esta sección. Para obtener más información sobre el uso de la API de OMA DM, consulte [OMA DM protocol support](#) en el sitio Microsoft Developer Network.

Para dispositivos Android Enterprise: Puede crear su propia configuración XML personalizada mediante el sistema de administración de MX (MXMS). La creación de contenido XML personalizado con la API de MXMS no se describe en este artículo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de escritorios y tabletas Windows

Contenido XML: Escriba, o copie y pegue, el código XML personalizado que se va a agregar a la directiva.

Tras hacer clic en **Siguiente**, Citrix Endpoint Management comprueba la sintaxis del contenido XML. Los errores de sintaxis aparecerán bajo el cuadro del contenido. Antes de continuar, debe corregir los errores que haya.

Si no hay errores de sintaxis, aparecerá la página de asignación **Directiva XML personalizada**.

Usar Windows AutoPilot para instalar y configurar dispositivos

Windows AutoPilot es un conjunto de tecnologías que se utilizan para instalar y preconfigurar dispositivos nuevos y, así, prepararlos para usarlos productivamente. Puede usar Windows AutoPilot para restablecer, reasignar y recuperar dispositivos. AutoPilot contribuye a eliminar parte de la complejidad que presenta actualmente la implementación de sistema operativo. Con AutoPilot, la tarea se reduce a un conjunto de operaciones y configuraciones simples para una preparación rápida y eficaz de los dispositivos nuevos.

Para obtener una breve descripción general del uso de Windows AutoPilot con Citrix Endpoint Management, consulte este vídeo.

[Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.](#)

Requisitos previos

- Personalización de marca de la empresa configurada en el portal de Azure Active Directory.
- La empresa tiene una suscripción Premium P1 o P2 de Azure Active Directory.
- Configurar Azure Active Directory como 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 de nube que usa Windows AutoPilot.
- Dispositivos con Windows 10 Professional, Enterprise o Education preinstalado (versión 1703 o una posterior) o Windows 11 Professional, Enterprise o Education.
- Dispositivos con acceso a Internet.

Para obtener más información sobre la configuración de requisitos previos, consulte la documentación de Microsoft Windows en AutoPilot: <https://docs.microsoft.com>.

Para configurar la reimplementación automática de Windows en Citrix Endpoint Management para los dispositivos AutoPilot

1. Siga los pasos para agregar una directiva de XML personalizado a la directiva Contenido XML personalizado. Agregue lo siguiente a **Contenido XML**:

```
1 <Add>
2 <CmdID>\_cmdid\_</CmdID>
3 <Item>
4 <Target>
5 <LocURI>./Vendor/MSFT/Policy/Config/CredentialProviders/
   DisableAutomaticReDeploymentCredentials</LocURI>
6 </Target>
7 <Meta>
8 <Format xmlns="syncml:metinf">int</Format>
9 </Meta>
10 <Data>0</Data>
11 </Item>
12 </Add>
13
14 <!--NeedCopy-->
```

2. En la pantalla de bloqueo de Windows, presione las teclas **CTRL + tecla Windows + R**.
3. Inicie sesión con una cuenta de Azure Active Directory.
4. El dispositivo verifica que el usuario tenga derechos para volver a implementar el dispositivo. A continuación, el dispositivo vuelve a implementarse.
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 con Windows 11

Nota:

Los dispositivos con Windows 11 solo admiten el modo quiosco de una sola aplicación.

En el cuadro de texto **Contenido XML**, copie y pegue este script XML y, a continuación, reemplace estas cadenas con sus parámetros:

- `your_username_here`(dos instancias): El nombre de usuario que quiere crear en el dispositivo. Mantenga los mismos parámetros para ambas instancias.
- `your_password_here`: La contraseña del usuario.

- `your_UWP_app_id_here`: AUMID de la aplicación UWP que quiere implementar en el dispositivo.

Script XML:

```

1  <Add>
2      <CmdID>\_cmdid\_</CmdID>
3      <Item>
4          <Target>
5              <LocURI>./Device/Vendor/MSFT/Accounts/Users/
                  your_username_here/Password</LocURI>
6          </Target>
7          <Meta>
8              <Format xmlns="syncml:metinf">chr</Format>
9          </Meta>
10         <Data>your_password_here</Data>
11     </Item>
12 </Add>
13 <Replace>
14     <CmdID>\_cmdid\_</CmdID>
15     <Item>
16         <Target>
17             <LocURI>./Device/Vendor/MSFT/AssignedAccess/Configuration</
                LocURI>
18         </Target>
19         <Meta>
20             <Format xmlns="syncml:metinf">chr</Format>
21         </Meta>
22         <Data><![CDATA[<AssignedAccessConfiguration
23             xmlns="http://schemas.microsoft.com/AssignedAccess/2017/config"
24             xmlns:rs5="http://schemas.microsoft.com/AssignedAccess/201810/
                config">
25             <Profiles>
26                 <Profile Id="{
27 AFF9DA33-AE89-4039-B646-3A5706E92957 }
28 ">
29                 <KioskModeApp AppUserModelId="your_UWP_app_id_here"
                    />
30                 </Profile>
31             </Profiles>
32             <Configs>
33                 <Config>
34                     <Account>your_username_here</Account>
35                     <DefaultProfile Id="{
36 AFF9DA33-AE89-4039-B646-3A5706E92957 }
37 ">
38                     </Config>
39                 </Configs>
40             </AssignedAccessConfiguration>]]></Data>
41     </Item>
42 </Replace>
43 <!--NeedCopy-->

```

Directiva de Defender

November 29, 2023

Windows Defender es una protección contra malware incluida en Windows 10 y Windows 11. En Citrix Endpoint Management, puede usar la directiva Defender para configurar la directiva Microsoft Defender en escritorios y tabletas con Windows 10 o Windows 11.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de tabletas y escritorios Windows

The screenshot shows the 'Defender policy' configuration page in the Citrix Endpoint Management console. The left sidebar has three tabs: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' tab is selected, showing a list of platforms with 'Windows Desktop/Tablet' checked. The main content area displays the 'Defender policy' settings, which are configured for Windows 10 desktop and tablet devices. The settings include:

- Allow scans of archived files: ☐
- Allow cloud protection: ☒
- Allow a full scan of removable drives: ☒
- Allow real-time monitoring: ☒
- Allow scans of network files: ☒
- Allow access to the Windows Defender UI: ☒

Below these settings are three input fields for 'Excluded extensions', 'Excluded paths', and 'Excluded processes', each with a help icon. At the bottom, there is a 'Submit samples for further analysis' section with a 'Send safe samples' button. Navigation buttons 'Back' and 'Next >' are at the bottom right.

- **Permitir el examen de archivos archivados:** Permite o impide que Defender examine archivos ya archivados. Está **desactivado** de forma predeterminada.
- **Permitir la protección de la nube:** Permite o impide que Defender envíe información de Defender a Microsoft sobre la actividad de malware. Está **activado** de forma predeterminada.
- **Permitir un examen completo de las unidades extraíbles:** Permite o impide que Defender examine las unidades extraíbles, como los dispositivos USB. Está **activado** de forma predeterminada.
- **Permitir la supervisión en tiempo real:** Está **activado** de forma predeterminada.

- **Permitir el examen de archivos de red:** Permite o impide que Defender examine archivos de red. Está **activado** de forma predeterminada.
- **Permitir el acceso a la IU de Windows Defender:** Especifica si los usuarios pueden acceder a la interfaz de usuario de Windows Defender. Esta configuración se aplica la próxima vez que se inicie el dispositivo del usuario. Si tiene el valor **No**, los usuarios no recibirán ninguna notificación de Windows Defender. Está **activado** de forma predeterminada.
- **Extensiones excluidas:** Las extensiones a excluir de los exámenes en tiempo real o programados. Para separar las extensiones, use el carácter |. Por ejemplo: `lib\|obj`.
- **Rutas excluidas:** Las rutas a excluir de los exámenes en tiempo real o programados. Para separar las rutas, use el carácter |. Por ejemplo: `C:\Example|C:\Example1`.
- **Procesos excluidos:** Los procesos a excluir de los exámenes en tiempo real o programados. Para separar los procesos, use el carácter |. Por ejemplo: `C:\Example.exe|C:\Example1.exe`.
- **Enviar muestras para un análisis más profundo:** Controla si se envían a Microsoft archivos que pueden requerir un análisis más profundo para determinar si son malintencionados. Opciones: **Preguntar siempre**, **Enviar muestras seguras**, **Nunca enviar**, **Enviar todas las muestras**. El valor predeterminado es **Enviar muestras seguras**.

Directiva de Device Guard

November 29, 2023

Device Guard es una función de seguridad disponible en Windows 10 y Windows 11. Esta función permite seguridad en la virtualización porque usa el hipervisor de Windows para poder ofrecer servicios de seguridad en el dispositivo. La directiva de Device Guard permite habilitar funciones de seguridad, tales como el arranque seguro, el bloqueo UEFI y la virtualización.

Requisitos previos

- Escritorios y tabletas con Windows 10 o Windows 11 y una licencia Enterprise o Education
- Device Guard habilitado en Windows

Para obtener más información sobre Device Guard, consulte <https://docs.microsoft.com/en-us/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](#).

Parámetros de tabletas y escritorios Windows

The screenshot shows the Citrix Endpoint Management console. The top navigation bar includes tabs for Device Policies, Apps, Media, Actions, Content Collaboration, Enrollment Profiles, and Delivery Groups. The left sidebar shows the 'Device Guard' policy selected. The main content area displays the 'Device Guard' policy configuration for Windows Desktop/Tablet. The policy description states: 'This policy configures virtualization-based security settings on Windows 10 desktops and tablets. The policy applies to devices running Windows 10 Enterprise or Education, version 1709 (RS3) or later.' The configuration options include: 'Enable virtualization-based security' (toggle switch), 'Configure LSA protection' (dropdown menu showing 'Turns off Credential Guard'), and 'Specify platform security level' (dropdown menu showing 'Turns on VBS with Secure Boot'). There is also a 'Deployment Rules' link at the bottom.

- **Habilitar seguridad para virtualización:** Permite inhabilitar o habilitar las funciones de seguridad para la virtualización. La seguridad para la virtualización utiliza el hipervisor de Windows para ofrecer servicios de seguridad.
- **Configurar la protección de LSA:** Le permite configurar Credential Guard. Este parámetro permite a los usuarios activar Credential Guard con la seguridad basada en la virtualización para ayudarles 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 próximo reinicio. Las opciones son **Activa la seguridad VBS con Arranque seguro** y **Activa la seguridad VBS con Arranque seguro y acceso directo a la memoria**. El valor predeterminado es **Activa la seguridad VBS con Arranque seguro**.

Citrix Endpoint Management envía consultas a un dispositivo para determinar si la configuración de seguridad basada en la virtualización coincide con la configuración en el servidor. Si las configuraciones coinciden, Citrix Endpoint Management no implementa esta directiva en el dispositivo. En cambio, si las configuraciones de seguridad no coinciden, Citrix Endpoint Management implementa la directiva.

Directiva de Device Health Attestation

November 29, 2023

En Citrix Endpoint Management, puede requerir que los dispositivos con Windows 10 o Windows 11 informen de su estado. Para ello, deben enviar datos concretos e información del tiempo de ejecución al servicio Health Attestation Service (HAS) para el análisis. El servicio 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 estado para implementar las acciones automáticas que se hayan configurado.

Los datos que se comprueban en el servicio HAS son:

- AIKPresent
- BitLockerStatus
- BootDebuggingEnabled
- BootManagerRevListVersion
- CodeIntegrityEnabled
- CodeIntegrityRevListVersion
- Directiva del programa de implementación de Apple
- ELAMDriverLoaded
- IssuedAt
- KernelDebuggingEnabled
- PCR
- ResetCount
- RestartCount
- SafeModeEnabled
- SBCPHash
- SecureBootEnabled
- TestSigningEnabled
- VSMEnabled
- WinPEEnabled

Para obtener información, consulte la página [Device Health Attestation CSP](#) de Microsoft.

Puede configurar DHA mediante Microsoft Cloud o un servidor DHA Windows local, de la siguiente manera:

- Para configurar DHA mediante Microsoft Cloud, agregue una directiva Device Health Attestation y configúrela como se describe en este artículo.
- Para configurar DHA a través de un servidor DHA Windows local, configure un servidor DHA. A continuación, agregue una directiva Device Health Attestation y configúrela como se describe en este artículo.

Para configurar un servidor DHA, instale el rol de servidor DHA en una máquina con Windows Server 2016 Technical Preview 5 o una versión posterior. Para obtener instrucciones, consulte [Configurar un servidor Device Health Attestation local](#).

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de escritorios y tabletas Windows

Si configura DHA a través de Microsoft Cloud

- **Habilitar Device Health Attestation:** Seleccione si se debe requerir Device Health Attestation. El valor predeterminado es **Desactivado**.

Si configura DHA a través de un servidor DHA Windows local

- **Habilitar Device Health Attestation:** Establezca el parámetro en **Sí**.
- **Configurar Health Attestation Service local:** Establezca el parámetro en **Sí**.
- **Nombre FQDN del servidor DHA local:** Introduzca el nombre de dominio completo del servidor DHA que configuró.
- **Versión de API de DHA local:** Elija la versión del servicio DHA instalado en el servidor DHA.

Directiva de nombre de dispositivo

November 29, 2023

Puede definir nombres para dispositivos iOS y macOS supervisados de forma que pueda reconocerlos fácilmente. Puede usar macros, texto o una combinación de ambos para definir el nombre del dispositivo. Por ejemplo, para establecer el número de serie del dispositivo como nombre, puede utilizar \${device.serialnumber}. Para establecer el nombre del dispositivo como una combinación del nombre de usuario y el dominio, puede utilizar \${user.username}@ejemplo.com. Para obtener más información acerca de las macros, consulte [Macros en Citrix Endpoint Management](#).

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS y macOS

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
Device Name Policy This policy lets you apply a name on a supervised device on iOS and macOS devices. Available in iOS 8 and later.						
1 Policy Info						
2 Platforms						
<input checked="" type="checkbox"/> iOS						
<input checked="" type="checkbox"/> macOS						
3 Assignment						
Device name * <input type="text"/>						
► Deployment Rules						

- **Nombre del dispositivo:** Escriba la macro, una combinación de ellas o una combinación de macros y texto para darle a cada dispositivo un nombre único. Por ejemplo, use \${device.serialnumber} para establecer el número de serie de cada dispositivo como su nombre, o bien utilice \${device.serialnumber} \${user.username} para incluir el ID de Apple del usuario en el nombre del dispositivo.

Directiva de configuración de la educación

November 29, 2023

La directiva de configuración de la educación define:

- Los parámetros de la aplicación Aula de Apple para dispositivos de profesores.
- Los certificados que se utilizan para la autenticación de cliente entre los dispositivos de profesores y estudiantes.

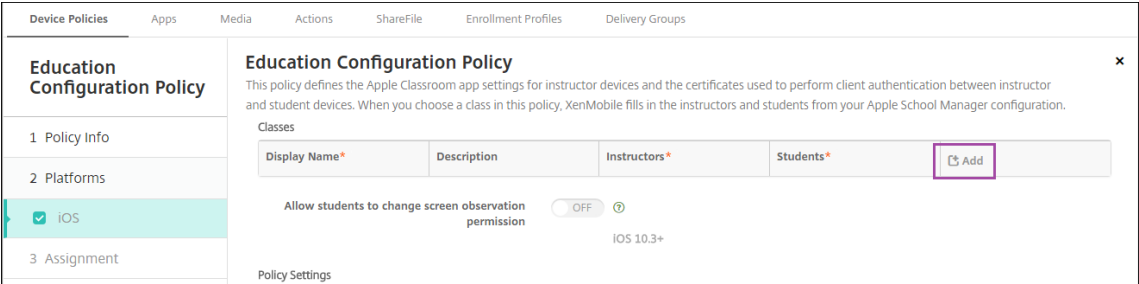
La directiva Configuración de la educación está disponible en dispositivos iOS (iPadOS).

Cuando elige una clase en esta directiva, la consola de Citrix Endpoint Management rellena los profesores y los estudiantes a partir de la configuración de Apple School Manager. Cree una sola directiva si los parámetros de la aplicación Aula de Apple en esa directiva son los mismos para todas las clases.

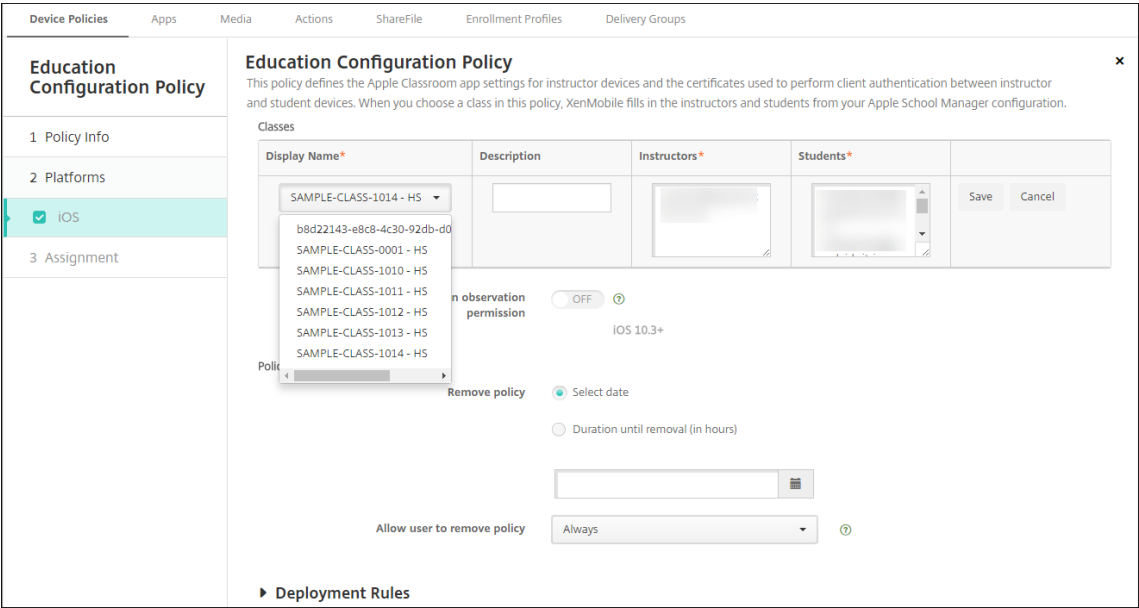
Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

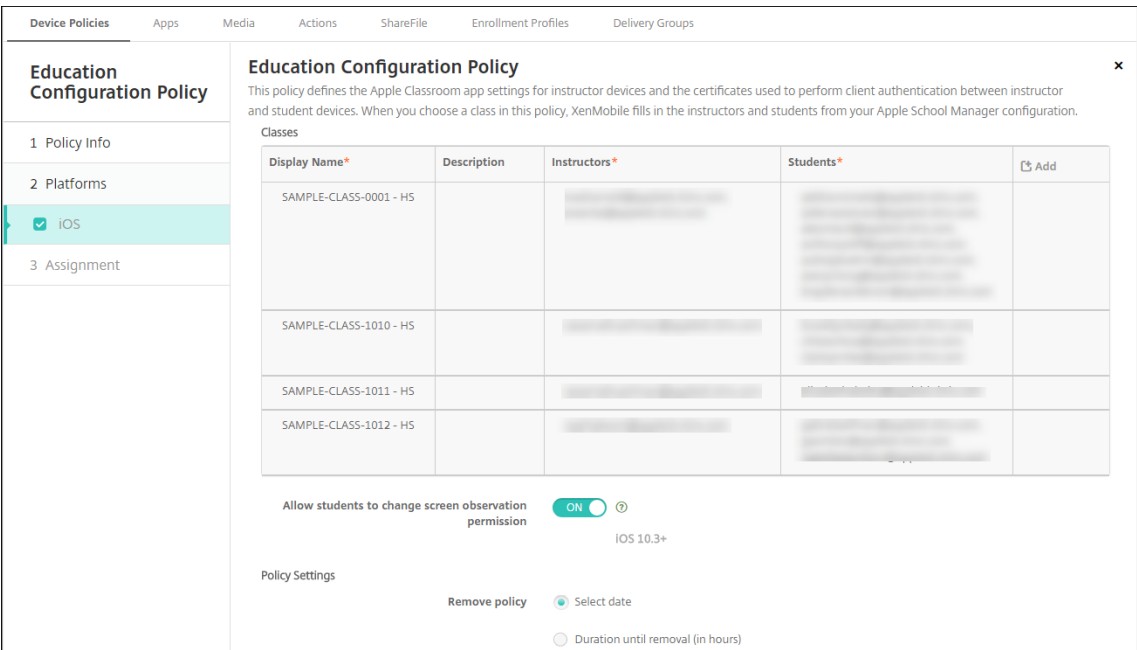
- **Clases:** Para agregar una clase, haga clic en **Agregar**.



Haga clic en la lista **Nombre simplificado**. Aparecerá una lista de las clases, obtenida a partir de su cuenta conectada de Apple School Manager.



Cuando elige una clase desde **Nombre simplificado**, Citrix Endpoint Management rellena los profesores y los estudiantes. Continúe agregando clases.



- **Permitir a los estudiantes cambiar permisos de observación de pantalla:** Si está **activado**, los estudiantes inscritos en clases administradas pueden elegir si permiten que su profesor vea las pantallas de sus dispositivos o no. El valor predeterminado es **Desactivado**.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - ★ **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - ★ **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.

Para modificar la información de clases en la directiva

Puede agregar una descripción a una clase (el “Nombre simplificado” en la aplicación Aula). También puede agregar o quitar profesores y estudiantes. Citrix Endpoint Management no guarda dichos cambios en la cuenta de Apple School Manager. Para obtener más información, consulte “Administrar datos de profesores, estudiantes y clases” en [Integrar en funciones de Apple Educación](#).

Coloque el puntero sobre la columna **Agregar** de la clase que quiere modificar y, a continuación, haga clic en el icono de lápiz.

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery Groups

Education Configuration Policy

1 Policy Info2 Platforms3 Assignment

Education Configuration Policy

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Classes

Display Name*	Description	Instructors*	Students*	Add
SAMPLE-CLASS-0001 - HS				

Para eliminar una clase de la directiva, coloque el cursor sobre la columna **Agregar** de la clase que quiere eliminar y, a continuación, haga clic en el icono de papelera.

Directiva de opciones de Endpoint Management

March 1, 2024

Puede agregar una directiva “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](#).

Parámetros de Android

Endpoint Management Options Policy

This policy lets you configure parameters for connections to Endpoint Management.

Device agent configuration

Traybar notification - hide traybar icon ☐ OFF

Connection time-out(s) *

Keep-alive interval(s) *

Remote support

Prompt the user before allowing remote control ☐ OFF

Before a file transfer

► Deployment Rules

- **Bandeja de notificaciones: ocultar icono:** Seleccione si el icono de la barra de la bandeja será visible o no. El valor predeterminado es **Desactivado**.
- **Tiempos de espera de conexión:** Escriba la cantidad de tiempo en segundos que una conexión puede estar inactiva antes de que se agote el tiempo de espera. El valor predeterminado es de 20 segundos.
- **Intervalos de Keep-Alive:** Escriba la cantidad de tiempo en segundos para mantener una conexión abierta. El valor predeterminado es de 120 segundos.
- **Preguntar al usuario antes de permitir el control remoto:** Seleccione si pedir confirmación al usuario antes de permitir el control por asistencia remota. El valor predeterminado es **Desactivado**.
- **Antes de una transferencia de archivos:** En la lista, haga clic en si se debe avisar al usuario sobre una transferencia de archivo o si se pide permiso al usuario. Los valores disponibles son: **No advertir al usuario**, **Advertir al usuario** y **Pedir permiso al usuario**. El valor predeterminado es **No advertir al usuario**.

Parámetros de Android Enterprise

Endpoint Management Options Policy

This policy lets you configure parameters for connections to Endpoint Management.

Device agent configuration

Traybar notification - hide traybar icon



► Deployment Rules

Compatible a partir de la versión 7 de Android.

Bandeja de notificaciones: ocultar icono: Seleccione si el icono de la barra de la bandeja será visible o no. El valor predeterminado es **Desactivado**.

Nota:

Si quiere habilitar el servicio de VPN para dispositivos con Android Enterprise, puede habilitar la opción **Habilitar VPN permanente** en la **directiva de dispositivos VPN**. Si ya habilitó la opción **Habilitar VPN permanente** en la **directiva de dispositivos de opciones de Endpoint Management** en una versión anterior, asegúrese de habilitarla de nuevo en la **directiva de dispositivos VPN**.

Directiva de desinstalación de Citrix Endpoint Management

November 29, 2023

En Citrix Endpoint Management, puede agregar una directiva de dispositivo para desinstalar Citrix Endpoint Management de dispositivos Android. Cuando se implementa, esta directiva elimina Citrix Endpoint Management de todos los dispositivos que contenga el grupo de implementación.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de Android

- **Desinstalar Citrix Endpoint Management de los dispositivos:** Seleccione si quiere desinstalar Citrix Endpoint Management de todos los dispositivos en los que se implementará esta di-

rectiva. El valor predeterminado es **Desactivado**.

Directiva de Exchange

March 1, 2024

Puede usar la directiva de Exchange ActiveSync para configurar un cliente de correo electrónico en los dispositivos de los usuarios con el fin de que estos, a su vez, puedan acceder al correo electrónico de su empresa alojado en Exchange. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en los siguientes apartados.

Para poder crear esta directiva, debe conocer el nombre de host o la dirección IP del servidor Exchange. Para obtener más información acerca de los parámetros 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](#).

Parámetros de iOS

Exchange

1 Policy Info

2 Platforms Clear All

☒ iOS

☐ macOS

☐ Android HTC

☐ Android Enterprise

☐ Samsung SAFE

☐ Samsung Knox

☐ Windows Phone

☐ Windows Desktop/Tablet

3 Assignment

Exchange

This policy configures Microsoft Exchange ActiveSync so user devices can access corporate email, calendar, contacts, and other synced services hosted on Exchange.

Exchange ActiveSync account name *

Exchange ActiveSync host name *

Use SSL

ON

Domain

User

Email address

Use OAuth

OFF

 iOS 12.0+

Password

Email sync interval

3 days

Identity credential (keystore or PKI credential)

None

- **Nombre de la 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 proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. El valor predeterminado es **Activado**.
- **Dominio:** Escriba el dominio donde reside el servidor Exchange. Puede utilizar la macro de sistema `$user.domainname` en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **Usuario.** Especifique el nombre de usuario de la cuenta de usuario de Exchange. Puede utilizar la macro de sistema `$user.username` en este campo para buscar automáticamente los nombres de los usuarios.
- **Dirección de correo electrónico:** Especifique la dirección completa de correo electrónico. Puede utilizar la macro de sistema `$user.mail` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Usar OAuth:** Si está **activado**, la conexión usa OAuth para la autenticación. El valor predeterminado es **Desactivado**. Esta opción se aplica a iOS 12.0 y versiones posteriores.
- **Contraseña:** Escriba 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, seleccione la frecuencia de sincronización del correo electrónico con el servidor Exchange Server. El valor predeterminado es de **3 días**.
- **Credencial de identidad (PKI o almacén de claves):** En la lista, haga clic en una credencial opcional de identidad si ha configurado un proveedor de identidades para Citrix Endpoint Management. Este campo es necesario solamente si Exchange requiere una autenticación de certificado del cliente. El valor predeterminado es **Ninguno**.
- **Autorizar el movimiento de correo electrónico entre cuentas:** Seleccione si permitir que los usuarios:
 - muevan correos electrónicos de esta cuenta a otra
 - reenvíen correos electrónicos desde otra cuenta
 - respondan desde otra cuenta.

El valor predeterminado es **Desactivado**.

- **Enviar correo electrónico solo desde aplicación de correo electrónico.** Seleccione esta opción para obligar a los usuarios a utilizar la aplicación Correo de iOS para enviar correos electrónicos. El valor predeterminado es **Desactivado**.
- **Impedir que los usuarios sincronicen direcciones recientes:** Seleccione esta opción si quiere evitar 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 firma S/MIME:** Seleccione si esta cuenta admite la firma S/MIME. El valor predeterminado es **Activado**. Si se **activa**, aparecen los siguientes campos.
 - **Credencial de identidad para firma.** Seleccione la credencial de firma que se va a usar.
 - **El usuario puede anular la firma S/MIME:** Si se **activa**, 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 **activa**, los usuarios pueden seleccionar, en la configuración de sus dispositivos, la credencial de firma que se va a usar. El valor predeterminado es **Desactivado**. Esta opción se aplica a iOS 12.0 y versiones posteriores.
- **Habilitar cifrado S/MIME:** Seleccione si esta cuenta admite el cifrado S/MIME. El valor predeterminado es **Desactivado**. Si se **activa**, aparecen los siguientes campos.
 - **Credencial de identidad para cifrado.** Seleccione la credencial de cifrado que se va a usar.
 - **Habilitar cambio de opción S/MIME para cada mensaje:** Cuando se **activa**, los usuarios ven una opción para activar o desactivar el cifrado S/MIME para cada mensaje que escriban. El valor predeterminado es **Desactivado**.
 - **El usuario puede supeditar el cifrado S/MIME:** Si se **activa**, 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 supeditar el UUID del certificado de cifrado S/MIME:** Si se **activa**, los usuarios pueden activar y desactivar el cifrado S/MIME y la identidad del 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.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.

Servicios de Exchange sincronizados

La configuración de Servicios de Exchange sincronizados le permite sincronizar las funciones siguientes:

- Calendarios
- Contactos
- Mail
- Notas
- Recordatorios

Parámetros de macOS

Exchange

1 Policy Info

2 Platforms Clear All

☐ iOS

☒ macOS

☐ Android HTC

☐ Android Enterprise

☐ Samsung SAFE

☐ Samsung Knox

☐ Windows Phone

☐ Windows Desktop/Tablet

3 Assignment

Exchange

This policy configures Microsoft Exchange ActiveSync so user devices can access corporate email, calendar, contacts, and other synced services hosted on Exchange.

Exchange ActiveSync account name *

User *

Email address *

Use OAuth

OFF macOS 10.14+

Password

macOS 10.14+

Internal Exchange host

Internal server port

Internal server path

Use SSL for internal Exchange host

ON

External Exchange host

External server port

- **Nombre de la 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 utilizar la macro de sistema `$user.username` en este campo para buscar automáticamente los nombres de los usuarios.
- **Dirección de correo electrónico:** Especifique la dirección completa de correo electrónico. Puede utilizar la macro de sistema `$user.mail` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Usar OAuth:** Si está **activado**, la conexión usa 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:** En este campo, se indica la URL que se va a cargar en una vista web para autenticarse mediante OAuth cuando no usa el servicio de detección automática. Este campo aparece tras **activarse** la configuración **Usar OAuth**.
- **Contraseña:** Escriba una contraseña opcional para la cuenta de usuario de Exchange. Esta configuración no aparece cuando **Usar OAuth** está **activado**.
- **Host de Exchange interno.** Si quiere que los nombres de host interno y externo de Exchange difieran, puede escribir un nombre de host interno de Exchange.
- **Puerto del servidor interno.** Si quiere que los puertos de servidor interno y externo de Exchange difieran, puede escribir un número de puerto para el servidor interno de Exchange.
- **Ruta del servidor interno.** Si quiere que las rutas de servidor interno y externo de Exchange difieran, puede escribir una ruta de servidor interno de Exchange.
- **Usar SSL para el host de Exchange interno.** Seleccione si proteger las conexiones entre los dispositivos de los usuarios y el host interno de Exchange. El valor predeterminado es **Activado**.
- **Host de Exchange externo.** Si quiere que los nombres de host interno y externo de Exchange difieran, puede escribir un nombre de host externo de Exchange.
- **Puerto del servidor externo.** Si quiere que los puertos de servidor interno y externo de Exchange difieran, puede escribir un número de puerto para el servidor externo de Exchange.
- **Ruta del servidor externo.** Si quiere que las rutas de servidor interno y externo de Exchange difieran, puede escribir una ruta de servidor externo de Exchange.
- **Usar SSL para el host de Exchange externo.** Seleccione si proteger las conexiones entre los dispositivos de los usuarios y el host interno de Exchange. El valor predeterminado es **Activado**.
- **Permitir Mail Drop.** Seleccione si permitir que los usuarios compartan archivos entre dos equipos Mac de forma inalámbrica (sin tener que conectarse a una red existente). El valor predeterminado es **Desactivado**.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar 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**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.

- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Parámetros de escritorios y tabletas Windows

Exchange	Exchange
1 Policy Info	This policy configures Microsoft Exchange ActiveSync so user devices can access corporate email, calendar, contacts, and other synced services hosted on Exchange.
2 Platforms Clear All	<p>Account name or display name *</p> <input type="text"/>
<input type="checkbox"/> iOS	<p>Server name or IP address *</p> <input type="text"/>
<input type="checkbox"/> macOS	<p>Domain</p> <input type="text"/>
<input type="checkbox"/> Android HTC	<p>User ID or user name *</p> <input type="text"/>
<input type="checkbox"/> Android Enterprise	<p>Email address *</p> <input type="text"/>
<input type="checkbox"/> Samsung SAFE	<p>Use SSL connection</p> <input type="checkbox"/> OFF
<input type="checkbox"/> Samsung Knox	<p>Sync items</p>
<input checked="" type="checkbox"/> Windows Phone	<p>Past days to sync</p> <input type="text" value="All content"/>
<input checked="" type="checkbox"/> Windows Desktop/Tablet	<p>Sync scheduling</p>
3 Assignment	<p>Frequency</p> <input type="text" value="When item arrives"/>
	<p>Logging level</p> <input type="text" value="Disabled"/>

Nota:

Esta directiva no permite establecer la contraseña de usuario. Los usuarios deben establecer ese parámetro desde sus dispositivos después de que se envíe la directiva.

- **Nombre de cuenta o nombre simplificado.** Escriba el nombre de la cuenta de Exchange ActiveSync.
- **Nombre o dirección IP del servidor:** Escriba el nombre de host o la dirección IP del servidor Exchange.
- **Dominio:** Escriba el dominio donde reside el servidor Exchange. Puede utilizar la macro de sistema `$user.domainname` en este campo para buscar automáticamente los nombres de dominio de los usuarios.
- **ID de usuario o nombre de usuario:** Especifique el nombre de usuario para la cuenta de Exchange. Puede utilizar la macro de sistema `$user.username` en este campo para buscar automáticamente los nombres de los usuarios.
- **Dirección de correo electrónico:** Especifique la dirección completa de correo electrónico. Puede utilizar la macro de sistema `$user.mail` en este campo para buscar automáticamente las cuentas de correo electrónico de los usuarios.
- **Usar conexión SSL:** Seleccione si proteger las conexiones entre los dispositivos de los usuarios y el servidor Exchange. El valor predeterminado es **Desactivado**.

- **Días pasados a sincronizar:** En la lista, haga clic en la cantidad de días pasados con los que se sincronizará todo el contenido del dispositivo con el servidor Exchange. El valor predeterminado es **Todo el contenido**.
- **Frecuencia:** En la lista, haga clic en la programación que se usará para sincronizar los datos que se envíen al dispositivo desde el servidor Exchange. El valor predeterminado es **Cuando llega el mensaje**.
- **Nivel de registro:** En la lista, haga clic en **Inhabilitado**, **Básico** o **Avanzado** para especificar el nivel de detalle que se seguirá a la hora de registrar la actividad de Exchange. Está **inhabilitado** de forma predeterminada.

Directiva de archivos

November 7, 2022

Puede agregar e implementar archivos para que los usuarios accedan en sus dispositivos Android y Android Enterprise. Especifique el directorio donde quiere almacenar el archivo en el dispositivo. Por ejemplo, quiere que los usuarios reciban un documento de empresa o un archivo .pdf. Implemente el archivo en los dispositivos e informe a los usuarios de 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 dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de Android Enterprise

- **Archivo para importar:** Para seleccionar el archivo que quiere importar, haga clic en **Examinar** y, a continuación, vaya a la ubicación del archivo.
- **Carpeta de destino:** En la lista, seleccione la ubicación en que quiere 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 sirve por las restricciones impuestas por Google en el acceso a la ubicación de destino.
- **Nombre del archivo de destino:** Opcional. Si debe cambiar el nombre de un archivo antes de implementarlo en un dispositivo, escriba el nombre del archivo.
 - **Si ya existe el archivo:** en la lista, seleccione si quiere copiar un archivo existente. La opción predeterminada es **Copiar el archivo solo si es diferente**.

Importante:

La directiva Archivos ya no permite agregar scripts en Android Enterprise. Si una directiva existente contiene un script, aparece un mensaje de error al seleccionar la directiva y puede agregar de nuevo la directiva para resolver el problema.

Parámetros de Android

- **Archivo para importar:** Para seleccionar el archivo que quiere importar, haga clic en **Examinar** y, a continuación, vaya a la ubicación del archivo.
- **Tipo de archivo:** Seleccione **Archivo** o **Script**.
- **Ejecutar inmediatamente:** Al seleccionar **Script**, aparece la opción **Ejecutar inmediatamente**. No sucede nada cuando se habilita este parámetro. Los usuarios deben ejecutar el script manualmente.
- **Reemplazar expresiones de macros:** Seleccione si quiere reemplazar nombres de token de macro en un script por una propiedad de usuario o de dispositivo. Para obtener la sintaxis de las macros, consulte [Macros](#). De forma predeterminada, está **desactivado**.
- **Carpeta de destino:** En la lista, seleccione la ubicación en que quiere 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 sirve por las restricciones impuestas por Google en el acceso a la ubicación de destino.

- **Nombre del archivo de destino:** Opcional. Si debe cambiar el nombre de un archivo antes de implementarlo en un dispositivo, escriba el nombre del archivo.
- **Si ya existe el archivo:** en la lista, seleccione si quiere copiar un archivo existente. La opción predeterminada es **Copiar el archivo solo si es diferente**.

Directiva de FileVault

November 29, 2023

En macOS, la funcionalidad de cifrado de disco completo (FileVault 2) protege el volumen del sistema cifrando su contenido. El usuario inicia sesión en un dispositivo macOS con FileVault habilitado con su contraseña de cuenta cada vez que se inicia el dispositivo. Si el usuario pierde la contraseña, una clave de recuperación le permite desbloquear el disco y restablecerla.

Esta directiva de dispositivo permite al usuario de FileVault configurar pantallas y definir parámetros, como claves de recuperación. Para obtener más información acerca de FileVault, consulte el artículo de asistencia de Apple.

Para agregar la directiva de FileVault, vaya a **Configurar > Directivas de dispositivo**.

Parámetros de macOS

FileVault 2 Policy	FileVault 2 Policy
1 Policy Info	This policy lets you enable FileVault device encryption on enrolled macOS devices.
2 Platforms Clear All	Enable FileVault 2 <input checked="" type="checkbox"/> ?
<input checked="" type="checkbox"/> macOS	FileVault 2 Settings
3 Assignment	Prompt for FileVault setup during logout <input type="checkbox"/> ?
	Maximum times to skip FileVault setup <input type="text" value="0"/> ?
	Recovery key type <input type="text" value="Personal & institutional recovery key"/> ?
	Show personal recovery key <input type="checkbox"/> ?
	Institutional Recovery Key certificate * <input type="text" value="None"/> ?
	Escrow Personal Recovery Key <input type="checkbox"/> ?
	Deployment Rules

- **Habilitar FileVault:** Si está **activado**, se pide al usuario que habilite FileVault una vez pasados los cierres de sesión indicados en la opción **Máximo de veces que se puede omitir la configu-**

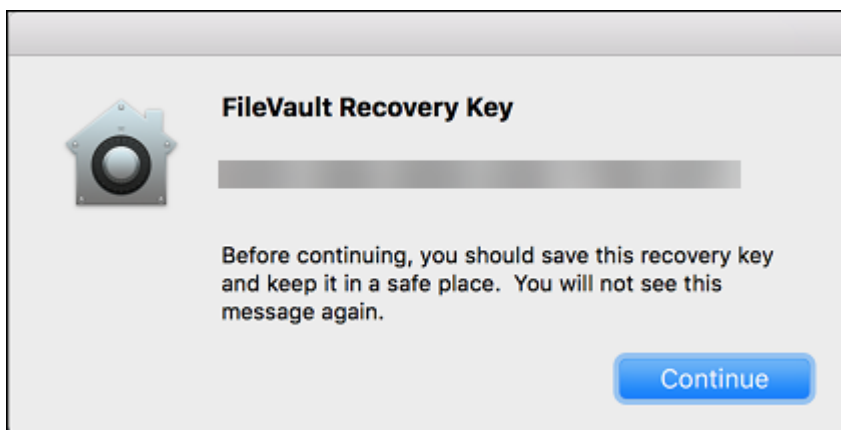
ración de FileVault. Si está **desactivado**, los usuarios no reciben ningún mensaje para habilitar FileVault, pero aún pueden habilitar FileVault ellos mismos.

- **Solicitar la configuración de FileVault durante el cierre de sesión:** Si el valor es **Sí**, se presentará un mensaje a los usuarios en el que se les pide que habiliten FileVault cuando cierren la sesión.
- **Máximo de veces que se puede omitir la configuración de FileVault:** La cantidad máxima de veces que el usuario puede omitir la configuración de FileVault. Cuando el usuario alcanza ese máximo, debe configurar FileVault para iniciar sesión. Si es **0**, el usuario debe habilitar FileVault durante el primero intento de inicio de sesión. El valor predeterminado es **0**.
- **Tipo de clave de recuperación:** Un usuario que olvide la contraseña puede escribir una clave de recuperación para desbloquear el disco y poder restablecerla. Opciones de la clave de recuperación:
 - **Clave de recuperación personal:** Una clave de recuperación personal es única para cada usuario. Durante la configuración de FileVault, un usuario elige si crear una clave de recuperación o permitir que su cuenta de iCloud desbloquee el disco. Para mostrar la clave de recuperación al usuario una vez completada la configuración de FileVault, active **Mostrar clave de recuperación personal**. Al mostrar la clave, el usuario puede anotarla para usarla en el futuro. Para permitir a los usuarios buscar su clave si la pierden, habilite **Clave de recuperación personal de custodia**.

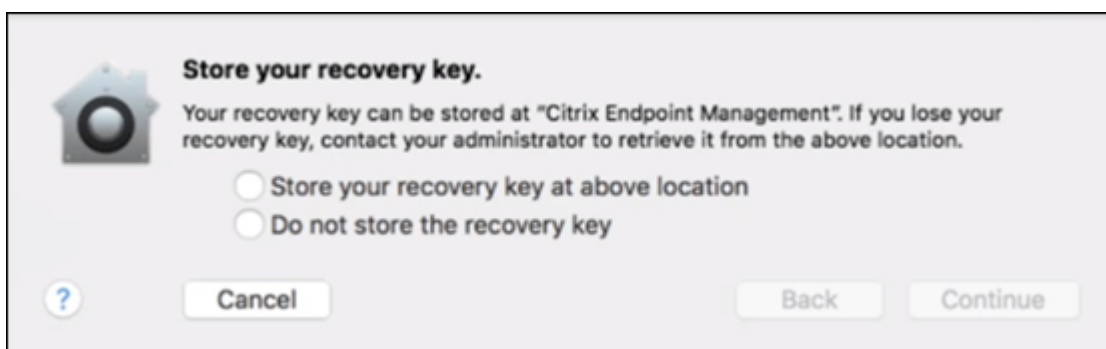
Puede rotar claves personales de recuperación mediante acciones de seguridad. Para obtener más información sobre la rotación de claves personales de recuperación, consulte [Acciones de seguridad](#).

Para obtener más información acerca de la administración de claves de recuperación, consulte el sitio de asistencia de Apple.
 - **Clave de recuperación institucional:** Puede crear una clave de recuperación institucional (o principal) y un certificado de FileVault, que podrá utilizar para desbloquear los dispositivos de los usuarios. Para obtener más información, consulte la página de asistencia de Apple. Utilice Citrix Endpoint Management para implementar el certificado de FileVault en los dispositivos. Para obtener más información, consulte [Certificados y autenticación](#).
 - **Clave de recuperación personal e institucional:** Cuando activa ambos tipos de claves de recuperación, solo deberá desbloquear un dispositivo si el usuario 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**, deberá seleccionar el certificado de clave de recuperación para esa clave.

- **Mostrar clave de recuperación personal:** Si el valor es **Sí**, el dispositivo del usuario muestra la clave de recuperación personal al usuario después de configurar FileVault. Está **desactivado** de forma predeterminada.

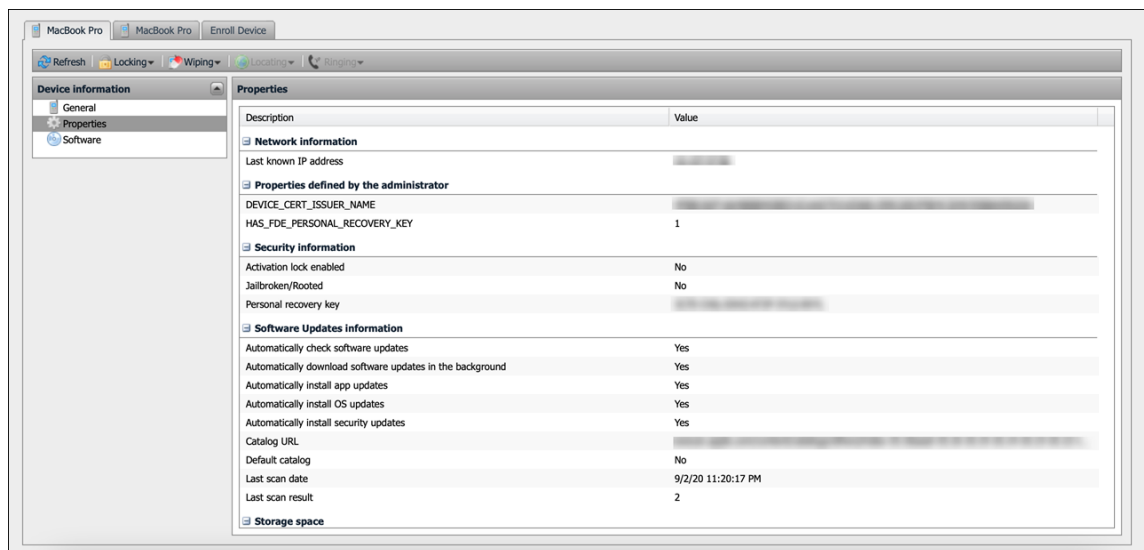


- **Clave de recuperación personal de custodia:** Cuando está habilitada esta opción, los usuarios pueden almacenar una copia de la clave de recuperación personal para cada dispositivo con Citrix Endpoint Management.



Para acceder a la clave desde Citrix Endpoint Management, vaya a **Administrar > Dispositivos**, seleccione el dispositivo macOS y haga clic en **Modificar**. A continuación, vaya a **Datos del dispositivo > General** y busque la **Clave de recuperación personal**.

Para permitir a los usuarios ver su clave de recuperación desde Self Help Portal, habilite **Clave de recuperación personal de custodia** y **Mostrar clave de recuperación personal al usuario**. La clave aparece en Self Help Portal en la página **Propiedades**, en **Información de seguridad**. Para obtener más información sobre Self-Help Portal, consulte [Self-Help Portal](#).



Puede habilitar el parámetro **Clave de recuperación personal de depósito de garantía** incluso si no activa el parámetro **Habilitar FileVault**. Si inhabilita el parámetro **Habilitar FileVault**, los usuarios aún pueden habilitar FileVault por su cuenta. En este caso, habilite **Clave de recuperación personal de custodia** para que los usuarios puedan almacenar 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 con FileVault habilitado en la consola.

Directiva de firewall

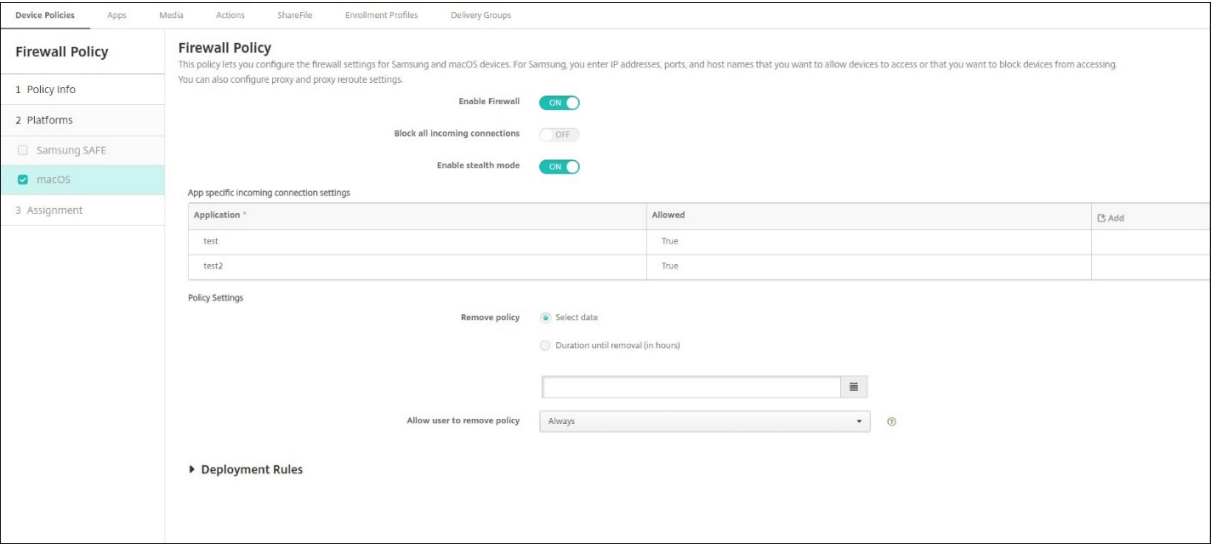
July 7, 2022

Esta directiva permite configurar los parámetros del firewall para dispositivos Samsung, macOS y Windows.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de macOS

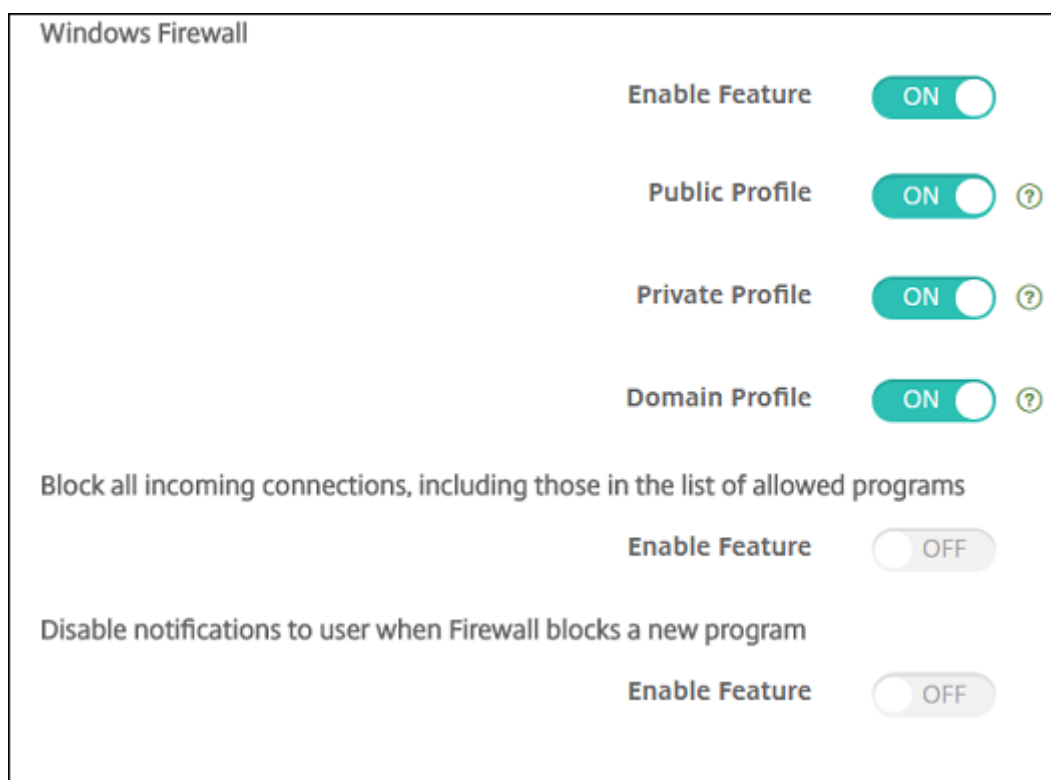
Requiere macOS 10.12 y posterior.



- **Habilitar firewall.** Para habilitar el firewall, **active** esta opción.
- **Bloquear todas las conexiones entrantes.** Cuando esta opción está **activada**, bloquea todas las conexiones entrantes, excepto las conexiones necesarias para los servicios básicos.
- **Habilitar el modo sigiloso.** En este modo, el dispositivo no responde ni reconoce intentos de acceder a él desde la red por parte de aplicaciones de prueba con ICMP, tales como Ping. Para habilitar este modo, **active** esta opción.
- **Parámetros de conexión entrante específicos de la aplicación.** Para permitir que aplicaciones concretas reciban conexiones, agréguelas y establezca **Permitido** en **True**.

Parámetros de tabletas y escritorios Windows

Requiere dispositivos de escritorio y tableta con Windows 10 (versión 1709 o una posterior) o Windows 11.



- **Habilitar función.** Controla el tráfico entrante y saliente de los equipos en los que se implementará esta directiva. De forma predeterminada, está **activado**.
- **Perfil público.** Controla el Firewall de Windows mientras los equipos están conectados a redes que no son de confianza en los sitios públicos (por ejemplo, en una cafetería o un aeropuerto). De forma predeterminada, está **activado**.
- **Perfil privado.** Controla el Firewall de Windows mientras los equipos están conectados a redes de confianza (por ejemplo, la red doméstica). De forma predeterminada, está **activado**.
- **Perfil de dominio.** Controla el Firewall de Windows mientras los equipos están conectados a redes de dominio (por ejemplo, el lugar de trabajo). De forma predeterminada, está **activado**.
- **Bloquear todas las conexiones entrantes, incluidas las de la lista de programas permitidos.** De forma predeterminada está **desactivado**.
- **Inhabilitar las notificaciones al usuario cuando el firewall bloquea un programa nuevo.** De forma predeterminada está **desactivado**.

Directiva de fuentes

November 29, 2023

En Citrix Endpoint Management, puede agregar una directiva para agregar más fuentes de texto a

dispositivos iOS y macOS. Las fuentes deben tener el formato TrueType (.ttf) u OpenType (.otf). No se admiten las colecciones de fuentes (.ttc o .otc).

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Nombre visible para el usuario:** Escriba el nombre que verán los usuarios en sus listas de fuentes.
- **Archivo de la fuente:** Seleccione el archivo de fuentes que se va a agregar a los dispositivos de los usuarios. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.

Parámetros de macOS

- **Nombre visible para el usuario:** Escriba el nombre que verán los usuarios en sus listas de fuentes.
- **Archivo de la fuente:** Seleccione el archivo de fuentes que se va a agregar a los dispositivos de los usuarios. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar 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**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.

- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Directiva de diseño de pantalla de inicio

November 29, 2023

La directiva “Diseño de pantalla inicial” permite especificar la distribución de las aplicaciones y las carpetas que aparezcan en la pantalla de inicio de iOS en los dispositivos iOS administrados.

Importante:

La implementación de varias directivas de diseño de pantalla inicial en un dispositivo provoca un error de iOS en el dispositivo. Esta limitación se aplica tanto si la pantalla inicial se define a través de esta directiva de Citrix Endpoint Management o 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](#).

Parámetros de iOS

Device Policies

Apps

Media

Actions

Content Collaboration

Enrollment Profiles

Delivery Groups

Home Screen Layout Policy

1 Policy Info

2 Platforms

Clear All

✓ iOS

3 Assignment

Home Screen Layout Policy

This policy defines a layout of apps, folders and web clips for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application, you should enter its bundle identifier. For a folder, you should enter a list of bundle identifiers separated with commas. For a web clip, you should enter its URL.

Dock

Type	Display Name *	Value *	<div>Add</div>
------	----------------	---------	----------------

Page 1

Type	Display Name *	Value *	<div>Add</div>
------	----------------	---------	----------------

Page 2

Type	Display Name *	Value *	<div>Add</div>
------	----------------	---------	----------------

Page 3

Type	Display Name *	Value *	<div>Add</div>
------	----------------	---------	----------------

Page 4

Type	Display Name *	Value *	<div>Add</div>
------	----------------	---------	----------------

Page 5

Type	Display Name *	Value *	<div>Add</div>
------	----------------	---------	----------------

Policy Settings

Back

Next >

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

745

- Haga clic en **Agregar** para agregar cada una de las áreas de la pantalla que quiera configurar (como **Dock** o **Página 1**).

- **Tipo:** Elija **Aplicación**, **Carpeta** o **Clip web**.

El parámetro **Uso restringido de aplicaciones > Permitir solo algunas aplicaciones** en la [directiva de restricciones](#) puede evitar que los clips web aparezcan correctamente en la pantalla de inicio. Para que los clips web aparezcan correctamente, realice una de las siguientes acciones:

- Establezca **Uso restringido de aplicaciones** en **Permitir todas las aplicaciones** o en **No permitir algunas aplicaciones**.
- Con **Uso restringido de aplicaciones** configurado en **Permitir solo algunas aplicaciones**, agregue una aplicación con el ID de paquete `com.apple.webapp` para permitir clips web.

The screenshot shows the 'Home Screen Layout Policy' configuration page. The sidebar on the left has three sections: '1 Policy Info', '2 Platforms' (with a 'Clear All' link), and '3 Assignment'. Under '2 Platforms', 'iOS' is selected with a checkmark. The main content area is titled 'Home Screen Layout Policy' and includes a description: 'This policy defines a layout of apps, folders and web clips for the home screen. It is supported only on iOS 9.3 and later supervised devices. For an application, you should enter its bundle identifier. For a folder, you should enter a list of bundle identifiers separated with commas. For a web clip, you should enter its URL.' Below this is a table for adding items to the 'Dock'. The table has columns for 'Type', 'Display Name', and 'Value'. A dropdown menu is open for the 'Type' column, showing options: 'Application', 'Folder', and 'WebClip'. There are 'Save' and 'Cancel' buttons for the first row, and an 'Add' button at the bottom right.

- **Nombre simplificado:** El nombre de la aplicación o la carpeta que aparecerá en la pantalla de inicio.
- **Valor:** Para las aplicaciones, introduzca el ID de paquete. En caso de carpetas, introduzca una lista de identificadores de paquete, separados por comas. En caso de clips web, introduzca el ID del paquete `com.apple.webClip.managed` y configure la dirección URL del clip web en la directiva de clips web. Si existe más de un valor de clip web con la misma URL, el comportamiento no está definido en dispositivos iOS 11.3 y versiones posteriores.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.

- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible en iOS 9.3 y versiones posteriores.

Directiva de importación de perfiles de iOS y macOS

November 29, 2023

Puede importar, en Citrix Endpoint Management, archivos XML de configuración de dispositivos iOS y macOS. El archivo contiene las restricciones y las directivas seguridad de los dispositivos que se preparan con Apple Configurator 2 o ProfileCreator. 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 ProfileCreator:

- **System Policy Control:** La directiva identifica las aplicaciones firmadas por los desarrolladores certificados de Apple y permite a los usuarios descargar las aplicaciones verificadas desde la tienda de aplicaciones de Mac.

Al configurar la directiva:

- Seleccione **Enable Gatekeeper** para asegurarse de que los usuarios solo ejecutan software verificado y de confianza.
- Seleccione **Allow Identified Developers** para asegurarse de que los usuarios instalen solo aquellas aplicaciones que están firmadas por desarrolladores de Apple certificados.

- **Privacy Preferences Policy Control:** La directiva permite conceder o restringir el acceso entre aplicaciones a determinados archivos o funciones, como servicios de ubicación, cámara y captura de pantalla.

Configure los parámetros que piensa implementar. Para obtener más información, consulte [Ajustes de carga de MDM “Control de la política de preferencias de privacidad”](#).

- **Kernel Extensions Policy:** La directiva permite a los usuarios instalar extensiones de aplicaciones que amplían las capacidades nativas del sistema operativo. Las extensiones del núcleo se ejecutan a nivel del núcleo.

Configure los parámetros que piensa implementar. Para obtener más información, consulte [Ajustes de carga de MDM “Política de extensiones de kernel”](#).

- **Ethernet Settings Policy:** La directiva permite administrar la conexión de red Ethernet.

Configure los parámetros que piensa implementar. Para obtener más información, consulte [Ajustes de Ethernet](#).

Utilice Apple Configurator 2 o ProfileCreator para configurar las siguientes directivas para dispositivos macOS e iOS:

- **Directiva de Wi-Fi:** La directiva permite administrar la forma en que los usuarios conectan sus dispositivos a una red inalámbrica.

Al configurar la directiva:

- Agregue el SSID de destino al principio de la lista de prioridades.
- Elija el modo de conexión que se va a utilizar cuando el usuario se conecte a una red. Si selecciona **Sistema**, el dispositivo utilizará 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 [Ajustes de Wi-Fi](#).

- **Directiva de restricciones:** La directiva permite o restringe el uso de ciertas funciones en los dispositivos de usuario.

Configure los parámetros que piensa implementar. Para obtener más información, consulte [Revisar las restricciones](#).

- **Directiva VPN:** La directiva proporciona una conexión a redes privadas cifrada a nivel de dispositivo.

Configure los parámetros que piensa implementar. Para obtener más información, consulte [VPN overview](#).

Crear un perfil de configuración con Apple Configurator 2

1. Instale Apple Configurator 2 desde el App Store de Apple.
2. Inicie Apple Configurator 2 y vaya a **Archivo > Nuevo perfil**. Aparecerá una nueva ventana de configuración.
3. En el panel de parámetros **General**, escriba un nombre y un identificador del perfil y, a continuación, agregue las opciones de carga adicional.
4. En el panel de la izquierda, seleccione una carga útil, haga clic en **Configurar** e introduzca los parámetros. No firme su perfil, ya que los perfiles firmados no se admiten.

Para añadir varias cargas útiles dentro de un único perfil, seleccione una carga útil y haga clic en el botón **Añadir carga** de 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**.

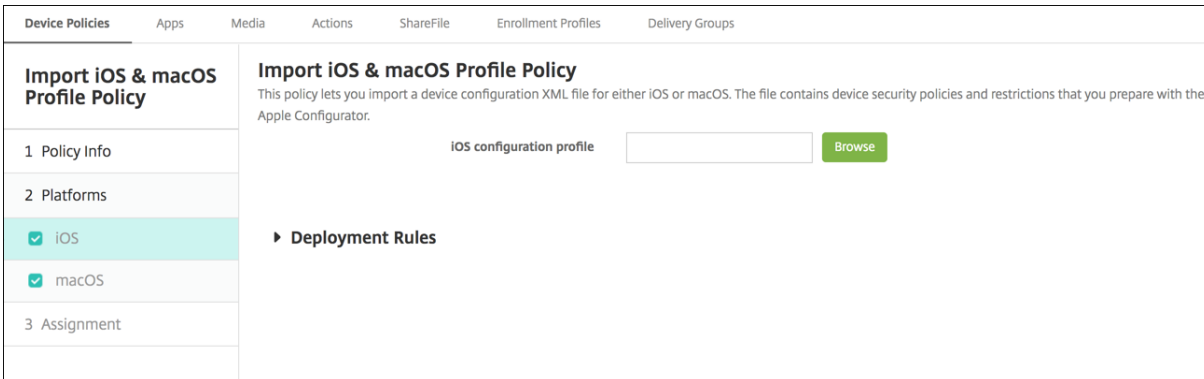
Crear un perfil de configuración con ProfileCreator

1. Instale ProfileCreator desde [GitHub](#).
2. Inicie ProfileCreator y vaya a **File > New**. Aparecerá una nueva ventana de configuración.
3. En el panel de parámetros **General**, escriba un nombre y una descripción del perfil y, a continuación, agregue las opciones de carga adicional.
 - Recomendación: Seleccione **Prevent users from removing this profile**.
 - Establezca **Payload Scope** en **System** o en **User**.
4. En el panel izquierdo, elija la directiva, configure los parámetros y haga clic en **Add**, en la esquina superior derecha.

Para configurar varias directivas dentro de un solo perfil, seleccione una directiva y haga clic en el botón **Add**.
5. Vaya a **File > Export**, elija un nombre y una ubicación para guardar el archivo XML y haga clic en **Save**.

Para importar un archivo de configuración para la directiva de perfiles iOS y macOS en la consola de Citrix Endpoint Management, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS y macOS



The screenshot displays the 'Import iOS & macOS Profile Policy' configuration page in the Citrix Endpoint Management console. The left sidebar shows the 'Device Policies' section with the 'Import iOS & macOS Profile Policy' option selected. The main content area is titled 'Import iOS & macOS Profile Policy' and includes a description: 'This policy lets you import a device configuration XML file for either iOS or macOS. The file contains device security policies and restrictions that you prepare with the Apple Configurator.' Below this, there is a section for 'iOS configuration profile' with a text input field and a green 'Browse' button. Further down, there is a 'Deployment Rules' section with a right-pointing arrow.

- **Perfil de configuración de iOS o Perfil de configuración de macOS:** Seleccione el archivo de configuración que quiera importar. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.

Directiva de dispositivos de administración de Keyguard

November 29, 2023

Android Keyguard administra las pantallas de bloqueo del dispositivo y de Work Challenge. Esta directiva le permite controlar funciones de Keyguard del perfil de trabajo y funciones de Keyguard avanzadas del dispositivo en Android Enterprise. Puede controlar:

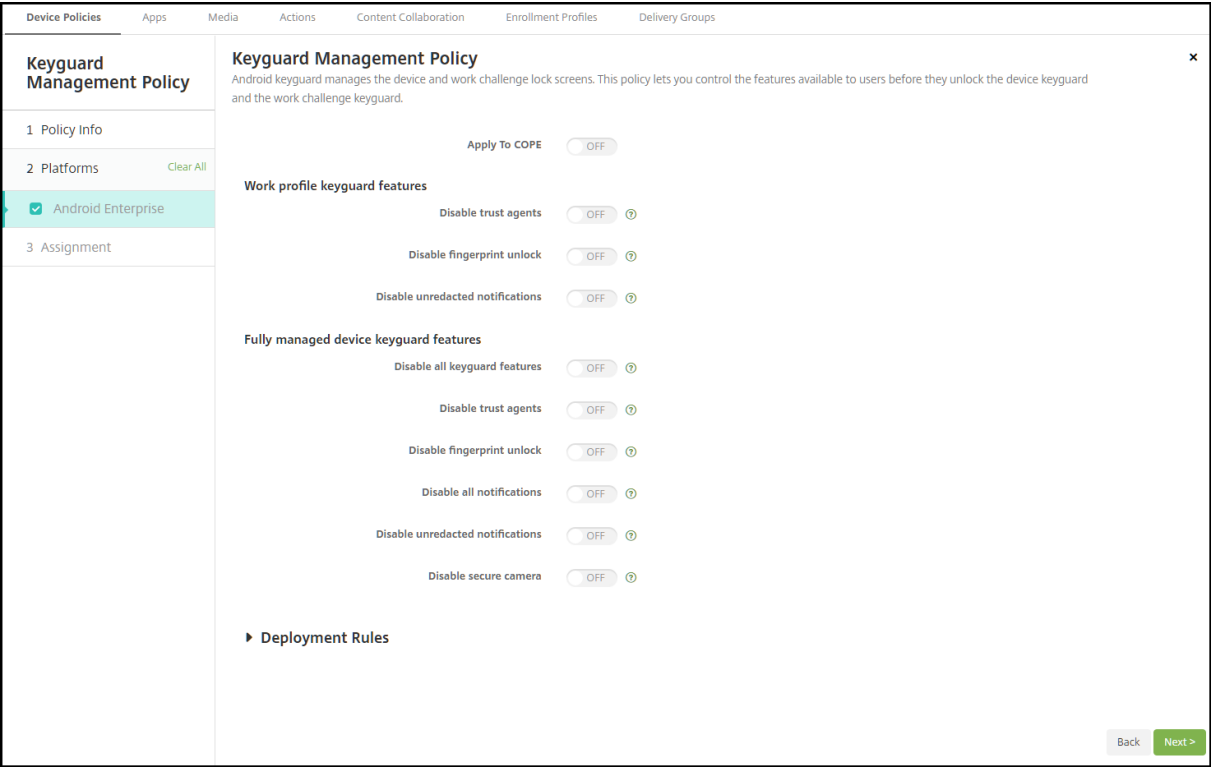
- Administración de Keyguard en dispositivos de perfil de trabajo. Puede especificar las funciones disponibles para los usuarios antes de que desbloqueen el Keyguard del dispositivo y el Keyguard de Work Challenge. Por ejemplo, de forma predeterminada, los usuarios pueden usar desbloqueo mediante huella digital y ver notificaciones sin redactar en la pantalla de bloqueo.
- Administración de Keyguard en dispositivos dedicados y totalmente administrados. 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 desactivar 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 con acceso privado). Puede utilizar una directiva de administración de Keyguard para aplicar configuraciones independientes al dispositivo y al perfil de trabajo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Vea este vídeo para obtener más información:



Parámetros de Android Enterprise



- **Aplicar a COPE:** Permite configurar los parámetros de la directiva de dispositivos de adminis-

tración de Keyguard para dispositivos totalmente administrados con perfiles de trabajo.

Si el valor es **Sí**, puede aplicar configuraciones independientes al dispositivo y al perfil de trabajo en dispositivos totalmente administrados con perfiles de trabajo.

Si el valor es **No**, puede aplicar la configuración a dispositivos de perfil de trabajo o dispositivos totalmente administrados. Los parámetros que configure para los perfiles de trabajo solo se aplicarán a los dispositivos de perfil de trabajo. Los parámetros que configure para dispositivos totalmente administrados solo se aplicarán a los dispositivos totalmente administrados.

El valor predeterminado es **Desactivado**.

- **Funciones de Keyguard del perfil de trabajo:** Controla si las siguientes funciones estarán disponibles antes de que un usuario desbloquee el Keyguard del perfil de trabajo (pantalla de bloqueo).
 - **Inhabilitar agentes de confianza:** Si el valor es **No**, los agentes de confianza pueden operar en pantallas de Keyguard seguras cuando se establece un desafío en el perfil de trabajo. Establézcalo en **Sí** para inhabilitar todos los agentes de confianza en el perfil de trabajo. El valor predeterminado es **Desactivado**.
 - **Inhabilitar autenticación biométrica:** Si el valor es **No**, la autenticación biométrica está disponible en las pantallas de Keyguard seguras cuando se establece un desafío en el perfil de trabajo. Establezca el valor en **Sí** para inhabilitar la autenticación biométrica en el perfil de trabajo. Esta configuración inhabilita el desbloqueo por huella dactilar, la autenticación facial y la autenticación del iris. El valor predeterminado es **Desactivado**. Para Android 9.0 y versiones posteriores.
 - **Inhabilitar desbloqueo mediante huella digital:** Si el valor es **No**, el desbloqueo mediante huella digital está disponible en pantallas Keyguard seguras cuando se establece un desafío en el perfil de trabajo. Establézcalo en **Sí** para inhabilitar el desbloqueo mediante huella digital en el perfil de trabajo. El valor predeterminado es **Desactivado**.
 - **Inhabilitar autenticación facial:** Si el valor es **No**, la autenticación facial está disponible en las pantallas de Keyguard seguras cuando se establece un desafío en el perfil de trabajo. Establezca el valor en **Sí** para inhabilitar la autenticación facial en el perfil de trabajo. El valor predeterminado es **Desactivado**. Para Android 9.0 y versiones posteriores.
 - **Inhabilitar autenticación de iris:** Si el valor es **No**, la autenticación de iris está disponible en las pantallas de Keyguard seguras cuando se establece un desafío en el perfil de trabajo. Establezca el valor en **Sí** para inhabilitar la autenticación de iris en el perfil de trabajo. El valor predeterminado es **Desactivado**. Para Android 9.0 y versiones posteriores.
 - **Inhabilitar notificaciones sin redactar:** Si el valor es **No**, las notificaciones redactadas y sin redactar aparecen en las pantallas de Keyguard seguras. Establezca el valor en **Sí** para inhabilitar las notificaciones sin redactar y mostrar solo las notificaciones redactadas. El valor predeterminado es **Desactivado**.

- **Funciones de Keyguard del dispositivo totalmente administradas:** Controla si las siguientes funciones están disponibles antes de que un usuario desbloquee el Keyguard del dispositivo (pantalla de bloqueo). Estas funciones son aplicables a dispositivos totalmente administrados o dedicados.
 - **Inhabilitar todas las funciones de Keyguard:** Si el valor es **No**, todas las personalizaciones actuales y futuras de Keyguard estarán disponibles en las pantallas seguras de Keyguard. Establézcalo en **Sí** para desactivar todas las personalizaciones de Keyguard. El valor predeterminado es **Desactivado**.
 - **Inhabilitar agentes de confianza:** Si el valor es **No**, los agentes de confianza pueden operar en pantallas de Keyguard seguras. Establézcalo en **Sí** para inhabilitar los agentes de confianza. El valor predeterminado es **Desactivado**.
 - **Inhabilitar autenticación biométrica:** Si el valor es **No**, la autenticación biométrica está disponible en las pantallas de Keyguard seguras cuando se establece un desafío en el dispositivo. Establezca el valor en **Sí** para inhabilitar la autenticación biométrica en el dispositivo. Las funciones de autenticación biométrica inhabilitadas son el desbloqueo por huella digital, autenticación facial y autenticación de iris. El valor predeterminado es **Desactivado**. Para Android 9.0 y versiones posteriores.
 - **Inhabilitar desbloqueo mediante huella digital:** Si el valor es **No**, el desbloqueo mediante huella digital está disponible en pantallas Keyguard seguras cuando se establece un desafío en el dispositivo. Establézcalo en **Sí** para inhabilitar el desbloqueo mediante huella digital en el dispositivo. El valor predeterminado es **Desactivado**.
 - **Inhabilitar autenticación facial:** Si el valor es **No**, la autenticación facial está disponible en las pantallas de Keyguard seguras cuando se establece un desafío en el dispositivo. Establezca el valor en **Sí** para inhabilitar la autenticación facial en el dispositivo. El valor predeterminado es **Desactivado**. Para Android 9.0 y versiones posteriores.
 - **Inhabilitar autenticación de iris:** Si el valor es **No**, la autenticación de iris está disponible en las pantallas de Keyguard seguras cuando se establece un desafío en el dispositivo. Establezca el valor en **Sí** para inhabilitar la autenticación de iris en el dispositivo. El valor predeterminado es **Desactivado**. Para Android 9.0 y versiones posteriores.
 - **Inhabilitar todas las notificaciones:** Si el valor es **No**, todas las notificaciones aparecerán en las pantallas seguras de Keyguard. Establézcalo en **Sí** para mostrar todas las notificaciones. El valor predeterminado es **Desactivado**.
 - **Inhabilitar notificaciones sin redactar:** Si el valor es **No**, las notificaciones redactadas y sin redactar aparecen en las pantallas de Keyguard seguras. Establezca el valor en **Sí** para inhabilitar las notificaciones sin redactar y mostrar solo las notificaciones redactadas. El valor predeterminado es **Desactivado**.
 - **Inhabilitar cámara segura:** Si el valor es **No**, la cámara segura está disponible en las pantallas seguras de Keyguard. Establézcalo en **Sí** para inhabilitar la cámara segura. El valor predeterminado es **Desactivado**.

Directiva de quiosco

November 29, 2023

La directiva Quiosco permite restringir los dispositivos al modo quiosco porque limita las aplicaciones que se pueden ejecutar en ellos: Citrix Endpoint Management no controla qué parte del dispositivo se bloquea en modo quiosco. El dispositivo administra la configuración del modo quiosco después de que se haya implementado 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 bloqueo de aplicaciones. Para obtener información sobre cómo configurar iPads como quioscos, consulte [Configurar un iPad como un quiosco](#). También puede configurar un iPad para que abra un solo sitio web. Para obtener información, consulte la [Directiva de clips web](#).

Parámetros de tabletas y escritorios Windows

Para tabletas y escritorios Windows, la directiva Quiosco se aplica solo a los usuarios locales y a los usuarios inscritos en Azure AD.

El modo Quiosco en tabletas y escritorios Windows se pueden ejecutar una o varias aplicaciones.

Nota:

La directiva de quiosco solo se aplica a dispositivos con Windows 10.

Para implementar un quiosco de una sola aplicación en dispositivos con Windows 11, puede usar la directiva de XML personalizado para implementar el script XML que proporcionamos a los dispositivos. Para obtener más información, consulte [Implementar un quiosco de una sola aplicación en dispositivos con Windows 11](#).

- **AUMID de aplicación UWP:** Haga clic en **Agregar**, seleccione la aplicación de la Plataforma universal de Windows (UWP) e introduzca el ID de modelo de usuario de la aplicación (AUMID) para cada aplicación UWP. Por ejemplo, introduzca el siguiente AUMID:
 - `Microsoft.WindowsCalculator_8wekyb3d8bbwe!App`
- **Ruta de la aplicación Win32 y AUMID de la aplicación Win32:** Haga clic en **Agregar**, seleccione la aplicación de escritorio de Windows (Win32) e introduzca la ruta y el AUMID de 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 la página 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 Quiosco. Opciones disponibles:
 - **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:** Escriba el nombre del usuario que recibirá la directiva Quiosco.
 - Para crear un nombre de usuario local en el dispositivo de destino, introduzca el nombre. El nombre del usuario local no debe contener el dominio. Si escribe un nombre existente, Citrix Endpoint Management no crea ningún usuario ni cambia la contraseña actual.
 - Para agregar a un usuario de Azure AD, escriba 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 especificado al crear un usuario en Azure AD. El usuario asignado no puede ser administrador de Azure AD.

- **Contraseña:** No hay ningún parámetro 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 poder ofrecer a los usuarios una forma fácil de ver y administrar aplicaciones. El valor predeterminado es **Desactivado**.
- Haga clic en **Siguiente** y guarde los cambios.

Para una aplicación UWP que quiera 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.

```
1 $installedapps = get-AppxPackage
2
3 $aumidList = @()
4 foreach ($app in $installedapps)
5 {
6
7     foreach ($id in (Get-AppxPackageManifest $app).package.applications
8         .application.id)
9     {
10         $aumidList += $app.packagefamilyname + "!" + $id
11     }
12 }
13
14
15
16 $aumidList
17 <!--NeedCopy-->
```

Parámetros de Android Enterprise

Para dispositivos Android Enterprise dedicados, que también se conocen como dispositivos de uso único y propiedad de la empresa (COSU), puede incluir aplicaciones en la lista de permitidos y establecer el modo de bloqueo de tarea.

Para permitir una aplicación, haga clic en **Agregar**. Puede agregar varias aplicaciones a la lista de permitidos. Para obtener más información, consulte [Android Enterprise](#).

- **Aplicaciones que permitir:** Indique el nombre del paquete de la aplicación que quiere incluir en la lista de permitidos o seleccione la aplicación en 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 cargadas en Citrix Endpoint Management. De forma predeterminada, los servicios Citrix Secure Hub y Google Play están en la lista de permitidos.

The screenshot shows the Citrix Endpoint Management interface. The top navigation bar includes 'Endpoint Management', 'Analyze', 'Manage', and 'Configure'. Below this, a sub-navigation bar lists 'Device Policies', 'Apps', 'Media', 'Actions', 'Content Collaboration', 'Enrollment Profiles', and 'Delivery Groups'. The 'Device Policies' section is active, showing a 'Kiosk policy' configuration page. On the left, a sidebar lists '1 Policy Info', '2 Platforms' (with 'Clear All' and 'Windows Desktop/Tablet' options), and '3 Assignment'. Under 'Platforms', 'Android Enterprise' is selected. The main content area for the 'Kiosk policy' includes a description: 'This policy lets you specify a set of apps available on Android corporate owned devices for dedicated use. Apps you add to the allow list are available on the device. Apps you set to allow lock task mode are pinned to the device screen when the user opens the app. Users cannot exit the app using the Back button. No Home button appears when an app is in lock task mode.' Below this is the 'Allowed apps' section with a table. The table has two columns: 'Apps to allow' and 'Lock task mode'. The 'Apps to allow' column has a dropdown menu set to 'Make a selection'. The 'Lock task mode' column has two radio buttons: 'Allow' (selected) and 'Block'. At the bottom right of the table are 'Save' and 'Cancel' buttons. Below the table is a link for 'Deployment Rules'.

- **Modo de bloqueo de tarea:** Seleccione **Permitir** para que la aplicación quede anclada en la pantalla del dispositivo cuando el usuario la abra. Elija **Bloquear** para que la aplicación no quede anclada. El valor predeterminado es **Permitir**.

Cuando una aplicación se encuentra en el modo de bloqueo de tarea, esa aplicación queda anclada a la pantalla del dispositivo cuando el usuario la abre. No aparece el botón Inicio y el botón **Atrás** está desactivado. El usuario sale de la aplicación mediante una acción programada en la aplicación, como cerrar sesión.

Directiva de configuración del Launcher

November 29, 2023

Citrix Launcher permite personalizar la experiencia de usuario en los dispositivos Android Enterprise y Android antiguos implementados por Citrix Endpoint Management.

Para controlar estas funciones de Citrix Launcher, utilice una directiva de configuración de Launcher:

- Administre los dispositivos Android Enterprise y los dispositivos Android antiguos de manera que los usuarios solo puedan acceder a las aplicaciones que especifique.
- Si lo prefiere, puede especificar una imagen de logo personalizada como icono de Citrix Launcher, así como una imagen de fondo para Citrix Launcher.
- Especifique una contraseña que los usuarios deban introducir para salir de Launcher.

Citrix Launcher no está diseñado como una capa de seguridad adicional situada sobre la capa que la plataforma del dispositivo ya proporciona.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de Android Enterprise y Android

- **Definir una imagen de logotipo:** Seleccione si utilizar una imagen personalizada como logotipo para el icono de Citrix Launcher. El valor predeterminado es **Desactivado**.
- **Imagen de logotipo:** Cuando habilite **Definir una imagen de logotipo**, deberá seleccionar un archivo de imagen. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo. Los tipos de archivo admitidos son: PNG, JPG, JPEG y GIF.
- **Definir una imagen de fondo:** Seleccione si utilizar una imagen personalizada como imagen de fondo de Citrix Launcher. El valor predeterminado es **Desactivado**.
- **Imagen de fondo:** Cuando habilite **Definir una imagen de fondo**, deberá seleccionar un archivo de imagen. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo. Los tipos de archivo admitidos son: PNG, JPG, JPEG y GIF.
- **Aplicaciones permitidas:** Haga clic en **Agregar** y lleve a cabo lo siguiente para permitir cada aplicación en Citrix Launcher:
 - **Aplicación nueva que agregar:** Escriba el nombre completo de la aplicación que se va a agregar. Por ejemplo, com.android.calendar para la aplicación Calendario de Android.
 - Haga clic en **Guardar** para agregar la aplicación, o bien haga clic en **Cancelar** para no agregarla.
- **Contraseña:** La contraseña que el usuario debe introducir para salir de Citrix Launcher.

Directiva de LDAP

November 29, 2023

En Citrix Endpoint Management, puede crear una directiva de protocolo LDAP para dispositivos iOS con el fin de proporcionar información sobre el servidor LDAP a utilizar, incluida la información de cuenta necesaria. La directiva también ofrece un conjunto de directivas de búsquedas LDAP a usar cuando se consulta el servidor LDAP.

Es necesario el nombre de host del servidor 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](#).

Parámetros de iOS

- **Descripción de la cuenta.** Indique una descripción opcional de la cuenta.
- **Nombre de usuario de la cuenta.** Si quiere, escriba un nombre de usuario.
- **Contraseña de la cuenta.** Escriba una contraseña opcional. Use este campo solo con perfiles cifrados.
- **Nombre de host de LDAP.** Escriba el nombre de host del servidor LDAP. Este campo es obligatorio.
- **Usar SSL.** Seleccione si utilizar una Secure Sockets Layer (SSL) en la conexión al servidor LDAP. El valor predeterminado es **Activado**.
- **Parámetros de búsqueda.** Agregue las opciones de búsqueda que se van a usar cuando se consulte el servidor LDAP. Puede insertar tantas opciones de búsqueda como quiera, pero debe agregar al menos una opción de búsqueda para que la cuenta se pueda utilizar. Haga clic en **Agregar** y lleve a cabo lo siguiente:
 - **Descripción.** Introduzca una descripción de la opción de búsqueda. Este campo es obligatorio.
 - **Ámbito.** Seleccione **Base**, **Un nivel** o **Subárbol** para definir los niveles de búsqueda en el árbol LDAP. El valor predeterminado es **Base**.
 - * El nivel **Base** busca en el nodo al que apunta Búsqueda base.
 - * El nivel **Un nivel** busca en el nodo Base y en un nivel por debajo de él.
 - * El nivel **Subárbol** busca en el nodo Base y en todos sus elementos secundarios, independientemente de la cantidad de niveles de profundidad.
 - **Base de búsqueda.** Escriba la ruta al nodo en el que iniciar la búsqueda. Por ejemplo, ou=usuarios o 0=empresa de ejemplo. Este campo es obligatorio.
 - Haga clic en **Guardar** para agregar la opción de búsqueda, o bien haga clic en **Cancelar** para descartarla.
 - Repita estos pasos para cada opción de búsqueda que quiera agregar.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva.

Parámetros de macOS

- **Descripción de la cuenta.** Indique una descripción opcional de la cuenta.
- **Nombre de usuario de la cuenta.** Si quiere, escriba un nombre de usuario.
- **Contraseña de la cuenta.** Escriba una contraseña opcional. Use este campo solo con perfiles cifrados.
- **Nombre de host de LDAP.** Escriba el nombre de host del servidor LDAP. Este campo es obligatorio.
- **Usar SSL.** Seleccione si utilizar una Secure Sockets Layer (SSL) en la conexión al servidor LDAP. El valor predeterminado es **Activado**.
- **Parámetros de búsqueda.** Agregue las opciones de búsqueda que se van a usar cuando se consulte el servidor LDAP. Puede insertar tantas opciones de búsqueda como quiera, pero debe agregar al menos una opción de búsqueda para que la cuenta se pueda utilizar. Haga clic en **Agregar** y lleve a cabo lo siguiente:
 - **Descripción.** Introduzca una descripción de la opción de búsqueda. Este campo es obligatorio.
 - **Ámbito.** Seleccione **Base**, **Un nivel** o **Subárbol** para definir los niveles de búsqueda en el árbol LDAP. El valor predeterminado es **Base**.
 - * El nivel **Base** busca en el nodo al que apunta Búsqueda base.
 - * El nivel **Un nivel** busca en el nodo Base y en un nivel por debajo de él.
 - * El nivel **Subárbol** busca en el nodo Base y en todos sus elementos secundarios, independientemente de la cantidad de niveles de profundidad.
 - **Base de búsqueda.** Escriba la ruta al nodo en el que iniciar la búsqueda. Por ejemplo, ou=usuarios o 0=empresa de ejemplo. Este campo es obligatorio.
 - Haga clic en **Guardar** para agregar la opción de búsqueda, o bien haga clic en **Cancelar** para descartarla.
 - Repita estos pasos para cada opción de búsqueda que quiera agregar.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar 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**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.

- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Directiva de localización geográfica

November 29, 2023

En Citrix Endpoint Management, puede crear directivas de localización geográfica para aplicar límites geográficos. Cuando los usuarios abandonen el perímetro definido, también llamado *geocerca*, Citrix Endpoint Management puede realizar determinadas acciones. Por ejemplo, puede configurar la directiva para emitir un mensaje de advertencia para los usuarios cuando estos abandonen el perímetro definido. También puede configurar la directiva para borrar datos empresariales de los usuarios cuando estos abandonen un perímetro, inmediatamente o pasado un período. Para obtener información acerca de las acciones de seguridad (como el seguimiento y la localización de un dispositivo), consulte [Acciones de seguridad](#).

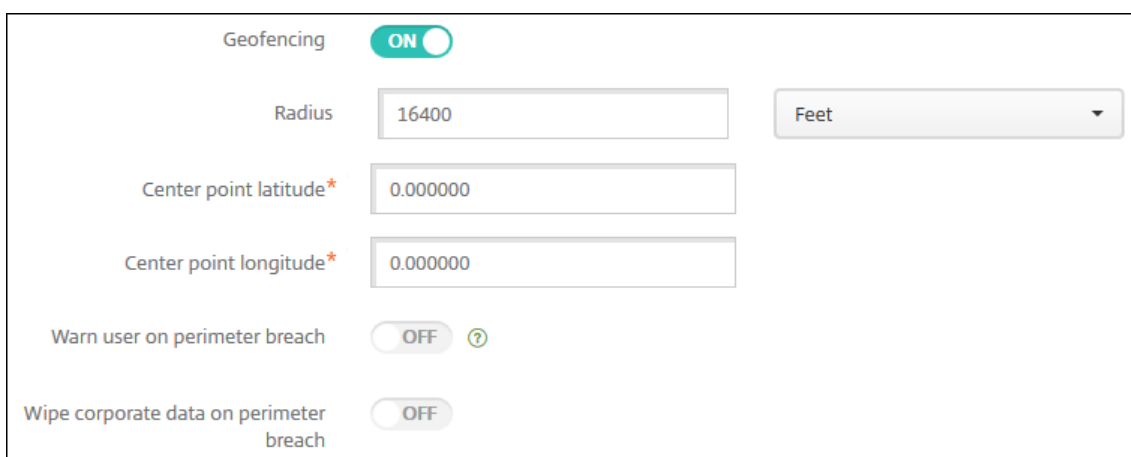
Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

Location Policy	
1 Policy Info	Location Policy This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.
2 Platforms	Device agent configuration
<input checked="" type="checkbox"/> iOS	Location Timeout: 1 Minutes
<input type="checkbox"/> Android	Tracking duration: 6 Hours
<input type="checkbox"/> Android Enterprise	Accuracy: 328 Feet
3 Assignment	Report if Location Services are disabled: OFF
	Geofencing: OFF

- **Tiempo de espera de la localización:** Escriba un número y haga clic en **Segundos** o **Minutos** para definir la frecuencia con que Citrix Endpoint Management intenta establecer la ubicación del dispositivo. Los valores válidos varían entre 60 y 900 segundos o entre 1 y 15 minutos. El valor predeterminado es **1 minuto**.
- **Duración del seguimiento:** Escriba un número y haga clic en **Horas** o **Minutos** para definir la duración con que Citrix Endpoint Management realiza el seguimiento del 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 haga clic en **Metros**, **Pies** o **Yardas**, la precisión con que Citrix Endpoint Management realiza el seguimiento del dispositivo. Los valores válidos son de 10 a 5000 yardas, de 30 a 15 000 pies o de 10 a 5000 metros. El valor predeterminado es **328 pies (100 metros)**.
- **Notificar si los servicios de localización están inhabilitados:** Seleccione esta opción si quiere que el dispositivo envíe un informe a Citrix Endpoint Management cuando el usuario desactive el GPS. El valor predeterminado es **Desactivado**.
- **Geocerca**



Geofencing ☒

Radius Feet

Center point latitude*

Center point longitude*

Warn user on perimeter breach ☐ ?

Wipe corporate data on perimeter breach ☐

Al habilitar Geocercas, configure estos parámetros:

- **Radio:** Escriba un número y haga clic en las unidades que se van a utilizar para medir el radio. El valor predeterminado es **16400 pies (5000 metros)**. Los valores válidos para el radio del perímetro son:
 - De 164 a 16 400 pies
 - De 50 a 50 000 metros
 - De 54 a 54 680 yardas
 - 1–31 millas
- **Latitud del punto central:** Escriba una latitud (por ejemplo, 37.787454) para definir la latitud del punto central de la geocerca.
- **Longitud del punto central:** Escriba una longitud (por ejemplo, 122.402952) para definir la longitud del punto central de la geocerca.
- **Advertir al usuario cuando salga del perímetro:** Seleccione si emitir un mensaje de advertencia cuando los usuarios abandonen el perímetro definido. El valor predeterminado es **Desactivado**. No se requiere conexión alguna a Citrix Endpoint Management para mostrar el mensaje de advertencia.
- **Borrar datos de empresa si sale del perímetro.** Seleccione si borrar los datos de los dispositi-

tivos de los usuarios cuando estos abandonen el perímetro. El valor predeterminado es **Desactivado**. Si habilita esta opción, aparecerá el campo **Demora del borrado local**.

- Escriba un número y haga clic en **Segundos** o **Minutos** para establecer el tiempo de demora antes de eliminar los datos de empresa que contengan los dispositivos de los usuarios. Esta demora ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que Citrix Endpoint Management borre sus dispositivos de manera selectiva. El valor predeterminado es de **0 segundos**.

Parámetros de Android (AD heredado)

El seguimiento de la ubicación de Android requiere Android 9 o una versión posterior.

Location Policy

This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.

1 Policy Info

2 Platforms [Clear All](#)

☐ iOS

☒ **Android**

☐ Android Enterprise

3 Assignment

Device agent configuration

Poll interval: 15 Minutes

Report if Location Services is disabled: ☐ OFF

Geofencing: ☐ OFF

Enable Tracking: ☐ OFF

Deployment Rules

- **Intervalo de sondeo:** Escriba un número y haga clic en **Minutos**, **Horas** o **Días** para definir la frecuencia con que Citrix Endpoint Management intentará establecer la ubicación del dispositivo. Los valores válidos varían entre 15 y 1440 minutos o entre 1 y 24 horas, o bien se puede indicar cualquier cantidad de días. El valor predeterminado es **15 minutos**.
- **Notificar si los servicios de localización están inhabilitados:** Seleccione esta opción si quiere que el dispositivo envíe un informe a Citrix Endpoint Management cuando el usuario desactive el GPS. El valor predeterminado es **Desactivado**.
- **Geocerca**

Geofencing ☒ ON

Radius: 16400 Feet

Center point latitude *: 0.000000

Center point longitude *: 0.000000

Warn user on perimeter breach: ☐ OFF

Device connects to Endpoint Management for policy refresh

☒ Perform no action on perimeter breach

☐ Wipe corporate data on perimeter breach

☐ Lock device locally

Al habilitar Geocercas, configure estos parámetros:

- **Radio:** Escriba un número y haga clic en las unidades que se van a utilizar para medir el radio. El valor predeterminado es **16400 pies (5000 metros)**. Los valores válidos para el radio del perímetro son:
 - De 164 a 164 000 pies
 - De 1 a 50 kilómetros
 - De 50 a 50 000 metros
 - De 54 a 54 680 yardas
 - 1–31 millas
- **Latitud del punto central:** Escriba una latitud (por ejemplo, 37.787454) para definir la latitud del punto central de la geocerca.
- **Longitud del punto central:** Escriba una longitud (por ejemplo, 122.402952) para definir la longitud del punto central de la geocerca.
- **Advertir al usuario cuando salga del perímetro:** Seleccione si emitir un mensaje de advertencia cuando los usuarios abandonen el perímetro definido. El valor predeterminado es **Desactivado**. No se requiere conexión alguna a Citrix Endpoint Management para mostrar el mensaje de advertencia.
- **El dispositivo se conecta a Citrix Endpoint Management para actualizar directivas:** Seleccione una de las opciones siguientes para el momento en que los usuarios abandonen el perímetro:
 - **No realizar ninguna acción si sale del perímetro.** No hacer nada. Esta es la opción predeterminada.
 - **Borrar datos de empresa si sale del perímetro.** Borrar datos empresariales del dispositivo una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparecerá el campo **Demora del borrado local**.
 - ★ Escriba un número y haga clic en **Segundos** o **Minutos** para establecer el tiempo de demora antes de eliminar los datos de empresa que contengan los dispositivos de los usuarios. Esta demora ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que Citrix Endpoint Management borre sus dispositivos de manera selectiva. El valor predeterminado es de **0 segundos**.
 - **Bloquear dispositivo localmente:** Bloquear los dispositivos de los usuarios una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparecerá el campo **Demora del bloqueo**.
 - ★ Escriba un número y haga clic en **Segundos** o **Minutos** para establecer el tiempo de demora antes de bloquear los dispositivos de los usuarios. Esta demora ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que Citrix Endpoint Management bloquee sus dispositivos. El valor predeterminado es de **0 segundos**.

- **Habilitar seguimiento:** Seleccione si el dispositivo realizará un seguimiento de la ubicación del usuario. El valor predeterminado es **Desactivado**.

Parámetros de Android Enterprise

Para que el seguimiento de ubicación de Android funcione, asegúrese de que se cumplen los siguientes requisitos:

- Android 9 o una versión posterior
- El parámetro Permitir compartir ubicaciones está habilitado en la directiva Restricciones para Android Enterprise
- Programación de conexiones (se recomienda Firebase Cloud Messaging)

The screenshot shows the 'Device Policies' section in the Citrix Endpoint Management console. The 'Location Policy' is selected, and the 'Android Enterprise' platform is chosen. The configuration includes options for 'Apply To COPE' (OFF), 'Managed device' (Location Mode: Off), 'Managed profile' (Report if Location Services is disabled: OFF, Geofencing: OFF), and a 'Deployment Rules' link.

Device Policies	Apps	Media	Actions	Content Collaboration	Enrollment Profiles	Delivery Groups
Location Policy This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.						
1 Policy Info						
2 Platforms Select All						
<input type="checkbox"/> iOS						
<input type="checkbox"/> Android (legacy DA)						
<input checked="" type="checkbox"/> Android Enterprise						
3 Assignment						
Location Policy Apply To COPE <input type="checkbox"/> OFF						
Managed device Location Mode <input type="text" value="Off"/> ?						
Managed profile Report if Location Services is disabled <input type="checkbox"/> OFF						
Geofencing <input type="checkbox"/> OFF						
► Deployment Rules						

Aplicar a dispositivos totalmente administrados con un perfil de trabajo

Para dispositivos totalmente administrados con perfiles de trabajo (conocidos anteriormente como dispositivos COPE), solo está disponible el parámetro de modo de ubicación.

- **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa:** Le permite configurar el modo de ubicación para dispositivos totalmente administrados con perfiles de trabajo. Cuando este parámetro está activado, configure los parámetros del perfil de trabajo:
 - **Notificar si los servicios de localización están inhabilitados:** Seleccione esta opción si quiere que el dispositivo envíe un informe a Citrix Endpoint Management cuando el usuario desactive el GPS. El valor predeterminado es **Desactivado**.
 - **Geocerca:** Consulte los parámetros del apartado Dispositivo administrado en este artículo.

Cuando **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa** está desactivado, los parámetros se aplican al dispositivo administrado y al perfil de trabajo, como se muestra en las secciones siguientes. El valor predeterminado es **Desactivado**.

Dispositivo administrado

- **Modo de ubicación:** Especifique el grado de detección de la localización que se va a habilitar. Puede utilizar la acción de seguridad Localizar solamente cuando el modo de ubicación esté establecido en **Alta precisión** o **Ahorro de batería**. El valor predeterminado es **Alta precisión**.
 - **Alta precisión:** Permite todos los métodos de detección de la ubicación, incluidos GPS, redes y otros sensores.
 - **Solo sensores:** Habilita solo GPS y otros sensores.
 - **Ahorro de batería:** Habilita solo el proveedor de la ubicación de red.
 - **Desactivado:** Inhabilita la detección de la ubicación.

- **Geocerca:**

Geofencing ☒ ON

Poll interval * 10 Minutes ?

Radius * 16400 Feet ?

Center point latitude * 0.000000

Center point longitude * 0.000000

Warn user on perimeter breach ☐ OFF ?

Device connects to Endpoint Management for policy refresh

- ☒ Perform no action on perimeter breach
- ☐ Wipe corporate data on perimeter breach
- ☐ Lock device locally

Al habilitar **Geocercas**, configure estos parámetros:

- **Intervalo de sondeo:** Escriba un número y haga clic en **Minutos**, **Horas** o **Días** para definir la frecuencia con que Citrix Endpoint Management intentará establecer la ubicación del dispositivo. Los valores válidos varían entre 1 y 1440 minutos o entre 1 y 24 horas, o bien se puede indicar cualquier cantidad de días. El valor predeterminado es **10 minutos**. Si este valor es menos de 10 minutos, puede afectar de forma negativa a la duración de la batería del dispositivo.

- **Radio:** Escriba un número y haga clic en las unidades que se van a utilizar para medir el radio. El valor predeterminado es **16400 pies (5000 metros)**. Los valores válidos para el radio del perímetro son:
 - De 164 a 164 000 pies
 - De 1 a 50 kilómetros
 - De 50 a 50 000 metros
 - De 54 a 54 680 yardas
 - 1–31 millas
- **Latitud del punto central:** Escriba una latitud (por ejemplo, 37.787454) para definir la latitud del punto central de la geocerca. 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 indica la ubicación del dispositivo en la página **Detalles del dispositivo > General**, en la sección **Seguridad**.
- **Longitud del punto central:** Escriba una longitud (por ejemplo, 122.402952) para definir la longitud del punto central de la geocerca.
- **Advertir al usuario cuando salga del perímetro:** Seleccione si emitir un mensaje de advertencia cuando los usuarios abandonen el perímetro definido. El valor predeterminado es **Desactivado**. No se requiere conexión alguna a Citrix Endpoint Management para mostrar el mensaje de advertencia.
- **El dispositivo se conecta a Citrix Endpoint Management para actualizar directivas:** Seleccione una de las opciones siguientes para el momento en que los usuarios abandonen el perímetro:
 - **No realizar ninguna acción si sale del perímetro.** No hacer nada. Este es el valor predeterminado.
 - **Borrar datos de empresa si sale del perímetro.** Borrar datos empresariales del dispositivo una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparecerá el campo **Demora del borrado local**.
 - * Escriba un número y haga clic en **Segundos** o **Minutos** para establecer el tiempo de demora antes de eliminar los datos de empresa que contengan los dispositivos de los usuarios. Esta demora ofrece a los usuarios la oportunidad de volver a la ubicación permitida antes de que Citrix Endpoint Management borre sus dispositivos de manera selectiva. El valor predeterminado es de **0 segundos**.
 - **Bloquear dispositivo localmente:** Bloquear los dispositivos de los usuarios una vez transcurrido un período de tiempo especificado. Si habilita esta opción, aparecerá el campo **Demora del bloqueo**.
 - * Escriba un número y haga clic en **Segundos** o **Minutos** para establecer el tiempo de demora antes de bloquear los dispositivos de los usuarios. Esta demora ofrece a los

usuarios la oportunidad de volver a la ubicación permitida antes de que Citrix Endpoint Management bloquee sus dispositivos. El valor predeterminado es de **0 segundos**.

Perfil de trabajo

- **Notificar si los servicios de localización están inhabilitados:** Seleccione esta opción si quiere que el dispositivo envíe un informe a Citrix Endpoint Management cuando el usuario desactive el GPS. El valor predeterminado es **Desactivado**.
- **Geocerca:** Consulte los parámetros del apartado Dispositivo administrado en este artículo.

Directiva de mensaje de pantalla bloqueada

December 6, 2021

La directiva “Mensaje de pantalla bloqueada” permite establecer mensajes para que aparezcan en estos dispositivos iOS si se pierden:

- La ventana de inicio de sesión en iPads compartidos
- La pantalla de bloqueo en dispositivos iOS supervisados

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Datos de la etiqueta de inventario del dispositivo:** Etiqueta de inventario del dispositivo. Los dispositivos Apple truncan las cadenas largas, así que debe verificar las cadenas antes de implementar la directiva en producción. La longitud de las cadenas depende del modelo del dispositivo Apple y de la configuración de Apple, que puede cambiar.
- **Nota al pie en la ventana de inicio de sesión y en la pantalla bloqueada:** Información de ayuda para devolver el dispositivo, como una dirección u otros datos de contacto. Por ejemplo, su mensaje puede tener el formato “Si encuentra este dispositivo, devuélvalo a”. Los dispositivos Apple truncan las cadenas largas, así que debe verificar las cadenas antes de implementar la directiva en producción. La longitud de las cadenas depende del modelo del dispositivo Apple y de la configuración de Apple, que puede cambiar.
- **Configuraciones de directivas**

- **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Directiva de correo

November 29, 2023

En Citrix Endpoint Management, puede agregar una directiva de dispositivo 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](#).

Parámetros de iOS y macOS

Mail Policy	
1 Policy Info	
2 Platforms Select All	
<input checked="" type="checkbox"/> iOS	
<input type="checkbox"/> macOS	
3 Assignment	

Allow Mail Drop ☐ OFF iOS 9.2+

Enable S/MIME Signing ☒ ON iOS 10.3+

Signing identity credential

None

 iOS 5.0+

S/MIME Signing User Overrideable ☐ OFF iOS 12.0+

S/MIME Signing Certificate UUID User Overrideable ☐ OFF iOS 12.0+

Enable S/MIME Encryption ☒ ON iOS 10.3+

Encryption identity credential

None

 iOS 5.0+

Enable per message S/MIME switch ☐ OFF

S/MIME Encrypt By Default User Overrideable ☐ OFF iOS 12.0+

S/MIME Encryption Certificate UUID User Overrideable ☐ OFF iOS 12.0+

- **Descripción de la cuenta.** Indique una descripción de la cuenta. Esta descripción aparece en las aplicaciones Correo y Ajustes. Este campo es obligatorio.

- **Tipo de cuenta.** Elija **IMAP** o **POP** para seleccionar el protocolo que se va a usar para las cuentas de usuario. El valor predeterminado es **IMAP**. Si selecciona **POP**, desaparece la opción **Prefijo de ruta**.
- **Prefijo de ruta.** Escriba **Bandeja de entrada** o introduzca el prefijo de la ruta de su cuenta de correo electrónico IMAP. Este campo es obligatorio.
- **Nombre simplificado de usuario.** Escriba el nombre de usuario completo que se va a usar para los mensajes, entre otros. Este campo es obligatorio.
- **Correo electrónico.** Escriba la dirección de correo electrónico completa de la cuenta. Este campo es obligatorio.
- **Configuración de correos electrónicos entrantes**
 - **Nombre de host del servidor de correo.** Escriba el nombre del host o la dirección IP del servidor de correo entrante. Este campo es obligatorio.
 - **Puerto del servidor de correo.** 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.** En la lista, haga clic en el tipo de autenticación que se va a usar. El valor predeterminado es **Contraseña**. Si se selecciona **Ninguno**, desaparece el campo **Contraseña**.
 - **Contraseña.** Si quiere, escriba una contraseña para el servidor de correo entrante.
 - **Usar SSL.** Seleccione esta opción si el servidor de correo entrante utiliza la autenticación de Secure Sockets Layer (SSL). El valor predeterminado es **Desactivado**.
- **Configuración de correos electrónicos salientes**
 - **Nombre de host del servidor de correo.** Escriba el nombre de host o la dirección IP del servidor de correos salientes. Este campo es obligatorio.
 - **Puerto del servidor de correo.** Escriba el número de puerto del servidor de correo saliente. Si no indica ningún número de puerto, se utiliza el puerto predeterminado para el protocolo especificado.
 - **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 método de autenticación que se va a utilizar. El valor predeterminado es **Contraseña**.
 - **Contraseña.** Si quiere, escriba una contraseña para el servidor de correo saliente.
 - **La contraseña de salida es la misma que la de entrada.** Seleccione si las contraseñas de correo entrante y saliente son iguales. El valor predeterminado es **No**, lo que significa que las contraseñas son diferentes.

- **Usar SSL.** Seleccione esta opción si el servidor de correo saliente utiliza la autenticación de Secure Sockets Layer (SSL). El valor predeterminado es **Desactivado**.

- **Directiva**

- **Autorizar el movimiento de correo entre cuentas:** Seleccione si permitir que los usuarios:
 - * muevan correos electrónicos de esta cuenta a otra
 - * reenvíen correos electrónicos desde otra cuenta
 - * respondan desde otra cuenta.

El valor predeterminado es **Desactivado**.

- **Enviar correo electrónico solo desde aplicación de correo.** Seleccione esta opción para obligar a los usuarios a utilizar la aplicación de correo de iOS para enviar correos electrónicos.
- **Inhabilitar sincronización de correo reciente.** Seleccione esta opción si quiere 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 permitir Apple Mail Drop en dispositivos que ejecutan iOS 9.2 y versiones posteriores. El valor predeterminado es **Desactivado**.
- **Habilitar firma S/MIME:** Seleccione si esta cuenta admite la firma S/MIME. El valor predeterminado es **Activado**. Si se **activa**, aparecen los siguientes campos.
 - * **Credencial de identidad para firma.** Seleccione la credencial de firma que se va a usar.
 - * **Firma S/MIME reemplazable por el usuario:** Si se **activa**, 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 de certificado de firma S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden seleccionar, en la configuración de sus dispositivos, la credencial de firma que se va a usar. El valor predeterminado es **Desactivado**. Esta opción se aplica a iOS 12.0 y versiones posteriores.
- **Habilitar cifrado S/MIME:** Seleccione si esta cuenta admite el cifrado S/MIME. El valor predeterminado es **Desactivado**. Si se **activa**, aparecen los siguientes campos.
 - * **Credencial de identidad para cifrado.** Seleccione la credencial de cifrado que se va a usar.
 - * **Habilitar cambio de opción S/MIME para cada mensaje:** Cuando se **activa**, los usuarios ven una opción para activar o desactivar el cifrado S/MIME para cada mensaje que escriban. El valor predeterminado es **Desactivado**.

- * **Cifrado S/MIME predeterminado reemplazable por el usuario:** Si se **activa**, 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 de certificado de cifrado S/MIME reemplazable por el usuario:** Si se **activa**, los usuarios pueden activar y desactivar el cifrado S/MIME y la identidad del 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.

- **Configuraciones de directivas**

- **Quitar directiva:** Para quitar la directiva más adelante, configure este parámetro para quitarla **en una fecha concreta** o durante una **demora hasta la eliminación (en horas)**.
- **Permitir que el usuario elimine la directiva:** Permite que los usuarios eliminen la directiva de correo **Siempre**, solo con un **Código de acceso requerido** o **Nunca**. Solo disponible para macOS.
- **Ámbito del perfil:** Solo para macOS, elija si la directiva se aplica en el nivel de **usuario** o en todo el **sistema**.

Directiva de configuraciones administradas

March 1, 2024

La directiva Configuraciones administradas controla varias opciones de configuración y restricciones de aplicaciones. Puede crear esta directiva para cada aplicación de Android Enterprise que quiera controlar.

El desarrollador de aplicaciones define las opciones y los textos de ayuda disponibles para la aplicación. Si en un texto de ayuda se menciona el uso de un “valor de plantilla”, use en su lugar la macro correspondiente de Citrix Endpoint Management. Para obtener más información, consulte [Remote configuration overview](#) (en el sitio para desarrolladores de Android) y [Macros](#).

Los parámetros de configuración de una aplicación pueden incluir elementos tales como:

- Parámetros de la aplicación de correo electrónico
- Permitir o bloquear direcciones URL para un explorador web
- Opción para controlar la sincronización del contenido de aplicaciones a través de una conexión móvil o solo mediante una conexión Wi-Fi

Para obtener información sobre la configuración que aparece para las aplicaciones, contacte con el desarrollador de la aplicación.

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 las redes VPN por aplicación

Para crear una red VPN por aplicación para AE, debe seguir otros pasos adicionales, además de configurar la directiva de configuraciones administradas. Además, debe comprobar que se cumplen estos requisitos previos:

- NetScaler Gateway local
- Estas aplicaciones están instaladas en el dispositivo:
 - Citrix SSO
 - Citrix Secure Hub

He aquí un flujo de trabajo general para configurar una VPN por aplicación para dispositivos AE:

1. Configure un perfil de VPN tal y como se describe en este artículo.
2. Configure Citrix ADC para aceptar el tráfico de la VPN por aplicación. Para obtener información detallada, consulte [Configuración de VPN completa en NetScaler Gateway](#).

Limitaciones

Estas limitaciones se aplican a las VPN por aplicación en dispositivos Android 11 o con una versión posterior en el entorno Android Enterprise debido a [restricciones de visibilidad de los paquetes](#) incorporadas en Android 11:

- Si una aplicación que forma parte de la lista de permitidas o denegadas se implementa en un dispositivo después de que se haya iniciado la sesión de VPN, el usuario final deberá reiniciar la sesión de VPN para que la aplicación pueda enrutar su tráfico a través tal sesión de VPN.
- Si se usa una VPN por aplicación a través de una sesión de VPN permanente, después de instalar una nueva aplicación en el dispositivo, el usuario final deberá reiniciar el perfil de trabajo o reiniciar el dispositivo para que el tráfico de la aplicación se enrute a través de la sesión de VPN.

Nota:

Estas limitaciones no se aplican si utiliza Citrix SSO para Android 23.8.1 o una versión posterior. Para obtener más información, consulte [Reinicio automático de VPN permanente](#).

Parámetros de Android Enterprise

Una vez que haya optado por agregar una directiva Configuraciones administradas, aparece un mensaje para seleccionar una aplicación concreta. Si no hay aplicaciones de Android Enterprise agregadas a Citrix Endpoint Management, no podrá continuar.

Después de seleccionar una aplicación, defina las configuraciones de la directiva. Las configuraciones son específicas de cada aplicación.

Android Enterprise Managed Configurations

1 Policy Info

2 Platforms Clear All

☒ Android Enterprise

3 Assignment

Android Enterprise Managed Configurations ×

This policy lets you control a variety of app configuration options and app restrictions. The options available for an app and the tooltips are defined by the app developer. If a tooltip mentions using a "templated value", use the corresponding Endpoint Management macro instead.

Restrictions for importing documents

☐ Box

☐ DropBox

☐ Drive

Restrictions for sharing the DocuSign app

☐ Box

☐ DropBox

☐ Drive

☐ Evernote

Restrictions for sharing envelopes and documents

☐ Box

☐ DropBox

☐ Drive

☐ Evernote

Configurar perfiles de VPN para Android Enterprise

Haga que los perfiles de VPN estén disponibles para los dispositivos Android Enterprise mediante la aplicación Citrix SSO con la directiva Configuraciones administradas.

Comience por agregar Citrix SSO a la consola de Citrix Endpoint Management como una aplicación de la tienda de Google Play. Consulte [Agregar una aplicación de la tienda pública de aplicaciones](#).

Device Policies **Apps** Media Actions ShareFile Enrollment Profiles Delivery Groups

> Apps



Search

Use the [MDX Service](#) on Citrix Cloud to wrap an app for delivery.

Add

Category

Export

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated
<input type="checkbox"/>		Citrix SSO	Public App Store	Default	3/19/19 8:36:03 am	4/9/19 3:25:17 pm
<input type="checkbox"/>		E1-GOOGLE	Enterprise	Default	2/14/19 7:33:58 am	2/14/19 7:33:58 am

Vea este vídeo para obtener más información:



Crear una configuración administrada por Android Enterprise para Citrix SSO

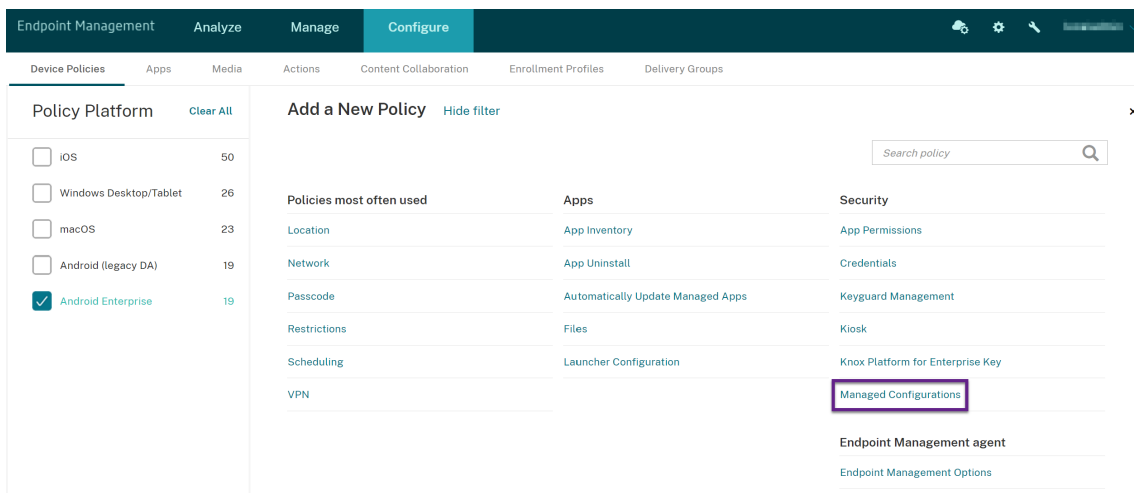
Configure la directiva Configuraciones administradas para que Citrix SSO pueda crear perfiles VPN. Los dispositivos que tienen instalada la aplicación Citrix SSO y la directiva implementada pueden acceder a los perfiles VPN que cree.

Citrix Endpoint Management utiliza el certificado de usuario en el almacén de claves del dispositivo si:

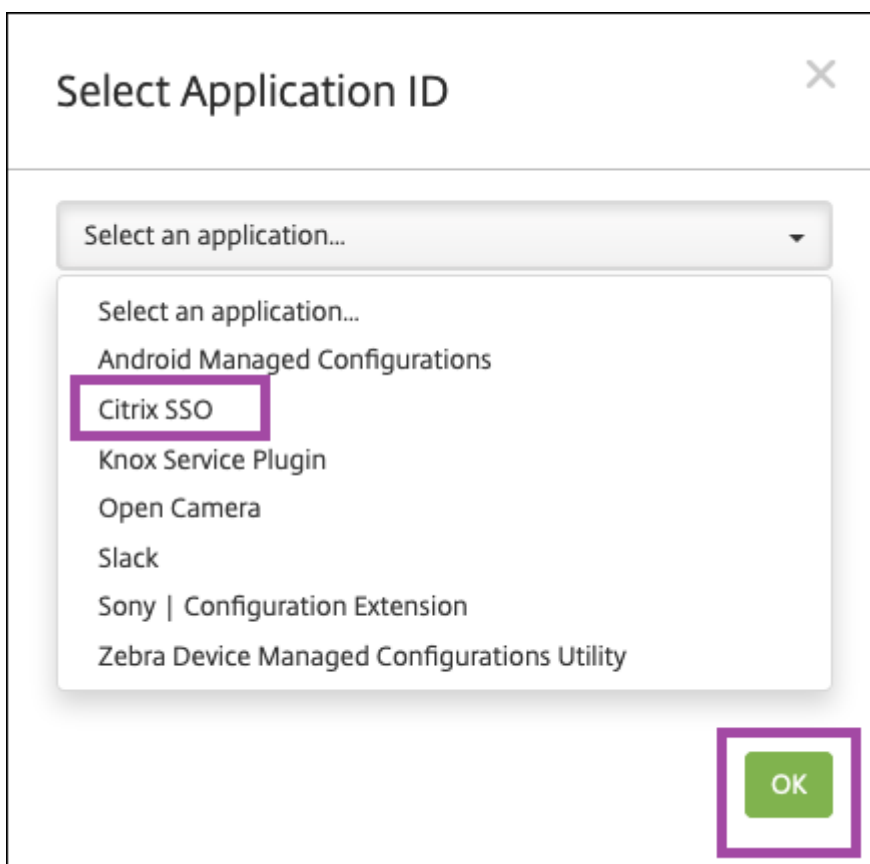
- NetScaler Gateway está configurado para la autenticación por certificados.
- **Entregar certificado de usuario para autenticación** está habilitado en la página **Parámetros > NetScaler Gateway** de Citrix Endpoint Management.

Necesita el FQDN y el puerto de 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 la configuración de la VPN de Citrix SSO. Haga clic en **Siguiente**.

The screenshot shows the Citrix Endpoint Management console. On the left, under 'Android Enterprise Managed Configurations', there are three tabs: '1 Policy Info' (selected), '2 Platforms' (with a 'Clear All' link), and '3 Assignment'. The 'Policy Info' tab is active. The main area is titled 'Policy Information' with the package name 'com.citrix.CitrixVPN'. It contains two fields: 'Policy Name' with the value 'Citrix SSO VPN Configuration' and 'Description' with the value 'VPN Profile'.

5. Configure los parámetros del perfil de VPN.

- **Nombre del perfil VPN:** Escriba un nombre para el perfil VPN. Si va a crear más de un perfil de VPN, utilice un nombre único para cada perfil. Si no proporciona un nombre, la dirección que puso en el campo **Dirección del servidor** se utiliza como nombre del perfil de VPN.
- **Dirección del servidor(*):** Escriba el FQDN de NetScaler Gateway. Si el puerto de NetScaler Gateway no es 443, escriba también el puerto. Utilice un formato de URL. Por ejemplo, <https://gateway.mycompany.com:8443>.
- **Nombre de usuario (opcional):** Indique el nombre de usuario que utilizan los usuarios finales para autenticarse en NetScaler Gateway. Puede utilizar la macro {user.username} de Citrix Endpoint Management para este campo (consulte [Macros](#)). Si usted no proporciona un nombre de usuario, se pedirá a los usuarios que proporcionen uno cuando se conecten a NetScaler Gateway.
- **Contraseña (opcional):** Indique la contraseña que utilizan los usuarios finales para autenticarse en NetScaler Gateway. Si usted no proporciona una contraseña, se pedirá a los usuarios que proporcionen una contraseña 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 Credenciales, la aplicación obtiene el certificado y autentica la VPN sin ninguna acción por parte de los usuarios.
- **Asignaciones de certificados de Gateway (opcional):** Objeto JSON que describe las asignaciones de certificado usadas con NetScaler Gateway. Valor de ejemplo: { "hash-alg": "sha256", "pinset": ["AA", "BB"] }. Para obtener más información, consulte [Fijación de certificados de NetScaler Gateway con Android Citrix SSO](#).

- **Tipo de VPN por aplicación (opcional):** Si utiliza VPN por aplicación para restringir las aplicaciones que usan esta VPN, puede configurar este parámetro. Si selecciona **Permitir**, el tráfico de red de los nombres de paquetes de aplicaciones indicados en la **lista de aplicaciones de Per App VPN** se redirige a través de la VPN. El tráfico de red de todas las demás aplicaciones se redirige fuera de la VPN. Si selecciona **No permitir**, el tráfico de red de los nombres de paquetes de aplicaciones indicados en la **lista de aplicaciones de Per App VPN** se redirige fuera de la VPN. El tráfico de red de todas las demás aplicaciones se redirige a través de la VPN. El valor predeterminado es **Permitir**.
- **Lista de aplicaciones de Per App VPN:** Una lista de aplicaciones cuyo tráfico está permitido o bloqueado en la VPN, en función del valor de **Tipo de VPN por aplicación**. Indique 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 estar escritos en esta lista tal y como lo están en la tienda de Google Play. Esta lista es opcional. Mantenga esta lista vacía para aprovisionar la VPN en todo el dispositivo.
- **Perfil VPN predeterminado:** Escriba el nombre del perfil VPN que quiere utilizar cuando los usuarios toquen el botón de conexión de 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, este se marca como perfil predeterminado. Para la VPN permanente, este campo debe establecerse en el nombre del perfil de VPN que se utilizará para establecer la VPN permanente.
- **Inhabilitar perfiles de usuario:** Si este parámetro está activado, los usuarios no pueden crear sus propias VPN en sus dispositivos. Si este parámetro está desactivado, los usuarios pueden crear sus propias VPN en sus dispositivos. El valor predeterminado es Desactivado.
- **Bloquear servidores que no son de confianza:** Está desactivado en cualquiera de los siguientes casos:
 - Al utilizar un certificado autofirmado para NetScaler Gateway.
 - Cuando el certificado raíz de la entidad de certificación que emite el certificado de NetScaler Gateway no está en la lista de entidades de certificación del sistema.

Si este parámetro está activado, el sistema operativo Android valida el certificado de NetScaler Gateway. Si se produce un error en la validación, no se permite la conexión. Está activado de forma predeterminada.

Android Enterprise Managed Configurations

1 Policy Info

2 Platforms Clear All

☒ Android Enterprise

3 Assignment

Policy Information

com.citrix.CitrixVPN

Policy Name *

Citrix SSO VPN Configuration

Description

VPN Profile

6. También puede crear parámetros personalizados. Se admiten los parámetros personalizados **XenMobileDeviceId** y **UserAgent**. Seleccione la configuración de VPN actual y haga clic en **Agregar**.

Android Enterprise Managed Configurations

1 Policy Info

2 Platforms Clear All

☒ Android Enterprise

Custom Parameters

Add

Delete

Configuration

Click 'Add' to add new Configuration

Nombre del parámetro	Descripción	Valor
XenMobileDeviceId	Este campo es el ID de dispositivo que se utilizará para la comprobación de acceso de red basada en la inscripción de dispositivos en Citrix Endpoint Management. Si Citrix Endpoint Management se inscribe y administra el dispositivo, se permite la conexión VPN. De lo contrario, la autenticación queda denegada al establecer la VPN.	Para que Citrix Endpoint Management determine el estado de inscripción y administración de los dispositivos, el valor de XenMobileDeviceID debe establecerse en <code>DeviceID_\${ device.id }</code> .

Nombre del parámetro	Descripción	Valor
UserAgent	Este texto se agrega al encabezado HTTP User-Agent para realizar una comprobación adicional en NetScaler Gateway. La aplicación Citrix SSO agrega el valor de este texto al encabezado HTTP User-Agent durante la comunicación con NetScaler Gateway.	Escriba el texto que quiere agregar al encabezado HTTP User-Agent. Este texto debe ajustarse a las especificaciones HTTP de User-Agent.
EnableDebugLogging	Habilite los registros de depuración en la aplicación Citrix SSO para ayudar a solucionar los problemas de conectividad de VPN con VPN permanentes. Puede habilitarlos en cualquiera de las configuraciones de VPN administradas. Los registros de depuración surten efecto cuando se procesan las configuraciones administradas.	True: Habilita los registros de depuración. Valor predeterminado: False



Para crear otro parámetro personalizado, haga clic de nuevo en **Agregar**.

7. También puede crear más configuraciones de perfil de VPN. Haga clic en **Agregar** en la lista de configuraciones. Aparecerá una nueva configuración en la lista. Seleccione la nueva configuración y repita el paso 5 y, si quiere, el paso 6.

Android Enterprise
Managed
Configurations

1 Policy Info

2 Platforms Clear All

☒ Android Enterprise

3 Assignment

List of additional VPN profiles

Add

Delete

Configuration-0

VPN Profile Name

Profile2

Server Address(*)

https://gw2.mycompany.com:8443

Username (optional)

Password (optional)

Certificate Alias (optional)

Per-App VPN Type (optional)

Allow

PerAppVPN app list

8. Cuando haya creado todos los perfiles de VPN que quiera, haga clic en **Siguiente**.
9. Configure las reglas de implementación de esta configuración administrada para Citrix SSO.
10. Haga clic en **Guardar**.

Esta configuración administrada para Citrix SSO aparece ahora en la lista de directivas de dispositivo configuradas.

Para habilitar la permanencia de los perfiles de VPN configurados, establezca la [directiva de opciones de Citrix Endpoint Management](#).

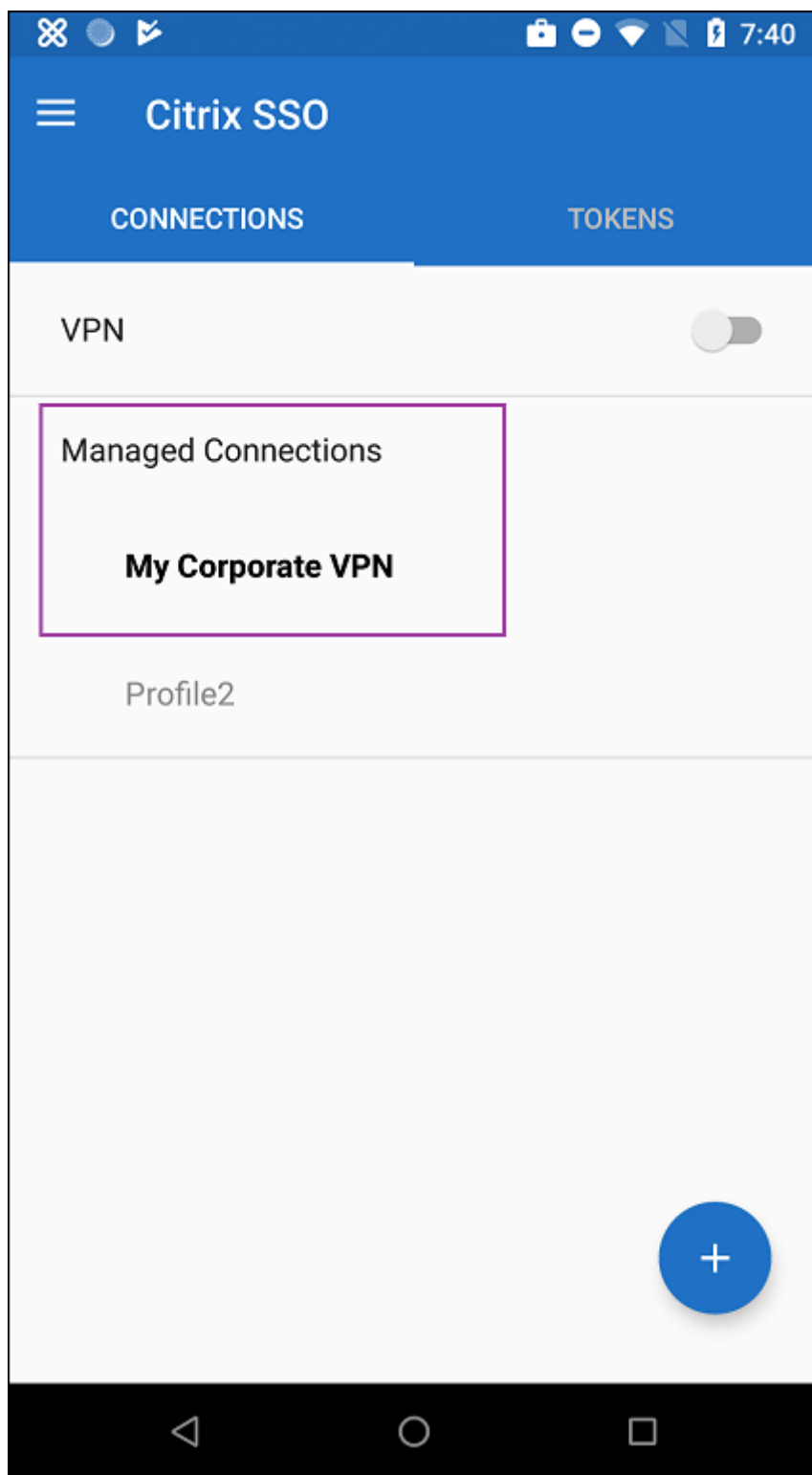
Nota:

Se necesita Citrix Secure Hub 19.5.5 o una versión posterior para la VPN permanente en Android Enterprise.

Acceder a perfiles de VPN desde el dispositivo

Para acceder a los perfiles de VPN creados, los usuarios de Android Enterprise instalan Citrix SSO desde la tienda de Google Play administrada.

Los perfiles de VPN configurados aparecen en el área **Conexiones administradas** de la aplicación. Los usuarios tocan en el perfil de VPN para conectarse a través de ese perfil de VPN.



Después de que los usuarios se hayan autenticado y conectado, aparece una marca de verificación junto al perfil de VPN. El icono con forma de llave indica que la VPN está conectada.

Administrar dispositivos Zebra Android con Zebra OEMConfig

Administre dispositivos Zebra Android con la herramienta administrativa OEMConfig de Zebra Technologies. Para obtener información sobre la aplicación Zebra OEMConfig, consulte el [sitio web de Zebra Technologies](#).

Citrix Endpoint Management es compatible con la versión 9.2 de Zebra OEMConfig y versiones posteriores. Para obtener información sobre los requisitos del sistema para instalar Zebra OEMConfig en dispositivos, consulte [OEMConfig Setup](#) en el sitio web de Zebra Technologies.

Por ahora se admiten estos dispositivos Zebra:

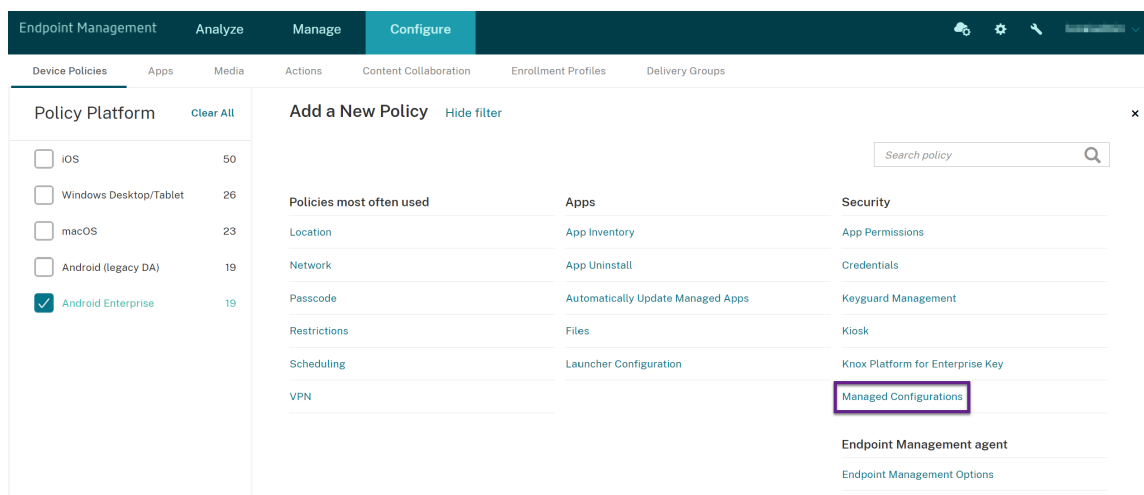
- EC50, EC55, ET56
- TC52x, TC52x-HC
- TC52ax, TC52ax-HC
- TC57x

Para empezar: En la consola de Citrix Endpoint Management, agregue la aplicación Zebra OEMConfig como una aplicación de la tienda de Google Play Store. Consulte [Agregar una aplicación de la tienda pública de aplicaciones](#).

Crear una configuración administrada por Android Enterprise para la aplicación Zebra OEMConfig

Configure la directiva Configuraciones administradas para la aplicación Zebra OEMConfig. Esta directiva se aplica a los dispositivos Zebra que tienen instalada la aplicación Zebra OEMConfig y la directiva implementada.

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 **Zebra OEMConfig powered by MX** de la lista y haga clic en **Aceptar**.
4. Escriba un nombre y una descripción para la 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 desactivar la cámara frontal del dispositivo, seleccione **Camera Configuration** y establezca **Use of Front Camera** en **Off**.
 - Para cambiar el formato de la hora de los dispositivos, seleccione **Clock Configuration** y establezca **Time Format** en **12** (12 horas) o en **24** (24 horas).

Para obtener una lista y descripciones de toda la configuración disponible, consulte [Zebra Managed Configurations](#) en el sitio web de Zebra Technologies.

1. Si quiere, también puede crear más configuraciones de Zebra OEMConfig. Haga clic en **Agregar** en 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 correspondientes, haga clic en **Siguiente**.
3. Configure las reglas de implementación de esta configuración administrada para Zebra OEM-Config.
4. Haga clic en **Guardar**.

Directiva de dominios administrados

December 6, 2021

Puede definir los dominios administrados que se aplicarán al correo electrónico y al explorador web Safari. Los dominios administrados ayudan a proteger la información empresarial porque gestionan las aplicaciones que pueden abrir los documentos descargados desde dominios mediante Safari.

Para dispositivos iOS supervisados, especifique:

- Las direcciones URL o los subdominios para controlar la forma en que los usuarios pueden abrir documentos, datos adjuntos y archivos descargados del explorador web.
- Las direcciones URL desde las que los usuarios pueden guardar contraseñas en Safari.

Para ver los pasos necesarios para poner 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 consta en la lista de dominios administrados de correo electrónico, el mensaje se marca en el dispositivo del usuario para avisarle de que envía un mensaje a una persona fuera del dominio empresarial.

Para elementos como documentos, datos adjuntos o descargas: Cuando un usuario intente abrir un elemento con Safari desde un dominio que no conste en la lista de dominios web administrados, la aplicación empresarial correspondiente abrirá el elemento. Si el elemento no es de un dominio web que conste en la lista de dominios web administrados, el usuario no podrá abrir el elemento con la aplicación empresarial. Deberá usar una aplicación personal no administrada.

Para dispositivos supervisados, incluso si no especifica dominios de relleno automático de contraseñas en 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 dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

Para especificar dominios:

Formato	Descripción
<code>example.com</code>	Toda ruta incluida en <code>example.com</code> se trata como administrada, pero no <code>site.example.com/</code> .
<code>foo.example.com</code>	Toda ruta incluida en <code>foo.example.com</code> se trata como administrada, pero no <code>example.com/</code> ni <code>bar.example.com/</code> .
<code>*.example.com</code>	Toda ruta incluida en <code>foo.example.com</code> o <code>bar.example.com</code> se trata como administrada, pero no <code>example.com/</code> .
<code>example.com/sub</code>	Tanto <code>example.com/sub</code> como toda ruta que incluya se trata como administrada, pero no <code>example.com/</code> .
<code>foo.example.com/sub</code>	Toda ruta incluida en <code>foo.example.com/sub</code> se trata como administrada, pero no <code>example.com</code> , <code>example.com/sub</code> , <code>foo.example.com/</code> ni <code>bar.example.com/sub</code> .
<code>*.example.com/sub</code>	Toda ruta incluida en <code>foo.example.com/sub</code> o <code>bar.example.com/sub</code> se trata como administrada, pero no <code>example.com</code> ni <code>foo.example.com/</code> .

Reglas:

- Las “www” iniciales y las barras diagonales finales de las direcciones URL se omiten cuando se comparan los dominios.
- Si una entrada contiene un número de puerto, solo se consideran administradas las direcciones que especifican ese número de puerto. De lo contrario, solo se consideran administrados los puertos estándar (el puerto 80 para HTTP y el puerto 443 para HTTPS). Por ejemplo, el patrón `*.example.com:8080` coincide con `https://site.example.com:8080/page.html`, pero no `https://site.example.com/page.html`, mientras que el patrón `*.example.com` coincide con `https://site.example.com/page.html` y `https://site.example.com/page.html`, pero no `https://site.example.com:8080/page.html`.
- Las definiciones de dominios web administrados de Safari son acumulativas. Los modelos definidos por todas las cargas útiles de dominios web administrados de Safari se usan para

coincidir con una solicitud de URL.

Parámetros:

- **Dominios administrados**

- **Dominios de correo electrónico no marcados:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir en la lista cada dominio de correo electrónico:
 - * **Dominio de correo electrónico administrado:** Escriba el dominio de correo electrónico.
 - * Haga clic en **Guardar** para guardar el dominio del correo electrónico, o bien haga clic en **Cancelar** para no guardarlo.
- **Dominios web Safari administrados:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir en la lista cada dominio web:
 - * **Dominio web administrado:** Escriba el dominio web.
 - * Haga clic en **Guardar** para guardar el dominio web, o bien haga clic en **Cancelar** para no guardarlo.
- **Dominios de relleno automático de contraseña en Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir en la lista cada dominio de relleno automático:
 - * **Dominio de relleno automático de contraseña en Safari:** Escriba el dominio de relleno automático.
 - * Haga clic en **Guardar** para guardar el dominio de relleno automático, o bien haga clic en **Cancelar** para descartarlo.

- **Configuraciones de directivas**

- **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Directiva de máximo de usuarios residentes

November 29, 2023

La directiva Máximo de usuarios residentes es para dispositivos compartidos con iOS (iPadOS). Para obtener más información acerca de iPads compartidos, consulte [Integrar con funciones de Apple Educación](#).

Esta directiva debe implementarse cuando el iPad se encuentre en la fase “en espera de configuración” del asistente de configuración. Apple no permite que esta directiva se implemente una vez que los iPads compartidos se hayan inscrito.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Máximo de usuarios residentes:** La cantidad máxima de usuarios que pueden tener un iPad compartido. Si la cantidad de usuarios especificada en esta directiva supera la cantidad máxima de usuarios que admite el dispositivo, Citrix Endpoint Management usa la cantidad máxima del dispositivo. El valor predeterminado es **5** usuarios.

Apple recomienda que mantenga el valor de “Máximo de usuarios residentes” lo más bajo posible. Un valor bajo maximiza la cantidad de almacenamiento que podrá ofrecer el iPad a cada usuario. Además, un valor bajo minimiza la comunicación con iCloud y ofrece una experiencia de inicio de sesión más rápida. Para obtener información sobre cómo gestiona Apple el almacenamiento compartido en un iPad, consulte <https://developer.apple.com/education/shared-ipad/>.

The screenshot shows the Citrix Endpoint Management console interface. At the top, there are tabs for 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Device Policies' tab is selected. On the left, there is a sidebar with a list of policy steps: '1 Policy Info', '2 Platforms', '3 Assignment', and '4 Deployment Rules'. The '3 Assignment' step is highlighted in teal. The main content area displays the 'Maximum Resident Users Policy'. It includes a description: 'This policy sets the maximum number of users for a Shared iPad. If the number of users specified in this policy is greater than the maximum number of users supported by the device, the device maximum is used instead. Available in iOS 9.3 and later.' Below this, there is a field labeled 'Maximum resident users *' with a value of '3' entered. To the right of the field is a help icon. At the bottom of the main content area, there is a section titled 'Deployment Rules' with a right-pointing arrow.

Directiva de opciones de MDM

November 29, 2023

Con la directiva “Opciones de MDM”, puede administrar el Bloqueo de activación de Buscar mi iPhone o iPad en dispositivos iOS supervisados. Para ver los pasos necesarios para poner un dispositivo iOS en modo supervisado, consulte [Implementar dispositivos con Apple Configurator 2](#).

El bloqueo de activación es una función de Buscar mi iPhone o iPad que evita la reactivación de un dispositivo supervisado que se haya perdido o haya sido robado. El bloqueo de activación requiere el ID de Apple del usuario y la contraseña para poder desactivar Buscar mi iPhone o iPad, borrar el

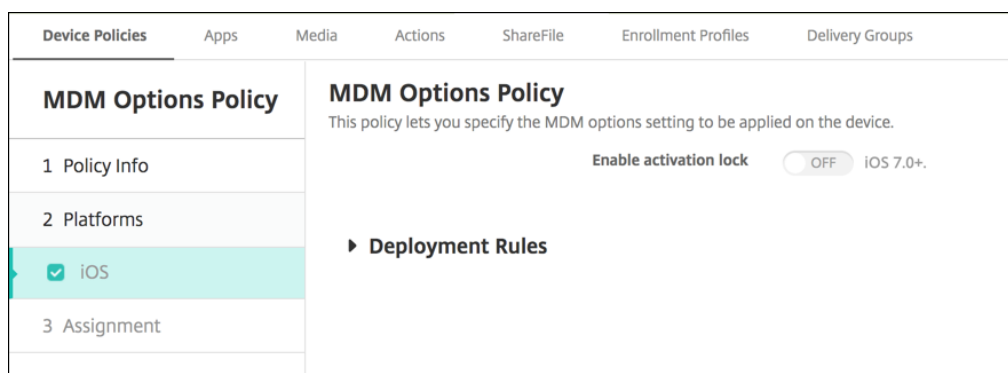
dispositivo o volver a activarlo. Para los dispositivos propiedad de la organización, es necesario omitir un bloqueo de activación para, por ejemplo, restablecer o reasignar dispositivos.

Para habilitar el bloqueo de activación, debe configurar e implementar la directiva 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 en un bloqueo de activación, debe emitir la acción de seguridad “Omisión del bloqueo de activación” desde la consola de Citrix Endpoint Management.

Por ejemplo, si un usuario devuelve un teléfono perdido o si usted quiere configurar uno antes o después de un borrado completo, cuando el teléfono le solicite las credenciales de la cuenta del App Store de Apple, puede omitir ese paso emitiendo la acción de seguridad “Omisión del 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 [Directivas de dispositivo](#).

Parámetros de iOS



- **Habilitar bloqueo de activación:** Seleccione si quiere habilitar la función Bloqueo de activación en los dispositivos en los que se implementará esta directiva. El valor predeterminado es **Desactivado**.

Después de habilitar el bloqueo de activación por haber implementado la directiva de opciones de MDM, la acción de seguridad **Omisión del bloqueo de activación** aparece cuando seleccione esos dispositivos en la página **Administrar > Dispositivos** y haga clic en **Seguridad**. Una omisión del bloqueo de activación permite quitar el bloqueo de activación en dispositivos supervisados antes de la activación del dispositivo sin saber el ID de Apple ni la contraseña de los usuarios de los dispositivos. Puede enviar una omisión del bloqueo de activación a un dispositivo antes o después de un borrado completo. Para obtener información, consulte [Omitir un bloqueo de activación de iOS](#).

Directiva de redes

March 1, 2024

La directiva de redes permite administrar cómo los usuarios conectan sus dispositivos a redes Wi-Fi. Para ello, debe definir los siguientes elementos:

- Tipos y nombres de red
- Directivas de autenticación y seguridad
- Uso de servidor proxy
- Otros datos relacionados con Wi-Fi

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Requisitos previos

Antes de crear una directiva, complete lo siguiente:

- Cree los grupos de entrega que va a utilizar.
- Averigüe el nombre y el tipo de red.
- Averigüe los métodos de autenticación o los tipos de seguridad que va a utilizar.
- Averigüe cualquier información del servidor proxy que pueda necesitar.
- Instalar los certificados de CA necesarios.
- Obtenga todas las claves compartidas necesarias.
- Cree una entidad PKI para la autenticación por certificado.
- Configure proveedores de credenciales.

Para obtener más información, consulte [Autenticación](#) y sus apartados.

Parámetros de iOS

Media

Actions

Content Collaboration

Enrollment Profiles

Delivery Groups

Network

This policy lets you configure a network profile for devices.

Network type

Standard

?

Network name *

?

Hide network

x

iOS 5.0+

Automatically join this wireless network

✓

?

Disable captive network detection

x

?

Use static MAC address

x

?

Security type

None

?

Proxy server settings

Proxy configuration

None

?

QoS settings

Fast Lane QoS marking

Do not restrict QoS marking

?

Policy settings

Remove policy

Select date

Duration until removal (in hours)

Back

Next >

- **Tipo de red:** En la lista, haga clic en **Estándar**, **Hotspot antiguo** o **Hotspot 2.0** para establecer el tipo de red que quiere usar.
- **Nombre de la red:** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo. No se aplica a **Hotspot 2.0**.
- **Ocultar red:** Elija si la red está oculta o no.
- **Conectarse automáticamente a esta red inalámbrica:** Elija si un dispositivo se una a la red automáticamente o no. Si un dispositivo está conectado a otra red, no se une a esta. El usuario debe desconectarse de la red anterior antes de que el dispositivo se pueda conectar automáticamente. El valor predeterminado es **Activado**.

- **Inhabilitar detección de red cautiva:** El asistente de red cautiva ayuda a los usuarios a acceder a redes de suscripción o con puntos de acceso Wi-Fi. Normalmente, estas redes se encuentran en cafeterías, hoteles y otros lugares públicos. Si está **activado**, los dispositivos pueden conectarse a redes cautivas, pero el usuario deberá 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 e iPadOS pueden usar una dirección MAC diferente cada vez que se conectan a una red. Si está **activado**, el dispositivo utiliza siempre la misma dirección MAC cuando se conecta a esta red. Si está **desactivado**, el dispositivo utiliza una dirección MAC diferente cada vez que se conecta a esta red. El valor predeterminado es **Desactivado**.
- **Tipo de seguridad.** En la lista, haga clic en el tipo de seguridad que quiere usar. No se aplica a **Hotspot 2.0**.
 - Ninguna. No requiere ninguna configuración adicional.
 - WEP
 - WPA/WPA2/WPA3 Personal
 - Cualquiera (Personal)
 - WEP Enterprise
 - WPA/WPA2/WPA3 Enterprise: Para la versión más reciente de Windows 10, configure el protocolo SCEP (Simple Certificate Enrollment Protocol) para usar WPA2 Enterprise. Así, 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 en **Parámetros > Proveedores de credenciales**. Para obtener más información, consulte [Proveedores de credenciales](#).
 - Cualquiera (Enterprise)

En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

- **Parámetros del servidor proxy**
 - **Configuración de proxy.** En la lista, elija **Ninguno**, **Manual** o **Automático** para seleccionar cómo se enruta la conexión VPN a través de un servidor proxy y, a continuación, configure las opciones adicionales. El valor predeterminado es **Ninguno**, que no requiere ninguna configuración adicional.
 - Si selecciona **Manual**, configure los siguientes 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:** Si quiere, escriba un nombre de usuario para la autenticación en el servidor proxy.
 - ★ **Contraseña:** Si quiere, escriba una contraseña para la autenticación en el servidor proxy.
- Si hace clic en **Automático**, configure los siguientes parámetros:
 - ★ **URL del servidor:** Escriba la dirección URL del archivo PAC que define la configuración de proxy.
 - ★ **Permitir conexión directa si no se puede acceder al archivo PAC:** Elija si permitir que los usuarios se conecten directamente al destino si no se puede acceder al archivo PAC. El valor predeterminado es **Activado**.
- **Marcado Fastlane QoS:** Si no restringe el marcado QoS en una red Wi-Fi compatible con Cisco Fast Lane QoS, todas las aplicaciones tendrán autorización para usar el marcado L2 y L3. Si quiere restringir el marcado QoS, especifique las aplicaciones que pueden usar marcado L2 y L3.
 - **Habilitar marcado QoS:** Si restringe el marcado QoS, use esta configuración para inhabilitarlo completamente o para incluir solo ciertas aplicaciones. Si está **desactivado**, inhabilita el marcado QoS por completo. Si está **activado**, configure una lista de aplicaciones que pueden usar el marcado QoS. El valor predeterminado es **Activado**.
 - **Permitir llamadas de audio/vídeo de Apple:** Elija si las aplicaciones de llamada de audio y vídeo pueden usar el marcado QoS. Si está **desactivado**, la calidad de las llamadas de audio y vídeo 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.
- **Parámetros de Hotspot 2.0**
 - **Nombre de operador mostrado:** Nombre descriptivo transmitido por el dispositivo Hotspot. Los usuarios pueden ver este nombre en su lista de redes Wi-Fi disponibles.
 - **Nombre de dominio:** El nombre de dominio usado para la negociación de Hotspot 2.0.
 - **Permitir la conexión con redes asociadas de itinerancia:** Si está **activado**, los dispositivos que salen de su red local pueden conectarse a redes asociadas.
 - **Identificadores de organización de Roaming Consortium (OI):** Agregue una lista de identificadores de organización a los que puede acceder el dispositivo. Un identificador de organización (OI) de Roaming Consortium pertenece a una organización con métodos de autenticación compartidos. Si la zona hotspot que configure no está disponible, el dispositivo se conecta a un OI de Roaming Consortium incluido aquí.
 - **Nombres de territorio NAI (Network Access Identifier):** Configure una lista de nombres de territorio utilizados para identificar a los usuarios en una red de roaming. Una NAI transmite en el formato `user@realm`.

- **Códigos MCC (Mobile Country Code) y MNC (Mobile Network Configuration):** Un código MCC consta de tres dígitos que identifican el país de una red. El código MNC consta de 2 o 3 dígitos únicos. Cuando se utilizan conjuntamente, los códigos MCC/MNC identifican de forma única a un operador de red móvil.

- **Configuraciones de directivas**

- **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - ★ **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - ★ **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar 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**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**. No disponible para iOS.

Parámetros de iOS para WPA, WPA Personal, Cualquiera (Personal)

Contraseña: Si quiere, escriba una contraseña. Si deja este campo en blanco, los usuarios pueden recibir un aviso para introducir la contraseña al iniciar sesión.

Parámetros de iOS para WEP Enterprise, WPA Enterprise, WPA2 Enterprise, WPA3 Enterprise, Cualquiera (Enterprise)

Al elegir uno de estos tipos de seguridad, los parámetros de EAP aparecen después de **Parámetros 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 parámetros asociados. Está **desactivado** de forma predeterminada para cada uno de los tipos de EAP disponibles.
- **Autenticación interna (TTLS).** *Solo es necesario cuando se habilita TTLS.* En la lista, seleccione el método de autenticación interna que quiere usar. Las opciones son: **PAP**, **CHAP**, **MSCHAP** o **MSCHAPv2**. El valor predeterminado es **MSCHAPv2**.
- **EAP-FAST con PAC:** Elija si quiere utilizar credenciales de acceso protegido (PAC).
 - Si selecciona **Usar PAC**, elija si quiere usar unas credenciales PAC de aprovisionamiento.

- ★ Si selecciona **Aprovisionar PAC**, elija si quiere permitir un protocolo anónimo de enlace TLS entre el cliente del usuario final y Citrix Endpoint Management.

- **Aprovisionar PAC anónimamente**

- **Autenticación:**

- **Nombre de usuario:** Escriba un nombre de usuario.
- **Contraseña por conexión.** Seleccione si quiere requerir una contraseña cada vez que los usuarios inicien sesión.
- **Contraseña:** Si quiere, escriba una contraseña. Si deja este campo en blanco, los usuarios pueden recibir un aviso para introducir la contraseña al iniciar sesión.
- **Credencial de identidad (PKI o almacén de claves):** En la lista, haga clic en el tipo de credencial de identidad. El valor predeterminado es **Ninguno**.
- **Identidad externa:** Opción *requerida solamente cuando se habilita PEAP, TTLS o EAP-FAST*. Escriba el nombre de usuario que será visible externamente. Puede aumentar la seguridad si escribe un término genérico como “anónimo” para que no pueda verse el nombre del usuario.
- **Requerir certificado TLS.** Elija si quiere requerir un certificado TLS.

- **Confianza**

- **Certificados de confianza.** Para agregar cada certificado de confianza, haga clic en **Agregar** y haga lo siguiente:
 - ★ **Aplicación.** En la lista, elija la aplicación que quiere agregar.
 - ★ Haga clic en **Guardar** para guardar el certificado, o bien en **Cancelar** para cancelar la operación.
- **Nombres de certificado de servidor de confianza.** Para agregar cada nombre común de los certificados de confianza del servidor, haga clic en **Agregar** y haga lo siguiente:
 - ★ **Certificado.** Escriba el nombre del certificado de servidor. Puede usar comodines para especificar el nombre, como wpa*.ejemplo.com.
 - ★ Haga clic en **Guardar** para guardar el nombre del certificado, o bien en **Cancelar** para cancelar la operación.
- **Permitir excepciones en la confianza.** Elija si quiere que el cuadro de diálogo de confianza en el certificado aparezca en los dispositivos de los usuarios cuando un certificado no sea de confianza. El valor predeterminado es **Activado**.

Parámetros de macOS

The screenshot shows the 'Configure' tab in the Citrix Endpoint Management console. On the left, a sidebar lists 'Device Policies' with sub-items: '1 Policy Info', '2 Platforms' (with a 'Clear All' link), and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: 'iOS', 'macOS' (checked), 'Android (legacy DA)', 'Android Enterprise', and 'Windows Desktop/Tablet'. The main area is titled 'Network' and contains the following settings:

- Network:** A dropdown menu set to 'Wi-Fi'.
- Network type:** A dropdown menu set to 'Standard'.
- Network name:** A text input field.
- Hide network:** A toggle switch set to 'Off'.
- Automatically join this wireless network:** A toggle switch set to 'On'.
- Security type:** A dropdown menu set to 'None'.
- Priority:** A text input field set to '0'.
- Proxy server settings:** A section header.
- Proxy configuration:** A dropdown menu set to 'None'.
- Policy settings:** A section header.
- Remove policy:** A button with a circular icon and the text 'Select date'.

- **Red:** En la lista, elija la opción de red que quiere 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, haga clic en **Estándar**, **Hotspot antiguo** o **Hotspot 2.0** para establecer el tipo de red que quiere usar.
- **Nombre de la red:** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo. No se aplica a **Hotspot 2.0**.
- **Ocultar red:** Elija si la red está oculta o no.
- **Conectarse automáticamente a esta red inalámbrica:** Seleccione si se conecta a la red automáticamente o no. Si un dispositivo ya está conectado a otra red, no se une a esta. El usuario debe desconectarse de la red anterior antes de que el dispositivo se pueda conectar automáticamente. El valor predeterminado es **Activado**.
- **Tipo de seguridad.** En la lista, haga clic en el tipo de seguridad que quiere usar. No se aplica a **Hotspot 2.0**.
 - Ninguna. No requiere ninguna configuración adicional.
 - WEP

- WPA o WPA2 Personal
- Cualquiera (Personal)
- WEP Enterprise
- WPA o WPA2 Enterprise
- Cualquiera (Enterprise)

En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

- **Prioridad:** En el caso de varias redes, escriba un número para definir la prioridad de la conexión de red. El dispositivo primero se conecta a la red con el número de prioridad más bajo. Se aceptan números negativos. El valor predeterminado es **0**.

- **Parámetros del servidor proxy**

- **Configuración de proxy.** En la lista, elija **Ninguno**, **Manual** o **Automático** para seleccionar cómo se enruta la conexión VPN a través de un servidor proxy y, a continuación, configure las opciones adicionales. El valor predeterminado es **Ninguno**, que no requiere ninguna configuración adicional.
- Si selecciona **Manual**, configure los siguientes 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:** Si quiere, escriba un nombre de usuario para la autenticación en el servidor proxy.
 - * **Contraseña:** Si quiere, escriba una contraseña para la autenticación en el servidor proxy.
- Si hace clic en **Automático**, configure los siguientes parámetros:
 - * **URL del servidor:** Escriba la dirección URL del archivo PAC que define la configuración de proxy.
 - * **Permitir conexión directa si no se puede acceder al archivo PAC:** Elija si permitir que los usuarios se conecten directamente al destino si no se puede acceder al archivo PAC. El valor predeterminado es **Activado**.

- **Parámetros de Hotspot 2.0**

- **Nombre de operador mostrado:** Nombre descriptivo transmitido por el dispositivo Hotspot. Los usuarios pueden ver este nombre en su lista de redes Wi-Fi disponibles.
- **Nombre de dominio:** El nombre de dominio usado para la negociación de Hotspot 2.0.
- **Permitir la conexión con redes asociadas de itinerancia:** Si está **activado**, los dispositivos que salen de su red local pueden conectarse a redes asociadas.
- **Identificadores de organización de Roaming Consortium (OI):** Agregue una lista de identificadores de organización a los que puede acceder el dispositivo. Un identificador

de organización (OI) de Roaming Consortium pertenece a una organización con métodos de autenticación compartidos. Si la zona hotspot que configure no está disponible, el dispositivo se conecta a un OI de Roaming Consortium incluido aquí.

- **Nombres de territorio NAI (Network Access Identifier):** Configure una lista de nombres de territorio utilizados para identificar a los usuarios en una red de roaming. Una NAI transmite en el formato `user@realm`.
- **Códigos MCC (Mobile Country Code) y MNC (Mobile Network Configuration):** Un código MCC consta de tres dígitos que identifican el país de una red. El código MNC consta de 2 o 3 dígitos únicos. Cuando se utilizan conjuntamente, los códigos MCC/MNC identifican de forma única a un operador de red móvil.

- **Configuraciones de directivas**

- **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar 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**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Parámetros de macOS para WPA, WPA Personal, WPA 2 Personal, Cualquiera (Personal)

- **Contraseña:** Si quiere, escriba una contraseña. Si deja este campo en blanco, los usuarios pueden recibir un aviso para introducir la contraseña al iniciar sesión.

Parámetros de macOS para WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Cualquiera (Enterprise)

- **Modo de conexión:** Si está **activado**, elija el modo de conexión que quiere utilizar cuando el usuario se une a la red. El valor predeterminado es **Desactivado**.
 - **Sistema:** Si esta opción está marcada, el dispositivo utiliza las credenciales del sistema para autenticar al usuario. De forma predeterminado está vacío.

- **Ventana de inicio de sesión:** Si esta opción está marcada, el dispositivo utiliza las mismas credenciales introducidas en la ventana de inicio de sesión para autenticar al usuario. De forma predeterminado está vacío.

Al elegir uno de estos tipos de seguridad, los parámetros de EAP aparecen después de **Parámetros 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 parámetros asociados. Está **desactivado** de forma predeterminada para cada uno de los tipos de EAP disponibles.
- **Autenticación interna (TTLS).** *Solo es necesario cuando se habilita TTLS.* En la lista, seleccione el método de autenticación interna que quiere usar. Las opciones son: **PAP**, **CHAP**, **MSCHAP** o **MSCHAPv2**. El valor predeterminado es **MSCHAPv2**.
- **EAP-FAST con PAC:** Elija si quiere utilizar credenciales de acceso protegido (PAC).
 - Si selecciona **Usar PAC**, elija si quiere usar unas credenciales PAC de aprovisionamiento.
 - ★ Si selecciona **Aprovisionar PAC**, elija si quiere permitir un protocolo anónimo de enlace TLS entre el cliente del usuario final y Citrix Endpoint Management.
 - **Aprovisionar PAC anónimamente**
- **Autenticación:**
 - **Usar autenticación de Active Directory:** Elija si habilitar la autenticación de Active Directory. Disponible para macOS 10.7 y versiones posteriores. Para que esta opción esté disponible, siga estos pasos:
 - ★ Establezca **PEAP** como el protocolo EAP.
 - ★ Establezca el ámbito del perfil en **Sistema**. Puede usar esta opción de configuración solamente al aplicar la directiva a todo el sistema.
 - **Nombre de usuario:** Escriba un nombre de usuario.
 - **Contraseña por conexión.** Seleccione si quiere requerir una contraseña cada vez que los usuarios inicien sesión.
 - **Contraseña:** Si quiere, escriba una contraseña. Si deja este campo en blanco, los usuarios pueden recibir un aviso para introducir la contraseña al iniciar sesión.
 - **Credencial de identidad (PKI o almacén de claves):** En la lista, haga clic en el tipo de credencial de identidad. El valor predeterminado es **Ninguno**.
 - **Identidad externa:** Opción *requerida solamente cuando se habilita PEAP, TTLS o EAP-FAST*. Escriba el nombre de usuario que será visible externamente. Puede aumentar la seguridad si escribe un término genérico como “anónimo” para que no pueda verse el nombre del usuario.

- **Requerir certificado TLS.** Elija si quiere requerir un certificado TLS.
- **Confianza**
 - **Certificados de confianza.** Para agregar cada certificado de confianza, haga clic en **Agregar** y haga lo siguiente:
 - * **Aplicación.** En la lista, elija la aplicación que quiere agregar.
 - * Haga clic en **Guardar** para guardar el certificado, o bien en **Cancelar** para cancelar la operación.
 - **Nombres de certificado de servidor de confianza.** Para agregar cada nombre común de los certificados de confianza del servidor, haga clic en **Agregar** y haga lo siguiente:
 - * **Certificado.** Escriba el nombre del certificado de servidor que quiere agregar. Puede usar comodines para especificar el nombre, como wpa.*.ejemplo.com.
 - * Haga clic en **Guardar** para guardar el nombre del certificado, o bien en **Cancelar** para cancelar la operación.
- **Permitir excepciones en la confianza.** Elija si quiere que el cuadro de diálogo de confianza en el certificado aparezca en los dispositivos de los usuarios cuando un certificado no sea de confianza. El valor predeterminado es **Activado**.

Parámetros de Android Enterprise

The screenshot displays the 'Device Policies' section of the Citrix Endpoint Management console. The 'Network' policy is selected, and the 'Android Enterprise' platform is chosen from the list on the left. The main configuration area shows fields for 'Network name', 'Authentication' (set to 'Open'), 'Encryption' (set to 'WEP'), and 'Password'. There is also a 'Hide network' toggle switch. A 'Deployment Rules' section is visible below the main configuration. At the bottom right, there are 'Back' and 'Next >' buttons.

- **Nombre de la red:** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **Autenticación:** En la lista, elija el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
 - Abierta
 - Compartida

- WPA
- WPA-PSK
- WPA2
- WPA2-PSK
- 802.1x EAP

En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados. El valor predeterminado es **Abierta**.

Parámetros de Android Enterprise para red abierta y compartida

- **Cifrado:** En la lista, elija **Inhabilitado** o **WEP**. El valor predeterminado es **WEP**.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Ocultar red:** Elija si la red está oculta o no.

Parámetros de Android Enterprise para WPA, WPA-PSK, WPA2, WPA2-PSK

- **Cifrado:** En la lista, elija **TKIP** o **AES**. El valor predeterminado es **TKIP**.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Ocultar red:** Elija si la red está oculta o no.

Parámetros de 802.1x para Android Enterprise

- **Tipo de EAP:** En la lista, elija **PEAP**, **TLS** o **TTLS**. El valor predeterminado es **PEAP**.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Autenticación fase 2:** En la lista, elija **Ninguna**, **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 que será visible externamente. Puede aumentar la seguridad si escribe un término genérico como “anónimo” para que no pueda verse el nombre del usuario.
- **Certificado de CA:** En la lista, elija el certificado que se va a utilizar.
- **Dominio:** escriba el nombre de dominio requerido. Para obtener más información, consulte [Dominio](<https://developer.android.com/reference/android/net/wifi/WifiEnterpriseConfig#setDomainSuffix>).

Nota:

Al configurar la directiva de wifi en dispositivos con Android 13 o una versión posterior, es

obligatorio actualizar los campos de **Certificado de CA** y **Dominio**. Si no se actualizan, se producirá un error en la configuración.

- **Credencial de identidad:** En la lista, elija la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
- **Ocultar red:** Elija si la red está oculta o no.

Parámetros de Android (AD heredado)

- **Nombre de la red:** Escriba el SSID que se muestra en la lista de redes disponibles del dispositivo del usuario.
- **Autenticación:** En la lista, elija el tipo de seguridad que se va a utilizar en 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 aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

Parámetros de Android para red abierta y compartida

- **Cifrado:** En la lista, elija **Inhabilitado** o **WEP**. El valor predeterminado es **WEP**.

- **Contraseña:** Si quiere, escriba una contraseña.
- **Ocultar red:** Elija si la red está oculta o no.

Parámetros de Android para WPA, WPA-PSK, WPA2, WPA2-PSK

- **Cifrado:** En la lista, elija **TKIP** o **AES**. El valor predeterminado es **TKIP**.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Ocultar red:** Elija si la red está oculta o no.

Parámetros de Android para 802.1x

- **Tipo de EAP:** En la lista, elija **PEAP**, **TLS** o **TTLS**. El valor predeterminado es **PEAP**.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Autenticación fase 2:** En la lista, elija **Ninguna**, **PAP**, **MSCHAP**, **MSCHAPv2** o **GTC**. El valor predeterminado es **PAP**.
- **Identidad:** Escriba el nombre de usuario y el dominio opcionales.
- **Anónimo:** Escriba el nombre de usuario opcional que será visible externamente. Puede aumentar la seguridad si escribe un término genérico como “anónimo” para que no pueda verse el nombre del usuario.
- **Certificado de CA:** En la lista, elija el certificado que se va a utilizar.
- **Credencial de identidad:** En la lista, elija la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
- **Ocultar red:** Elija si la red está oculta o no.

Parámetros de escritorios y tabletas Windows

The screenshot displays the Citrix Endpoint Management console interface. The top navigation bar includes 'Endpoint Management', 'Analyze', 'Manage', and 'Configure' (highlighted). Below this, a sub-navigation bar lists 'Device Policies', 'Apps', 'Media', 'Actions', 'Content Collaboration', 'Enrollment Profiles', and 'Delivery Groups'. The 'Device Policies' section is expanded, showing a list of policies: '1 Policy Info', '2 Platforms' (with a 'Clear All' link), and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: 'iOS', 'macOS', 'Android (legacy DA)', 'Android Enterprise', and 'Windows Desktop/Tablet' (which is checked and highlighted). The main content area is titled 'Network' and contains the following configuration options:

- Network name:** A text input field.
- Authentication:** A dropdown menu set to 'Open'.
- Hide network:** A toggle switch.
- Connect automatically:** A toggle switch.
- Proxy server settings:**
 - Host name or IP address:** A text input field.
 - Port:** A text input field.
- Deployment Rules:** A link to expand the section.

- **Nombre de la red:** SSID que se muestra en la lista de redes disponibles.
- **Autenticación:** En la lista, haga clic en el tipo de seguridad que se va a utilizar en la conexión Wi-Fi.
 - Abierta
 - WPA Personal
 - WPA2 Personal
 - WPA Enterprise
 - WPA-2 Enterprise: Para la versión más reciente de Windows 10, configure SCEP para que use 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 en Parámetros > Proveedores de credenciales**. Para obtener más información, consulte [Proveedores de credenciales](#).

En las siguientes secciones aparecen las opciones que usted configura para cada uno de los tipos de conexión mencionados.

Parámetros abiertos de Windows 10 y Windows 11

- **Ocultar red:** Elija si la red está oculta o no.
- **Conectar automáticamente:** Elija si establecer conexión con la red de forma automática.

Parámetros de WPA Personal y 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 seleccionado.
- **Ocultar red:** Elija si la red está oculta o no.
- **Conectar automáticamente:** Elija si establecer conexión con la red de forma automática.

Parámetros 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 o no.
- **Conectar automáticamente:** Elija si establecer conexión con la red de forma automática.
- **¿Habilitar SCEP?:** Elija si enviar el certificado a los dispositivos de usuario mediante SCEP.

- **Proveedor de credenciales para SCEP:** En la lista, seleccione el proveedor de credenciales del protocolo SCEP. El valor predeterminado es **Ninguno**.

Directiva de uso de red

November 29, 2023

Puede definir reglas de uso de la red para especificar la forma en que los dispositivos iOS utilizan, por ejemplo, redes de datos móviles. Las reglas se aplican a las aplicaciones administradas y a las tarjetas SIM especificadas. Las aplicaciones administradas son aquellas que se implementan en los dispositivos de los usuarios por medio de Citrix Endpoint Management. No se incluyen en este grupo aquellas aplicaciones que los usuarios descargan directamente a sus dispositivos (sin que se implementen por medio de Citrix Endpoint Management). Tampoco se incluyen las aplicaciones que estaban ya instaladas en los dispositivos cuando estos se inscribieron en Citrix Endpoint Management. Esta directiva se aplica a las tarjetas SIM para dispositivos iOS 13. Se pueden configurar reglas de aplicación, reglas de tarjeta SIM o ambas. Las reglas de tarjeta SIM afectan a todas las aplicaciones administradas en ese dispositivo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Reglas de aplicación**
 - **Permitir itinerancia de datos móviles:** Seleccione si las aplicaciones indicadas pueden usar una conexión de datos móviles durante la itinerancia. El valor predeterminado es **Desactivado**.
 - **Permitir datos móviles:** Seleccione si las aplicaciones especificadas pueden usar la conexión de datos móviles. El valor predeterminado es **Desactivado**.
 - **Coincidencias de identificador de aplicación:** Haga clic en **Agregar** para agregar cada aplicación a la lista y, a continuación, configure lo siguiente:
 - * **Identificador de la aplicación:** Introduzca un identificador de la aplicación.
 - Haga clic en **Guardar** para guardar la aplicación en la lista, o bien haga clic en **Cancelar** para no guardarla.
- **Reglas de SIM**
 - **Directiva de asistencia para Wi-Fi de SIM:** Habilitar la opción **Cambiar de Wi-Fi deficiente** hace que la directiva de asistencia para Wi-Fi cambie de una conexión Wi-Fi defi-

ciente a conexiones móviles de manera más agresiva. Esta configuración puede aumentar el uso de datos móviles y afectar a la duración de la batería.

- **ICCID de las SIM:** Para cada tarjeta SIM que quiera agregar a la lista, haga clic en **Agregar** y, a continuación, configure lo siguiente:

- * **ICCID:** Introduzca el número de 19 o 20 dígitos de la tarjeta SIM que quiere agregar.

Directiva de Office

November 29, 2023

Citrix Endpoint Management permite implementar productos de Microsoft Office 365 mediante el proveedor de servicios de configuración (CSP) de Office. Al configurar la directiva de dispositivos de Office, puede implementar aplicaciones de Microsoft Office en cualquier dispositivo con Windows 10 (versión 1709 o una posterior) o Windows 11.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de escritorios y tabletas Windows

Office

Assign Office 365 apps to windows 10 devices. Supported platforms: Windows 10 1709 and later versions

Choose the product id based on your plan

Product ID: O365ProPlusRetail

Select the Office 365 apps that you want to install as part of the suite

- ☒ Access
- ☒ Excel
- ☒ OneDrive for Business (Groove)
- ☒ OneDrive for Business (Next Gen Sync Client)
- ☒ OneNote
- ☒ Outlook
- ☒ PowerPoint
- ☒ Publisher
- ☒ Skype For Business
- ☒ Word
- ☐ Project Online Desktop Client
- ☐ Visio Pro for Office 365

If you own licenses for these additional Office apps you can also assign them

OS Version: 32-bit

Update channel: Monthly

Properties

Automatically accept the app end user license agreement: ☒ ON

User shared computer activation: ☐ OFF

- **ID de producto:** Seleccione un ID de producto basado en su plan de Office 365. Las opciones son **O365ProPlusRetail**, **O365BusinessRetail** o **O365SmallBusPremRetail**.
- **Aplicaciones de Office 365:** Seleccione las aplicaciones de Office 365 que quiere implementar. De manera predeterminada, se seleccionan todas las aplicaciones.
- **Aplicaciones de Office adicionales:** Si posee licencias para **Project Online Desktop Client** o **Visio Pro para Office 365**, puede seleccionar estas aplicaciones para que se instalen.
- **Versión de Office:** Seleccione si instalar la versión de Office de **32 bits** o de **64 bits**.
- **Canal de actualización:** Elija con qué frecuencia quiere instalar actualizaciones. Las opciones son: **Mensual**, **Mensual (dirigido)**, **Semestral** o **Semestral (dirigido)**.
- **Propiedades:**
 - **Aceptar automáticamente el contrato de licencia del usuario final de la aplicación:** Seleccione **Sí** o **No**. Está **activado** de forma predeterminada.
 - **Activación de equipo de usuario compartido:** Seleccione si el equipo es compartido o no. Las opciones son **Sí** o **No**. Está **desactivado** de forma predeterminada.
- **Idioma de Office:** Office se instala automáticamente en cualquier idioma que ya tenga instalado Windows. Puede seleccionar idiomas adicionales a instalar.

Directiva de información de la organización

November 29, 2023

En Citrix Endpoint Management, puede agregar una directiva de dispositivo para especificar la información de su organización que se utilizará en los mensajes de alerta que envíe 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](#).

Parámetros 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 asistencia de la organización.
- **Correo:** Escriba la dirección de correo electrónico de asistencia.
- **Actividad de la organización:** Escriba una palabra o frase que describa los servicios que administra esa organización.

Directiva de actualización del SO

March 1, 2024

La directiva “Actualización del SO” permite implementar:

- Las actualizaciones más recientes del sistema operativo en dispositivos iOS supervisados.

La directiva “Actualización del SO” solo funciona con dispositivos supervisados e inscritos en el Programa de implementación de Apple.

- Las actualizaciones de software más recientes (de sistema operativo y de aplicaciones) en dispositivos macOS inscritos en el Programa de implementación que ejecutan macOS 10.11.5 y versiones posteriores.

Nota:

Actualmente, Apple limita las actualizaciones del SO a las versiones principales únicamente. Los administradores no tienen permiso para actualizar las versiones secundarias. Para obtener más información, consulte [este artículo](#) de la documentación de Apple.

- Las actualizaciones más recientes del sistema operativo en escritorios y tabletas supervisados con Windows 10 o Windows 11.

También puede utilizar la directiva Actualización del SO para administrar parámetros de la optimización de la entrega para escritorios y tabletas con Windows 10 (versión 1607 o una posterior) o Windows 11. La optimización de distribución (o de entrega) es un servicio de actualización de clientes punto a punto que ofrece Microsoft para las actualizaciones de Windows 10 o 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 al compartir la tarea de descarga entre múltiples dispositivos. Para obtener más información, consulte el artículo [Configurar Optimización de distribución para actualizaciones de Windows 10](#) de Microsoft.

- Las actualizaciones más recientes del sistema operativo en dispositivos Android Enterprise administrados (Android 7.0 y versiones posteriores).

Importante:

La directiva de actualización de SO no le permite inhabilitar completamente las actualizaciones. Para retrasar las actualizaciones hasta 90 días, cree una directiva de restricciones. Consulte [Directiva de restricciones](#).

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

OS update

This policy lets you deploy OS updates. The policy supports supervised devices. Available for: iOS 10.3+. For devices running a version prior to iOS 10.3, this policy supports devices that are both supervised and enrolled with automated device enrollment.

OS update options *

☒ Download only ⓘ

☐ Download and/or install ⓘ

OS update frequency (1-365 days) *

7 ⓘ

OS update version *

☒ Latest version ⓘ

☐ Specified version only ⓘ **iOS 11.3+**

Los siguientes parámetros son para dispositivos supervisados con iOS.

- **Opciones de actualización de SO:** Ambas opciones descargan las actualizaciones más recientes del sistema operativo en los dispositivos supervisados siguiendo la frecuencia de **Frecuencia de actualización de SO**. El dispositivo pide al usuario que instale las actualizaciones. La solicitud sigue visible después de que el usuario desbloquee el dispositivo.

- **Frecuencia de actualización de SO:** Determina la frecuencia con que Citrix Endpoint Management comprueba el estado de las actualizaciones y actualiza el sistema operativo del dispositivo. El valor predeterminado es de **7 días**.
- **Versión de actualización del SO:** Especifica la versión que se usará para actualizar los dispositivos iOS supervisados. El valor predeterminado es **Versión más reciente**.
 - **Versión más reciente:** Seleccione esta opción para actualizar a la versión más reciente del sistema operativo.
 - **Solo la versión especificada:** Seleccione esta opción para actualizar a una versión concreta del sistema operativo y luego escriba el número de versión.

Parámetros de macOS

The screenshot displays the 'Software update' configuration page in the Citrix Endpoint Management console. On the left, under 'OS update', the 'macOS' option is selected. The main panel, titled 'Software update', includes a description: 'This policy deploys the latest OS and app updates to macOS devices. Available for: macOS 10.11.5+'. Below this, several settings are shown with toggle switches and dropdown menus:

- Software update options ***: A dropdown menu set to 'Automatically install macOS updates'.
- Critical updates**: A toggle switch that is turned on (checked).
- Install XProtect, MRT, and GateKeeper automatically**: A toggle switch that is turned on (checked).
- Allow installing macOS pre-release software**: A toggle switch that is turned on (checked).
- Automatically install App Store app updates**: A toggle switch that is turned on (checked).

- **Opciones de actualizaciones de software:** Controla de qué modo los dispositivos macOS comprueban e instalan las actualizaciones. Seleccione entre las siguientes opciones:
 - **Instalar automáticamente actualizaciones de macOS:** Las actualizaciones se descargan e instalan automáticamente.
 - **Descargar nuevas actualizaciones cuando estén disponibles:** Las actualizaciones se descargan, pero deben instalarse manualmente.
 - **Comprobar actualizaciones:** Comprueba si existen actualizaciones, pero no las descarga ni las instala automáticamente.
 - **No comprobar si hay actualizaciones:** No comprueba la existencia de actualizaciones ni las descarga ni las instala automáticamente. Los usuarios aún pueden instalar actualizaciones manualmente.
- **Actualizaciones críticas:** Permite la instalación automática de actualizaciones críticas de macOS.
- **Instalar automáticamente las actualizaciones de XProtect, MRT y Gatekeeper:** Permite a los dispositivos macOS instalar automáticamente actualizaciones del software de seguridad.

- **Permitir la instalación de software de prelanzamiento de macOS:** Permite que los usuarios instalen versiones prelanzamiento del software de macOS.
- **Instalar automáticamente las actualizaciones de aplicaciones de App Store:** Permite que las aplicaciones de App Store se actualicen automáticamente.

Obtener el estado para las acciones de actualización de iOS y macOS

Para iOS y macOS, Citrix Endpoint Management no implementa la directiva Controlar actualización del SO en los dispositivos. En vez de ello, Citrix Endpoint Management utiliza la directiva para enviar estos comandos MDM a los dispositivos:

- Programación del examen de actualizaciones de SO: Solicita que el dispositivo realice un examen exhaustivo para buscar actualizaciones del sistema operativo. (Opcional para iOS)
- Actualizaciones disponibles del sistema operativo: Consulta el dispositivo para obtener una lista de las actualizaciones del sistema operativo disponibles.
- Programación de actualización de SO: Solicita que el dispositivo realice actualizaciones de macOS, actualizaciones de aplicaciones o ambas. Por lo tanto, el sistema operativo del dispositivo determina cuándo descargar o instalar las actualizaciones del sistema operativo y las aplicaciones.

La página **Administrar > Dispositivos > Detalles del dispositivo** muestra el estado de los exámenes programados de actualizaciones del SO, las actualizaciones disponibles del SO y las actualizaciones programadas de macOS y aplicaciones.

Devices	Users	Enrollment Invitations
Device details		
1 General	General Identifiers	
2 Properties	Serial Number	
3 User Properties	IMEI/MEID NONE	
4 Assigned Policies	ActiveSync ID	
5 Apps	WIFI MAC Address	
6 Media	Bluetooth MAC Address	
7 Actions	Device Ownership <input type="radio"/> Corporate <input type="radio"/> BYOD	
8 Delivery Groups	Security	
9 Certificates	Strong ID	
10 Connections	Full Wipe of Device No device wipe.	
	Selective Wipe of Device No device selective wipe.	
	Lock Device No device lock.	
	Schedule OS Update Scan Schedule OS update scan was done at 10/6/17 1:34:53 pm.	
	Available OS Update Available OS update was done at 10/6/17 1:35:10 pm.	
	Schedule OS Update Schedule OS update was done at 10/6/17 1:35:15 pm with the install action "Download and/or install".	
	Next >	

Para obtener más información sobre el estado de las acciones de actualización, vaya a la página **Administrar > Dispositivos > Detalles del dispositivo (Grupos de entrega)**.

Devices

Users

Enrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Assigned Policies

5 Apps

6 Media

7 Actions

8 Delivery Groups

9 Certificates

10 Connections

macos | MacBook

Delivery Groups

Success (1) Pending (0) Failed (0)

Delivery Groups

Time

MacOS DEP DG10/6/17 1:35:28 pm

Showing 1 - 1 of 1 Items

- Details

Status	Action	Channel/User	Date
Success	Get Available OS Update Sent	SYSTEM	10/6/17 1:34:53 pm
Success	Schedule OS Update Scan Acknowledged	SYSTEM	10/6/17 1:34:53 pm
Success	Schedule OS Update Scan Sent	SYSTEM	10/6/17 1:34:53 pm
Success	Software inventory response	macos	10/6/17 1:34:20 pm
Done	Software inventory requested	macos	10/6/17 1:34:20 pm
Success	Mobileconfig response : MacOS DEP Webclip OSX (Profile already installed)	macos	10/6/17 1:34:20 pm

Para obtener más información, como la lista de las actualizaciones disponibles del sistema operativo y el último intento de instalación, vaya a la página **Administrar > Dispositivos > Detalles del dispositivo (Propiedades)**.

Devices	Users	Enrollment Invitations
<div>Device details</div> <div>DEP account nameDEP Account FR</div>		
1 General	<div>DEP profile assigned10/6/17 1:08:16 pm</div>	
2 Properties	<div>DEP profile pushed10/6/17 1:08:16 pm</div>	
3 User Properties	<div>DEP registration by</div>	
4 Assigned Policies	<div>DEP registration date1/20/17 4:42:06 pm</div>	
5 Apps	<div>DescriptionMB 12.0 SPACE GRAY/1.1GHZ/8GB/256GB-FRA</div>	
6 Media	<div>Device modelMacBook</div>	
7 Actions	<div>Device nameFrankD MacBook</div>	
8 Delivery Groups	<div>Model IDMacBook8,1</div>	
9 Certificates	<div>OS Update Install Failure Message</div>	
10 Connections	<div>OS Update Install StatusSuccess</div>	
	<div>OS Update Is CriticalNo</div>	
	<div>OS Update Last Install Attempt10/6/17 1:35:15 pm</div>	
	<div>OS Update VersionmacOS Sierra Update, iTunes</div>	
	<div>Operating system build16B2657</div>	

Devices	Users	Enrollment Invitations
<div>Device details</div> <div>Properties</div>		
1 General	<div>~ Custom</div>	
2 Properties	<div>AutoCheckEnabledtrue</div>	
3 User Properties	<div>AutomaticAppInstallationEnabledfalse</div>	
4 Assigned Policies	<div>AutomaticOSInstallationEnabledfalse</div>	
5 Apps	<div>AutomaticSecurityUpdatesEnabledtrue</div>	
6 Media	<div>BackgroundDownloadEnabledtrue</div>	
7 Actions	<div>CatalogURLhttps://swscan.apple.com/content/catalogs/others/index-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz</div>	
8 Delivery Groups	<div>IsDefaultCatalogtrue</div>	
9 Certificates	<div>PerformPeriodicChecktrue</div>	
10 Connections	<div>PreviousScanDate2017-10-06T11:28:41Z</div>	
	<div>PreviousScanResult0</div>	

Parámetros de tabletas y escritorios Windows

OS update

This policy lets you deploy OS updates to supported, supervised devices.

1 Policy Info

2 Platforms Select All

- ☐ iOS
- ☐ macOS
- ☒ Windows Desktop/Tablet
- ☐ Android Enterprise

3 Assignment

Active hours

Select the active hours mode **Not configured**

Automatic update

Automatic update behavior **Automatically install and restart**

Windows automatic update settings

Scan for app updates from Microsoft update **Not configured**

Specify updates branch **Not configured**

Configure number of days to defer feature updates ☐

Configure number of days to defer quality updates ☐

Pause quality updates **Not configured**

Allow updates only in approval list **Not configured**

- **Seleccionar modo de horas de actividad:** Seleccione un modo para definir las horas de actividad durante las que realizar las actualizaciones de sistema operativo por franja de horas o por horas de inicio y finalización. Puede especificar una franja horaria o una hora de inicio y finalización. Tras seleccionar un modo, aparecerán más parámetros: **Especificar rango máximo de horas de actividad** o **Inicio de las horas de actividad** y **Fin de las horas de actividad**. La opción **No configurada** permite a Windows ejecutar las actualizaciones de SO en cualquier momento. El valor predeterminado es **No configurada**.
- **Comportamiento de actualización automática:** Define el comportamiento a la hora de descargar, instalar y reiniciar el servicio Windows Update en los dispositivos de usuario. El valor predeterminado es **Instalar y reiniciar automáticamente**.
 - **Notificar al usuario antes de descargar la actualización:** Windows notifica a los usuarios cuando hay actualizaciones disponibles. Windows no descarga ni instala automáticamente las actualizaciones. Los usuarios deben iniciar las acciones de descarga e instalación.
 - **Instalar automáticamente y notificarlo para programar el reinicio del dispositivo:** Windows descarga automáticamente las actualizaciones en redes de uso no medido. Windows instala las actualizaciones durante el Mantenimiento automático, cuando el dispositivo no está en uso y está enchufado a la red eléctrica (no consume carga de la batería). Si el Mantenimiento automático no puede instalar las actualizaciones durante dos días, Windows Update las instala inmediatamente. Si la instalación requiere un reinicio, Windows pide al usuario que fije la hora del reinicio. El usuario tiene un máximo de siete días para programar el reinicio. Después de siete días, Windows obliga al dispositivo a reiniciarse. 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.
 - **Instalar y reiniciar automáticamente:** Este es el valor predeterminado. Windows

descarga automáticamente las actualizaciones en redes sin uso medido. Windows instala las actualizaciones durante el Mantenimiento automático, cuando el dispositivo no está en uso y está enchufado a la red eléctrica (no consume carga de la batería). Si el Mantenimiento automático no puede instalar las actualizaciones durante dos días, Windows Update las instala inmediatamente. Si la instalación requiere un reinicio, Windows reinicia automáticamente el dispositivo cuando el dispositivo está inactivo.

- **Instalar automáticamente y reiniciar a una hora especificada:** Si selecciona esta opción, aparecen más parámetros para que indique el día y la hora de reinicio. De forma predeterminada, es a las 3:00 todos los días. La instalación automática ocurre a la hora especificada y el reinicio del dispositivo ocurre tras una cuenta atrás de 15 minutos. Si el usuario tiene la sesión iniciada cuando Windows esté listo para el reinicio, el usuario puede interrumpir la cuenta atrás de 15 minutos para atrasar el reinicio.
 - **Instalar automáticamente y reiniciar sin control por parte del usuario final:** Windows descarga automáticamente las actualizaciones en redes de uso no medido. Windows instala las actualizaciones durante el Mantenimiento automático, cuando el dispositivo no está en uso y está enchufado a la red eléctrica (no consume carga de la batería). Si el Mantenimiento automático no puede instalar las actualizaciones durante dos días, Windows Update las instala inmediatamente. Si la instalación requiere un reinicio, Windows reinicia automáticamente el dispositivo cuando el dispositivo está inactivo. Esta opción también provoca que el panel de control del usuario sea de solo lectura.
 - **Desactivar actualizaciones automáticas:** Las actualizaciones automáticas de Windows se inhabilitan en el dispositivo.
- **Buscar actualizaciones de aplicaciones en Microsoft Update:** Especifica si Windows acepta actualizaciones de otras aplicaciones Microsoft desde el servicio Microsoft Update. El valor predeterminado es **No configurada**.
 - **No configurada:** Utilice esta opción si no quiere configurar el comportamiento. Windows no cambia la interfaz de usuario relacionada en los dispositivos de usuario. Los usuarios pueden aceptar o rechazar las actualizaciones para otras aplicaciones Microsoft.
 - **Sí:** Windows permite que las actualizaciones de las aplicaciones se instalen desde el servicio Windows Update. El parámetro relacionado en el dispositivo del usuario está inactivo, por lo que el usuario no puede modificarlo.
 - **No:** Windows no permite que las actualizaciones de las aplicaciones se instalen desde el servicio Windows Update. El parámetro relacionado en el dispositivo del usuario está inactivo, por lo que el usuario no puede modificarlo.
 - **Especificar rama de actualizaciones:** Especifica la rama del servicio Windows Update que se va a utilizar para las actualizaciones. El valor predeterminado es **No configurada**.
 - **No configurada:** Utilice esta opción si no quiere configurar el comportamiento. Windows no cambia la interfaz de usuario relacionada en los dispositivos de usuario. Los usuarios

pueden elegir la rama del servicio Windows Update.

- **Rama actual:** Windows recibe actualizaciones provenientes de la rama actual (Current Branch). El parámetro relacionado en el dispositivo del usuario está inactivo, por lo que el usuario no puede modificarlo.
- **Rama actual para empresas:** Windows recibe actualizaciones provenientes de la rama actual para empresas (Current Branch for Business). El parámetro relacionado en el dispositivo del usuario está inactivo, por lo que el usuario no puede modificarlo.
- **Configurar cuántos días se pueden posponer las actualizaciones de funciones:** Si tiene el valor **Sí**, Windows pospone las actualizaciones de las funciones durante la cantidad especificada de días; el usuario no puede modificar el parámetro. Cuando tiene el valor **No**, el usuario puede cambiar la cantidad de días que se pospondrán las actualizaciones de las funciones. Está **desactivado** de forma predeterminada.
- **Configurar cuántos días se pueden posponer las actualizaciones de calidad:** Si tiene el valor **Sí**, Windows pospone las actualizaciones de calidad durante la cantidad especificada de días; el usuario no puede modificar el parámetro. Cuando tiene el valor **No**, el usuario puede cambiar la cantidad de días que se pospondrán las actualizaciones de calidad. Está **desactivado** de forma predeterminada.
- **Poner en pausa actualizaciones de calidad:** Especifica si pausar las actualizaciones de calidad durante 35 días. El valor predeterminado es **No configurada**.
 - **No configurada:** Utilice esta opción si no quiere configurar el comportamiento. Windows no cambia la interfaz de usuario relacionada en los dispositivos de usuario. Los usuarios pueden optar por pausar actualizaciones de calidad durante 35 días.
 - **Sí:** Windows pausa la instalación de actualizaciones de calidad desde el servicio Windows Update durante 35 días. El parámetro relacionado en el dispositivo del usuario está inactivo, por lo que el usuario no puede modificarlo.
 - **No:** Windows no pausa la instalación de actualizaciones de calidad desde el servicio Windows Update. El parámetro relacionado en el dispositivo del usuario está inactivo, por lo que el usuario no puede modificarlo.
- **Permitir solo las actualizaciones en la lista de aprobación:** Especifica si se deben instalar solo las actualizaciones que apruebe un servidor MDM. Citrix Endpoint Management no admite la configuración de una lista de actualizaciones aprobadas. El valor predeterminado es **No configurada**.
 - **No configurada:** Utilice esta opción si no quiere configurar el comportamiento. Windows no cambia la interfaz de usuario relacionada en los dispositivos de usuario. Los usuarios pueden elegir las actualizaciones que quieren permitir.
 - **Sí, instalar solo actualizaciones aprobadas:** Permite que solo se instalen las actualizaciones aprobadas.

- **No, instalar todas las actualizaciones aplicables:** Permite que se instalen todas las actualizaciones correspondientes en el dispositivo.
- **Usar servidor de actualización interno:** Especifica si obtener actualizaciones desde el servicio Windows Update o un servidor interno de actualizaciones a través de Windows Server Update Services (WSUS). Si tiene el valor **No**, los dispositivos usan el servicio Windows Update. Si tiene el valor **Sí**, los dispositivos se conectan al servidor WSUS especificado para las actualizaciones. Está **desactivado** de forma predeterminada.
 - **Aceptar actualizaciones firmadas por entidades distintas de Microsoft:** Especifica si aceptar actualizaciones firmadas por entidades de terceros que no sean Microsoft. Esta función requiere que el dispositivo confíe en el certificado de proveedores de terceros. Está **desactivado** de forma predeterminada.
 - **Permitir conexión con el servicio de actualización de Microsoft:** Permite que Windows Update presente en el dispositivo se conecte periódicamente al servicio de actualización de Microsoft, incluso aunque el dispositivo esté configurado para obtener actualizaciones desde un servidor WSUS. Está **activado** de forma predeterminada.
 - **Servidor WSUS:** Especifique la URL del servidor WSUS.
 - **Servidor de intranet alternativo para alojar actualizaciones:** Especifique la URL de un servidor de intranet alternativo para alojar actualizaciones y recibir información.
- **Configurar optimización de la entrega:** Usar o no la optimización de entrega para las actualizaciones de Windows 10 o Windows 11. El valor predeterminado es **Desactivado**.
- **Tamaño de caché:** El tamaño máximo de la memoria caché para la optimización de entrega. Un valor de **0** significa una memoria caché ilimitada. El valor predeterminado es **10 GB**.
- **Permitir caché en nodo homólogo de VPN:** Permite o no que los dispositivos participen en el almacenamiento en caché entre homólogos cuando están conectados a la red del dominio a través de la red VPN. Si tiene el valor **Sí**, el dispositivo puede descargar o cargar a otros dispositivos de red del dominio, ya sea en la red VPN o en la red del dominio corporativo. El valor predeterminado es **Desactivado**.
- **Método de descarga:** El método de descarga que la optimización de entrega puede usar para descargar actualizaciones de Windows, aplicaciones y actualizaciones de aplicaciones. El valor predeterminado es **HTTP combinado con nodos homólogos dentro de la misma NAT**. Las opciones son:
 - **Solo HTTP, sin usar nodos homólogos:** Inhabilita el almacenamiento en memoria caché entre nodos homólogos, pero permite la optimización de entrega para descargar contenido de los servidores Windows Update o Windows Server Update Services (WSUS).
 - **HTTP combinado con nodos homólogos dentro de la misma NAT:** Permite el intercambio entre nodos homólogos en la misma red. El servicio en la nube de Optimización de entrega (o distribución) busca otros clientes que se conectan a Internet mediante la misma IP pública que el cliente de destino. Luego, esos clientes intentan conectarse a otros nodos

homólogos en la misma red mediante su IP de subred privada.

- **HTTP combinado con nodos homólogos en un grupo privado:** Selecciona automáticamente un grupo basándose en el sitio de Servicios de dominio de Active Directory (AD DS) del dispositivo o el dominio en que se autentica el dispositivo. La comunicación con nodos homólogos se produce en subredes internas, entre dispositivos que pertenecen al mismo grupo, incluidos los dispositivos en oficinas remotas.
 - **HTTP combinado con nodos homólogos en Internet:** Habilita las fuentes de nodos homólogos en Internet para la optimización de entrega.
 - **Modo de descarga simple, sin nodos homólogos:** Inhabilita el uso de los servicios de optimización de entrega en la nube. La optimización de entrega cambia a este modo automáticamente cuando los servicios de la optimización de entrega en la nube no están disponibles, no se puede establecer contacto con ellos, o bien cuando el tamaño del archivo de contenido es inferior a 10 MB. En este modo, la optimización de entrega proporciona una experiencia de descarga fiable, sin almacenamiento en caché de los nodos homólogos.
 - **No usar optimización de entrega y usar BITS en su lugar:** Permite a los clientes usar BranchCache. Para obtener más información, consulte el artículo [BranchCache](#) de Microsoft.
- **Ancho de banda máximo para descarga:** El ancho de banda máximo para descargas, en KB/segundo. El valor predeterminado es **0**, lo que significa un ajuste de ancho de banda dinámico.
 - **Porcentaje de ancho de banda máximo para descargas:** El ancho de banda máximo para descargas que la optimización de entrega puede usar en todas las actividades de descarga simultáneas. El valor es un porcentaje del ancho de banda disponible para las descargas. El valor predeterminado es **0**, lo que significa un ajuste dinámico.
 - **Ancho de banda máximo para carga:** El ancho de banda máximo para cargas, en KB/segundo. El valor predeterminado es **0**. Un valor de **0** significa un ancho de banda ilimitado.
 - **Capacidad de carga de datos mensual:** El tamaño máximo, en GB, que la optimización de entrega puede cargar en los nodos homólogos en Internet cada mes natural. El valor predeterminado es 20 GB. Un valor de **0** significa cargas mensuales ilimitadas.

Cómo gestiona Citrix Endpoint Management las actualizaciones aprobadas para escritorios y tabletas Windows

Puede indicar si instalar solo las actualizaciones aprobadas. Citrix Endpoint Management gestiona las actualizaciones de la siguiente manera:

- Cuando se trata de una actualización de seguridad (por ejemplo, definiciones de Windows Defender), Citrix Endpoint Management aprueba automáticamente la actualización y envía un comando de instalación al dispositivo durante la siguiente sincronización.

- Cuando se trata de todos los demás tipos de actualización, Citrix Endpoint Management espera la aprobación de estos antes de enviar el comando de instalación al dispositivo.

Requisitos previos

- Debe cargar el certificado raíz de Microsoft en el servidor Citrix Endpoint Management como un 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 Actualización del SO.
2. Cambie el parámetro Permite **solo las actualizaciones en la lista de aprobación** a **Sí, instalar solo actualizaciones aprobadas**.

Para aprobar una actualización

1. En la directiva Actualización del SO, desplácese hacia abajo hasta la tabla **Actualizaciones pendientes**. Citrix Endpoint Management obtiene las actualizaciones que aparecen en la tabla desde los dispositivos.
2. Busque actualizaciones con un **Estado de aprobación** que sea **Pendiente**.
3. Haga clic en la fila de la actualización que quiere aprobar y, a continuación, haga clic en el icono de modificación de esa fila (en la columna **Agregar**).

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

OS Update policy

1 Policy info

2 Platforms

☐ iOS

☐ macOS

☐ Samsung SAFE

☒ Windows Desktop/Tablet

3 Assignment

Internal update server

Specify updates branch

Not configured

Configure number of days to defer feature updates

Off

Configure number of days to defer quality updates

Off

Pause quality updates

Not configured

Allow updates only in approval list

Yes, install only approved updates

Use internal update server

Off

Windows updates

Pending updates

Update Id	Title	Description	Support info	Approval status	Add
b16fea38-0360-4961-84a8-7e501c1e0334	2017-10 Cumulative Update for Windows 10 Version 1703 for x64-based Systems (KB4013167)	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft knowledge base article. After you install this update, you may have to restart your system.	http://support.microsoft.com/help/4041676	Pending	
87a7129e-b646-4c33-b167-759e3f9e6211	Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - October 2017 (KB890800)	After the download, this tool runs one time to check your computer for infection by specific, prevalent malicious software (including Botnet, Sasser, and Mydoom) and helps remove any infection that is found. If an infection is found, the tool will display a status report the next time that you start your computer. A new version of the tool will be offered every month. If you want to manually run the tool on your computer, you can download a copy from the Microsoft Download Center, or you can run an online version from microsoft.com. This tool is not a replacement for an antivirus product. To help protect your computer, you should use an antivirus product.	http://support.microsoft.com/kb/890800	Pending	
eefca5a7-c854-4d6d-a742-1012a96054f7	2017-10 Security Update for Adobe Flash Player for Windows 10 Version 1703 for x64-based Systems (KB4049179)	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the associated Microsoft knowledge base article. After you install this update, you may have to restart your system.	http://support.microsoft.com/help/4049179	Pending	

4. Para aprobar la actualización, haga clic en **Aprobada** y, a continuación, haga clic en **Guardar**.

Pending updates					
Update Id	Title	Description	Support info	Approval status	
b16fea38-	2017-10 Cumulative Update for Windows 10	A security issue has been identified in a Microsoft software product that could affect your system. You can help protect your system by installing this update from Microsoft. For a complete listing of the issues that are included in this update, see the	http://support.microsoft.com/help/4041676	<input type="radio"/> Pending <input checked="" type="radio"/> Approved	<div>Save Cancel</div>

Nota:

Aunque la tabla “Actualizaciones pendientes” contiene los comandos de agregar y eliminar, esos comandos no producen ningún cambio en la base de datos de Citrix Endpoint Management. Modificar el estado de la aprobación es la única acción disponible para las actualizaciones pendientes.

Para ver el estado de las actualizaciones Windows de un dispositivo, vaya a **Administrar > Dispositivos > Propiedades**.

Windows updates		Add
Update for Adobe Flash Player for Windows 10 Version 1703 for x64-based Systems (KB4051613)	Approved to install	✕
Windows Malicious Software Removal Tool for Windows 8, 8.1, 10 and Windows Server 2012, 2012 R2, 2016 x64 Edition - October 2017 (KB890830)	Approved to install	

Cuando se publica una actualización, el **ID de actualización** aparece en la primera columna con un estado (Correcto o Fallo). Puede crear un informe o una acción automatizada para dispositivos con actualizaciones fallidas. También aparecen la fecha y la hora de la publicación.

Cómo funcionan las actualizaciones para implementaciones nuevas y posteriores El efecto que produce la directiva Actualización del SO difiere según si se trata de una primera implementación en un dispositivo o una implementación posterior (donde el dispositivo ya había obtenido actualizaciones).

- Para que Citrix Endpoint Management consulte las actualizaciones de un dispositivo, debe configurar y asignar a un grupo de entrega al menos una directiva Actualización del SO.

Citrix Endpoint Management envía consultas a un dispositivo para saber si hay actualizaciones que se puedan instalar durante la sincronización MDM de ese dispositivo.

- Una vez implementada la primera directiva Actualización del SO, la lista de actualizaciones Windows está vacía porque ningún dispositivo ha informado aún sobre las actualizaciones que pueda necesitar.
- Cuando los dispositivos que se encuentren en el grupo de entrega asignado informen de actualizaciones necesarias, Citrix Endpoint Management guardará esas actualizaciones en su base de datos. Para aprobar las actualizaciones notificadas, modifique de nuevo la directiva.

La aprobación de las actualizaciones solo se aplica a la directiva que se modifica. Las actualizaciones aprobadas en una directiva no se muestran como aprobadas en otra directiva. La próxima vez que se sincronice el dispositivo, Citrix Endpoint Management le enviará un comando para indicarle que se ha aprobado la actualización.

- Para una segunda directiva Actualización del SO, la lista de actualizaciones ya contiene las actualizaciones guardadas en la base de datos de Citrix Endpoint Management. Deberá aprobar actualizaciones para cada directiva.

Durante cada sincronización de dispositivo, Citrix Endpoint Management envía consultas a ese dispositivo sobre el estado de una actualización aprobada hasta que el dispositivo informe que se ha instalado una actualización. Para las actualizaciones que requieren el reinicio del dispositivo después de instalarse, Citrix Endpoint Management enviará consultas sobre el estado de la actualización hasta que el dispositivo informe que está instalada.

- Citrix Endpoint Management no restringe las actualizaciones que se muestran en la página de configuración de directiva por dispositivo ni por grupo de entrega. Aparecen en la lista todas aquellas actualizaciones sobre las que hayan informado los dispositivos.

Parámetros de Android Enterprise

OS update
This policy lets you control OS updates for work-managed devices. Available for: Android 7.0+.

System update policy: Automatic

Allow over-the-air upgrade: ☒

Control Enterprise FOTA: ☐

Freeze Period: ☒ A 9.0+

Start Date (MM-DD) *: 01-01

End Date (MM-DD) *: 01-30

- **Directiva de actualización del sistema:** Determina cuándo se producen las actualizaciones del sistema. Si habilita el parámetro **Controlar Enterprise FOTA**, las actualizaciones se producen automáticamente, independientemente de la configuración de este parámetro.
 - **Automática:** Las actualizaciones se instalan en cuanto están disponibles.
 - **Intervalo:** Las actualizaciones se instalan automáticamente durante el intervalo de mantenimiento diario, especificado en los campos **Hora de inicio** y **Hora de fin**.
 - * **Hora de inicio:** El inicio del intervalo de mantenimiento, medido en cantidad de minutos (de **0** a **1440**) desde la medianoche según la hora local del dispositivo. El valor predeterminado es **0**.
 - * **Hora de fin:** La finalización del intervalo de mantenimiento, medido en cantidad de minutos (de **0** a **1440**) desde la medianoche según la hora local del dispositivo. El valor predeterminado es **120**.
 - **Posponer:** Permite a los usuarios posponer una actualización hasta 30 días.
 - **Predeterminado:** Establece la directiva de actualización en el valor predeterminado del sistema.

- **Permitir actualización inalámbrica:** Si se inhabilita, los dispositivos de usuario no pueden recibir actualizaciones de software por conexión inalámbrica. El valor predeterminado es **Activado**.
- **Período de congelación:** Si está **activado**, las actualizaciones del sistema operativo no se instalan en el dispositivo durante el intervalo de fechas especificado para las directivas de actualización **Automática**, **Posponer** e **Intervalo**. Solo se puede configurar un período de congelación para un dispositivo. La duración del período de congelación no puede exceder los 90 días.
 - **Fecha de inicio/Fecha de finalización:** El intervalo de fechas en el que las actualizaciones del sistema operativo no se instalan si el **período de congelación** está habilitado.
- **Período de congelación:** Si está **activado**, las actualizaciones del sistema operativo no se instalan en el dispositivo durante el intervalo de fechas especificado para las directivas de actualización **Automática**, **Posponer** e **Intervalo**. Solo se puede configurar un período de congelación para un dispositivo. La duración del período de congelación no puede exceder los 90 días.
 - **Fecha de inicio/Fecha de finalización:** El intervalo de fechas en el que las actualizaciones del sistema operativo no se instalan si el **período de congelación** está habilitado.

Directiva de código de acceso

November 29, 2023

En Citrix Endpoint Management, cree una directiva de código de acceso en función de los requisitos de su empresa. Puede solicitar códigos de acceso en los dispositivos de los usuarios y configurar varias reglas de formatos y de códigos de acceso. Cree directivas para iOS, macOS, Android, Android Enterprise y escritorios y tabletas 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 dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

The screenshot shows the 'Passcode' policy configuration in the Citrix Endpoint Management console. The left sidebar has 'Device Policies' selected, with 'Passcode' as the active policy. The main content area is divided into two sections: 'Passcode requirements' and 'Passcode security'.

Passcode requirements:

- Passcode required:** A toggle switch is turned on.
- Minimum length:** A dropdown menu is set to 6.
- Allow simple passcodes:** A toggle switch is turned on.
- Require characters:** A toggle switch is turned off.
- Minimum number of symbols:** A dropdown menu is set to 0.

Passcode security:

- Device lock grace period:** A dropdown menu is set to Immediately.
- Lock device after inactivity, in minutes:** A dropdown menu is set to None.
- Passcode expiration in days (1-730):** A text input field is set to 0.
- Previous passcodes saved (0-50):** A text input field is set to 0.
- Maximum failed sign-on attempts:** A dropdown menu is set to Not defined.

- **Requerir código de acceso.** Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una directiva de código de acceso para dispositivos iOS. La página se expande para que pueda definir las opciones de configuración de los requisitos de los códigos de acceso, la seguridad de dichos códigos y configuraciones de directiva.
- **Requisitos de código de acceso**
 - **Longitud mínima:** En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
 - **Permitir códigos de acceso sencillos:** Seleccione si permitir códigos de acceso simples. Los códigos de acceso simples constan de conjuntos de caracteres secuenciales o repetidos. El valor predeterminado es **Activado**.
 - **Caracteres requeridos:** Seleccione si se debe requerir que los códigos de acceso contengan al menos una letra. El valor predeterminado es **Desactivado**.
 - **Cantidad mínima de símbolos:** En la lista, haga clic en la cantidad de símbolos que debe contener 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 que debe transcurrir antes de que los usuarios deban introducir un código de acceso para desbloquear un dispositivo bloqueado. El valor predeterminado es **Inmediatamente**.
 - **Bloquear dispositivo tras inactividad:** En el cuadro, introduzca la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor puede variar entre 1 y 15 minutos. Establezca el valor en **Ninguno** para inhabilitar la directiva. El valor predeterminado es **Ninguno**.
 - **Caducidad del código de acceso en días (1-730):** Escriba la cantidad de días tras los que

el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.

- **Contraseñas anteriores guardadas (0-50):** Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es **0**, lo que significa que los usuarios pueden volver a usar las contraseñas.
- **Cantidad máxima de intentos de inicio de sesión fallidos:** En la lista, haga clic en la cantidad de veces que un usuario puede fallar al intentar iniciar sesión.
 - ★ Si establece una cantidad mayor que 6, después del sexto intento, el dispositivo impone una demora entre intentos. La demora aumenta con cada intento fallido. Después del intento final, todos los datos y los parámetros se borran de forma segura.
 - ★ Si establece la cantidad en 6 o menor, el dispositivo se borra sin implementar una demora.
 - ★ Si selecciona **No definido**, después de 6 intentos, los dispositivos imponen un límite de tiempo creciente entre intentos, pero no se borran.

El valor predeterminado es **No definido**.

- **Configuraciones de directivas**

- **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - ★ **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - ★ **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Parámetros de macOS

The screenshot displays the 'Passcode Policy' configuration page in the Citrix Endpoint Management console. The left sidebar contains a navigation menu with the following items: '1 Policy Info', '2 Platforms', '3 Assignment', and '4 Settings'. The '2 Platforms' section is expanded, showing a list of operating systems with checkboxes: 'iOS' (unchecked), 'macOS' (checked), 'Android' (checked), 'Samsung KNOX' (checked), 'Android for Work' (checked), 'Windows Phone' (checked), and 'Windows Desktop/Tablet' (checked). The main content area is titled 'Passcode Policy' and includes a description: 'This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.' Below the description, there is a toggle switch for 'Passcode required' which is currently set to 'OFF'. There is also a text input field for 'Delay after failed sign-on attempts, in minutes'. Under the 'Policy Settings' section, there is a dropdown menu for 'Profile scope' set to 'User' and a label 'macOS 10.7+'. At the bottom, there is a section for 'Deployment Rules'.

- **Requerir código de acceso.** Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una directiva de código de acceso para dispositivos iOS. La página se expande para que pueda definir las opciones de configuración de los requisitos de los códigos de acceso, la seguridad de dichos códigos y configuraciones de directiva.
- Si **Requerir código de acceso** está inhabilitado, junto a **Demora posterior a intentos de inicio de sesión fallidos (minutos)**, escriba la cantidad de minutos de espera antes de permitir que los usuarios vuelvan a introducir sus códigos de acceso.
- Si habilita **Requerir código de acceso**, configure los siguientes parámetros:
- **Requisitos de código de acceso**
 - **Longitud mínima:** En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.
 - **Permitir códigos de acceso sencillos:** Seleccione si permitir códigos de acceso simples. Los códigos de acceso simples constan de conjuntos de caracteres secuenciales o repetidos. El valor predeterminado es **Activado**.
 - **Caracteres requeridos:** Seleccione si se debe requerir que los códigos de acceso contengan al menos una letra. El valor predeterminado es **Desactivado**.
 - **Cantidad mínima de símbolos:** En la lista, haga clic en la cantidad de símbolos que debe contener 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 que debe transcurrir antes de que los usuarios deban introducir un código de acceso para desbloquear un dispositivo bloqueado. El valor predeterminado es **Ninguno**.

- **Bloquear dispositivo tras inactividad:** En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor puede estar entre 1 y 5 minutos. Establezca el valor en **Ninguno** para inhabilitar la directiva. El valor predeterminado es **Ninguno**.
- **Caducidad del código de acceso en días (1-730):** Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
- **Contraseñas anteriores guardadas (0-50):** Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es **0**, lo que significa que los usuarios pueden volver a usar las contraseñas.
- **Cantidad máxima de intentos de inicio de sesión fallidos:** En la lista, haga clic en la cantidad de veces que un usuario puede fallar al intentar iniciar sesión.
 - * Si establece una cantidad mayor que 6, después del sexto intento, el dispositivo impone una demora entre intentos. La demora aumenta con cada intento fallido. Después del intento final, el dispositivo se bloquea.
 - * Si establece la cantidad en 6 o menor, el dispositivo se bloquea sin implementar una demora.
 - * Si selecciona **No definido**, después de 6 intentos, los dispositivos imponen un límite de tiempo creciente entre intentos, pero no se bloquean.

El valor predeterminado es **No definido**.

- **Demora posterior a intentos de inicio de sesión fallidos (minutos):** Introduzca la cantidad de minutos antes de que aparezca la ventana de inicio de sesión después de que un usuario haya alcanzado la cantidad máxima de intentos fallidos.
- **Forzar el restablecimiento de código de acceso:** Si está **desactivado**, no es necesario que los usuarios restablezcan su código de acceso la próxima vez que se autentifiquen después de que su dispositivo haya recibido esta directiva. El valor predeterminado es **Activado**.

• Configuraciones de directivas

- **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar 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**, **Código de acceso requerido** o

Nunca en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.

- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Parámetros de Android (AD heredado)

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
Passcode Policy This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.						
1 Policy Info						
2 Platforms						
<input type="checkbox"/> iOS						
<input type="checkbox"/> macOS						
<input checked="" type="checkbox"/> Android						
<input checked="" type="checkbox"/> Samsung KNOX						
<input checked="" type="checkbox"/> Android for Work						
<input checked="" type="checkbox"/> Windows Phone						
<input checked="" type="checkbox"/> Windows Desktop/Tablet						
3 Assignment						
Passcode Policy This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.						
Passcode Required <input type="checkbox"/> OFF						
Encryption						
Enable encryption <input type="checkbox"/> OFF A 3.0+						
Samsung SAFE						
Use same passcode across all users <input type="checkbox"/> OFF						
► Deployment Rules						

Nota:

El valor predeterminado para Android es **No**.

- **Requerir código de acceso.** Seleccione esta opción para requerir un código de acceso y para mostrar las opciones de configuración de una directiva de código de acceso para dispositivos Android. La página se expande para que pueda definir las opciones de configuración de los requisitos de los códigos de acceso, la seguridad de dichos códigos y el cifrado.
- **Requisitos de código de acceso**
 - **Longitud mínima:** En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es 6.
 - **Reconocimiento biométrico:** Seleccione si habilitar el reconocimiento biométrico. Si habilita esta opción, se oculta el campo Caracteres requeridos. El valor predeterminado es **Desactivado**.
 - **Caracteres requeridos:** En la lista, haga clic en **No hay restricciones, Números y letras, Solo números** o **Solo letras** para configurar la composición de los códigos de acceso. El valor predeterminado es **No hay restricciones**.
 - **Reglas avanzadas.** Seleccione si aplicar reglas avanzadas de códigos de acceso. El valor predeterminado es **Desactivado**.

- Si habilita **Reglas avanzadas**, en cada una de las siguientes listas, haga clic en la cantidad mínima de cada tipo de carácter que un código de acceso debe contener:

- * **Símbolos:** La cantidad mínima de símbolos.
- * **Letras:** La cantidad mínima de letras.
- * **Letras minúsculas:** La cantidad mínima de minúsculas.
- * **Letras mayúsculas:** La cantidad mínima de mayúsculas.
- * **Números o símbolos:** La cantidad mínima de números o símbolos.
- * **Números:** La cantidad mínima de números.

- **Seguridad del código de acceso**

- **Bloquear dispositivo tras inactividad:** En la lista, haga clic en la cantidad de tiempo que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **Ninguno**.
- **Caducidad del código de acceso en días (1-730):** Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
- **Contraseñas anteriores guardadas (0-50):** Introduzca la cantidad de contraseñas utilizadas a guardar. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es **0**, lo que significa que los usuarios pueden volver a usar las contraseñas.
- **Cantidad máxima de intentos de inicio de sesión fallidos.** En la lista, haga clic en la cantidad de veces que un usuario puede fallar al intentar iniciar sesión antes de que se borre el contenido del dispositivo. El valor predeterminado es **No definido**.

- **Cifrado**

- **Habilitar cifrado.** Seleccione si habilitar el cifrado. La opción está disponible independientemente de la opción de configuración **Requerir código de acceso**.

Para cifrar sus dispositivos, los usuarios deben empezar con una batería cargada y mantener el dispositivo enchufado hasta que se haya completado el cifrado. El proceso puede durar una hora como mínimo. Si interrumpen el proceso de cifrado, pueden perder alguno o todos los datos de los dispositivos. Una vez cifrado el dispositivo, el proceso no se puede revertir excepto si se restablece a los valores de fábrica (proceso con el que se borrarán todos los datos hasta entonces almacenados en el dispositivo).

Parámetros de Android Enterprise

Passcode Policy

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock. Note: When devices running Samsung Knox 3.0 are enrolled in work profile mode, device passcode settings for Knox 3.0 and later do not apply to the device passcode, even if you configure them. The descriptions of these settings tell you which ones these are.

Device passcode required ☒ ON

Show apps and shortcuts while passcode is not in compliance ☐ OFF ⓘ

Passcode requirements for device passcode

Minimum length 6

Allow users to make password visible (Knox 3.0+) ☐ OFF ⓘ

Biometric recognition ☐ OFF

Required characters Numbers only

Forbidden Strings (Knox 3.0+) ⓘ

Back Next >

Para dispositivos Android Enterprise, se puede requerir: un código de acceso para el dispositivo, una comprobación de seguridad para el perfil de trabajo de Android Enterprise o ambos.

- **Código de acceso de dispositivo obligatorio:** Requiere un código de acceso en el dispositivo. Cuando esta opción esté **activada**, establezca las configuraciones de **Requisitos del código de acceso del dispositivo** y **Seguridad del código de acceso del dispositivo**. El valor predeterminado es **Desactivado**.
- **Mostrar aplicaciones y accesos directos mientras el código de acceso no cumpla los requisitos:** Cuando este parámetro está **activado**, las aplicaciones y los accesos directos del dispositivo no se ocultan, incluso cuando el código de acceso no cumple los requisitos. Cuando este parámetro está **desactivado**, las aplicaciones y los accesos directos se ocultan cuando el código de acceso no cumple los requisitos. Si se habilita este parámetro, Citrix recomienda crear una acción automatizada para marcar el dispositivo como no conforme cuando el código de acceso no cumpla los requisitos. El valor predeterminado es **Desactivado**.
- **Requisitos del código de acceso del dispositivo:**
 - **Longitud mínima:** Especifica la longitud mínima del código de acceso. El valor predeterminado es 6.
 - **Reconocimiento biométrico:** Permite el reconocimiento biométrico. Si esta opción está **activada**, se oculta el campo **Caracteres requeridos**. El valor predeterminado es **Desactivado**.
 - **Caracteres requeridos:** Especifica los tipos de caracteres necesarios para los códigos de acceso. En la lista, elija **No hay restricciones**, **Números y letras**, **Solo números** o **Solo letras**. Use **No hay restricciones** solo para dispositivos con Android 7.0. Android 7.1 y las versiones posteriores no respetan la configuración **No hay 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 esté **activada**, establezca las configuraciones de **Cantidad mínima de** y **Cantidad máxima de**. Esta configuración no está disponible para dispositivos Android con versiones anteriores a Android 5.0. El valor predeterminado es **Desactivado**.
- **Cantidad mínima de:**
 - * **Símbolos:** Especifica la cantidad mínima de símbolos. El valor predeterminado es **0**.
 - * **Letras:** Especifica la cantidad mínima de letras. El valor predeterminado es **0**.
 - * **Letras minúsculas:** Especifica la cantidad mínima de minúsculas. El valor predeterminado es **0**.
 - * **Letras mayúsculas:** Especifica la cantidad mínima de mayúsculas. El valor predeterminado es **0**.
 - * **Números o símbolos:** Especifica la cantidad mínima de números o símbolos. El valor predeterminado es **0**.
 - * **Números:** Especifica la cantidad mínima de números. El valor predeterminado es **0**.
 - * **Caracteres cambiados:** Para dispositivos con Samsung Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida. Solo para dispositivos totalmente administrados. Esta configuración no se aplica a los dispositivos inscritos como dispositivos de perfil de trabajo. Especifica la cantidad de caracteres que los usuarios deben cambiar de su código de acceso anterior. El valor predeterminado es **0**.
- **Cantidad máxima de:** Para dispositivos con Samsung Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida. Solo para dispositivos totalmente administrados. Esta configuración no se aplica a los dispositivos inscritos como dispositivos de perfil de trabajo.
 - * **Cantidad de veces que puede aparecer un carácter:** Especifica la cantidad máxima de veces que se puede repetir un carácter en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.
 - * **Longitud de la 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 la 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 del dispositivo (a partir de Android 12):**
 - **Aplicar complejidad de 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 o una versión posterior y Citrix Secure Hub 22.9 o una versión posterior.

– **Nivel de complejidad:** Niveles predefinidos de complejidad de contraseñas.

- * **Nada:** No se requiere contraseña.
- * **Baja:** 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 con un mínimo de cuatro números
 - Letras con un mínimo de cuatro caracteres
 - Letras y números con un mínimo de cuatro caracteres
- * **Alta:** Las contraseñas pueden ser:
 - Un PIN sin secuencias repetidas (4444) ni secuencias ordenadas (1234) y con un mínimo de ocho números
 - Letras con un mínimo de seis caracteres
 - Letras y números con un mínimo de seis caracteres

Nota:

Para los dispositivos BYOD, los parámetros del código de acceso, como la longitud mínima, los caracteres obligatorios, el reconocimiento biométrico y las reglas avanzadas, no se aplican a partir de Android 12. En su lugar, utilice la complejidad de códigos de acceso.

• **Seguridad del código de acceso del dispositivo:**

- **Borrar dispositivo después (de los intentos fallidos de inicio de sesión):** Especifica la cantidad máxima de veces que un usuario puede fallar al intentar iniciar sesión antes de que el dispositivo se borre por completo. El valor predeterminado es **No definido**.
 - **Bloquear dispositivo tras inactividad:** Especifica los minutos que un dispositivo puede estar inactivo antes de bloquearse. Establezca el valor en 0 para inhabilitar la directiva.
 - **Caducidad del código de acceso en días (1-730):** Especifica la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
 - **Contraseñas anteriores guardadas (0-50):** Especifica la cantidad de contraseñas utilizadas que se guardan. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es **0**, lo que significa que los usuarios pueden volver a usar las contraseñas.
- **Desafío de seguridad de perfil de trabajo obligatorio:** Habilite esta opción para obligar a los usuarios a completar una comprobación de seguridad si quieren 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 esté **activada**, establezca las configuraciones

de **Requisitos del código de acceso para el desafío de seguridad del perfil de trabajo** y **Seguridad del código de acceso para el desafío de seguridad del perfil de trabajo**. El valor predeterminado es **Desactivado**.

- **Requisitos del 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:** Permite el reconocimiento biométrico. Si esta opción está **activada**, se oculta el campo **Caracteres requeridos**. El valor predeterminado es **Desactivado**.
 - **Caracteres requeridos:** Especifica los tipos de caracteres necesarios para los códigos de acceso. En la lista, elija **No hay restricciones**, **Números y letras**, **Solo números** o **Solo letras**. Use **No hay restricciones** solo para dispositivos con Android 7.0. Android 7.1 y las versiones posteriores no respetan la configuración **No hay 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 esté **activada**, establezca las configuraciones de **Cantidad mínima de** y **Cantidad máxima de**. Esta configuración no está disponible para dispositivos Android con versiones anteriores a Android 5.0. El valor predeterminado es **Desactivado**.
 - **Cantidad mínima de:**
 - * **Símbolos:** Especifica la cantidad mínima de símbolos. El valor predeterminado es **0**.
 - * **Letras:** Especifica la cantidad mínima de letras. El valor predeterminado es **0**.
 - * **Letras minúsculas:** Especifica la cantidad mínima de minúsculas. El valor predeterminado es **0**.
 - * **Letras mayúsculas:** Especifica la cantidad mínima de mayúsculas. El valor predeterminado es **0**.
 - * **Números o símbolos:** Especifica la cantidad mínima de números o símbolos. El valor predeterminado es **0**.
 - * **Números:** Especifica la cantidad mínima de números. El valor predeterminado es **0**.
 - * **Caracteres cambiados:** Para dispositivos con Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida. Especifica la cantidad de caracteres que los usuarios deben cambiar de su código de acceso anterior. El valor predeterminado es **0**.
 - **Cantidad máxima de:** Para dispositivos con Knox 3.0 y versiones posteriores que tengan configurada una clave de licencia Knox válida.
 - * **Cantidad de veces que puede aparecer un carácter:** Especifica la cantidad máxima de veces que se puede repetir un carácter en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.
 - * **Longitud de la secuencia alfabética:** Especifica la longitud máxima de una secuen-

cia alfabética en un código de acceso. El valor predeterminado es **0**, lo que significa que no hay límite máximo.

- * **Longitud de la 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 de códigos de acceso para el desafío de seguridad de los perfil de trabajo (a partir de Android 12):**

- **Aplicar complejidad de 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 o una versión posterior y Citrix Secure Hub 22.9 o una versión posterior.

- **Nivel de complejidad:** Niveles predefinidos de complejidad de contraseñas.

- * **Nada:** No se requiere contraseña.

- * **Baja:** 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 con un mínimo de cuatro números
- Letras con un mínimo de cuatro caracteres
- Letras y números con un mínimo de cuatro caracteres

- * **Alta:** Las contraseñas pueden ser:

- Un PIN sin secuencias repetidas (4444) ni secuencias ordenadas (1234) y con un mínimo de ocho números
- Letras con un mínimo de seis caracteres
- Letras y números con un mínimo de seis caracteres

Nota:

Si habilita la complejidad de códigos 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 contenedor después (de los intentos fallidos de inicio de sesión):** Especifica la cantidad máxima de veces que un usuario puede fallar al intentar iniciar sesión antes de que el perfil de trabajo y sus datos se borren del dispositivo. Los usuarios tienen que reinicializar el perfil de trabajo después del borrado. El valor predeterminado es **No definido**.
- **Bloquear contenedor tras inactividad:** Especifica los minutos que un dispositivo puede estar inactivo antes de bloquear el perfil de trabajo. El valor puede estar comprendido entre 0 y 999 minutos. Establezca el valor en 0 para inhabilitar la directiva.

- **Caducidad del código de acceso en días (1-730):** Especifica la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 1 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
- **Contraseñas anteriores guardadas (0-50):** Especifica la cantidad de contraseñas utilizadas que se guardan. Los usuarios no pueden usar ninguna contraseña que esté incluida en esta lista. Cualquier valor entre 0 y 50 es válido. El valor predeterminado es **0**, lo que significa que los usuarios pueden volver a usar las contraseñas.

Parámetros de escritorios y tabletas Windows

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
Passcode Policy This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.						
<div> <div> 1 Policy Info </div> <div> 2 Platforms </div> <div> <input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Android <input type="checkbox"/> Samsung KNOX <input type="checkbox"/> Android for Work <input checked="" type="checkbox"/> Windows Desktop/Tablet </div> <div> 3 Assignment </div> </div>						
<div> <div> Passcode required <input checked="" type="checkbox"/> ON </div> <div> Passcode security </div> <div> Lock device after (minutes of inactivity) (0-999) <input type="text" value="0"/> </div> <div> Passcode expiration in 0-730 days * <input type="text" value="0"/> </div> <div> Previous passwords saved (0-24) <input type="text" value="0"/> ⓘ </div> <div> Passcode requirements </div> <div> Minimum length <input type="text" value="6"/> </div> <div> Deployment Rules </div> </div>						

- **Código de acceso requerido:** Seleccione esta opción para requerir un código de acceso en los dispositivos de escritorio y tabletas Windows. Está **activado** de forma predeterminada, lo que requiere un código de acceso. La página se contrae y las siguientes opciones desaparecen cuando se inhabilita esta opción de configuración.
- **Seguridad del código de acceso**
 - **Bloquear dispositivo tras inactividad:** Introduzca los minutos que un dispositivo puede estar inactivo antes de bloquearse. El valor predeterminado es **0**.
 - **Caducidad del código de acceso (0-730 días):** Escriba la cantidad de días tras los que el código de acceso caduca. Cualquier valor entre 0 y 730 es válido. El valor predeterminado es **0**, lo que significa que el código de acceso no caduca nunca.
 - **Contraseñas anteriores guardadas (0-24):** Introduzca la cantidad de códigos de acceso utilizados a guardar. Los usuarios no pueden usar ningún código de acceso que esté incluido en esta lista. Cualquier valor entre 1 y 24 es válido. En este campo, introduzca un número entre 1 y 24. El valor predeterminado es **0**.
- **Requisitos de código de acceso**

- **Longitud mínima:** En la lista, haga clic en la longitud mínima del código de acceso. El valor predeterminado es **6**.

Directiva de período de gracia de bloqueo de código de acceso

December 6, 2021

La directiva Período de gracia de bloqueo de código de acceso es para dispositivos compartidos con iOS (iPadOS). Para obtener más información acerca de iPads compartidos, consulte [Integrar con funciones de Apple Educación](#).

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Período de gracia de bloqueo de código de acceso:** La cantidad de minutos que una pantalla de iPad compartido permanece bloqueada antes de que el usuario deba escribir un código de acceso para desbloquearla. Cambiar esta configuración a un valor menos restrictivo no tendrá efecto hasta que el usuario cierre la sesión. El valor predeterminado es **Inmediatamente**.

De forma predeterminada, el iPad compartido se bloquea automáticamente después de dos minutos de inactividad.

The screenshot shows the configuration page for the 'Passcode Lock Grace Period Policy'. The left sidebar contains a navigation menu with '1 Policy Info', '2 Platforms', '3 Assignment', and 'iOS' (which is selected and highlighted in teal). The main content area has a title 'Passcode Lock Grace Period Policy' and a description: 'This policy sets the number of minutes that a Shared iPad screen is locked before the user must enter a passcode to unlock the screen. Changing this setting to a less restrictive value doesn't take effect until a user signs out. Available in iOS 9.3.2 and later.' Below the description, there is a field 'Passcode lock grace period' with a dropdown menu set to '1 minute' and an information icon. At the bottom, there is a section for 'Deployment Rules'.

Directiva de hotspot personal

May 25, 2021

Puede permitir que los usuarios se conecten a Internet aunque estén fuera del alcance de una red Wi-Fi mediante la conexión de datos móviles a través de la función Compartir Internet de sus dispositivos iOS.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Inhabilitar hotspot personal:** Seleccione si quiere inhabilitar la función de hotspot personal (Compartir Internet) en los dispositivos de los usuarios. El valor predeterminado es **No**, lo que desactiva la función de hotspot personal de los dispositivos de los usuarios. Esta directiva no inhabilita la función. Los usuarios pueden seguir mediante la función de hotspot personal (Compartir Internet) en sus dispositivos. Sin embargo, cuando se implementa la directiva, dicha función se desactiva (no está activa de forma predeterminada).

Directiva de eliminación de perfiles

November 29, 2023

En Citrix Endpoint Management, puede crear una directiva de eliminación de perfiles de aplicaciones. Una vez implementada, la directiva elimina el perfil de 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](#).

Parámetros de macOS

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

Profile Removal Policy

1 Policy Info

2 Platforms

☐ iOS

☒ macOS

3 Assignment

Profile Removal Policy

This policy lets you remove a profile for iOS or macOS from a device.

Profile ID *

This field is mandatory.

Deployment scope

User

macOS 10.7+

Comment

Deployment Rules

- **ID de perfil:** En la lista, haga clic en el ID del perfil de aplicación. Este campo es obligatorio.
- **Ámbito de implementación:** En la lista, haga clic en **Usuario** o **Sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

- **Comentario:** Puede escribir un comentario opcional.

Directiva de perfil de datos

November 29, 2023

Por regla general, cuando se desarrolla y se firma con código una aplicación empresarial iOS, se incluye un perfil de datos de distribución empresarial, que requiere Apple para que la aplicación funcione en dispositivos iOS. Si falta o ha caducado un perfil de datos, la aplicación se bloquea cuando un usuario toca en ella para abrirla.

El problema principal con los perfiles de datos es que caducan al año de generarse en el portal de desarrolladores de Apple, por lo que se debe hacer un seguimiento de la fecha de caducidad de todos los perfiles de datos en todos los dispositivos iOS que inscriban los usuarios. El seguimiento de las fechas de caducidad no solo implica estar al día de las fechas de caducidad en sí, sino también saber qué usuarios utilizan qué versión de la aplicación. Existen dos soluciones: enviar por correo electrónico los perfiles de datos a los usuarios o ponerlos en un portal web para que se puedan descargar e instalar desde allí. Estas soluciones funcionan, pero no son infalibles, puesto que los usuarios deben actuar siguiendo las instrucciones de un correo o visitar el portal Web para descargar e instalar el perfil en cuestión.

Si quiere que este proceso sea transparente para los usuarios, en Citrix Endpoint Management puede instalar y quitar perfiles de datos con directivas de dispositivo. Se quitan los perfiles que falten o hayan caducado y se instalan perfiles actualizados en los dispositivos de los usuarios, por lo que tocar una aplicación solo la abre para su uso.

Antes de crear una directiva de perfiles de datos, cree un archivo de perfil de datos. 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](#).

Parámetros de iOS

- **Perfil de datos de iOS:** Seleccione el archivo del perfil de datos que quiere importar. Para ello, haga clic en **Examinar** y vaya a la ubicación de ese archivo.

Directiva de eliminación de perfiles de datos

December 6, 2021

Un perfil de datos le permite distribuir aplicaciones iOS a dispositivos de usuario. Apple requiere firmar una aplicación mediante un perfil de datos para autorizar que la aplicación funcione en dispositivos iOS. Para obtener más información, consulte [Directiva de perfil de aprovisionamiento](#).

Para quitar o reemplazar un perfil de datos anterior, utilice la directiva de eliminación de perfiles de datos.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

The screenshot shows the 'Provisioning Profile Removal Policy' configuration page. The top navigation bar has tabs for 'Analyze', 'Manage', 'Configure' (selected), and 'Monitor'. Below this, there are sub-tabs: 'Device Policies', 'Apps', 'Media', 'Actions', 'Content Collaboration', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Provisioning Profile Removal Policy' with a description: 'This policy lets remove a provisioning profile from an iOS device.' On the left, there is a sidebar with a list of steps: '1 Policy Info', '2 Platforms' (with a 'Clear All' link), '3 Assignment', and '4 iOS' (which is selected and highlighted in green). The main area contains a form with a dropdown menu labeled 'iOS provisioning profile *' with the text 'Select an option' and a 'Comment' text box. Below the form, there is a section titled 'Deployment Rules'.

- **Perfil de datos de iOS:** En la lista, haga clic en el perfil de datos que quiere quitar.
- **Comentario:** Si lo prefiere, agregue un Comentario:

Directiva de proxy

December 6, 2021

Con la directiva “Proxy”, puede especificar una configuración global del proxy HTTP para los dispositivos iOS compatibles. Puede implementar solamente 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, coloque en modo supervisado todos los dispositivos iOS para los que quiere establecer un proxy global de HTTP. Para obtener información detallada, consulte [Imple-](#)

mentar dispositivos mediante [Apple Configurator 2](#) o [Implementar dispositivos mediante el Programa de implementación de Apple](#).

Establezca reglas de implementación para inscribir dispositivos antes de enviar la directiva de proxy a los dispositivos.

Parámetros de iOS

- **Configuración de proxy:** Haga clic en **Manual** o **Automática** para determinar cómo se configurará el proxy en los dispositivos de los usuarios.
 - Si hace clic en **Manual**, configure los siguientes 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:** Si quiere, escriba un nombre de usuario para la autenticación en el servidor proxy.
 - * **Contraseña:** Si quiere, escriba una contraseña para la autenticación en el servidor proxy.
 - Si hace clic en **Automática**, configure los siguientes parámetros:
 - * **URL del archivo PAC del proxy:** Escriba la dirección URL del archivo PAC que define la configuración de proxy.
 - * **Permitir conexión directa si no se puede acceder al archivo PAC:** Seleccione si quiere permitir que los usuarios se conecten directamente al destino si no se puede acceder al archivo PAC. De forma predeterminada, está **activado**.
- **Permitir omisión del proxy para acceder a redes cautivas:** Seleccione si permitir que el dispositivo omita el servidor proxy y pueda acceder a redes cautivas. De forma predeterminada, está **desactivado**.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Directiva de restricciones

March 1, 2024

Nota:

Cuando una actualización de versión incluye nuevas configuraciones de la directiva Restricciones, debe modificar y guardar la directiva. Citrix Endpoint Management no implementará la directiva Restricciones actualizada hasta que la guarde.

La directiva “Restricciones” permite o prohíbe a los usuarios utilizar funciones determinadas en sus dispositivos, como la cámara. Puede establecer restricciones de seguridad y restricciones de contenido multimedia. También puede establecer restricciones a los tipos de aplicaciones que los usuarios pueden y no pueden instalar. El valor predeterminado de la mayoría de las opciones de restricción es **Activado** o *permite*. Las excepciones principales son la función “Seguridad: Forzar” de iOS y todas las funciones de tabletas Windows, que están **desactivadas** o establecidas en *restringe* de forma predeterminada.

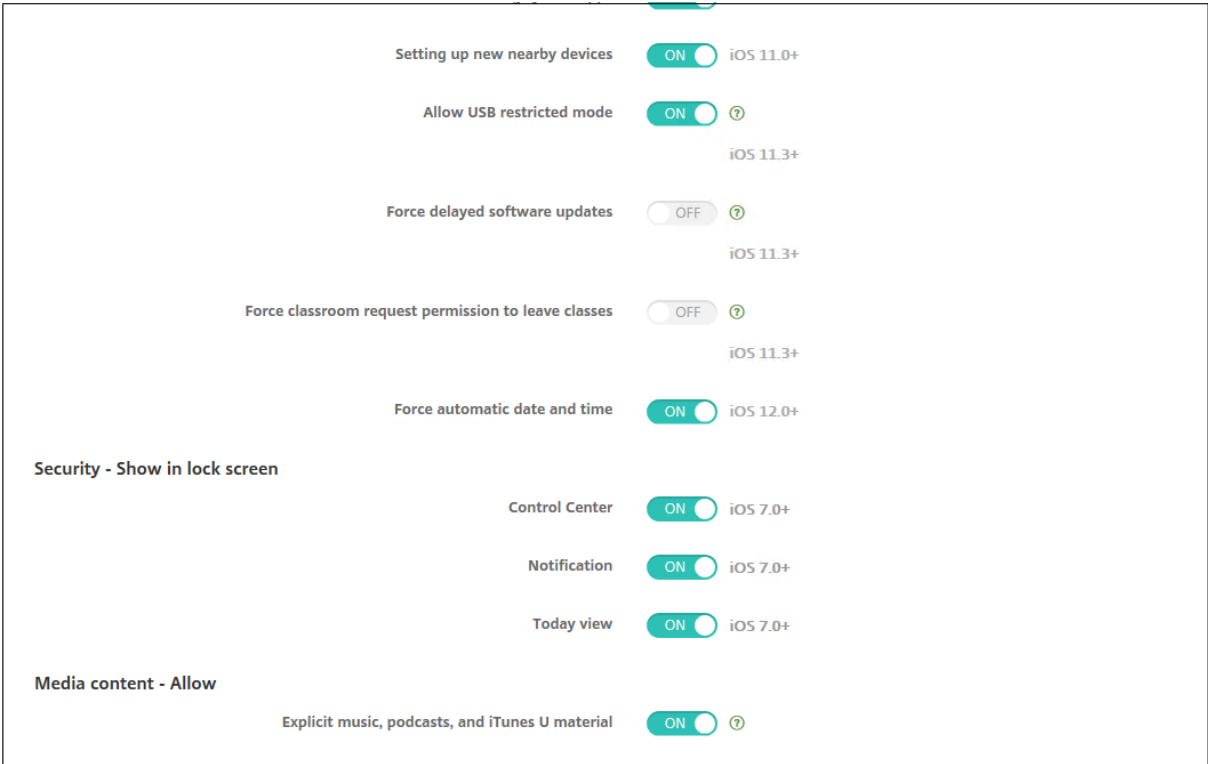
Si **activa** una opción, significa que el usuario puede realizar la operación o usar la función. Por ejemplo:

- **Cámara:** Si la opción está establecida en **Sí**, el usuario puede usar la cámara en su dispositivo. Si está **desactivada**, el usuario no puede usar la cámara en su dispositivo.
- **Capturas de pantalla:** Si está **activado**, el usuario puede tomar capturas de pantalla en su dispositivo. Si está **desactivado**, el usuario no puede tomar capturas de pantalla en su dispositivo.

Si tiene configuradas las directivas de restricciones y de quiosco, la directiva de restricciones tiene prioridad.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

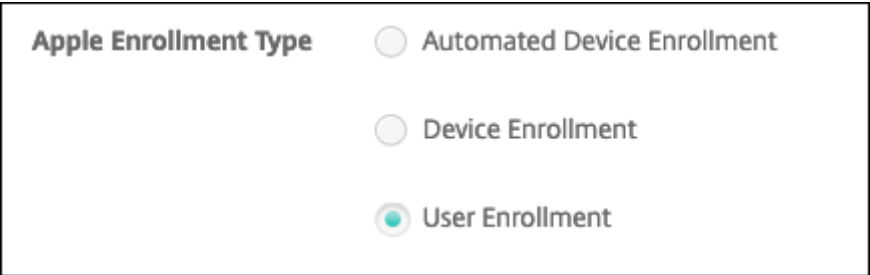


Algunas configuraciones de directiva de restricciones de iOS solo se aplican a versiones específicas de iOS, como se indica aquí y en la página de la directiva Restricciones de la consola de Citrix Endpoint Management.

Estas configuraciones se aplican cuando el dispositivo está inscrito en modo de inscripción de usuarios, en modo no supervisado (MDM completo) o en modo supervisado. En la tabla siguiente, se muestran los modos de inscripción disponibles en cada configuración para iOS 13 y versiones posteriores.

- **Inscripción automatizada de dispositivos:** Dispositivos supervisados. Se trata de dispositivos inscritos mediante la inscripción en bloque.
- **Inscripción de dispositivos:** Dispositivos no supervisados. Estos dispositivos se inscriben de forma individual y el dispositivo es completamente MDM.
- **Inscripción de usuarios:** Dispositivos en los que solo se administran usuarios específicos. Para obtener más información acerca de la inscripción de usuarios, consulte la documentación de Apple.

Es posible que las configuraciones de la directiva de restricciones de iOS se apliquen cuando el dispositivo se inscribe en modo de inscripción de usuario, en modo no supervisado (MDM completo) o en modo supervisado. En la tabla siguiente, se muestran los modos de inscripción disponibles para cada configuración de directiva de restricciones para iOS 13 y versiones posteriores.



Como se señala en la tabla, algunas configuraciones que anteriormente estaban disponibles en modo no supervisado y supervisado están disponibles solo en modo supervisado, a partir de iOS 13. Se aplican las siguientes reglas:

- Si un dispositivo supervisado posterior a iOS 13 se inscribe en Citrix Endpoint Management, se le aplica la configuración.
- Si un dispositivo no supervisado posterior a iOS 13 se inscribe en Citrix Endpoint Management, no se le aplica la configuración.
- Si un dispositivo iOS 12 (o anterior) ya inscrito en Citrix Endpoint Management se actualiza a iOS 13, no hay cambios. La configuración se aplica al dispositivo del mismo modo que antes de la actualización.

Para obtener información sobre cómo poner un dispositivo iOS en modo supervisado, consulte [Configurar dispositivos con Apple Configurator 2](#).

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Permitir controles del hardware			
Cámara	No	Sí	Sí
FaceTime	No	No	Sí
Capturas de pantalla	Sí	No	Sí
Permitir que la aplicación Aula observe remotamente las pantallas de los alumnos	No	No	Sí
Permitir que la aplicación Aula use AirPlay y Ver pantalla sin preguntar	No	No	Sí
Fotos en streaming	No	Sí	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Permitir compartir fotos en streaming	No	Sí	Sí
Permitir sesión temporal de iPad compartido	No	No	Sí
Marcado por voz	No	Sí	Sí
Siri	Sí	Sí	Sí
Permitir durante bloqueo del dispositivo	Sí	Sí	Sí
Filtro de lenguaje explícito de Siri	No	No	Sí
Instalar aplicaciones	No	No	Sí
Permitir obtención global en segundo plano durante la itinerancia	No	Sí	Sí
Permitir aplicaciones			
App Store de Apple	No	No	Sí
Compras en la aplicación	No	Sí	Sí
Requerir contraseña del App Store de Apple para todas las 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 ventanas emergentes	No	Sí	Sí
Aceptar cookies	No	Sí	Sí
Red: Permite acciones de iCloud			

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Datos y documentos de iCloud	No	No	Sí
Copia de seguridad de iCloud	No	Sí	Sí
Llavero de fotos de iCloud	No	Sí	Sí
Fototeca iCloud	No	Sí	Sí
Seguridad: Forzar			
Copias de seguridad cifradas	Sí	Sí	Sí
Seguimiento de publicidad limitado	No	Sí	Sí
Código de acceso para enlazar con AirPlay por primera vez	Sí	Sí	Sí
Apple Watch emparejado para usar detección de muñeca	Sí	Sí	Sí
Compartir documentos administrados con AirDrop	Sí	Sí	Sí
Seguridad: Permitir			
Aceptar certificados SSL que no son de confianza	No	Sí	Sí
Permitir actualización automática de parámetros de confianza de certificados	No	Sí	Sí
Requerir área de pegado administrada	Sí	Sí	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Documentos de aplicaciones administradas en aplicaciones no administradas	Sí	Sí	Sí
Las aplicaciones no administradas pueden leer contactos administrados	No	No	Sí
Las aplicaciones administradas pueden registrar contactos no administrados	No	No	Sí
Documentos de aplicaciones no administradas en aplicaciones administradas	Sí	Sí	Sí
Envío de información de diagnóstico a Apple	Sí	Sí	Sí
Permitir Touch ID para desbloquear el dispositivo	No	Sí	Sí
Desbloqueo automático	No	Sí	Sí
Notificaciones de Cartera durante bloqueo de dispositivo	No	Sí	Sí
Handoff	No	Sí	Sí
Sincronización de iCloud para aplicaciones administradas	Sí	Sí	Sí
Copia de seguridad de libros de la empresa	Sí	Sí	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Sincronización de notas y subrayados de libros de la empresa	Sí	Sí	Sí
Resultados de Internet en Spotlight	No	Sí	Sí
Confianza en aplicaciones de empresa	No	Sí	Sí
Permitir la publicidad personalizada de Apple	No	Sí	Sí
Parámetros solo para dispositivos supervisados:			
Permitir			
Permitir modificación de eSIM	No	No	Sí
Borrar todo el contenido y los parámetros	No	No	Sí
Tiempo de uso	No	No	Sí
Podcasts	No	No	Sí
Instalar perfiles de configuración	No	No	Sí
Modificación de Touch ID y Face ID	No	No	Sí
Instalar aplicaciones desde el dispositivo	No	No	Sí
Teclas de acceso rápido	No	No	Sí
Apple Watch emparejado	No	No	Sí
Modificación de código de acceso	No	No	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Modificación de nombre de dispositivo	No	No	Sí
Modificación de fondo de pantalla	No	No	Sí
Descarga automática de aplicaciones	No	No	Sí
AirDrop	No	No	Sí
iMessage	No	No	Sí
Contenido de Siri generado por el usuario	No	No	Sí
iBooks	No	No	Sí
Quitar aplicaciones	No	Sí	Sí
Game Center	No	No	Sí
Añadir amigos	No	No	Sí
Juegos multijugador	No	No	Sí
Modificar parámetros de cuenta	No	No	Sí
Modificar parámetros de datos móviles de las aplicaciones	No	No	Sí
Modificar parámetros de datos móviles de las aplicaciones	No	No	Sí
Permitir conexiones de unidades de red	No	No	Sí
Permitir conexiones de dispositivos USB	No	No	Sí
Permitir Buscar mi dispositivo	No	No	Sí
Permitir parámetros de Buscar a mis amigos	No	No	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Permitir modificar parámetros de Buscar a mis amigos	No	No	Sí
Emparejar hosts que no tienen Configurator	No	No	Sí
Teclado predictivo	No	No	Sí
Teclado con corrección automática	No	No	Sí
Teclado con revisión ortográfica	No	No	Sí
Permitir teclado QuickPath	No	No	Sí
Búsqueda de definiciones	No	No	Sí
ID único de paquete de la aplicación			
Noticias	No	No	Sí
Servicio Apple Music	No	No	Sí
Apple Music	No	No	Sí
Modificación de notificaciones	No	No	Sí
Uso de aplicaciones restringidas	No	No	Sí
Modificación de envío de diagnósticos	No	No	Sí
Modificación de Bluetooth	No	No	Sí
Permitir dictado	No	No	Sí
Modificar si la red Wi-Fi está activada o no	No	No	Sí
Unirse solo a redes Wi-Fi instaladas por una directiva de redes	No	No	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Permitir que la aplicación Aula use AirPlay y Ver pantalla sin preguntar	No	No	Sí
Permitir que la aplicación Aula bloquee una aplicación y bloquee el dispositivo sin preguntar	No	No	Sí
Unirse automáticamente a las clases de la aplicación Aula sin preguntar	No	No	Sí
Permitir AirPrint	No	No	Sí
Permitir el almacenamiento de las credenciales de AirPrint en el Llavero	No	No	Sí
Permitir la detección de impresoras AirPrint mediante iBeacons	No	No	Sí
Permitir AirPrint solo en destinos con certificados de confianza	No	No	Sí
Agregar configuraciones VPN	No	No	Sí
Modificar parámetros de planes de datos móviles	No	No	Sí
Eliminar aplicaciones de sistema	No	No	Sí
Configurar nuevos dispositivos cercanos	No	No	Sí
Permitir modo restringido de USB	No	No	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Forzar demora de actualizaciones de software	No	No	Sí
Demora forzosa para actualizaciones de software	No	No	Sí
Forzar permiso del aula para abandonar clases	No	No	Sí
Forzar autenticación antes de autorrelleno	No	No	Sí
Forzar fecha y hora automáticas	No	No	Sí
Autorrelleno de contraseñas	No	No	Sí
Solicitud de contraseña a los contactos cercanos	No	No	Sí
Compartir contraseña	No	No	Sí
Permitir modificación de Compartir Internet	No	No	Sí
Permitir arranque en modo de recuperación mediante un dispositivo no emparejado	No	No	Sí
Instalar respuesta de seguridad rápida	No	No	Sí
Eliminar respuesta rápida de seguridad	No	No	Sí
Permitir la protección de la privacidad del correo	No	No	Sí
NFC	No	No	Sí
Permitir clips de aplicaciones	No	No	Sí

Parámetro	Inscripción de usuarios	No supervisado	Supervisado
Seguridad: Mostrar en pantalla de bloqueo			
Centro de control	Sí	Sí	Sí
Notificación	Sí	Sí	Sí
Vista Hoy	Sí	Sí	Sí
Contenido multimedia: Permitir			
Música, podcasts y contenido de iTunes U explícito	No	No	Sí
Contenido sexual explícito en iBooks	No	Sí	Sí
Región de calificación	No	Sí	Sí
Películas	No	Sí	Sí
Programas de TV	No	Sí	Sí
Aplicaciones	No	Sí	Sí

- **Permitir controles del hardware**

- **Cámara:** Permite que los usuarios usen la cámara en sus dispositivos.
 - * **FaceTime:** Permite que los usuarios usen FaceTime en sus dispositivos. Para dispositivos iOS supervisados.
- **Capturas de pantalla:** Permite que los usuarios hagan capturas de pantalla en sus dispositivos.
 - * **Permitir que la aplicación Aula observe remotamente las pantallas de los alumnos:** Si no se activa esta restricción, el profesor no puede usar la aplicación Aula para observar de forma remota las pantallas de los alumnos. Está activado de forma predeterminada; así, un profesor puede utilizar la aplicación Aula para observar las pantallas de los alumnos. El parámetro **Permitir que la aplicación Aula use AirPlay y Ver pantalla sin preguntar** determina si los alumnos reciben una solicitud para conceder permiso al profesor. Para dispositivos iOS supervisados.
 - * **Permitir que la aplicación Aula utilice AirPlay y ver la pantalla sin preguntar:** Si esta restricción está seleccionada, el profesor puede utilizar AirPlay y ver la pantalla

en el dispositivo de un alumno sin solicitar permiso. Está desactivado de forma predeterminada. Para dispositivos iOS supervisados.

- **Fotos en streaming:** Permite que los usuarios usen MyPhotoStream para compartir fotos a través de iCloud con todos sus dispositivos iOS.
- **Permitir compartir fotos en streaming:** Permite que los usuarios usen 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.
- **Marcado por voz:** Habilita el marcado por voz en los dispositivos de los usuarios.
- **Siri:** Permite Siri a los usuarios.
 - * **Permitir durante bloqueo del dispositivo:** Permite a los usuarios usar Siri mientras sus dispositivos están bloqueados.
 - * **Filtro de lenguaje explícito de Siri.** Habilitar el filtro de lenguaje explícito de Siri. El valor predeterminado es la restricción de esta función, lo que significa que no se aplica ningún filtro de palabras malsonantes. Para obtener más información sobre la seguridad y Siri, consulte [Directivas de Siri y dictado](#).
- **Instalación de aplicaciones:** Permite que los usuarios instalen aplicaciones. Para dispositivos iOS supervisados.
- **Permitir obtención global en segundo plano durante la itinerancia:** Permite que los dispositivos sincronicen automáticamente cuentas de correo electrónico con iCloud mientras el dispositivo está en itinerancia. Si está **desactivada**, no permite la obtención global de datos en segundo plano cuando un teléfono iOS está en itinerancia. Está **activado** de forma predeterminada.

- **Permitir aplicaciones**

- **App Store de Apple:** Permite que los usuarios accedan al App Store de Apple. Para dispositivos iOS supervisados.
- **Compras en la aplicación:** Permite que los usuarios hagan compras desde la aplicación.
 - * **Requerir contraseña del App Store de Apple para todas las compras:** Solicita una contraseña para las compras desde la aplicación. El valor predeterminado es la restricción de esta función, lo que significa que no se pide contraseña para realizar compras en la aplicación.
- **Safari:** Permite que los usuarios accedan a Safari. Para dispositivos iOS supervisados.
 - * **Autorrelleno:** Permite que los usuarios configuren el autorrelleno de nombres de usuario y contraseñas en Safari.
 - * **Forzar advertencia de fraude.** Si este parámetro está habilitado y los usuarios visitan un sitio web sospechoso de “phishing”, Safari advierte a los usuarios. El valor pre-

determinado es la restricción de esta función, lo que significa que no se emite ninguna advertencia.

- * **Habilitar JavaScript:** Permite que JavaScript se ejecute en Safari.
- * **Bloquear elementos emergentes.** Bloquear los elementos emergentes cuando se visitan sitios web. El valor predeterminado es la restricción de esta función, lo que significa que no se bloquean los elementos emergentes.
- **Aceptar cookies.** Defina el nivel al que se aceptan las cookies. En la lista, elija una opción para permitir o restringir las cookies. El valor predeterminado es **Siempre**, lo que permite que todos los sitios guarden cookies en Safari. Las demás opciones son: **Solo del sitio web actual**, **Nunca** y **Solo de sitios web visitados**.

- **Red: Permite acciones de iCloud**

- **Datos y documentos de iCloud:** Permite que los usuarios sincronicen con iCloud los documentos y los datos. Para dispositivos iOS supervisados.
- **Copia de seguridad de iCloud:** Permite que los usuarios guarden copias de seguridad de sus dispositivos en iCloud.
- **Permitir llavero de iCloud:** Permite que los usuarios guarden sus nombres de usuario, contraseñas, información de redes Wi-Fi y datos de tarjeta de crédito en el Llavero de iCloud.
- **Fototeca iCloud:** Permite que los usuarios accedan a su biblioteca de fotos de iCloud.

- **Seguridad: Forzar**

El valor predeterminado es restringir las siguientes funciones, lo que significa que ninguna de las funciones de seguridad está habilitada.

- **Copias de seguridad cifradas.** Forzar el cifrado de las copias de seguridad que se almacenarán en iCloud.
- **Limitar seguimiento de anuncios:** Bloquear el seguimiento de anuncios segmentados.
- **Código de acceso para enlazar con AirPlay por primera vez:** Requiere que los dispositivos de usuario con AirPlay habilitado se verifiquen con un código de uso único en pantalla para poder usar AirPlay.
- **Apple Watch emparejado para usar detección de muñeca:** Requiere a un Apple Watch enlazado que use la **detección de muñeca**.
- **Compartir documentos administrados con AirDrop:** Al **activar** esta opción, AirDrop aparece como un destino no administrado para colocar contenido.

- **Seguridad: Permitir**

- **Aceptar certificados SSL que no son de confianza:** Permite que los usuarios acepten certificados SSL que no son de confianza cuando visitan sitios web.

- **Permitir actualización automática de parámetros de confianza de certificados:** Permite la actualización automática de los certificados de confianza.
- **Requerir área de pegado administrada:** 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, puede configurar lo siguiente:

- ★ **Requerir área de pegado administrada:** 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 dispositivos iOS, los usuarios no pueden copiar y pegar datos de aplicaciones administradas en aplicaciones no administradas, pero pueden copiar y pegar datos de aplicaciones no administradas en aplicaciones administradas.
- **Documentos de aplicaciones administradas en aplicaciones no administradas:** Permite que los usuarios muevan datos desde aplicaciones administradas (corporativas) a aplicaciones no administradas (personales).
 - **Documentos de aplicaciones no administradas en aplicaciones administradas:** Permite que los usuarios muevan datos desde aplicaciones no administradas (personales) a aplicaciones administradas (corporativas).
 - **Envío de información de diagnóstico a Apple:** Permite el envío a Apple de datos anónimos de diagnóstico sobre los dispositivos de los usuarios.
 - **Touch ID o Face ID para desbloquear el dispositivo:** Permite que los usuarios usen Touch ID o Face ID para desbloquear sus dispositivos.
 - **Desbloqueo automático:** si está **desactivado**, el usuario no podrá usar el Apple Watch para desbloquear un iPhone emparejado. De forma predeterminada, está **activado**. Disponible para iOS 14.5 o posterior.
 - **Notificaciones de Cartera durante bloqueo de dispositivo:** Permite que las notificaciones de Cartera aparezcan en la pantalla de bloqueo.
 - **Handoff:** Permite que los usuarios transfieran actividades desde un dispositivo iOS a otro dispositivo iOS cercano.
 - **Sincronización de iCloud para aplicaciones administradas:** Permite que los usuarios sincronicen con iCloud las aplicaciones administradas.
 - **Copia de seguridad de libros de la empresa:** Permite que se guarden copias de seguridad de los libros de la empresa en iCloud.
 - **Sincronización de notas y subrayados de libros de la empresa:** Permite la sincronización con iCloud de las notas y los resaltados agregados por los usuarios a los libros

de la empresa.

- **Confianza en aplicaciones de empresa:** Permite la confianza en las aplicaciones de empresa. Las aplicaciones de empresa son aquellas aplicaciones personalizadas para su organización. Pueden crearse de forma interna o pueden desarrollarse y adquirirse de un proveedor externo. Para obtener más información, consulte [Instalar apps de empresa personalizadas en iOS](#).
- **Resultados de Internet en Spotlight:** Permite que Spotlight muestre los resultados de búsquedas encontrados en Internet, además de los encontrados en el dispositivo.
- **Las aplicaciones no administradas pueden leer contactos administrados:** Opcional. Solo disponible si **Documentos de aplicaciones administradas en aplicaciones no administradas** está desactivado. Si esta directiva 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 pueden registrar contactos no administrados:** Opcional. Si está habilitado, se permite que las aplicaciones administradas agreguen contactos a los contactos de 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 la publicidad personalizada de Apple:** si está **desactivado**, la plataforma de publicidad de Apple no usará los datos de los usuarios para ofrecer anuncios personalizados. De forma predeterminada, está **activado**. Disponible para iOS 14.0 o posterior.

- **Parámetros solo para dispositivos supervisados: Permitir**

Estos parámetros solo se aplican a dispositivos supervisados. Para ver los pasos necesarios para poner un dispositivo iOS en modo supervisado, consulte [Implementar dispositivos con Apple Configurator 2](#).

- **Permitir modificación de eSIM:** Permite a los usuarios cambiar la configuración de eSIM en su dispositivo.
- **Borrar todo el contenido y los parámetros:** Permite que los usuarios borren todo el contenido y los parámetros de sus dispositivos.
- **Tiempo de uso:** Permite a los usuarios habilitar Tiempo de uso.
- **Podcasts:** Permite que los usuarios descarguen y sincronicen podcasts.
- **Instalación de perfiles de configuración:** Permite que los usuarios instalen un perfil de configuración distinto del implementado.
- **Modificación de Touch ID y Face ID:** Permite que los usuarios cambien o eliminen su Touch ID o Face ID.
- **Instalar aplicaciones desde el dispositivo:** Permite que los usuarios instalen aplica-

ciones. Al inhabilitar este parámetro, los usuarios finales no pueden instalar nuevas aplicaciones. El App Store está inhabilitado y su icono se quita de la pantalla de inicio.

- **Teclas de acceso rápido:** Permite que los usuarios creen métodos de teclado abreviados y personalizados para palabras o frases que usan con frecuencia.
- **Apple Watch emparejado:** Permite que los usuarios enlacen un Apple Watch a un dispositivo supervisado.
- **Modificación de código de acceso:** Permite que los usuarios cambien el código de acceso en un dispositivo supervisado.
- **Modificación de nombre de dispositivo:** Permite que los usuarios cambien el nombre de su dispositivo.
- **Modificar de fondo de pantalla:** Permite que los usuarios cambien el fondo de pantalla en sus dispositivos.
- **Descarga automática de aplicaciones:** Permite descargar aplicaciones.
- **AirDrop:** Permite que los usuarios compartan fotos, vídeos, sitios web y ubicaciones, entre otros, con dispositivos iOS cercanos.
- **iMessage:** Permite que los usuarios envíen mensajes de texto por Wi-Fi con iMessage.
- **Contenido de Siri generado por el usuario:** Permite que Siri haga consultas de contenido generado por usuarios desde la web. Los llamados consumidores y periodistas no tradicionales generan el contenido generado por el usuario. Por ejemplo, el contenido de Twitter o Facebook se considera como contenido generado por el usuario.
- **iBooks:** Permite que los usuarios usen la aplicación iBooks.
- **Eliminar aplicaciones:** Permite que los usuarios quiten aplicaciones de sus dispositivos.
- **Game Center:** Permite que los usuarios jueguen en línea a través de Game Center en sus dispositivos.
 - * **Agregar amigos:** Permite que los usuarios envíen notificaciones a amigos para participar en un juego.
 - * **Juegos multijugador:** Permite que los usuarios inicien juegos multijugador en sus dispositivos.
- **Modificar parámetros de cuenta:** Permite que los usuarios modifiquen los ajustes de cuenta de su dispositivo.
- **Permitir modificar parámetros de datos móviles de las aplicaciones:** Permite que los usuarios modifiquen el modo en que las aplicaciones usan los datos móviles.
- **Permitir conexiones de 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:** Inhabilita la opción **Buscar mi dispositivo** en la aplicación Buscar.
- **Permitir parámetros de Buscar a mis amigos:** Inhabilita la opción **Buscar a mis amigos** en la aplicación Buscar.
- **Permitir modificar parámetros de Buscar a mis amigos:** Permite que los usuarios cambien los parámetros de Buscar a mis amigos.
- **Emparejar hosts que no tienen Configurator:** Permite al administrador controlar con qué dispositivos puede emparejarse el dispositivo de un usuario. Si se inhabilita este parámetro, se impide el emparejamiento excepto con el host supervisor que ejecuta Apple Configurator. Si no se ha configurado ningún certificado de host supervisor, todo el emparejamiento estará inhabilitado.
- **Teclado predictivo:** Permite que los usuarios usen el teclado predictivo para sugerir palabras mientras teclean en sus dispositivos. Inhabilite esta opción en situaciones tales como la administración de textos estándar donde no quiere que los usuarios tengan acceso a sugerencias de palabras.
- **Teclado con corrección automática:** Permite que los usuarios usen la corrección automática del teclado en sus dispositivos. Inhabilite esta opción en situaciones tales como la administración de textos estándar donde no quiere que los usuarios tengan acceso a la corrección automática.
- **Teclado con revisión ortográfica:** Permite que los usuarios usen la revisión ortográfica mientras teclean en sus dispositivos. Inhabilite esta opción en situaciones tales como la administración de textos estándar donde no quiere que los usuarios tengan acceso a la revisión ortográfica.
- **Búsqueda de definiciones:** Permite que los usuarios usen la búsqueda de definiciones mientras teclean en sus dispositivos. Inhabilite esta opción en situaciones tales como la administración de textos estándar donde no quiere que los usuarios tengan acceso a la búsqueda de definiciones mientras teclean.
- **ID único de paquete de aplicaciones:** Cree una lista de las aplicaciones a las que se permite conservar 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 este proceso para cada aplicación que quiera agregar.
- **News:** Permite que los usuarios usen la aplicación News.

- **Servicio Apple Music:** Permite que los usuarios usen el servicio Apple Music. Si no quiere permitir el uso del servicio Apple Music, la aplicación Música se ejecuta en el modo clásico.
- **Apple Music:** Permite que los usuarios usen Apple Music.
- **Modificación de notificaciones:** Permite que los usuarios modifiquen los parámetros de notificación.
- **Uso de aplicaciones restringidas:** Permite que los usuarios usen todas las aplicaciones, o bien usen o no usen las aplicaciones en función de los ID de paquete que proporcione. Se aplica solo a los dispositivos supervisados. Si selecciona **Permitir solo algunas aplicaciones**, agregue una aplicación con el ID de paquete `com.apple.webapp` para permitir clips web.

Nota:

A partir de iOS 11, Apple introdujo cambios en las directivas que están disponibles para las restricciones a aplicaciones. Apple ya no permite eliminar el acceso a la aplicación Ajustes y a la aplicación Teléfono al restringir el paquete de aplicaciones iOS correspondiente.

Después de configurar la directiva de restricciones para bloquear algunas aplicaciones y, a continuación, implementar la directiva: Si quiere permitir más adelante algunas o todas esas aplicaciones, cambiar y volver a implementar la directiva de restricciones no cambia esas restricciones. En este caso, iOS no aplica los cambios en el perfil de iOS. Para proceder, use la directiva de eliminación de perfiles para eliminar el perfil de iOS y, a continuación, implemente la directiva de restricciones actualizada.

Si quiere cambiar este parámetro a **Permitir solo algunas aplicaciones**, antes de implementar esta directiva, indique a los usuarios de los 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, los usuarios podrían tener que inhabilitar la autenticación de dos factores en sus dispositivos para poder iniciar sesión en sus cuentas de Apple y acceder a las aplicaciones permitidas.

- **Modificación de envío de diagnósticos:** Permite que los usuarios modifiquen los parámetros de envío de información de diagnóstico y análisis de aplicaciones en el panel **Ajustes > Diagnóstico y uso**.
- **Modificación de Bluetooth:** Permite que los usuarios modifiquen los parámetros de Bluetooth.
- **Permitir dictado:** Solo en dispositivos supervisados. Cuando esta restricción está **desactivada**, no se permite la entrada de comandos de dictado ni de voz a texto. Está **activado** de forma predeterminada.

- **Modificar si la red Wi-Fi está activada o no:** Impide que la conexión Wi-Fi se active o desactive en Ajustes o Centro de control. El acceso al modo avión tampoco tiene ningún efecto. Esta restricción no impide seleccionar qué red Wi-Fi utilizar.
- **Unirse solo a redes Wi-Fi instaladas por una directiva de redes:** Opcional. Solo dispositivos supervisados. Cuando esta restricción se **activa**, el dispositivo solo puede conectarse a aquellas redes Wi-Fi que se hayan configurado a través de un perfil de configuración. Está **desactivado** de forma predeterminada.
- **Permitir que la aplicación Aula utilice AirPlay y ver la pantalla sin preguntar:** Si esta restricción está seleccionada, el profesor puede utilizar AirPlay y ver la pantalla en el dispositivo de un alumno sin solicitar permiso. Está desactivado de forma predeterminada. Para dispositivos iOS supervisados.
- **Permitir que la aplicación Aula bloquee una aplicación y bloquee el dispositivo sin preguntar:** Si esta restricción está **activada** (Sí), la aplicación Aula bloquea automáticamente los dispositivos de usuario de una aplicación y bloquea el dispositivo sin avisar a los usuarios. Está **desactivado** de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
- **Unirse automáticamente a las clases de la aplicación Aula sin preguntar:** Si esta restricción está **activada** (Sí), la aplicación Aula unirá automáticamente los usuarios a las clases sin avisar a los primeros. Está **desactivado** de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
- **Permitir AirPrint:** Si esta restricción está **desactivada**, los usuarios no podrán imprimir con AirPrint. Está **activado** de forma predeterminada. Cuando esta restricción se **activa**, aparecen estas restricciones adicionales. Para dispositivos supervisados con iOS 11 (versión mínima).
 - * **Permitir el almacenamiento de las 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. Está activado de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
 - * **Permitir la detección de impresoras AirPrint mediante iBeacons:** Si esta restricción no está seleccionada, la detección de impresoras AirPrint mediante iBeacons está desactivada. Este parámetro impide que balizas falsas de AirPrint por Bluetooth se adjudiquen tráfico de red. Está activado de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
 - * **Permitir AirPrint solo en destinos con certificados de confianza:** Si se selecciona esta restricción, los usuarios pueden utilizar AirPrint para imprimir solamente en destinos con certificados de confianza. Está desactivado de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).

- **Agregar configuraciones VPN:** Si esta restricción está **desactivada** (No), los usuarios no podrán crear configuraciones VPN. Está **activado** de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
- **Modificar parámetros de planes de datos móviles:** Si esta restricción está **desactivada** (No), los usuarios no podrán modificar los parámetros de planes de datos móviles. Está **activado** de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
- **Eliminar aplicaciones del sistema:** Si esta restricción está **desactivada** (No), los usuarios no podrán quitar aplicaciones del sistema que haya presentes en su dispositivo. Está **activado** de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
- **Configurar nuevos dispositivos cercanos:** Si esta restricción está desactivada, los usuarios no podrán configurar nuevos dispositivos cercanos. Está activado de forma predeterminada. Para dispositivos supervisados con iOS 11 (versión mínima).
- **Permitir modo restringido de USB:** Si está **desactivado** (No), el dispositivo siempre se puede conectar a accesorios USB mientras esté bloqueado. De forma predeterminada, está **activado**. Disponible solamente para dispositivos supervisados iOS 11.3 y versiones posteriores.
- **Forzar demora de actualizaciones de software:** Si está **activado**, retrasa el momento en que el usuario ve las actualizaciones de software. Con esta restricción activada, el usuario no ve una actualización de software hasta que transcurra la cantidad especificada de días después de la fecha de publicación de la actualización. El valor predeterminado es **Desactivado**. Disponible solamente para dispositivos supervisados iOS 11.3 y versiones posteriores. La directiva de actualización de SO contiene más parámetros para controlar la frecuencia con la que los dispositivos reciben actualizaciones. Consulte [Directiva de actualización del SO](#).
- **Demora forzosa para actualizaciones de software (días):** Permite especificar una cantidad de días para retrasar una actualización de software en el dispositivo. La demora máxima es **90** días. El valor predeterminado es **30** días. Disponible solamente para dispositivos supervisados iOS 11.3 y versiones posteriores.
- **Forzar permiso del aula para abandonar clases:** Si está **activado** (Sí), un alumno matriculado en un curso no gestionado con Aula debe solicitar el permiso del profesor cuando intenta abandonar la clase. El valor predeterminado es **Desactivado**. Disponible solamente para dispositivos supervisados iOS 11.3 y versiones posteriores.
- **Forzar autenticación antes de autorrelleno:** Obliga al usuario a autenticarse antes de que pueda utilizar la función de autorrelleno.

- **Forzar fecha y hora automáticas:** Permite configurar automáticamente la fecha y la hora en los dispositivos supervisados. Si está **activado**, los usuarios de los dispositivos no pueden desmarcar **Establecer automáticamente** en **General > Fecha y hora**. La zona horaria en el dispositivo se actualiza solo cuando el dispositivo puede determinar su ubicación. Es decir, cuando un dispositivo tiene una conexión móvil o una conexión Wi-Fi con los servicios de ubicación habilitados. El valor predeterminado es **Desactivado**. Disponible solamente para dispositivos supervisados iOS 12 y versiones posteriores.
 - **Autorrelleno de contraseñas:** Opcional. Si está inhabilitado, los usuarios no pueden usar las funciones de autorrelleno de contraseñas o sugerencias de contraseñas seguras. De forma predeterminada, está **activado**. Disponible a partir de iOS 12.
 - **Solicitud de contraseña a los contactos cercanos:** Opcional. Si está inhabilitado, los dispositivos de los usuarios no solicitan contraseñas de los dispositivos cercanos. De forma predeterminada, está **activado**. Disponible a partir de iOS 12.
 - **Compartir contraseña:** Opcional. Si está inhabilitado, los usuarios no pueden compartir sus contraseñas mediante la función de contraseñas de AirDrop. De forma predeterminada, está **activado**. Disponible a partir de iOS 12.
 - **Permitir modificación de Compartir Internet:** Impide que los usuarios cambien la configuración de hotspot personal.
 - **Permitir la recuperación desde un dispositivo no emparejado:** si está **activado**, permite que los dispositivos se inicien en modo recuperación desde un dispositivo no emparejado. El valor predeterminado es **Desactivado**. Disponible para iOS 14.5 o posterior.
 - **Instalar respuesta de seguridad rápida:** si está **desactivado**, prohíbe la instalación de respuestas de seguridad rápidas. El valor predeterminado es **Activado**.
 - **Eliminar respuesta rápida de seguridad:** si está **desactivado**, prohíbe la eliminación de las respuestas rápidas de seguridad. El valor predeterminado es **Activado**.
 - **Permitir la protección de la privacidad del correo:** si está **desactivado**, inhabilita la protección de la privacidad del correo en el dispositivo. El valor predeterminado es **Activado**. Disponible para iOS 15.2 o posterior.
 - **NFC:** si está **desactivado**, inhabilita NFC. El valor predeterminado es **Activado**. Disponible para iOS 14.2 o posterior.
 - **Permitir clips de aplicaciones:** si está **desactivada**, impide que un usuario agregue clips de aplicaciones y elimina los clips de aplicaciones existentes en el dispositivo. El valor predeterminado es **Activado**. Disponible para iOS 14.0 o posterior.
- **Seguridad: Mostrar en pantalla de bloqueo**

- **Centro de control:** Permite el acceso al Centro de control en la pantalla de bloqueo. El Centro de control facilita a los usuarios la modificación de las funciones Modo Avión, Wi-Fi, Bluetooth, No molestar y Bloquear rotación.
- **Notificación:** Permite notificaciones en la pantalla de bloqueo.
- **Vista Hoy:** Permite la vista Hoy, que agrupa información diversa, como el tiempo y los eventos del calendario para el día en curso en la pantalla de bloqueo.

- **Contenido multimedia: Permitir**

- **Música, podcasts y contenido de iTunes U explícito:** Permite material explícito en los dispositivos de los usuarios.
- **Contenido sexual explícito en iBooks:** Permite la descarga de material explícito desde iBooks.
- **Región de calificación:** Defina la región desde donde se obtienen las calificaciones de control parental. En la lista, haga clic en un país para establecer la región de las clasificaciones. El valor predeterminado es **Estados Unidos**.
- **Películas:** Establezca si se permiten películas en los dispositivos de los usuarios. Si permite las películas, puede configurar también un nivel de clasificación de estas. En la lista, haga clic en una opción para permitir o restringir las películas en el dispositivo. El valor predeterminado es “Permitir todas las películas”.
- **Programas de TV:** Defina si se permiten programas de TV en los dispositivos de los usuarios. Si permite los programas de TV, puede configurar también un nivel de clasificación de estos. En la lista, haga clic en una opción para permitir o restringir los programas de TV en el dispositivo. El valor predeterminado es “Permitir todos los programas de TV”.
- **Aplicaciones:** Defina si se permiten aplicaciones en los dispositivos de los usuarios. Si permite aplicaciones, puede configurar también un nivel de clasificación de estas. En la lista, haga clic en una opción para permitir o restringir las aplicaciones en el dispositivo. El valor predeterminado es “Permitir todas las aplicaciones”.

- **Configuraciones de directivas**

- **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.
- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible en iOS 9.3 y versiones posteriores.

Parámetros de macOS

Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Preferences

Restrict items in System Preferences

OFF

Apps

Allow use of Game Center

ON

macOS 10.11+

Allow adding Game Center friends

ON

Allow multiplayer gaming

ON

Allow Game Center account modification

ON

Allow App Store adoption

ON

Allow Safari AutoFill

ON

Require admin password to install or update apps

OFF

Restrict App Store to software update only

OFF

Restrict which apps are allowed to open

OFF

Widgets

Allow only the following Dashboard widgets to run

OFF

Media

Parámetro	No supervisado	Supervisado
Aplicaciones		
Permitir el uso de Game Center	No	Sí
Permitir la incorporación de amigos a Game Center	No	Sí
Permitir juegos multijugador	No	Sí
Permitir la modificación de cuentas de Game Center	Sí	Sí
Permitir la adopción del App Store	Sí	Sí
Permitir autorrelleno en Safari	No	Sí
Requerir contraseña de administrador para instalar o actualizar aplicaciones	Sí	Sí

Parámetro	No supervisado	Supervisado
Restringir App Store a actualizaciones de software solamente	Sí	Sí
Restringir las aplicaciones que se pueden abrir	Sí	Sí
Archivos 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 búsquedas	Sí	Sí
Permitir el uso de contraseñas de iCloud para cuentas locales	Sí	Sí
Permitir datos y documentos de iCloud	Sí	Sí
Permitir escritorio y documentos de iCloud	No	Sí
Permitir sincronización de llavero de iCloud	No	Sí
Permitir Correo de iCloud	Sí	Sí
Permitir Contactos de iCloud	Sí	Sí
Permitir Calendarios de iCloud	Sí	Sí
Permitir Recordatorios de iCloud	Sí	Sí
Permitir Favoritos 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 el Mac	Sí	Sí

Parámetro	No supervisado	Supervisado
Forzar demora de actualizaciones de software	No	Sí
Autorrelleno de contraseñas	No	Sí
Solicitud de contraseña a los contactos cercanos	No	Sí
Compartir contraseña	Sí	Sí

- **Preferencias**

- **Restringir elementos de Preferencias del Sistema:** Permita o restrinja el acceso de los usuarios a Preferencias del Sistema. Está **desactivado** de forma predeterminada, lo que concede a los usuarios acceso completo a las preferencias del sistema. Si esta opción se habilita, defina las siguientes opciones de configuración:

- * **Panel de Preferencias del Sistema:** Elija si las opciones que seleccione se habilitarán o inhabilitarán. Todas las opciones están **activadas** de forma predeterminada.

- Usuarios y grupos
 - General
 - Accesibilidad
 - App Store
 - Actualización de software
 - Bluetooth
 - CD y DVD
 - Fecha y hora
 - Escritorio y protector de pantalla
 - Pantallas
 - Dock
 - Ahorro de energía
 - Extensiones
 - FibreChannel
 - iCloud
 - Ink
 - Cuentas de Internet
 - Teclado
 - Idioma y texto
 - Mission Control
 - Puntero
 - Red

- Notificaciones
- Control parental
- 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 que los usuarios jueguen en línea a través de Game Center en sus dispositivos. El valor predeterminado es **Activado**.
- **Permitir agregar amigos de Game Center:** Permite que los usuarios envíen notificaciones a amigos para participar en un juego. El valor predeterminado es **Activado**.
- **Permitir juegos multijugador:** Permite que los usuarios inicien juegos multijugador. El valor predeterminado es **Activado**.
- **Permitir modificar cuenta de Game Center:** Permite que los usuarios modifiquen la configuración de sus cuentas de Game Center. El valor predeterminado es **Activado**.
- **Permitir adopción de App Store:** Permite o restringir que el App Store de Apple adopte aplicaciones ya existentes en OS X. Está **activado** de forma predeterminada.
- **Permitir autorrelleno en Safari:** Permite que Safari rellene automáticamente campos en sitios web con contraseñas, direcciones y demás 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. Está **desactivado** de forma predeterminada, lo que significa que no se requiere contraseña de administrador.
- **Restringir App Store a actualizaciones de software solamente:** Restringe el App Store a solo actualizaciones, lo que inhabilita todas las fichas del App Store de Apple salvo las actualizaciones (Updates). Está **desactivado** de forma predeterminada, lo que permite el acceso total al App Store.
- **Restringir las aplicaciones que se puede abrir:** Restringe o permite las aplicaciones que puedan utilizar los usuarios. Está desactivado de forma predeterminada, lo que permite el uso de todas las aplicaciones. Si activa esta opción, defina los siguientes parámetros:
 - * **Aplicaciones permitidas:** Haga clic en **Agregar**, escriba el nombre y el ID de paquete

de una aplicación cuyo inicio esté permitido y, a continuación, haga clic en **Guardar**. Para las aplicaciones de productividad móvil de Citrix, use el ID del campo **ID del paquete** al agregar la aplicación. Repita este paso para cada aplicación con permiso para iniciarse.

- * **Carpetas no permitidas:** Haga clic en **Agregar**, escriba la ruta de la carpeta a la que quiera restringir el acceso de los usuarios (por ejemplo, /Aplicaciones/Utilidades) y, a continuación, haga clic en **Guardar**. Repita este paso para cada carpeta a la que no quiera que accedan los usuarios.
- * **Carpetas permitidas:** Haga clic en **Agregar**, escriba la ruta de la carpeta a la que quiera permitir el acceso por parte de los usuarios y, a continuación, haga clic en **Guardar**. Repita este paso para cada carpeta a la que quiera que los usuarios puedan acceder.

- **Widgets**

- **Permitir solo la ejecución de estos widgets del panel de mandos:** Si está **activado**, los usuarios solo pueden ejecutar los widgets del panel de mandos configurados en este parámetro. Está **desactivado** de forma predeterminada, lo que permite a los usuarios ejecutar todos los widgets. Si activa esta opción, defina el siguiente parámetro:
 - * **Widgets permitidos:** Haga clic en **Agregar**, escriba el nombre y el ID de un widget que se pueda ejecutar y, a continuación, haga clic en **Guardar**. Repita este paso para cada widget que quiera ejecutar en el panel de mandos.

- **Archivos multimedia**

- **Permitir AirDrop:** Permite que los usuarios compartan fotos, vídeos, sitios web, ubicaciones y otros objetos con dispositivos iOS cercanos.

- **Compartir**

- **Habilitar automáticamente nuevos servicios de uso compartido:** Seleccione si el uso compartido de los servicios se habilita automáticamente.
- **Correo:** Seleccione si permitir un buzón compartido.
- **Facebook:** Seleccione si permitir una cuenta compartida de Facebook.
- **Servicios de vídeo: Flickr, Vimeo, Tudou y Youku:** Seleccione si permitir servicios de vídeos compartidos.
- **Agregar a Aperture:** Seleccione si habilitar la capacidad de compartir elementos agregados a Aperture.
- **Sina Weibo:** Seleccione si permitir una cuenta compartida de Sina Weibo.
- **Twitter:** Seleccione si permitir una cuenta compartida de Twitter.
- **Mensajes:** Seleccione si permitir el acceso compartido a los mensajes.
- **Agregar a iPhoto:** Seleccione si permitir la capacidad compartida de agregar contenido a iPhoto.

- **Agregar a la lista de lectura:** Seleccione si permitir la capacidad compartida de agregar contenido a la lista de lectura.
- **AirDrop:** Seleccione si permitir una cuenta compartida de AirDrop.

- **Funcionalidad**

- **Bloquear imagen de escritorio:** Seleccione si los usuarios pueden cambiar la imagen de sus escritorios. Está **desactivado** de forma predeterminada, lo que significa que los usuarios pueden cambiar la imagen del escritorio.
- **Permitir el uso de la cámara:** Seleccione si los usuarios pueden usar la cámara en sus Mac. Está **desactivado** de forma predeterminada, con lo que los usuarios no pueden utilizar la cámara.
- **Permitir Apple Music:** Permite a los usuarios usar el servicio Apple Music (a partir de macOS 10.12). Si no quiere permitir el uso del servicio Apple Music, la aplicación Música se ejecuta en el modo clásico. Se aplica solo a los dispositivos supervisados. Está **activado** de forma predeterminada.
- **Permitir sugerencias de Spotlight:** Seleccione si los usuarios pueden usar sugerencias de Spotlight en las búsquedas de sus equipos Mac y para proporcionar sugerencias de Spotlight procedentes de Internet y el App Store. Está **desactivado** de forma predeterminada, lo que impide que los usuarios utilicen sugerencias de Spotlight.
- **Permitir búsquedas:** Seleccione si los usuarios pueden buscar la definición de palabras con el menú contextual o el menú de búsqueda de Spotlight. Está desactivado de forma predeterminada, lo que impide que los usuarios utilicen Buscar en sus equipos 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 su Mac. Si se habilita esta directiva, los usuarios usarán solo un ID y una contraseña para *todas* las pantallas de inicio de sesión de sus Mac. Está **activado** de forma predeterminada, lo que permite a los usuarios utilizar su ID de Apple y su contraseña de iCloud para acceder a su Mac.
- **Permitir datos y documentos de iCloud:** Seleccione si quiere permitir que los usuarios accedan a documentos y datos almacenados en iCloud desde sus equipos Mac. De forma predeterminada está **activado**, lo que impide a los usuarios utilizar documentos y datos de iCloud en sus Mac.
 - * **Permitir escritorio y documentos de iCloud** (a partir de macOS 10.12.4): El valor predeterminado está seleccionado.
- **Permitir sincronización de llavero de iCloud:** Permite la sincronización del llavero de iCloud (a partir de macOS 10.12). El valor predeterminado es **Activado**.
- **Permitir Correo de iCloud:** Permite que los usuarios utilicen Correo de iCloud (a partir de macOS 10.12). El valor predeterminado es **Activado**.
- **Permitir Contactos de iCloud:** Permite que los usuarios utilicen Contactos de iCloud (a partir de macOS 10.12). El valor predeterminado es **Activado**.

- **Permitir Calendarios de iCloud:** Permite que los usuarios utilicen Calendarios de iCloud (a partir de macOS 10.12). El valor predeterminado es **Activado**.
- **Permitir Recordatorios de iCloud:** Permite que los usuarios utilicen Recordatorios de iCloud (a partir de macOS 10.12). El valor predeterminado es **Activado**.
- **Permitir Favoritos de iCloud:** Permite que los usuarios sincronicen Favoritos de iCloud (a partir de macOS 10.12). El valor predeterminado es **Activado**.
- **Permitir Notas de iCloud:** Permite que los usuarios utilicen Notas de iCloud (a partir de macOS 10.12). El valor predeterminado es **Activado**.
- **Permitir fotos de iCloud:** Si **desactiva** este parámetro, cualquier foto que no se haya descargado totalmente desde la biblioteca de fotos de iCloud se eliminará del almacenamiento local del dispositivo (a partir de macOS 10.12). El valor predeterminado es **Activado**.
- **Permitir desbloqueo automático.** Para obtener información acerca de esta opción y Apple Watch, consulte <https://www.imore.com/auto-unlock> (macOS 10.12 y versiones posteriores). El valor predeterminado es **Activado**.
- **Permitir Touch ID para desbloquear el Mac** (a partir de macOS 10.12.4): El valor predeterminado es **Activado**.
- **Forzar demora de actualizaciones de software:** Si está **activado**, retrasa el momento en que el usuario ve las actualizaciones de software. Los usuarios no ven una actualización de software hasta que transcurra la cantidad especificada de días después de la fecha de publicación de la actualización. El valor predeterminado es **Desactivado**. Disponible solo para dispositivos supervisados que ejecutan macOS 10.13.4 y versiones posteriores. La directiva de actualización de SO contiene más parámetros para controlar la frecuencia con la que los dispositivos reciben actualizaciones. Consulte [Directiva de actualización del SO](#).
- **Demora forzosa para actualizaciones de software (días):** Permite especificar una cantidad de días para retrasar una actualización de software en el dispositivo. El valor máximo es 90 días. El valor predeterminado es **30**. Disponible solo para dispositivos supervisados que ejecutan macOS 10.13.4 y versiones posteriores.
- **Autorrelleno de contraseñas:** Opcional. Si está inhabilitado, los usuarios no pueden usar las funciones de autorrelleno de contraseñas o sugerencias de contraseñas seguras. El valor predeterminado es **activado** (macOS 10.14 y versiones posteriores).
- **Solicitud de contraseña a los contactos cercanos:** Opcional. Si está inhabilitado, los dispositivos de los usuarios no solicitan contraseñas de los dispositivos cercanos. El valor predeterminado es **activado** (macOS 10.14 y versiones posteriores).
- **Compartir contraseña:** Opcional. Si está inhabilitado, los usuarios no pueden compartir sus contraseñas mediante la función de contraseñas de AirDrop. El valor predeterminado es **activado** (macOS 10.14 y versiones posteriores).

Parámetros de Android

- **Cámara:** Permite que los usuarios usen la cámara en sus dispositivos. Si está **desactivado**, se inhabilita la cámara. Está **activado** de forma predeterminada.

Parámetros de Android Enterprise

Apply to fully managed devices with a work profile/Work profile on corporate-owned devices

☒ ?

For fully managed devices with a work profile, apply the policy to:

☒ Work profile

☐ Managed device

Security

Allow account management

☐ × ?

Allow copy and paste from work profile

☐ × ?

Allow data sharing from personal profile

☐ × ?

Allow screen capture

☐ × ?

Allow use of camera

☐ × ?

Allow configuring location provider

☒ ?

Allow location sharing

☐ × ?

Allow user to configure user credentials

☒ ?

Allow printing

☐ × ?

Cuando un dispositivo Android nuevo o restablecido a los valores de fábrica se inscribe en el modo de perfil de trabajo, los dispositivos con Android 9.0-10.x se inscriben como dispositivos totalmente

administrados con un perfil de trabajo. Los dispositivos con Android 11 o una versión posterior se inscriben como un perfil de trabajo en dispositivos propiedad de la empresa. La directiva de restricciones puede aplicarse tanto al perfil de trabajo del dispositivo como al dispositivo administrado.

En los dispositivos inscritos en el modo de perfil de trabajo en dispositivos propiedad de la empresa, estas restricciones no funcionan:

- Permitir servicio de copia de seguridad
- Habilitar aplicaciones del sistema
- Impedir que Keyguard bloquee el dispositivo
- Permitir el uso de la barra de estado
- Mantener encendida la pantalla del dispositivo
- Permitir al usuario controlar los parámetros de la aplicación
- Permitir que el usuario configure las credenciales de usuario
- Permitir configuración VPN
- Permitir almacenamiento USB masivo
- Permitir restablecimiento de valores de fábrica
- Permitir la desinstalación de aplicaciones
- Permitir aplicaciones que no son de Google Play
- Permitir copiar y pegar contenido entre perfiles
- Habilitar verificación de la aplicación
- Permitir administración de cuentas
- Permitir impresión
- Permitir NFC
- Permitir incorporación de usuarios

De forma predeterminada, los parámetros de **depuración por USB y fuentes desconocidas** están inhabilitados 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 propiedad de la empresa:** Permite configurar los parámetros 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 con acceso privado). Si esta configuración está **activada**, seleccione una de estas configuraciones:

- **Perfil de trabajo:** Las configuraciones de restricciones que defina se aplicarán únicamente al perfil de trabajo del dispositivo.
- **Dispositivo administrado:** Las configuraciones de restricciones que defina se aplicarán únicamente al dispositivo.

Si está **desactivada**, las configuraciones de credenciales que indique se aplicarán al dispositivo, con la excepción de aquellas que se aplican explícitamente al perfil de trabajo. El valor predeterminado es **Desactivado**.

Cuando **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa** está desactivado, configure estos parámetros:

- **Seguridad**
 - **Permitir administración de cuentas:** Permite que se agreguen cuentas a perfiles de trabajo y dispositivos administrados. El valor predeterminado es **Desactivado**.
 - **Permitir copiar y pegar contenido desde el perfil de trabajo:** Si está **activado**, los usuarios pueden copiar y pegar datos de las aplicaciones del perfil de trabajo a las aplicaciones del perfil personal. El valor predeterminado es **Desactivado**.

- **Permitir compartir datos desde el perfil personal:** Si está **activado**, 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 **Desactivado**.
- **Permitir capturas de pantalla:** Permite a los usuarios grabar o tomar una captura de la pantalla del dispositivo. El valor predeterminado es **Desactivado**.
- **Permitir el uso de la cámara:** Permite a los usuarios tomar fotos y hacer vídeos con la cámara del dispositivo. El valor predeterminado es **Desactivado**.
- **Permitir configuración VPN:** Permite a los usuarios crear configuraciones VPN. Para dispositivos de perfil de trabajo con Android 6 y versiones posteriores y para dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Permitir servicio de copia de seguridad:** Permite que los usuarios hagan copias de seguridad de los datos de aplicaciones y datos del sistema presentes en sus dispositivos. De forma predeterminada, está **activado**.
- **Permitir NFC:** Permite que los usuarios envíen páginas web, fotos, vídeos y otro contenido desde sus dispositivos a otro dispositivo a través de NFC. Para MDM 4.0 y versiones posteriores. De forma predeterminada, está **activado**.
- **Permitir configuración de proveedor de ubicación:** Permite a los usuarios activar el GPS en sus dispositivos. Para la API 28 de Android y versiones posteriores. De forma predeterminada, está **activado**.
- **Permitir compartir ubicaciones:** En el caso de perfiles administrados, el propietario del dispositivo puede modificar esta configuración. El valor predeterminado es **Desactivado**.

Consejo:

En Citrix Endpoint Management puede crear directivas de localización geográfica para aplicar límites geográficos. Consulte [Directiva de ubicación](#).

- **Permitir que el usuario configure las credenciales de usuario:** Especifique si los usuarios pueden configurar credenciales en el almacén de claves administrado. De forma predeterminada, está **activado**.
- **Permitir impresión:** Si está **activado**, la configuración permite a los usuarios imprimir contenido en cualquier impresora accesible desde el dispositivo del usuario. El valor predeterminado es **Desactivado**. Disponible a partir de Android 9.
- **Permitir depuración por USB:** De forma predeterminada, está **desactivado**.

• Aplicaciones

- **Habilitar aplicaciones del sistema:** Permite a los usuarios ejecutar aplicaciones de dispositivos preinstaladas. El valor predeterminado es **Desactivado**. Para habilitar aplicaciones concretas, 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 quiera habilitar en el dispositivo. **Active** la configuración **Habilitar aplicaciones del sistema** 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>. En dispositivos Android Enterprise, puede restringir los permisos de las aplicaciones mediante la directiva [Permisos de aplicaciones Android Enterprise](#).
- **Inhabilitar aplicaciones:** Bloquea la ejecución de una lista especificada de aplicaciones en dispositivos. El valor predeterminado es **Desactivado**. Para inhabilitar una aplicación instalada, **active** la configuración y haga clic en **Agregar** en la tabla **Lista de aplicaciones**.
 - * **Lista de aplicaciones:** Una lista de las aplicaciones que quiera bloquear. **Active** el parámetro **Inhabilitar aplicaciones** y agregue la aplicación. Escriba el nombre del paquete de la aplicación. Cambiar e implementar una lista de aplicaciones sobrescribe la lista anterior de las aplicaciones. Por ejemplo: Si inhabilita com.ejemplo1 y com.ejemplo2 y, más adelante, cambia la lista a com.ejemplo1 y com.ejemplo3, Citrix Endpoint Management habilita com.ejemplo2.
- **Habilitar verificación de la aplicación.** Permite al sistema operativo examinar aplicaciones para detectar comportamiento malintencionado. De forma predeterminada, está **activado**.
- **Habilitar aplicaciones de Google:** Permite que los usuarios descarguen aplicaciones desde Servicios de Google para Móviles en el dispositivo. De forma predeterminada, está **activado**.
- **Permitir aplicaciones que no son de Google Play:** Permite la instalación de aplicaciones desde 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 al usuario controlar los parámetros de la aplicación:** Permite a los usuarios desinstalar aplicaciones, inhabilitarlas, borrar la memoria caché y los datos, forzar la detención de cualquier aplicación y borrar los valores predeterminados. Los usuarios realizan estas acciones desde la aplicación Configuración. De forma predeterminada, está **desactivado**.
- **Permitir la desinstalación de aplicaciones:** Permite a los usuarios desinstalar aplica-

ciones desde Google Play Store administrado. El valor predeterminado es **Desactivado**.

- **Perfil de trabajo BYOD**

- **Habilitar aplicaciones conectadas:** Si se habilita, los usuarios pueden seleccionar aplicaciones que puedan comunicarse a través de los perfiles profesionales y personales mediante datos profesionales y personales. Una vez habilitada, haga clic en **Agregar**, seleccione las aplicaciones que quiera y haga clic en **Guardar**. Se necesita un perfil de trabajo para habilitar esta función. El valor predeterminado es **Desactivado**.
- **Permitir widgets de la aplicación de perfil de trabajo en la pantalla de inicio:** Si se **activa**, los usuarios pueden colocar widgets de la aplicación de perfil de trabajo en la pantalla de inicio del dispositivo. Si esta configuración está **desactivada**, los usuarios no pueden colocar widgets de la aplicación 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 quiere permitir en la pantalla de inicio. **Active** la configuración **Permite widgets de la aplicación de perfil de trabajo en la pantalla de inicio** y agregue la aplicación. Haga clic en **Agregar** y seleccione, de la lista, la aplicación cuyos widgets quiere permitir en la pantalla de inicio. Haga clic en **Guardar**. Repita este proceso para permitir más widgets de aplicación.
- **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 las llamadas entrantes (Android 7.0 y versiones posteriores). El valor predeterminado es **Desactivado**.

- **Solo dispositivo totalmente administrado**

- **Permitir incorporación de usuarios:** Permite a los usuarios agregar nuevos usuarios a un dispositivo. De forma predeterminada, está **activado**.
- **Permitir itinerancia de datos:** Permite que los usuarios usen su conexión de datos móviles durante la itinerancia. Está desactivado de forma predeterminada, 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 se **activa**, esta configuración habilita la barra de estado en dispositivos administrados y dispositivos dedicados (también conocidos como dispositivos COSU). Esta configuración inhabilita las notificaciones, los parámetros rápidos y otras capas 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 posterior. El valor predeterminado es **Desactivado**.

- **Permitir Bluetooth:** Permite a los usuarios usar Bluetooth. De forma predeterminada, está **activado**.
 - * **Permitir la opción Compartir Bluetooth:** Si no está activado, los usuarios no pueden establecer la opción Compartir Bluetooth saliente en sus dispositivos. Está activado de forma predeterminada.
 - **Permitir configuración de fecha y hora:** Permite a los usuarios cambiar la fecha y la hora en sus dispositivos. De forma predeterminada, está **activado**.
 - **Restablecer valores de fábrica:** Permite que los usuarios restablezcan sus dispositivos a los valores de fábrica. De forma predeterminada, está **activado**.
 - **Mantener encendida la pantalla del dispositivo:** Si se **activa**, la pantalla del dispositivo permanece encendida mientras el dispositivo está conectado. El valor predeterminado es **Desactivado**.
 - **Permitir almacenamiento USB masivo:** Permite la transferencia de archivos de datos de gran tamaño entre los dispositivos de los usuarios y un equipo a través de una conexión USB. De forma predeterminada, está **activado**.
 - **Permitir micrófono:** Permite que los usuarios usen el micrófono en sus dispositivos. De forma predeterminada, está **activado**.
 - **Permitir anclaje a red:** Permite a los usuarios configurar zonas hotspot portátiles y anclar datos. El valor predeterminado es **Desactivado**.
 - **Impedir que Keyguard bloquee el dispositivo:** Si se **activa**, esta configuración desactiva Keyguard 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 redes Wi-Fi y conectarse a ellas. De forma predeterminada, está **activado**.
 - **Permitir transferencia de archivos:** Permite transferencias de archivos a través de USB. El valor predeterminado es **Desactivado**.
- **Samsung**
 - **Habilitar almacén de claves TIMA:** El almacén de claves TIMA ofrece almacenamiento seguro de claves basado en TrustZone para las claves simétricas. Los pares de claves de RSA y los certificados se enrutan al proveedor de almacenamiento de claves predeterminado para su almacenamiento. El valor predeterminado es **Desactivado**.
 - **Permitir uso compartido de lista:** Permite que los usuarios compartan contenido entre las aplicaciones en la lista de Compartir a través de. De forma predeterminada, está **activado**.
 - **Habilitar registros 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 dispositivo totalmente administrado**

- **Habilitar verificación de arranque seguro ODE:** Permite usar la verificación ODE de arranque de confianza para establecer una cadena de confianza desde el cargador de arranque hasta la imagen del sistema. De forma predeterminada, está **activado**.
- **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 que los usuarios recuperen el firmware en sus dispositivos. De forma predeterminada, está **activado**.
- **Permitir cifrado rápido:** Permite el cifrado únicamente del espacio de memoria utilizado. Este cifrado es diferente del cifrado de disco completo, que cifra todos los datos. Estos datos incluyen parámetros, datos de aplicaciones, archivos y aplicaciones descargados, archivos multimedia y más. De forma predeterminada, está **activado**.
- **Modo Common Criteria:** Coloca el dispositivo en el modo Common Criteria. La configuración de Common Criteria impone procesos estrictos de seguridad. De forma predeterminada, está **activado**.
- **Habilitar pancarta de arranque:** Muestra un mensaje o pancarta sobre el uso del sistema aprobado por el DoD cuando los dispositivos de los usuarios se reinician. El valor predeterminado es **Desactivado**.
- **Permitir cambios en los parámetros:** Permite que los usuarios cambien parámetros en sus dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Habilitar el uso de datos en segundo plano:** Permite que las aplicaciones sincronicen datos en segundo plano en dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Permitir portapapeles:** Permite que los usuarios copien datos al portapapeles de sus dispositivos.
 - ★ **Permitir el uso compartido del portapapeles:** Permite que los usuarios compartan el contenido del portapapeles entre sus dispositivos y un equipo (MDM 4.0 y versiones posteriores).
- **Permitir tecla Inicio:** Permite que los usuarios usen la tecla **Inicio** en sus dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Permitir ubicaciones falsas:** Permite que los usuarios indiquen una ubicación de GPS falsa. Para dispositivos totalmente administrados. El valor predeterminado es **Desactivado**.
- **NFC:** Permite que los usuarios usen la transmisión de datos en proximidad o NFC (Near Field Communication) en sus dispositivos totalmente administrados (MDM 3.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir apagado:** Permite que los usuarios apaguen sus dispositivos totalmente administrados (MDM 3.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir Wi-Fi Direct:** Permite a los usuarios conectarse directamente a otro dispositivo a través de su conexión Wi-Fi. De forma predeterminada, está **activado**. Si está **activado**,

debe habilitar la configuración **Permitir cambios de Wi-Fi**.

- **Permitir tarjetas SD:** Permite que los usuarios usen tarjetas SD, si están disponibles, en sus dispositivos. De forma predeterminada, está **activado**.
- **Permitir almacenamiento de hosts de USB:** Permite que los dispositivos de los usuarios actúen como host de USB cuando un dispositivo USB se conecta a ellos. Los dispositivos de los usuarios suministran energía al dispositivo USB. De forma predeterminada, está **activado**.
- **Permitir marcador por voz:** Permite que los usuarios usen el marcador por voz en sus dispositivos (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir S Beam:** Permite que los usuarios compartan contenido con otras personas a través de NFC y Wi-Fi Direct (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir S Voice:** Permite que los usuarios usen el asistente personal inteligente y el explorador de conocimientos en sus dispositivos (MDM 4.0 y versiones posteriores). De forma predeterminada, está **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 opción **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 opción **Permitir anclaje a red** también debe estar **activada**.
 - * **Permitir la opción Compartir Bluetooth:** Si no está activado, los usuarios no pueden establecer la opción Compartir Bluetooth saliente en sus dispositivos. Está activado de forma predeterminada.
- **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 opción **Permitir anclaje a red** también debe estar **activada**.
- **Permitir MMS entrantes:** Permite que los usuarios reciban mensajes MMS. El valor predeterminado es **Desactivado**. Si está **activado**, debe activar la configuración **Permitir SMS**.
- **Permitir MMS salientes:** Permite que los usuarios envíen mensajes MMS. El valor predeterminado es **Desactivado**. Si está **activado**, debe activar la configuración **Permitir SMS**.
- **Permitir SMS entrantes:** Permite que los usuarios reciban mensajes SMS. El valor predeterminado es **Desactivado**. Si está **activado**, debe activar la configuración **Permitir SMS**.
- **Permitir SMS salientes:** Permite que los usuarios envíen mensajes SMS. El valor predeterminado es **Desactivado**. Si está **activado**, debe activar la configuración **Permitir SMS**.

- **Configurar redes móviles:** Permite a los usuarios utilizar su conexión de datos móviles. El valor predeterminado es **Desactivado**.
- **Límite diario (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada día. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
- **Límite semanal (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada semana. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
- **Límite mensual (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada mes. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
- **Permitir solo conexiones VPN seguras:** Permite que los usuarios usen solamente conexiones seguras (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir grabación de audio:** Permite que los usuarios graben sonido con sus dispositivos (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**. Si está **activado**, debe activar la configuración **Permitir micrófono**.
- **Permitir grabación de vídeo:** Permite que los usuarios graben vídeo con sus dispositivos (MDM 4.0 y versiones posteriores). 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 utilizar datos móviles para enviar mensajes push. El valor predeterminado es **Desactivado**. Si está **activado**, debe habilitar la opción **Permitir itinerancia de datos**.
- **Permitir sincronización automática en itinerancia:** Permite a los usuarios utilizar datos móviles para la sincronización. El valor predeterminado es **Desactivado**. Si está **activado**, debe habilitar la opción **Permitir itinerancia de datos**.
- **Permitir llamadas de voz en itinerancia:** Permite a los usuarios utilizar datos móviles para llamadas de voz. El valor predeterminado es **Desactivado**. Si está **activado**, debe habilitar la opción **Permitir itinerancia de datos**.

- **Samsung: Dispositivo totalmente administrado**

- **Habilitar comprobación de revocación:** Habilita la comprobación de certificados revocados. El valor predeterminado es **Desactivado**.

Si **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa** está activado y **Para dispositivos totalmente administrados con perfil de trabajo, la directiva se aplica a** está establecido en **Perfil de trabajo**, configure estos parámetros:

- **Seguridad**

- **Permitir administración de cuentas:** Permite que se agreguen cuentas a perfiles de tra-

bajo y dispositivos administrados. El valor predeterminado es **Desactivado**.

- **Permitir copiar y pegar contenido entre perfiles:** Si está **activado**, los usuarios pueden copiar y pegar contenido entre aplicaciones del perfil de Android Enterprise y aplicaciones del área personal. El valor predeterminado es **Desactivado**.
- **Permitir capturas de pantalla:** Permite a los usuarios grabar o tomar una captura de la pantalla del dispositivo. El valor predeterminado es **Desactivado**.
- **Permitir el uso de la cámara:** Permite a los usuarios tomar fotos y hacer vídeos con la cámara del dispositivo. El valor predeterminado es **Desactivado**.
- **Permitir configuración de proveedor de ubicación:** Permite a los usuarios activar el GPS en sus dispositivos. Para la API 28 de Android y versiones posteriores. De forma predeterminada, está **activado**.
- **Permitir compartir ubicaciones:** En el caso de perfiles administrados, el propietario del dispositivo puede modificar esta configuración. El valor predeterminado es **Desactivado**.

Consejo:

En Citrix Endpoint Management puede crear directivas de localización geográfica para aplicar límites geográficos. Consulte [Directiva de ubicación](#).

- **Permitir que el usuario configure las credenciales de usuario:** Especifique si los usuarios pueden configurar credenciales en el almacén de claves administrado. De forma predeterminada, está **activado**.
- **Permitir impresión:** Si está **activado**, la configuración permite a los usuarios imprimir contenido en cualquier impresora accesible desde el dispositivo del usuario. El valor predeterminado es **Desactivado**. Disponible a partir de Android 9.

• **Aplicaciones**

- **Habilitar aplicaciones del sistema:** Permite a los usuarios ejecutar aplicaciones de dispositivos preinstaladas. El valor predeterminado es **Desactivado**. Para habilitar aplicaciones concretas, 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 quiera habilitar en el dispositivo. **Active** la configuración **Habilitar aplicaciones del sistema** 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>. En dispositivos Android

Enterprise, puede restringir los permisos de las aplicaciones mediante la directiva [Permisos de aplicaciones Android Enterprise](#).

- **Inhabilitar aplicaciones:** Bloquea la ejecución de una lista especificada de aplicaciones en dispositivos. El valor predeterminado es **Desactivado**. Para inhabilitar una aplicación instalada, **active** la configuración y haga clic en **Agregar** en la tabla **Lista de aplicaciones**.
 - ★ **Lista de aplicaciones:** Una lista de las aplicaciones que quiera bloquear. **Active** el parámetro **Inhabilitar aplicaciones** y agregue la aplicación. Escriba el nombre del paquete de la aplicación. Cambiar e implementar una lista de aplicaciones sobre-cribe la lista anterior de las aplicaciones. Por ejemplo: Si inhabilita com.ejemplo1 y com.ejemplo2 y, más adelante, cambia la lista a com.ejemplo1 y com.ejemplo3, Citrix Endpoint Management habilita com.ejemplo2.
- **Habilitar verificación de la aplicación.** Permite al sistema operativo examinar aplicaciones para detectar comportamiento malintencionado. De forma predeterminada, está **activado**.
- **Habilitar aplicaciones de Google:** Permite que los usuarios descarguen aplicaciones desde Servicios de Google para Móviles en el dispositivo. De forma predeterminada, está **activado**.
- **Permitir aplicaciones que no son de Google Play:** Permite la instalación de aplicaciones desde tiendas que no sean Google Play. El valor predeterminado es **Desactivado**.
- **Permitir al usuario controlar los parámetros de la aplicación:** Permite a los usuarios desinstalar aplicaciones, inhabilitarlas, borrar la memoria caché y los datos, forzar la detención de cualquier aplicación y borrar los valores predeterminados. Los usuarios realizan estas acciones desde la aplicación Configuración. De forma predeterminada, está **desactivado**.
- **Permitir la desinstalación de aplicaciones:** Permite a los usuarios desinstalar aplicaciones desde Google Play Store administrado. El valor predeterminado es **Desactivado**.

- **Perfil de trabajo BYOD**

- **Permitir widgets de la aplicación de perfil de trabajo en la pantalla de inicio:** Si se **activa**, los usuarios pueden colocar widgets de la aplicación de perfil de trabajo en la pantalla de inicio del dispositivo. Si esta configuración está **desactivada**, los usuarios no pueden colocar widgets de la aplicación 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 quiere permitir en la pantalla de inicio. **Active** la configuración **Permite widgets de la aplicación de perfil de trabajo en la pantalla de inicio** y agregue la aplicación. Haga clic en **Agregar** y seleccione, de la lista, la aplicación cuyos widgets quiere permitir en la pantalla de inicio. Haga clic en **Guardar**. Repita este proceso para permitir más widgets de aplicación.

- **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 las llamadas entrantes (Android 7.0 y versiones posteriores). El valor predeterminado es **Desactivado**.

- **Samsung**

- **Habilitar almacén de claves TIMA:** El almacén de claves TIMA ofrece almacenamiento seguro de claves basado en TrustZone para las claves simétricas. Los pares de claves de RSA y los certificados se enrutan al proveedor de almacenamiento de claves predeterminado para su almacenamiento. El valor predeterminado es **Desactivado**.
- **Permitir uso compartido de lista:** Permite que los usuarios compartan contenido entre las aplicaciones en la lista de Compartir a través de. De forma predeterminada, está **activado**.
- **Habilitar registros de auditoría:** Permite la creación de registros de auditoría de eventos para el análisis forense de un dispositivo. El valor predeterminado es **Desactivado**.

- **Samsung: Dispositivo totalmente administrado**

- **Habilitar comprobación de revocación:** Habilita la comprobación de certificados revocados. El valor predeterminado es **Desactivado**.

Si **Aplicar a dispositivos totalmente administrados con un perfil de trabajo/Perfil de trabajo en dispositivos propiedad de la empresa** está activado y **Para dispositivos totalmente administrados con perfil de trabajo, la directiva se aplica a** está establecido en **Dispositivo administrado**, configure estos parámetros:

- **Seguridad**

- **Permitir administración de cuentas:** Permite que se agreguen cuentas a perfiles de trabajo y dispositivos administrados. El valor predeterminado es **Desactivado**.
- **Permitir copiar y pegar contenido entre perfiles:** Si está **activado**, los usuarios pueden copiar y pegar contenido entre aplicaciones del perfil de Android Enterprise y aplicaciones del área personal. El valor predeterminado es **Desactivado**.
- **Permitir capturas de pantalla:** Permite a los usuarios grabar o tomar una captura de la pantalla del dispositivo. El valor predeterminado es **Desactivado**.
- **Permitir el uso de la cámara:** Permite a los usuarios tomar fotos y hacer vídeos con la cámara del dispositivo. El valor predeterminado es **Desactivado**.
- **Permitir configuración VPN:** Permite a los usuarios crear configuraciones VPN. Para dispositivos de perfil de trabajo con Android 6 y versiones posteriores y para dispositivos totalmente administrados. De forma predeterminada, está **activado**.

- **Permitir servicio de copia de seguridad:** Permite que los usuarios hagan copias de seguridad de los datos de aplicaciones y datos del sistema presentes en sus dispositivos. De forma predeterminada, está **activado**.
- **Permitir NFC:** Permite que los usuarios envíen páginas web, fotos, vídeos y otro contenido desde sus dispositivos a otro dispositivo a través de NFC. Para MDM 4.0 y versiones posteriores. De forma predeterminada, está **activado**.
- **Permitir configuración de proveedor de ubicación:** Permite a los usuarios activar el GPS en sus dispositivos. Para la API 28 de Android y versiones posteriores. De forma predeterminada, está **activado**.
- **Permitir compartir ubicaciones:** En el caso de perfiles administrados, el propietario del dispositivo puede modificar esta configuración. El valor predeterminado es **Desactivado**.

Consejo:

En Citrix Endpoint Management puede crear directivas de localización geográfica para aplicar límites geográficos. Consulte [Directiva de ubicación](#).

- **Permitir que el usuario configure las credenciales de usuario:** Especifique si los usuarios pueden configurar credenciales en el almacén de claves administrado. De forma predeterminada, está **activado**.
- **Permitir impresión:** Si está **activado**, la configuración permite a los usuarios imprimir contenido en cualquier impresora accesible desde el dispositivo del usuario. El valor predeterminado es **Desactivado**. Disponible a partir de Android 9.
- **Permitir depuración por USB:** De forma predeterminada, está **desactivado**.

• Aplicaciones

- **Habilitar aplicaciones del sistema:** Permite a los usuarios ejecutar aplicaciones de dispositivos preinstaladas. El valor predeterminado es **Desactivado**. Para habilitar aplicaciones concretas, 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 quiera habilitar en el dispositivo. **Active** la configuración **Habilitar aplicaciones del sistema** 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>. En dispositivos Android Enterprise, puede restringir los permisos de las aplicaciones mediante la directiva [Permisos de aplicaciones Android Enterprise](#).

- **Inhabilitar aplicaciones:** Bloquea la ejecución de una lista especificada de aplicaciones en dispositivos. El valor predeterminado es **Desactivado**. Para inhabilitar una aplicación instalada, **active** la configuración y haga clic en **Agregar** en la tabla **Lista de aplicaciones**.
 - * **Lista de aplicaciones:** Una lista de las aplicaciones que quiera bloquear. **Active** el parámetro **Inhabilitar aplicaciones** y agregue la aplicación. Escriba el nombre del paquete de la aplicación. Cambiar e implementar una lista de aplicaciones sobrescribe la lista anterior de las aplicaciones. Por ejemplo: Si inhabilita com.ejemplo1 y com.ejemplo2 y, más adelante, cambia la lista a com.ejemplo1 y com.ejemplo3, Citrix Endpoint Management habilita com.ejemplo2.
 - **Habilitar verificación de la aplicación.** Permite al sistema operativo examinar aplicaciones para detectar comportamiento malintencionado. De forma predeterminada, está **activado**.
 - **Habilitar aplicaciones de Google:** Permite que los usuarios descarguen aplicaciones desde Servicios de Google para Móviles en el dispositivo. De forma predeterminada, está **activado**.
 - **Permitir aplicaciones que no son de Google Play:** Permite la instalación de aplicaciones desde tiendas que no sean Google Play. El valor predeterminado es **Desactivado**.
 - **Permitir al usuario controlar los parámetros de la aplicación:** Permite a los usuarios desinstalar aplicaciones, inhabilitarlas, borrar la memoria caché y los datos, forzar la detención de cualquier aplicación y borrar los valores predeterminados. Los usuarios realizan estas acciones desde la aplicación Configuración. De forma predeterminada, está **desactivado**.
 - **Permitir la desinstalación de aplicaciones:** Permite a los usuarios desinstalar aplicaciones desde Google Play Store administrado. El valor predeterminado es **Desactivado**.
- **Solo dispositivo totalmente administrado**
 - **Permitir incorporación de usuarios:** Permite a los usuarios agregar nuevos usuarios a un dispositivo. De forma predeterminada, está **activado**.
 - **Permitir itinerancia de datos:** Permite que los usuarios usen su conexión de datos móviles durante la itinerancia. Está desactivado de forma predeterminada, 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 se **activa**, esta configuración habilita la barra de estado en dispositivos administrados y dispositivos dedicados (también conocidos como dispositivos COSU). Esta configuración inhabilita las notificaciones, los parámetros rápidos y otras capas 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 posterior. El valor predeterminado es **Desactivado**.

- **Permitir Bluetooth:** Permite a los usuarios usar Bluetooth. De forma predeterminada, está **activado**.
 - * **Permitir la opción Compartir Bluetooth:** Si no está activado, los usuarios no pueden establecer la opción Compartir Bluetooth saliente en sus dispositivos. Está activado de forma predeterminada.
- **Permitir configuración de fecha y hora:** Permite a los usuarios cambiar la fecha y la hora en sus dispositivos. De forma predeterminada, está **activado**.
- **Restablecer valores de fábrica:** Permite que los usuarios restablezcan sus dispositivos a los valores de fábrica. De forma predeterminada, está **activado**.
- **Permitir la protección contra el restablecimiento a los valores de fábrica:** Si está **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 este se configuró antes del reinicio. Si está **desactivado**, no se requiere ninguna autenticación después del restablecimiento. El valor predeterminado es **Activado**.
- **Mantener encendida la pantalla del dispositivo:** Si se **activa**, la pantalla del dispositivo permanece encendida mientras el dispositivo está conectado. El valor predeterminado es **Desactivado**.
- **Permitir almacenamiento USB masivo:** Permite la transferencia de archivos de datos de gran tamaño entre los dispositivos de los usuarios y un equipo a través de una conexión USB. De forma predeterminada, está **activado**.
- **Permitir micrófono:** Permite que los usuarios usen el micrófono en sus dispositivos. De forma predeterminada, está **activado**.
- **Permitir anclaje a red:** Permite a los usuarios configurar zonas hotspot portátiles y anclar datos. El valor predeterminado es **Desactivado**. Cuando esta configuración está activa, están disponibles estas opciones para los dispositivos Samsung:
- **Impedir que Keyguard bloquee el dispositivo:** Si se **activa**, esta configuración desactiva Keyguard 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 redes Wi-Fi y conectarse a ellas. De forma predeterminada, está **activado**.
- **Permitir transferencia de archivos:** Permite transferencias de archivos a través de USB. El valor predeterminado es **Desactivado**.

- **Samsung**

- **Habilitar almacén de claves TIMA:** El almacén de claves TIMA ofrece almacenamiento seguro de claves basado en TrustZone para las claves simétricas. Los pares de claves de RSA

y los certificados se enrutan al proveedor de almacenamiento de claves predeterminado para su almacenamiento. El valor predeterminado es **Desactivado**.

- **Permitir uso compartido de lista:** Permite que los usuarios compartan contenido entre las aplicaciones en la lista de Compartir a través de. De forma predeterminada, está **activado**.
- **Habilitar registros 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 dispositivo totalmente administrado**

- **Habilitar verificación de arranque seguro ODE:** Permite usar la verificación ODE de arranque de confianza para establecer una cadena de confianza desde el cargador de arranque hasta la imagen del sistema. De forma predeterminada, está **activado**.
- **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 que los usuarios recuperen el firmware en sus dispositivos. De forma predeterminada, está **activado**.
- **Permitir cifrado rápido:** Permite el cifrado únicamente del espacio de memoria utilizado. Este cifrado es diferente del cifrado de disco completo, que cifra todos los datos. Estos datos incluyen parámetros, datos de aplicaciones, archivos y aplicaciones descargados, archivos multimedia y más. De forma predeterminada, está **activado**.
- **Modo Common Criteria:** Coloca el dispositivo en el modo Common Criteria. La configuración de Common Criteria impone procesos estrictos de seguridad. De forma predeterminada, está **activado**.
- **Habilitar pancarta de arranque:** Muestra un mensaje o pancarta sobre el uso del sistema aprobado por el DoD cuando los dispositivos de los usuarios se reinician. El valor predeterminado es **Desactivado**.
- **Permitir cambios en los parámetros:** Permite que los usuarios cambien parámetros en sus dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Habilitar el uso de datos en segundo plano:** Permite que las aplicaciones sincronicen datos en segundo plano en dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Permitir portapapeles:** Permite que los usuarios copien datos al portapapeles de sus dispositivos. De forma predeterminada, está **activado**.
 - ★ **Permitir el uso compartido del portapapeles:** Permite que los usuarios compartan el contenido del portapapeles entre sus dispositivos y un equipo (MDM 4.0 y versiones posteriores).
- **Permitir tecla Inicio:** Permite que los usuarios usen la tecla **Inicio** en sus dispositivos totalmente administrados. De forma predeterminada, está **activado**.
- **Permitir ubicaciones falsas:** Permite que los usuarios indiquen una ubicación de GPS

falsa. Para dispositivos totalmente administrados. El valor predeterminado es **Desactivado**.

- **NFC:** Permite que los usuarios usen la transmisión de datos en proximidad o NFC (Near Field Communication) en sus dispositivos totalmente administrados (MDM 3.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir apagado:** Permite que los usuarios apaguen sus dispositivos totalmente administrados (MDM 3.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir Wi-Fi Direct:** Permite a los usuarios conectarse directamente a otro dispositivo a través de su conexión Wi-Fi. De forma predeterminada, está **activado**. Si está **activado**, debe habilitar la configuración **Permitir cambios de Wi-Fi**.
- **Permitir tarjetas SD:** Permite que los usuarios usen tarjetas SD, si están disponibles, en sus dispositivos. De forma predeterminada, está **activado**.
- **Permitir almacenamiento de hosts de USB:** Permite que los dispositivos de los usuarios actúen como host de USB cuando un dispositivo USB se conecta a ellos. Los dispositivos de los usuarios suministran energía al dispositivo USB. De forma predeterminada, está **activado**.
- **Permitir marcador por voz:** Permite que los usuarios usen el marcador por voz en sus dispositivos (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir S Beam:** Permite que los usuarios compartan contenido con otras personas a través de NFC y Wi-Fi Direct (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
- **Permitir S Voice:** Permite que los usuarios usen el asistente personal inteligente y el explorador de conocimientos en sus dispositivos (MDM 4.0 y versiones posteriores). De forma predeterminada, está **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 opción **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 opción **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 opción **Permitir anclaje a red** también debe estar **activada**.
- **Permitir MMS entrantes:** Permite que los usuarios reciban mensajes MMS. El valor predeterminado es **Desactivado**. Si está **activado**, debe activar la configuración **Permitir SMS**.


- **Permitir MMS salientes:** Permite que los usuarios envíen mensajes MMS. El valor predeterminado es **Desactivado**. Si está **activado**, debe activar la configuración **Permitir SMS**.
 - **Permitir SMS entrantes:** Permite que los usuarios reciban mensajes SMS. El valor predeterminado es **Desactivado**. Si está **activado**, debe activar la configuración **Permitir SMS**.
 - **Permitir SMS salientes:** Permite que los usuarios envíen mensajes SMS. El valor predeterminado es **Desactivado**. Si está **activado**, debe activar la configuración **Permitir SMS**.
 - **Configurar redes móviles:** Permite a los usuarios utilizar su conexión de datos móviles. El valor predeterminado es **Desactivado**.
 - **Límite diario (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada día. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
 - **Límite semanal (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada semana. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
 - **Límite mensual (MB).** Introduzca la cantidad de datos móviles (en MB) que los usuarios pueden usar cada mes. El valor predeterminado es 0, lo que inhabilita esta función (MDM 4.0 y versiones posteriores).
 - **Permitir solo conexiones VPN seguras:** Permite que los usuarios usen solamente conexiones seguras (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**.
 - **Permitir grabación de audio:** Permite que los usuarios graben sonido con sus dispositivos (MDM 4.0 y versiones posteriores). De forma predeterminada, está **activado**. Si está **activado**, debe activar la configuración **Permitir micrófono**.
 - **Permitir grabación de vídeo:** Permite que los usuarios graben vídeo con sus dispositivos (MDM 4.0 y versiones posteriores). 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 utilizar datos móviles para enviar mensajes push. El valor predeterminado es **Desactivado**. Si está **activado**, debe habilitar la opción **Permitir itinerancia de datos**.
 - **Permitir sincronización automática en itinerancia:** Permite a los usuarios utilizar datos móviles para la sincronización. El valor predeterminado es **Desactivado**. Si está **activado**, debe habilitar la opción **Permitir itinerancia de datos**.
 - **Permitir llamadas de voz en itinerancia:** Permite a los usuarios utilizar datos móviles para llamadas de voz. El valor predeterminado es **Desactivado**. Si está **activado**, debe habilitar la opción **Permitir itinerancia de datos**.
- **Samsung: Dispositivo totalmente administrado**
 - **Habilitar comprobación de revocación:** Habilita la comprobación de certificados revocados. El valor predeterminado es **Desactivado**.

Parámetros de escritorios y tabletas Windows

Restrictions


This policy allows or restricts the use of certain features on user devices, such as the camera. You can also set security restrictions, restrictions on media content, and the types of apps users can and can't install.


Wi-Fi settings

Allow internet sharing 

Allow auto-connect to Wi-Fi Sense hotspots 

Connectivity

Allow Bluetooth 

Allow VPN over cellular 

Allow VPN over cellular while roaming 

Allow cellular data roaming 

• Parámetros de Wi-Fi

- **Permitir compartir Internet:** Permite que un dispositivo comparta su conexión de Internet con otros dispositivos convirtiéndolo en una zona hotspot de Wi-Fi.

• Conectividad

- **Permitir Bluetooth:** Permite que el dispositivo se conecte a través de Bluetooth.
- **Permitir VPN por red móvil:** Permite que el dispositivo se conecte por VPN a una red de telefonía móvil.
- **Permitir VPN por red móvil durante la itinerancia:** Permite que el dispositivo se conecte por VPN cuando el dispositivo se mueve entre redes de telefonía móvil.
- **Permitir itinerancia de datos móviles:** Permite que los usuarios usen su conexión de datos móviles durante la itinerancia.

• Cuentas

- **Permitir conexión con cuenta de Microsoft:** Permite que el dispositivo use una cuenta de Microsoft para servicios y autenticación de conexiones no relacionados con correo electrónico.
- **Permitir correo electrónico que no es de Microsoft:** Permite que el usuario agregue cuentas de correo electrónico que no son de Microsoft.

• Sistema

- **Permitir tarjeta de almacenamiento:** Permite que el dispositivo use una tarjeta de almacenamiento.

- **Telemetría:** En la lista, haga clic en una opción para permitir o impedir que el dispositivo envíe información de telemetría. El valor predeterminado es **Permitida**. Las demás opciones son: **No permitida** y **Permitida, excepto para solicitudes de datos secundarios**.
- **Permitir el acceso de la aplicación al servicio de localización:** Permite el acceso de la aplicación a los servicios de localización.
- **Permitir la versión Tech Preview de compilaciones internas:** Permite que los usuarios obtengan una versión Tech Preview de las compilaciones internas de Microsoft.
- **Cámara:** Solo escritorios o tabletas Windows.
 - **Permitir el uso de la cámara:** Permite que los usuarios usen la cámara del dispositivo.
- **Bluetooth:** Solo para escritorios o tabletas Windows.
 - **Permitir modo detectable:** Permite que los dispositivos Bluetooth encuentren el dispositivo local.
 - **Nombre del dispositivo local:** Un nombre para el dispositivo local.
- **Experiencia:** Solo para escritorios o tabletas Windows.
 - **Permitir Cortana:** Permite que los usuarios accedan al asistente personal inteligente y explorador de conocimientos llamado Cortana.
 - **Permitir detección de dispositivos:** Permite la detección de red del dispositivo.
 - **Permitir desinscripción manual de MDM:** Permite que los usuarios desinscriban manualmente sus dispositivos de Citrix Endpoint Management MDM.
 - **Permitir sincronizar parámetros del dispositivo:** Permite que los usuarios sincronicen parámetros entre dispositivos con Windows 10 o Windows 11 durante la itinerancia.
- **Encima de bloqueo:** Solo para escritorios o tabletas Windows.
 - **Permitir notificaciones del sistema en la pantalla de bloqueo:** Permite notificaciones del sistema en la pantalla de bloqueo. Solo para escritorios o tabletas Windows.
- **Aplicaciones**
 - **Permitir actualizaciones automáticas desde la tienda de aplicaciones:** Permite que las aplicaciones de la tienda de aplicaciones se actualicen automáticamente. Solo para escritorios o tabletas Windows.
- **Privacidad:** Solo para escritorios o tabletas Windows.
 - **Permitir personalización de entradas:** Permite ejecutar el servicio de personalización de entradas. El servicio de personalización de entradas mejora las entradas predictivas como el lápiz y el teclado táctil en función de lo que escribe un usuario.
- **Configuración:** Solo para escritorios o tabletas Windows.

- **Permitir reproducción automática:** Permite que los usuarios cambien los parámetros de la reproducción automática.
- **Permitir Sensor de datos:** Permite que los usuarios cambien los parámetros de Sensor de datos.
- **Permitir fecha y hora:** Permite que los usuarios cambien los parámetros de la fecha y la hora.
- **Permitir idioma:** Permite que los usuarios cambien los parámetros de idioma.
- **Permitir suspensión:** Permite que los usuarios cambien los parámetros de suspensión.
- **Permitir región:** Permite que los usuarios cambien los parámetros de región.
- **Permitir opciones de inicio de sesión:** Permite que los usuarios cambien los parámetros de inicio de sesión.
- **Permitir área de trabajo:** Permite que los usuarios cambien los parámetros del área de trabajo.
- **Permitir su cuenta:** Permite que los usuarios cambien los parámetros de cuenta.

Parámetros de Amazon

Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Allow hardware controls

Factory reset

ON

Profiles

ON

Allow apps

Non-Amazon Appstore apps

ON

Social networks

ON

Network

Bluetooth

ON

WiFi switch

ON

WiFi settings

ON

Cellular data

ON

Roaming data

ON

- **Permitir controles del hardware**
 - **Restablecer valores de fábrica:** Permite que los usuarios restablezcan sus dispositivos a los valores de fábrica.
 - **Perfiles:** Permite que los usuarios cambien el perfil de hardware en sus dispositivos.
- **Permitir aplicaciones**

- **Aplicaciones que no son de la Tienda Apps de Amazon:** Permite que los usuarios instalen en sus dispositivos aplicaciones que no provienen de la tienda Amazon Appstore.
- **Redes sociales:** Permite que los usuarios accedan a redes sociales desde sus dispositivos.
- **Red**
 - **Bluetooth:** Permite que los usuarios usen Bluetooth.
 - **Conmutador Wi-Fi:** Permite que las aplicaciones cambien el estado de la conectividad de las redes Wi-Fi.
 - **Parámetros de Wi-Fi:** Permite que los usuarios cambien los parámetros de las redes Wi-Fi.
 - **Configurar redes móviles:** Permite que los usuarios usen su conexión de datos móviles.
 - **Datos de itinerancia:** Permite que los usuarios usen su conexión de datos móviles durante la itinerancia.
 - **Servicios de localización:** Permite que los usuarios usen GPS.
- **Acciones de USB:**
 - **Depuración:** Permite que los dispositivos de los usuarios se conecten mediante USB a un equipo para su depuración.

Directiva de itinerancia

November 29, 2023

En Citrix Endpoint Management, puede agregar una directiva de dispositivo para configurar si se permite la itinerancia de voz y de datos en dispositivos iOS admitidos. Si se inhabilita la itinerancia de voz, 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](#).

Parámetros de iOS

- **Inhabilitar itinerancia de voz:** Seleccione si inhabilitar la itinerancia de voz. Si se inhabilita esta opción, la itinerancia de datos se inhabilita automáticamente. El valor predeterminado es **No**, lo que permite la itinerancia de voz.
- **Inhabilitar itinerancia de datos.** Seleccione si inhabilitar la itinerancia de datos. Esta opción solo está disponible cuando la itinerancia de voz está habilitada. El valor predeterminado es **No**, lo que permite la itinerancia de datos.

Directiva de SCEP

November 29, 2023

Esta directiva le permite configurar dispositivos iOS y macOS para obtener un certificado desde un servidor SCEP externo mediante el Protocolo de inscripción de certificados simple (SCEP). Para entregar un certificado a dispositivos mediante SCEP desde una infraestructura de clave pública que está conectada a Citrix Endpoint Management, cree una entidad de infraestructura de clave pública y un proveedor de 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](#).

Parámetros de iOS

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
SCEP Policy This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.						
SCEP Policy						
1 Policy Info						
2 Platforms						
<input checked="" type="checkbox"/> iOS		URL base *				
<input checked="" type="checkbox"/> macOS		Instance name *				
3 Assignment		Subject X.500 name (RFC 2253)				
		Subject alternative names type				
		Maximum retries				
		Retry delay				
		Challenge password				
		Key size (bits)				
		Use as digital signature				
		Use for key encipherment				

- **URL base.** Escriba la dirección del servidor SCEP para definir dónde se enviarán las solicitudes SCEP, ya sea por HTTP o por HTTPS. La clave privada no se envía con la solicitud de firma de certificado (CSR), por lo que es posible que enviar la solicitud sin cifrar sea una opción segura. Si la contraseña de un solo uso está configurada para su reutilización, use HTTPS para proteger la contraseña. Este paso es obligatorio.
- **Nombre de la instancia.** Escriba cualquier cadena que reconozca el servidor SCEP. Por ejemplo, puede ser un nombre de dominio, como ejemplo.org. Si una entidad de certificación dispone de varios certificados de CA, puede usar este campo para diferenciar el dominio pertinente. Este paso es obligatorio.
- **Nombre de sujeto X.500 (RFC 2253):** Escriba la representación de un nombre de X.500 como

una matriz de identificadores OID y valores. Por ejemplo, `/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar`, que se traduce en: `[[[“C”, “US”]], [[“O”, “Apple Inc.”]], ..., [[“1.2.5.3”, “bar”]]]`. Los identificadores OID se pueden representar como números con puntos y que disponen de accesos directos para el país (C), la localidad (L), el estado (ST), la organización (O), la unidad organizativa (OU) y el 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 entidad de certificación para emitir un certificado. Puede especificar **Ninguno**, **Nombre RFC 822**, **Nombre DNS** o **URI**.
- **Máximo de reintentos.** Escriba la cantidad de veces que un dispositivo vuelve a intentar conectarse cuando el servidor SCEP envía la respuesta PENDIENTE. El valor predeterminado es **3**.
- **Demora entre reintentos.** Escriba la cantidad de segundos que deben transcurrir entre los reintentos. El primer reintento se produce sin retraso. El valor predeterminado es **10**.
- **Verificar contraseña.** Escriba un secreto previamente compartido.
- **Tamaño de la clave (bits):** Seleccione **2048** o un valor superior para el tamaño de la clave en bits.
- **Usar como firma digital:** Elija si quiere utilizar el certificado como firma digital. El servidor SCEP verifica el uso de certificados como firma digital antes de utilizar la clave pública para descifrar el hash.
- **Usar para el cifrado de claves:** Elija si quiere utilizar el certificado para el cifrado de claves. Un servidor comprueba primero si el certificado proporcionado por un cliente se puede usar para el cifrado de claves. A continuación, el servidor utiliza la clave pública en un certificado para verificar que una parte de los datos se cifró mediante la clave privada. Si no es así, la operación no se puede realizar.
- **Huella digital SHA-256 (cadena hexadecimal):** Si la entidad de certificación utiliza HTTP, utilice este campo para la huella digital del certificado de CA. El dispositivo utiliza la huella digital para confirmar la autenticidad de la respuesta de la entidad de certificación durante la inscripción. Puede proporcionar una huella digital SHA-256 o puede seleccionar un certificado para importar su firma.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones

posteriores.

Parámetros de macOS

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

SCEP Policy

1 Policy Info

2 Platforms

☐ iOS

☒ macOS

3 Assignment

SCEP Policy

This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.

URL base *

Instance name *

Subject X.500 name (RFC 2253)

Subject alternative names type

None

Maximum retries

3

Retry delay

10

Challenge password

Key size (bits)

1024

Use as digital signature

OFF

Use for key encipherment

OFF

- **URL base.** Escriba la dirección del servidor SCEP para definir dónde se enviarán las solicitudes SCEP, ya sea por HTTP o por HTTPS. La clave privada no se envía con la solicitud de firma de certificado (CSR), por lo que es posible que enviar la solicitud sin cifrar sea una opción segura. Si la contraseña de un solo uso está configurada para su reutilización, use HTTPS para proteger la contraseña. Este paso es obligatorio.
- **Nombre de la instancia.** Escriba cualquier cadena que reconozca el servidor SCEP. Por ejemplo, puede ser un nombre de dominio, como ejemplo.org. Si una entidad de certificación dispone de varios certificados de CA, puede usar este campo para diferenciar el dominio pertinente. Este paso es obligatorio.
- **Nombre de sujeto X.500 (RFC 2253):** Escriba la representación de un nombre de X.500 como una matriz de identificadores OID y valores. Por ejemplo, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, que se traduce en: [[[“C”, “US”]], [[“O”, “Apple Inc.”]], ..., [[“1.2.5.3”, “bar”]]]. Los identificadores OID se pueden representar como números con puntos y que disponen de accesos directos para el país (C), la localidad (L), el estado (ST), la organización (O), la unidad organizativa (OU) y el 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 entidad de certificación para emitir un certificado. Puede especificar **Ninguno**, **Nombre RFC 822**, **Nombre DNS** o **URI**.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

894

- **Máximo de reintentos.** Escriba la cantidad de veces que un dispositivo vuelve a intentar conectarse cuando el servidor SCEP envía la respuesta PENDIENTE. El valor predeterminado es **3**.
- **Demora entre reintentos.** Escriba la cantidad de segundos que deben transcurrir entre los reintentos. El primer reintento se produce sin retraso. El valor predeterminado es **10**.
- **Verificar contraseña.** Escriba un secreto previamente compartido.
- **Tamaño de la clave (bits):** Seleccione **2048** o un valor superior para el tamaño de la clave en bits.
- **Usar como firma digital:** Elija si quiere utilizar el certificado como firma digital. El servidor SCEP verifica el uso de certificados como firma digital antes de utilizar la clave pública para descifrar el hash.
- **Usar para el cifrado de claves:** Elija si quiere utilizar el certificado para el cifrado de claves. Un servidor comprueba primero si el certificado proporcionado por un cliente se puede usar para el cifrado de claves. A continuación, el servidor utiliza la clave pública en un certificado para verificar que una parte de los datos se cifró mediante la clave privada. Si no es así, la operación no se puede realizar.
- **Huella digital SHA-256 (cadena hexadecimal):** Si la entidad de certificación utiliza HTTP, utilice este campo para la huella digital del certificado de CA. El dispositivo utiliza la huella digital para confirmar la autenticidad de la respuesta de la entidad de certificación durante la inscripción. Puede proporcionar una huella digital SHA-256 o puede seleccionar un certificado para importar su firma.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar 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**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
 - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Directivas de Siri y dictado

November 29, 2023

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 a través de los servicios de nube de Apple, y por lo tanto existen fuera del contenedor seguro de Citrix Endpoint Management. El texto resultado del dictado, sin embargo, queda dentro del contenedor.

Citrix Endpoint Management permite bloquear los servicios de dictado y Siri, si sus necesidades de seguridad lo exigen.

En las implementaciones de administración de aplicaciones móviles (MAM), la directiva **Bloquear dictado** para cada aplicación tiene el valor **Sí** (activado) de forma predeterminada, lo que inhabilita el micrófono del dispositivo. Configúrela con el valor **No** si quiere permitir el dictado. La directiva se encuentra en la consola de Citrix Endpoint Management, en **Configurar > Aplicaciones**. Seleccione la aplicación, haga clic en **Modificar** y, a continuación, haga clic en **iOS**.

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
MDX		App Restrictions				
1 App Information		Block camera <input checked="" type="checkbox"/> ON ?				
2 Platform		Block Photo Library <input checked="" type="checkbox"/> ON ?				
<input checked="" type="checkbox"/> iOS		Block mic record <input checked="" type="checkbox"/> ON ?				
<input type="checkbox"/> Android		Block dictation <input type="checkbox"/> OFF ?				
<input type="checkbox"/> Windows Phone		Block location services <input checked="" type="checkbox"/> ON ?				
<input type="checkbox"/> Windows Desktop/Tablet		Block SMS compose <input checked="" type="checkbox"/> ON ?				
3 Approvals (optional)						
4 Delivery Group Assignments (optional)						

En las implementaciones MDM (administración de dispositivos móviles), también puede inhabilitar Siri desde la directiva de Siri, en **Configurar > Directivas de dispositivo**. El uso de Siri está permitido de manera predeterminada.

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
<h2>Restrictions Policy</h2> <p>This policy allows or restricts users from using certain features on their devices, such as the camera media content and on certain types of apps users can and cannot install.</p> <p>Allow hardware controls</p>						
<h3>1 Policy Info</h3>						
<h3>2 Platforms</h3>						
<input checked="" type="checkbox"/> iOS						
<input checked="" type="checkbox"/> macOS						
<input checked="" type="checkbox"/> Samsung SAFE						
<input checked="" type="checkbox"/> Samsung KNOX						
<input checked="" type="checkbox"/> Windows Phone						
<input checked="" type="checkbox"/> Windows Desktop/Tablet						
<input checked="" type="checkbox"/> Amazon						
<div><div>Camera</div><div>ON</div></div> <div><input checked="" type="checkbox"/> FaceTime ?</div> <div><div>Screen shots</div><div>ON</div></div> <div><div>Photo streams</div><div>ON</div> iOS 5.0+</div> <div><div>Shared photo streams</div><div>ON</div> iOS 6.0+</div> <div><div>Voice dialing</div><div>ON</div></div> <div><div>Siri</div><div>ON</div></div> <div><input checked="" type="checkbox"/> Allow while device is locked</div> <div><input type="checkbox"/> Siri profanity filter</div>						

Hay algunas cuestiones a tener en cuenta a la hora de decidir si se permiten Siri y el dictado:

- De acuerdo con la información que Apple ha hecho pública, Apple guarda datos de clips de voz y Siri por un máximo de dos años. Se asigna un número aleatorio a los datos, para representar al usuario, y los archivos de voz se asocian con dicho número.
- Puede consultar la directiva de privacidad de Apple yendo a **Ajustes > General > Teclados** en cualquier dispositivo iOS, y tocando el enlace bajo **Habilitar dictado**.

Directiva de cuenta SSO

November 29, 2023

La directiva “Cuenta SSO” permite crear cuentas de inicio de sesión único (SSO) en Citrix Endpoint Management. Con esas cuentas, los usuarios solo necesitan iniciar sesión una vez para acceder a Citrix Endpoint Management y a los recursos internos de la empresa desde varias aplicaciones. Así, no es necesario que los usuarios almacenen credenciales en el dispositivo. Las credenciales de usuario de empresa de la cuenta SSO se pueden usar en varias aplicaciones, incluidas las aplicaciones del App Store de Apple. Esta directiva está pensada para funcionar con un servidor 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](#).

Parámetros de iOS

- **Nombre de cuenta.** Escriba el nombre de la cuenta SSO de Kerberos que aparece en los dispositivos de los usuarios. Este campo es obligatorio.
- **Nombre principal de Kerberos.** Escriba el nombre de la entidad de seguridad asignada a Kerberos. Este campo es obligatorio.
- **Credencial de identidad (credencial PKI o de almacén de claves).** En la lista, haga clic en una de las credenciales de identidad opcionales que se pueden usar para renovar la credencial de Kerberos sin la interacción del usuario.
- **Territorio de Kerberos.** Escriba el territorio de Kerberos designado a esta directiva. Por regla general, se trata de su nombre de dominio en letras mayúsculas (por ejemplo, EJEMPLO.COM). Este campo es obligatorio.
- **Direcciones URL permitidas.** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada URL que deba requerir el inicio Single Sign-On:
 - **URL permitida:** Introduzca una URL que deba requerir SSO cuando un usuario la visite desde el dispositivo iOS.

Por ejemplo: cuando un usuario intenta abrir un sitio web y este sitio pide una comprobación de Kerberos, si ese sitio no está en la lista de direcciones URL, el dispositivo iOS no intenta el inicio Single Sign-On con el token de Kerberos que se haya almacenado en caché en el dispositivo después de un inicio de sesión Kerberos previo. La coincidencia debe ser exacta en la parte de 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 de HTTP estándar. Esto podría significar casi cualquier cosa, desde un desafío de contraseña estándar hasta un error HTTP si la URL solo está configurada para SSO mediante Kerberos.
 - Haga clic en **Agregar** para agregar la URL, o bien haga clic en **Cancelar** para no agregarla.
- **Identificadores de aplicaciones.** Haga clic en **Agregar** y lleve a cabo lo siguiente para cada aplicación que pueda emplear este inicio de sesión:
 - **Identificador de aplicación.** Escriba el identificador de aplicación perteneciente a una aplicación que pueda utilizar esta credencial. Si no se agrega ningún identificador de aplicación, esta credencial coincidirá con **todos** los identificadores de aplicación.
- **Configuraciones de directivas**

- **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Directiva de tiendas

November 29, 2023

En Citrix Endpoint Management, puede crear una directiva para especificar si los dispositivos mostrarán un clip web del almacén 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](#).

Parámetros de escritorios y tabletas Windows, iOS y Android

Para cada plataforma que quiera configurar, seleccione si aparecerá un clip web del almacén de aplicaciones en los dispositivos de los usuarios. El valor predeterminado es **Activado**.

Directiva de calendarios suscritos

November 29, 2023

En Citrix Endpoint Management, puede agregar una directiva de dispositivo para agregar un calendario suscrito a la lista de calendarios en los dispositivos iOS. La lista de calendarios públicos a los que puede suscribirse está disponible en la página de asistencia 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 para poder agregarlo a la lista de calendarios suscritos en los dispositivos de los usuarios.

Parámetros de iOS

- **Descripción.** Introduzca una descripción del calendario. Este campo es obligatorio.
- **URL.** Introduzca la dirección URL del calendario. Puede introducir una dirección URL [webcal](#) : // o un enlace [https](#) : // a un archivo de iCalendar (.ics). Este campo es obligatorio.
- **Nombre de usuario.** Escriba el nombre de inicio de sesión del usuario. Este campo es obligatorio.
- **Contraseña.** Escriba una contraseña opcional de usuario.
- **Usar SSL.** Seleccione si utilizar una conexión de Secure Sockets Layer (SSL) para el calendario. El valor predeterminado es **Desactivado**.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Directiva de términos y condiciones

November 29, 2023

En Citrix Endpoint Management, puede crear directivas de términos y condiciones cuando quiera que los usuarios acepten aquellas directivas específicas de la empresa que rijan las conexiones a la red corporativa. Cuando los usuarios inscriban sus dispositivos en Citrix Endpoint Management, se les presentarán los términos y las condiciones, y deberán aceptarlos para llevar a cabo la inscripción. Si rechazan dichos términos y condiciones, se cancelará el proceso de inscripción.

Si la empresa tiene usuarios internacionales y quiere que acepten los términos y las condiciones en su idioma nativo, puede crear directivas distintas para los términos y las condiciones en diferentes idiomas. Debe suministrar un archivo para cada combinación de plataforma e idioma que quiera implementar. Para dispositivos Android y iOS, debe proporcionar archivos PDF. Para dispositivos Windows, debe suministrar archivos de texto (.txt) y los archivos de imagen correspondientes.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS y Android

- **Archivos a importar:** Seleccione el archivo de términos y condiciones a importar; para ello, haga clic en **Examinar** y, a continuación, vaya a 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 términos y condiciones diferentes. El valor predeterminado es **Desactivado**.

Nota:

Los términos y condiciones no se muestran si el dispositivo iOS está inscrito en el Programa de inscripción de dispositivos (DEP).

Configuración de tabletas Windows

- **Archivos a importar:** Seleccione el archivo de términos y condiciones a importar; para ello, haga clic en **Examinar** y, a continuación, vaya a la ubicación del archivo.
- **Imagen:** Para seleccionar el archivo de imagen a importar, haga clic en **Examinar** y vaya a la ubicación de ese archivo.
- **Términos y condiciones predeterminados:** Seleccione si este archivo es el documento predeterminado para los usuarios que son miembros de varios grupos con términos y condiciones diferentes. El valor predeterminado es **Desactivado**.

Directiva de túnel

November 29, 2023

Los túneles de aplicaciones están diseñados para aumentar la continuidad del servicio y la fiabilidad de la transferencia de datos para las aplicaciones móviles. Los túneles de aplicaciones se usan para definir parámetros de proxy entre el componente del cliente de cualquier aplicación del dispositivo móvil y el componente del servidor de aplicaciones. Puede configurar la directiva Túnel para dispositivos Android.

Todo tráfico de aplicaciones enviado a través de un túnel definido en esta directiva se dirigirá a través de Citrix Endpoint Management antes de redirigirse 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](#).

Parámetros de Android

Tunnel Policy

This policy lets you configure an app tunnel. While doing so, you can choose if the tunnel will be used for the remote support app.

Use this tunnel for remote support ☐ OFF

Connection configuration

Connection initiated by ?

Maximum connections per device * ?

Define connection time out ☐ OFF ?

Block cellular connections passing by this tunnel ☐ OFF ?

App device parameters

Client port * ?

App server parameters

IP address or server name *

Server port *

- **Conexión iniciada por.** Haga clic en **Dispositivo** o **Servidor** para indicar la fuente que inicia la conexión.
- **Conexiones máximas por dispositivo:** Escriba la cantidad de conexiones TCP simultáneas que puede establecer la aplicación. Este campo solo se aplica a conexiones iniciadas desde un dispositivo.
- **Definir el tiempo de espera de la conexión:** Seleccione si quiere establecer el intervalo de tiempo que una aplicación puede estar inactiva antes de que se cierre el túnel.
 - **Tiempo de espera de la conexión.** Si **activa** el parámetro **Definir el tiempo de espera de la conexión**, escriba la cantidad de tiempo en segundos que una aplicación puede estar inactiva antes de que se cierre el túnel.
- **Bloquear el paso de las conexiones de móvil por este túnel.** Seleccione si este túnel se bloqueará cuando el dispositivo se encuentre en el modo de itinerancia. Las conexiones Wi-Fi y USB no se bloquean.
- **Puerto cliente:** Escriba el número de puerto del cliente. En la mayoría de los casos, este es el mismo valor que el del puerto del servidor.
- **Dirección IP o nombre del servidor.** Escriba el nombre o la dirección IP del servidor de aplicaciones. Este campo solo se aplica a conexiones iniciadas desde un dispositivo.
- **Puerto del servidor.** Escriba el número de puerto del servidor.

Directiva de VPN

March 1, 2024

La directiva “VPN” permite configurar los parámetros de una red privada virtual (VPN) que permita a los dispositivos de los usuarios conectarse de forma segura a los recursos de la empresa. Puede configurar la directiva de VPN para las plataformas siguientes. Cada plataforma requiere un conjunto diferente de valores, que se describen detalladamente en este artículo.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Requisitos para las redes VPN por aplicación

Puede configurar la función de VPN por aplicación para estas plataformas a través de directivas VPN:

- iOS
- macOS
- Android (AD heredado)

Para Android Enterprise, use la [directiva Configuraciones administradas](#) para configurar perfiles de VPN.

Las opciones de VPN por aplicación están disponibles para ciertos tipos de conexión. Esta tabla indica cuándo están disponibles las opciones de VPN por aplicación.

Plataforma	Tipo de conexión	Comentario
iOS	Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix SSO o SSL personalizado.	
macOS	Cisco AnyConnect, Juniper SSL, SSL F5, SonicWALL Mobile Connect, Ariba VIA o SSL personalizado.	
Android (AD heredado)	Citrix SSO	

Para crear una VPN por aplicación en dispositivos iOS y Android (AD heredado) mediante la aplicación Citrix SSO, debe realizar otros pasos, además de la configuración de la directiva VPN. Además, debe comprobar que se cumplen estos requisitos previos:

- NetScaler Gateway local
- Estas aplicaciones están instaladas en el dispositivo:
 - Citrix SSO
 - Citrix Secure Hub

He aquí un flujo de trabajo general para configurar una VPN por aplicación en dispositivos iOS y Android mediante la aplicación Citrix SSO:

1. Configure una directiva de dispositivos VPN tal y como se describe en este artículo.
 - Para iOS, consulte [Configurar el protocolo Citrix SSO para iOS](#). Después de configurar el protocolo de Citrix SSO para iOS a través de una directiva de dispositivos VPN, también debe crear una directiva de atributos de aplicación para asociar las aplicaciones 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 por certificado para Citrix Endpoint Management. Consulte [Autenticación con certificado de cliente o certificado y dominio](#).
 - Para Android (AD heredado), consulte [Configurar el protocolo Citrix SSO para Android](#).
 - Para el campo **Tipo de autenticación para la conexión**, si selecciona **Certificado o Contraseña y certificado**, primero debe configurar la autenticación por certificado para Citrix Endpoint Management. Consulte [Autenticación con certificado de cliente o certificado y dominio](#).
2. Configure Citrix ADC para aceptar el tráfico de la VPN por aplicación. Para obtener información detallada, consulte [Configuración de VPN completa en NetScaler Gateway](#).

Parámetros de iOS

Tenga en cuenta que el tipo de conexión VPN de Citrix en la directiva VPN para iOS no admite iOS 12. Lleve a cabo estos pasos para eliminar la directiva de VPN existente y crear otra directiva de VPN con el tipo de conexión Citrix SSO:

1. Elimine su directiva de VPN para iOS.
2. Agregue una directiva de redes VPN para iOS con la siguiente configuración:
 - **Tipo de conexión: Citrix SSO**
 - **Habilitar VPN por aplicación: Sí**
 - **Tipo de proveedor: Túnel de paquete**
3. Agregue una directiva de atributos de aplicaciones para iOS. En **Identificador de VPN por aplicación**, elija **iOS_VPN**.

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
VPN Policy This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.						
1 Policy Info						
2 Platforms						
<input checked="" type="checkbox"/> iOS						
<input checked="" type="checkbox"/> macOS						
<input checked="" type="checkbox"/> Android						
<input checked="" type="checkbox"/> Samsung SAFE						
<input checked="" type="checkbox"/> Samsung KNOX						
<input checked="" type="checkbox"/> Windows Phone						
<input checked="" type="checkbox"/> Windows Desktop/Tablet						
<input checked="" type="checkbox"/> Amazon						
3 Assignment						
VPN Policy This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.						
Connection name <input type="text"/> ⓘ						
Connection type <input type="text" value="L2TP"/> ⓘ						
Server name or IP address * <input type="text"/> ⓘ						
User account <input type="text"/> ⓘ						
<input checked="" type="radio"/> Password authentication <input type="radio"/> RSA SecureID authentication						
Shared secret <input type="text"/> ⓘ						
Send all traffic <input type="checkbox"/> OFF ⓘ						
Proxy configuration <input type="text" value="None"/> ⓘ						

- **Nombre de la conexión:** Escriba un nombre para la conexión.
- **Tipo de conexión:** En la lista, seleccione el protocolo que se va a usar para esta conexión. El valor predeterminado es **L2TP**.
 - **L2TP:** Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida.
 - **PPTP:** Túnel punto a punto.
 - **IPsec:** La conexión VPN de su empresa.
 - **Cisco Legacy AnyConnect.** Este tipo de conexión requiere que el cliente VPN de Cisco Legacy AnyConnect esté instalado en el dispositivo del usuario. Cisco ha empezado a retirar progresivamente el cliente Cisco Legacy AnyConnect, basado en un framework de VPN que se ha retirado.
Para utilizar el cliente actual de Cisco AnyConnect, use el **Tipo de conexión** llamado **SSL personalizado**. Para conocer la configuración requerida, consulte “Configurar el protocolo SSL personalizado” en esta sección.
 - **Juniper SSL:** Cliente SSL VPN de Juniper Networks.
 - **F5 SSL:** Cliente SSL VPN de F5 Networks.
 - **SonicWALL Mobile Connect:** Cliente VPN unificado de Dell para iOS.
 - **Ariba VIA:** Cliente de acceso virtual a Internet de Ariba Networks.
 - **IKEv2 (solo iOS).** Intercambio de claves por red versión 2 solo para iOS.
 - **AlwaysOn IKEv2:** Acceso permanente mediante IKEv2.
 - **Configuración dual de AlwaysOn IKEv2:** Acceso permanente mediante la configuración dual de IKEv2.

- **Citrix SSO:** Cliente de Citrix SSO para iOS 12 y versiones posteriores.
- **SSL personalizado:** Secure Sockets Layer (SSL) personalizada. Se requiere este tipo de conexión para el cliente Cisco AnyConnect que tiene un ID de paquete **com.cisco.anyconnect**. Indique el **Nombre de conexión** llamado **Cisco AnyConnect**. También puede implementar la directiva de VPN y habilitar un filtro de Control de acceso a red (NAC) para dispositivos iOS. El filtro NAC bloquea una conexión VPN para dispositivos que tienen instaladas aplicaciones no conformes. La configuración requiere configuraciones específicas para la directiva de VPN de iOS, como se describe en la siguiente sección de iOS. Para obtener más información sobre otras configuraciones necesarias para habilitar el filtro NAC, consulte [Control de acceso a red](#).

En las siguientes secciones se ofrecen las opciones de configuración para cada uno de los tipos de conexión mencionados.

Configurar el protocolo L2TP para iOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- Seleccione **Autenticación por contraseña** o **Autenticación con RSA SecureID**.
- **Secreto compartido:** Escriba la clave de secreto compartido de IPsec.
- **Enviar todo el tráfico:** Seleccione si enviar todo el tráfico por la red privada virtual (VPN). El valor predeterminado es **Desactivado**.

Configurar el protocolo PPTP para iOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- Seleccione **Autenticación por contraseña** o **Autenticación con RSA SecureID**.
- **Nivel de cifrado.** En la lista, seleccione un nivel de cifrado. El valor predeterminado es **Ninguno**.
 - **Ninguno:** No se usa ningún cifrado.
 - **Automático:** Se usa el nivel más alto de cifrado que admite el servidor.
 - **Máximo (128 bits):** Se usa siempre el cifrado de 128 bits.
- **Enviar todo el tráfico:** Seleccione si enviar todo el tráfico por la red privada virtual (VPN). El valor predeterminado es **Desactivado**.

Configurar el protocolo IPsec para iOS

- **Nombre o dirección IP del servidor:** Escriba el nombre 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 elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Secreto compartido**.
- Si ha seleccionado **Secreto compartido**, configure los siguientes parámetros:
 - **Nombre del grupo:** Escriba un nombre de grupo opcional.
 - **Secreto compartido:** Escriba una clave opcional de secreto compartido.
 - **Usar autenticación híbrida:** Seleccione si utilizar la autenticación híbrida. Con la autenticación híbrida, el servidor se autentica primero en el cliente, y, a continuación, se autentica en el servidor. El valor predeterminado es **Desactivado**.
 - **Pedir contraseña:** Seleccione si solicitar a los usuarios sus contraseñas cuando se conectan a la red. El valor predeterminado es **Desactivado**.
- Si habilita **Certificado**, defina las siguientes configuraciones:
 - **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
 - **Pedir PIN al conectar:** Seleccione esta opción para obligar a los usuarios a introducir su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
 - **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**.
- **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. El valor predeterminado es **Desactivado**.
- **Dominios de Safari:** Haga clic en **Agregar** para agregar un nombre de dominio de Safari.

Configurar el protocolo Cisco Legacy AnyConnect para iOS

Para realizar la transición del cliente Cisco Legacy AnyConnect al nuevo cliente Cisco AnyConnect, use el protocolo “SSL personalizado”.

- **Identificador de paquete de proveedor.** Para el cliente Legacy AnyConnect, el ID de paquete es com.cisco.anyconnect.gui.
- **Nombre o dirección IP del servidor:** Escriba el nombre 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 elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
 - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
 - Si habilita **Certificado**, defina las siguientes configuraciones:
 - * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
 - * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
 - * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Incluir todas las redes:** Seleccione si permitir que todas las redes utilicen esta conexión. El valor predeterminado es **Desactivado**.
- **Excluir redes locales:** Seleccione si prohibir que las redes locales usen la conexión. El valor predeterminado es **Desactivado**.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**. Si activa esta opción, defina las siguientes configuraciones:
 - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. El valor predeterminado es **Desactivado**.
 - **Tipo de proveedor:** Seleccione si la VPN por aplicación se ofrece como **proxy de aplicación** o como **túnel de paquete**. El valor predeterminado es **Proxy de aplicación**.
 - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - * **Dominio:** Escriba el dominio que se va a agregar.
 - * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo Juniper SSL para iOS

- **Identificador de paquetes de proveedor:** Si el perfil de su VPN por aplicación contiene el identificador de paquetes de una aplicación con varios proveedores de VPN del mismo tipo, especifique el proveedor que quiere utilizar aquí.

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Territorio:** Escriba un nombre opcional para el territorio Kerberos.
- **Rol:** Escriba un nombre opcional para el rol.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
 - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
 - Si habilita **Certificado**, defina las siguientes configuraciones:
 - * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
 - * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
 - * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**. Si activa esta opción, defina las siguientes configuraciones:
 - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. El valor predeterminado es **Desactivado**.
 - **Tipo de proveedor:** Seleccione si la VPN por aplicación se ofrece como **proxy de aplicación** o como **túnel de paquete**. El valor predeterminado es **Proxy de aplicación**.
 - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - * **Dominio:** Escriba el dominio que se va a agregar.
 - * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo F5 SSL para iOS

- **Identificador de paquetes de proveedor:** Si el perfil de su VPN por aplicación contiene el identificador de paquetes de una aplicación con varios proveedores de VPN del mismo tipo, especifique el proveedor que quiere utilizar aquí.
- **Nombre o dirección IP del servidor:** Escriba el nombre 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 elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
 - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
 - Si habilita **Certificado**, defina las siguientes configuraciones:
 - * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
 - * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
 - * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**. Si activa esta opción, defina las siguientes configuraciones:
 - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red.
 - **Tipo de proveedor:** Seleccione si la VPN por aplicación se ofrece como **proxy de aplicación** o como **túnel de paquete**. El valor predeterminado es **Proxy de aplicación**.
 - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - * **Dominio:** Escriba el dominio que se va a agregar.
 - * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo SonicWALL para iOS

- **Identificador de paquetes de proveedor:** Si el perfil de su VPN por aplicación contiene el identificador de paquetes de una aplicación con varios proveedores de VPN del mismo tipo, especifique el proveedor que quiere utilizar aquí.
- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Dominio o grupo de inicio de sesión:** Escriba un dominio o grupo opcional de inicio de sesión.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.

- Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
- Si habilita **Certificado**, defina las siguientes configuraciones:
 - * **Credencial de identidad**: En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
 - * **Pedir PIN al conectar**: Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
 - * **Habilitar VPN a demanda**: Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación**: Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**. Si activa esta opción, configure los siguientes parámetros:
 - **Correspondencia de aplicación a demanda habilitada**: Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red.
 - **Tipo de proveedor**: Seleccione si la VPN por aplicación se ofrece como **proxy de aplicación** o como **túnel de paquete**. El valor predeterminado es **Proxy de aplicación**.
 - **Dominios de Safari**: Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - * **Dominio**: Escriba el dominio que se va a agregar.
 - * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo Ariba VIA para iOS

- **Identificador de paquetes de proveedor**: Si el perfil de su VPN por aplicación contiene el identificador de paquetes de una aplicación con varios proveedores de VPN del mismo tipo, especifique el proveedor que quiere utilizar aquí.
- **Nombre o dirección IP del servidor**: Escriba el nombre 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 elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
 - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
 - Si habilita **Certificado**, defina las siguientes configuraciones:

- ★ **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
- ★ **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
- ★ **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**. Si activa esta opción, defina las siguientes configuraciones:
 - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red.
 - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - ★ **Dominio:** Escriba el dominio que se va a agregar.
 - ★ Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar protocolos IKEv2 para iOS

Esta sección incluye parámetros utilizados para los protocolos IKEv2, Always On IKEv2 y de configuración dual de Always On IKEv2. Para el protocolo de configuración dual de Always On IKEv2, configure todos estos parámetros tanto para redes móviles como para redes Wi-Fi.

- **Permitir que el usuario inhabilite la conexión automática:** Para protocolos Always On. Seleccione si permitir a los usuarios inhabilitar 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 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 del dispositivo:** Seleccione **Secreto compartido**, **Certificado** o **Certificado de dispositivo basado en la identidad del dispositivo** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Secreto compartido**.
 - Si elige **Secreto compartido**, escriba una clave opcional de secreto compartido.

- Si elige **Certificado**, elija la **Credencial de identidad** que quiere utilizar. El valor predeterminado es **Ninguno**.
- Si elige **Certificado de dispositivo basado en la identidad del dispositivo**, seleccione el **Tipo de identidad del dispositivo** que quiere utilizar. El valor predeterminado es **IMEI**. Para utilizar esta opción, importe certificados en bloque con la API de REST. Consulte [Cargar certificados en bloque con la API de REST](#). Solo está disponible si selecciona **Always On IKEv2**.
- **Autenticación extendida habilitada:** Seleccione si habilitar el Protocolo de autenticación extensible (EAP). Si lo **activa**, escriba la **Cuenta de usuario** y la **Contraseña de autenticación**.
- **Intervalo DPD (Dead Peer Detection):** Seleccione la frecuencia con que un nodo establece contacto con otro del mismo nivel con el fin de garantizar que este permanece contactable. El valor predeterminado es **Ninguno**. Las opciones son:
 - **Ninguno:** Inhabilita la opción Dead Peer Detection (detección de actividad en un nodo del mismo nivel).
 - **Bajo:** Establece contacto con un nodo del mismo nivel cada 30 minutos.
 - **Medio:** Establece contacto con un nodo del mismo nivel cada 10 minutos.
 - **Alto:** Establece contacto con un nodo del mismo nivel cada minuto.
- **Inhabilitar movilidad y multihoming:** Seleccione si inhabilitar esta función.
- **Utilizar atributos de subred interna IPv4/IPv6:** Seleccione si habilitar esta función.
- **Inhabilitar redirecciones:** Seleccione si inhabilitar las redirecciones.
- **Habilitar opción de reserva:** Si está habilitado, esta configuración permite que un túnel de datos móviles lleve tráfico apto para Wi-Fi Assist y requiera una VPN. El valor predeterminado es **Desactivado**.
- **Habilitar NAT Keep-Alive mientras el dispositivo está en modo de suspensión:** Para los protocolos Always On. Los paquetes Keep-Alive mantienen las asignaciones NAT para las conexiones IKEv2. El chip envía esos paquetes regularmente cuando el dispositivo está activado. Si este parámetro está activado, el chip envía paquetes Keep-Alive incluso aunque el dispositivo esté en modo de suspensión. El intervalo predeterminado es de 20 segundos por Wi-Fi y 110 segundos por red móvil. Puede cambiar el intervalo con el parámetro Intervalo de NAT Keep-Alive.
- **Intervalo de NAT Keep-Alive (segundos):** El valor predeterminado es de 20 segundos.
- **Habilitar PFS (Perfect Forward Secrecy):** Seleccione si habilitar esta función.

- **Direcciones IP de servidores DNS.** Opcional. Una lista de cadenas de direcciones IP pertenecientes a servidores 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 dominios que se utiliza para calificar totalmente los nombres de host de etiqueta única.
- **Agregar dominios complementarios a la lista de resolución:** Opcional. Determina si agregar la lista de dominios suplementarios de correspondencia a la lista de dominios de búsqueda para la resolución. De forma predeterminada, está **activado**.
- **Dominios suplementarios de correspondencia.** Opcional. Una lista de los dominios que se utilizan para determinar qué consultas DNS van a usar los parámetros de resolución DNS que contienen las direcciones de servidor DNS. Esta clave crea una configuración de DNS dividido donde solo los hosts de dominios determinados van a resolverse mediante la resolución DNS del túnel. Los hosts que no consten en uno de los dominios de esta lista se resuelven con la resolución predeterminada del sistema.

Si este parámetro contiene una cadena vacía, esa cadena se utilizará como el dominio predeterminado. Así, una configuración de túnel dividido puede dirigir todas las consultas DNS a los servidores DNS de las redes VPN antes de dirigir las a los servidores DNS principales. Si el túnel VPN es la ruta predeterminada de la red, los servidores DNS de la lista pasan a ser la resolución predeterminada. En ese caso, se ignora la lista de los dominios complementarios de correspondencia.

- **Parámetros de IKE SA y Parámetros de Child SA:** Configure estos parámetros para cada opción de asociación de seguridad (SA):
 - **Algoritmo de cifrado:** En la lista, seleccione el algoritmo de cifrado IKE que se va a usar. El valor predeterminado es **3DES**.
 - **Algoritmo de integridad:** En la lista, seleccione el algoritmo de integridad que se va a usar. El valor predeterminado es **SHA-256**.
 - **Grupo Diffie-Hellman:** En la lista, seleccione el número de grupo de Diffie Hellman. El valor predeterminado es **2**.
 - **Tiempo de vida de IKE (en minutos):** Escriba un número entero comprendido entre 10 y 1440 que represente la vigencia de la asociación de seguridad (intervalo de regeneración de claves). El valor predeterminado es **1440** minutos.
- **Excepciones de servicios:** Para los protocolos Always On. Las excepciones de servicios son aquellos servicios del sistema que se eximen de la VPN de Always On. Configure estos parámetros de excepciones de servicios:

- **Correo de voz:** En la lista, seleccione cómo gestionar la excepción del correo de voz. El valor predeterminado es **Permitir tráfico a través de túnel**.
- **AirPrint:** En la lista, seleccione cómo gestionar la excepción de AirPrint. El valor predeterminado es **Permitir tráfico a través de túnel**.
- **Permitir tráfico desde hojas Web cautivas fuera del túnel VPN.** Seleccione si permitir que los usuarios se conecten a puntos de acceso a Internet (hotspots) públicos que se encuentren fuera del túnel VPN. El valor predeterminado es **Desactivado**.
- **Permitir tráfico desde todas las aplicaciones de redes cautivas fuera del túnel VPN:** Seleccione si permitir todas las aplicaciones provenientes de hotspots que se encuentren fuera del túnel VPN. El valor predeterminado es **Desactivado**.
- **Identificadores de paquetes de aplicaciones de redes cautivas:** Para cada ID de paquete de aplicación de red de hotspot al que los usuarios tengan autorizado el acceso, haga clic en **Agregar** y escriba el **Identificador de paquete** de aplicación relativo a la red del hotspot. Haga clic en **Guardar** para guardar el identificador del paquete de aplicación.
- **VPN por aplicación:** Configure estas opciones para los tipos de conexión IKEv2.
 - **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**.
 - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. El valor predeterminado es **Desactivado**.
 - **Dominios de Safari:** Haga clic en **Agregar** para agregar un nombre de dominio de Safari.
- **Configuración de proxy.** Seleccione cómo se enruta la conexión VPN a través de un servidor proxy. El valor predeterminado es **Ninguno**.

Configurar el protocolo Citrix SSO para iOS

El cliente de Citrix SSO está disponible en el Apple Store.

- **Nombre o dirección IP del servidor:** Escriba el nombre 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 elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
 - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
 - Si habilita **Certificado**, defina las siguientes configuraciones:

- ★ **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
- ★ **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
- ★ **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**. Si activa esta opción, configure los siguientes parámetros:
 - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red.
 - **Tipo de proveedor:** Seleccione si la VPN por aplicación se ofrece como **proxy de aplicación** o como **túnel de paquete**. El valor predeterminado es **Proxy de aplicación**.
 - **Tipo de proveedor:** Establezca la configuración en **Túnel de paquete**.
 - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - ★ **Dominio:** Escriba el dominio que se va a agregar.
 - ★ Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **XML personalizado:** Haga clic en **Agregar** y especifique los pares clave/valor para agregar cada parámetro XML personalizado. Los parámetros disponibles son:
 - **disableL3:** Inhabilita conexiones VPN a nivel del sistema. Permite únicamente conexiones VPN por aplicación. No se necesita ningún **Valor**.
 - **user agent:** Asocia, a esta directiva, las directivas de NetScaler Gateway dirigidas a clientes con plug-in VPN. El **Valor** de esta clave se agrega automáticamente al plug-in VPN para las solicitudes iniciadas por el plug-in.

Configurar el protocolo SSL personalizado para iOS

Para realizar la transición del cliente Cisco Legacy AnyConnect al nuevo cliente Cisco AnyConnect:

1. Configure la directiva de VPN con el protocolo SSL personalizado. Implemente esa directiva en los dispositivos iOS.
2. Cargue el cliente Cisco AnyConnect desde <https://apps.apple.com/us/app/cisco-secure-client/id1135064690>, agregue la aplicación a Citrix Endpoint Management y, a continuación,

implementela en los dispositivos iOS.

3. Quite la directiva de VPN antigua que hubiera en los dispositivos iOS.

Parámetros:

- **Identificador de SSL personalizado (formato DNS inverso).** Establézcalo en el ID del paquete. Para el cliente Cisco AnyConnect, use **com.cisco.anyconnect**.
- **Identificador de paquete de proveedor.** Si la aplicación especificada en **Identificador de 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 o dirección IP del servidor:** Escriba el nombre 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 elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
 - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
 - Si habilita **Certificado**, defina las siguientes configuraciones:
 - * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
 - * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
 - * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda para iOS.
- **Incluir todas las redes:** Seleccione si permitir que todas las redes utilicen esta conexión. El valor predeterminado es **Desactivado**.
- **Excluir redes locales:** Seleccione si prohibir que las redes locales usen la conexión. El valor predeterminado es **Desactivado**.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**. Si activa esta opción, configure los siguientes parámetros:
 - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red.
 - **Tipo de proveedor.** El tipo de proveedor indica si este es un servicio proxy o un servicio VPN. Para el servicio VPN, elija **Túnel de paquete**. Para el servicio proxy, elija **Proxy de aplicación**. Para el cliente Cisco AnyConnect, elija **Túnel de paquete**.

- **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - * **Dominio:** Escriba el dominio que se va a agregar.
 - * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **XML personalizado:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada parámetro XML personalizado:
 - **Nombre del parámetro:** Escriba el nombre del parámetro que se va a agregar.
 - **Valor:** Escriba el valor asociado al **Nombre del parámetro**.
 - Haga clic en **Guardar** para guardar el parámetro, o bien haga clic en **Cancelar** para no guardarlo.

Configurar la directiva de VPN para admitir NAC

1. Se requiere el **Tipo de conexión** de **SSL personalizado** para configurar el filtro NAC.
2. Especifique **VPN** como **Nombre de conexión**.
3. En **Identificador de SSL personalizado**, escriba **com.citrix.NetScalerGateway.ios.app**
4. En **Identificador de paquete de proveedor**, escriba **com.citrix.NetScalerGateway.ios.app.vpnplugin**

Los valores de los pasos 3 y 4 se toman de la instalación requerida de Citrix SSO para el filtrado de NAC. No se configura una contraseña de autenticación. Para obtener más información sobre el uso de la función NAC, consulte [Control de acceso a red](#).

Configurar opciones de Habilitar VPN a demanda para iOS

- **Dominio a demanda:** Por cada dominio y acción asociada que deben realizarse cuando los usuarios se conecten, pinche en **Agregar** y haga lo siguiente:
 - **Dominio:** Escriba el dominio que se va a agregar.
 - **Acción:** En la lista, seleccione en una de las posibles acciones:
 - **Establecer siempre:** El dominio siempre activa una conexión VPN.
 - **No establecer nunca:** El dominio no activa nunca una conexión VPN.
 - **Establecer si es necesario:** El dominio activa un intento de conexión VPN si falla la resolución de nombres de dominio. El error 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 bien haga clic en **Cancelar** para no guardarlo.
- **Reglas a demanda**

- **Acción:** En la lista, seleccione la acción que se debe realizar. El valor predeterminado es **EvaluateConnection**. Las acciones posibles son:
 - ★ **Permitir:** Al activarse, permite que la VPN a demanda se conecte.
 - ★ **Conectar:** Inicia incondicionalmente una conexión VPN.
 - ★ **Desconectar:** Quita la conexión VPN y no vuelve a conectarse a demanda mientras la regla se cumpla.
 - ★ **EvaluateConnection:** Evalúa la matriz ActionParameters para cada conexión.
 - ★ **Ignorar:** Deja activa cualquier conexión VPN existente, pero no vuelve a conectarse a demanda mientras la regla se cumpla.
- **DNSDomainMatch:** Para agregar cada dominio que se va a cotejar con la lista de búsqueda de dominios de un dispositivo, haga clic en **Agregar** y lleve a cabo lo siguiente:
 - ★ **Dominio DNS:** Escriba el nombre del dominio. Puede usar el prefijo comodín “*” para abarcar varios dominios. Por ejemplo: *.ejemplo.com abarca midominio.ejemplo.com, tudominio.ejemplo.com y sudominio.ejemplo.com.
 - ★ Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **DNSServerAddressMatch:** Para agregar cada dirección IP con la que puede coincidir cualquier servidor DNS indicado en la red, haga clic en **Agregar** y lleve a cabo lo siguiente:
 - ★ **Dirección del servidor DNS:** Escriba la dirección del servidor DNS que quiere agregar. Puede usar el sufijo comodín “*” para abarcar varios servidores DNS. Por ejemplo: 17.* abarca cualquier servidor DNS incluido en la subred de clase A.
 - ★ Haga clic en **Guardar** para guardar el servidor DNS, o bien haga clic en **Cancelar** para no guardarlo.
- **InterfaceTypeMatch:** En la lista, seleccione el tipo de hardware de interfaz de red principal que se está utilizando. El valor predeterminado es **No especificado**. Los valores posibles son:
 - ★ **No especificado:** Coincide con cualquier hardware de interfaz de red. Esta es la opción predeterminada.
 - ★ **Ethernet:** Solo coincide con el hardware de interfaz de red Ethernet.
 - ★ **Wi-Fi:** Solo coincide con el hardware de interfaz de red Wi-Fi.
 - ★ **Móvil:** Solo coincide con el hardware de interfaz de red móvil.
- **SSIDMatch:** Haga clic en **Agregar** y haga lo siguiente para agregar cada SSID que se va a cotejar con la red actual.
 - ★ **SSID:** Escriba el SSID que se va a agregar. Si no se trata de una red Wi-Fi, o bien si el SSID no aparece, el cotejo falla. Deje esta lista vacía para que abarque cualquier SSID.
 - ★ Haga clic en **Guardar** para guardar el SSID, o bien haga clic en **Cancelar** para descartarlo.
- **URLStringProbe:** Escriba una URL a capturar. Si la URL se captura correctamente sin redirección, se cumple esta regla.

- **ActionParameters: Domains:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada dominio que va a comprobar EvaluateConnection:
 - * **Dominio:** Escriba el dominio que se va a agregar.
 - * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **ActionParameters: DomainAction:** En la lista, seleccione el **comportamiento de la red VPN** correspondiente para los dominios especificados en **ActionParameters: Domains**. El valor predeterminado es **ConnectIfNeeded**. Las acciones posibles son:
 - * **ConnectIfNeeded:** El dominio activa un intento de conexión VPN si falla la resolución de nombres de dominio. El error ocurre cuando el servidor DNS no puede resolver el dominio, redirige a un servidor diferente o agota el tiempo de espera.
 - * **NeverConnect:** El dominio no activa nunca una conexión VPN.
- **Action Parameters: RequiredDNSServers:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada servidor DNS que se use para resolver los dominios especificados:
 - * **Servidor DNS:** Solo válido si **ActionParameters : DomainAction** es **ConnectIfNeeded**. Escriba la dirección IP del servidor DNS. Este servidor puede residir fuera de la configuración de red actual del dispositivo. Si el servidor DNS no es accesible, se establece una conexión VPN. Este servidor DNS debe ser un servidor DNS interno o un servidor DNS externo de confianza.
 - * Haga clic en **Save** para guardar el servidor DNS, o bien haga clic en **Cancel** para no guardarlo.
- **ActionParameters : RequiredURLStringProbe:** Si quiere, escriba una URL en formato HTTP o HTTPS (preferentemente este) para llevar a cabo un sondeo con la ayuda de una solicitud GET. Si el nombre de host de la URL no se puede resolver, o si el servidor es inaccesible o el servidor no responde, se establece una conexión VPN. Válido solamente si **ActionParameters: DomainAction = ConnectIfNeeded**.
- **OnDemandRules : XML content.** Escriba o copie y pegue las reglas a demanda de la configuración XML.
 - * Haga clic en **Diccionario de comprobación** para validar la sintaxis del 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 de proxy:** En la lista, seleccione cómo se redirige la conexión VPN a través de un servidor proxy. El valor predeterminado es **Ninguno**.
 - * Si habilita **Manual**, configure los siguientes 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 el servidor proxy.
- **Contraseña:** Escriba una contraseña opcional de servidor proxy.
- * Si selecciona **Automático**, configure este parámetro:
 - **URL del servidor proxy:** Escriba la URL del servidor proxy. Este campo es obligatorio.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo 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 SSL personalizado.

Para configurar una VPN por aplicación:

1. En **Configurar > Directivas de dispositivo**, cree una directiva de red VPN. Por ejemplo:

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

VPN Policy

1 Policy Info

2 Platforms

☒ iOS

☐ macOS

☐ Android

☐ Samsung SAFE

☐ Samsung KNOX

☐ Windows Phone

☐ Windows Desktop/Tablet

☐ Amazon

3 Assignment

VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name

XenMobile

?

Connection type

Custom SSL

?

Custom SSL identifier (reverse DNS format) *

com.example.custom.identifier

?

Provider bundle identifier

com.example.bundle.identifier

?

Server name or IP address *

app-domain.example.com

?

User account

administrator

?

Authentication type for the connection

Password

?

Auth Password

?

Per-app VPN

Enable per-app VPN

ON

IOS 7.0+

On-demand match app enabled

ON

?

Provider type

App proxy

?

Safari domains

?

Back

Next >

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

VPN Policy

1 Policy Info

2 Platforms

☒ iOS

☐ macOS

☐ Android

☐ Samsung SAFE

☐ Samsung KNOX

☐ Windows Phone

☐ Windows Desktop/Tablet

☐ Amazon

3 Assignment

Enable per-app VPN

ON

IOS 7.0+

On-demand match app enabled

ON

?

Provider type

App proxy

?

Safari domains

?

Domain *

Add

Custom XML

Custom parameters

Parameter name *

Value

Add

Proxy

Proxy configuration

None

?

Policy Settings

Remove policy

Select date

Duration until removal (in hours)

Allow user to remove policy

Always

?

Deployment Rules

Back

Next >

2. En **Configurar > Directivas de dispositivo**, cree una directiva de atributos de aplicaciones para asociar una aplicación a la directiva de VPN por aplicación. Para **Identificador de VPN por aplicación**, elija el nombre de la directiva de VPN creada en el paso 1. Para **ID de paquete de la aplicación administrada**, elija un ID de la lista de aplicaciones o introduzca el ID de paquete de aplicación (si implementa una directiva Inventario de aplicaciones en iOS, la lista contendrá aplicaciones).

Parámetros de macOS

- **Nombre de la conexión:** Escriba un nombre para la conexión.
- **Tipo de conexión:** En la lista, seleccione el protocolo que se va a usar para esta conexión. El valor predeterminado es L2TP.
 - **L2TP:** Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida.
 - **PPTP:** Túnel punto a punto.
 - **IPsec:** La conexión VPN de su empresa.
 - **Cisco AnyConnect:** Cliente VPN de Cisco AnyConnect.
 - **Juniper SSL:** Cliente SSL VPN de Juniper Networks.
 - **F5 SSL:** Cliente SSL VPN de F5 Networks.
 - **SonicWALL Mobile Connect:** Cliente VPN unificado de Dell para iOS.
 - **Ariba VIA:** Cliente de acceso virtual a Internet de Ariba Networks.
 - **Citrix VPN:** Cliente VPN de Citrix.
 - **SSL personalizado:** Secure Sockets Layer (SSL) personalizada.

En las siguientes secciones se ofrecen las opciones de configuración para cada uno de los tipos de conexión mencionados.

Configurar el protocolo L2TP para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- Seleccione **Autenticación por contraseña**, **Autenticación con RSA SecureID**, **Autenticación Kerberos** o **Autenticación CryptoCard**. El valor predeterminado es **Autenticación por contraseña**.
- **Secreto compartido:** Escriba la clave de secreto compartido de IPsec.
- **Enviar todo el tráfico:** Seleccione si enviar todo el tráfico por la red privada virtual (VPN). El valor predeterminado es **Desactivado**.

Configurar el protocolo PPTP para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- Seleccione **Autenticación por contraseña**, **Autenticación con RSA SecureID**, **Autenticación Kerberos** o **Autenticación CryptoCard**. El valor predeterminado es **Autenticación por contraseña**.
- **Nivel de cifrado.** Seleccione el nivel de cifrado pertinente. El valor predeterminado es **Ninguno**.
 - **Ninguno:** No se usa ningún cifrado.
 - **Automático:** Se usa el nivel más alto de cifrado que admite el servidor.
 - **Máximo (128 bits):** Se usa siempre el cifrado de 128 bits.
- **Enviar todo el tráfico:** Seleccione si enviar todo el tráfico por la red privada virtual (VPN). El valor predeterminado es **Desactivado**.

Configurar el protocolo IPsec para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre 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 elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Secreto compartido**.
 - Si habilita la autenticación **Secreto compartido**, configure los siguientes parámetros:

- * **Nombre del grupo:** Escriba un nombre de grupo opcional.
- * **Secreto compartido:** Escriba una clave opcional de secreto compartido.
- * **Usar autenticación híbrida:** Seleccione si utilizar la autenticación híbrida. Con la autenticación híbrida, el servidor se autentica primero en el cliente, y, a continuación, se autentica en el servidor. El valor predeterminado es **Desactivado**.
- * **Pedir contraseña:** Seleccione si solicitar a los usuarios sus contraseñas cuando se conectan a la red. El valor predeterminado es **Desactivado**.
- Si habilita la autenticación **Certificado**, configure los siguientes parámetros:
 - * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
 - * **Pedir PIN al conectar:** Seleccione esta opción para obligar a los usuarios a introducir su PIN cuando se conecten a la red. El valor predeterminado es **Desactivado**.
 - * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.

Configurar el protocolo Cisco AnyConnect para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre 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 elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
 - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
 - Si habilita **Certificado**, defina las siguientes configuraciones:
 - * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
 - * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
 - * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.
 - **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El

valor predeterminado es **Desactivado**. Si activa esta opción, defina las siguientes configuraciones:

- ★ **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. El valor predeterminado es **Desactivado**.
- ★ **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - **Dominio:** Escriba el dominio que se va a agregar.
 - Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo Juniper SSL para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Territorio:** Escriba un nombre opcional para el territorio Kerberos.
- **Rol:** Escriba un nombre opcional para el rol.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
 - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
 - Si habilita **Certificado**, defina las siguientes configuraciones:
 - ★ **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
 - ★ **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
 - ★ **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**. Si activa esta opción, configure los siguientes parámetros:
 - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. El valor predeterminado es **Desactivado**.

- **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - * **Dominio:** Escriba el dominio que se va a agregar.
 - * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo F5 SSL para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre 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 elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
 - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
 - Si habilita **Certificado**, defina las siguientes configuraciones:
 - * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
 - * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
 - * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**. Si activa esta opción, defina las siguientes configuraciones:
 - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. El valor predeterminado es **Desactivado**.
 - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - * **Dominio:** Escriba el dominio que se va a agregar.
 - * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo SonicWALL Mobile Connect para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre o la dirección IP del servidor VPN.
- **Cuenta de usuario:** Escriba una cuenta de usuario opcional.
- **Dominio o grupo de inicio de sesión:** Escriba un dominio o grupo opcional de inicio de sesión.
- **Tipo de autenticación para la conexión:** En la lista, seleccione **Contraseña** o **Certificado** para elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
 - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
 - Si habilita **Certificado**, defina las siguientes configuraciones:
 - * **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
 - * **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
 - * **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**. Si activa esta opción, defina las siguientes configuraciones:
 - **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. El valor predeterminado es **Desactivado**.
 - **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - * **Dominio:** Escriba el dominio que se va a agregar.
 - * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo Ariba VIA para macOS

- **Nombre o dirección IP del servidor:** Escriba el nombre 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 elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.

- Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
- Si habilita **Certificado**, defina las siguientes configuraciones:
 - * **Credencial de identidad**: En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
 - * **Pedir PIN al conectar**: Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
 - * **Habilitar VPN a demanda**: Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.
- **Habilitar VPN por aplicación**: Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**. Si activa esta opción, defina las siguientes configuraciones:
 - **Correspondencia de aplicación a demanda habilitada**: Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red. El valor predeterminado es **Desactivado**.
 - **Dominios de Safari**: Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - * **Dominio**: Escriba el dominio que se va a agregar.
 - * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar el protocolo SSL personalizado para macOS

- **Identificador de SSL personalizado (formato DNS inverso)**. Escriba el identificador de SSL en formato DNS inverso. Este campo es obligatorio.
- **Nombre o dirección IP del servidor**: Escriba el nombre 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 elegir el tipo de autenticación de esta conexión. El valor predeterminado es **Contraseña**.
 - Si habilita **Contraseña**, escriba una contraseña opcional de autenticación en el campo **Contraseña de autenticación**.
 - Si habilita **Certificado**, defina las siguientes configuraciones:

- ★ **Credencial de identidad:** En la lista, seleccione la credencial de identidad que se va a usar. El valor predeterminado es **Ninguno**.
- ★ **Pedir PIN al conectar:** Seleccione si solicitar a los usuarios sus PIN cuando se conectan a la red. El valor predeterminado es **Desactivado**.
- ★ **Habilitar VPN a demanda:** Seleccione si permitir la activación de una conexión VPN cuando los usuarios se conectan a la red. El valor predeterminado es **Desactivado**. Para obtener información acerca de la configuración de parámetros cuando la opción **Habilitar VPN a demanda** está **activada**, consulte Configurar opciones de Habilitar VPN a demanda.
- **VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. El valor predeterminado es **Desactivado**. Si activa esta opción, defina las siguientes configuraciones:
 - ★ **Correspondencia de aplicación a demanda habilitada:** Seleccione si activar automáticamente conexiones de red VPN por aplicación cuando las aplicaciones asociadas al servicio VPN por aplicación inician una comunicación de red.
 - ★ **Dominios de Safari:** Haga clic en **Agregar** y lleve a cabo lo siguiente para incluir cada dominio de Safari que puede activar una conexión VPN por aplicación:
 - **Dominio:** Escriba el dominio que se va a agregar.
 - Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **XML personalizado:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada parámetro XML personalizado:
 - **Nombre del parámetro:** Escriba el nombre del parámetro que se va a agregar.
 - **Valor:** Escriba el valor asociado al **Nombre del parámetro**.
 - Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

Configurar opciones de Habilitar VPN a demanda

- **Dominio a demanda:** Para agregar un dominio y la acción asociada que se realizará cuando los usuarios se conecten a él, haga clic en **Agregar** y lleve a cabo lo siguiente:
 - **Dominio:** Escriba el dominio que se va a agregar.
 - **Acción:** En la lista, seleccione en una de las posibles acciones:
 - ★ **Establecer siempre:** El dominio siempre activa una conexión VPN.
 - ★ **No establecer nunca:** El dominio no activa nunca una conexión VPN.
 - ★ **Establecer si es necesario:** El dominio activa un intento de conexión VPN si falla la resolución de nombres de dominio. El error 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 bien haga clic en **Cancelar** para no guardarlo.

- **Reglas a demanda**

- **Acción:** En la lista, seleccione la acción que se debe realizar. El valor predeterminado es **EvaluateConnection**. Las acciones posibles son:

- * **Permitir:** Al activarse, permite que la VPN a demanda se conecte.
- * **Conectar:** Inicia incondicionalmente una conexión VPN.
- * **Desconectar:** Quita la conexión VPN y no vuelve a conectarse a demanda mientras la regla se cumpla.
- * **EvaluateConnection:** Evalúa la matriz **ActionParameters** para cada conexión.
- * **Ignorar:** Deja activa cualquier conexión VPN existente, pero no vuelve a conectarse a demanda mientras la regla se cumpla.

- **DNSDomainMatch:** Para los dominios que se pueden cotejar con la lista de dominios de la búsqueda de un dispositivo, haga clic en **Agregar** y lleve a cabo lo siguiente:

- * **Dominio DNS:** Escriba el nombre del dominio. Puede usar el prefijo comodín “*” para abarcar varios dominios. Por ejemplo: *.ejemplo.com abarca midominio.ejemplo.com, tudominio.ejemplo.com y sudominio.ejemplo.com.
- * Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.

- **DNSServerAddressMatch:** Para agregar cada dirección IP con la que puede coincidir cualquier servidor DNS indicado en la red, haga clic en **Agregar** y lleve a cabo lo siguiente:

- * **Dirección del servidor DNS:** Escriba la dirección del servidor DNS que quiere agregar. Puede usar el sufijo comodín “*” para abarcar varios servidores DNS. Por ejemplo: 17.* abarca cualquier servidor DNS incluido en la subred de clase A.
- * Haga clic en **Guardar** para guardar el servidor DNS, o bien haga clic en **Cancelar** para no guardarlo.

- **InterfaceTypeMatch:** En la lista, haga clic en el tipo de hardware de interfaz de red principal que se está utilizando. El valor predeterminado es **No especificado**. Los valores posibles son:

- * **No especificado:** Coincide con cualquier hardware de interfaz de red. Esta es la opción predeterminada.
- * **Ethernet:** Solo coincide con el hardware de interfaz de red Ethernet.
- * **Wi-Fi:** Solo coincide con el hardware de interfaz de red Wi-Fi.
- * **Móvil:** Solo coincide con el hardware de interfaz de red móvil.

- **SSIDMatch:** Haga clic en **Agregar** y haga lo siguiente para agregar cada SSID que se va a cotejar con la red actual.

- * **SSID:** Escriba el SSID que se va a agregar. Si no se trata de una red Wi-Fi, o bien si el SSID no aparece, el cotejo falla. Deje esta lista vacía para que abarque cualquier SSID.

- ★ Haga clic en **Guardar** para guardar el SSID, o bien haga clic en **Cancelar** para descartarlo.
 - **URLStringProbe:** Escriba una URL a capturar. Si la URL se captura correctamente sin redirección, se cumple esta regla.
 - **ActionParameters: Domains:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada dominio que va a comprobar EvaluateConnection:
 - ★ **Dominio:** Escriba el dominio que se va a agregar.
 - ★ Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
 - **ActionParameters: DomainAction:** En la lista, seleccione el **comportamiento de la red VPN** correspondiente para los dominios especificados en **ActionParameters: Domains**. El valor predeterminado es **ConnectIfNeeded**. Las acciones posibles son:
 - ★ **ConnectIfNeeded:** El dominio activa un intento de conexión VPN si falla la resolución de nombres de dominio. El error ocurre cuando el servidor DNS no puede resolver el dominio, dirige a un servidor diferente o agota el tiempo de espera.
 - ★ **NeverConnect:** El dominio no activa nunca una conexión VPN.
 - **Action Parameters: RequiredDNSServers:** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada servidor DNS que se use para resolver los dominios especificados:
 - ★ **Servidor DNS:** Solo válido si **ActionParameters : DomainAction** es **ConnectIfNeeded**. Escriba la dirección IP del servidor DNS que agregar. Este servidor puede residir fuera de la configuración de red actual del dispositivo. Si el servidor DNS no es accesible, se establece una conexión VPN. Este debe ser un servidor DNS interno o un servidor DNS externo de confianza.
 - ★ Haga clic en **Save** para guardar el servidor DNS, o bien haga clic en **Cancel** para no guardarlo.
 - **ActionParameters : RequiredURLStringProbe:** Si quiere, escriba una URL en formato HTTP o HTTPS (preferentemente este) para llevar a cabo un sondeo con la ayuda de una solicitud GET. Si el nombre de host de la URL no se puede resolver, o si el servidor es inaccesible o el servidor no responde, se establece una conexión VPN. Válido solamente si **ActionParameters: DomainAction = ConnectIfNeeded**.
 - **OnDemandRules : XML content:** Escriba o copie y pegue las reglas a demanda de la configuración XML.
 - ★ Haga clic en **Diccionario de comprobación** para validar la sintaxis del 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 de proxy:** En la lista, seleccione cómo se redirige la conexión VPN a través de un servidor proxy. El valor predeterminado es **Ninguno**.

- ★ Si habilita **Manual**, configure los siguientes 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 el servidor proxy.
 - **Contraseña:** Escriba una contraseña opcional de servidor proxy.
- ★ Si selecciona **Automático**, configure este parámetro:
 - **URL del servidor proxy:** Escriba la URL del servidor proxy. Este campo es obligatorio.

- **Configuraciones de directivas**

- **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - ★ **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - ★ **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar 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**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.
- **Ámbito del perfil:** Seleccione si esta directiva se aplica a un **usuario** o a todo el **sistema**. El valor predeterminado es **Usuario**. Esta opción solo está disponible para macOS 10.7 y versiones posteriores.

Parámetros de Android (AD heredado)

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
VPN Policy ✕ This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.						
1 Policy Info						
2 Platforms						
<input type="checkbox"/> iOS						
<input type="checkbox"/> macOS						
<input checked="" type="checkbox"/> Android						
<input checked="" type="checkbox"/> Samsung SAFE						
<input checked="" type="checkbox"/> Samsung KNOX						
<input type="checkbox"/> Windows Phone						
<input type="checkbox"/> Windows Desktop/Tablet						
<input type="checkbox"/> Amazon						
3 Assignment						
VPN Policy						
Connection name * <input type="text"/> ⓘ						
Server name or IP address * <input type="text"/> ⓘ						
Connection type Cisco AnyConnect ▼						
Identity credential None ▼ ⓘ						
Backup VPN server <input type="text"/> ⓘ						
User group <input type="text"/> ⓘ						
Automatic VPN policy OFF ⓘ						
Deployment Rules						

Configurar el protocolo VPN de Cisco AnyConnect para Android

- **Nombre de la conexión.** Escriba un nombre para la conexión VPN de Cisco AnyConnect. Este campo es obligatorio.
- **Nombre o dirección IP del servidor.** 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 reserva:** Escriba la información del servidor VPN de reserva.
- **Grupo de usuarios.** Escriba la información del grupo de usuarios.
- **Redes de confianza**
 - **Directiva de VPN automática.** Habilite o inhabilite esta opción para establecer cómo reaccionará la red privada virtual ante redes con las que se haya establecido una relación de confianza o de no confianza. Si habilita esta opción, configure los siguientes parámetros:
 - * **Directiva de redes de confianza.** En la lista, seleccione la directiva pertinente. El valor predeterminado es **Desconectar**. Las opciones posibles son:
 - **Desconectar.** El cliente termina la conexión VPN en la red de confianza. Este es el valor predeterminado.
 - **Conectar.** El cliente inicia una conexión VPN en la red de confianza.
 - **No hacer nada:** El cliente no lleva a cabo ninguna acción.
 - **Pausa:** 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 abandona esa red de confianza, la sesión se reanuda. Este parámetro elimina la necesidad de establecer una nueva sesión VPN después de abandonar una red de confianza.

- **Directiva de redes no seguras:** En la lista, seleccione la directiva pertinente. El valor predeterminado es **Conectar**. Las opciones posibles son:
 - **Conectar.** El cliente inicia una conexión VPN en una red que no es de confianza.
 - **No hacer nada:** El cliente no lleva a cabo ninguna acción. Esta opción inhabilita la opción “VPN permanente”.
- **Dominios de confianza.** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada sufijo de dominio que tenga la interfaz de red cuando el cliente se encuentra en la red de confianza:
 - **Dominio:** Escriba el dominio que se va a agregar.
 - Haga clic en **Guardar** para guardar el dominio, o bien haga clic en **Cancelar** para no guardarlo.
- **Servidores de confianza.** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada dirección de servidor que tenga la interfaz de red cuando el cliente se encuentra en la red de confianza:
 - **Servidores.** Escriba el servidor que se va a agregar.
 - Haga clic en **Guardar** para guardar el servidor, o bien haga clic en **Cancelar** para descartarlo.

Configurar el protocolo Citrix SSO para Android

- **Nombre de la conexión.** Escriba un nombre para la conexión VPN. Este campo es obligatorio.
- **Nombre o dirección IP del servidor.** 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 aparecen para el tipo de conexión:
 - **Nombre de usuario y Contraseña.** Escriba las credenciales de la red VPN para los **tipos de autenticación** que sean **Contraseña** o **Contraseña y certificado**. Opcional. Si no proporciona las credenciales de VPN, la aplicación Citrix VPN solicitará un nombre de usuario y una contraseña.
 - **Credencial de identidad:** Aparece cuando los valores de los **Tipos de autenticación** son **Contraseña** o **Contraseña y certificado**. En la lista, seleccione una credencial de identidad.
- **Habilitar VPN por aplicación:** Seleccione si habilitar redes VPN para cada aplicación. Si no habilita VPN por aplicación, todo el tráfico pasará por el túnel VPN de Citrix. Si habilita VPN por aplicación, especifique los siguientes parámetros. El valor predeterminado es **Desactivado**.
 - **Lista de permitidos o Lista de bloqueados:** Con **Lista de permitidos**, todas las aplicaciones que contenga la lista de permitidos pasarán a través del túnel de esta red VPN. Con

Lista de bloqueados, todas las aplicaciones, excepto aquellas de la lista de bloqueados, pasarán a través de esta red VPN.

- **Lista de aplicaciones:** Las aplicaciones de una lista de permitidos o una lista de bloqueados. Haga clic en **Agregar** y, a continuación, escriba una lista separada por comas de nombres de paquetes de aplicación.
- **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** en **Valor**. Si está habilitado, Citrix Endpoint Management no muestra las conexiones VPN que haya agregado el usuario y este no puede agregar conexiones. Este parámetro es una restricción global y se aplica a todos los perfiles de red VPN.
 - **userAgent:** Un valor de cadena. Puede especificar una cadena personalizada de agente de usuario que se enviará en cada solicitud HTTP. La cadena del agente de usuario indicada se agrega al agente de usuario existente de Citrix VPN.

Configurar redes VPN para poder utilizar NAC

1. Utilice el **Tipo de conexión** llamado **SSL personalizado** para configurar el filtro NAC.
2. Especifique **VPN** como **Nombre de conexión**.
3. Para **XML personalizado**, haga clic en **Agregar** y lleve a cabo lo siguiente:
 - **Nombre del parámetro:** Escriba **XenMobileDeviceId**. Este campo es el ID de dispositivo que se utilizará para la comprobación de acceso a red basada en la inscripción de dispositivos en Citrix Endpoint Management. Si Citrix Endpoint Management se inscribe y administra el dispositivo, se permite la conexión VPN. De lo contrario, la autenticación queda denegada al establecer la VPN.
 - **Valor:** Escriba **DeviceID_\${device.id}**, que es el valor del parámetro **XenMobileDeviceId**.
 - Haga clic en **Guardar** para guardar el parámetro.

Configurar redes VPN para Android Enterprise

Para configurar redes VPN para dispositivos Android Enterprise, cree una directiva Configuraciones administradas por Android Enterprise para la aplicación Citrix SSO. Consulte [Configurar perfiles de VPN para Android Enterprise](#).

Parámetros de Android Enterprise

Endpoint Management

Analyze

Manage

Configure

Device Policies

Apps

Media

Actions

Content Collaboration

Enrollment Profiles

Delivery Groups

VPN Policy

1 Policy Info

2 Platforms

3 Assignment

VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection for the intranet. For Windows Phone devices, this policy supports only supervised devices running Windows 10 or later.

Enable always-on VPN

VPN package

Enable lockdown

Applications excluded from lockdown

☐

iOS

☐

macOS

☐

Android (legacy DA)

☒

Android Enterprise

☐

Windows Desktop/Tablet

com.citrix.CitrixVPN

com.citrix.mail.droid

Add

Deployment Rules

- **Habilitar VPN permanente:** Seleccione si la VPN está siempre habilitada. El valor predeterminado es **Desactivado**. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario se desconecta manualmente.
- **Paquete VPN:** Escriba el nombre del paquete para el uso de dispositivos de la aplicación VPN.
- **Habilitar bloqueo:** Si no está habilitada, ninguna aplicación puede acceder a la red si no existe una conexión VPN. Si está habilitada, las aplicaciones que configure en esta configuración pueden acceder a la red aunque no exista ninguna conexión VPN. Disponible para dispositivos Android 10 y versiones posteriores.
- **Aplicaciones excluidas del bloqueo:** Haga clic en **Agregar** para escribir los nombres de los paquetes de las aplicaciones que quiere que omitan la configuración de bloqueo.

Parámetros de escritorios y tabletas Windows

VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

1 Policy Info

2 Platforms

- ☐ iOS
- ☐ macOS
- ☐ Android
- ☐ Samsung SAFE
- ☐ Samsung KNOX
- ☒ Windows Phone
- ☒ Windows Desktop/Tablet
- ☐ Amazon

3 Assignment

VPN Policy Configuration:

- Connection name *
- Profile type: Native
- Server address *
- Remember credential: OFF
- DNS suffix
- Tunnel type *: L2TP
- Authentication method *: EAP
- EAP method *: TLS
- Trusted networks
- Require smart card certificate: OFF
- Automatically select client certificate: OFF
- Always-on VPN: OFF

Back Next >

- **Nombre de la conexión:** Escriba el nombre de la conexión. Este campo es obligatorio.
- **Tipo de perfil:** En la lista, seleccione **Nativo** o **Plug-in**. El valor predeterminado es **Nativo**.
- **Configuración de tipo de perfil nativo.** Estos parámetros se aplican a la red VPN integrada en los dispositivos Windows de los usuarios.
 - **Dirección de servidor:** Escriba el nombre de dominio completo o la dirección IP del servidor VPN. Este campo es obligatorio.
 - **Recordar credencial:** Seleccione si almacenar la credencial en la memoria caché. El valor predeterminado es **Desactivado**. Cuando está habilitada, 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 a usar. El valor predeterminado es **L2TP**. Las opciones posibles son:
 - * **L2TP:** Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida.
 - * **PPTP:** Túnel punto a punto.
 - * **IKEv2:** Versión 2 de Intercambio de claves por red.
 - **Método de autenticación:** En la lista, seleccione el método de autenticación que se va a usar. El valor predeterminado es **EAP**. Las opciones posibles son:
 - * **EAP:** Protocolo de autenticación extensible (EAP).
 - * **MSCHAPv2:** Se usa el protocolo CHAP (protocolo de autenticación por desafío mutuo de Microsoft) para la autenticación mutua. Esta opción no está disponible cuando se

selecciona **IKEv2** como tipo de túnel.

- **Método de EAP:** En la lista, seleccione el método de EAP que se va a usar. El valor predeterminado es **TLS**. Este campo no está disponible si se habilita la autenticación MSCHAPv2. Las opciones posibles son:
 - ★ **TLS:** Transport Layer Security.
 - ★ **PEAP:** Protocolo de autenticación extensible protegido (Protected Extensible Authentication Protocol).
- **Redes de confianza:** Escriba una lista de redes, separadas por comas, que no necesiten una conexión VPN para acceder a ellas. Por ejemplo, cuando los usuarios utilizan la red inalámbrica de la empresa, pueden acceder directamente a recursos protegidos.
- **Requerir certificado de tarjeta inteligente:** Seleccione si se debe requerir un certificado de tarjeta inteligente. El valor predeterminado es **Desactivado**.
- **Seleccionar automáticamente el certificado del cliente:** Seleccione si elegir automáticamente el certificado de cliente para la autenticación. El valor predeterminado es **Desactivado**. Esta opción no está disponible si habilita **Requerir certificado de tarjeta inteligente**.
- **VPN permanente:** Seleccione si la red VPN siempre está activada. El valor predeterminado es **Desactivado**. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario se desconecta manualmente.
- **Omitir para direcciones locales:** Escriba la dirección y el número de puerto para permitir que los recursos locales omitan el servidor proxy.
- **Configuración de tipo de perfil del plug-in.** Estos parámetros se aplican a plug-ins VPN obtenidos de la Tienda Windows e instalados en los dispositivos de los usuarios.
 - **Dirección de servidor:** Escriba el nombre de dominio completo o la dirección IP del servidor VPN. Este campo es obligatorio.
 - **Recordar credencial:** Seleccione si almacenar la credencial en la memoria caché. El valor predeterminado es **Desactivado**. Cuando está habilitada, las credenciales se almacenan en caché siempre que sea posible.
 - **Sufijo DNS:** Escriba el sufijo DNS.
 - **ID de aplicación de cliente:** Escriba el nombre de familia del paquete que tenga el plug-in VPN.
 - **XML de perfil de plug-in.** Seleccione el perfil personalizado de plug-in VPN que se va a usar. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo. Para obtener información más detallada e indicaciones referentes al formato, póngase en contacto con el proveedor del plug-in.
 - **Redes de confianza:** Escriba una lista de redes, separadas por comas, que no necesiten una conexión VPN para acceder a ellas. Por ejemplo, cuando los usuarios utilizan la red inalámbrica de la empresa, pueden acceder directamente a recursos protegidos.

- **VPN permanente:** Seleccione si la red VPN siempre está activada. El valor predeterminado es **Desactivado**. Cuando está habilitada, la conexión VPN permanece activa hasta que el usuario se desconecta manualmente.
- **Omitir para direcciones locales:** Escriba la dirección y el número de puerto para permitir que los recursos locales omitan el servidor proxy.

Parámetros de Amazon

VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

1 Policy Info

2 Platforms

- ☒ iOS
- ☒ macOS
- ☒ Android
- ☒ Samsung SAFE
- ☒ Samsung KNOX
- ☒ Windows Phone
- ☒ Windows Desktop/Tablet
- ☒ Amazon

3 Assignment

VPN Policy

Connection name *

Vpn Type: L2TP PSK

Server address *

User name: administrator

Password:

L2TP Secret

IPsec Identifier

IPsec pre-shared key

DNS search domains

DNS servers

Forwarding routes

► Deployment Rules

Back Next >

- **Nombre de la conexión:** Escriba el nombre de la conexión.
- **Tipo de VPN.** Seleccione el tipo de conexión. Las opciones posibles son:
 - **L2TP PSK:** Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación de clave previamente compartida. Este es el valor predeterminado.
 - **L2TP RSA:** Protocolo Layer 2 Tunneling Protocol (L2TP) con la autenticación RSA.
 - **IPSEC XAUTH PSK:** Protocolo de seguridad de Internet con clave previamente compartida y autenticación ampliada.
 - **IPSEC HYBRID RSA:** Protocolo de seguridad de Internet con autenticación RSA híbrida.
 - **PPTP:** Túnel punto a punto.

En las siguientes secciones se ofrecen las opciones de configuración para cada uno de los tipos de conexión mencionados.

Configurar L2TP PSK para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Secreto L2TP:** Escriba la clave de secreto compartida.
- **Identificador de IPsec:** Escriba el nombre de la conexión VPN que verán los usuarios en sus dispositivos cuando se conecten.
- **Clave precompartida de IPsec:** Escriba la clave secreta.
- **Dominios de búsqueda de DNS:** Escriba los dominios que se cotejarán con la lista de búsqueda de dominios de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se van a usar para resolver los dominios especificados.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
 - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
 - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Configurar L2TP RSA para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Secreto L2TP:** Escriba la clave de secreto compartida.
- **Dominios de búsqueda de DNS:** Escriba los dominios que se cotejarán con la lista de búsqueda de dominios de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se van a usar 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 usar.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
 - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
 - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Configurar 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:** Si quiere, escriba una contraseña.
- **Identificador de IPsec:** Escriba el nombre de la conexión VPN que verán los usuarios en sus dispositivos cuando se conecten.
- **Clave precompartida de IPsec:** Escriba la clave de secreto compartida.
- **Dominios de búsqueda de DNS:** Escriba los dominios que se cotejarán con la lista de búsqueda de dominios de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se van a usar para resolver los dominios especificados.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
 - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
 - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Configurar 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:** Si quiere, escriba una contraseña.
- **Dominios de búsqueda de DNS:** Escriba los dominios que se cotejarán con la lista de búsqueda de dominios de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se van a usar 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 usar.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
 - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
 - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Configurar 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:** Si quiere, escriba una contraseña.
- **Dominios de búsqueda de DNS:** Escriba los dominios que se cotejarán con la lista de búsqueda de dominios de un dispositivo de usuario.

- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se van a usar 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 el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
 - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
 - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Configurar PPTP para Amazon

- **Dirección del servidor:** Escriba la dirección IP del servidor VPN.
- **Nombre de usuario:** Escriba un nombre de usuario opcional.
- **Contraseña:** Si quiere, escriba una contraseña.
- **Dominios de búsqueda de DNS:** Escriba los dominios que se cotejarán con la lista de búsqueda de dominios de un dispositivo de usuario.
- **Servidores DNS:** Escriba las direcciones IP de los servidores DNS que se van a usar para resolver los dominios especificados.
- **Cifrado PPP (MPPE).** Seleccione si habilitar el cifrado de datos con el Cifrado punto a punto de Microsoft (MPPE). El valor predeterminado es **Desactivado**.
- **Rutas de reenvío:** Si el servidor VPN de la empresa admite rutas de reenvío, haga clic en **Agregar** y lleve a cabo lo siguiente para usar cada ruta de reenvío:
 - **Ruta de reenvío:** Escriba la dirección IP de la ruta de reenvío.
 - Haga clic en **Guardar** para guardar la ruta, o bien haga clic en **Cancelar** para no guardarla.

Directiva de fondo de pantalla

August 9, 2021

La directiva “Fondo de pantalla” permite agregar un archivo JPG o PNG para establecer un fondo de pantalla en un dispositivo iOS para la pantalla de bloqueo, la pantalla de inicio o ambas pantallas. Esta directiva solo está disponible para dispositivos supervisados. Para usar fondos de pantalla diferentes en iPads y iPhones, debe crear varias directivas de fondo de escritorio y aplicarlas a los usuarios correspondientes.

En la siguiente tabla, se ofrece una lista de las dimensiones de imagen que recomienda 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
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE de 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 imagen en píxeles
iPad Pro (1.ª, 2.ª y 3.ª generación de 12,9 pulgadas)	2732 x 2048
iPad Pro (10,5 pulgadas)	2224 x 1668
iPad Pro (9,7 pulgadas)	1536 x 2048
iPad Air, 2	2048 x 1536

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Aplicar a.** En la lista, seleccione **Pantalla de bloqueo**, **Pantalla de inicio (lista de iconos)** o **Pantallas de inicio y de bloqueo** para definir dónde aparecerá el fondo de pantalla.
- **Archivo de fondo de pantalla:** Seleccione el archivo del fondo de pantalla. Para ello, deberá hacer clic en **Examinar** y, a continuación, ir a la ubicación del archivo.

Directiva de filtro de contenido web

November 29, 2023

Puede filtrar el contenido web en dispositivos iOS. Para ello, utilice la función de filtrado automático de Apple con sitios específicos que usted agregue a listas de sitios permitidos y sitios bloqueados. La directiva “Filtro de contenido web” solo está disponible para dispositivos iOS en modo supervisado. Para obtener información sobre cómo colocar un dispositivo iOS en modo supervisado, consulte [Implementar dispositivos mediante Apple Configurator 2](#).

Nota:

Los dispositivos Android no admiten el filtrado de contenido web.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Tipo de filtro.** En la lista, haga clic en **Integrado** o **Plug-in** y, a continuación, siga los procedimientos de la opción que elija. El valor predeterminado es **Integrado**.

Tipo de filtro integrado

- **Filtro de contenido web**
 - **Filtro automático habilitado.** Seleccione si utilizar la función de filtro automático de Apple para analizar sitios web en busca de contenido inadecuado. El valor predeterminado es **Desactivado**.
 - **Direcciones URL permitidas.** Esta lista se omite si la opción **Filtro automático habilitado** está **desactivada**. Si la opción **Filtro automático habilitado** está **activada**, los elementos de esta lista son siempre accesibles, independientemente de si el filtro automático

permite el acceso. Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada URL a la lista de permitidos:

- ★ 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 bien haga clic en **Cancelar** para no guardarlo.
- **URL bloqueada.** Los elementos de esta lista están siempre bloqueados. Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada URL a la lista de bloqueados:
- ★ Escriba la URL del sitio web que quiere bloquear. Debe agregar <https://> o <https://> antes de la dirección web.
 - ★ Haga clic en **Guardar** para guardar el sitio web en la lista de bloqueados, o bien haga clic en **Cancelar** para cancelar la operación.

- **Agregar lista de permitidos a marcadores**

- **Agregar lista de permitidos a marcadores:** Especifica los sitios a los que pueden acceder los usuarios. Agregue las URL de los sitios web para permitir el acceso a ellos.
- ★ **URL.** La URL de cada sitio web al que los usuarios pueden acceder. Por ejemplo, para permitir el acceso al almacén Citrix Secure Hub, agregue la URL del servidor de Citrix Endpoint Management a la lista **URL**. Debe agregar <https://> o <https://> antes de la dirección web. Este campo es obligatorio.
 - ★ **Carpeta de marcadores.** Escriba un nombre opcional para la carpeta de marcadores. Si este campo se deja en blanco, el marcador se agrega al directorio predeterminado de marcadores.
 - ★ **Título.** Escriba un título descriptivo para el sitio web. Por ejemplo, introduzca “Google” para la dirección URL <https://google.com>.
 - ★ Haga clic en **Guardar** para guardar el sitio web en la lista de permitidos, o bien haga clic en **Cancelar** para no guardarlo.

Tipo de filtro plug-in

- **Nombre del filtro.** Escriba un nombre único para el filtro.
- **Identificador.** Escriba el ID de paquete del plugin que proporciona el servicio de filtrado.
- **Dirección del servicio.** Escriba una dirección de servidor opcional. Los formatos válidos son la URL, la dirección IP o el nombre de host.
- **Nombre de usuario.** Escriba un nombre de usuario opcional para el servicio.
- **Contraseña.** Escriba una contraseña opcional para el servicio.
- **Certificado.** En la lista, haga clic en el certificado de identidad opcional que se va a usar para autenticar al usuario en el servicio. El valor predeterminado es **Ninguno**.
- **Filtrar tráfico de WebKit.** Seleccione si se debe filtrar el tráfico WebKit.

- **Filtrar tráfico de socket.** Seleccione si filtrar el tráfico de sockets.
- **Datos personalizados.** Haga clic en **Agregar** y lleve a cabo lo siguiente para agregar cada clave personalizada al filtro Web:
 - **Clave.** Escriba la clave personalizada.
 - **Valor.** Escriba un valor para la clave personalizada.
 - Haga clic en **Guardar** para guardar la clave personalizada, o bien haga clic en **Cancelar** para cancelar la operación.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.

Directiva de clip web

March 1, 2024

Puede colocar accesos directos o clips web para que los sitios web aparezcan junto a las aplicaciones en los dispositivos de usuario. 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 e iPadOS, configure la directiva de diseño de pantalla de inicio para organizar los clips web que cree. Si restringe el acceso a aplicaciones en iOS, asegúrese de configurar la directiva de restricciones para permitir clips web. Para obtener información sobre la configuración de estas directivas, consulte [Directiva de diseño de pantalla inicio](#) y [Directiva de restricciones](#).

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de iOS

- **Etiqueta:** Escriba la etiqueta que aparecerá con el clip web.
- **URL:** Escriba la URL asociada al clip web. La URL debe comenzar por un protocolo; por ejemplo <https://server>.

- **Eliminable:** Seleccione si los usuarios pueden quitar el clip web. El valor predeterminado es **Desactivado**. Esta opción no se admite en los iPads compartidos.
- **Icono a actualizar:** Seleccione el icono que se utilizará para el clip web. Para ello, haga clic en **Examinar** para ir a la ubicación del archivo.
- **Icono precompuesto:** Seleccione si habrá efectos que se aplicarán al icono (como esquinas redondeadas, sombra paralela y brillo de reflejos, entre otros). El valor predeterminado es **No**, con lo que se agregan efectos.
- **Pantalla completa:** Seleccione si la página web enlazada se abre en modo de pantalla completa. Esta configuración también permite a un iPad abrir solo un sitio web. Como alternativa, para configurar iPads para que se ejecuten en modo quiosco, utilice la directiva de bloqueo de aplicaciones. Para obtener más información, consulte [Configurar un iPad como un quiosco](#). El valor predeterminado es **Desactivado**.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.
 - * **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar la eliminación de la directiva. Disponible solo para iOS 6.0 y versiones posteriores.
 - **Ámbito del perfil:** Seleccione si esta directiva se aplica a un usuario o a todo el sistema. El valor predeterminado es **Sistema**. Disponible solo para iOS 9.3 y versiones posteriores.

Parámetros de macOS

- **Etiqueta:** Escriba la etiqueta que aparecerá con el clip web.
- **URL:** Escriba la URL asociada al clip web. La URL debe comenzar por un protocolo; por ejemplo <https://server>.
- **Icono a actualizar:** Seleccione el icono que se utilizará para el clip web. Para ello, haga clic en **Examinar** para ir a la ubicación del archivo.
- **Configuraciones de directivas**
 - **Quitar directiva:** Elija un método para programar la eliminación de directivas. Las opciones disponibles son **Seleccionar fecha** y **Demora hasta la eliminación (en horas)**.
 - * **Seleccionar fecha:** Haga clic en el calendario para seleccionar la fecha específica de la eliminación.

- ★ **Demora hasta la eliminación (en horas):** Introduzca un número, en horas, hasta que tenga lugar 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**, **Código de acceso requerido** o **Nunca** en el menú. Si selecciona **Código de acceso requerido**, introduzca un código en el campo **Código de acceso para la eliminación**.

Parámetros de Android

- **Regla:** Seleccione si esta directiva agrega o quita clips 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 quiere usar un archivo de icono. El valor predeterminado es **Desactivado**.
- **Archivo del icono:** Si **activa** el parámetro **Definir un icono**, deberá seleccionar el archivo de icono que se va a usar. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.

Parámetros de escritorios y tabletas Windows

- **Nombre:** Escriba la etiqueta que aparecerá con el clip web.
- **URL:** Escriba la URL asociada al clip web.

Directiva de Agente de Windows

November 29, 2023

Utilice la directiva “Agente Windows” para ejecutar scripts de PowerShell en escritorios y tabletas Windows administrados. Puede apuntar a los archivos de script cargados en Citrix Endpoint Management como una aplicación empresarial y a otros servidores que alojan scripts. Para obtener más información sobre cómo agregar aplicaciones de empresa, consulte [Agregar aplicaciones](#).

Todos los scripts se ejecutan en estado privilegiado; no es necesario ejecutar scripts 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 este script devuelve un resultado determinado. En función del 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 un archivo MST.

Para agregar o configurar esta directiva, vaya a **Configurar > Directivas de dispositivo**. Para obtener más información, consulte [Directivas de dispositivo](#).

Parámetros de tabletas y escritorios Windows

Device Policies

Apps

Media

Actions

Content Collaboration

Enrollment Profiles

Delivery Groups

Windows Agent policy

1 Policy Info

2 Platforms

Clear All

☒ Windows Desktop/Tablet

3 Assignment

Windows Agent policy

This policy lets you configure, schedule, and run PowerShell scripts on MDM-managed devices.

Add

Delete

example

Config name *

example

Task type *

PowerShell

Script type *

Uploaded script

Script *

Select an option

Schedule *

Run once

Deployment Rules

Back

Next >

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

950

Device Policies

Apps

Media

Actions

Content Collaboration

Enrollment Profiles

Delivery Groups

Windows Agent policy

1 Policy Info

2 Platforms

Clear All

☒ Windows Desktop/Tablet

3 Assignment

Windows Agent policy

This policy lets you configure, schedule, and run PowerShell scripts on MDM-managed devices.

Add

Delete

example

Config name *

example

Task type *

PowerShell

Script type *

Script location (URL)

Script location (URL) *

Schedule *

Run once

Deployment Rules

Back

Next >

- **Nombre de la configuración:** Escriba un nombre descriptivo para la configuración.
- **Tipo de tarea:** Seleccione **PowerShell**.
- **Tipo de script:** Seleccione **Script cargado** para los scripts que cargó en Citrix Endpoint Management o seleccione **Ubicación del script (URL)** para los scripts alojados externamente. Para obtener más información sobre cómo cargar un script en Citrix Endpoint Management, consulte [Agregar aplicaciones Win32 como aplicaciones de empresa](#).
 - **Seleccionar script:** Si ha elegido **Script cargado**, seleccione el script a ejecutar.
 - **Ubicación del script (URL):** Si eligió **Ubicación del script (URL)**, escriba la ubicación del script que se ejecutará. Esta URL debe entregar el script como carga útil. Citrix Endpoint Management no admite las URL que entregan scripts como descarga de JavaScript. El script también debe estar disponible públicamente.
- **Programación:** Seleccione **Ejecutar una vez** para ejecutar el script seleccionado una vez o seleccione **Ejecutar periódicamente** para ejecutar el script de manera recurrente.
 - **Ejecutar cada (horas):** Escriba las horas que deben pasar entre cada ejecución del script.

Para consultar el estado de un script, vaya a **Administrar > Dispositivos** en la consola. Seleccione el dispositivo donde quiere consultar el estado del script y haga clic en **Modificar**. En **Propiedades**, puede consultar el estado de los scripts haciendo clic en **Descargar**, en la sección del encabezado **Agente Windows**.

Implementar un script de PowerShell para desencadenar 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.

```
1 $body = @{
2   }
3
4 $firewallEnabled = Get-ItemPropertyValue HKLM:\SYSTEM\
    CurrentControlSet\Services\SharedAccess\Parameters\
    FirewallPolicy\StandardProfile -Name EnableFirewall
5 if($firewallEnabled -eq 1){
6
7   $body["firewallEnabled"]="true"
8 }
9 else {
10
11   $body["firewallEnabled"]="false"
12 }
13
14 $body | ConvertTo-Json -Depth 10
15 <!--NeedCopy-->
```

Este script devuelve un valor de

```
1 {
2
3   "firewallEnabled": "true"
4 }
5
6 <!--NeedCopy-->
```

o

```
1 {
2
3   "firewallEnabled": "false"
4 }
5
6 <!--NeedCopy-->
```

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 Agente de Windows tal y como se describe en este artículo. El script debe estar 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 donde quiere consultar el estado del script y haga clic en **Modificar**.

- c) Haga clic en **Descargar** en el encabezado **Agente Windows**.
5. Configure una acción automatizada basada en el estado recibido. Para obtener más información acerca de la configuración de acciones automatizadas, consulte [Crear una acción automatizada basada en un resultado de la directiva Agente Windows](#). En esa sección, se muestran las acciones automatizadas específicas creadas para el script de ejemplo y la directiva de Agente de Windows.

Directiva de configuración de GPO de Windows

November 29, 2023

La directiva de configuración de GPO de Windows permite:

- Usar la consola de Citrix Endpoint Management para importar objetos de directiva de grupo (GPO) e implementarlos en dispositivos con Windows 10 o Windows 11.
- Configurar objetos de directiva de grupo (GPO) para cualquier dispositivo Windows admitido por Citrix Workspace Environment Management.
- Configurar objetos de directivas de grupo a nivel de dispositivo y usuario.

Importar objetos de directiva de grupo para la implementación en dispositivos con Windows 10 o Windows 11

En lugar de depender de un administrador de AD para utilizar la consola de administración de directivas de grupo para administrar los GPO, puede importar e implementar los 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 al administrador de AD que exporte los GPO desde la consola de Administración de directivas de grupo y que le proporcione los archivos.
2. En la consola Citrix Endpoint Management, vaya a **Configurar > Directivas de dispositivo** y cree una directiva **Configuración de GPO de Windows**.
3. Haga clic en **Cargar**, busque el archivo y, a continuación, haga clic en **Abrir** para importar el archivo.

The screenshot displays the 'Windows GPO Configuration Policy' configuration interface. The top navigation bar includes 'Device Policies', 'Apps', 'Media', 'Actions', 'Content Collaboration', 'Enrollment Profiles', and 'Delivery Groups'. The left sidebar shows a tree view with '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' section is expanded, showing a 'Policy Name' field, a 'Description' text area, and an 'Auto save' toggle set to 'ON'. Below this is an 'Upload GPO policy' section with a description and an 'Upload' button.

Para obtener información sobre la configuración de GPO, consulte [Parámetros de tabletas y escritorios Windows](#) en este artículo.

Configurar GPO para su implementación en Citrix Workspace Environment Management

La directiva de configuración de GPO de Windows permite configurar GPO para cualquier dispositivo Windows admitido Citrix Workspace Environment Management. 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 acerca de la instalación del agente Workspace Environment Management, consulte [Instalación y configuración](#).

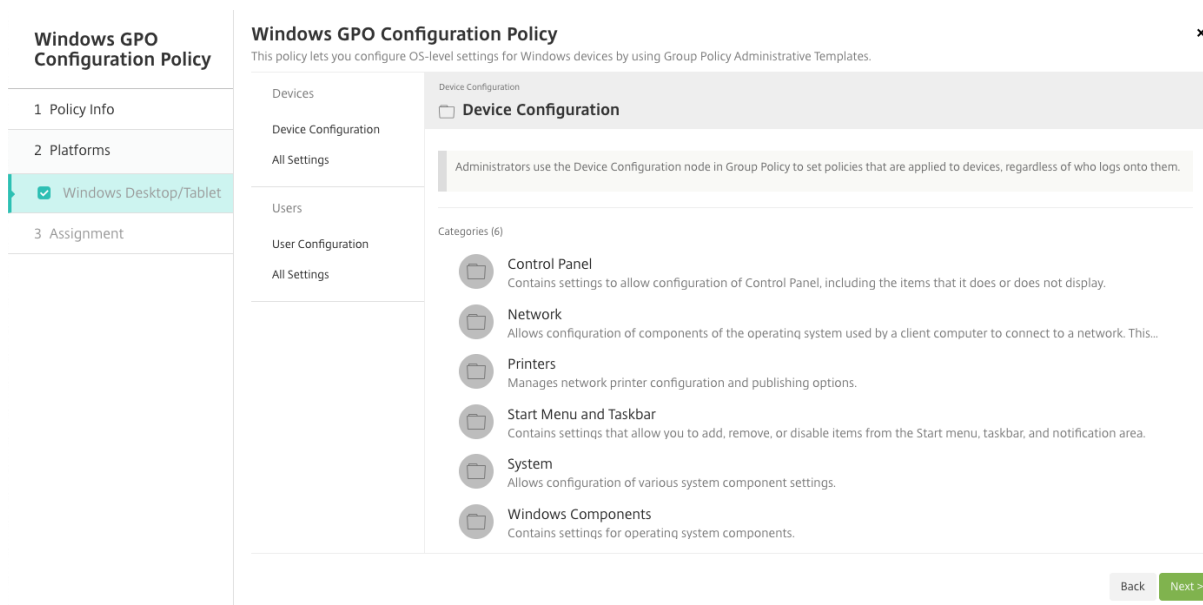
Esta directiva utiliza todos los archivos ADMX del sistema operativo Windows. Si quiere cargar un archivo ADMX de terceros, utilice la directiva Configuración de aplicaciones. Para obtener más información sobre cómo cargar archivos ADMX de terceros, consulte [Directiva Configuración de aplicaciones](#).

- Puede enviar configuraciones de GPO en cualquier dispositivo admitido en WEM, incluso si Citrix Endpoint Management no presenta compatibilidad con el dispositivo de forma nativa. Para ver una lista de los dispositivos admitidos, consulte [Requisitos del sistema operativo](#).
- Esta directiva requiere que un dispositivo tenga instalado y configurado el agente WEM. No es necesario inscribir los dispositivos con MDM o MAM.
- Citrix Endpoint Management envía la configuración de GPO a través del canal WEM. (Microsoft no permite enviar parámetros a nivel de dispositivo a través del canal MDM). Los dispositivos que reciben la directiva de configuración de GPO de Windows se ejecutan en el modo de Endpoint Management denominado WEM (Citrix Workspace Environment Management). En la lista **Administrar > Dispositivos** de dispositivos inscritos, la columna **Modo** para 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](#).

Parámetros de tabletas y escritorios Windows

Esta directiva permite configurar objetos de directivas de grupo a nivel de dispositivo y usuario.



Seleccione y configure el objeto de directiva de grupo de Windows para implementarlo en sus dispositivos Windows. Puede modificar la **Configuración del dispositivo** y la **Configuración de usuario**. Las directivas se enumeran en una estructura árbol. Haga clic en **Todos los parámetros** para mostrar todos los parámetros. Para obtener información acerca de los parámetros, descargue una hoja de referencia de objeto de directiva de grupo desde [Microsoft](#).

Para configurar un parámetro, primero debe habilitarlo. Durante la configuración, Citrix Endpoint Management guarda automáticamente los cambios para que esos parámetros se mantengan. Si intenta salir de la página antes de guardar un parámetro, un mensaje emergente le indicará que hay cambios no guardados.

Si un parámetro tiene dos opciones, aparece la selección de un botón de opción. Con más de dos opciones, aparece un menú.

Nota:

Si necesita verificar qué parámetros configuró, puede hacer lo siguiente.

1. En la consola de Citrix Endpoint Management, abra la directiva de **Configuración de GPO de Windows** que quiera modificar.
2. En **Dispositivos** o **Usuarios**, seleccione **Todos los parámetros**.

3. Ordene la tabla por **Estado**, en ascendente. Todas las directivas no configuradas tienen el estado **No configurado**. Las directivas que configure aparecen en la parte superior.

Directiva de Windows Hello para empresas

February 11, 2022

Windows Hello para empresas permite a los usuarios iniciar sesión en dispositivos Windows mediante su cuenta de Active Directory o Azure Active Directory. La directiva “Windows Hello para empresas” se utiliza para habilitar la función, de modo que los usuarios puedan aprovisionar Windows Hello para empresas en sus dispositivos. La directiva también permite configurar limitaciones de códigos de acceso y otras funciones de seguridad.

Vaya a **Configurar > Directivas de dispositivo** para agregar la directiva de Windows Hello para empresas. Configure estos parámetros:

Parámetros de escritorios y tabletas Windows

Device Policies

Apps

Media

Actions

Content Collaboration

Enrollment Profiles

Delivery Groups

Windows Hello for Business policy

1 Policy Info

2 Platforms

Clear All

Windows Phone

Windows Desktop/Tablet

3 Assignment

Windows Hello for Business policy

Windows Hello for Business

Use Windows Hello for Business

Require security device

PIN complexity

Minimum PIN length *

4

Maximum PIN length *

127

Uppercase letters

Do not allow

Lowercase letters

Do not allow

Special characters

Do not allow

Digits

Require

History *

0

Expiration *

0

Biometrics

Use biometrics

Deployment Rules

Back

Next >

- **Usar Windows Hello para empresas.** Habilite esta función para permitir que los usuarios aprovisionen Windows Hello para empresas en su dispositivo.
- **Requerir dispositivo de seguridad.** Para exigir que los usuarios tengan un módulo TPM (Trusted Platform Module) para iniciar sesión.
- **Longitud mínima/máxima del PIN.** La longitud mínima y la longitud máxima para los PIN de los usuarios. La **longitud mínima del PIN** es **4** de manera predeterminada. La **longitud máxima del PIN** es **127** de manera predeterminada.
- **Letras mayúsculas, Letras minúsculas, Caracteres especiales.** Seleccione si quiere **Permitir**, **Requerir** o **No permitir** cada uno de estos tipos de caracteres. El valor predeterminado es **No permitir**.
- **Dígitos.** Seleccione si quiere **Permitir**, **Requerir** o **No permitir** dígitos. El valor predeterminado es **Requerir**.
- **Historial.** La cantidad de PIN anteriores que los usuarios no pueden volver a utilizar. El valor predeterminado es **0**, lo que significa que los usuarios pueden reutilizar todos los PIN.
- **Caducidad.** La cantidad de días antes de que un usuario deba cambiar su PIN. El valor prede-

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

957

terminado es **0**, lo que significa que los PIN no caducan.

- **Usar biometría:** Permite el uso de biometría en lugar de PIN para el inicio de sesión de los usuarios.

Agregar aplicaciones

March 1, 2024

Al agregar aplicaciones a Citrix Endpoint Management, estas se pueden gestionar vía la administración de aplicaciones móviles (MAM). Citrix Endpoint Management simplifica la entrega de aplicaciones, la gestión de licencias de software, la configuración y la administración del ciclo de vida de las aplicaciones.

Habilitar aplicaciones para MDX es una etapa importante en la preparación de algunos tipos de aplicaciones para su distribución a los dispositivos de los usuarios. Para ver una introducción a MDX, consulte [Componentes de Citrix Endpoint Management](#) e [Introducción al SDK de MAM](#).

- Citrix recomienda habilitar aplicaciones para MDX con la ayuda del SDK de MAM. Si no, puede seguir empaquetando aplicaciones para MDX hasta que el MDX Toolkit quede obsoleto y se retire. Consulte [Elementos retirados](#).
- No puede utilizar MDX Toolkit para empaquetar aplicaciones móviles de productividad de Citrix. Obtenga los archivos MDX de las aplicaciones móviles de productividad desde las descargas de Citrix.

Agregar aplicaciones a la consola de Citrix Endpoint Management implica:

- Configurar las opciones de las aplicaciones
- Opcionalmente, puede organizar las aplicaciones en categorías para organizarlas en Citrix Secure Hub
- Opcionalmente, puede definir flujos de trabajo para que se requiera aprobación antes de permitir a los usuarios acceder a una aplicación
- Implementar las aplicaciones a los usuarios

En este artículo, se describen los flujos de trabajo generales para agregar aplicaciones. Consulte los siguientes artículos para conocer datos concretos de cada plataforma:

- [Distribuir aplicaciones de Android Enterprise](#)
- [Distribuir aplicaciones de Apple](#)

Importante:

Citrix Endpoint Management permite agregar y mantener hasta 300 aplicaciones. Si supera este

límite, el sistema se volverá inestable.

Tipos y funciones de aplicaciones

En la tabla siguiente, se resumen los tipos de aplicaciones que se pueden implementar con Citrix Endpoint Management.

Tipo de aplicación	Fuentes	Notas	Consulte
MDX	Aplicaciones iOS y Android desarrolladas internamente para los usuarios. Aplicaciones móviles de productividad de Citrix.	Desarrolle aplicaciones iOS o Android con el SDK de MAM o empaquéte las con MDX Toolkit. Para las aplicaciones móviles de productividad, descargue los archivos MDX de la tienda pública de descargas de Citrix. A continuación, agregue las aplicaciones a Citrix Endpoint Management.	Agregar una aplicación MDX
Tienda pública de aplicaciones	Aplicaciones gratuitas o de pago provenientes de tiendas públicas de aplicaciones, como Google Play o el App Store de Apple.	Cargue las aplicaciones, habilítelas para MDX y, a continuación, agréguelas a Citrix Endpoint Management.	Agregar una aplicación de la tienda pública de aplicaciones

Tipo de aplicación	Fuentes	Notas	Consulte
Web y SaaS	La red interna (aplicaciones web) o una red pública (SaaS).	Citrix Endpoint Management ofrece inicio de sesión único SSO móvil a aplicaciones SaaS nativas desde dispositivos iOS y Android inscritos en MDM. O bien, use conectores de aplicación SAML.	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 de empresa están en ubicaciones de red de entrega de contenido o servidores de Citrix Endpoint Management.	Agregue las aplicaciones a Citrix Endpoint Management.	Agregar una aplicación de empresa
Enlace web	Direcciones web de Internet, direcciones web de intranet o aplicaciones web que no requieren inicio SSO.	Configure enlaces web en Citrix Endpoint Management.	Agregar un enlace web

Al planificar la distribución de aplicaciones, tenga en cuenta los siguiente:

- Acerca de las instalaciones silenciosas
- Acerca de aplicaciones obligatorias y opcionales

- Acerca de las categorías de aplicaciones
- Entregar aplicaciones de empresa desde la CDN de Citrix
- Habilitar aplicaciones de Microsoft 365
- Aplicar flujos de trabajo
- Personalizar la marca en el almacén de aplicaciones y Citrix Secure Hub
- Citrix Virtual Apps and Desktops a través del almacén de aplicaciones

Acerca de las instalaciones silenciosas

Citrix ofrece la instalación y la actualización de versiones de manera silenciosa de aplicaciones iOS, Android Enterprise y Samsung. La instalación silenciosa significa que no se pide a los usuarios que instalen las aplicaciones que usted implementa en el dispositivo. Las aplicaciones se instalan automáticamente en segundo plano.

Requisitos previos para implementar la instalación silenciosa:

- Para iOS, coloque el dispositivo iOS administrado en modo supervisado. Para obtener más información, consulte [Directiva de importación de perfiles de iOS y macOS](#).
- Para Android Enterprise, las aplicaciones se instalan en el perfil de trabajo de Android del dispositivo. Para obtener más información, consulte [Android Enterprise](#).
- Para dispositivos Samsung, habilite Samsung Knox en el dispositivo.

Para ello, configure la directiva de clave de licencia MDM de Samsung para que genere códigos de acceso de licencia ELM y Knox de Samsung. Para obtener más información, consulte [Directivas de claves de licencia para la administración de dispositivos móviles \(MDM\) Samsung](#).

Acerca de aplicaciones obligatorias y opcionales

Cuando se agregan aplicaciones a un grupo de entrega, se puede elegir si serán opcionales u obligatorias. Citrix recomienda implementar aplicaciones con la opción **Requerido**.

- Las aplicaciones necesarias se instalan silenciosamente en los dispositivos del usuario, lo que minimiza la interacción con ellas. 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 reciben inmediatamente actualizaciones en situaciones como estas:

- Se carga una nueva aplicación y se marca como obligatoria.

- Se marca una aplicación existente como obligatoria.
- Un usuario elimina una aplicación obligatoria.
- Hay una actualización de Citrix Secure Hub disponible.

Requisitos para la implementación forzosa de las aplicaciones obligatorias

- Citrix Secure Hub 10.5.15 para iOS y 10.5.20 para Android (versiones mínimas)
- SDK de MAM o MDX Toolkit 10.6 (versión mínima)
- Después de actualizar la versión de Citrix Endpoint Management y Citrix Secure Hub, los usuarios que tengan dispositivos inscritos deberán cerrar la sesión y, a continuación, iniciarla en Citrix Secure Hub para obtener las actualizaciones necesarias de las aplicaciones en la implementación.

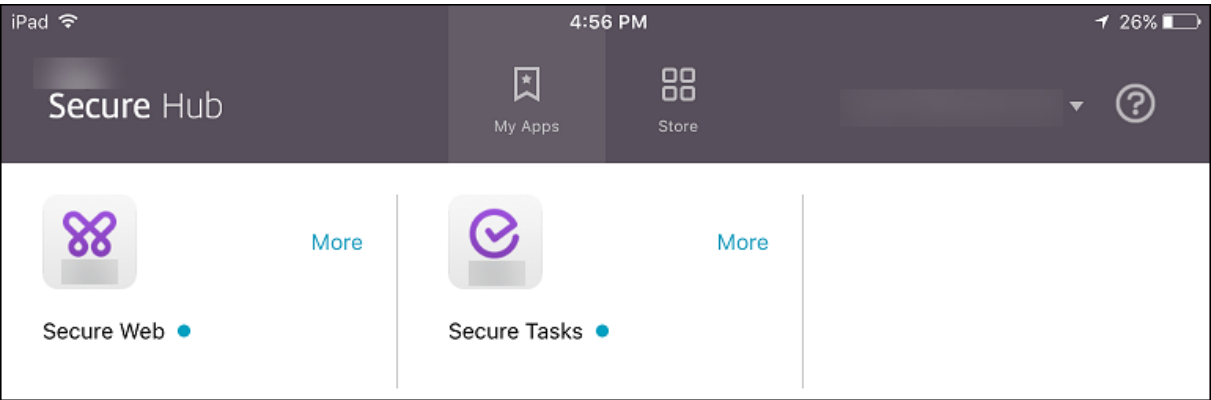
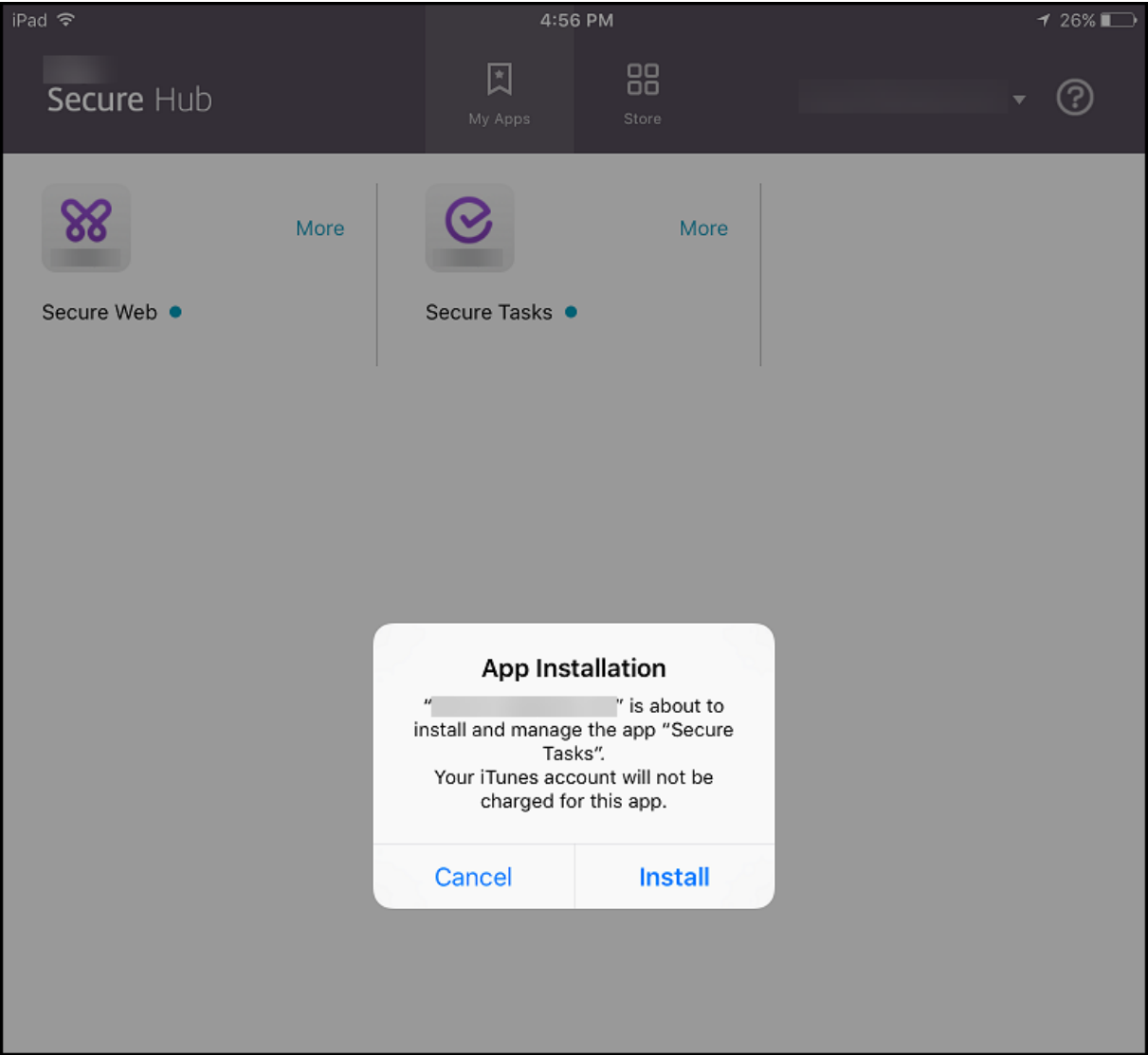
Ejemplos

En los siguientes ejemplos, se muestra la secuencia de agregar la aplicación llamada Secure Tasks a un grupo de entrega y, a continuación, implementar ese grupo de entrega.

The first screenshot shows the 'Apps' configuration page for a delivery group. On the left, a sidebar lists navigation options: Device Policies, Apps, Actions, ShareFile, Enrollment Profiles, and Delivery Groups. The 'Apps' section is selected. The main area is titled 'Apps' and contains a search bar and a list of available apps: Angry Bird, Box, Fit, and SecureNotes. A hand icon with an arrow points from the 'SecureNotes' app to the 'Required Apps' list on the right. The 'Required Apps' list includes SecureWeb, Enterprise-01, GTM, and SecureTask (which is highlighted with a red box). Below this, the 'Optional Apps' list includes Jira and Office365_SAML.

The second screenshot shows the 'Delivery Groups' page. It features a search bar, a 'Show filter' link, and a toolbar with icons for Add, Edit, Deploy (highlighted with a red box), Delete, and Export. Below the toolbar is a table with columns for Status, Name, Last Updated, and Disabled. The table contains two rows: 'AllUsers' (last updated Apr 18 2017 2:43 AM) and 'DeliveryGroup-01' (last updated Apr 19 2017 8:47 AM). The 'DeliveryGroup-01' row is highlighted in green. At the bottom, it shows 'Showing 1 - 2 of 2 items' and 'Items per page: 10'.

Una vez implementada la aplicación de ejemplo (Secure Tasks) en el dispositivo del usuario, Citrix Secure Hub pide al usuario que instale la aplicación.



Importante:

Las aplicaciones obligatorias habilitadas con MDX, incluidas las aplicaciones de empresa y las aplicaciones de tiendas públicas, se actualizan de versión de inmediato. Esta actualización de

versión se produce incluso si configura una directiva MDX para un período de gracia de actualización de la aplicación y el usuario elige actualizar la aplicación más tarde.

Flujo de trabajo en iOS para aplicaciones obligatorias de empresa y tienda pública

1. Implemente la aplicación de aplicaciones móviles de productividad 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. Se actualiza la aplicación en la pantalla de inicio. Y, para las aplicaciones de tiendas públicas, la actualización de versión se inicia automáticamente. No se solicita la actualización a los usuarios.
5. Los usuarios abren la aplicación desde la pantalla de inicio. Las aplicaciones se actualizan de versión inmediatamente, aunque establezca un período de gracia de actualización y el usuario toque actualizar la aplicación más tarde

Flujo de trabajo en Android para aplicaciones obligatorias de empresa

1. Implemente la aplicación de aplicaciones móviles de productividad 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. Se actualiza la versión de la aplicación. (los dispositivos Nexus solicitan instalar las actualizaciones, mientras que los dispositivos Samsung realizan una instalación silenciosa).
4. Los usuarios abren la aplicación desde la pantalla de inicio. Las aplicaciones se actualizan de versión inmediatamente, aunque establezca un período de gracia de actualización y el usuario toque actualizar la aplicación más tarde (los dispositivos Samsung llevan a cabo una instalación silenciosa).

Flujo de trabajo en Android para aplicaciones obligatorias de tienda pública

1. Implemente la aplicación de aplicaciones móviles de productividad 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. Aparece el icono de actualización en el almacén.

4. La actualización de versión comienza automáticamente. (Los dispositivos Nexus piden a los usuarios que instalen la actualización.)
5. Abra la aplicación desde la pantalla de inicio. Se actualiza la versión de la aplicación. No se solicita el período de gracia a los usuarios. (los dispositivos Samsung llevan a cabo una instalación silenciosa).

Desinstalar una aplicación cuando está configurada como obligatoria

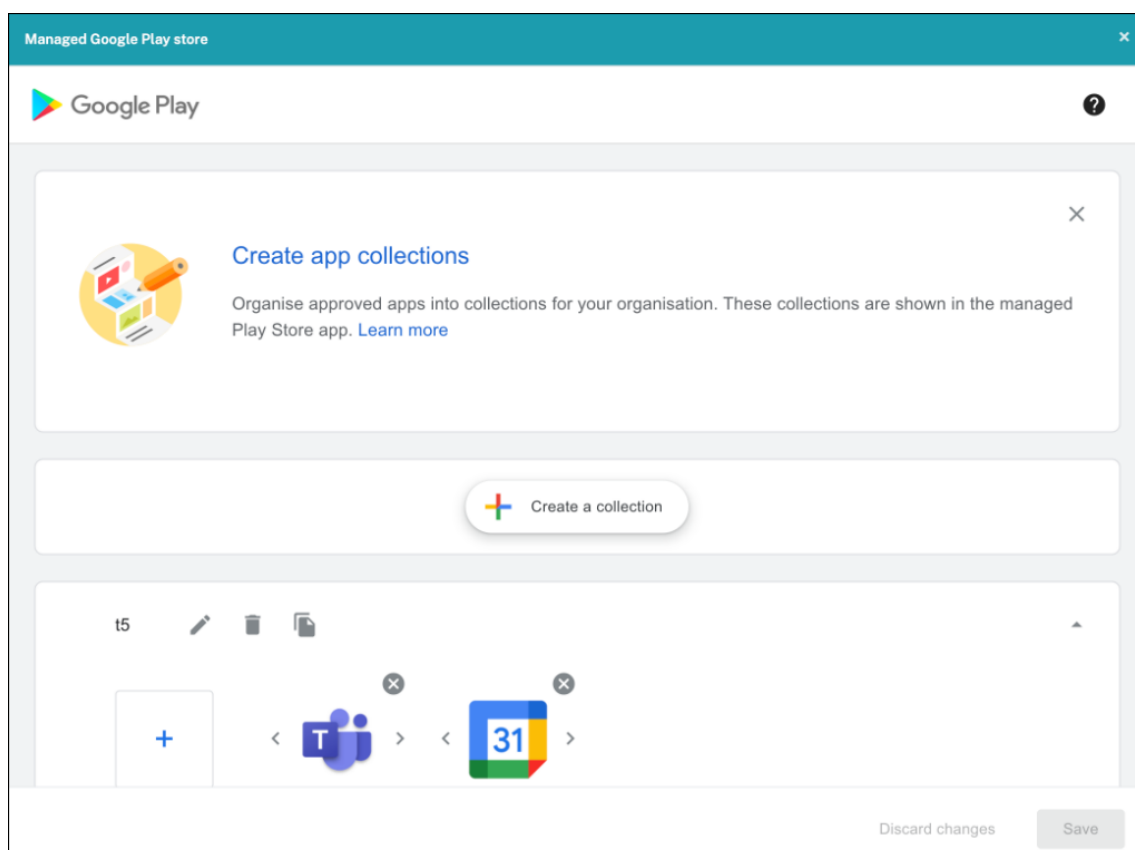
Puede permitir que los usuarios desinstalen una aplicación configurada como obligatoria. Para ello, vaya a **Configurar > Grupos de entrega** y mueva la aplicación de **Aplicaciones obligatorias** a **Aplicaciones opcionales**.

Recomendado: Use un grupo de entrega específico para cambiar temporalmente una aplicación a opcional, de modo que usuarios concretos puedan desinstalarla. Entonces, puede cambiar una aplicación obligatoria a opcional, implementarla en ese grupo de entrega y desinstalarla de esos dispositivos. Después de eso, si quiere que en las inscripciones futuras de ese grupo de entrega se requiera la aplicación, puede volver a establecerla como obligatoria.

Organizar aplicaciones (Android Enterprise)

Cuando los usuarios inician sesión en Citrix Secure Hub, reciben una lista de las aplicaciones, los enlaces web y los almacenes que se hayan configurado en Citrix Endpoint Management. En Android Enterprise, puede organizar estas aplicaciones en colecciones para permitir que los usuarios accedan solo a determinadas aplicaciones, almacenes o enlaces web. Por ejemplo, crea una colección Finanzas y, a continuación, agrega aplicaciones a la colección que solo pertenecen al ámbito financiero. O bien puede configurar una colección llamada Ventas y asignarle aplicaciones de ventas.

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones > Organizar aplicaciones**. Aparece la ventana **Google Play Store administrado**.



2. Haga clic en **Crear una colección** y seleccione las aplicaciones que quiere agregar a esa colección.
3. Cuando haya terminado de agregar colecciones, haga clic en **Guardar**.

Nota:

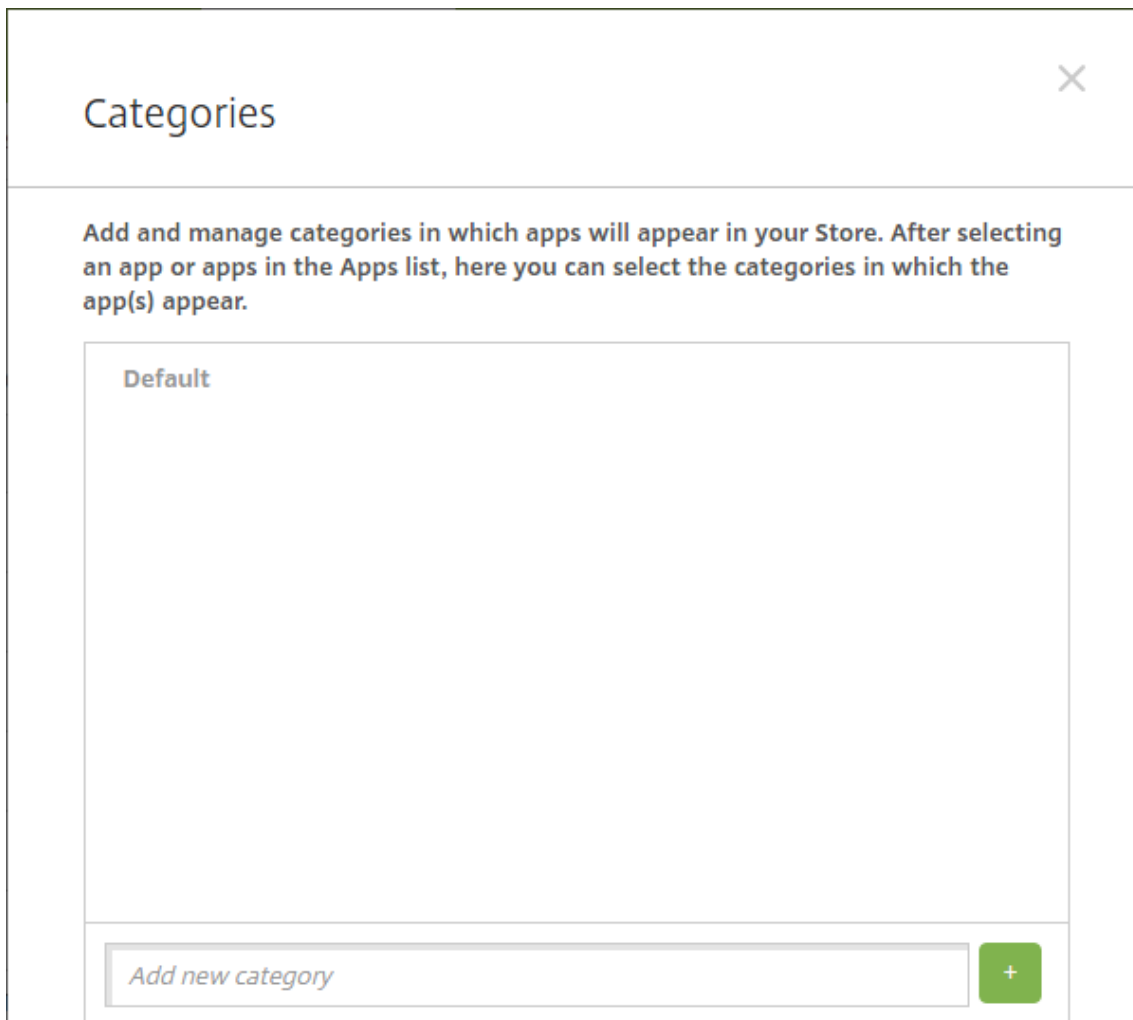
Los administradores de TI deben aprobar una aplicación antes de que se pueda agregar a una colección en la ventana Google Play Store administrado. Un administrador de TI puede aprobar una aplicación desde <https://play.google.com/work>. En una versión futura, no necesitará aprobar una aplicación antes de agregarla a una colección.

Acerca de las categorías de aplicaciones (iOS y MDX)

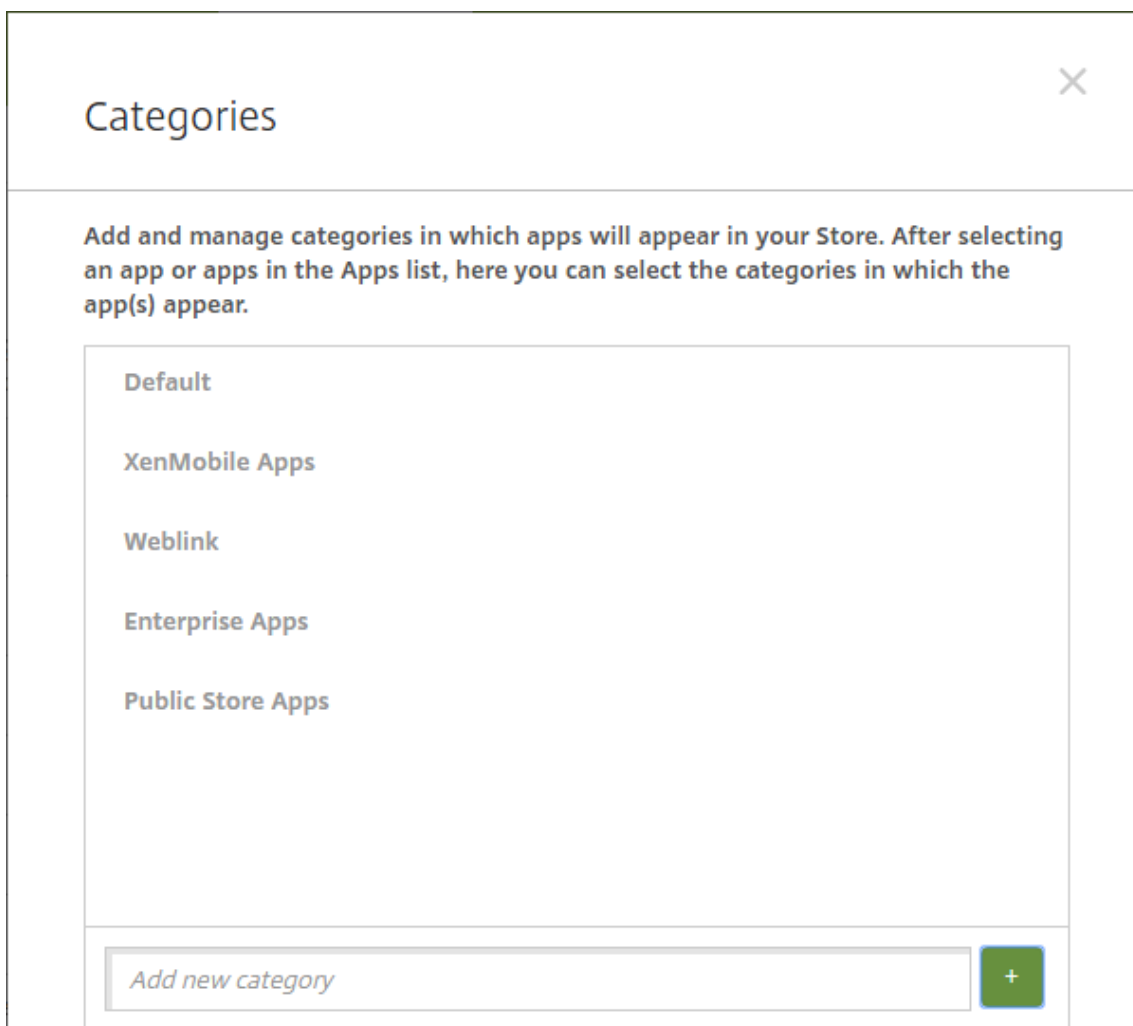
Cuando los usuarios inician sesión en Citrix Secure Hub, reciben una lista de las aplicaciones, los enlaces web y los almacenes que se hayan configurado en Citrix Endpoint Management. En iOS o MDX, puede usar categorías de aplicaciones para que los usuarios accedan solo a determinadas aplicaciones, tiendas o enlaces web. Por ejemplo, puede crear una categoría llamada Finanzas y agregar a esa categoría aplicaciones que solo pertenezcan al ámbito financiero. O bien puede configurar una categoría llamada Ventas y asignarle aplicaciones de ventas.

Al configurar o modificar una aplicación, un enlace web o un almacén, puede agregarla a una o varias 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 agregar cada categoría, lleve a cabo lo siguiente:
 - Escriba el nombre de la categoría que quiere agregar en el campo **Agregar nueva categoría**, situado en la parte inferior del cuadro de diálogo. Por ejemplo, puede escribir “Aplicaciones de empresa” para crear una categoría que contenga las aplicaciones de la empresa.
 - Haga clic en el signo más (+) para agregar la categoría. La categoría recién creada se agregará y aparecerá en el cuadro de diálogo **Categorías**.



3. Cuando haya terminado de agregar categorías, cierre el cuadro de diálogo **Categorías**.
4. En la página **Aplicaciones**, puede colocar una aplicación existente en una categoría nueva.
 - Seleccione la aplicación que quiera categorizar.
 - Haga clic en **Edit**. Aparecerá la página **Información de la aplicación**.
 - En la lista **Categoría de la aplicación**, aplique la nueva categoría marcando la casilla de la categoría en cuestión. Desmarque las casillas de aquellas categorías existentes que no quiera aplicar a la aplicación.
 - Haga clic en la ficha **Asignaciones de grupo de entrega** o haga clic en **Siguiente** en las páginas restantes de la configuración de la aplicación.
 - Haga clic en **Guardar** en la página **Asignaciones de grupo de entrega** para aplicar la nueva categoría. La nueva categoría se aplicará a la aplicación y aparecerá 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 definir sus datos y configuraciones de directiva. Para obtener información sobre las directivas de aplicaciones que están disponibles para cada tipo de plataforma de dispositivos, consulte:

- [Introducción al SDK de MAM](#)
- [Vista general de las directivas MDX](#)

1. Para las aplicaciones móviles de productividad de Citrix, descargue los archivos MDX de tienda pública; es decir, vaya a <https://www.citrix.com/downloads>. Vaya a **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.
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**. Aparecerá el cuadro de diálogo **Agregar aplicación**.

Add App [Close]

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX Apps wrapped with the MDX Service to include app policies. You can deploy MDX apps obtained from internal and public stores. Example: Secure Mail	Public App Store Free or paid apps available in a public app store, such as iTunes or Google Play, for download. Example: GoToMeeting
Web & SaaS Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps. Example: GoogleApps_SAML	Enterprise Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps. Example: Quick-iLaunch
Web Link A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.	

4. Haga clic en **MDX**. Aparecerá la página **Información de la aplicación MDX**.
5. En el panel **Información de la aplicación**, escriba la información siguiente:
 - **Nombre:** Introduzca un nombre descriptivo para la aplicación. Este nombre figurará en **Nombre de la aplicación**, en la tabla **Aplicaciones**.
 - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
 - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte [Acerca de las categorías de aplicaciones](#).

6. Haga clic en **Siguiente**. Aparecerá la página de las **plataformas de la aplicación**.
7. En **Plataformas**, seleccione las plataformas que quiera agregar. Si solo piensa configurar una plataforma, desmarque las demás.
8. Para seleccionar un archivo MDX para cargarlo, haga clic en **Cargar** y vaya a la ubicación del archivo.
9. En la página **Detalles de la aplicación**, configure lo siguiente:
 - **Nombre de archivo:** Escriba el nombre del archivo asociado a la aplicación.
 - **Descripción de la aplicación:** Escriba una descripción de la aplicación.
 - **Versión de la aplicación:** Si quiere, escriba el número de versión de la aplicación.
 - **ID del paquete:** Escriba el ID del paquete de la aplicación de Google Play Store administrado.
 - **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
 - **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
 - **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
 - **Quitar aplicación si se quita el perfil MDM:** Seleccione si quiere quitar la aplicación de un dispositivo iOS cuando se quite el perfil de MDM. El valor predeterminado es **Activado**.
 - **Impedir copia de seguridad de datos de la aplicación:** Seleccione si impedir que los usuarios realicen copias de seguridad de los datos de la aplicación en dispositivos iOS. El valor predeterminado es **Activado**.
 - **Seguimiento del producto:** Especifique qué tipo de seguimiento de producto quiere enviar a los dispositivos iOS. Si tiene un seguimiento diseñado para prueba, puede seleccionarlo y asignárselo a sus usuarios. El valor predeterminado es **Producción**.
 - **Forzar administración de la aplicación:** Si se instala una aplicación como no administrada, seleccione si solicitar a los usuarios permiso para administrarla en dispositivos iOS no supervisados. El valor predeterminado es **Activado**.
 - **Aplicación implementada mediante las compras por volumen:** Seleccione si quiere implementar la aplicación a través de las compras por volumen de Apple. Si está **activado**, se implementa una versión MDX de la aplicación y se utiliza las compras por volumen para implementar la aplicación, Citrix Secure Hub muestra solo la instancia de compras por volumen. El valor predeterminado es **Desactivado**.
10. Configure las **directivas MDX**. Las directivas MDX varían según la plataforma. Además, estas directivas incluyen opciones para tales áreas de directiva como autenticación, seguridad de los dispositivos y restricciones a aplicaciones. En la consola, se ofrece información descriptiva sobre cada una de las directivas.

11. Configurar las reglas de implementación. Para obtener información, consulte [Configurar las reglas de implementación](#).
12. Expanda **Configuración del almacén**.

The screenshot shows the 'Store Configuration' section. It includes an 'App FAQ' section with a button to 'Add a new FAQ question and answer'. Below this is the 'App screenshots' section, which contains five placeholder boxes, each with a 'Choose File' button. At the bottom, there are two toggle switches: 'Allow app ratings' and 'Allow app comments', both of which are currently turned 'ON'.

Si quiere, puede configurar lo siguiente:

- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

13. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.

The screenshot shows the Citrix Endpoint Management console interface. On the left, a sidebar contains a navigation menu with the following items: 'MDX', '1 App Information', '2 Platform', '3 Approvals (optional)', and '4. Delivery Group Assignments (optional)' (which is highlighted in blue). The main content area is titled 'Delivery Group Assignments (optional)' and includes the instruction 'Assign this app to one or more delivery groups.' Below this, there is a 'Choose delivery groups' section with a search bar and a list of delivery groups. The list includes 'AllUsers' (checked) and 'OA DG for Mac users' (unchecked). To the right of this list is a box titled 'Delivery groups to receive app assignment' which contains the 'AllUsers' group. At the bottom of the main area, there is a link for 'Deployment Schedule'.

14. Junto a **Elegir grupos de entrega**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione un grupo o varios de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.
15. Expanda **Programación de implementación** y, a continuación, configure estos 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:** Seleccione **En cada conexión** para implementar la aplicación cada vez que se conecte el dispositivo. Elija **Solo cuando haya fallado la implementación anterior** para implementar la aplicación cuando el dispositivo no haya recibido previamente la aplicación. El valor predeterminado es **En cada conexión**.

La opción **Implementar para conexiones permanentes** se aplica una vez configurada la clave de implementación en segundo plano para la programación en **Parámetros > Propiedades de servidor**.

La opción permanente:

- No está disponible para dispositivos iOS
- No está disponible para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management a partir de la versión 10.18.19 o una posterior
- No se recomienda para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19

La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Im-**

plementar para conexiones permanentes.

16. Haga clic en **Guardar**.

Agregar una aplicación de la tienda pública de aplicaciones

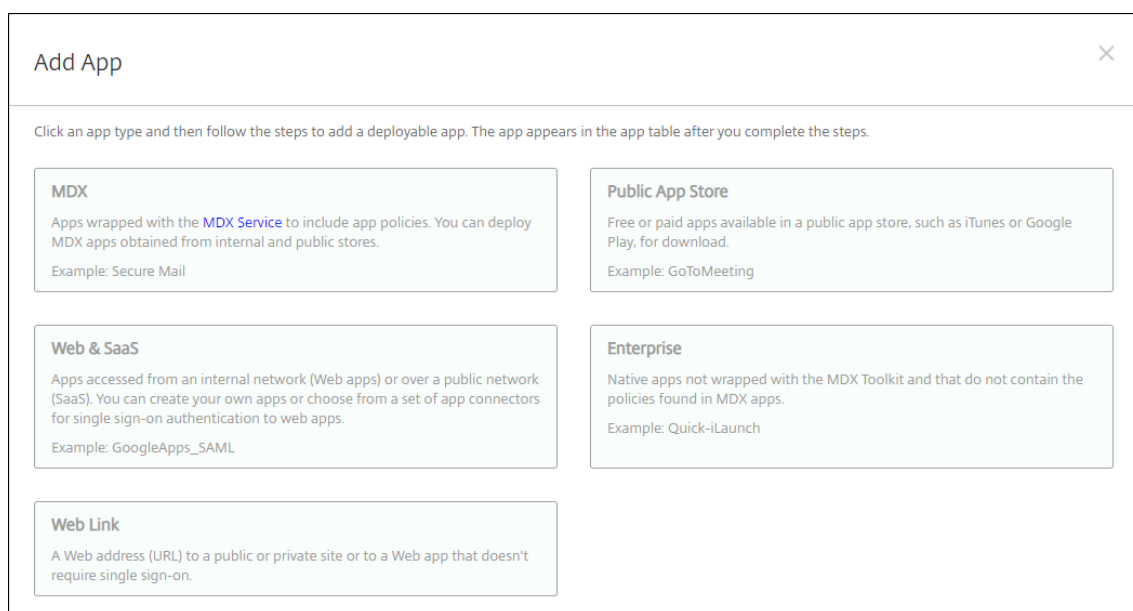
Se pueden agregar a Citrix Endpoint Management tanto aplicaciones gratuitas como de pago, que estén disponibles en una tienda pública de aplicaciones, como el App Store de Apple o Google Play.

Puede configurar ciertos parámetros para obtener los nombres y las descripciones de las aplicaciones desde Apple App Store. Cuando obtiene la información de la aplicación, facilitada desde el almacén, Citrix Endpoint Management sobrescribe el nombre y la descripción existentes. Configure manualmente la información de la aplicación de Google Play Store.

Cuando agrega una aplicación de pago proveniente de una tienda pública a Android Enterprise, puede ver el estado de las licencias de compra en bloque. Ese estado está compuesto por la cantidad total de las licencias disponibles, la cantidad actualmente en uso y la dirección de correo electrónico de cada usuario que consume cada licencia. El plan de compra en bloque de Android Enterprise simplifica el proceso de buscar, comprar y distribuir aplicaciones y otros datos en bloque.

Configure información sobre la aplicación y elija las plataformas en las que entregarla:

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones > Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.



Add App [Close]

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX Apps wrapped with the MDX Service to include app policies. You can deploy MDX apps obtained from internal and public stores. Example: Secure Mail	Public App Store Free or paid apps available in a public app store, such as iTunes or Google Play, for download. Example: GoToMeeting
Web & SaaS Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps. Example: GoogleApps_SAML	Enterprise Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps. Example: Quick-iLaunch
Web Link A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.	

2. Haga clic en **Tienda pública de aplicaciones**. Aparecerá la página **Información de la aplicación**.
3. En el panel **Información de la aplicación**, escriba la información siguiente:

- **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en **Nombre de la aplicación**, en la tabla **Aplicaciones**.
 - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
 - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte [Acerca de las categorías de aplicaciones](#).
4. Haga clic en **Siguiente**. Aparecerá la página de las **plataformas de la aplicación**.
 5. En **Plataformas**, seleccione las plataformas que quiera agregar. Si solo piensa configurar una plataforma, desmarque las demás.

A continuación, configure los parámetros de la aplicación para cada plataforma. Consulte:

- Configurar parámetros de aplicación para aplicaciones de Google Play
- [Aplicaciones administradas de la tienda de aplicaciones](#)
- Configurar parámetros de aplicación para aplicaciones iOS

Cuando termine de configurar los parámetros de una plataforma, defina las reglas de implementación de esa plataforma y los parámetros de tienda de aplicaciones.

1. Configurar las reglas de implementación. Para obtener información, consulte [Configurar las reglas de implementación](#).
2. Expanda **Configuración del almacén**.

The screenshot displays the 'Store Configuration' section. It includes an 'App FAQ' section with a button to 'Add a new FAQ question and answer'. Below this is the 'App screenshots' section, which contains five placeholder boxes, each with a 'Choose File' button. At the bottom, there are two toggle switches: 'Allow app ratings' and 'Allow app comments', both of which are currently turned 'ON'.

Si quiere, puede configurar lo siguiente:

- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

Configurar parámetros de aplicación para aplicaciones de Google Play

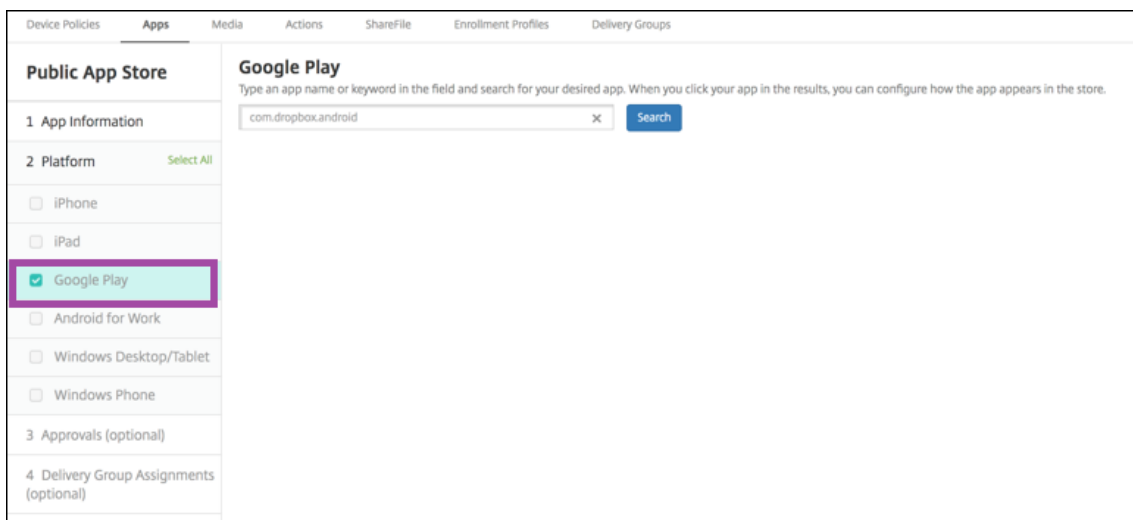
Nota:

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 Google Play Store**. (consulte [Propiedades de servidor](#)). Al establecer esta propiedad en **true**, todos los usuarios de

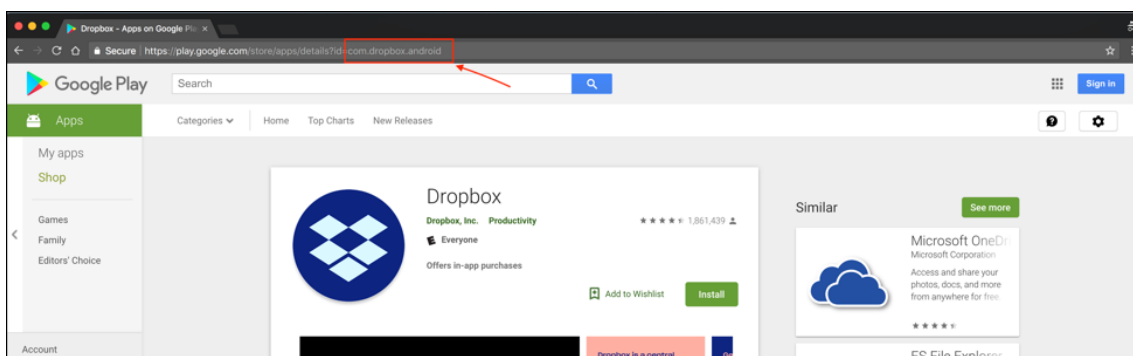
Android Enterprise pueden acceder a aplicaciones de la tienda pública de Google Play. A continuación, puede usar la [directiva Restricciones](#) para controlar el acceso a estas aplicaciones.

La configuración de las aplicaciones de Google Play Store requiere pasos diferentes a los de otras plataformas. Configure manualmente la información de la aplicación de Google Play Store.

1. Compruebe que **Google Play** esté marcado en **Plataformas**.



2. Vaya a Google Play Store. Desde Google Play Store, copie el ID del paquete. El ID está en la URL de la aplicación.



3. Al agregar una aplicación de la tienda pública en la consola de Citrix Endpoint Management, pegue el ID del paquete en la barra de búsqueda. Haga clic en **Search**.

The screenshot shows the 'Public App Store' configuration page. The 'Google Play' tab is active. A search bar at the top right contains the package ID 'com.dropbox.android' and a 'Search' button. The left sidebar has four sections: '1 App Information', '2 Platform' (with 'Google Play' selected), '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'.

4. Si el ID del paquete es válido, aparece una interfaz de usuario que le permite introducir los detalles de la aplicación.

The screenshot shows the 'App Details' configuration page. The 'Google Play' tab is active. The 'App Details' section includes fields for 'Name', 'Description', 'Version', 'Package ID', and 'Image URL'. The 'Image URL' field is highlighted with a green box. The 'Upload Image' button is also visible. The left sidebar shows '1 App Information', '2 Platform' (with 'Google Play' selected), '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'.

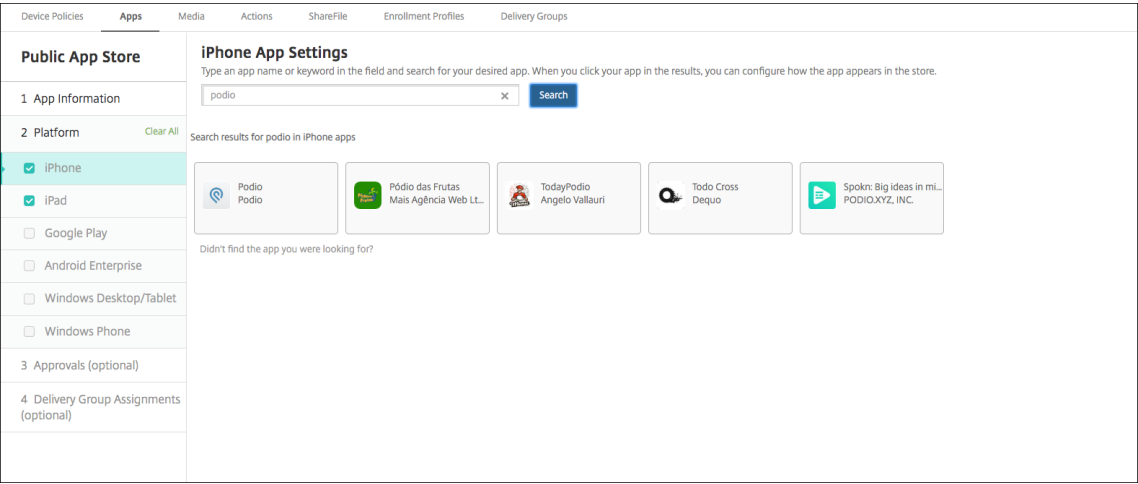
5. Puede configurar la URL de la imagen para que aparezca con la aplicación en el almacén. Para usar la imagen de Google Play Store:
- Vaya a Google Play Store. Haga clic con el botón secundario en la imagen de la aplicación y copie la dirección de la imagen.
 - Pegue la dirección de la imagen en el campo **URL de imagen**.
 - Haga clic en **Cargar imagen**. La imagen aparece junto a **Imagen**.

Si no configura ninguna imagen, aparecerá la imagen genérica de Android con la aplicación.

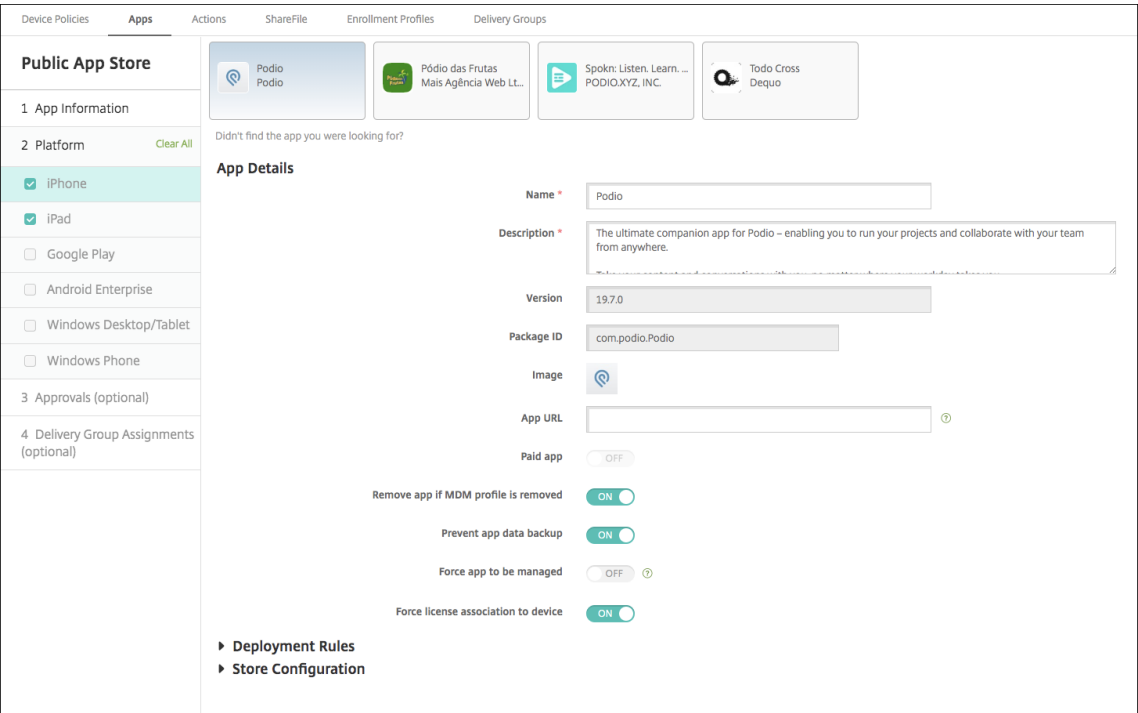
Configurar parámetros de aplicación para aplicaciones iOS

1. Introduzca el nombre de la aplicación en el cuadro de búsqueda y haga clic en **Buscar**. Aparecerán las aplicaciones que coincidan con los criterios de búsqueda. Aparecerán las aplicaciones que coincidan con los criterios de búsqueda.

En la siguiente imagen, se muestran los resultados de la búsqueda **podio** en aplicaciones de un teléfono iPhone.



2. Haga clic en la aplicación que quiera agregar.
3. Los campos **Detalles de la aplicación** aparecen rellenos con información relativa a la aplicación seleccionada (incluido el nombre, la descripción, el número de versión y la imagen asociada).



4. Configure estos parámetros:

- Si fuera necesario, cambie el nombre y la descripción de la aplicación.
- **URL de aplicación:** Introduzca una lista de direcciones URL separadas por comas para iniciar las 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.
- **Quitar aplicación si se quita el perfil MDM:** Seleccione si quiere quitar la aplicación cuando se quite el perfil de MDM. El valor predeterminado es **Activado**.
- **Impedir copia de seguridad de datos de la aplicación:** Seleccione si quiere impedir que la aplicación realice copias de seguridad de los datos. El valor predeterminado es **Activado**.
- **Seguimiento del producto:** Especifique qué tipo de seguimiento de producto quiere enviar a los dispositivos de usuario. Si tiene un seguimiento diseñado para prueba, puede seleccionarlo y asignárselo a sus usuarios. El valor predeterminado es **Producción**.
- **Forzar administración de la aplicación:** Si se instala una aplicación como no administrada, seleccione si solicitar a los usuarios permiso para administrarla 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 pide a los usuarios que permitan la administración de aplicaciones.
- **Forzar asociación de licencia con el dispositivo:** Seleccione si asociar una aplicación (desarrollada con la opción de asociación a un dispositivo habilitada) a un dispositivo en lugar de a un usuario. Si la aplicación que ha elegido no admite la asignación a un dispositivo, este campo no se puede cambiar.

5. Configurar las reglas de implementación. Para obtener información, consulte [Configurar las reglas de implementación](#).

6. Expanda **Configuración del almacén**.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings ☒

Allow app comments ☒

Si quiere, puede configurar lo siguiente:

- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

7. Para iPhone o iPad, expanda **Compras por volumen**.

- a) Si quiere que Citrix Endpoint Management aplique una licencia de compras por volumen a la aplicación, en la lista **Licencia de compras por volumen**, haga clic en **Cargar un archivo de licencias de compras por volumen**.
- b) En el cuadro de diálogo que aparece, importe la licencia.

La tabla “Asignación de licencias” muestra la cantidad de licencias de la aplicación que

están en uso, frente al total de las licencias disponibles.

Puede desvincular las licencias de compras por volumen de un usuario en particular. Si lo hace, finaliza las asignaciones y libera licencias.

- c) Al agregar su cuenta de compras por volumen, habilite **Actualización automática de aplicaciones**. Este parámetro garantiza que las aplicaciones de los dispositivos de usuario se actualicen automáticamente cuando aparece una actualización en el Apple Store. Si una aplicación tiene habilitado el parámetro **Forzar administración de la aplicación**, esta se actualiza sin avisar al usuario. La actualización se produce independientemente de si la aplicación es obligatoria u opcional.
8. Después de completar los parámetros de **Compras por volumen**, haga clic en **Siguiente**. Aparecerá la página **Aprobaciones**.

Para utilizar flujos de trabajo que requieran aprobación antes de permitir que los usuarios accedan a la aplicación, consulte Aplicar flujos de trabajo. Si no necesita flujos de trabajo de aprobación, vaya al siguiente paso.
9. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.
10. Junto a **Elegir grupos de entrega**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione un grupo o varios de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.
11. Expanda **Programación de implementación** y, a continuación, configure estos 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:** Seleccione **En cada conexión** para implementar la aplicación cada vez que se conecte el dispositivo. Elija **Solo cuando haya fallado la implementación anterior** para implementar la aplicación cuando el dispositivo no haya recibido previamente la aplicación. El valor predeterminado es **En cada conexión**.

La opción **Implementar para conexiones permanentes** se aplica una vez configurada la clave de implementación en segundo plano para la programación en **Parámetros > Propiedades de servidor**.

La opción permanente:

- No está disponible para dispositivos iOS
- No está disponible para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management a partir de la versión 10.18.19 o una posterior

- No se recomienda para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19

La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Implementar para conexiones permanentes**.

12. Haga clic en **Guardar**.

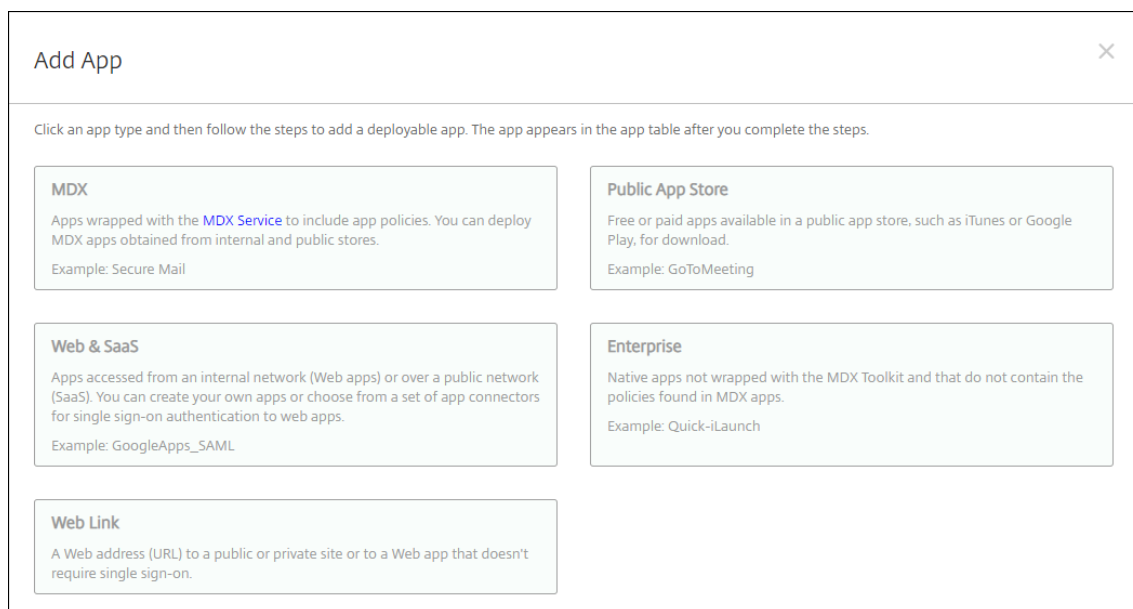
Agregar una aplicación web o SaaS

Con la consola de Citrix Endpoint Management, es posible ofrecer a los usuarios el inicio de sesión único, conocido como Single Sign-On (SSO), para sus aplicaciones de empresa, web y SaaS.

Puede crear su propio conector en Citrix Endpoint Management cuando agrega una aplicación web o una aplicación 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, tras guardar los parámetros anteriores, la aplicación aparece en la ficha **Aplicaciones** de la consola de Citrix Endpoint Management.

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones > Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.

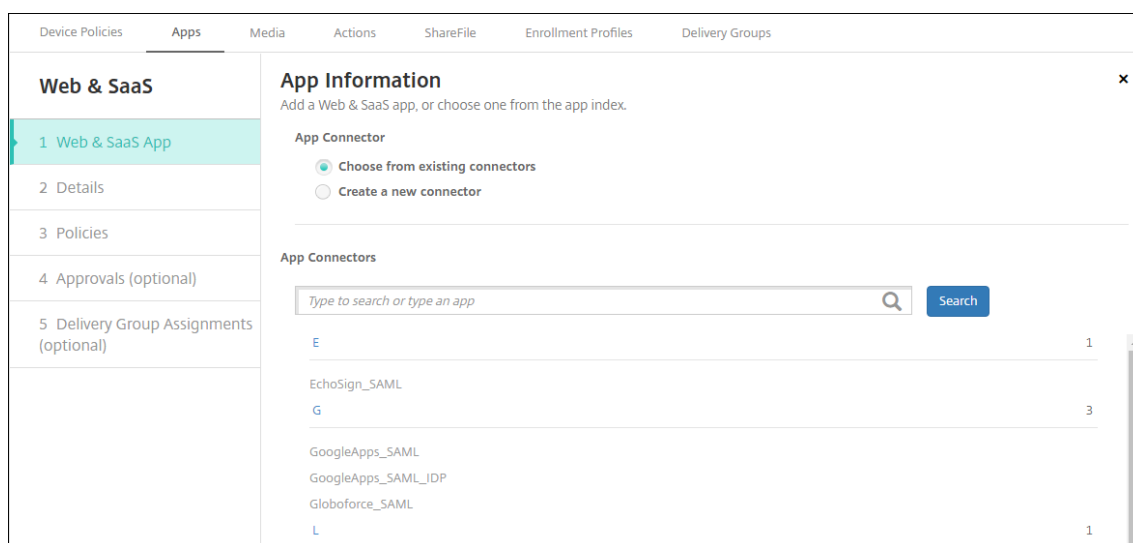


Add App [Close]

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX Apps wrapped with the MDX Service to include app policies. You can deploy MDX apps obtained from internal and public stores. Example: Secure Mail	Public App Store Free or paid apps available in a public app store, such as iTunes or Google Play, for download. Example: GoToMeeting
Web & SaaS Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps. Example: GoogleApps_SAML	Enterprise Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps. Example: Quick-iLaunch
Web Link A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.	

2. Haga clic en **Web y SaaS**. Aparecerá la página **Información de la aplicación**.



3. Configure un conector de aplicación nuevo o existente, como se muestra a continuación.

Para configurar un conector de aplicación existente

1. En la página **Información de la aplicación**, la opción **Elegir entre los conectores existentes** ya está seleccionada, como se muestra anteriormente. En la lista **Conectores de aplicación**, haga clic en el conector que quiera usar. Aparecerá la información del conector de aplicación.
2. Configure estos parámetros:
 - **Nombre de la aplicación:** Acepte el nombre que ya aparece o escriba uno nuevo.
 - **Descripción de la aplicación:** Acepte la descripción que ya aparece o escriba una propia.
 - **URL:** Acepte la URL que ya aparece o escriba la dirección web de la aplicación. Según el conector que elija, este campo puede tener un marcador de posición que se debe reemplazar antes de pasar a la siguiente página.
 - **Nombre de dominio:** Si corresponde, escriba el nombre de dominio de la aplicación. Este campo es obligatorio.
 - **Aplicación alojada en la red interna:** Seleccione si la aplicación se ejecuta en un servidor de la red interna. Si los usuarios se conectan desde una ubicación remota a la aplicación interna, deben hacerlo a través de NetScaler Gateway. Si **activa** esta opción, se agrega 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:** En la lista, si quiere, haga clic en una categoría que se va a aplicar a la aplicación.
 - **Aprovisionamiento de cuentas de usuario:** Seleccione si quiere crear cuentas de usuario para la aplicación. Si usa el conector Globoforce_SAML, debe habilitar esta opción para ofrecer una integración correcta de SSO.

- Si habilita **Aprovisionamiento de cuentas de usuario**, configure los siguientes parámetros:
 - **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 finalizan los derechos del usuario:** En la lista desplegable, haga clic en la acción que se debe realizar cuando los usuarios ya no pueden acceder a la aplicación. La opción predeterminada es **Inhabilitar la cuenta**.
 - **Regla de nombre de usuario**
 - * Para agregar cada regla de nombre de usuario, haga lo siguiente:
 - **Atributos del usuario:** En la lista desplegable, haga clic en el atributo de usuario que quiere agregar a la regla.
 - **Longitud (caracteres):** En la lista desplegable, haga clic en la cantidad de caracteres del atributo de usuario que se usarán en la regla de nombre de usuario. El valor predeterminado es **Todo**.
 - **Regla:** Cada atributo de usuario que agregue se adjunta 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 contraseña**
 - **Validez (días):** Escriba la cantidad de días durante los que la contraseña será válida. Cualquier valor entre **0 y 90** es válido. El valor predeterminado es 90.
 - **Restablecer automáticamente la contraseña cuando caduque:** Seleccione si quiere restablecer la contraseña automáticamente cuando esta caduque. El valor predeterminado es **Desactivado**. Si no habilita este campo, los usuarios no pueden abrir la aplicación después de que caduquen sus contraseñas.

Para configurar un nuevo conector de aplicaciones

1. En la página **Información de la aplicación**, seleccione **Crear un nuevo conector**. Aparecerán los campos de información del conector de aplicaciones.

The screenshot shows the 'App Information' form in the Citrix Endpoint Management console. The left sidebar is titled 'Web & SaaS' and contains a list of steps: 1 Web & SaaS App (highlighted), 2 Details, 3 Policies, 4 Approvals (optional), and 5 Delivery Group Assignments (optional). The main form area is titled 'App Information' with a subtitle 'Add a Web & SaaS app, or choose one from the app index.' and a close button (X). The form contains the following fields and options:

- App Connector:** Radio buttons for 'Choose from existing connectors' and 'Create a new connector' (selected).
- Name ***: A text input field.
- Description ***: A text input field.
- Logon URL ***: A text input field.
- SAML version:** Radio buttons for '1.1' (selected) and '2.0'.
- Entity ID ***: A text input field.
- Relay state URL**: A text input field.
- Name ID format:** Radio buttons for 'Email Address' (selected) and 'Unspecified'.
- ACS URL ***: A text input field.
- Image:** Radio buttons for 'Use default' (selected) and 'Upload your own app image'.
- Add:** A green button at the bottom.

2. Configure estos parámetros:

- **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, que puede ser <https://www.example.com/login>. Este campo es obligatorio.
- **Versión 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 del relé:** Escriba la dirección web de la aplicación SAML. Esta es la URL de respuesta de la aplicación.
- **Formato de ID de nombre:** Seleccione **Correo electrónico** o **No especificado**. El valor predeterminado es **Correo electrónico**.
- **URL de ACS:** Escriba la URL del servicio de aserción de consumidor (ACS) del proveedor de identidades o de servicios. La URL del servicio ACS proporciona a los usuarios Single Sign-On (SSO).
- **Imagen:** Seleccione si usar la imagen predeterminada de Citrix o cargar su propia imagen de la aplicación. El valor predeterminado es "Usar predeterminada".
 - Si quiere cargar su propia imagen, haga clic en **Examinar**, vaya a la ubicación del archivo y selecciónelo. El archivo debe ser PNG. No se puede cargar archivos JPEG o GIF. Cuando se agrega un gráfico personalizado, no se puede modificar más tarde.

3. Cuando haya terminado, haga clic en **Agregar**. Aparecerá la página **Detalles**.
4. Haga clic en **Siguiente**. Aparecerá la página **Directiva de aplicación**.

The screenshot shows the 'App Policy' configuration page in Citrix Endpoint Management. The left sidebar has a navigation menu with the following items: 'Web & SaaS', '1 Web & SaaS App', '2 Details', '3 Policies' (highlighted), '4 Approvals (optional)', and '5 Delivery Group Assignments (optional)'. The main content area is titled 'App Policy' and includes a sub-header 'Fill in app information'. Below this, there are three sections: 'Device Security' with a toggle for 'Block jailbroken or rooted' set to 'ON'; 'Network Requirements' with toggles for 'WiFi required' and 'Internal network required' both set to 'OFF'; and 'Internal WiFi networks' with an empty text input field. At the bottom of the main area is a section for 'Store Configuration'. The bottom right of the page has 'Back' and 'Next >' buttons.

5. Configure estos parámetros:

- **Seguridad del dispositivo**
- **Bloquear si está liberado por jailbreak o rooting:** Seleccione si impedir que los dispositivos liberados por jailbreak o por rooting accedan a la aplicación. De forma predeterminada, está **activado**.
- **Requisitos de la red**
- **Se requiere Wi-Fi:** Seleccione si se necesita una conexión Wi-Fi para ejecutar la aplicación. De forma predeterminada está **desactivado**.
- **Se requiere red interna:** Seleccione si se necesita una red interna para ejecutar la aplicación. De forma predeterminada está **desactivado**.
- **Redes Wi-Fi internas:** Si habilitó la opción **Se requiere Wi-Fi**, escriba la red inalámbrica interna que se va a usar.

6. Expanda **Configuración del almacén**.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings ☒ ON

Allow app comments ☒ ON

Si quiere, puede configurar lo siguiente:

- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

7. Haga clic en **Siguiente**. Aparecerá la página **Aprobaciones**.

The screenshot displays the 'Approvals (optional)' configuration screen in Citrix Endpoint Management. The top navigation bar includes tabs for Device Policies, Apps, Media, Actions, ShareFile, Enrollment Profiles, and Delivery Groups. The left sidebar lists the setup steps: 1 Web & SaaS App, 2 Details, 3 Policies, 4 Approvals (optional) (highlighted), and 5 Delivery Group Assignments (optional). The main content area is titled 'Approvals (optional)' with a close button (X). Below the title is a description: 'Apply an existing workflow or create a new workflow to require approval before allowing users to access the app.' A 'Workflow to Use' dropdown menu is set to 'None'. At the bottom right, there are 'Back' and 'Next >' buttons.

Para utilizar flujos de trabajo que requieran aprobación antes de permitir que los usuarios accedan a la aplicación, consulte Aplicar flujos de trabajo. Si no necesita flujos de trabajo de aprobación, vaya al siguiente paso.

8. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.
9. Junto a **Elegir grupos de entrega**, escriba para buscar un grupo de entrega o seleccione un grupo o varios. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.
10. Expanda **Programación de implementación** y, a continuación, configure estos 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:** Seleccione **En cada conexión** para implementar la aplicación cada vez que se conecte el dispositivo. Elija **Solo cuando haya fallado la implementación anterior** para implementar la aplicación cuando el dispositivo no haya recibido previamente la aplicación. El valor predeterminado es **En cada conexión**.

La opción **Implementar para conexiones permanentes** se aplica una vez configurada la clave de implementación en segundo plano para la programación en **Parámetros > Propiedades de servidor**.

La opción permanente:

- No está disponible para dispositivos iOS
- No está disponible para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management a partir de la versión 10.18.19 o una posterior

- No se recomienda para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19

La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Implementar para conexiones permanentes**.

11. Haga clic en **Guardar**.

Agregar una aplicación de empresa

En Citrix Endpoint Management, las aplicaciones de empresa son aplicaciones privadas que se desarrollan u obtienen de otra fuente. A excepción de las aplicaciones privadas de Android Enterprise entregadas como aplicaciones habilitadas para MDX, las aplicaciones de empresa no están preparadas con el SDK de MAM o el MDX Toolkit. Puede cargar una aplicación de empresa en la ficha **Aplicaciones** de la consola de Citrix Endpoint Management. Las aplicaciones de empresa admiten las siguientes plataformas (y sus tipos de archivo correspondientes):

- iOS (archivo IPA)
- macOS (archivo PKG)

Citrix Endpoint Management no limita el tamaño de los archivos PKG que cargue, pero sí limita los tiempos de carga de archivos. De forma predeterminada, debe completar la carga en un plazo de 100 segundos. Para obtener información, consulte [Propiedades de servidor](#).

- Android (archivo APK)
- Android Enterprise (archivo APK)
- Consulte también Agregar aplicaciones Win32 como aplicaciones de empresa.
- Consulte también [Aplicaciones privadas habilitadas para MDX](#).

No se admite la opción de agregar aplicaciones descargadas desde Google Play como aplicaciones de empresa. En vez de ello, agregue las aplicaciones de Google Play Store como aplicaciones provenientes del tienda pública de aplicaciones. Consulte Agregar una aplicación de la tienda pública de aplicaciones.

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones > Agregar**. Aparecerá el cuadro de diálogo **Agregar aplicación**.

Add App

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the [MDX Service](#) to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: Secure Mail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

Web Link

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

2. Haga clic en **Empresa**. Aparecerá la página **Información de la aplicación**.
3. En el panel **Información de la aplicación**, escriba la información siguiente:
 - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en “Nombre de la aplicación”, en la tabla “Aplicaciones”.
 - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
 - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.
4. Haga clic en **Siguiente**. Aparecerá la página de las **plataformas de la aplicación**.
5. En **Plataformas**, seleccione las plataformas que quiera agregar. Si solo piensa configurar una plataforma, desmarque las demás.
6. Elija un archivo que cargar correspondiente a la plataforma seleccionada. Para ello, haga clic en **Cargar** y vaya a la ubicación del archivo.
7. Haga clic en **Siguiente**. Aparecerá la página de información referente a la aplicación para la plataforma pertinente.
8. Configure los parámetros para el tipo de plataforma, como:
 - **Nombre de archivo:** Si quiere, escriba un nuevo nombre para la aplicación.
 - **Descripción de la aplicación:** Si quiere, indique una nueva descripción de la aplicación.
 - **Versión de la aplicación:** Este campo no se puede cambiar.
 - **Versión mínima de SO:** Si quiere, escriba la versión más antigua del sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

990

- **Versión máxima de SO:** Si quiere, escriba la versión más reciente del sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
 - **Dispositivos excluidos:** Si quiere, escriba el fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
 - **ID del paquete:** Identificador único de la aplicación.
 - **Quitar aplicación si se quita el perfil MDM:** Seleccione si quiere quitar la aplicación de un dispositivo cuando se quite el perfil de MDM. El valor predeterminado es **Activado**. Esta configuración no se aplica a macOS.
 - **Impedir copia de seguridad de datos de la aplicación:** Seleccione si quiere impedir que la aplicación realice copias 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 instalar una aplicación como administrada en dispositivos no supervisados. El tipo de dispositivo determina cómo procesa Citrix Endpoint Management esta opción cuando se habilita. Si habilita esta configuración, la aplicación se actualizará sin solicitárselo al usuario. La actualización se produce independientemente de si la aplicación es obligatoria u opcional. El valor predeterminado es **Desactivado**.
 - En los dispositivos iOS, si la aplicación ya estaba instalada, los usuarios recibirán un mensaje para permitir que la aplicación se administre. Si implementa una aplicación en dispositivos donde la aplicación no existe, esta se instala como aplicación administrada, independientemente del estado de esta opción. 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 pide a los usuarios que permitan la administración de aplicaciones.
 - Para los dispositivos macOS, habilite la opción y, a continuación, implemente la aplicación en los dispositivos. La aplicación se instala automáticamente como aplicación administrada y los usuarios no reciben ningún mensaje. Si implementa una aplicación en dispositivos donde la aplicación no existe, esta se instala como aplicación administrada, independientemente del estado de esta opción. Disponible en macOS 11.0 y versiones posteriores.
9. Configurar las reglas de implementación. Para obtener información, consulte [Configurar las reglas de implementación](#).
10. Expanda **Configuración del almacén**.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings ☒

Allow app comments ☒

Si quiere, puede configurar lo siguiente:

- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

11. Haga clic en **Siguiente**. Aparecerá la página **Aprobaciones**.

Para utilizar flujos de trabajo que requieran aprobación antes de permitir que los usuarios accedan a la aplicación, consulte Aplicar flujos de trabajo. Si no necesita flujos de trabajo de aprobación, vaya al siguiente paso.

12. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.
13. Junto a **Elegir grupos de entrega**, escriba el nombre de un grupo de entrega para buscarlo, o

bien seleccione un grupo o varios de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.

14. Expanda **Programación de implementación** y, a continuación, configure estos 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:** Seleccione **En cada conexión** para implementar la aplicación cada vez que se conecte el dispositivo. Elija **Solo cuando haya fallado la implementación anterior** para implementar la aplicación cuando el dispositivo no haya recibido previamente la aplicación. El valor predeterminado es **En cada conexión**.

La opción **Implementar para conexiones permanentes** se aplica una vez configurada la clave de implementación en segundo plano para la programación en **Parámetros > Propiedades de servidor**.

La opción permanente:

- No está disponible para dispositivos iOS
- No está disponible para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management a partir de la versión 10.18.19 o una posterior
- No se recomienda para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19

La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Implementar para conexiones permanentes**.

15. Haga clic en **Guardar**.

Agregar aplicaciones Win32 como aplicaciones de empresa

Puede cargar archivos MSI, APPX, AppxBundle, PS1 o EXE en Citrix Endpoint Management para implementar aplicaciones Win32 en dispositivos administrados de escritorios y tabletas con Windows 10 o Windows 11. Después de usar Citrix Endpoint Management para implementar los archivos, el dispositivo Windows instala la aplicación como se muestra a continuación:

- Si la aplicación actualizada quita la versión antigua durante la instalación, el dispositivo solo contiene la aplicación con la versión actualizada.

- Si la aplicación actualizada no puede quitar la versión anterior, pero se puede instalar la nueva versión, el dispositivo incluye ambas versiones de la aplicación. Sin embargo, Citrix Endpoint Management ya no tiene la información referente a la versión anterior.
- Si la aplicación actualizada no se puede instalar cuando existe una versión anterior, no se instala la aplicación nueva. En ese caso, debe implementar la directiva de desinstalación de aplicaciones para quitar la versión anterior. A continuación, puede implementar la nueva versión.

Requisitos

- Windows 10 (versión 1607 o una 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 tipo de implementación, Microsoft no admite archivos MSI con más de una aplicación, archivos MSI anidados ni una instalación interactiva.

Buscar metadatos Cuando agregue una aplicación Win32 a Citrix Endpoint Management, especifique los metadatos de esa aplicación. Para buscar estos metadatos, use la aplicación Orca en un equipo Windows y tome nota de la información siguiente:

- Código del producto
- Nombre del producto
- Versión del producto
- Tipo de instalación del paquete, ya sea por usuario o por máquina

Agregar 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. Deje sin marcar las casillas de todas las plataformas salvo **Escritorio o tableta Windows**.
3. En la página **Aplicación de empresa de escritorio o tableta Windows**, haga clic en **Cargar** y vaya al archivo.
4. Configure estos parámetros:

Windows Desktop/Tablet Enterprise App ✕

Use an MSI viewing tool, such as Orca, to obtain information such as product code and version. You must assign MSI apps to delivery groups as required apps.

Upload an .appx or .appxbundle or .msi file Upload

App name *

Description *

App version *

Minimum OS version

Maximum OS version

Excluded devices

Product Code * ?

Installation Context Device ?

- **Nombre de la aplicación:** El nombre extraído de los metadatos de la aplicación.
- **Descripción:** Una descripción de la aplicación.
- **Versión de la aplicación:** El número de versión extraído de los metadatos de la aplicación.
- **Versión mínima de SO:** Opcional. La versión más antigua de sistema operativo que se puede ejecutar en el dispositivo para utilizar la aplicación.
- **Versión máxima de SO:** Opcional. La versión más reciente de sistema operativo que debe ejecutar el dispositivo para utilizar la aplicación.
- **Dispositivos excluidos:** Opcional. El fabricante o los modelos de los dispositivos en los que no se puede ejecutar la aplicación.
- **Código de producto:** El código de producto de la aplicación MSI, en formato UUID, extraído de los metadatos de la aplicación.
- **Contexto de instalación:** En función de los metadatos de la aplicación, seleccione si quiere instalar la aplicación para el usuario o el dispositivo. Esta configuración no está disponible para archivos EXE.
- **Línea de comandos:** Las opciones de línea de comandos a usar cuando se llama a MSISEXEC.exe
- **Instalar línea de comandos:** Agregar argumentos de línea de comandos para instalar silenciosamente los archivos EXE.
- **Desinstalar línea de comandos:** Agregar argumentos de línea de comandos para desinstalar archivos EXE silenciosamente.
- **Recuento de reintentos:** La cantidad de veces que puede volver a intentar la operación de descargar e instalar antes de que la instalación se marque como fallida.
- **Tiempo de espera:** La cantidad de minutos que se ejecuta el proceso de instalación antes

de que el instalador lo interprete como fallido y deje de supervisar el proceso.

- **Intervalo de reintentos:** La cantidad de minutos que transcurren entre las operaciones de nuevos intentos.

5. Configurar las reglas de implementación. Para obtener información, consulte [Configurar las reglas de implementación](#).

6. Expanda **Configuración del almacén**.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings ☒ ON

Allow app comments ☒ ON

Si quiere, puede configurar lo siguiente:

- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite 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 aplicación obligatoria.
9. Después de implementarla, indique a los usuarios que la aplicación está disponible.

Actualizar la versión de una aplicación Win32

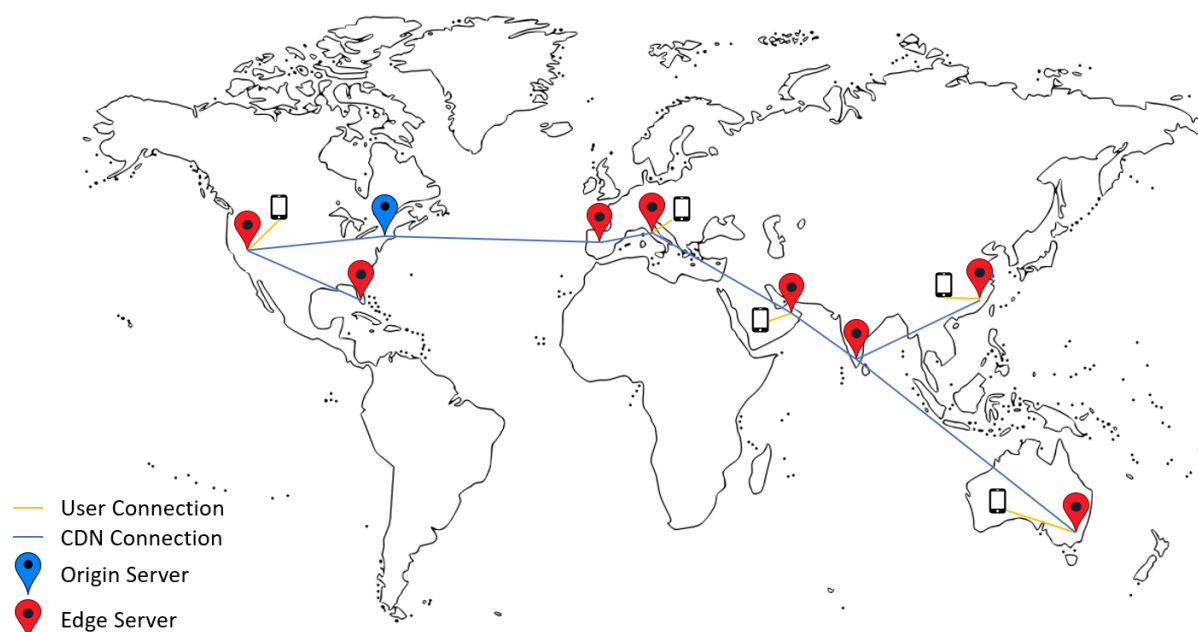
1. Busque los metadatos de la aplicación como se ha descrito anteriormente en “Buscar metadatos”.
2. Vaya a **Configurar > Aplicaciones** para cargar la nueva versión de la aplicación. Actualice la **Versión de la aplicación**. Si la nueva versión de la aplicación tiene otro **Código de producto**, actualice ese parámetro.
3. Envíe los cambios e implemente la aplicación.

Entregar aplicaciones de empresa y MDX desde la CDN de Citrix

Puede entregar aplicaciones de empresa y MDX desde la red de entrega de contenido (CDN) de Citrix Content Delivery. Una CDN hace referencia a un grupo de servidores distribuidos geográficamente que funcionan de manera coordinada para ofrecer una entrega rápida y segura del contenido de las aplicaciones. Un servidor local entrega las aplicaciones a los dispositivos móviles.

Una CDN mejora los tiempos de descarga de aplicaciones porque distribuye contenido más cerca (geográficamente) de los dispositivos móviles a través de un punto de distribución de la red CDN. CDN entrega aplicaciones desde la ubicación del punto de presencia (POP) más cercana a un usuario.

En el siguiente diagrama, se muestra un ejemplo de cómo la red CDN distribuye aplicaciones al servidor perimetral más cercano de los usuarios de dispositivos móviles. Un servidor perimetral almacena en caché contenido sobre el servidor de origen cuando los dispositivos móviles solicitan aplicaciones.



Los usuarios se pueden conectar a las aplicaciones mediante Citrix Secure Hub. Al agregar una aplicación, Citrix Endpoint Management crea el conector de aplicación correspondiente.

La compatibilidad con la CDN de Citrix para aplicaciones de empresa está disponible para las siguientes plataformas:

- iOS (inscripción en MDM o MAM)
- Android (inscripción en MDM o MAM)
- Escritorio o tableta Windows (inscripción en MDM)
- macOS (inscripción en MDM)

La compatibilidad con la CDN de Citrix para aplicaciones MDX está disponible para las siguientes plataformas:

- iOS (inscripción en MDM o MAM)
- Android (inscripción en MDM o MAM)

Cómo funciona CDN

En un servicio CDN, los servidores están vinculados entre sí con el objetivo de entregar más rápido las aplicaciones. Para lograr este objetivo, las aplicaciones se colocan de forma segura en diferentes puntos de distribución por todo el mundo. El servidor DNS de los dispositivos móviles que se utiliza 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 proviene de Fort Lauderdale, Florida. La CDN utiliza el punto de distribución local más cercano a esa ubicación para entregar la aplicación al dispositivo móvil. Gracias al uso de la CDN, se obtiene un mejor tiempo de descarga de la aplicación.

Cuando un dispositivo móvil solicita o envía por primera vez una aplicación de empresa, Citrix Endpoint Management copia la aplicación en el punto de distribución local y la conserva allí durante 24 horas para otras descargas de dispositivos locales.

Entregar aplicaciones de empresa desde la CDN de Citrix

Con la versión 19.4.1 de Citrix Endpoint Management, la entrega de aplicaciones de empresa es la entrega de CDN para todos los nuevos clientes multiarrendatario. Para clientes existentes anteriores a esta versión, siga las instrucciones de esta sección.

Para las aplicaciones de empresa que ya están en el servidor de Citrix Endpoint Management, Citrix Endpoint Management seguirá entregándolas desde el servidor hasta que se vuelvan a cargar después de completar los pasos siguientes.

Importante:

Solo los administradores de Citrix Cloud pueden habilitar CDN para una cuenta. La propiedad del 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 la cuenta. Para ello, en la consola de Citrix Endpoint Management, vaya a **Parámetros > Propiedades de servidor**.
- 2. Busque `app.delivery.cdn` y, a continuación, haga clic en **Modificar**.
- 3. Cambie el valor a **true**.

Key	app.delivery.cdn
Value *	true
Display name *	Application Delivery to enable CDN
Description	Application Delivery to enable CDN

4. En la consola de Citrix Endpoint Management, vuelva a cargar las aplicaciones de empresa:
- a) Vaya a **Configurar > Aplicaciones** y filtre la lista de aplicaciones por **Tipo (Empresa)** y **Plataforma**.
 - b) Seleccione una aplicación, haga clic en **Modificar > Siguiente > Cargar**.
 - c) Repita el paso anterior para cada aplicación de empresa.

Entregar aplicaciones MDX desde la CDN de Citrix

Con la versión 20.12.0 de Citrix Endpoint Management, la entrega de aplicaciones MDX es, de forma predeterminada, la entrega de CDN para todos los nuevos clientes multitarrentario. Para clientes existentes anteriores a 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 seguirá entregándolas desde el servidor hasta que se vuelvan a cargar después de completar los pasos siguientes.

Importante:

Solo los administradores de Citrix Cloud pueden habilitar CDN para una cuenta. La propiedad del 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 la cuenta. Para ello, en la consola de Citrix Endpoint Management, vaya a **Parámetros > Propiedades de servidor**.
2. Busque `app.delivery.cdn` y, a continuación, haga clic en **Modificar**.
3. Cambie el valor a **true**.

Key	app.delivery.cdn
Value *	true
Display name *	Application Delivery to enable CDN
Description	Application Delivery to enable CDN

4. En la consola de Citrix Endpoint Management, vuelva a cargar las aplicaciones MDX:

- a) Vaya a **Configurar > Aplicaciones** y filtre la lista de aplicaciones por **Tipo (MDX)** y **Plataforma**.
- b) Seleccione una aplicación, haga clic en **Modificar > Siguiente > 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 de intranet. Un enlace web también puede apuntar a una aplicación web que no requiere autenticación SSO. Una vez configurado el enlace web, este aparece como un icono en el almacén de aplicaciones. Cuando los usuarios inician sesión en Citrix Secure Hub, el enlace aparece con la lista de aplicaciones y escritorios disponibles.

Puede configurar enlaces web desde la ficha **Apps** de la consola de Citrix Endpoint Management. Una vez configurado el enlace web, aparece como un icono de enlace en la lista de la tabla **Aplicaciones**. Cuando los usuarios inician sesión en Citrix Secure Hub, el enlace aparece con la lista de aplicaciones y escritorios disponibles.

Vea este vídeo para obtener más información:

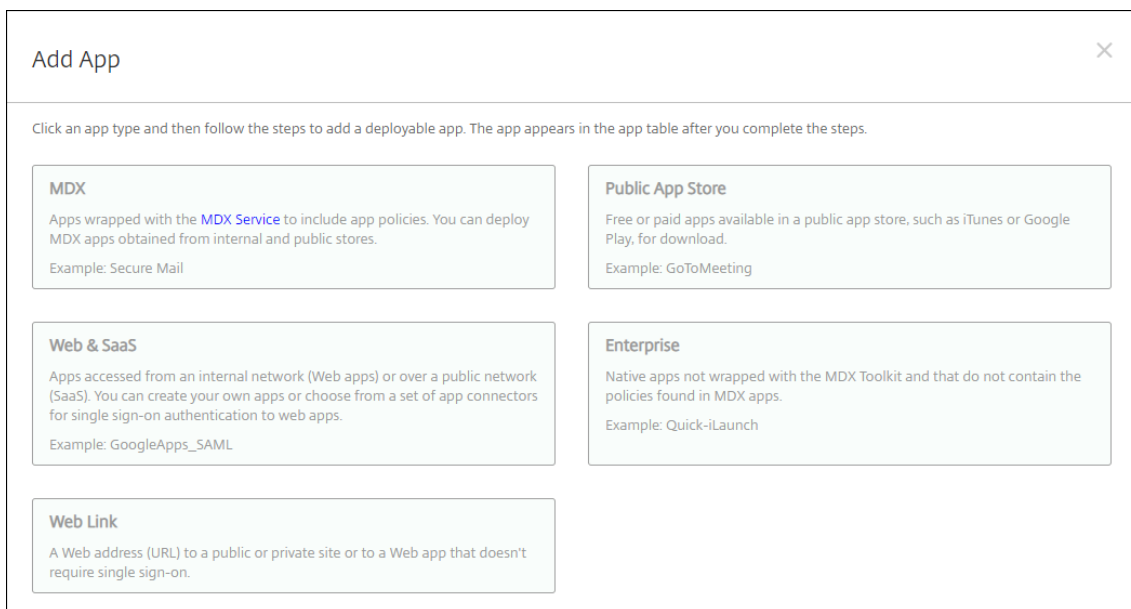


Para agregar el enlace, debe proporcionar la siguiente información:

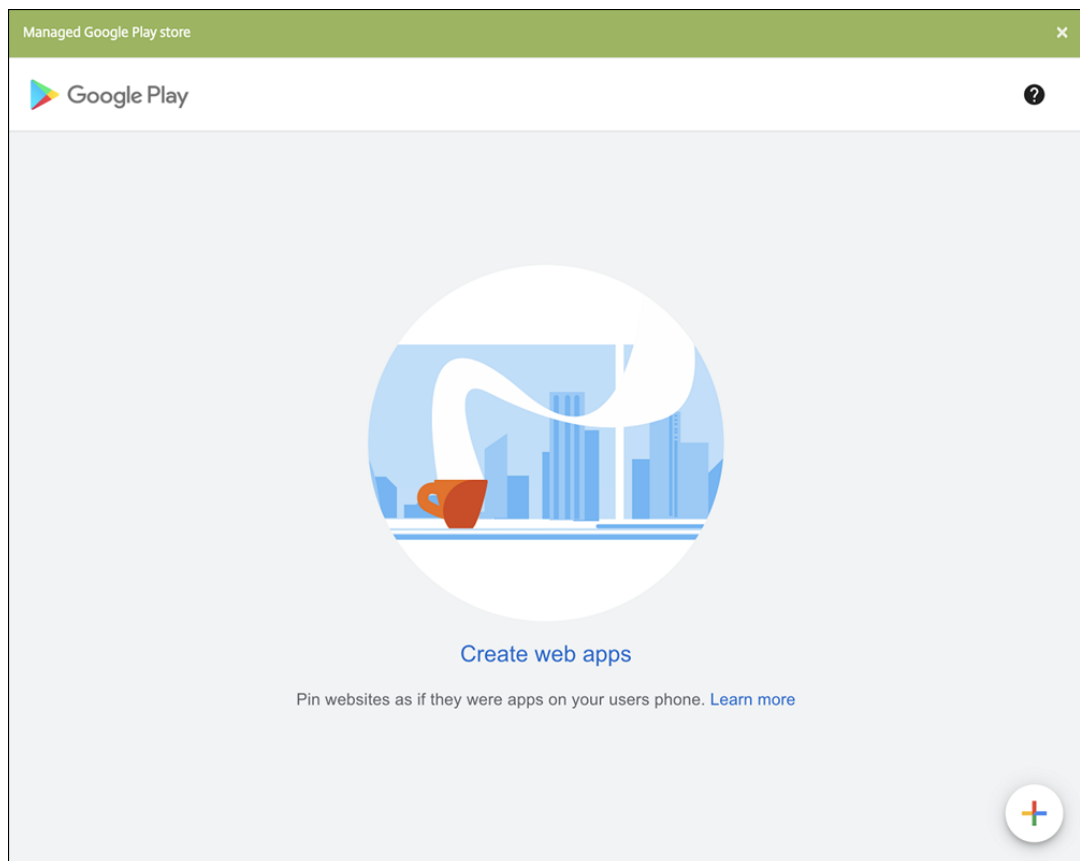
- Nombre del enlace
- Descripción del enlace
- Dirección web (URL)
- Categoría

- Rol
- Imagen en formato PNG (optativo)

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 **Enlace web**. Aparecerá la página **Información de la aplicación**.
3. En el panel **Información de la aplicación**, escriba la información siguiente:
 - **Nombre:** Escriba un nombre descriptivo para la aplicación. Este nombre figurará en "Nombre de la aplicación", en la tabla "Aplicaciones".
 - **Descripción:** Escriba, si quiere, una descripción de la aplicación.
 - **Categoría de la aplicación:** En la lista, puede hacer clic en la categoría a la que se agregará la aplicación. Para obtener más información acerca de las categorías de aplicaciones, consulte Acerca de las categorías de aplicaciones.
4. Haga clic en **Siguiente**. Aparecerá la página de las **plataformas de la aplicación**.
5. En **Plataformas**, seleccione **Otras plataformas** para agregar una aplicación web para iOS, Android (AD heredado) y Windows 8 o seleccione **Android Enterprise**. Desmarque la casilla de las plataformas que no quiera incluir.
 - Si selecciona **Otras plataformas**, vaya al siguiente paso para configurar los parámetros.
 - Si selecciona **Android Enterprise**, haga clic en el botón **Cargar** para abrir Google Play Store administrado. No es necesario registrarse con una cuenta de desarrollador para publicar una aplicación web. Haga clic en el icono **Más** situado en la esquina inferior derecha para continuar.



Configure estos parámetros:

- **Título:** Escriba el nombre de la aplicación web.
- **URL:** Indique la dirección web de la aplicación.
- **Pantalla:** Indique cómo mostrar la aplicación web en los dispositivos de usuario. Las opciones disponibles son: **Pantalla completa**, **Independiente** e **Interfaz de usuario mínima**.
- **Icono:** Cargue su propia imagen para la aplicación web.

Managed Google Play store

Google Play

← New web app

Title *

URL * https://

Display

☒ Full screen
 ☐ Standalone
 ☐ Minimal UI

Web app will use the entire screen
 Web app shows the phone's navigation and status bars
 Web app shows the phone's navigation and status bars, the URL bar, and the Refresh button

Icon

Upload icon

Icons should be 512px square, png or jpeg. Your app title and image must follow the Google Play Developer Program Policies.

Cuando haya terminado, haga clic en **Crear**. La aplicación web puede tardar hasta 10 minutos en publicarse.

6. Para plataformas que no sean Android Enterprise, configure estas opciones:

- **Nombre de la aplicación:** Acepte el nombre que ya aparece o escriba uno nuevo.
- **Descripción de la aplicación:** Acepte la descripción que ya aparece o escriba una propia.
- **URL:** Acepte la URL que ya aparece o escriba la dirección web de la aplicación. Según el conector que elija, este campo puede tener un marcador de posición que se debe reemplazar antes de pasar a la siguiente página.
- **Aplicación alojada en la red interna:** Seleccione si la aplicación se ejecuta en un servidor de la red interna. Si los usuarios se conectan desde una ubicación remota a la aplicación interna, deben hacerlo a través de NetScaler Gateway. Si **activa** esta opción, se agrega 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:** En la lista, si quiere, haga clic en una categoría que se va a aplicar a la aplicación.
- **Imagen:** Seleccione si usar la imagen predeterminada de Citrix o cargar su propia imagen de la aplicación. El valor predeterminado es “Usar predeterminada”.
 - Si quiere cargar su propia imagen, haga clic en **Examinar**, vaya a la ubicación del

archivo y selecciónelo. El archivo debe ser PNG. No se puede cargar archivos JPEG o GIF. Cuando se agrega un gráfico personalizado, no se puede modificar más tarde.

7. Configurar las reglas de implementación. Para obtener información, consulte [Configurar las reglas de implementación](#).
8. Expanda **Configuración del almacén**.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings ☒

Allow app comments ☒

Si quiere, puede configurar lo siguiente:

- **Preguntas frecuentes sobre aplicaciones:** Haga clic en **Agregar nueva pregunta y respuesta** para crear una pregunta frecuente para la aplicación.
- **Agregar capturas de pantalla para teléfonos/tabletas:** Agrega capturas de pantalla que aparecen en la tienda de aplicaciones.
- **Permitir puntuación de aplicaciones:** Permite a los usuarios calificar la aplicación en la tienda de aplicaciones.
- **Permitir comentarios de aplicaciones:** Permite a los usuarios dejar comentarios sobre la aplicación en la tienda de aplicaciones.

9. Haga clic en **Siguiente**. Aparecerá la página **Asignación de grupos de entrega**.

10. Junto a **Elegir grupos de entrega**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione un grupo o varios de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.
11. Expanda **Programación de implementación** y, a continuación, configure estos 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:** Seleccione **En cada conexión** para implementar la aplicación cada vez que se conecte el dispositivo. Elija **Solo cuando haya fallado la implementación anterior** para implementar la aplicación cuando el dispositivo no haya recibido previamente la aplicación. El valor predeterminado es **En cada conexión**.

La opción **Implementar para conexiones permanentes** se aplica una vez configurada la clave de implementación en segundo plano para la programación en **Parámetros > Propiedades de servidor**.

La opción permanente:

- No está disponible para dispositivos iOS
- No está disponible para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management a partir de la versión 10.18.19 o una posterior
- No se recomienda para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19

La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Implementar para conexiones permanentes**.

12. Haga clic en **Guardar**.

Habilitar aplicaciones de Microsoft 365

Puede abrir el contenedor MDX para permitir a Citrix Secure Mail, Citrix Secure Web y Citrix Files que transfieran documentos y datos a las aplicaciones de Microsoft Office 365. Para obtener más información, consulte [Permitir la interacción segura con aplicaciones Office 365](#).

Aplicar flujos de trabajo

Configure estos parámetros para asignar o crear un flujo de trabajo:

- **Flujo de trabajo para usar:** En la lista desplegable, haga clic en un flujo de trabajo existente o haga clic en **Crear un flujo de trabajo**. El valor predeterminado es **Ninguno**.

Si selecciona **Crear un flujo de trabajo** configure los siguientes parámetros:

- **Nombre:** Escriba un nombre único para el flujo de trabajo.
- **Descripción:** Si quiere, escriba una descripción del flujo de trabajo.
- **Plantillas de correo electrónico de aprobación:** En la lista, seleccione la plantilla de aprobación por correo electrónico que se va a asignar al flujo de trabajo. Cuando haga clic en el icono con forma de ojo situado a la derecha de este campo, aparecerá un cuadro de diálogo en el que puede obtener una vista previa de la plantilla.
- **Niveles de aprobación administrativa:** En la lista, seleccione la cantidad de niveles de aprobación administrativa necesarios para este flujo de trabajo. El valor predeterminado es 1 nivel. Las opciones posibles son:
 - * No se necesita
 - * 1 nivel
 - * 2 niveles
 - * 3 niveles
- **Seleccionar dominio de Active Directory:** En la lista, seleccione el dominio correspondiente de Active Directory que se va a usar para el flujo de trabajo.
- **Buscar aprobadores adicionales requeridos:** Escriba el nombre de la persona obligatoria adicional en el campo de búsqueda y, a continuación, haga clic en **Buscar**. Los nombres se originan en Active Directory.
- Cuando el nombre aparezca en el campo, marque la casilla situada al lado. El nombre y la dirección de correo electrónico aparecen en la lista **Aprobadores adicionales requeridos seleccionados**.

Para quitar a una persona de la lista **Aprobadores adicionales requeridos seleccionados**, 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 requeridos seleccionados** tienen marcas de verificación junto a sus nombres en la lista de resultados de la búsqueda. Desplácese por la lista y desmarque la casilla situada junto a cada nombre que quiera quitar.

Personalizar la marca en el almacén de aplicaciones y Citrix Secure Hub

Puede definir el modo en que las aplicaciones aparecen en el almacén y agregar un logotipo a Citrix Secure Hub y al almacén de aplicaciones. Las funciones de personalización de marca están disponibles para dispositivos iOS y Android.

Antes de comenzar, compruebe que la imagen de personalización de marca está preparada y se puede acceder a ella.

La imagen personalizada debe cumplir los siguientes requisitos:

- El archivo debe estar en formato PNG.
 - Use un texto o logotipo blancos puros con un fondo transparente de 72 ppp.
 - El logotipo de empresa no puede superar la altura ni el ancho de 170 píxeles x 25 píxeles (1x) ni de 340 píxeles x 50 píxeles (2x).
 - Asigne a los archivos el nombre `Header . png` y `Header@2x . png`.
 - Cree un archivo ZIP con los archivos, no una carpeta con los archivos en ella.
1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
 2. En **Cliente**, haga clic en **Personalización de marca del cliente**. Aparecerá la página **Personalización de marca del cliente**.

Settings > Client Branding

Client Branding

You can set the way apps appear in the store and add a logo to brand Secure Hub on mobile devices.

Store name*

Default store view

☐ Category

☒ A-Z

Device

☒ Phone

☐ Tablet

Branding file Browse

Note:

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.
- A .zip file should be created from the files, not a folder with the files inside of it.

Configure los siguientes parámetros:

- **Nombre del almacén:** El nombre de almacén que aparecerá en la información de la cuenta de usuario. Si cambia el nombre, también se cambia la URL que se usa para acceder a los servicios del almacén. Por lo general, no es necesario cambiar el nombre predeterminado.

Importante:

El nombre del almacén solo puede tener caracteres alfanuméricos.

- **Vista predeterminada de almacén:** 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 marca:** Seleccione un archivo o un ZIP con las imágenes que se van a usar para la personalización de marca. Para ello, haga clic en **Examinar** y vaya a la ubicación del archivo.

3. Haga clic en **Guardar**.

Para implementar este paquete en los dispositivos de los usuarios, debe crear un paquete de implementación e implementarlo en los dispositivos.

Citrix Virtual Apps and Desktops a través del almacén de aplicaciones

Citrix Endpoint Management puede recopilar aplicaciones desde Citrix Virtual Apps and Desktops y ponerlas a disposición de los usuarios de dispositivos móviles a través del almacén de aplicaciones. Los usuarios se suscriben a las aplicaciones directamente desde el almacén de aplicaciones y las inician desde Citrix Workspace. La aplicación Citrix Workspace debe estar instalada en los dispositivos del usuario para iniciar las aplicaciones.

Para configurar este parámetro, se 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 con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. Haga clic en **Virtual Apps and Desktops**. Aparecerá la página **Virtual Apps and Desktops**.

Settings > Virtual Apps and Desktops

Virtual Apps and Desktops

Allows users to add Virtual Apps and Desktops through Secure Hub.

Host *	<input type="text" value="FQDN or IP address"/>
Port *	<input type="text" value="80"/>
Relative Path *	<input type="text" value="Example: /Citrix/PNAgent/config.xml"/>
Use HTTPS	<input type="checkbox" value="OFF"/>
Use Cloud Connector	<input checked="" type="checkbox" value="ON"/> ?
Resource Location *	<input type="text" value="Select an option"/> ?
Allowed Relative Paths *	<input type="text" value="/Citrix/Store/*"/> ?

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 habilitar la autenticación segura entre StoreFront y el dispositivo cliente. El valor predeterminado es **Desactivado**.
- **Usar Cloud Connector: Active** el parámetro para usar Cloud Connector para conexiones al servidor de StoreFront. A continuación, especifique una **Ubicación de recursos** y las **Rutas relativas permitidas** para la conexión.
 - **Ubicación de recursos:** Elija una de 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 utilizar un asterisco (*) como comodín.

Supongamos que la ubicación de recursos es `https://StoreFront.company.com` y quiere ofrecer acceso a las siguientes direcciones 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 de StoreFront especificado.
5. Haga clic en **Guardar**.

Tipos de conectores de aplicaciones

March 1, 2024

En la tabla siguiente se muestran los conectores y los tipos de conectores que están disponibles en Citrix Endpoint Management cuando se agrega una aplicación web o SaaS. También puede crear un conector a Citrix Endpoint Management al agregar una aplicación web o SaaS.

En la tabla también se indica si el conector admite el uso de administración de cuentas de usuario, que permite crear cuentas automáticamente o con un flujo de trabajo.

Nombre del conector	SSO SAML	Admite la administración de cuentas de usuario
EchoSign_SAML	S	S
Globoforce_SAML		Nota: Al utilizar este conector, debe habilitar la opción User Management for Provisioning para una correcta integración con el inicio de sesión SSO.
GoogleApps_SAML	S	S
GoogleApps_SAML_IDP	S	S
Lynda_SAML	S	S
Office365_SAML	S	S
Salesforce_SAML	S	S

Nombre del conector	SSO SAML	Admite la administración de cuentas de usuario
Salesforce_SAML_SP	S	S
SandBox_SAML	S	
SuccessFactors_SAML	S	
ShareFile_SAML	S	
ShareFile_SAML_SP	S	
WebEx_SAML_SP	S	S

Citrix Launcher

March 1, 2024

Citrix Launcher permite personalizar la experiencia de usuario en los dispositivos Android Enterprise y Android antiguos implementados por Citrix Endpoint Management. Con Citrix Launcher, puede impedir que los usuarios accedan a determinados parámetros del dispositivo y restringir los dispositivos a una aplicación o a un pequeño grupo de aplicaciones.

Android 6.0 es la versión mínima de Android que se admite para que Citrix Secure Hub administre Citrix Launcher.

Para controlar estas funciones de Citrix Launcher, utilice una **directiva de configuración de Launcher**:

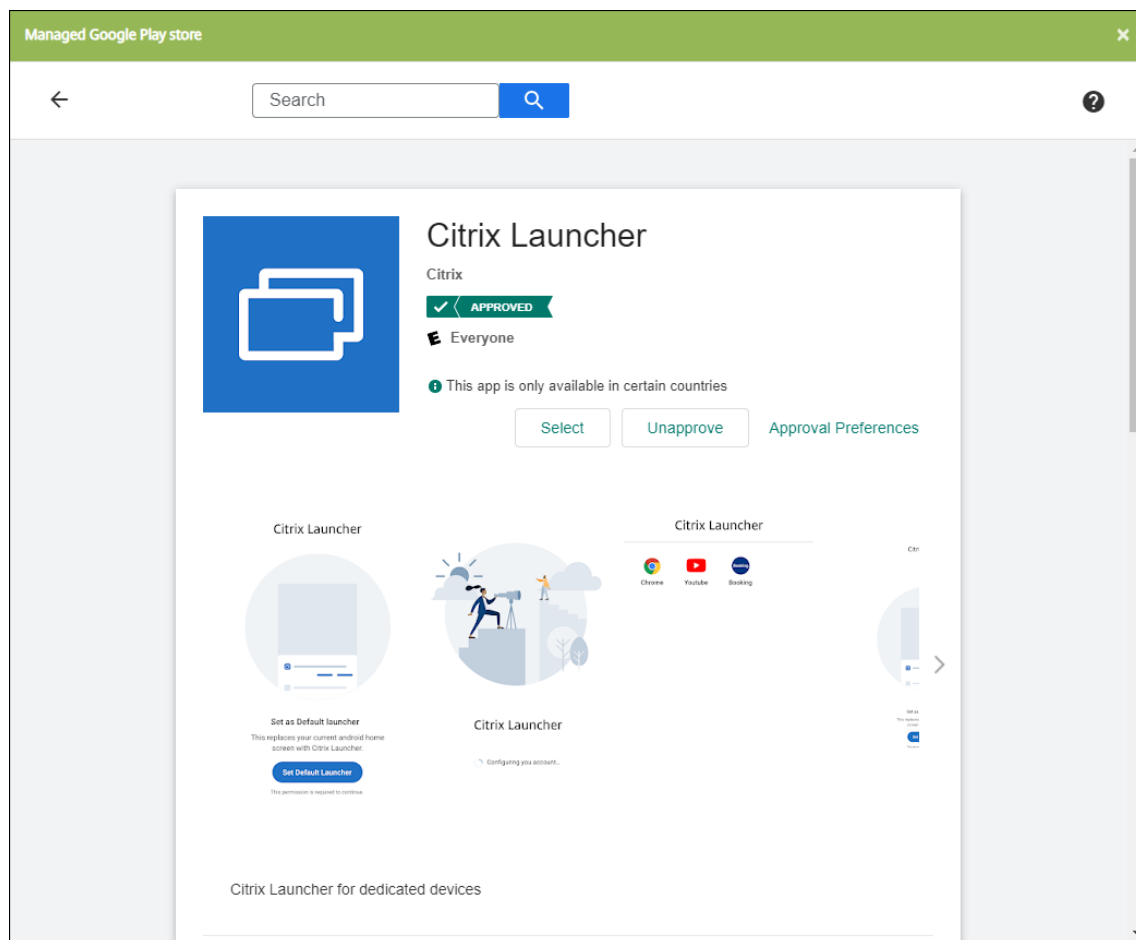
- Administre los dispositivos Android Enterprise y los dispositivos Android antiguos de manera que los usuarios solo puedan acceder a las aplicaciones que especifique.
- Si lo prefiere, puede especificar una imagen de logo personalizada como icono de Citrix Launcher, así como una imagen de fondo para Citrix Launcher.
- Especifique una contraseña que los usuarios deban introducir para salir de Launcher.

Citrix Launcher no está diseñado como una capa de seguridad adicional situada sobre la capa que la plataforma del dispositivo ya proporciona.

Configurar Citrix Launcher para dispositivos Android Enterprise

1. Agregue la aplicación Citrix Launcher (com.citrix.launcher.droid) a Citrix Endpoint Management como aplicación de tienda pública. En **Configurar > Aplicaciones**, haga clic en **Agregar** y, a

continuación, en **Tienda pública de aplicaciones**. Para obtener más información, consulte [Agregar una aplicación de tienda pública](#).



2. En la directiva de quiosco, especifique qué aplicaciones deben estar disponibles en los dispositivos propiedad de la empresa para uso dedicado (también conocidos como dispositivos Android de uso único y propiedad de la empresa [COSU]). Vaya a **Configurar > Directivas de dispositivo**, haga clic en **Agregar** y seleccione **Quiosco**. A continuación, seleccione la aplicación Citrix Launcher y cualquier otra aplicación de la lista de permitidos. Si ha agregado aplicaciones anteriormente a la lista, no es necesario que las vuelva a cargar. Para obtener más información, consulte [Parámetros de Android Enterprise](#).
3. Agregue la directiva de configuración del Launcher. Vaya a **Configurar > Directivas de dispositivo**, haga clic en **Agregar** y seleccione **Configuración de Launcher**. En la directiva de configuración de Launcher, agregue cualquiera de las aplicaciones especificadas en la directiva de quiosco. No es necesario agregar todas las aplicaciones especificadas en la directiva de quiosco. Solo debe agregar la aplicación Citrix Launcher en la directiva de quiosco. Para obtener más información, consulte [Directiva de configuración del 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](#) en 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 sustituye el iniciador Citrix Secure Hub predeterminado. Si cierra la aplicación Citrix Launcher, Citrix Secure Hub volverá a ser el iniciador predeterminado.

Configurar Citrix Launcher para dispositivos Android antiguos

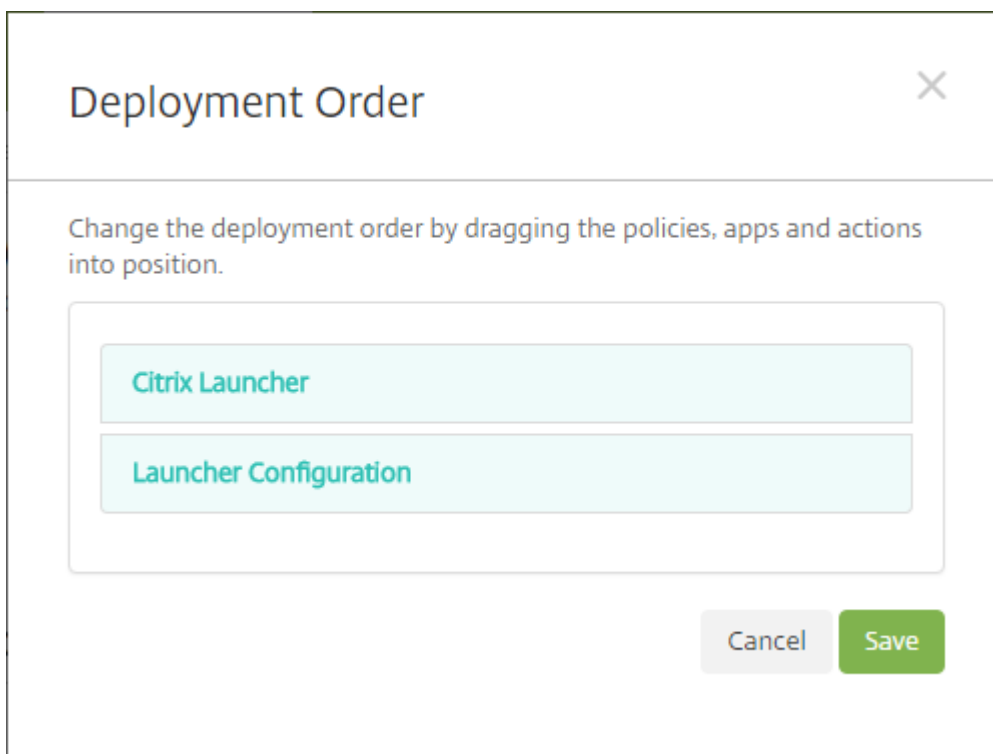
Nota:

En agosto de 2020, Citrix dejó de ofrecer soporte para CitrixLauncher.apk con dispositivos Android antiguos. Puede continuar usando la aplicación Citrix Launcher antigua (com.citrix.launcher) con dispositivos Android, pero no recibirá nuevas actualizaciones de funcionalidad.

1. Para localizar la aplicación Citrix Launcher, vaya a la [página de descargas de Citrix Endpoint Management](#) y busque **Citrix Launcher**. Descargue el archivo más reciente. El archivo está listo para cargarlo en Citrix Endpoint Management y no requiere empaquetado.
2. Agregue la directiva de configuración del Launcher. Vaya a **Configurar > Directivas de dispositivo**, haga clic en **Agregar** y seleccione **Configuración de Launcher**. Para obtener más información, consulte [Directiva de configuración del 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, haga clic en **Empresa**. Para obtener información más detallada, consulte [Agregar una aplicación de empresa](#).
4. Cree un grupo de entrega e implemente recursos. Para obtener más información, consulte la sección [Agregar un grupo de entrega e implementar recursos](#) en este artículo.

Agregar un grupo de entrega e implementar recursos

1. Cree un grupo de entrega de Citrix Launcher con la siguiente configuración en **Configurar > Grupos de entrega**.
 - En la página **Directivas**, agregue una **Directiva de configuración del Launcher**.
 - En la página **Aplicaciones**, arrastre **Citrix Launcher** a **Aplicaciones obligatorias**.
 - En la página **Summary**, haga clic en **Deployment Order** y compruebe que la aplicación **Citrix Launcher** precede a la directiva **Launcher Configuration**.



2. Para implementar recursos en un grupo de entrega, envíe 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 utilizar Citrix Launcher, puede utilizar funciones que ya están disponibles.

Para aprovisionar dispositivos dedicados:

1. Cree un perfil de inscripción estableciendo el **Modo propietario del dispositivo** en **Dispositivo dedicado**. Consulte [Aprovisionar dispositivos Android Enterprise dedicados](#) y [Perfiles de inscripción](#).
2. Cree una directiva de quiosco para agregar aplicaciones a la lista de permitidos y establecer el modo de bloqueo de tarea. Si ha agregado aplicaciones anteriormente a la lista, no es necesario que las vuelva a cargar. Para obtener más información, consulte [Parámetros de Android Enterprise](#).
3. Inscriba cada dispositivo en el perfil de inscripción que ha creado.

Agregar aplicaciones mediante las compras por volumen de Apple

November 29, 2023

Apple Business Manager (ABM) y Apple School Manager (ASM) permiten adquirir licencias para aplicaciones y libros por volumen y sincronizar la información de compras por volumen 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 contenidos por volumen simplifica el proceso de búsqueda, compra y distribución de aplicaciones y libros para las organizaciones.

Para obtener más información sobre la compra de contenidos mediante ABM o ASM, consulte el [Manual de uso de Apple Business Manager](#) o el [Manual de uso de Apple School Manager](#). En este artículo se describe cómo sincronizar licencias adquiridas por volumen de ABM y ASM con Citrix Endpoint Management y cómo administrar las licencias.

Nota:

El Programa de compras por volumen (VPP) de Apple no está disponible desde el 14 de enero de 2021. La función de compras por volumen estaba integrada en ABM y ASM. Si actualmente utiliza el programa de inscripción de dispositivos (DEP) o el programa VPP, puede actualizarse a ABM o ASM. Para obtener más información, consulte [Actualizar desde los programas de implementación de Apple](#), en la documentación de Apple.

Acerca de las compras por volumen de Apple

Al comprar contenidos por volumen mediante ABM o ASM, tenga en cuenta lo siguiente:

- Puede comprar licencias para este contenido:
 - Aplicaciones y libros públicos
 - Aplicaciones personalizadas desarrolladas específicamente para su organización
- Puede implementar aplicaciones y libros adquiridos por volumen en dispositivos que son propiedad de la organización y dispositivos BYOD. Los dispositivos propiedad de la organización inscritos a través de ABM o ASM admiten la inscripción en MDM o MDM+MAM, pero no en MAM.
- Para obtener más información sobre la distribución de aplicaciones, consulte [Distribuir aplicaciones de Apple](#).
- Para obtener una lista de los problemas conocidos, consulte el artículo [CTX222633](#) de Knowledge Center.

Agregar una cuenta de compras por volumen

Después de comprar contenido en el portal de ABM o ASM, descargue del portal el token de contenidos asociado a Citrix Endpoint Management. A continuación, en Citrix Endpoint Management, cree una cuenta de compras por volumen basada en este código de contenidos. Este código permite a Citrix Endpoint Management sincronizar las licencias de contenidos de ABM o ASM.

Con las compras por volumen, puede comprar contenidos e implementarlos en los dispositivos mediante licencias administradas. Si utiliza códigos de canje y quiere cambiar a licencias administradas, consulte el [documento de soporte de Apple](#).

Para agregar una cuenta de compras 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 del código de contenidos en una ubicación segura.
2. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
3. Haga clic en **Compras por volumen**. Aparecerá la página de configuración de **Compras por volumen**.

Settings > Volume Purchase

Volume Purchase

Configure these iOS-specific settings. When saved and validated, the volume purchase apps are added to the table on the Apps tab.

Store user password in Secure Hub ☒ ⓘ

User property for volume purchase country mapping ⓘ

Volume Purchase Accounts

[Add](#) | [Force synchronization](#)

<input type="checkbox"/>	Name	Suffix	Organization	Country	Expiration Date	User Login	Last Sync Date	
<input type="checkbox"/>	VPP	VPP	Citrix System	United States	3/25/22 7:53:55 pm		8/10/21 3:00:00 pm	

4. Configure los siguientes parámetros:

- **Guardar contraseña del usuario en Citrix Secure Hub:** Seleccione si quiere almacenar un nombre de usuario y la contraseña correspondiente en Citrix Secure Hub para la autenticación en Citrix Endpoint Management. El valor predeterminado es **Activado**.
- **Propiedad de usuario para la asignación de país de las compras por volumen:** Escriba un código de asignación de país para que los usuarios puedan descargar aplicaciones de la tienda de aplicaciones específica del país. Contacte con el administrador de contenidos para obtener este código.

Citrix Endpoint Management utiliza el código de asignación de país para elegir la agrupación de propiedades de las compras 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 compras por volumen**.

Add a volume purchase account ×

Define Business to Business (B2B) credentials will make this volume purchase account available as a B2B account.

Name *

Suffix *

Company Token * ?

User Login ?

User Password ?

App Auto Update ☐ ?

Cancel Save

6. Configure estos parámetros de cuenta:

Nota:

Si utiliza Apple Configurator 1, cargue un archivo de licencias de esta manera: Haga clic en **Configurar > Aplicaciones**, vaya a la página de la plataforma y expanda **Compras por volumen**.

- **Nombre:** Escriba un nombre descriptivo para la aplicación.
- **Sufijo:** Escriba el sufijo que aparecerá con los nombres de las aplicaciones heredados 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 la empresa:** Copie y pegue el token de contenidos que descargó en el paso 1.
- **Inicio de sesión del usuario:** (Opcional) Escriba un nombre de usuario para el administrador de esta cuenta de compras por volumen. Si se han configurado, se necesitan el nombre de usuario y la contraseña para sincronizar las aplicaciones personalizadas adquiridas por volumen con Citrix Endpoint Management.
- **Contraseña de usuario:** (Opcional) Escriba una contraseña para el nombre de usuario indicado.
- **Actualización automática de aplicaciones:** Si está **activada**, las aplicaciones adquiridas por volumen y las aplicaciones opcionales de la consola de Citrix Endpoint Management

se actualizan automáticamente cuando hay una nueva versión disponible. Sin embargo, debe actualizar manualmente las aplicaciones de empresa y las aplicaciones de tienda pública en la consola de Citrix Endpoint Management. Si este parámetro está **desactivado**, puede actualizar manualmente las aplicaciones adquiridas por volumen en la consola de Citrix Endpoint Management. Una vez actualizada una aplicación en la consola, los dispositivos que tienen la aplicación instalada también reciben esa actualización. El valor predeterminado es **Desactivado**.

Una vez agregada correctamente la cuenta de volumen, aparece un mensaje que le notifica lo siguiente:

- En la página **Configurar > Aplicaciones**, las aplicaciones adquiridas por volumen aparecen en la lista Aplicaciones. Los nombres de las aplicaciones aparecen con el sufijo configurado.
- En la página **Configurar > Medios**, los libros adquiridos por volumen aparecen en la lista Medios. Los nombres de los libros aparecen con el sufijo configurado.

Configurar aplicaciones adquiridas por volumen

Una vez agregada una cuenta de compras por volumen, la información de las aplicaciones se sincroniza con Citrix Endpoint Management y aparece en la página **Configurar > Aplicaciones**. Ahora puede configurar estas aplicaciones, ajustar el grupo de entrega y definir las configuraciones de directivas para dispositivos de iOS y macOS. Después de completar la configuración, los usuarios pueden inscribir sus dispositivos.

Al configurar una aplicación adquirida por volumen, tenga en cuenta estos parámetros:

- En la página **Configurar > Aplicaciones**:
 - Para que Citrix Endpoint Management implemente una aplicación en un dispositivo en lugar de hacerlo un usuario, active **Forzar asociación de licencia con el dispositivo**. Cuando este parámetro está activo, los usuarios no tienen que usar su ID de Apple y pueden descargar las aplicaciones sin iniciar sesión en su cuenta del App Store.
 - Se recomienda activar **Forzar administración de la aplicación** para una aplicación, de modo que se instale automáticamente como una aplicación administrada.

Nota:

Para que el parámetro **Forzar administración de la aplicación** surta efecto, debe configurar la propiedad de servidor `apple.app.force.managed` en **True** en la página **Parámetros > Propiedades de servidor**. Para obtener información, consulte [Propiedades de servidor](#).

Device Policies Apps Media Actions Content Collaboration Enrollment Profiles Delivery Groups

Public App Store

1 App Information

2 Platform

- ☒ iPhone
- ☒ iPad
- ☐ Android (legacy DA)
- ☐ Android Enterprise
- ☐ Windows Desktop/Tablet
- ☐ Windows Phone

3 Approvals (optional)

4 Delivery Group Assignments (optional)

iPhone App Settings

Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

App Details

Name

Description

Version [Check for Updates](#)

Package ID

Image

App URL

Paid app ☐

Remove app if MDM profile is removed ☒

Prevent app data backup ☒

Force app to be managed ☒

Force license association to device ☐

Deployment Rules

Store Configuration

Volume purchase

- En la página **Configurar > Grupo de entrega**:

Para que la aplicación se instale de forma silenciosa en dispositivos de usuario con una interacción mínima de los usuarios, vaya a la página **Aplicaciones** y, a continuación, arrastre la aplicación a la lista **Aplicaciones obligatorias**. De forma predeterminada, todas 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 las licencias de una aplicación. Si fuera necesario, puede recuperar una licencia utilizada y ponerla a disposición de otro usuario o dispositivo.

- Haga clic en **Configurar > Aplicaciones**.
- Seleccione una aplicación y haga clic en **Modificar**.
- Vaya a la página **Plataforma** y, a continuación, expanda **Compras por volumen**.
En la tabla **Asignación de ID de compras por volumen**, puede rastrear cuántas licencias se utilizan y qué usuario o dispositivo las usa.

Device Policies Apps Media Actions ShareFile Enrollment Profiles Delivery Groups

Public App Store

1 App Information

2 Platform

- ☒ iPhone
- ☒ iPad
- ☐ Google Play

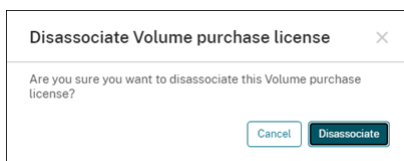
Volume purchase Account test

Volume purchase ID Assignment

License Usage: 2 of 10

<input type="checkbox"/>	License ID	Usage Status	Associated User	Associated Device	Device Serial Number	Device Phone Number	
<input type="checkbox"/>	8447476795	Used					
<input type="checkbox"/>	8447476794	Used					

- Para recuperar una licencia, seleccione la licencia y, a continuación, haga clic en **Desasociar**.



- Haga clic en **Desasociar** para confirmar la acción.

Retirar a un usuario de la cuenta de compras por volumen

Si asocia licencias de aplicación a los usuarios, puede retirar a usuarios de las cuentas de compras por volumen para recuperar todas las licencias que tengan asignadas. Un caso de uso de ejemplo es el momento en que un usuario se va de su organización.

- Haga clic en **Administrar > Dispositivos**.
- Seleccione el dispositivo que pertenece al usuario de destino y, a continuación, haga clic en **Modificar**.
- Vaya a la página **Propiedades de usuario** y seleccione las cuentas de compras por volumen que sean necesarias.
- Haga clic en **Retirar**.

Citrix Endpoint Management revoca al usuario las licencias de aplicación existentes en las cuentas de compras por volumen seleccionadas.

Sincronizar la información de las aplicaciones

Citrix Endpoint Management sincroniza periódicamente la información de las aplicaciones con ABM o ASM. Si es necesario, puede sincronizar manualmente la información de las aplicaciones. La sincronización se asegura de que las licencias de aplicación y otra información de las aplicaciones reflejen todos los cambios. Un ejemplo de estos cambios es la eliminación manual de una aplicación de la cuenta de compras por volumen.

Cambiar el intervalo de sincronización predeterminado

De forma predeterminada, Citrix Endpoint Management actualiza el punto de referencia para las licencias del programa 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 de servidor `vpp.baseline`. Para obtener información, consulte [Propiedades de servidor](#).

Sincronizar manualmente la información de las aplicaciones

Puede forzar una sincronización con ABM o ASM para obtener inmediatamente la información más reciente de las aplicaciones.

1. Haga clic en **Parámetros > Compras por volumen**.
2. Seleccione una cuenta de compras por volumen y, a continuación, haga clic en **Forzar sincronización**. O bien haga clic en **Forzar sincronización** sin seleccionar ninguna cuenta de compras por volumen para sincronizar todas las cuentas.

Settings > Volume Purchase

Volume Purchase

Configure these iOS-specific settings. When saved and validated, the volume purchase apps are added to the table on the Apps tab.

Store user password in Secure Hub ☒ ⓘ

User property for volume purchase country mapping ⓘ

Volume Purchase Accounts

[Add](#) | [Force synchronization](#)

<input type="checkbox"/>	Name	Suffix	Organization	Country	Expiration Date	User Login	Last Sync Date	⌵
<input type="checkbox"/>	VPP	VPP	Citrix System	United States	3/25/22 7:53:55 pm		8/10/21 3:00:00 pm	

3. Confirme la acción de sincronización. La sincronización comienza.

Es posible que la sincronización tarde varios minutos en función de la cantidad de licencias de compras por volumen. Una vez completada la sincronización, Citrix Endpoint Management actualiza la página **Compra por volumen** y cambia la fecha y la hora de sincronización en la columna **Fecha de la última sincronización**.

Comprobar si hay actualizaciones para las aplicaciones

Si activa el parámetro **Actualización automática de aplicaciones** al agregar una cuenta de compras por volumen, Citrix Endpoint Management comprueba periódicamente si hay nuevas versiones de las aplicaciones opcionales y compradas por volumen y las actualiza. Si es necesario, puede buscar manualmente la nueva versión de cualquier aplicación y aplicar las actualizaciones de dicha aplicación en Citrix Endpoint Management.

Una vez que Citrix Endpoint Management haya recibido una nueva versión de una aplicación obligatoria, envía la nueva versión a los dispositivos para que se instale de manera silenciosa sin solicitárselo a los usuarios.

Para buscar y aplicar nuevas versiones de aplicaciones

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. Vaya a la página **Plataforma** y, a continuación, haga clic en **Buscar actualizaciones** junto a **Versión**.
5. En el cuadro de diálogo **Actualización** que aparece, aplique la actualización si hay una nueva versión disponible.

Renovar el token de contenidos de su cuenta de compras por volumen

Los tokens de contenidos caducan al año. Cuando el token se acerca a la fecha de caducidad, Citrix Endpoint Management muestra una advertencia de caducidad de la licencia. Renueve el token de contenidos a tiempo para no interrumpir el servicio de los 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 con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
3. Haga clic en **Compras por volumen**. Aparecerá la página de configuración de Compras por volumen.
4. Modifique la cuenta de compras por volumen con la información del token actualizado.

Utilice ShareFile con Citrix Endpoint Management

March 1, 2024

Citrix Endpoint Management tiene dos opciones para integrarse con ShareFile. Son conectores de zonas de almacenamiento y Citrix Files.

Citrix Files

Puede configurar Citrix Endpoint Management para que proporcione acceso a su cuenta de ShareFile. Esa configuración:

- Permite a los usuarios móviles acceder al conjunto de las funcionalidades de ShareFile (como compartir archivos, sincronizarlos y usar conectores de zona de almacenamiento).
- Puede ofrecer a Citrix Files la autenticación Single Sign-On para usuarios de las aplicaciones móviles de productividad y unas directivas completas de control de acceso.
- Proporciona la configuración de ShareFile, la supervisión a 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 Enterprise, consulte [SAML para Single Sign-On en Citrix Files](#).

Conectores de zonas de almacenamiento

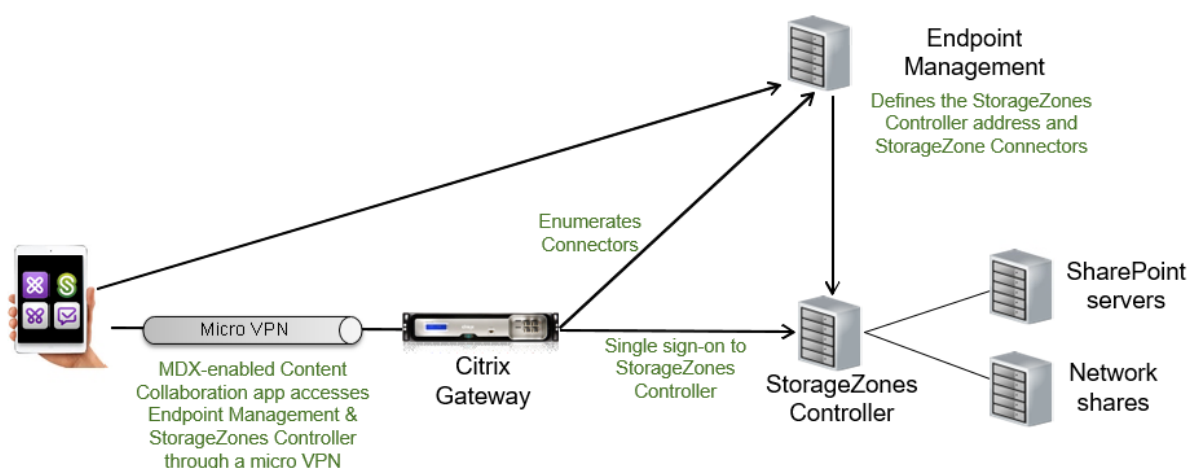
Puede configurar Citrix Endpoint Management para que solo ofrezca acceso a los conectores de zonas de almacenamiento que haya creado desde la consola de Citrix Endpoint Management. Esa configuración:

- Ofrece un acceso móvil seguro a los repositorios existentes de almacenamiento local (como sitios de SharePoint y recursos compartidos de red).
- No es necesario configurar un subdominio de ShareFile ni alojar datos de Citrix Files.
- Proporciona a los usuarios acceso móvil a los datos a través de las aplicaciones móviles de productividad de Citrix Files para iOS y Android. Los usuarios pueden modificar los documentos de Microsoft Office. Los usuarios también pueden ver en vista previa los archivos PDF de Adobe y hacer anotaciones en ellos desde dispositivos móviles.
- Cumple las restricciones de seguridad contra la filtración de datos de usuarios fuera de la red corporativa.
- Proporciona una configuración simple de conectores de zonas de almacenamiento desde la consola de Citrix Endpoint Management. Si más adelante decide usar la funcionalidad completa de Citrix Files con Citrix Endpoint Management, puede cambiar la configuración en la consola de Citrix Endpoint Management.

Para integrar Citrix Endpoint Management solamente en conectores de zonas de almacenamiento:

- ShareFile utiliza su configuración de inicio de sesión único SSO en NetScaler Gateway para autenticarse en 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.

En el siguiente diagrama, se muestra la arquitectura de alto nivel para usar Citrix Endpoint Management con conectores de zonas 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 para configurar el controlador de zonas de almacenamiento 5.0
- Compruebe que el servidor que ejecutará el controlador de zonas de almacenamiento cumple los requisitos del sistema. Para conocer los requisitos, consulte [Requisitos del sistema](#).

Los requisitos de las zonas de almacenamiento para datos de Citrix Files y para zonas de almacenamiento restringidas no se aplican cuando Citrix Endpoint Management se integra solo en conectores de zonas de almacenamiento.

Citrix Endpoint Management no admite los 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 un controlador de zonas de almacenamiento. Estos pasos son específicos de la integración de Citrix Endpoint Management en conectores de zonas de almacenamiento solamente. Algunos de estos artículos se encuentran en la documentación sobre los controladores de zonas de almacenamiento.

1. [Configurar NetScaler para los controladores de zonas de almacenamiento](#)

Puede usar NetScaler Gateway como un proxy DMZ para el controlador de zonas de almacenamiento.

2. [Instalar un certificado SSL](#)

Un controlador de zonas de almacenamiento que aloja zonas estándares requiere un certificado SSL. Un controlador de zonas de almacenamiento que aloja zonas restringidas y usa una dirección interna no necesita ningún certificado SSL.

3. [Preparar el servidor](#)

Se requiere la configuración de IIS y ASP.NET para los conectores de zonas de almacenamiento.

4. [Instalar controlador de zonas de almacenamiento](#)

5. [Preparar un controlador de zonas de almacenamiento para que solo se pueda usar 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 mediante otros métodos.

7. [Configurar el controlador de dominio de modo 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.

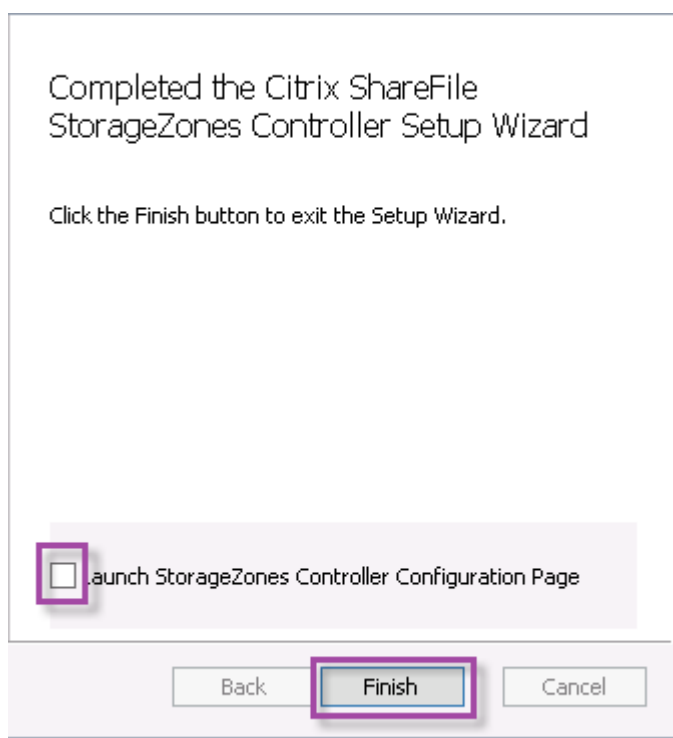
8. [Unir un controlador de zonas de almacenamiento secundario a una zona de almacenamiento](#)

Para configurar una zona de almacenamiento para alta disponibilidad, conecte al menos dos controladores de zonas de almacenamiento.

Instalar controlador de zonas de almacenamiento

1. Descargue e instale el software del controlador de zonas de almacenamiento:
 - a) Desde la página de descargas de Citrix Files, en <https://www.citrix.com/downloads/sharefile.html>, inicie sesión y descargue el instalador más reciente de controladores de zonas de almacenamiento.
 - b) Instalar el controlador de zonas de almacenamiento cambia el sitio web predeterminado en el servidor por la ruta de instalación del controlador. Habilite **Autenticación anónima** en el sitio web predeterminado.
2. En el servidor donde quiere instalar el controlador de zonas de almacenamiento, ejecute StorageCenter.msi.

Se iniciará el asistente de instalación del controlador de zonas de almacenamiento.
3. Responda a estas indicaciones:
 - En la página **Carpeta de destino**, si Internet Information Services (IIS) está instalado en la ubicación predeterminada, deje los valores predeterminados. Si no es así, vaya a la ubicación de instalación de IIS.
 - Cuando finalice la instalación, desmarque la casilla para **Iniciar la 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 probar que la instalación se ha realizado correctamente, vaya a <https://localhost/>. (si aparece un error de certificado, plantéese conectarse por HTTP). Si la instalación se realiza correctamente, aparece el logotipo de Citrix Files.

Si no aparece el logotipo de Citrix Files, borre la memoria caché del explorador web y vuelva a intentarlo.

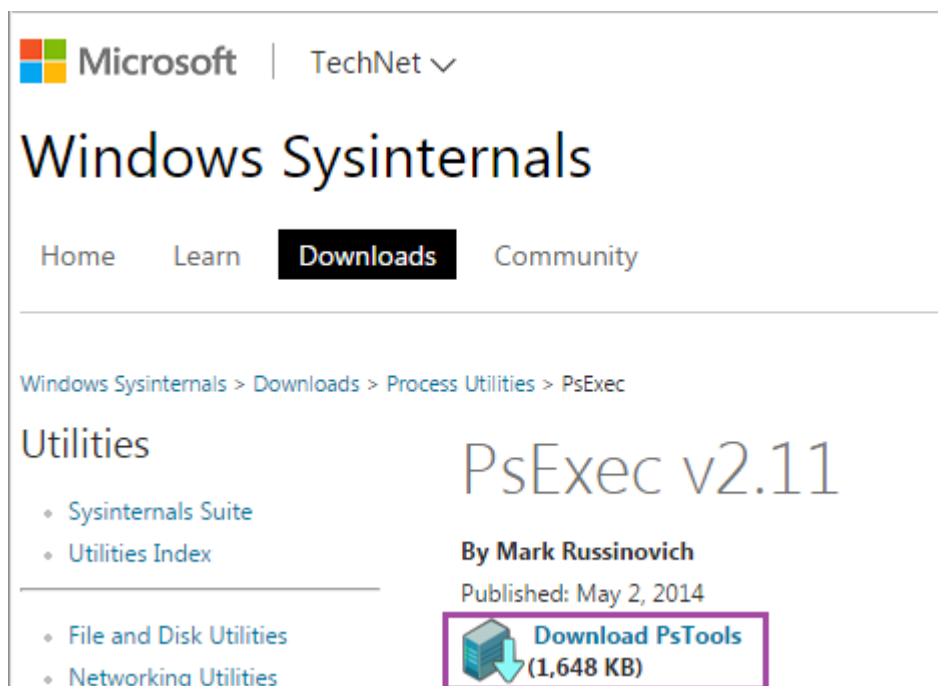
Importante:

Si va a clonar el controlador de zonas de almacenamiento, capture la imagen de disco antes de continuar con la configuración del controlador.

Preparar un controlador de zonas de almacenamiento para que solo se pueda usar con conectores de zonas de almacenamiento

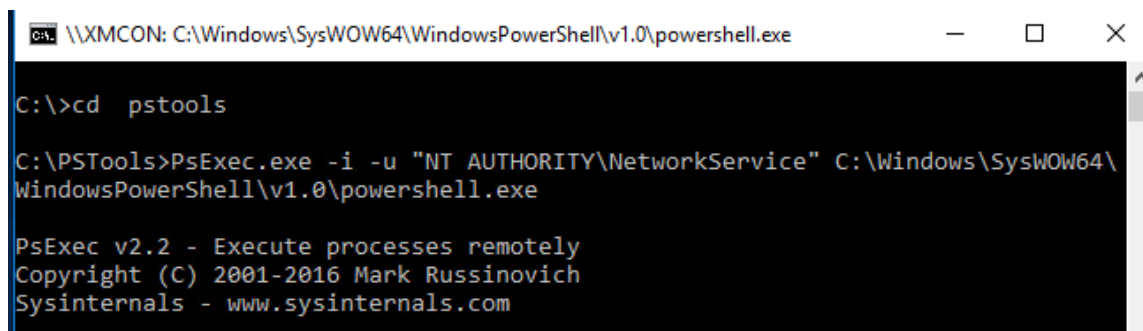
Para una integración solo con conectores de zonas de almacenamiento, no es necesario usar la consola administrativa del controlador de zonas de almacenamiento. Esa interfaz requiere una cuenta de administrador de Citrix Files, que no es necesaria para esta solución. Por eso, puede ejecutar un script de PowerShell para preparar el controlador de zonas de almacenamiento con el fin usarlo sin el plano de control de Citrix Files. El script lleva a cabo lo siguiente:

- Registra el controlador de zonas de almacenamiento actual como un controlador de zonas de almacenamiento principal. Puede unir más adelante controladores de zonas de almacenamiento secundarios al controlador principal.
 - Crea una zona y establece la frase secreta para ella.
1. En el servidor del controlador de zonas de almacenamiento, descargue la herramienta PsExec. Para ello, vaya a Microsoft [Windows Sysinternals](#) y, a continuación, haga clic en **Descargar PsTools**. Extraiga la herramienta en la raíz de la unidad C:.

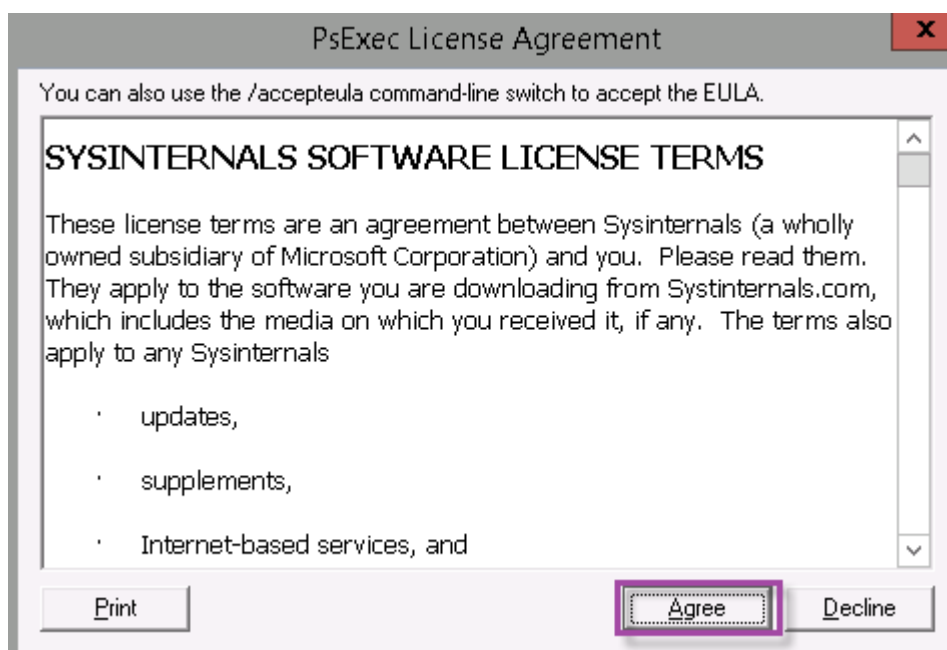


2. Ejecute la herramienta PsExec: Abra el símbolo del sistema como el usuario administrador y escriba lo siguiente:

```
1  ```\n2  cd c:\\pstools\n3  PsExec.exe -i -u "NT AUTHORITY\\NetworkService" C:\\Windows\\SysWOW64\n   \\WindowsPowerShell\\v1.0\\powershell.exe\n4  <!--NeedCopy-->  ```\n
```



3. Cuando se le pida, haga clic en **Agree** para ejecutar la herramienta Sysinternals.



Se abrirá una ventana de PowerShell.

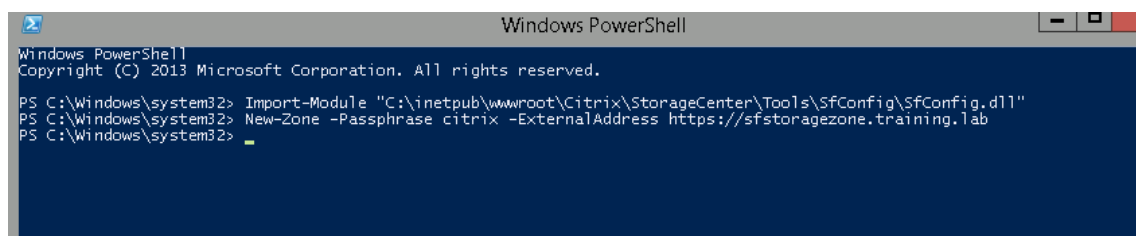
4. En la ventana de PowerShell, escriba lo siguiente:

```
1  ``
2  Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"
3  New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.
   com
4  <!--NeedCopy--> ``
```

Donde:

Passphrase: Es la frase secreta que quiere asignar al sitio. Apúntela. No podrá recuperar la frase secreta desde el Controller. Si pierde la frase secreta, no podrá volver a instalar zonas de almacenamiento ni 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.



Ahora, el controlador de zonas de almacenamiento principal está listo.

Antes de iniciar sesión en Citrix Endpoint Management para crear conectores de zonas de alma-

cenamiento, debe completar la configuración siguiente, si procede:

[Especificar un servidor proxy para las zonas de almacenamiento](#)

[Configurar el controlador de dominio de modo que confíe en el controlador de zonas de almacenamiento para la delegación](#)

[Unir un controlador de zonas de almacenamiento secundario 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 de zonas de almacenamiento secundario a una zona de almacenamiento

Para configurar una zona de almacenamiento para alta disponibilidad, conecte al menos dos controladores de zonas de almacenamiento. Para unir un controlador de zonas de almacenamiento secundario a una zona, instale el controlador de zonas de almacenamiento en un segundo servidor. Luego, una ese Controller a la zona del Controller principal.

1. Abra una ventana de PowerShell en el servidor del controlador de zonas de almacenamiento que quiere 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 de controladores de zonas de almacenamiento en Citrix Endpoint Management

Antes de agregar conectores de zonas de almacenamiento, configure la información de conexión de cada controlador de zonas de almacenamiento habilitado para conectores de zonas de almacenamiento. Los controladores de zonas de almacenamiento se pueden definir como se describe en esta sección, aunque también se pueden definir cuando se agregue un conector.

En su primera visita a la página **Configurar > ShareFile**, se resumen en la página las diferencias entre usar Citrix Endpoint Management para cuentas Enterprise y para conectores de zonas de almacenamiento.

Device PoliciesAppsMediaActionsContent CollaborationEnrollment ProfilesDelivery Groups

Choose a method for integrating Content Collaboration with Endpoint Management. Or, learn more about which mode to select.

Content Collaboration

Storage Zone Connectors Only

Access network shares and SharePoint data from mobile devices

✓

✓

Edit Microsoft Office documents from mobile devices

✓

✓

Preview and annotate Adobe PDF files from mobile devices

✓

✓

Store data in Citrix-managed or customer-managed storage zones or both

✓

Securely share files with people inside and outside the enterprise

✓

Sync files and data across multiple devices

✓

Access files through the Citrix Files website

✓

Access Office 365 content and Personal Cloud connectors from mobile devices

✓

Use auditing and reporting capabilities

✓

Configure Content Collaboration

Configure Connectors

Haga clic en **Configurar conectores** para continuar con los pasos de configuración de este artículo.

Device PoliciesAppsMediaActionsContent CollaborationEnrollment ProfilesDelivery Groups

Storage Zone Connectors

Storage zone connectors provide access to documents and folders in SharePoint sites and network file shares.

Add

Manage Storage Zones

Connector Name

Type

Storage Zone

Location

Delivery Groups

1. En **Configurar > ShareFile**, haga clic en **Administrar zonas de almacenamiento**.

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery Groups

StorageZone Connectors

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

Add

Manage StorageZones

Connector Name

Type

StorageZone

Location

Delivery Groups

2. En **Administrar zonas de almacenamiento**, agregue la información de conexión.

Manage Storage Zones

Add New

Name * ContentCollaborationTest

FQDN *

Port * 443

Secure Connection ON

Administrator user na...

Administrator passwo...

Add Cancel Save

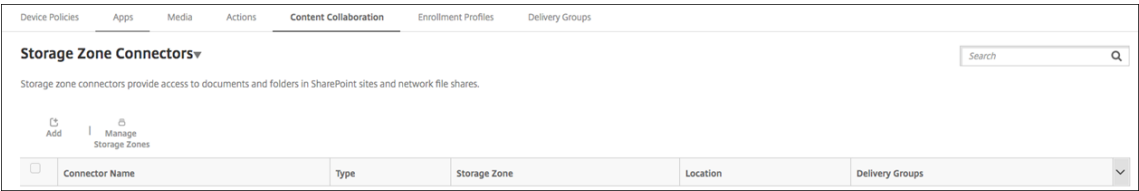
- **Nombre:** Un nombre descriptivo de la zona de almacenamiento, que se utiliza para identificar la zona de almacenamiento en Citrix Endpoint Management. No incluya espacios ni caracteres especiales en el nombre.
 - **FQDN y puerto:** El nombre de dominio completo y el número de puerto del controlador de zonas de almacenamiento al que se puede acceder desde el servidor Citrix Endpoint Management.
 - **Conexión segura:** Si usa SSL para las conexiones con el controlador de zonas de almacenamiento, use el parámetro predeterminado “Sí”. Si no utiliza SSL para las conexiones, desactive este parámetro.
 - **Nombre de usuario del administrador y Contraseña del administrador:** El nombre de usuario de la cuenta del administrador del servicio (en el formato dominio\admin) y la contraseña. También puede utilizar 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, compruebe que el servidor Citrix Endpoint Management pueda establecer conexión con el nombre de dominio completo del controlador de zonas de almacenamiento en el puerto 443.
 5. Para definir otra conexión del 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 del controlador de zonas de almacenamiento, seleccione el nombre de la conexión en **Administrar zonas de almacenamiento**. Haga clic en **Modificar** o **Eliminar**.

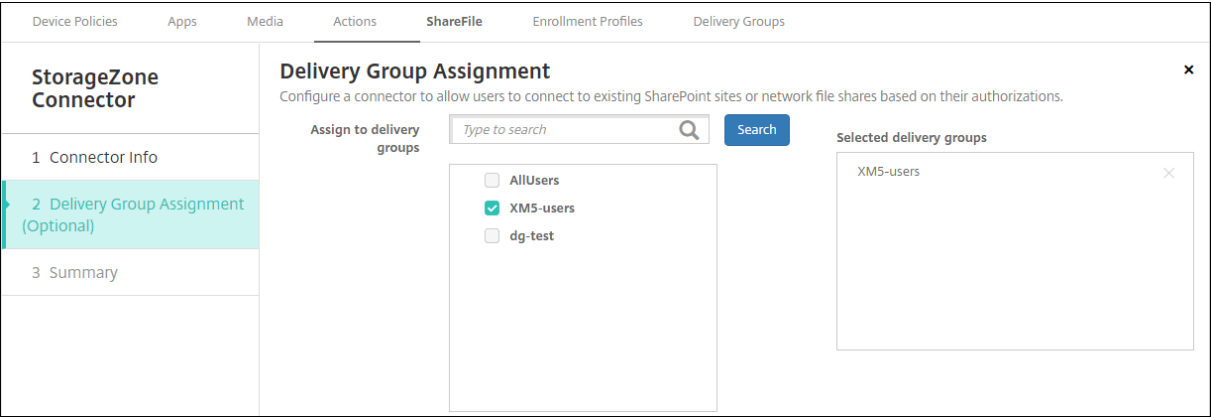
Agregar un conector de zonas de almacenamiento en Citrix Endpoint Management

1. Vaya a **Configurar > ShareFile** y, a continuación, haga clic en **Agregar**.



2. En la página **Información del conector**, configure los siguientes parámetros:

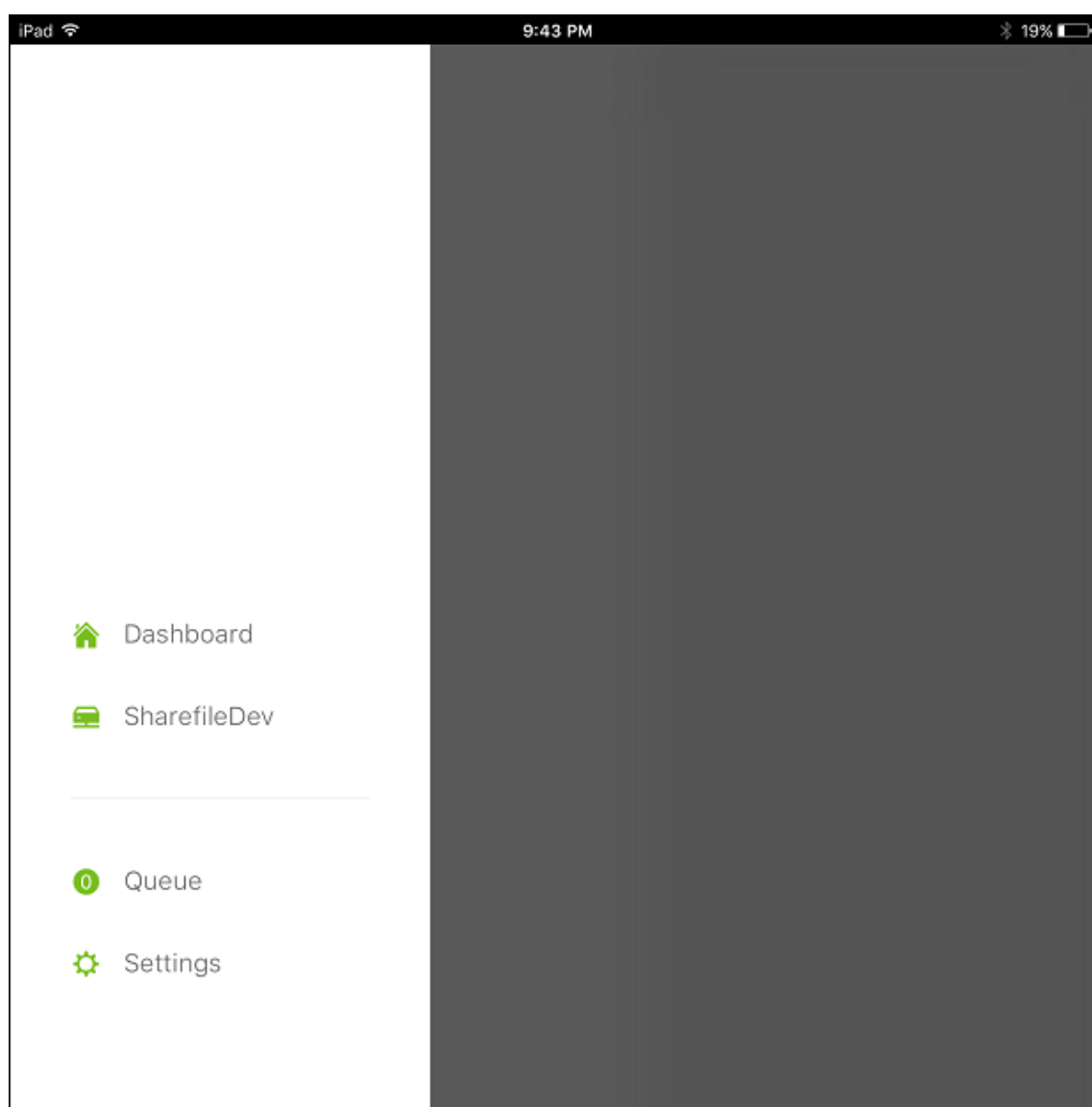
- **Nombre de conector:** Un nombre que identifica el conector de zonas de almacenamiento en Citrix Endpoint Management.
 - **Descripción:** Notas opcionales sobre este conector.
 - **Tipo:** Elija **SharePoint** o **Red**.
 - **Zona de almacenamiento:** Seleccione la zona de almacenamiento asociada al conector. Si la zona de almacenamiento no aparece, haga clic en **Administrar zonas de almacenamiento** para definir el controlador de zonas de almacenamiento.
 - **Ubicación:** Para SharePoint, especifique la URL del sitio en el nivel raíz de SharePoint, la colección del sitio o la biblioteca de documentos, en el formato `https://sharepoint.company.com`. Para un recurso compartido de red, especifique el nombre de dominio completo de la ruta Uniform Naming Convention (UNC) en el formato `\\server\share`.
3. En la página **Asignación de grupos de entrega**, puede asignar el conector a grupos de entrega. También puede asociar conectores a grupos de entrega desde **Configurar > Grupos de entrega**.

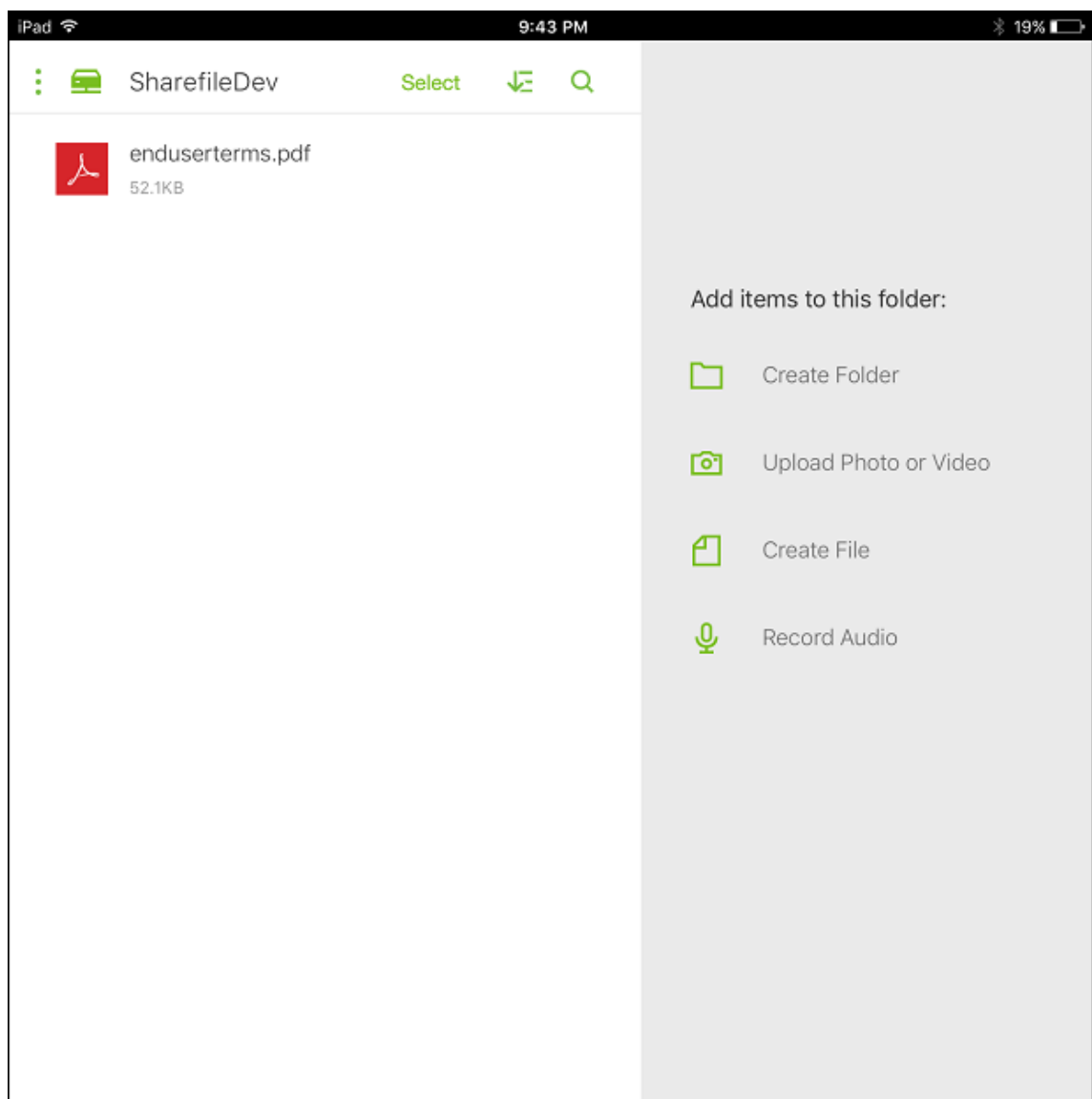


1. En la página **Resumen**, puede revisar las opciones que ha configurado. Para ajustar la configuración, haga clic en **Atrás**.
2. Haga clic en **Guardar** para guardar el conector.
3. Pruebe el conector:
 - a) Cuando empaquete los clientes de Citrix Files, establezca la directiva “Acceso de red” en **Túnel: SSO web**.

En este modo de canalización por túnel, el framework MDX finaliza el tráfico SSL/HTTP desde una aplicación MDX. A continuación, MDX inicia conexiones nuevas con conexiones internas en nombre del usuario. Esta configuración de directiva permite que el marco de MDX detecte y responda a los desafíos de autenticación emitidos por 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 admitido, compruebe el inicio Single Sign-On en Citrix Files y los conectores.

En los siguientes ejemplos, SharefileDev es el nombre de un conector.





Filtrar la lista de conectores de zonas de almacenamiento

Puede filtrar la lista de conectores de zonas 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**.

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery Groups

StorageZone Connectors▼

Show filter

Search

Q

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

Add

Manage StorageZones

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups	▼
<input type="checkbox"/>	TestNS	NetworkFile	iosDev		XM5-users	
<input type="checkbox"/>	TestSP	Sharepoint	iosDev		XM5-users,AllUsers	

Showing 1 - 2 of 2 items

2. Expanda los encabezados de los filtros para las selecciones necesarias. Para guardar un filtro, haga clic en **Guardar esta vista**, escriba el nombre del filtro y haga clic en **Guardar**.

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery Groups

Filters

Clear All

Type

Clear

☒ NetworkFile2

Clear

☐ Sharepoint1

Clear

Assigned Delivery Groups

Clear

StorageZone

Clear

SAVE THIS VIEW

StorageZone Connectors▼

Hide filter

Search

Q

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

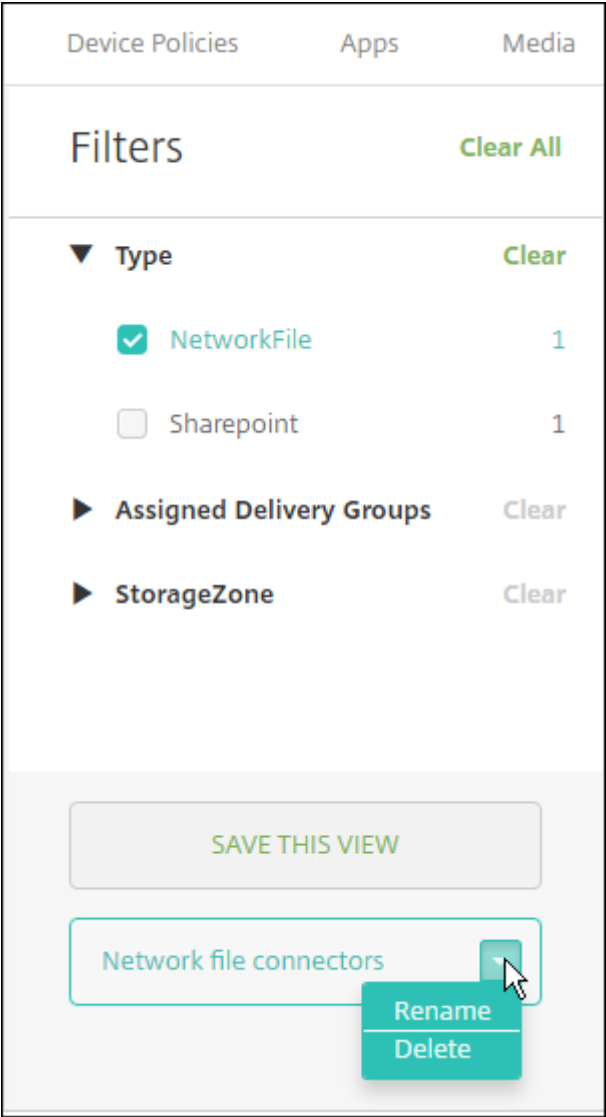
Add

Manage StorageZones

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups	▼
<input type="checkbox"/>	TestNS	NetworkFile	sz2	\\sz2\Storagezone	XM5-users	
<input type="checkbox"/>	testxm	NetworkFile	sz1	\\sz1\Storagezone	XM5-users	

Showing 1 - 2 of 2 items

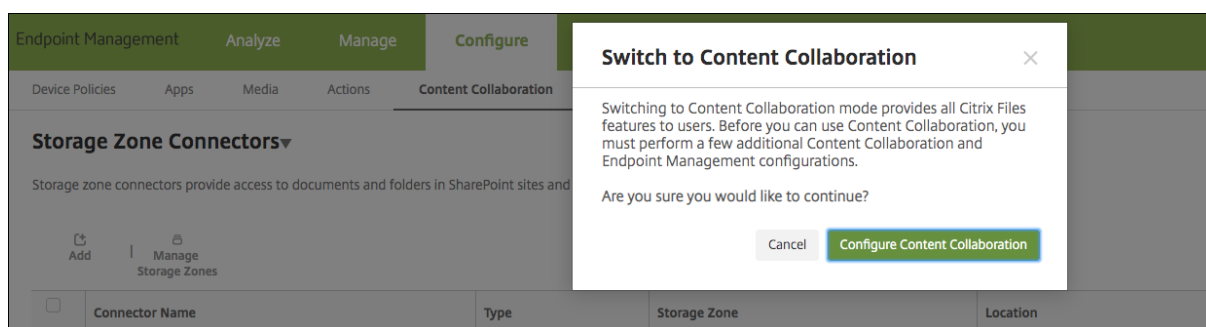
3. Para cambiar el nombre de un filtro o eliminarlo, haga clic en el icono de flecha situado junto al nombre del filtro.



Cambiar a una cuenta Enterprise

Después de integrar conectores de zonas de almacenamiento en Citrix Endpoint Management, puede cambiar al conjunto de funciones de Citrix Files Enterprise. Citrix Endpoint Management conserva los parámetros existentes de integración de conectores de zonas de almacenamiento.

Vaya a **Configurar > ShareFile**, haga clic en el menú desplegable **Conectores de zonas de almacenamiento** y, a continuación, haga clic en **Configurar ShareFile**.



Para obtener información sobre cómo configurar cuentas Enterprise, consulte [SAML para Single Sign-On en Citrix Files](#).

SmartAccess para aplicaciones HDX

March 1, 2024

Esta funcionalidad permite controlar el acceso a aplicaciones HDX en función de las propiedades del dispositivo, las propiedades de un usuario o las aplicaciones instaladas en un dispositivo. Puede usar esta función mediante acciones automatizadas que marcan el dispositivo como no conforme para denegarle el acceso a las aplicaciones. 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. A continuación, StoreFront permite o deniega el acceso en función de la directiva del control de acceso de la aplicación.

Para usar esta función, su implementación requiere:

- Citrix Virtual Apps and Desktops
- Citrix Endpoint Management
- Citrix Endpoint Management configurado con un certificado SAML que se utilizará para firmar y cifrar las etiquetas. El mismo certificado sin clave privada se carga en el servidor de StoreFront.

Para empezar a usar esta funcionalidad:

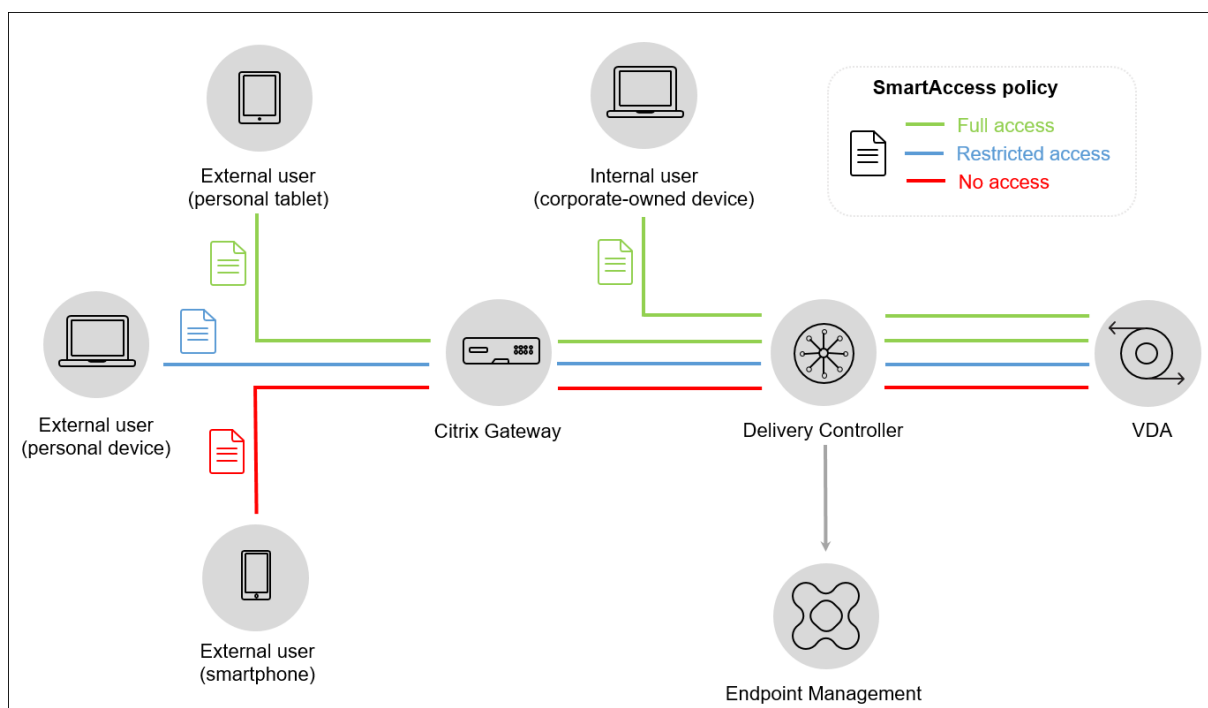
- Configure el certificado del servidor Citrix Endpoint Management para el almacén de StoreFront
- Configure al menos un grupo de entrega de Citrix Virtual Apps and Desktops con la directiva de SmartAccess requerida
- Establezca la acción automatizada en Citrix Endpoint Management

SmartAccess en aplicaciones HDX para dispositivos de punto final

Con esta funcionalidad, puede aplicar un control de acceso basado en directivas para restringir el acceso del dispositivo a las aplicaciones HDX. Puede aplicar los siguientes niveles de acceso a las aplicaciones HDX:

- **Acceso completo.** Un dispositivo puede acceder a todas las aplicaciones HDX que proporciona el almacén 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. Al intentar iniciar una aplicación HDX en Citrix Secure Hub, se desencadena una solicitud a un Delivery Controller. A continuación, 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, si el dispositivo está liberado por jailbreak, se deniega el acceso a una aplicación HDX.



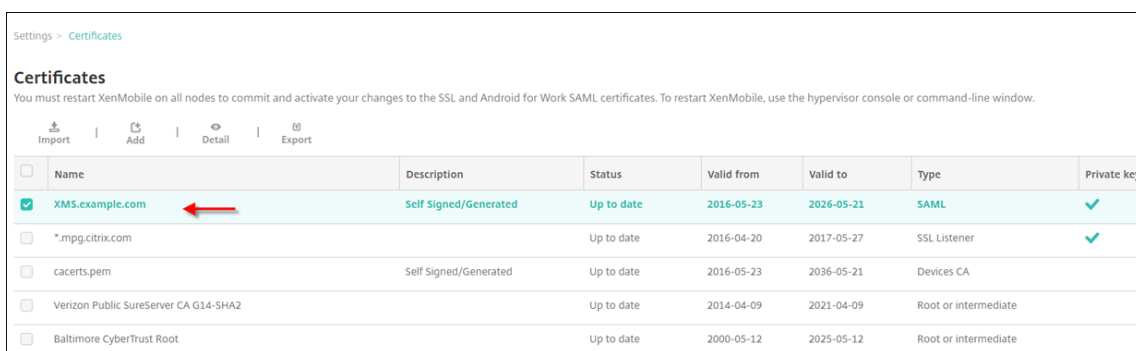
Exportar, configurar el certificado de Citrix Endpoint Management y cargarlo en el almacén de StoreFront

SmartAccess usa etiquetas cifradas y firmadas para la comunicación entre los servidores Citrix Endpoint Management y StoreFront. Para habilitar esta comunicación, agregue el certificado del servidor Citrix Endpoint Management al almacén de StoreFront.

Para obtener más información sobre la integración de StoreFront y Citrix Endpoint Management cuando Citrix Endpoint Management tiene habilitada la autenticación basada en certificados y dominios, consulte los artículos de [Knowledge Center](#).

Exportar el certificado SAML desde Citrix Endpoint Management

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**. Haga clic en **Certificados**.
2. Busque el certificado SAML para el servidor Citrix Endpoint Management.



Settings > Certificates

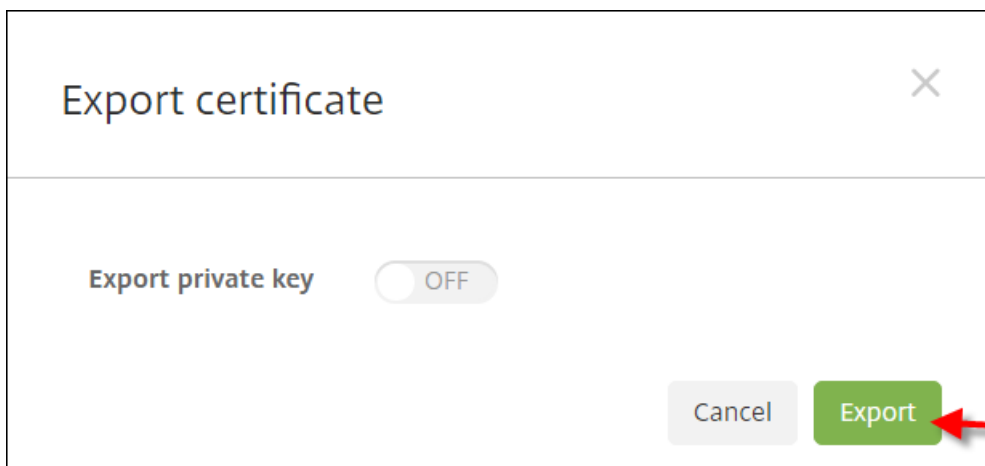
Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

Import | Add | Detail | Export

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key
<input checked="" type="checkbox"/>	XMS.example.com	Self Signed/Generated	Up to date	2016-05-23	2026-05-21	SAML	✓
<input type="checkbox"/>	*.mpg.citrix.com		Up to date	2016-04-20	2017-05-27	SSL Listener	✓
<input type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	2016-05-23	2036-05-21	Devices CA	
<input type="checkbox"/>	Verizon Public SureServer CA G14-SHA2		Up to date	2014-04-09	2021-04-09	Root or intermediate	
<input type="checkbox"/>	Baltimore CyberTrust Root		Up to date	2000-05-12	2025-05-12	Root or intermediate	

3. Compruebe que **Exportar clave privada** está establecido en **No**. Haga clic en **Exportar** para exportar el certificado al directorio de descargas.

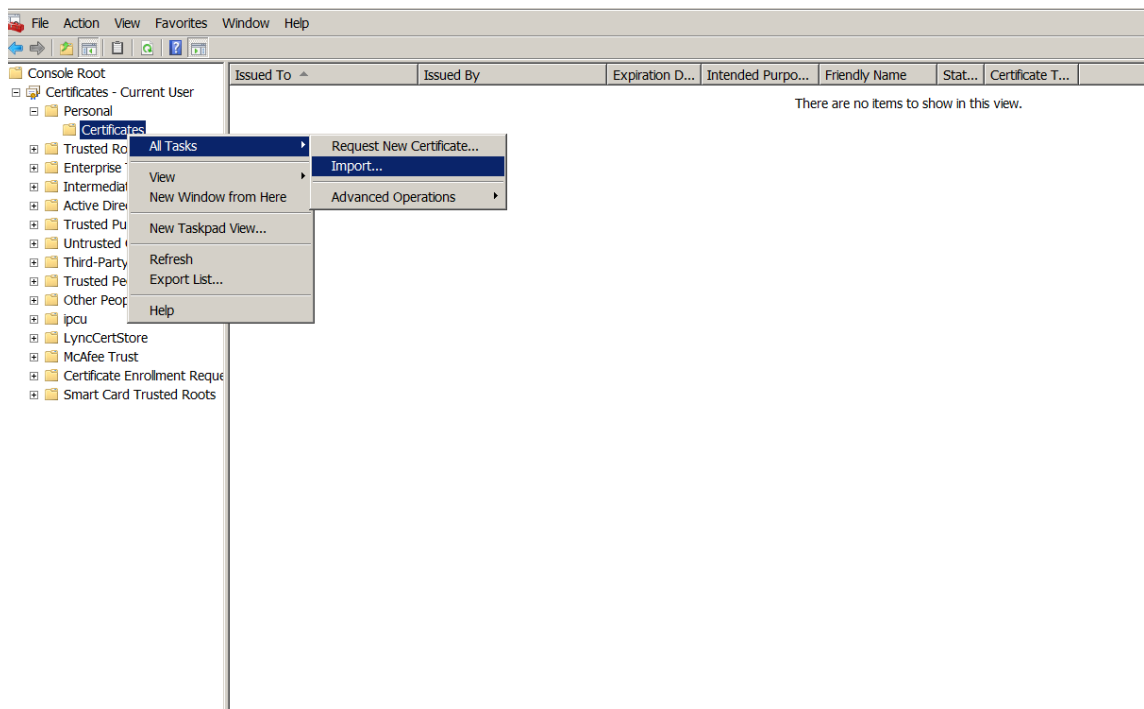


4. Busque el certificado en el directorio de descargas. El certificado raíz tiene el formato PEM.



Convertir el certificado de PEM a CER

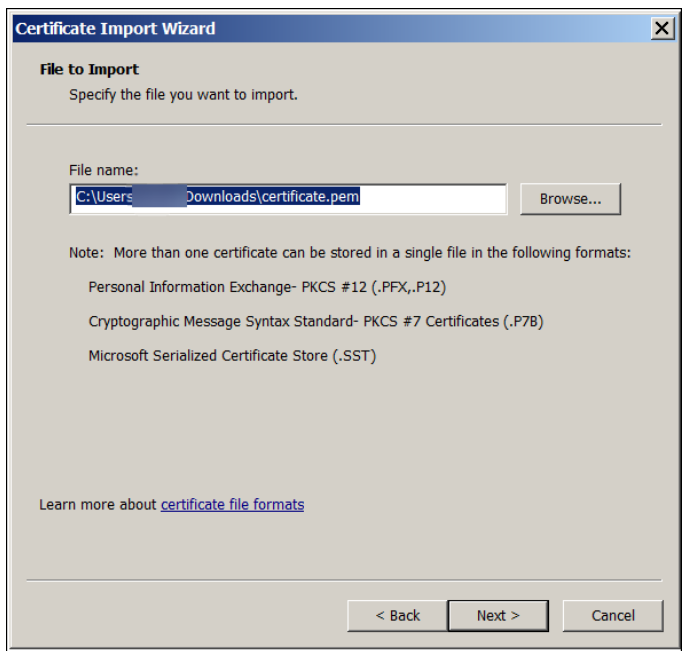
1. Abra Microsoft Management Console (MMC) y haga clic con el botón secundario en **Certificados** > **Todas las tareas** > **Importar**.



2. Cuando aparezca el asistente para la importación de certificados, haga clic en **Siguiente**.

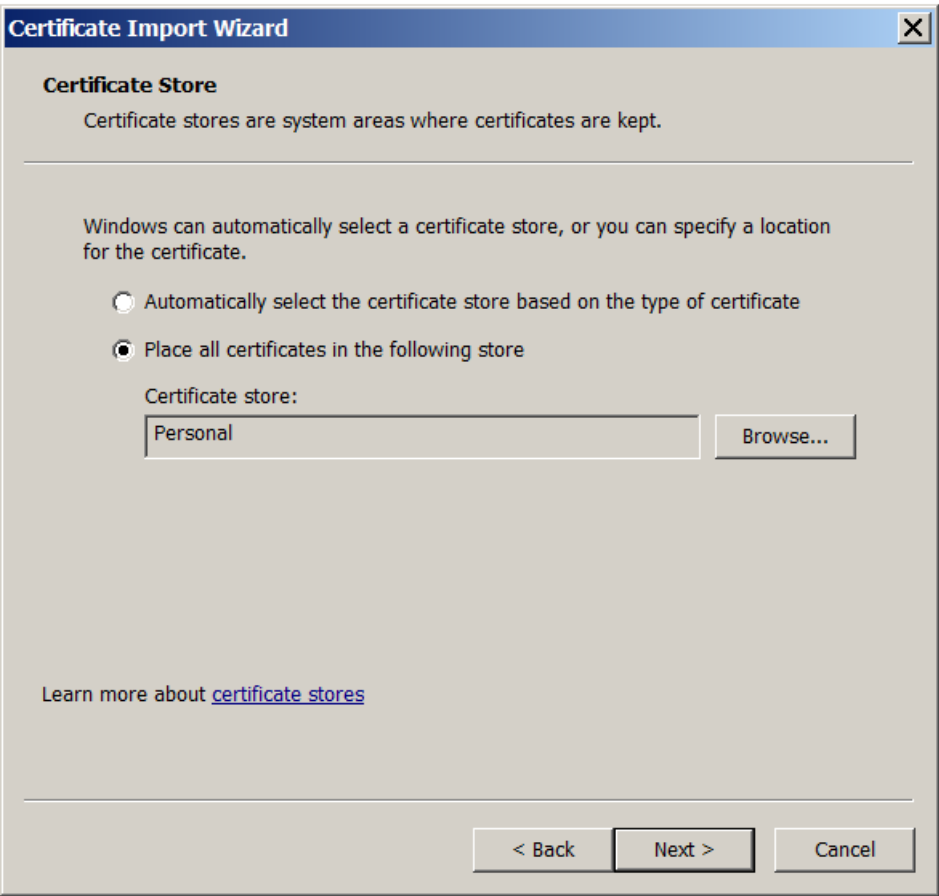


3. Vaya al certificado ubicado en el directorio de descargas.

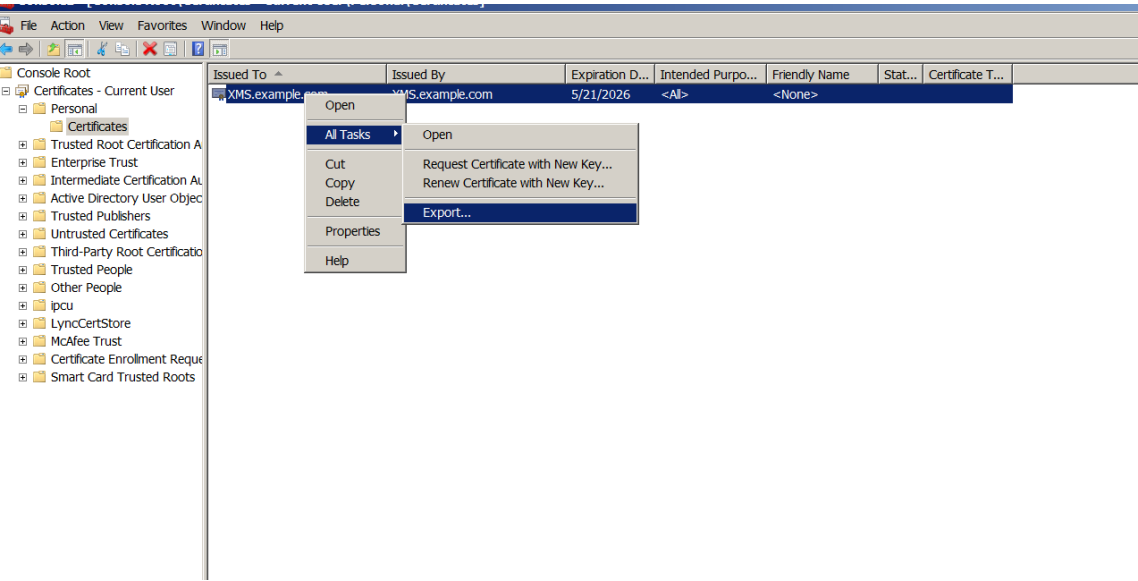


4. Seleccione **Colocar todos los certificados en el siguiente almacén** y, a continuación, selec-

cione **Personal** como almacén de certificados. Haga clic en **Siguiente**.



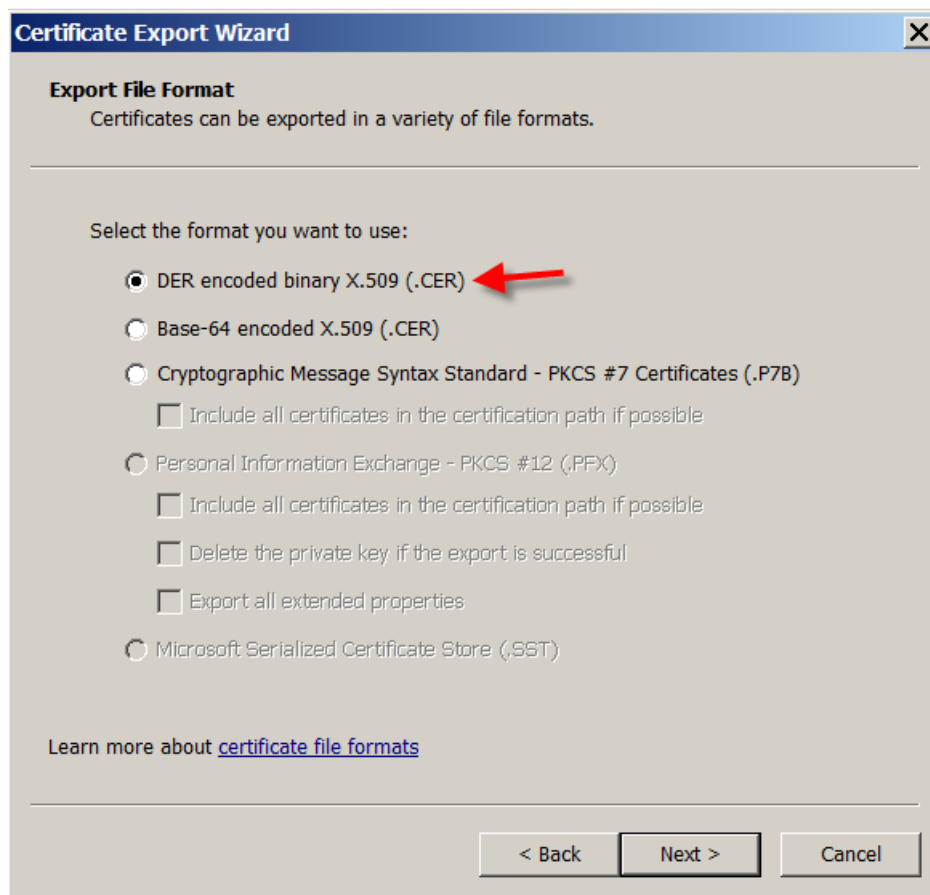
5. Revise los cambios y haga clic en **Finalizar**. Haga clic en **Aceptar** en la ventana de confirmación.
6. En la MMC, haga clic con el botón secundario en el certificado y seleccione **Todas las tareas > Exportar**.



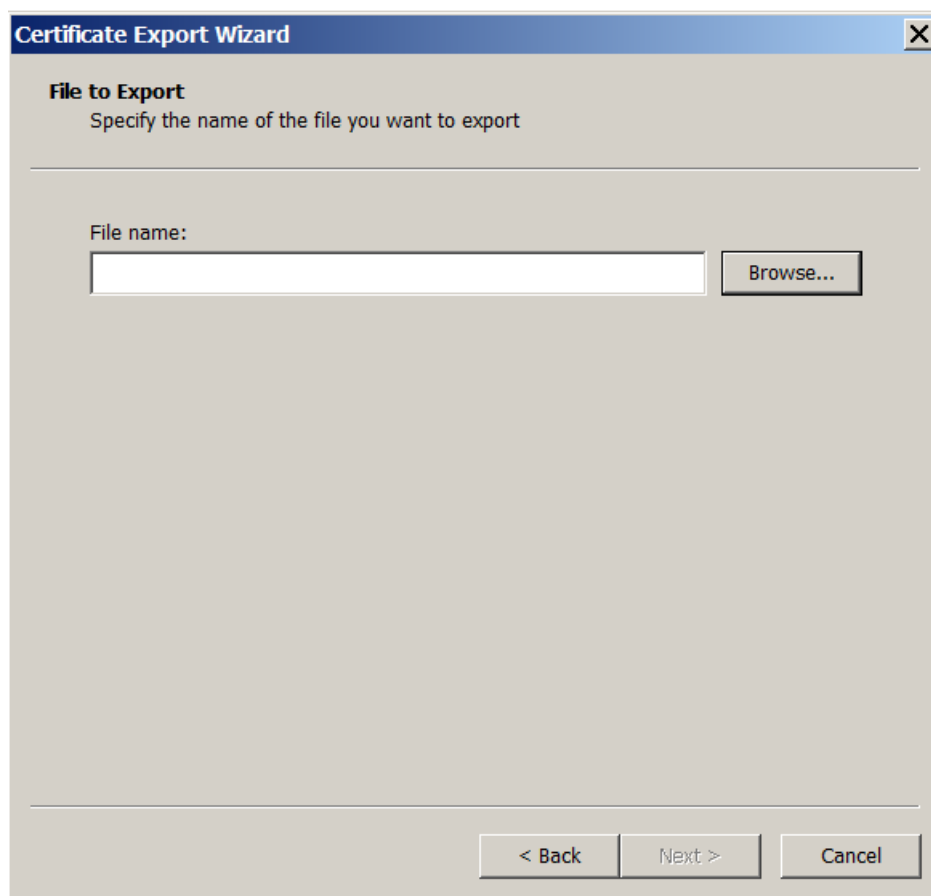
7. Cuando aparezca el asistente para la exportación de certificados, haga clic en **Siguiente**.



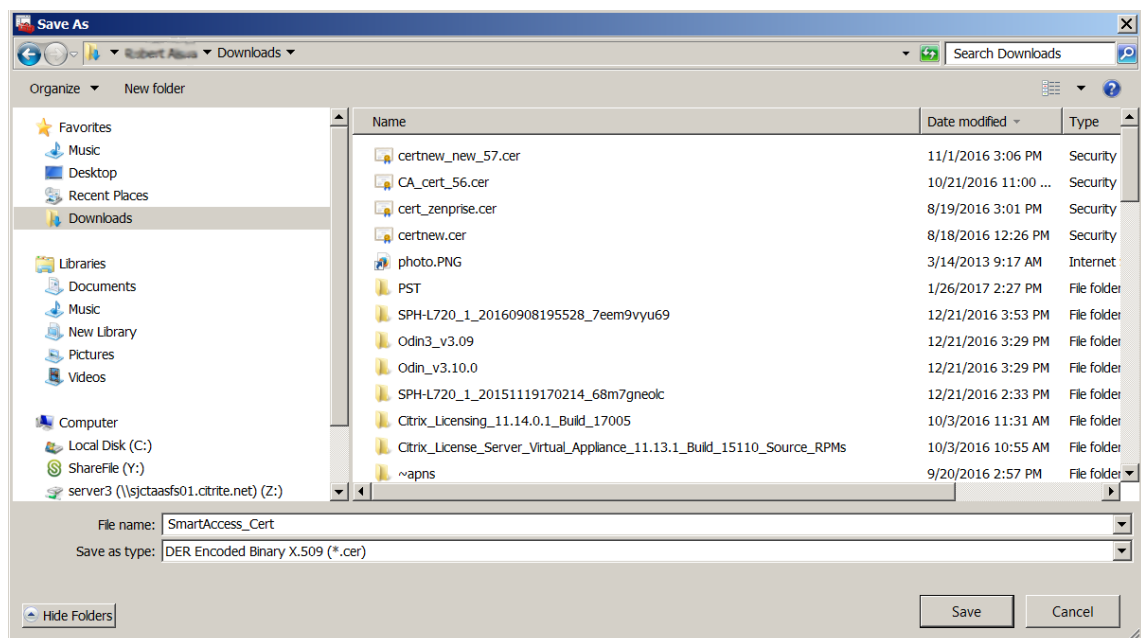
8. Seleccione el formato **DER binario codificado X.509 (.CER)**. Haga clic en **Siguiente**.



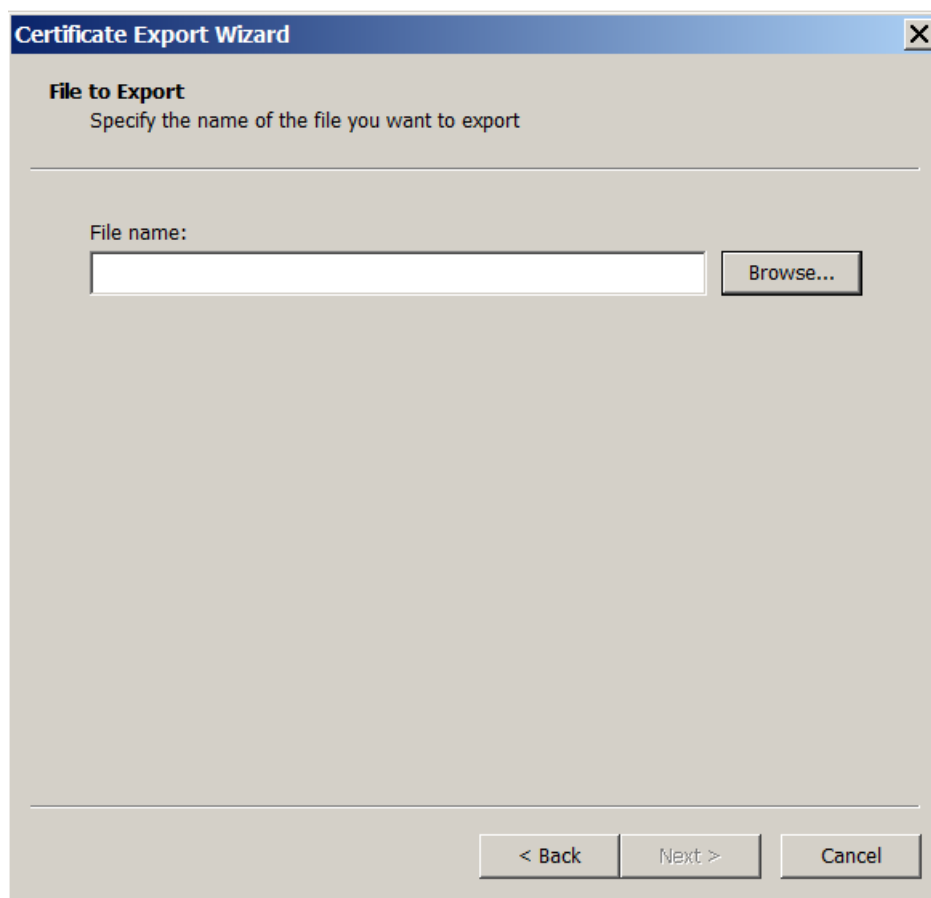
9. Vaya al certificado. Escriba un nombre para el certificado y haga clic en **Siguiente**.



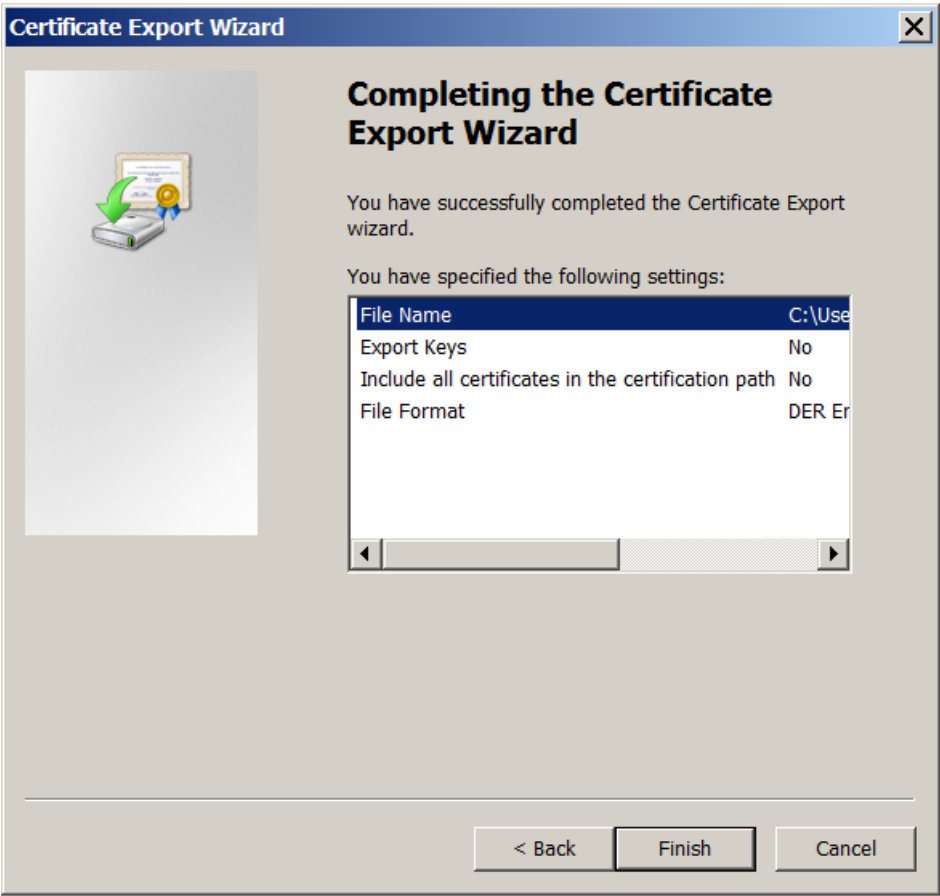
10. Guarde el certificado.



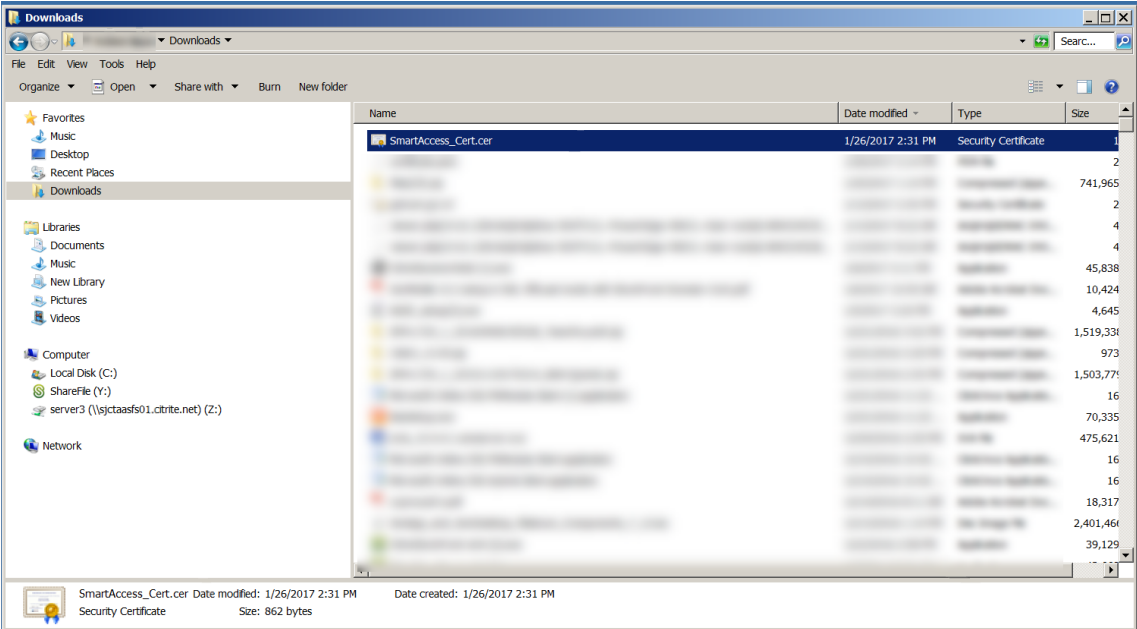
11. Vaya al certificado y haga clic en **Siguiente**.



12. Revise los cambios y haga clic en **Finalizar**. Haga clic en **Aceptar** en la ventana de confirmación.

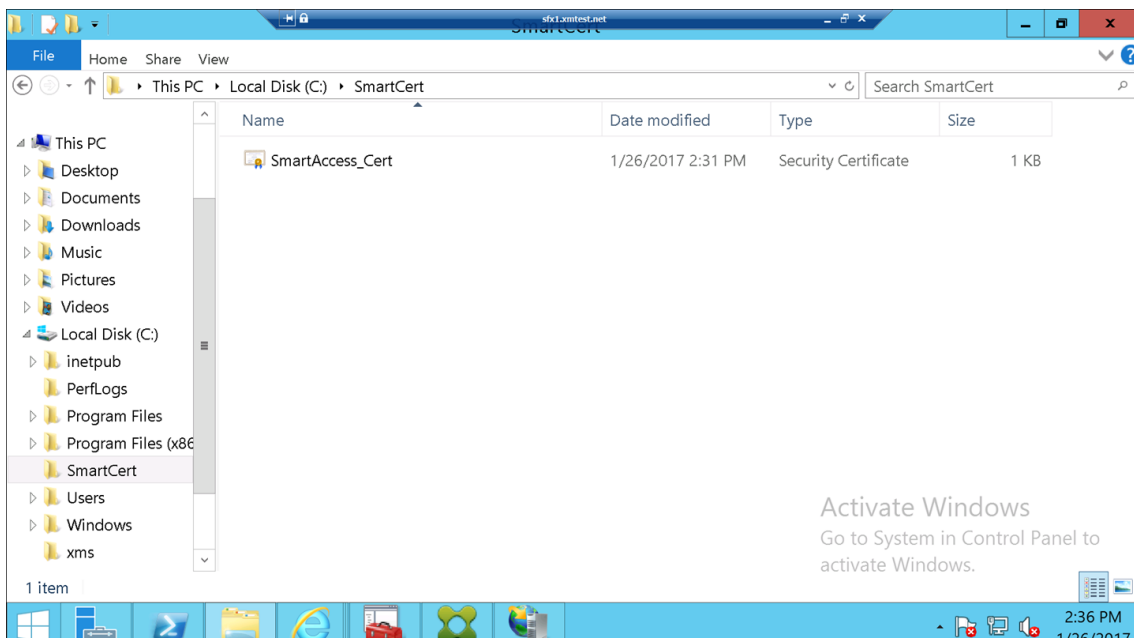


13. Busque el certificado en el directorio de descargas. El certificado está en formato CER.



Copiar el certificado al servidor de StoreFront

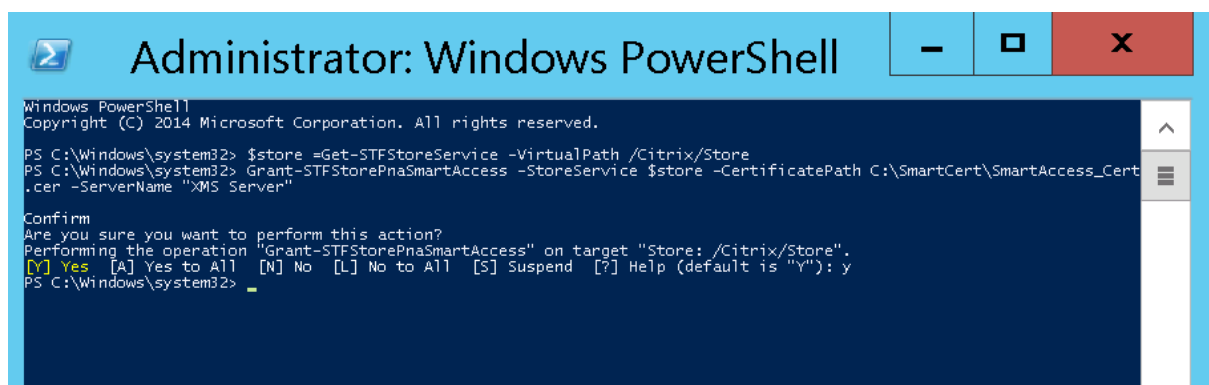
1. En el servidor de StoreFront, cree una carpeta llamada **SmartCert**.
2. Copie el certificado a la carpeta **SmartCert**.



Configurar el certificado en el almacén de StoreFront

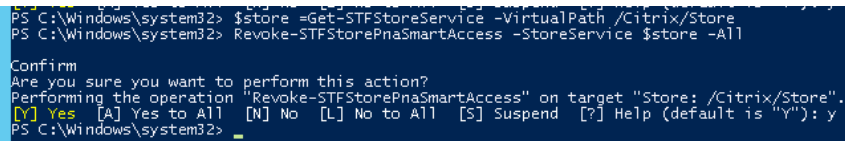
En el servidor de StoreFront, ejecute el siguiente comando de PowerShell para configurar el certificado del servidor Citrix Endpoint Management convertido que se encuentra en el almacén:

```
1 Grant-STFStorePnaSmartAccess -StoreService $store -
   CertificatePath "C:\xms\xms.cer" -ServerName "XMS server"
2 <!--NeedCopy-->
```



Si ya hay certificados existentes en el almacén de StoreFront, ejecute este comando de PowerShell para revocarlos:

```
1 Revoke-STFStorePnaSmartAccess - StoreService $store - All
2 <!--NeedCopy-->
```



```
PS C:\Windows\system32> $store = Get-STFStoreService -VirtualPath /Citrix/Store
PS C:\Windows\system32> Revoke-STFStorePnaSmartAccess -StoreService $store -All
Confirm
Are you sure you want to perform this action?
Performing the operation "Revoke-STFStorePnaSmartAccess" on target "Store: /Citrix/Store".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
PS C:\Windows\system32>
```

También 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:

```
1 $store = Get-STFStoreService - VirtualPath /Citrix/Store
2
3 Revoke-STFStorePnaSmartAccess - StoreService $store - ServerName "
  My XM Server"
4 <!--NeedCopy-->
```

- Revocar por huella digital:

```
1 $store = Get-STFStoreService - VirtualPath /Citrix/Store
2
3 Revoke-STFStorePnaSmartAccess - StoreService $store -
  CertificateThumbprint "[Thumbprint]"
4 <!--NeedCopy-->
```

- Revocar por objeto de servidor:

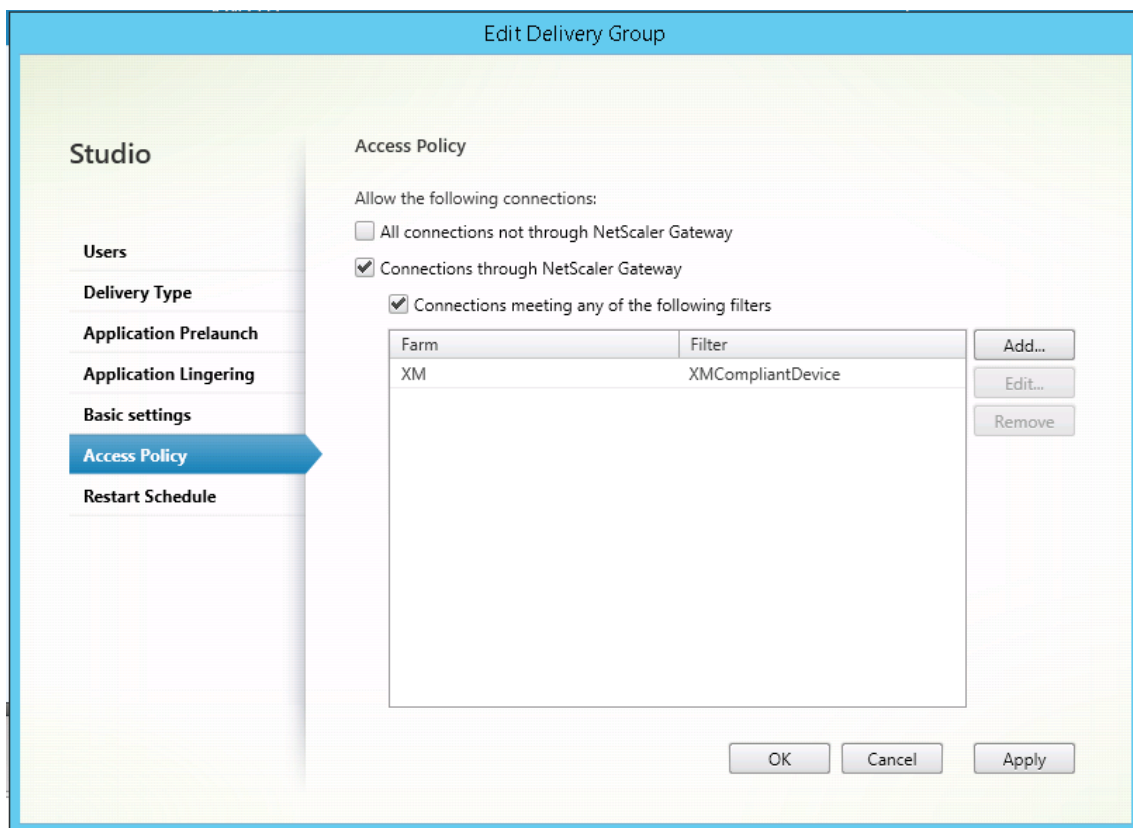
```
1 $store = Get-STFStoreService - VirtualPath /Citrix/Store
2
3 $access = Get-STFStorePnaSmartAccess - StoreService $store
4
5 Revoke-STFStorePnaSmartAccess - StoreService $store - SmartAccess
  $access.AccessConditionsTrusts[0]
6 <!--NeedCopy-->
```

Configurar la directiva de SmartAccess para Citrix Virtual Apps and Desktops

Para agregar la directiva de SmartAccess requerida al grupo que entrega 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 el grupo que entrega las aplicaciones a las que quiere controlar el acceso. Seleccione **Modificar grupo de entrega** en el panel **Acciones**.

4. En la página **Directiva de acceso**, seleccione **Conexiones a través de NetScaler Gateway** y **Conexiones que cumplan cualquiera de estos filtros**.
5. Haga clic en **Agregar**.
6. Agregue una directiva de acceso donde **Comunidad** es **XM** y **Filtro** es **XMCompliantDevice**.



7. Haga clic en **Aplicar** para aplicar los cambios que haya hecho y dejar la ventana abierta, o bien haga clic en **Aceptar** para aplicar los cambios y cerrar la ventana.

Establecer acciones automatizadas en Citrix Endpoint Management

La directiva de SmartAccess que se estableció en el grupo de entrega para una aplicación HDX deniega el acceso a un dispositivo cuando el dispositivo no es conforme. Puede utilizar acciones automatizadas para marcar el dispositivo como no conforme.

Devices									
<div> Add Import Export Refresh </div> <div> <div>Devices</div> <div>Show filter</div> <div>Search</div> </div>									
<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	Out of Compliance
<input type="checkbox"/>		MDM MAM	[redacted]	iOS	8.1	iPad	06/29/2016 10:37:56 am	212 days	
<input type="checkbox"/>		MDM MAM	[redacted]	iOS	10.2	iPhone	01/27/2017 10:10:59 am	0 day	True
<div>Showing 1 - 2 of 2 items</div> <div>Items per page: 10</div>									

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Acciones**. Aparecerá la página **Acciones**.
2. Haga clic en **Agregar** para agregar una acción. Aparecerá 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**. Aparecerá 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 la propiedad de usuario **eng5** o **eng6**.

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
-----------------	------	-------	----------------	-----------	---------------------	-----------------

Actions

- 1 Action Info
- 2 Details**
- 3 Assignment (optional)
- 4 Summary

Action details

Choose a trigger event and the associated action for that event.

Trigger

User property

Name

Is

eng5 eng6

Action

Mark the device as out of compliance

Is

True

0

Hours

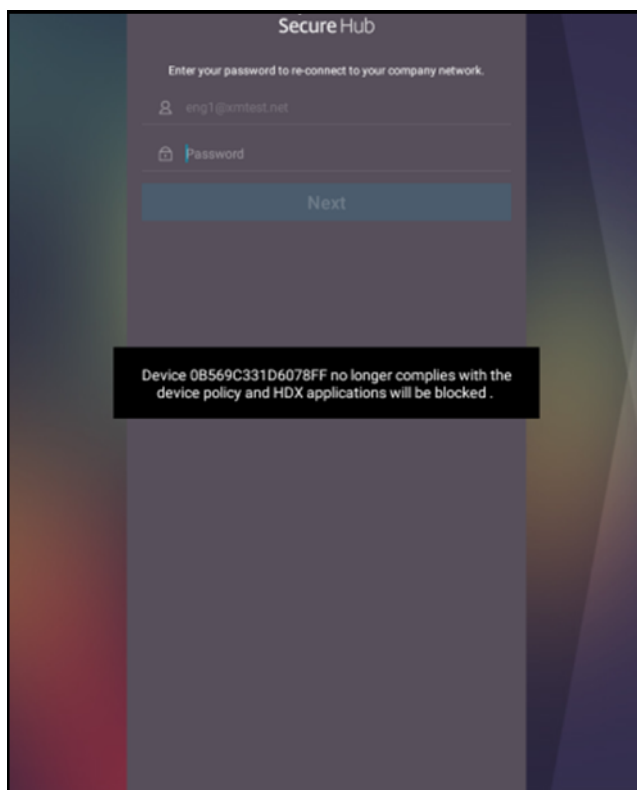
5. En la lista **Desencadenador**, elija **Propiedad de dispositivo**, **Propiedad de usuario** o **Nombre de la aplicación instalada**. SmartAccess no admite desencadenadores de eventos.
6. En la lista **Acción**:
 - Elija **Marcar dispositivo como No conforme**.
 - Elija **Es**.
 - Elija **Verdadero**.
 - Para que el dispositivo se marque como no conforme en cuanto se cumpla la condición del desencadenador, establezca el marco de tiempo en **0**.

7. Elija el grupo o 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, seleccione **Guardar**.

Cuando el dispositivo se marca como no conforme, las aplicaciones HDX ya no aparecen en el almacén Citrix Secure Hub. El usuario ya no está suscrito a la aplicación. No se envía ninguna notificación al dispositivo y nada en el almacén Citrix Secure Hub indica que las aplicaciones HDX estaban disponibles anteriormente.

Si quiere que se notifique a los usuarios cuando un dispositivo se marque como no conforme, cree una notificación y luego cree una acción automatizada para enviar esa notificación.

En este ejemplo se crea y se envía esta notificación cuando un dispositivo se marca como no conforme: “El número de serie o el número de teléfono del dispositivo ya no sigue la directiva de dispositivo y las aplicaciones HDX se bloquearán”.



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 con forma de engranaje, situado en la esquina superior derecha de la consola. Aparecerá la página **Parámetros**.
2. Haga clic en **Plantillas de notificaciones**. Aparecerá la página **Plantillas de notificaciones**.

3. Haga clic en **Agregar** para agregar una nueva plantilla de notificaciones en la página **Plantillas de notificaciones**.

4. Configure estos parámetros:

- **Nombre:** Bloqueo de aplicaciones HDX
- **Descripción:** Notificación del agente cuando el dispositivo no es conforme
- **Tipo:** Notificación ad hoc
- **Citrix Secure Hub:** Activado
- **Mensaje:** El dispositivo `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}` ya no sigue la directiva de dispositivo. Las aplicaciones HDX se bloquearán.

The screenshot shows the configuration interface for a notification template. The fields are as follows:

- Name:** HDX Application Block
- Description:** (Empty text area)
- Type:** Ad-Hoc Notification (Dropdown menu)
- SMTP:** Activate (Green button)
- Sender:** (Empty text field)
- Recipient:** (Empty text field)
- Subject:** (Empty text field)
- Message:** (Empty text area)
- Secure Hub:** Activated (Green button), Deactivate (Grey button)
- Message* (Preview):** Device `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` no longer complies with the device policy and HDX applications will be blocked.

Buttons: Cancel, Save

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 agregar una acción. Aparecerá la página **Información de la acción**.
3. En la página **Información de la acción**, escriba un nombre y una descripción para la acción:
 - **Nombre:** Notificación de HDX bloqueado
 - **Descripción:** Notificación de HDX bloqueado porque el dispositivo no es conforme

4. Haga clic en **Siguiente**. Aparecerá la página **Detalles de la acción**.

5. En la lista **Desencadenador**:

- Elija **Propiedad de dispositivo**.
- Elija **No conforme**.
- Elija **Es**.
- Elija **Verdadero**.

The screenshot shows the 'Detalles de la acción' (Action Details) page in Citrix Endpoint Management. The page is divided into two main sections: 'Trigger' and 'Action'. The 'Trigger' section includes dropdown menus for 'Device property', 'Out of compliance', 'Is', and 'True'. The 'Action' section includes dropdown menus for 'Send notification' and 'HDX Application Block', a text input field for 'Preview notification message' with the value '0', a dropdown menu for 'Minutes', and a text input field for 'Specify an action repeat interval' with a dropdown menu for 'Days'. A 'Next >' button is located at the bottom right of the page.

6. En la lista **Acción**, especifique las acciones que se producen cuando se cumple el desencadenador:

- Elija **Enviar notificación**.
- Elija **Bloqueo de aplicaciones HDX, la notificación que ha creado**.
- Elija **0**. Si este valor es 0, la notificación se enviará 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, se ha elegido **AllUsers**.

8. Revise el resumen de la acción.

9. Haga clic en **Siguiente** y, a continuación, seleccione **Guardar**.

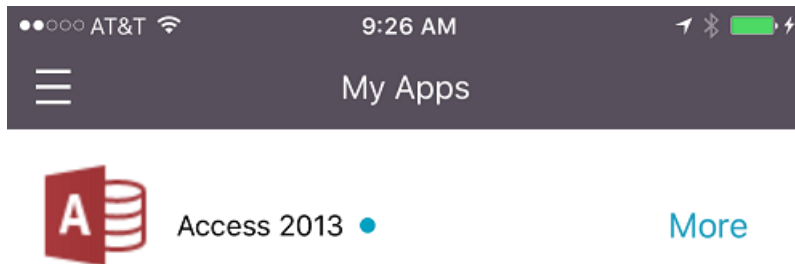
Para obtener información detallada acerca de la configuración de acciones automatizadas, consulte [Acciones automatizadas](#).

Cómo los usuarios recuperan el acceso a las aplicaciones HDX

Los usuarios pueden volver a obtener el acceso a las aplicaciones HDX después de que el dispositivo vuelva a ser conforme:

1. En el dispositivo, vaya al almacén Citrix Secure Hub para actualizar las aplicaciones en el almacén.
2. Vaya a la aplicación y toque **Agregar** en la aplicación.

Una vez agregada la aplicación, aparece en “Mis aplicaciones” con un punto azul, porque es una aplicación recién instalada.



Actualizar la versión de aplicaciones MDX o de empresa

November 29, 2023

En Citrix Endpoint Management, para actualizar la versión de una aplicación MDX o de empresa, debe inhabilitarla en la consola de Citrix Endpoint Management y cargar luego la nueva versión de esta.

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Aplicaciones**. Aparecerá la página **Aplicaciones**.
2. En el caso de dispositivos administrados (dispositivos inscritos en Citrix Endpoint Management con la Administración de dispositivos móviles), vaya directamente al paso 3. En el caso de dispositivos no administrados (dispositivos inscritos en Citrix Endpoint Management solo para la administración de aplicaciones empresariales), lleve a cabo lo siguiente:
 - a) Para actualizar una aplicación, en la tabla **Aplicaciones**, marque la casilla situada junto a dicha aplicación o haga clic en la línea que la contiene.

b) Haga clic en **Inhabilitar** en el menú que aparecerá.

Apps

Use the [MDX Service](#) on Citrix Cloud to wrap an app for delivery.

Add | Category | Export

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input checked="" type="checkbox"/>		Secure Web	MDX	Default	4/3/20 9:42:58 am	4/3/20 9:43:04 am	
<input type="checkbox"/>		Secure Mail	MDX	Default			
<input type="checkbox"/>		Citrix Files	MDX	Default			
<input type="checkbox"/>		AE App add	Public App Store	Default			
<input type="checkbox"/>		AE google chrome	Public App Store	Default			
<input type="checkbox"/>		Podio	Public App Store	Default			
<input type="checkbox"/>		AE App	Public App Store	Default			

Showing 1-7 of 7 items Items per page: 10

Deployment

0 Installed 0 Pending 0 Failed

Show more >

c) Haga clic en **Inhabilitar** en el cuadro de diálogo de confirmación. Aparecerá la etiqueta *Inhabilitada* en la columna **Inhabilitar** de la aplicación.

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		Secure Web	MDX	Default	4/3/20 9:42:58 am	4/3/20 9:43:04 am	Disabled
<input type="checkbox"/>		Secure Mail	MDX	Default	4/3/20 9:43:09 am	4/3/20 9:43:16 am	

Nota:

Mientras la aplicación está inhabilitada, los usuarios no pueden volver a conectarse a ella después de cerrar sesión. Inhabilitar una aplicación es opcional, aunque se recomienda inhabilitarla para evitar problemas de funcionalidad. Por ejemplo, es posible que los usuarios que soliciten descargar la aplicación al mismo tiempo que usted carga la nueva versión tengan problemas.

- Para actualizar una aplicación, en la tabla **Aplicaciones**, marque la casilla situada junto a dicha aplicación o haga clic en la línea que la contiene.
- Haga clic en **Modificar** en el menú que aparecerá. Aparecerá la página **Información de la aplicación**, con las plataformas que ha elegido para la aplicación seleccionada.
- Configure estos parámetros:
 - **Nombre:** Si quiere, puede cambiar el nombre de la aplicación.
 - **Descripción:** Si quiere, puede cambiar la descripción de la aplicación.
 - **Categoría de la aplicación:** Si quiere, puede cambiar la categoría de aplicación.
- Haga clic en **Siguiente**. Aparecerá la página de la primera plataforma seleccionada. Lleve a cabo lo siguiente para cada plataforma seleccionada:
 - Elija el archivo de sustitución que quiera cargar. Para ello, haga clic en **Cargar** y vaya a la ubicación del archivo. La aplicación se carga en Citrix Endpoint Management.

Si va a cargar una aplicación para Android Enterprise, aparecerá una ventana de Google Play administrado. Cargue la nueva versión de la aplicación aquí. Para obtener más información detallada, consulte [Distribuir aplicaciones de Android Enterprise](#).

- b) Si quiere, puede cambiar los datos de la aplicación y la configuración de directiva para la plataforma.
 - c) También puede configurar unas reglas de implementación y el almacén de aplicaciones. Para obtener más información, consulte [Agregar una aplicación MDX](#).
7. Haga clic en **Guardar**. Aparecerá la página **Aplicaciones**.
 8. Si ha inhabilitado la aplicación en el paso 2, haga lo siguiente:
 - a) En la ficha **Aplicaciones**, haga clic para seleccionar la aplicación actualizada y, en el menú que aparece, haga clic en **Habilitar**.
 - b) En el cuadro de confirmación que aparece, haga clic en **Habilitar**. Ahora, los usuarios podrán acceder a la aplicación y recibir una notificación que les pedirá actualizar la versión de la aplicación.

Agregar contenido multimedia

March 1, 2024

Puede agregar contenido multimedia a Citrix Endpoint Management para implementarlo en los dispositivos de usuario. Asimismo, puede utilizar Citrix Endpoint Management para implementar libros de Apple Books que obtiene a través de las compras por volumen de Apple.

Después de configurar una cuenta de compras por volumen en Citrix Endpoint Management, los libros gratuitos y adquiridos que posea aparecerán en **Configurar > Medios**. Los libros se configuran para la implementación en dispositivos iOS desde las páginas **Multimedia**. Para implementarlos, debe elegir grupos de entrega y especificar reglas de implementación.

La primera vez que el usuario recibe un libro y acepta la licencia de compras por volumen, los libros implementados se instalan en el dispositivo. Los libros aparecen en la aplicación Apple Books. La licencia de un libro no se puede desasociar del usuario; tampoco se puede quitar el libro del dispositivo. Citrix Endpoint Management instala libros como contenido multimedia obligatorio. Aunque un usuario elimine un libro instalado en el dispositivo, ese libro permanecerá en la aplicación Apple Books, listo para la descarga.

Requisitos previos

- Dispositivos iOS

- Configure las compras por volumen de Apple en Citrix Endpoint Management, como se describe en [Compras por volumen de Apple](#).

Configurar libros

Los libros de Apple Books obtenidos mediante las compras por volumen aparecen en la página **Configurar > Multimedia**.

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
Media Show filter <input type="text" value="Search"/>						
<input type="checkbox"/>	Icon	Media Name	Type	Created On	Last Updated	Vpp Account
<input type="checkbox"/>		The Wonderful Wizard of Oz - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:41 PM	test
<input type="checkbox"/>		Cool Werewolf Jokes For Kids - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:28 PM	test
<input type="checkbox"/>		Science Fiction Stories - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:32 PM	test
<input type="checkbox"/>		Coming Out - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:45 AM	test
<input type="checkbox"/>		Short Stories - VPP	Apple iBooks	6/15/17 1:29 PM	6/15/17 1:29 PM	test
<input type="checkbox"/>		A Diamond in My Pocket - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:39 AM	test
Showing 1 - 6 of 6 items Items per page: 10						

Para configurar un libro de Apple Books para la implementación

1. En **Configurar > Multimedia**, seleccione un libro y haga clic en **Modificar**. Aparecerá la página **Información del libro**.

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
iBook						
Book Information						
1 Book Information						
2 Platform						
iPhone						
iPad						
3 Delivery Group Assignments (optional)						
Name* Cool Werewolf Jokes For Kids - VPP ⓘ						
Description Cool Werewolf Jokes For Kids - VPP ⓘ						

El **Nombre** y la **Descripción** solo aparecen en los registros y la consola de Citrix Endpoint Management.

2. En las páginas **Parámetros de iBook para iPhone** y **Parámetros de iBook para iPad**, puede cambiar el nombre y la descripción del libro, aunque Citrix recomienda no cambiar estos parámetros. La imagen es para su información; este campo no se puede modificar. **iBook de pago** indica que el libro se ha adquirido a través de las compras por volumen de Apple.

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery Groups

iBook

1 Book Information

2 Platform

iPhone

iPad

3 Delivery Group Assignments (optional)

iPhone iBook Settings

Type a book title or keyword in the field and search for your desired iBook. Once you choose the iBook in the results, you can configure how the iBook appears in the store.

iBook Details

Name*

Cool Werewolf Jokes For Kids

Description*

Cool Werewolf Jokes For Kids - VPP

Image

Paid iBook

ON

► Deployment Rules

► Volume Purchase Program

También puede especificar reglas de implementación o ver la información de las compras por volumen.

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery Groups

iBook

1 Book Information

2 Platform

iPhone

iPad

3 Delivery Group Assignments (optional)

Paid iBook

ON

► Deployment Rules

▼ Volume purchase

Volume purchase License

Use Volume purchase company token

Volume purchase Account

test

Volume purchase ID Assignment

License Usage: 6 of 10

<input type="checkbox"/>	License ID	Usage Status	Associated User
<input type="checkbox"/>		Used	
<input type="checkbox"/>		Used	
<input type="checkbox"/>		Used	
<input type="checkbox"/>		Used	
<input type="checkbox"/>		Used	
<input type="checkbox"/>		Used	

Showing 1 - 6 of 6 items

3. Si lo prefiere, asigne el libro a grupos de entrega y configure una programación de implementación.

Device PoliciesAppsMediaActionsShareFileEnrollment ProfilesDelivery Groups

iBook

1 Book Information

2 Platform

iPhone

iPad

3 Delivery Group Assignments (optional)

Delivery Group Assignments (optional)

Assign this book to one or more delivery groups.

Choose delivery groups

Type to search

Search

☐ AllUsers

☐ test

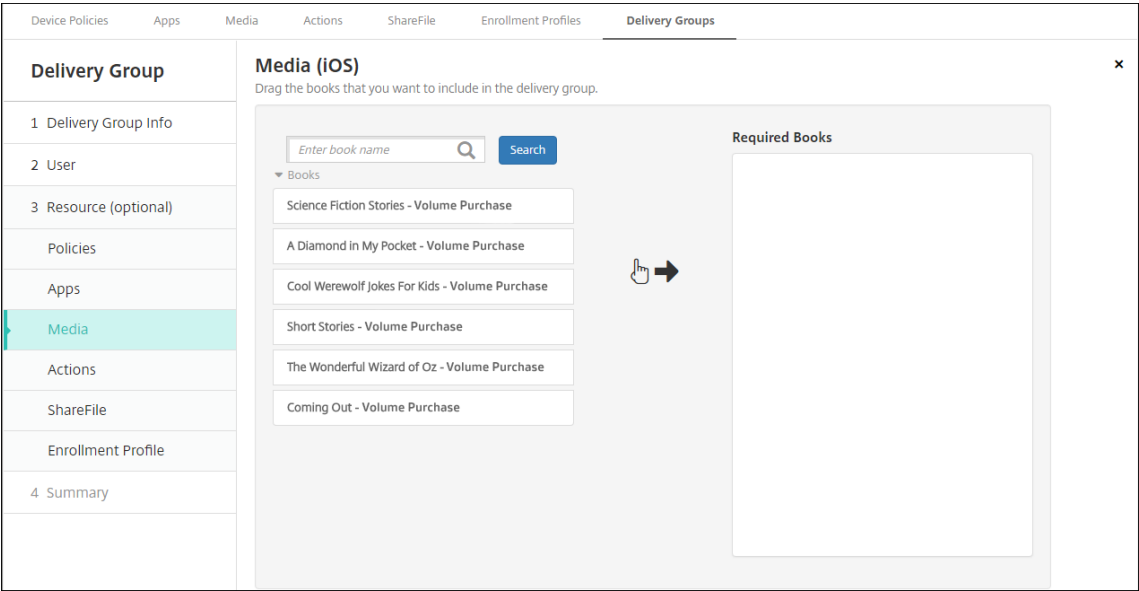
☐ as_grp_citrixw

► Deployment Schedule ⓘ

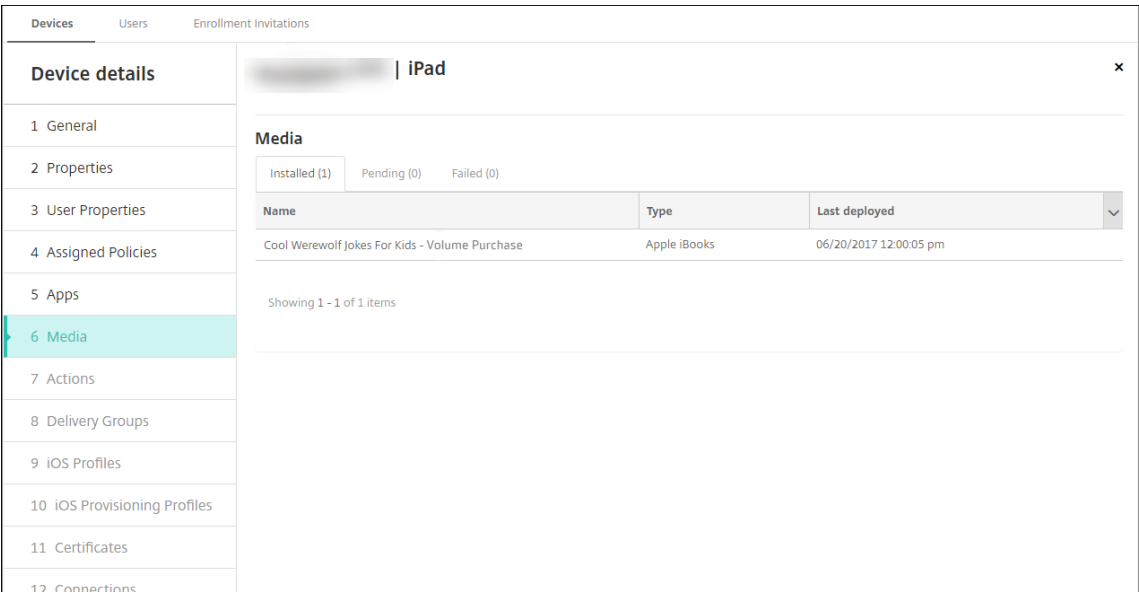
© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1062

También puede asignar libros a grupos de entrega desde la ficha **Multimedia** de **Configurar > Grupos de entrega**. Citrix Endpoint Management solo admite la implementación de libros obligatorios.



4. Puede ver el estado de la implementación desde la ficha **Multimedia** de **Administrar > Dispositivos**.

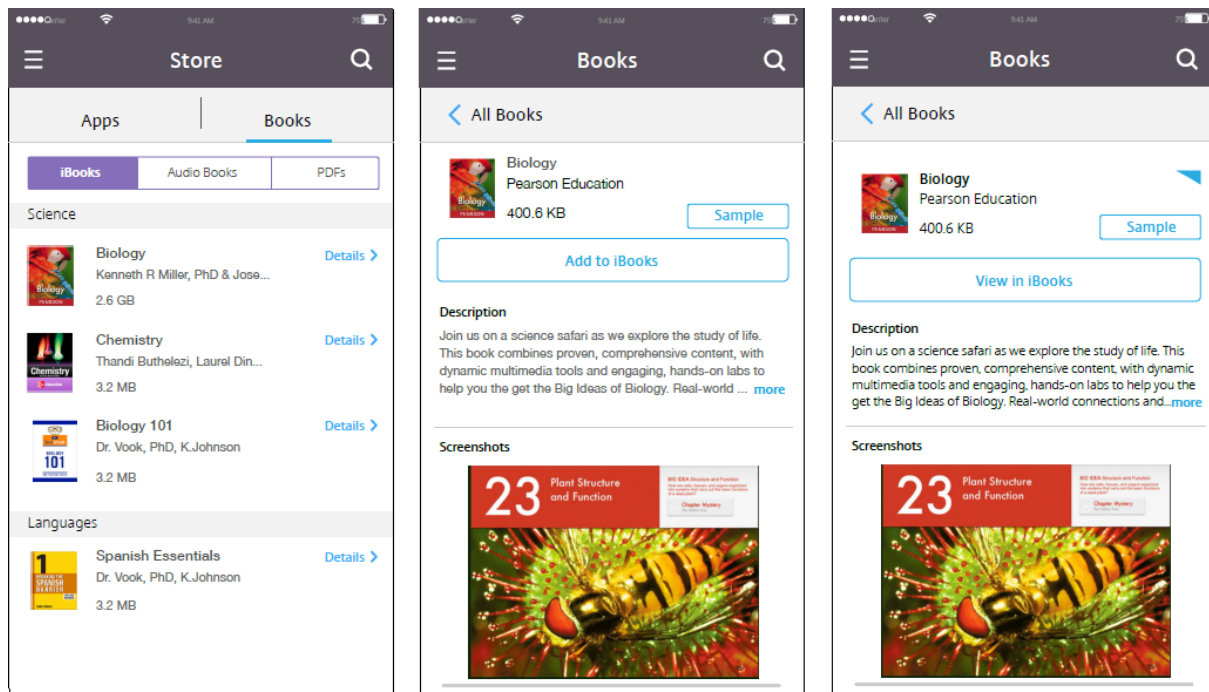


Nota:

En la página **Configurar > Medios**, si selecciona un libro y hace clic en **Eliminar**, Citrix Endpoint Management elimina ese libro de la lista. No obstante, la próxima vez que Citrix Endpoint Management se sincronice con las compras por volumen de Apple, el libro volverá a aparecer en la lista a menos que se haya quitado de las compras por volumen de

Apple. Eliminar un libro de la lista no lo quita del dispositivo.

Los libros aparecen en los dispositivos de usuario como se muestra en el siguiente ejemplo.



Implementar recursos

March 1, 2024

La configuración y la administración de dispositivos suelen implicar la creación de recursos (directivas, aplicaciones y contenido multimedia) y acciones en la consola de Citrix Endpoint Management y, posteriormente, su empaquetado por grupos de entrega. Los grupos de entrega definen categorías de usuarios para que pueda implementar en sus dispositivos directivas, aplicaciones, contenido multimedia y acciones que se hayan especificado. 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 incluido en varios grupos de entrega que tienen directivas duplicadas o contradictorias, Citrix Endpoint Management determina el orden de implementación. Consulte Pasos para el cálculo.

Acerca de los grupos de entrega

Por regla general, la inclusión en un grupo de entrega se basa en las características de los usuarios (por ejemplo, la empresa, el país, el departamento, el título y la dirección de la oficina). Los grupos de entrega permiten ejercer más control sobre quién obtiene qué recursos y cuándo lo hacen. Puede implementar un grupo de entrega en todos los usuarios o en un grupo definido de usuarios.

La instalación y configuración de Citrix Endpoint Management crea el grupo de entrega predeterminado, AllUsers. Este grupo contiene todos los usuarios locales y de Active Directory. No se puede eliminar el grupo AllUsers, pero sí se puede inhabilitar cuando no interese enviar recursos a todos los usuarios. Para obtener información detallada, consulte [Habilitar e inhabilitar el grupo de entrega AllUsers](#).

Al implementar un recurso en un grupo de entrega, se envía una notificación push a todos los usuarios del grupo de entrega. Para los dispositivos Apple, use el servicio de notificaciones push (APNs) de Apple para enviar notificaciones. Para obtener más información, consulte [Certificados APNs](#). Para dispositivos Android, use Firebase Cloud Messaging (FCM). Para obtener más información, consulte [Firebase Cloud Messaging](#). Para dispositivos Windows, use el servicio de notificaciones push de Windows (WNS).

Acerca de la implementación de recursos

Al trabajar en el envío de recursos a los dispositivos, tenga en cuenta lo siguiente:

- **Orden de implementación:** El orden de implementación es la secuencia que sigue Citrix Endpoint Management para enviar recursos (directivas, aplicaciones y contenido multimedia) y acciones a un dispositivo. El orden de implementación se aplica a los dispositivos de un grupo de entrega que tienen un perfil de inscripción configurado para la administración de dispositivos (MDM) o para una combinación de la administración de aplicaciones (MAM) y MDM.
- **Reglas de implementación:** Citrix Endpoint Management utiliza reglas de implementación que se especifican para las propiedades de los usuarios y los dispositivos con el fin de filtrar las directivas, las aplicaciones, las acciones, el contenido multimedia y los grupos de entrega. Por ejemplo, una regla de implementación puede especificar que debe enviarse el paquete de implementación cuando el nombre de dominio coincida con un valor determinado.

Dentro de un grupo de entrega, puede especificar un subconjunto de usuarios y dispositivos que reciban 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 implementación:** Citrix Endpoint Management utiliza la programación de la implementación especificada para acciones, aplicaciones, contenido multimedia y directi-

vas con el fin de controlar la implementación de esos elementos. Puede especificar que se produzca una implementación ahora, en una fecha y hora establecidas o cuando se cumplan ciertas condiciones de implementación. Especifique la programación al crear la regla. Consulte [Configurar las reglas de implementación](#).

Antes de agregar grupos de entrega, piense en cómo se relacionan el orden de implementación, las reglas y la programación con los objetivos de su implementación.

Orden de implementación

El orden de implementación es la secuencia con la que Citrix Endpoint Management envía recursos a los dispositivos. El orden de implementación es importante cuando existen requisitos previos para los recursos y dependencias entre los recursos. Los recursos incluyen directivas, aplicaciones, acciones y grupos de entrega.

Por ejemplo, si quiere aplicar una directiva de Wi-Fi con autenticación basada en certificados, debe aplicar la directiva de certificación antes que la directiva de Wi-Fi. De lo contrario, se producen errores. Por el contrario, para algunas directivas (como las de términos y condiciones, inventario de software y acciones), el orden de implementación no importa.

Al agregar 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 contradictorias. 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, tales como las reglas de implementación y la programación de la implementación, a los recursos. En esta tabla se muestra cuál de estos criterios puede aplicar a cada tipo de recurso.

Recurso	Plataforma del dispositivo	Reglas de implementación	Programación de la implementación	Usuario/Grupos
Directiva de dispositivo	S	S	S	-
Aplicación	S	S	S	-
Archivos multimedia	S	S	S	-
Acción	-	S	S	-
Grupo de entrega	-	S	-	S

Pasos para el 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. Identifica todos los grupos de entrega de un usuario específico, en función de los filtros de usuario, grupos y reglas de implementación.
2. Crea una lista ordenada de todos los recursos (directivas, acciones, contenido multimedia y aplicaciones) en los grupos de entrega seleccionados. La lista se basa en los filtros de plataforma de dispositivo, reglas de implementación y programación de la implementación. El algoritmo para ordenarlos es el siguiente:
 - a) Coloca los recursos de los grupos de entrega que tengan un orden de implementación definido por el administrador por delante de aquellos recursos de grupos de entrega que no lo tengan. Para obtener información detallada, consulte Ejemplo de cálculo con orden definido por el usuario.
 - b) En caso de haber dos grupos de entrega en las mismas circunstancias, ordena los recursos de los grupos de entrega por nombre de grupo en orden alfabético inverso. Por ejemplo, Citrix Endpoint Management coloca los recursos del grupo de entrega B por delante de los recursos del grupo de entrega A.
 - c) Durante el proceso de ordenamiento, si se especifica un orden definido por un administrador para los recursos de un grupo de entrega, mantiene ese orden. De lo contrario, los recursos del grupo de entrega se ordenan alfabéticamente por nombre de recurso.
 - d) Si el mismo recurso aparece más de una vez, quita el recurso duplicado. Entrega solo el primero de estos recursos.

Los recursos asociados a un orden definido por un administrador se implementan antes que los recursos sin un orden definido por un administrador.

Ejemplo de cálculo con orden definido por un administrador Supongamos que tiene dos grupos de entrega:

- Grupo de entrega Gestores de cuentas 1: Con un orden de recursos *no especificado*. Contiene las directivas **Red** y **Código de acceso**.
- Grupo de entrega Gestores de cuentas 2: Con un orden de recursos *especificado*. Contiene las directivas **Programación de conexiones**, **Restricciones**, **Código de acceso** y **Red** en orden.

Si el algoritmo de cálculo ordenara los grupos de implementación solo por nombre, Citrix Endpoint Management realizaría la implementación en este orden, empezando por el grupo de entrega Gestores de cuentas 1: **Red, Código de acceso, Programación de conexiones y Restricciones**. Citrix Endpoint Management omitiría **Código de acceso y Red**, por ser duplicados, del grupo de entrega Gestores de cuentas 2.

No obstante, 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 antes que los recursos del grupo de entrega Gestores de cuenta 1 en la lista. Como resultado, Citrix Endpoint Management implementa las directivas en este orden: **Programación de conexiones, Restricciones, Código de acceso y Red**. Citrix Endpoint Management omite las directivas **Red y Código de acceso** del grupo de entrega Gestores de cuentas 1, por ser duplicados. El algoritmo respeta el orden especificado por el administrador de Citrix Endpoint Management.

Configurar las reglas de implementación

Configurar las reglas de implementación para entregar recursos cuando se cumplan ciertas condiciones. Puede configurar reglas de implementación básicas o avanzadas.

▼ Deployment Rules

Base Advanced

Deploy when All conditions are met. New Rule

Deploy this resource rega... only shareable

Installed app name is equal to Secure Hub

Passcode compliant True

Manage cellular roaming domestic

Cuando agregue una regla de implementación con el editor de reglas básicas, seleccione primero cuándo implementar el recurso.

- **Todas:** Entregue el recurso cuando el usuario o dispositivo cumpla todas las condiciones que configure.
- **Cualquiera:** Entregue el recurso cuando el usuario o 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. Las reglas

disponibles varían en función del recurso que se implementará y la plataforma para la que se configura el recurso. Dentro de cada regla hay condiciones.

Puede especificar la implementación del recurso:

- Solo cuando se cumple la propiedad seleccionada o excepto cuando se cumple la propiedad seleccionada.
- Cuando la propiedad coincide exactamente con el texto que escribe, la propiedad contiene el texto que escribe o la propiedad no coincide con el texto que escribe.
- Cuando el dispositivo o el usuario cumplen con la propiedad seleccionada o no cumplen con la propiedad seleccionada.
- Cuando las propiedades del dispositivo o del usuario coinciden con una condición seleccionada de una lista predefinida.

Utilice el editor avanzado para crear reglas de implementación más complejas. Puede elegir más reglas y combinar distintos operadores lógicos booleanos al crear reglas avanzadas.

▼ Deployment Rules

Base **Advanced**

AND

- Passcode compliant True
- OR
- Installed app name contains Authenticator
- NOT
- Device ownership Unknown

AND OR NOT EDIT New Rule Delete

Trabajar con grupos de entrega

Puede trabajar con grupos de entrega de las siguientes formas:

- Agregar un grupo de entrega
- Implementación en grupos de entrega
- Eliminar un grupo de entrega
- Modificar un grupo de entrega
- Habilitar e inhabilitar el grupo de entrega AllUsers.

Agregar un grupo de entrega

Cuando crea un grupo de entrega, 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 va a usar el grupo de entrega para entregar otros servicios de Citrix Cloud, indique 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. Puede agregar usuarios de Active Directory solamente a grupos de entrega administrados en Citrix Cloud.

Si solo necesita administrar la movilidad de un grupo de entrega que contiene usuarios y aplicaciones, establezca **Administrar asignaciones de usuarios a En Citrix Endpoint Management**. En Citrix Cloud no se pueden ver grupos de entrega con usuarios administrados en Citrix Endpoint Management. Por lo tanto, no puede usar los grupos de entrega administrados en Citrix Endpoint Management para entregar otros servicios.

Nota:

Recomendamos agregar grupos de entrega antes de crear directivas de dispositivos 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.

The screenshot shows the 'Delivery Groups' configuration page in Citrix Endpoint Management. The left sidebar has a navigation menu with the following items: '1 Delivery Group Info', '2 Assignments' (selected), '3 Resource (optional)', 'Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profile', and '4 Summary'. The main content area is titled 'Assignments' and includes a sub-header 'Manage user assignments *'. There are two radio button options: 'In Endpoint Management' (selected) and 'In Citrix Cloud'. Below these are fields for 'Select domain' and 'Include user groups' with a search button. At the bottom, there are radio buttons for 'Or' and 'And', a toggle for 'Deploy to anonymous user', and links to 'Filter by User Properties' and 'Filter by Device Properties'.

- **Administrar asignaciones de usuarios:**

- **En Citrix Endpoint Management:** Seleccione esta opción si va a crear un grupo de entrega para usuarios y aplicaciones que necesitan solamente la administración de movilidad. En Citrix Cloud no se pueden ver los grupos de entrega cuyas asignaciones de usuarios se administran en Citrix Endpoint Management, y no se pueden utilizar para entregar otros servicios.
- **En Citrix Cloud:** Seleccione esta opción si quiere utilizar el grupo de entrega para entregar otros servicios. Estos servicios pueden incluir Citrix Virtual Apps and Desktops o ShareFile.

5. Agregue usuarios al grupo de entrega.

Importante:

No puede cambiar el parámetro **Administrar asignaciones de usuarios** una vez creado el grupo de entrega.

- **Seleccionar dominio:** En la lista, seleccione el dominio del que se elegirá a los usuarios.
- **Incluir grupos de usuarios:** Realice una de las siguientes acciones:

- En la lista de grupos de usuarios, haga clic en los grupos a agregar. Los grupos seleccionados aparecerán en la lista **Grupos de usuarios seleccionados**.
- Haga clic en **Buscar** para ver una lista de todos los grupos de usuarios del dominio seleccionado. También puede escribir el nombre completo o parcial de un grupo en el cuadro de búsqueda y, a continuación, hacer clic en **Buscar** para restringir 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** situada junto a cada grupo que quiera quitar.
 - Haga clic en **Buscar** para ver una lista de todos los grupos de usuarios del dominio seleccionado. También puede escribir el nombre completo o parcial de un grupo antes de hacer clic en **Buscar** para restringir la búsqueda. Desmarque la casilla de cada grupo que quiera quitar.
- **O/Y:** Seleccione si los usuarios pueden estar en cualquier grupo (O) o si deben estar en todos los grupos (Y) para que se implemente el recurso a ellos.
 - **Implementar para usuario anónimo:** Seleccione si implementar recursos para usuarios sin autenticar del grupo de entrega. Los usuarios sin autenticar son usuarios que no puede autenticar, pero a cuyos dispositivos les permitió conectarse a Citrix Endpoint Management de todas formas.
6. Expanda **Filtrar por propiedades de usuario** o **Filtrar por propiedades de dispositivo** para especificar cómo administrará los recursos el grupo de entrega.
- Si elige **Filtrar por propiedades de dispositivo**, expanda la plataforma del dispositivo para configurar las reglas de implementación:
 - **Propiedades del dispositivos: Android** (consulte Crear una regla para implementar recursos en dispositivos Android)
 - **Propiedades del dispositivo: iOS**
 - **Propiedades del dispositivo: Solo escritorio/tableta de Windows**
 - La ficha **Base** aparece de forma predeterminada. En la ficha **Base**, especifique cuándo implementar la directiva. Puede optar por implementar la directiva cuando se cumplan **todas** las condiciones o cuando se cumpla **cualquiera** de ellas. La opción predeterminada es **All**.
 - Haga clic en **Nueva regla** para definir las condiciones.
 - En las listas, elija las condiciones pertinentes. Por ejemplo, seleccione Propietario del dispositivo y BYOD.
 - Haga clic en **Nueva regla** para cada condición que quiera agregar.

- Haga clic en la ficha **Avanzado** para combinar las reglas con opciones booleanas. Las condiciones que haya elegido aparecerán en la ficha **Base**.
 - Haga clic en **SÍ, O o NO** y, a continuación, haga clic en **Nueva regla**.
 - En las listas, elija las condiciones que se agregarán a la regla y, a continuación, haga clic en el signo más (+) situado en el lado derecho.
En cualquier momento, puede seleccionar una condición para modificarla o eliminarla si hace clic en **Modificar** o en **Eliminar** respectivamente.
- 7. Haga clic en **Siguiente** para ir a la página **Directivas**. Si quiere, aquí puede agregar directivas, aplicaciones, contenido multimedia o acciones al grupo de entrega. Para obtener más detalles, consulte:
 - Agregar directivas a un grupo de entrega
 - Agregar aplicaciones a un grupo de entrega
 - Agregar contenido multimedia a un grupo de entrega
 - Agregar acciones a un grupo de entrega
- 8. Cuando tenga listo el 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**.

Agregar directivas a un grupo de entrega

1. En la lista **Recursos (opcional)**, haga clic en **Directivas**.
2. Lleve a cabo lo siguiente para agregar cada directiva:
 - Busque la directiva que quiera agregar en la lista de las directivas disponibles. También puede escribir el nombre completo o parcial de una directiva en el cuadro de búsqueda y, a continuación, hacer clic en **Buscar**.
 - Arrastre la directiva que quiera agregar al cuadro de la derecha.

Para quitar una directiva del cuadro, haga clic en la **X** situada junto al nombre de la directiva.

3. Haga clic en **Siguiente** para ir a la página **Aplicaciones**.

Agregar aplicaciones a un grupo de entrega

1. Lleve a cabo lo siguiente para agregar cada aplicación:
 - Busque la aplicación que quiera agregar en la lista de las aplicaciones disponibles. También puede escribir el nombre completo o parcial de una aplicación en el cuadro de búsqueda y, a continuación, hacer clic en **Buscar**.

- Arrastre la aplicación al cuadro **Aplicaciones obligatorias** o al cuadro **Aplicaciones opcionales**.

Para las aplicaciones marcadas como obligatorias, los usuarios reciben inmediatamente actualizaciones en situaciones como estas:

- Se carga una nueva aplicación y se marca como obligatoria.
- Se marca una aplicación existente como obligatoria.
- Un usuario elimina una aplicación obligatoria.
- Hay una actualización de Citrix Secure Hub disponible.

Para obtener información acerca de la implementación forzosa de las aplicaciones obligatorias, incluido cómo habilitar la función, consulte [Acerca de 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 contenido multimedia a un grupo de entrega

1. Lleve a cabo lo siguiente para agregar cada libro:

- Busque el libro que quiera agregar en la lista de los libros disponibles. También puede escribir el nombre completo o parcial de un libro en el cuadro de búsqueda y, a continuación, hacer clic en **Buscar**.
- Arrastre el libro que quiera agregar al cuadro **Libros obligatorios**.

En el caso de libros marcados como obligatorios, los usuarios reciben inmediatamente actualizaciones en situaciones como estas:

- Se carga un nuevo libro y se marca como obligatorio.
- Se marca un libro existente como obligatorio.
- Un usuario elimina un libro obligatorio.
- Hay una actualización de Citrix Secure Hub disponible.

Para quitar un libro del cuadro, haga clic en la **X** situada junto al nombre del libro.

2. Haga clic en **Siguiente** para ir a la página **Acciones**.

Agregar acciones a un grupo de entrega

1. Lleve a cabo lo siguiente para agregar cada acción:

- Busque la acción que quiera agregar en la lista de las acciones disponibles. También puede escribir el nombre completo o parcial de una acción en el cuadro de búsqueda y, a continuación, hacer clic en **Buscar**.

- Arrastre la acción que quiera agregar al cuadro de la derecha.

Para quitar una acción del cuadro, haga clic en la **X** situada 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 ShareFile varía según si ha configurado Citrix Endpoint Management (**Configurar > ShareFile**) para cuentas Enterprise o para conectores de zonas de almacenamiento.

- Si configuró cuentas Enterprise para usarlas con Citrix Endpoint Management, **active** la opción **Habilitar ShareFile**. Esta configuración proporciona al grupo de entrega acceso Single Sign-On al contenido y a los datos de ShareFile.
- En cambio, si configuró conectores de zonas de almacenamiento para usarlos con Citrix Endpoint Management, arrastre los que se incluirán 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 haya configurado para el grupo de entrega y cambiar el orden de implementación de los recursos. La página “Resumen” contiene los recursos por categoría. La página “Resumen” no muestra el orden de implementación.

Nota:

Haga clic en **Atrás** para volver a las páginas anteriores para cambiar la configuración.

Device Policies

Apps

Media

Actions

ShareFile

Enrollment Profiles

Delivery Groups

Delivery Group

1 Delivery Group Info

2 Assignments

3 Resource (optional)

Policies

Apps

Media

Actions

ShareFile

Enrollment Profile

4 Summary

Summary

Review the resources you are about to assign to the delivery group.

General

Name

IOS Education DG

Description

User

Include local user groups

local\SAMPLE-CLASS-1011 - ASM

local\SAMPLE-CLASS-0001 - ASM

local\SAMPLE-CLASS-1010 - ASM

Logic: OR

Resource

Policies 7

DEP Software Inventory

Test 1 HSL

Test 1 Notifications

SAMPLE CLASS 0001 Restrictions

Test Maximum Resident Users

ASM DEP Edu Config

Test Passcode Lock Grace Period

Apps 2

MY LITTLE PONY: MAGIC PRINCESS - ASM

Classroom - ASM

Media 2

Rome - ASM

The Spider Diaries, Book 1: The Eight-leg... - ASM

Actions 0

ShareFile

Disabled

Enrollment Profile

Global

Deployment Order

Back

Save

Para ver o cambiar el orden de implementación:

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1075

1. Haga clic en **Orden de implementación**.
2. En el cuadro de diálogo Orden de implementación, arrastre un recurso al lugar en el orden en el que quiere implementarlo. Los recursos se implementan de arriba a 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 relativas a las propiedades de dispositivo Android. Si inscribe varios dispositivos para un mismo usuario, puede crear filtros avanzados para Android Enterprise basados en el modo de inscripción de dispositivos o en el ID del paquete de aplicaciones 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 de dispositivo**.
3. En **Propiedades del dispositivo: Android**, abra la **ficha Avanzadas** y haga clic en **Nueva regla**.
4. En la lista, elija la condición que quiere agregar a la regla:
 - Para los nuevos dispositivos Android Enterprise, elija **Limit by raw device property name** y escriba **GOOGLE_AW_INSTALL_TYPE** en el primer campo de valores. A continuación, deberá establecer la condición equivalente a uno de los modos de inscripción.

- Para los dispositivos Android Enterprise existentes, elija **Limit by known device property name** y seleccione el **tipo de instalación de Android Enterprise** en el primer campo de valores. A continuación, deberá establecer la condición equivalente a uno de los modos de inscripción.
5. En el segundo campo, introduzca un modo de inscripción para sus dispositivos Android Enterprise:
- **DeviceAdministrator:** Especifica los dispositivos propiedad de la empresa destinados solo para su uso en el trabajo (también conocido como modo propietario del dispositivo)
 - **ManagedProfile:** Especifica dispositivos personales (BYOD) inscritos en Profile Management de trabajo (también conocido como modo propietario del perfil).
 - **CorporateOwnedSingleUse:** Especifica dispositivos dedicados (anteriormente conocidos como dispositivos de uso único y propiedad de la empresa).
 - **CorporateOwnedPersonallyEnabled:** Especifica dispositivos totalmente administrados con un perfil de trabajo (anteriormente conocidos como dispositivos propiedad de la empresa con acceso privado).
6. Termine de configurar el grupo de entrega tal y como se describe en [Agregar un grupo de entrega](#).

Para obtener más información, consulte [Perfiles y casos de implementación de dispositivos](#).

Para implementar un grupo de entrega en dispositivos Android Enterprise mediante el ID del paquete de aplicaciones del dispositivo:

1. En **Propiedades del dispositivo: Android**, abra la **ficha Avanzadas** 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.

Modificar un grupo de entrega

No se puede cambiar el nombre de un grupo de entrega existente. Para actualizar otros parámetros, vaya a **Configurar > Grupos de entrega**, seleccione el grupo que quiera modificar y, a continuación, haga clic en **Modificar**.

Habilitar e inhabilitar el grupo de entrega AllUsers

AllUsers es el único grupo de entrega que puede habilitar o inhabilitar. No se puede eliminar AllUsers, pero sí se pueden eliminar otros grupos de entrega.

Desde la página **Grupos de entrega**, para seleccionar el grupo de entrega AllUsers, seleccione la casilla de verificación situada junto al nombre **AllUsers** o haga clic en la línea que contiene **AllUsers**. A continuación, lleve a cabo una de las siguientes acciones:

- Haga clic en **Inhabilitar** para inhabilitar el grupo de entrega AllUsers. Este comando está disponible solamente si el grupo AllUsers está habilitado (valor predeterminado). Una vez **inhabilitado**, aparecerá bajo el encabezado **Inhabilitado** en la tabla del grupo de entrega.
- Haga clic en **Habilitar** para habilitar el grupo de entrega AllUsers. Este comando está disponible solamente si el grupo AllUsers está inhabilitado. **Inhabilitado** ya no aparecerá bajo el encabezado **Inhabilitado** en la tabla del grupo de entrega.

Implementación en grupos de entrega

La implementación en un grupo de entrega implica enviar una notificación push a todos los usuarios con tabletas Windows y dispositivos Apple o Android.

Para los usuarios con dispositivos de otras plataformas, si esos dispositivos ya están conectados a Citrix Endpoint Management, recibirán los recursos inmediatamente. De lo contrario, en función de cómo se haya configurado la directiva de programación, recibirán los recursos la próxima vez que se conecten.

Para que las actualizaciones de las aplicaciones aparezcan en la lista de actualizaciones disponibles de la instancia de App Store presente en los dispositivos Android de los usuarios, primero debe implementar una directiva “Inventario de aplicaciones” en los dispositivos de los usuarios.

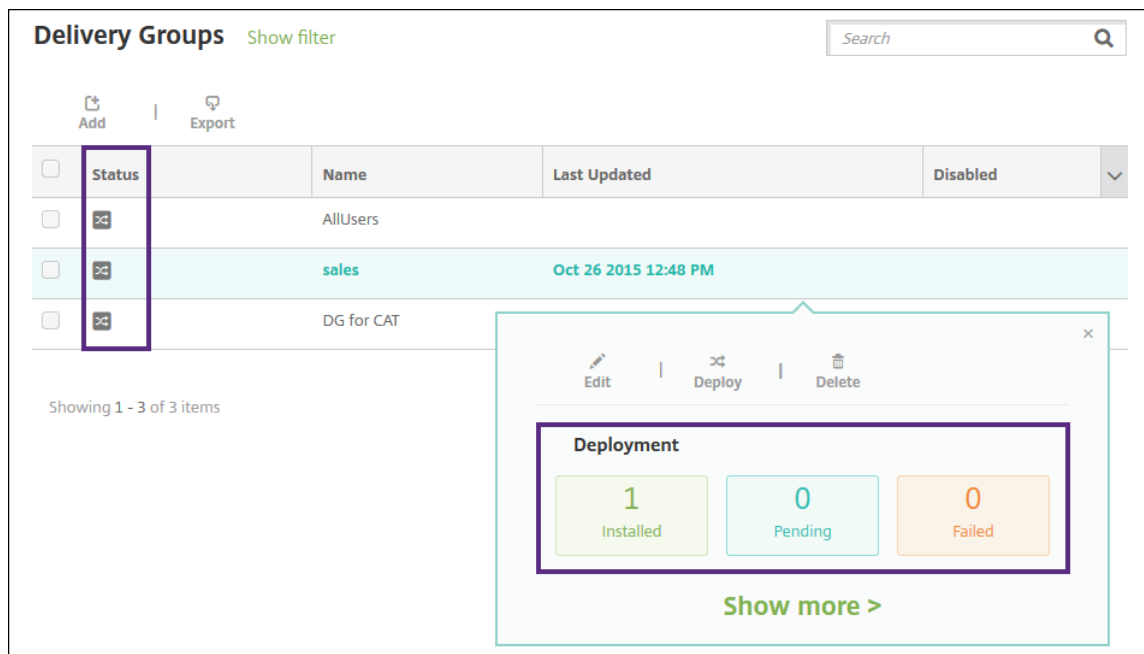
1. En la página **Grupos de entrega**, realice una de las siguientes acciones:
 - Para implementar recursos en más de un grupo de entrega a la vez, marque las casillas situadas junto a los grupos en los que quiere realizar la implementación.
 - Para implementar recursos en un solo grupo de entrega, marque la casilla que aparece junto a su nombre o haga clic en la línea que contiene su nombre.
2. Haga clic en **Deploy**.

Según cómo seleccione el grupo de entrega, el comando **Implementar** aparecerá encima o a la derecha del grupo de entrega.

Compruebe que aparecen en la lista los grupos en los que quiere implementar aplicaciones, directivas y acciones. Luego haga clic en **Implementar**. Las aplicaciones, las directivas y las acciones se implementan en los grupos seleccionados en función de la plataforma de los dispositivos y de la directiva de programación.

Puede comprobar el estado de implementación en la página **Grupos de entrega** de una de las siguientes maneras:

- Consulte el icono de implementación situado en el encabezado **Estado** del grupo de entrega. Este icono indica si ha habido algún error en la implementación.
- Haga clic en la línea que contiene el grupo de entrega para ver una etiqueta superpuesta donde se muestra si la implementación **se ha instalado, está pendiente o ha fallado**.



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 el nuevo grupo de entrega. A continuación, haga los cambios en el clon, como agregar perfiles de inscripción o nuevos conjuntos de usuarios de AD.

1. En la consola 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 grupo que quiera usar como base del nuevo grupo.
3. Seleccione **Clonar**.
4. En el cuadro de diálogo Clonar un grupo de entrega, escriba el nombre del nuevo grupo y, si quiere, una descripción.
5. Seleccione **Clonar**.

Eliminar grupos de entrega

No se puede eliminar el grupo de entrega AllUsers, pero sí se puede inhabilitar cuando no interese enviar recursos a todos los usuarios. Consulte Habilitar e inhabilitar el grupo de entrega AllUsers.

Importante:

No 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, marque las casillas situadas junto a los grupos que quiere eliminar.
 - Para eliminar un solo grupo de entrega, marque la casilla que aparece junto a su nombre o haga clic en la línea que contiene su nombre.
2. Haga clic en **Eliminar**.

Según cómo seleccione el grupo de entrega, el comando **Eliminar** aparecerá 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**, situado sobre la tabla **Grupos de entrega**. Citrix Endpoint Management extrae la información de la tabla **Grupos de entrega** y la convierte a un archivo CSV.
2. Abra o guarde el archivo CSV siguiendo los pasos habituales del explorador web que utilice.

Macros

March 1, 2024

Citrix Endpoint Management ofrece macros para rellenar datos de propiedades de usuario o dispositivo en el campo de texto de los siguientes elementos:

- Directivas
- Notificaciones
- Plantillas de inscripción
- Archivo XML de configuración del dispositivo
- Acciones automatizadas
- Solicitudes de firma de certificado provenientes del proveedor de credenciales

Citrix Endpoint Management reemplaza una macro por los valores correspondientes al usuario o al sistema. Por ejemplo, puede rellenar de antemano el valor del buzón de correo perteneciente a un solo usuario en un perfil de Exchange entre miles de usuarios.

Sintaxis de macros

Una macro puede presentar el siguiente formato:

- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]] }`

Incluya todos los elementos de sintaxis posteriores al signo de dólar (\$) entre llaves ({}).

- Los nombres de propiedad calificados hacen referencia ya sea a una propiedad de usuario, una propiedad de dispositivo o a una propiedad personalizada.
- Los nombres de propiedad calificados se componen de un prefijo, seguido del nombre en sí de la propiedad.
- Las propiedades del usuario tienen el formato `${ user.[PROPERTYNAME] (prefix="user.") }`.
- Las propiedades del dispositivo tienen el formato `${ device.[PROPERTYNAME] (prefix="device.") }`.
- Los nombres de propiedad distinguen mayúsculas de minúsculas.
- Una función puede ser una lista limitada o un enlace a una referencia externa que define las funciones. Esta macro para un mensaje de notificación incluye la función `firstnotnull`:

El dispositivo `${ firstnotnull(device.TEL_NUMBER,device.serialNumber) }` ha sido bloqueado...

- Para macros personalizadas (propiedades que usted define), el prefijo es `${ custom }`. Puede omitir el prefijo.

Este es el ejemplo de una macro frecuente, `${ user.username }`, que rellena el valor de nombre de usuario en el campo de texto de una directiva. Esta macro es útil para configurar perfiles de Exchange ActiveSync y otros perfiles utilizados por varios usuarios. En el siguiente ejemplo, se muestra cómo usar macros en una directiva de Exchange. La macro de **Usuario** es `${ user.username }`. La macro para **Dirección de correo electrónico** es `${ user.mail }`.

Device PoliciesAppsActionsShareFileEnrollment ProfilesDelivery Groups

Exchange Policy

1 Policy Info2 Platforms3 Assignment

Exchange Policy

This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.

Exchange ActiveSync account name*

Exchange01

Exchange ActiveSync host name*

exchange01.example.net

Use SSL

ON

Domain

example.net

User

\$user.username

Email address

\$user.mail

Password

Email sync interval

1 month

Identity credential (keystore or PKI credential)

None

Authorize email move between accounts

OFF

En el siguiente ejemplo, se muestra cómo usar macros en una solicitud de firma de certificado. La macro para el **nombre del sujeto** es **CN=\$user.username**. La macro para el **valor** de un **nombre alternativo del sujeto** es **\$user.userprincipalname**.

Settings > Credential Providers > Add credential provider

Credential Providers

1 General2 Certificate Signing Request3 Distribution4 Revocation XenMobile5 Revocation PKI6 Renewal

Credential Providers: Certificate Signing Request

Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.

Key algorithm

RSA

Key size*

2048

Signature algorithm

SHA256withRSA

Subject name*

CN=\$user.username

Subject alternative names

Type	Value*	Add
User Principal name	\$user.userprincipalname	

En el siguiente ejemplo, se muestra cómo usar macros en una plantilla de notificaciones. La plantilla de ejemplo define el mensaje enviado a un usuario cuando las aplicaciones HDX se bloquean debido a un dispositivo que no cumple las reglas. La macro para el **mensaje** es:

El dispositivo `${ firstnotnull(device.TEL_NUMBER,device.serialNumber) }` ya no sigue la directiva de dispositivo. Las aplicaciones HDX se bloquearán.

Settings > Notification Templates > Add Notification Template

Add Notification Template

Based on the types of templates you choose, you can notify users through supported channels, such as SMTP, SMS and Secure Hub.

Name*

HDX Application Block

Description

Type

Ad-Hoc Notification

Manual sending supported

Channels

Secure Hub

Activate

Message

Device
\${firstNotNull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked.

Para obtener más ejemplos de macros utilizadas en las notificaciones, vaya a **Parámetros > Plantillas de notificaciones**, seleccione una plantilla predefinida y haga clic en **Modificar**.

En el siguiente ejemplo, se muestra una macro en la directiva de nombre de dispositivo. Escriba la macro, una combinación de ellas o una combinación de macros y texto para darle a cada dispositivo un nombre único. Por ejemplo, para establecer el número de serie de un dispositivo como su nombre, puede utilizar `${ device.serialnumber }`. Use `${ device.serialnumber }` `${ user.username }` para incluir el nombre de usuario en el nombre del dispositivo. La directiva de nombre de dispositivo funciona en dispositivos supervisados iOS y macOS.

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

Device Name Policy

1 Policy Info

2 Platforms

✓ iOS

✓ Mac OS X

3 Assignment

Device Name Policy

This policy lets you apply a name on a supervised device on iOS and Mac OS X devices. Available in iOS 8 and later.

Device name*

`${device.serialnumber}`

► Deployment Rules

Macros para plantillas de notificaciones predeterminadas

Puede utilizar estas macros en las plantillas de notificaciones 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 contiene los términos “lista negra” y “lista blanca”. Estamos cambiando esos términos en una próxima versión a “lista de bloqueados” y “lista de permitidos”.

En este ejemplo se muestra cómo crear una notificación que incluya las direcciones URL de inscripción para varias plataformas de dispositivos. La macro para el **mensaje** es:

`${enrollment.urls}`

Settings > Notification Templates > Add Notification Template

Add Notification Template

Based on the types of templates you choose, you can notify users through supported channels, such as SMTP, SMS and Secure Hub.

Name*

Multi-platform enrollment

Description

Type

Enrollment Invitation

Manual sending not supported

Channels

SMTP

Channel cannot be activated until you define the SMTP server in the [Notification Server](#) section in Settings.

Sender

Test

Recipient

\${user.mail}

Subject

Enroll your device

Message

{enrollment.urls}

SMS

Channel cannot be activated until you define the SMS server in the [Notification Server](#) section in Settings.

Recipient

\${user.mobile}

Message

Cancel

Add

En estos ejemplos se muestra cómo crear mensajes para las notificaciones que solicitan a los usuarios hacer clic en la URL de inscripción correspondiente a la plataforma de sus dispositivos:

Ejemplo 1:

```
1 To enroll, click the link below that applies to your device platform:
2
3 ${
4   enrollment.ios.platform }
5   - ${
6     enrollment.ios.url }
7
8
9 ${
10  enrollment.macos.platform }
11  - ${
12    enrollment.macos.url }
13
14
15 ${
16  enrollment.android.platform }
17  - ${
18    enrollment.android.url }
19
20
```

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1085

```
21 <!--NeedCopy-->
```

Ejemplo 2:

```
1 To enroll an iOS device, click the link ${
2   enrollment.ios.url }
3   .
4
5 To enroll a macOS device, click the link ${
6   enrollment.macos.url }
7   .
8
9 To enroll an Android device, click the link ${
10  enrollment.android.url }
11  .
12
13 <!--NeedCopy-->
```

Macros para directivas específicas

En la directiva de nombre de dispositivo (para iOS y macOS), puede usar estas macros para **Nombre de dispositivo**:

- `${ device.serialnumber }`
- `${ user.username } @example.com`
- `${ device.serialnumber }`
- `${ device.serialnumber }`
- `${ user.username }`
- `${ enrollment.pin }`
- `${ user.dnsroot }`

Puede usar macros para los valores de los campos sin cadena, como el campo “Puerto del servidor proxy”, en la directiva de red de telefonía móvil (de iOS). Por ejemplo, ahora puede usar la macro `${ device.xyz }` o `${ setting.xyz }`, que se expande en un número entero.

También puede usar las macros para valores de campos sin cadena en un archivo XML de configuración de dispositivos que importe en Citrix Endpoint Management mediante la directiva para **importar perfil de iOS y macOS**.

En la directiva de clave de licencia MDM de Samsung, puede utilizar esta macro para **Clave de licencia ELM**:

- `${ elm.license.key }`

En la directiva de clip web, puede utilizar esta macro para **URL**:

- `${ webeas-url }`

Macros para obtener propiedades integradas de dispositivo

Nombre simplificado	Macros
ID de dispositivo	<code>\$device.id</code>
GUID del dispositivo	<code>\$device.uniqueid</code>
Número IMEI del dispositivo	<code>\$device.imei</code>
Familia de SO	<code>\$device.OSFamily</code>
Número de serie	<code>\$device.serialNumber</code>

Macros para todas las propiedades de dispositivo

Nombre simplificado: ¿Está suspendida la cuenta?

- **Elemento web:** `GOOGLE_AW_DIRECTORY_SUSPENDED`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_SUSPENDED }`

Nombre simplificado: Código de omisión del bloqueo de activación

- **Elemento web:** `ACTIVATION_LOCK_BYPASS_CODE`
- **Macros:** `${ device.ACTIVATION_LOCK_BYPASS_CODE }`

Nombre simplificado: Bloqueo de activación habilitado

- **Elemento web:** `ACTIVATION_LOCK_ENABLED`
- **Macros:** `${ device.ACTIVATION_LOCK_ENABLED }`

Nombre simplificado: Cuenta activa del App Store de Apple

- **Elemento web:** `ACTIVE_ITUNES`
- **Macros:** `${ device.ACTIVE_ITUNES }`

Nombre simplificado: Administrador inhabilitado

- **Elemento web:** `ADMIN_DISABLED`
- **Macros:** `${ device.ADMIN_DISABLED }`

Nombre simplificado: ¿Está AIK presente?

- **Elemento web:** `WINDOWS_HAS_AIK_PRESENT`

- **Macros:** `${ device.WINDOWS_HAS_AIK_PRESENT }`

Nombre simplificado: API de MDM de Amazon disponible

- **Elemento web:** `AMAZON_MDM`
- **Macros:** `${ device.AMAZON_MDM }`

Nombre simplificado: ID de dispositivo Android Enterprise

- **Elemento web:** `GOOGLE_AW_DEVICE_ID`
- **Macros:** `${ device.GOOGLE_AW_DEVICE_ID }`

Nombre simplificado: ¿Dispositivo habilitado para Android Enterprise?

- **Elemento web:** `GOOGLE_AW_ENABLED_DEVICE`
- **Macros:** `${ device.GOOGLE_AW_ENABLED_DEVICE }`

Nombre simplificado: Tipo de instalación de Android Enterprise

- **Elemento web:** `GOOGLE_AW_INSTALL_TYPE`
- **Macros:** `${ device.GOOGLE_AW_INSTALL_TYPE }`

Nombre simplificado: Estado de firma de antispyware

- **Elemento web:** `ANTI_SPYWARE_SIGNATURE_STATUS`
- **Macros:** `${ device.ANTI_SPYWARE_SIGNATURE_STATUS }`

Nombre simplificado: Estado de antispyware

- **Elemento web:** `ANTI_SPYWARE_STATUS`
- **Macros:** `${ device.ANTI_SPYWARE_STATUS }`

Nombre simplificado: Estado de firma del antivirus

- **Elemento web:** `ANTI_VIRUS_SIGNATURE_STATUS`
- **Macros:** `${ device.ANTI_VIRUS_SIGNATURE_STATUS }`

Nombre simplificado: Estado del antivirus

- **Elemento web:** `ANTI_VIRUS_STATUS`
- **Macros:** `${ device.ANTI_VIRUS_STATUS }`

Nombre simplificado: 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 simplificado: Clave de custodia del Programa de implementación de ASM

- **Elemento web:** `DEP_ESCROW_KEY`
- **Macros:** `${ device.DEP_ESCROW_KEY }`

Nombre simplificado: Etiqueta de inventario

- **Elemento web:** `ASSET_TAG`
- **Macros:** `${ device.ASSET_TAG }`

Nombre simplificado: Comprobar automáticamente las actualizaciones de software

- **Elemento web:** `AutoCheckEnabled`
- **Macros:** `${ device.AutoCheckEnabled }`

Nombre simplificado: Descargar automáticamente las actualizaciones de software en segundo plano

- **Elemento web:** `BackgroundDownloadEnabled`
- **Macros:** `${ device.BackgroundDownloadEnabled }`

Nombre simplificado: Instalar automáticamente las actualizaciones de aplicaciones

- **Elemento web:** `AutomaticAppInstallationEnabled`
- **Macros:** `${ device.AutomaticAppInstallationEnabled }`

Nombre simplificado: Instalar automáticamente las actualizaciones de SO

- **Elemento web:** `AutomaticOSInstallationEnabled`
- **Macros:** `${ device.AutomaticOSInstallationEnabled }`

Nombre simplificado: Instalar automáticamente las actualizaciones de seguridad

- **Elemento web:** `AutomaticSecurityUpdatesEnabled`
- **Macros:** `${ device.AutomaticSecurityUpdatesEnabled }`

Nombre simplificado: Estado de la actualización automática

- **Elemento web:** `AUTOUPDATE_STATUS`
- **Macros:** `${ device.AUTOUPDATE_STATUS }`

Nombre simplificado: RAM disponible

- **Elemento web:** `MEMORY_AVAILABLE`
- **Macros:** `${ device.MEMORY_AVAILABLE }`

Nombre simplificado: Actualizaciones de software disponibles

- **Elemento web:** `AVAILABLE_OS_UPDATE_HUMAN_READABLE`
- **Macros:** `${ device.AVAILABLE_OS_UPDATE_HUMAN_READABLE }`

Nombre simplificado: Espacio de almacenamiento disponible

- **Elemento web:** `FREEDISK`
- **Macros:** `${ device.FREEDISK }`

Nombre simplificado: Batería de reserva

- **Elemento web:** `BACKUP_BATTERY_PERCENT`
- **Macros:** `${ device.BACKUP_BATTERY_PERCENT }`

Nombre simplificado: Versión de banda base de firmware

- **Elemento web:** `MODEM_FIRMWARE_VERSION`
- **Macros:** `'${device.MODEM_FIRMWARE_VERSION}'`

Nombre simplificado: Carga de batería

- **Elemento web:** `BATTERY_CHARGING_STATUS`
- **Macros:** `${ device.BATTERY_CHARGING_STATUS }`

Nombre simplificado: Carga de batería

- **Elemento web:** `BATTERY_CHARGING`
- **Macros:** `${ device.BATTERY_CHARGING }`

Nombre simplificado: Batería restante

- **Elemento web:** `BATTERY_ESTIMATED_CHARGE_REMAINING`
- **Macros:** `${ device.BATTERY_ESTIMATED_CHARGE_REMAINING }`

Nombre simplificado: Tiempo de operación de la batería

- **Elemento web:** `BATTERY_RUNTIME`
- **Macros:** `${ device.BATTERY_RUNTIME }`

Nombre simplificado: Estado de la batería

- **Elemento web:** `BATTERY_STATUS`
- **Macros:** `${ device.BATTERY_STATUS }`

Nombre simplificado: PIN de BES

- **Elemento web:** `BES_PIN`
- **Macros:** `${ device.BES_PIN }`

Nombre simplificado: ID del agente del servidor BES

- **Elemento web:** `AGENT_ID`
- **Macros:** `${ device.AGENT_ID }`

Nombre simplificado: Nombre del servidor BES

- **Elemento web:** `BES_SERVER`
- **Macros:** `${ device.BES_SERVER }`

Nombre simplificado: Versión del servidor BES

- **Elemento web:** `BES_VERSION`
- **Macros:** `${ device.BES_VERSION }`

Nombre simplificado: Información de BIOS

- **Elemento web:** `BIOS_INFO`
- **Macros:** `${ device.BIOS_INFO }`

Nombre simplificado: Estado de BitLocker

- **Elemento web:** `WINDOWS_HAS_BIT_LOCKER_STATUS`
- **Macros:** `${ device.WINDOWS_HAS_BIT_LOCKER_STATUS }`

Nombre simplificado: Dirección MAC de Bluetooth

- **Elemento web:** `BLUETOOTH_MAC`
- **Macros:** `${ device.BLUETOOTH_MAC }`

Nombre simplificado: Boot Debugging Enabled?

- **Elemento web:** `WINDOWS_HAS_BOOT_DEBUGGING_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED }`

Nombre simplificado: Boot Manager Rev List Version

- **Elemento web:** `WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION`
- **Macros:** `${ device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION }`

Nombre simplificado: Código de operador

- **Elemento web:** `CARRIER_CODE`
- **Macros:** `${ device.CARRIER_CODE }`

Nombre simplificado: Versión de parámetros de operador

- **Elemento web:** `CARRIER_SETTINGS_VERSION`
- **Macros:** `${ device.CARRIER_SETTINGS_VERSION }`

Nombre simplificado: URL del catálogo

- **Elemento web:** `CatalogURL`
- **Macros:** `${ device.CatalogURL }`

Nombre simplificado: Móvil: Altitud

- **Elemento web:** `GPS_ALTITUDE_FROM_CELLULAR`
- **Macros:** `${ device.GPS_ALTITUDE_FROM_CELLULAR }`

Nombre simplificado: Móvil: Trayectoria

- **Elemento web:** `GPS_COURSE_FROM_CELLULAR`
- **Macros:** `${ device.GPS_COURSE_FROM_CELLULAR }`

Nombre simplificado: Móvil: Precisión horizontal

- **Elemento web:** `GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR`
- **Macros:** `${ device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR }`

Nombre simplificado: Móvil: Latitud

- **Elemento web:** `GPS_LATITUDE_FROM_CELLULAR`
- **Macros:** `${ device.GPS_LATITUDE_FROM_CELLULAR }`

Nombre simplificado: Móvil: Longitud

- **Elemento web:** `GPS_LONGITUDE_FROM_CELLULAR`
- **Macros:** `${ device.GPS_LONGITUDE_FROM_CELLULAR }`

Nombre simplificado: Móvil: Velocidad

- **Elemento web:** `GPS_SPEED_FROM_CELLULAR`
- **Macros:** `${ device.GPS_SPEED_FROM_CELLULAR }`

Nombre simplificado: Tecnología del móvil

- **Elemento web:** `CELLULAR_TECHNOLOGY`
- **Macros:** `${ device.CELLULAR_TECHNOLOGY }`

Nombre simplificado: Móvil: Marca de hora

- **Elemento web:** `GPS_TIMESTAMP_FROM_CELLULAR`
- **Macros:** `${ device.GPS_TIMESTAMP_FROM_CELLULAR }`

Nombre simplificado: Móvil: Precisión vertical

- **Elemento web:** `GPS_VERTICAL_ACCURACY_FROM_CELLULAR`
- **Macros:** `${ device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR }`

Nombre simplificado: ¿Cambiar la contraseña la próxima vez que se inicie sesión?

- **Elemento web:** `GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN`
- **Macros:** `'${device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN}'`

Nombre simplificado: ID de dispositivo cliente

- **Elemento web:** `CLIENT_DEVICE_ID`
- **Macros:** `${ device.CLIENT_DEVICE_ID }`

Nombre simplificado: Copia de seguridad en nube habilitada

- **Elemento web:** `CLOUD_BACKUP_ENABLED`
- **Macros:** `${ device.CLOUD_BACKUP_ENABLED }`

Nombre simplificado: Code Integrity Enabled?

- **Elemento web:** `WINDOWS_HAS_CODE_INTEGRITY_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED }`

Nombre simplificado: Code Integrity Rev List Version

- **Elemento web:** `WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION`
- **Macros:** `${ device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION }`

Nombre simplificado: Color

- **Elemento web:** COLOR
- **Macros:** \${ device.COLOR }

Nombre simplificado: Velocidad de reloj de CPU

- **Elemento web:** CPU_CLOCK_SPEED
- **Macros:** \${ device.CPU_CLOCK_SPEED }

Nombre simplificado: Tipo de CPU

- **Elemento web:** CPU_TYPE
- **Macros:** \${ device.CPU_TYPE }

Nombre simplificado: Hora de creación

- **Elemento web:** GOOGLE_AW_DIRECTORY_CREATION_TIME
- **Macros:** \${ device.GOOGLE_AW_DIRECTORY_CREATION_TIME }

Nombre simplificado: Actualizaciones de software críticas

- **Elemento web:** AVAILABLE_OS_UPDATE_IS_CRITICAL
- **Macros:** \${ device.AVAILABLE_OS_UPDATE_IS_CRITICAL }

Nombre simplificado: Red del operador actual

- **Elemento web:** CARRIER
- **Macros:** \${ device.CARRIER }

Nombre simplificado: Código móvil de país actual

- **Elemento web:** CURRENT_MCC
- **Macros:** \${ device.CURRENT_MCC }

Nombre simplificado: Código móvil de red actual

- **Elemento web:** CURRENT_MNC
- **Macros:** \${ device.CURRENT_MNC }

Nombre simplificado: Itinerancia de datos permitido

- **Elemento web:** DATA_ROAMING_ENABLED
- **Macros:** \${ device.DATA_ROAMING_ENABLED }

Nombre simplificado: Fecha de la última copia de seguridad en iCloud

- **Elemento web:** `LAST_CLOUD_BACKUP_DATE`
- **Macros:** `${ device.LAST_CLOUD_BACKUP_DATE }`

Nombre simplificado: Catálogo predeterminado

- **Elemento web:** `IsDefaultCatalog`
- **Macros:** `${ device.IsDefaultCatalog }`

Nombre simplificado: 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 simplificado: Directiva del Programa de implementación de Apple

- **Elemento web:** `WINDOWS_HAS_DEP_POLICY`
- **Macros:** `${ device.WINDOWS_HAS_DEP_POLICY }`

Nombre simplificado: Perfil del Programa de implementación de Apple asignado

- **Elemento web:** `PROFILE_ASSIGN_TIME`
- **Macros:** `${ device.PROFILE_ASSIGN_TIME }`

Nombre simplificado: Perfil del Programa de implementación de Apple enviado

- **Elemento web:** `PROFILE_PUSH_TIME`
- **Macros:** `${ device.PROFILE_PUSH_TIME }`

Nombre simplificado: Perfil del Programa de implementación de Apple eliminado

- **Elemento web:** `PROFILE_REMOVE_TIME`
- **Macros:** `${ device.PROFILE_REMOVE_TIME }`

Nombre simplificado: Autor del registro del Programa de implementación de Apple

- **Elemento web:** `DEVICE_ASSIGNED_BY`
- **Macros:** `${ device.DEVICE_ASSIGNED_BY }`

Nombre simplificado: Fecha de registro del Programa de implementación de Apple

- **Elemento web:** `DEVICE_ASSIGNED_DATE`
- **Macros:** `${ device.DEVICE_ASSIGNED_DATE }`

Nombre simplificado: Descripción

- **Elemento web:** DESCRIPTION
- **Macros:** \${ device.DESRIPTION }

Nombre simplificado: Modelo del dispositivo

- **Elemento web:** SYSTEM_OEM
- **Macros:** \${ device.SYSTEM_OEM }

Nombre simplificado: Nombre del dispositivo

- **Elemento web:** DEVICE_NAME
- **Macros:** \${ device.DEVICE_NAME }

Nombre simplificado: Tipo de dispositivo

- **Elemento web:** DEVICE_TYPE
- **Macros:** \${ device.DEVICE_TYPE }

Nombre simplificado: No Molestar activado

- **Elemento web:** DO_NOT_DISTURB
- **Macros:** \${ device.DO_NOT_DISTURB }

Nombre simplificado: ELAM Driver Loaded?

- **Elemento web:** WINDOWS_HAS_ELAM_DRIVER_LOADED
- **Macros:** \${ device.WINDOWS_HAS_ELAM_DRIVER_LOADED }

Nombre simplificado: Conformidad de cifrado

- **Elemento web:** ENCRYPTION_COMPLIANCE
- **Macros:** \${ device.ENCRYPTION_COMPLIANCE }

Nombre simplificado: ENROLLMENT_KEY_GENERATION_DATE

- **Elemento web:** ENROLLMENT_KEY_GENERATION_DATE
- **Macros:** \${ device.ENROLLMENT_KEY_GENERATION_DATE }

Nombre simplificado: ID de empresa

- **Elemento web:** ENTERPRISEID
- **Macros:** \${ device.ENTERPRISEID }

Nombre simplificado: Almacenamiento externo 1: espacio disponible

- **Elemento web:** `EXTERNAL_STORAGE1_FREE_SPACE`
- **Macros:** `${ device.EXTERNAL_STORAGE1_FREE_SPACE }`

Nombre simplificado: Almacenamiento externo 1: espacio disponible

- **Elemento web:** `EXTERNAL_STORAGE1_FREE_SPACE`
- **Macros:** `${ device.EXTERNAL_STORAGE1_FREE_SPACE }`

Nombre simplificado: Almacenamiento externo 1: nombre

- **Elemento web:** `EXTERNAL_STORAGE1_NAME`
- **Macros:** `${ device.EXTERNAL_STORAGE1_NAME }`

Nombre simplificado: Almacenamiento externo 1: espacio total

- **Elemento web:** `EXTERNAL_STORAGE1_TOTAL_SPACE`
- **Macros:** `${ device.EXTERNAL_STORAGE1_TOTAL_SPACE }`

Nombre simplificado: Almacenamiento externo 2: espacio disponible

- **Elemento web:** `EXTERNAL_STORAGE2_FREE_SPACE`
- **Macros:** `${ device.EXTERNAL_STORAGE2_FREE_SPACE }`

Nombre simplificado: Almacenamiento externo 2: nombre

- **Elemento web:** `EXTERNAL_STORAGE2_NAME`
- **Macros:** `${ device.EXTERNAL_STORAGE2_NAME }`

Nombre simplificado: Almacenamiento externo 2: espacio total

- **Elemento web:** `EXTERNAL_STORAGE2_TOTAL_SPACE`
- **Macros:** `${ device.EXTERNAL_STORAGE2_TOTAL_SPACE }`

Nombre simplificado: Almacenamiento externo cifrado

- **Elemento web:** `EXTERNAL_ENCRYPTION`
- **Macros:** `${ device.EXTERNAL_ENCRYPTION }`

Nombre simplificado: FileVault habilitado

- **Elemento web:** `IS_FILEVAULT_ENABLED`
- **Macros:** `${ device.IS_FILEVAULT_ENABLED }`

Nombre simplificado: Estado del firewall

- **Elemento web:** `DEVICE_FIREWALL_STATUS`
- **Macros:** `${ device.DEVICE_FIREWALL_STATUS }`

Nombre simplificado: Estado del firewall

- **Elemento web:** `DEVICE_FIREWALL_STATUS`
- **Macros:** `${ device.DEVICE_FIREWALL_STATUS }`

Nombre simplificado: Estado del firewall

- **Elemento web:** `FIREWALL_STATUS`
- **Macros:** `${ device.FIREWALL_STATUS }`

Nombre simplificado: Versión del firmware

- **Elemento web:** `FIRMWARE_VERSION`
- **Macros:** `${ device.FIRMWARE_VERSION }`

Nombre simplificado: Primera sincronización

- **Elemento web:** `ZMSP_FIRST_SYNC`
- **Macros:** `${ device.ZMSP_FIRST_SYNC }`

Nombre simplificado: Alias de Google Directory

- **Elemento web:** `GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS }`

Nombre simplificado: Apellidos de Google Directory

- **Elemento web:** `GOOGLE_AW_DIRECTORY_FAMILY_NAME`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_FAMILY_NAME }`

Nombre simplificado: Nombre de Google Directory

- **Elemento web:** `GOOGLE_AW_DIRECTORY_NAME`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_NAME }`

Nombre simplificado: Correo electrónico principal de Google Directory

- **Elemento web:** `GOOGLE_AW_DIRECTORY_PRIMARY`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_PRIMARY }`

Nombre simplificado: ID de usuario de Google Directory

- **Elemento web:** `GOOGLE_AW_DIRECTORY_USER_ID`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_USER_ID }`

Nombre simplificado: GPS: Altitud

- **Elemento web:** `GPS_ALTITUDE_FROM_GPS`
- **Macros:** `${ device.GPS_ALTITUDE_FROM_GPS }`

Nombre simplificado: GPS: Trayectoria

- **Elemento web:** `GPS_COURSE_FROM_GPS`
- **Macros:** `${ device.GPS_COURSE_FROM_GPS }`

Nombre simplificado: GPS: Precisión horizontal

- **Elemento web:** `GPS_HORIZONTAL_ACCURACY_FROM_GPS`
- **Macros:** `${ device.GPS_HORIZONTAL_ACCURACY_FROM_GPS }`

Nombre simplificado: GPS: Latitud

- **Elemento web:** `GPS_LATITUDE_FROM_GPS`
- **Macros:** `${ device.GPS_LATITUDE_FROM_GPS }`

Nombre simplificado: GPS: Longitud

- **Elemento web:** `GPS_LONGITUDE_FROM_GPS`
- **Macros:** `${ device.GPS_LONGITUDE_FROM_GPS }`

Nombre simplificado: GPS: Velocidad

- **Elemento web:** `GPS_SPEED_FROM_GPS`
- **Macros:** `${ device.GPS_SPEED_FROM_GPS }`

Nombre simplificado: GPS: Marca de hora

- **Elemento web:** `GPS_TIMESTAMP_FROM_GPS`
- **Macros:** `${ device.GPS_TIMESTAMP_FROM_GPS }`

Nombre simplificado: GPS: Precisión vertical

- **Elemento web:** `GPS_VERTICAL_ACCURACY_FROM_GPS`
- **Macros:** `${ device.GPS_VERTICAL_ACCURACY_FROM_GPS }`

Nombre simplificado: ID de dispositivo de hardware

- **Elemento web:** `HW_DEVICE_ID`
- **Macros:** `${ device.HW_DEVICE_ID }`

Nombre simplificado: Capacidades de cifrado del hardware

- **Elemento web:** `HARDWARE_ENCRYPTION_CAPS`
- **Macros:** `${ device.HARDWARE_ENCRYPTION_CAPS }`

Nombre simplificado: `HAS_CONTAINER`

- **Elemento web:** `HAS_CONTAINER`
- **Macros:** `${ device.HAS_CONTAINER }`

Nombre simplificado: Hash de la cuenta del App Store de Apple conectada actualmente

- **Elemento web:** `ITUNES_STORE_ACCOUNT_HASH`
- **Macros:** `${ device.ITUNES_STORE_ACCOUNT_HASH }`

Nombre simplificado: Red del operador local

- **Elemento web:** `SIM_CARRIER_NETWORK`
- **Macros:** `${ device.SIM_CARRIER_NETWORK }`

Nombre simplificado: Código móvil de país local

- **Elemento web:** `SIM_MCC`
- **Macros:** `${ device.SIM_MCC }`

Nombre simplificado: Código móvil de red local

- **Elemento web:** `SIM_MNC`
- **Macros:** `${ device.SIM_MNC }`

Nombre simplificado: ICCID

- **Elemento web:** `ICCID`
- **Macros:** `${ device.ICCID }`

Nombre simplificado: Identidad

- **Elemento web:** `AS_DEVICE_IDENTITY`
- **Macros:** `${ device.AS_DEVICE_IDENTITY }`

Nombre simplificado: Número IMEI/MEID

- **Elemento web:** `IMEI`
- **Macros:** `${ device.IMEI }`

Nombre simplificado: IMSI

- **Elemento web:** `SIM_ID`
- **Macros:** `${ device.SIM_ID }`

Nombre simplificado: Almacenamiento interno cifrado

- **Elemento web:** `LOCAL_ENCRYPTION`
- **Macros:** `${ device.LOCAL_ENCRYPTION }`

Nombre simplificado: Localización de IP

- **Elemento web:** `IP_LOCATION`
- **Macros:** `${ device.IP_LOCATION }`

Nombre simplificado: Dirección IPv4

- **Elemento web:** `IP_ADDRESSV4`
- **Macros:** `${ device.IP_ADDRESSV4 }`

Nombre simplificado: Dirección IPv6

- **Elemento web:** `IP_ADDRESSV6`
- **Macros:** `${ device.IP_ADDRESSV6 }`

Nombre simplificado: Issued At (Emitido)

- **Elemento web:** `WINDOWS_HAS_ISSUED_AT`
- **Macros:** `${ device.WINDOWS_HAS_ISSUED_AT }`

Nombre simplificado: Liberado por jailbreak o root

- **Elemento web:** `ROOT_ACCESS`
- **Macros:** `${ device.ROOT_ACCESS }`

Nombre simplificado: Kernel Debugging Enabled?

- **Elemento web:** `WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED }`

Nombre simplificado: Modo quiosco

- **Elemento web:** `IS_KIOSK`
- **Macros:** `${ device.IS_KIOSK }`

Nombre simplificado: Última dirección IP conocida

- **Elemento web:** `LAST_IP_ADDR`
- **Macros:** `${ device.LAST_IP_ADDR }`

Nombre simplificado: Última actualización de directivas

- **Elemento web:** `LAST_POLICY_UPDATE_TIME`
- **Macros:** `${ device.LAST_POLICY_UPDATE_TIME }`

Nombre simplificado: Fecha del último examen

- **Elemento web:** `PreviousScanDate`
- **Macros:** `${ device.PreviousScanDate }`

Nombre simplificado: Resultado del último examen

- **Elemento web:** `PreviousScanResult`
- **Macros:** `${ device.PreviousScanResult }`

Nombre simplificado: Últimas actualizaciones de software programadas

- **Elemento web:** `AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME`
- **Macros:** `${ device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME }`

Nombre simplificado: Último mensaje de fallo de actualizaciones de software programadas

- **Elemento web:** `AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG`
- **Macros:** `${ device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG }`

Nombre simplificado: Último estado de las actualizaciones de software programadas

- **Elemento web:** `AVAILABLE_OS_UPDATE_INSTALL_STATUS`
- **Macros:** `${ device.AVAILABLE_OS_UPDATE_INSTALL_STATUS }`

Nombre simplificado: Última sincronización

- **Elemento web:** `ZMSP_LAST_SYNC`
- **Macros:** `${ device.ZMSP_LAST_SYNC }`

Nombre simplificado: Servicio de localización habilitado

- **Elemento web:** `DEVICE_LOCATOR`
- **Macros:** `${ device.DEVICE_LOCATOR }`

Nombre simplificado: Dirección MAC

- **Elemento web:** `MAC_ADDRESS`
- **Macros:** `${ device.MAC_ADDRESS }`

Nombre simplificado: Conexión de red de la dirección MAC

- **Elemento web:** `MAC_NETWORK_CONNECTION`
- **Macros:** `${ device.MAC_NETWORK_CONNECTION }`

Nombre simplificado: Tipo de dirección MAC

- **Elemento web:** `MAC_ADDRESS_TYPE`
- **Macros:** `${ device.MAC_ADDRESS_TYPE }`

Nombre simplificado: Configuración de buzón

- **Elemento web:** `GOOGLE_AW_DIRECTORY_MAILBOX_SETUP`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP }`

Nombre simplificado: Batería principal

- **Elemento web:** `MAIN_BATTERY_PERCENT`
- **Macros:** `${ device.MAIN_BATTERY_PERCENT }`

Nombre simplificado: Modo perdido de MDM habilitado

- **Elemento web:** `IS_MDM_LOST_MODE_ENABLED`
- **Macros:** `${ device.IS_MDM_LOST_MODE_ENABLED }`

Nombre simplificado: `MDX_SHARED_ENCRYPTION_KEY`

- **Elemento web:** `MDX_SHARED_ENCRYPTION_KEY`
- **Macros:** `${ device.MDX_SHARED_ENCRYPTION_KEY }`

Nombre simplificado MEID

- **Elemento web:** `MEID`
- **Macros:** `${ device.MEID }`

Nombre simplificado: Número de teléfono móvil

- **Elemento web:** TEL_NUMBER
- **Macros:** \${ device.TEL_NUMBER }

Nombre simplificado: ID del modelo

- **Elemento web:** MODEL_ID
- **Macros:** \${ device.MODEL_ID }

Nombre simplificado: Número de modelo

- **Elemento web:** MODEL_NUMBER
- **Macros:** \${ device.MODEL_NUMBER }

Nombre simplificado: Tipo de adaptador de red

- **Elemento web:** NETWORK_ADAPTER_TYPE
- **Macros:** \${ device.NETWORK_ADAPTER_TYPE }

Nombre simplificado: Compilación del sistema operativo

- **Elemento web:** SYSTEM_OS_BUILD
- **Macros:** \${ device.SYSTEM_OS_BUILD }

Nombre simplificado: Edición del sistema operativo

- **Elemento web:** OS_EDITION
- **Macros:** \${ device.OS_EDITION }

Nombre simplificado: Idioma del sistema operativo (configuración regional)

- **Elemento web:** SYSTEM_LANGUAGE
- **Macros:** \${ device.SYSTEM_LANGUAGE }

Nombre simplificado: Versión del sistema operativo

- **Elemento web:** SYSTEM_OS_VERSION
- **Macros:** \${ device.SYSTEM_OS_VERSION }

Nombre simplificado: Dirección de la organización

- **Elemento web:** ORGANIZATION_ADDRESS
- **Macros:** \${ device.ORGANIZATION_ADDRESS }

Nombre simplificado: Correo electrónico de la organización

- **Elemento web:** ORGANIZATION_EMAIL
- **Macros:** \${ device.ORGANIZATION_EMAIL }

Nombre simplificado: Organization magic (Ámbito de actividad de la organización)

- **Elemento web:** ORGANIZATION_MAGIC
- **Macros:** \${ device.ORGANIZATION_MAGIC }

Nombre simplificado: Nombre de la organización

- **Elemento web:** ORGANIZATION_NAME
- **Macros:** \${ device.ORGANIZATION_NAME }

Nombre simplificado: Número de teléfono de la organización

- **Elemento web:** ORGANIZATION_PHONE
- **Macros:** \${ device.ORGANIZATION_PHONE }

Nombre simplificado: No conforme

- **Elemento web:** OUT_OF_COMPLIANCE
- **Macros:** \${ device.OUT_OF_COMPLIANCE }

Nombre simplificado: Propietario

- **Elemento web:** CORPORATE_OWNED
- **Macros:** \${ device.CORPORATE_OWNED }

Nombre simplificado: Código de acceso conforme

- **Elemento web:** PASSCODE_IS_COMPLIANT
- **Macros:** \${ device.PASSCODE_IS_COMPLIANT }

Nombre simplificado: Código de acceso conforme con configuración

- **Elemento web:** PASSCODE_IS_COMPLIANT_WITH_CFG
- **Macros:** \${ device.PASSCODE_IS_COMPLIANT_WITH_CFG }

Nombre simplificado: Código de acceso presente

- **Elemento web:** PASSCODE_PRESENT
- **Macros:** \${ device.PASSCODE_PRESENT }

Nombre simplificado: PCRO

- **Elemento web:** `WINDOWS_HAS_PCRO`
- **Macros:** `${ device.WINDOWS_HAS_PCRO }`

Nombre simplificado: Infracción de perímetro

- **Elemento web:** `GPS_PERIMETER_BREACH`
- **Macros:** `${ device.GPS_PERIMETER_BREACH }`

Nombre simplificado: Comprobación periódica

- **Elemento web:** `PerformPeriodicCheck`
- **Macros:** `${ device.PerformPeriodicCheck }`

Nombre simplificado: Hotspot personal activado

- **Elemento web:** `PERSONAL_HOTSPOT_ENABLED`
- **Macros:** `${ device.PERSONAL_HOTSPOT_ENABLED }`

Nombre simplificado: Código PIN de la geocerca

- **Elemento web:** `PIN_CODE_FOR_GEO_FENCE`
- **Macros:** `${ device.PIN_CODE_FOR_GEO_FENCE }`

Nombre simplificado: Plataforma

- **Elemento web:** `SYSTEM_PLATFORM`
- **Macros:** `${ device.SYSTEM_PLATFORM }`

Nombre simplificado: Nivel de API de la plataforma

- **Elemento web:** `API_LEVEL`
- **Macros:** `${ device.API_LEVEL }`

Nombre simplificado: Nombre de la directiva

- **Elemento web:** `POLICY_NAME`
- **Macros:** `${ device.POLICY_NAME }`

Nombre simplificado: Número de teléfono principal

- **Elemento web:** `IDENTITY1_PHONENUMBER`
- **Macros:** `${ device.IDENTITY1_PHONENUMBER }`

Nombre simplificado: Operador de SIM principal

- **Elemento web:** `IDENTITY1_CARRIER_NETWORK_OPERATOR`
- **Macros:** `${ device.IDENTITY1_CARRIER_NETWORK_OPERATOR }`

Nombre simplificado: ICCID de SIM principal

- **Elemento web:** `IDENTITY1_ICCID`
- **Macros:** `${ device.IDENTITY1_ICCID }`

Nombre simplificado: IMEI de SIM principal

- **Elemento web:** `IDENTITY1_IMEI`
- **Macros:** `${ device.IDENTITY1_IMEI }`

Nombre simplificado: IMSI de SIM principal

- **Elemento web:** `IDENTITY1_IMSI`
- **Macros:** `${ device.IDENTITY1_IMSI }`

Nombre simplificado: Itinerancia de SIM principal

- **Elemento web:** `IDENTITY1_ROAMING`
- **Macros:** `${ device.IDENTITY1_ROAMING }`

Nombre simplificado: Itinerancia de SIM principal

- **Elemento web:** `IDENTITY1_ROAMING_COMPLIANCE`
- **Macros:** `${ device.IDENTITY1_ROAMING_COMPLIANCE }`

Nombre simplificado: Nombre del producto

- **Elemento web:** `PRODUCT_NAME`
- **Macros:** `${ device.PRODUCT_NAME }`

Nombre simplificado: ID de dispositivo publicador

- **Elemento web:** `PUBLISHER_DEVICE_ID`
- **Macros:** `${ device.PUBLISHER_DEVICE_ID }`

Nombre simplificado: Reset Count (Recuento de restablecimientos)

- **Elemento web:** `WINDOWS_HAS_RESET_COUNT`
- **Macros:** `${ device.WINDOWS_HAS_RESET_COUNT }`

Nombre simplificado: Restart Count (Recuento de reinicios)

- **Elemento web:** `WINDOWS_HAS_RESTART_COUNT`
- **Macros:** `${ device.WINDOWS_HAS_RESTART_COUNT }`

Nombre simplificado: Safe Mode Enabled?

- **Elemento web:** `WINDOWS_HAS_SAFE_MODE`
- **Macros:** `${ device.WINDOWS_HAS_SAFE_MODE }`

Nombre simplificado: SBCP Hash

- **Elemento web:** `WINDOWS_HAS_SBCP_HASH`
- **Macros:** `${ device.WINDOWS_HAS_SBCP_HASH }`

Nombre simplificado: Pantalla: altura

- **Elemento web:** `SCREEN_HEIGHT`
- **Macros:** `${ device.SCREEN_HEIGHT }`

Nombre simplificado: Pantalla: cantidad de colores

- **Elemento web:** `SCREEN_NB_COLORS`
- **Macros:** `${ device.SCREEN_NB_COLORS }`

Nombre simplificado: Pantalla: tamaño

- **Elemento web:** `SCREEN_SIZE`
- **Macros:** `${ device.SCREEN_SIZE }`

Nombre simplificado: Pantalla: anchura

- **Elemento web:** `SCREEN_WIDTH`
- **Macros:** `${ device.SCREEN_WIDTH }`

Nombre simplificado: Pantalla: resolución horizontal

- **Elemento web:** `SCREEN_XDPI`
- **Macros:** `${ device.SCREEN_XDPI }`

Nombre simplificado: Pantalla: resolución vertical

- **Elemento web:** `SCREEN_YDPI`
- **Macros:** `${ device.SCREEN_YDPI }`

Nombre simplificado: Número de teléfono secundario

- **Elemento web:** `IDENTITY2_PHONENUMBER`
- **Macros:** `${ device.IDENTITY2_PHONENUMBER }`

Nombre simplificado: Operador de SIM secundaria

- **Elemento web:** `IDENTITY2_CARRIER_NETWORK_OPERATOR`
- **Macros:** `${ device.IDENTITY2_CARRIER_NETWORK_OPERATOR }`

Nombre simplificado: ICCID de SIM secundaria

- **Elemento web:** `IDENTITY2_ICCID`
- **Macros:** `${ device.IDENTITY2_ICCID }`

Nombre simplificado: IMEI de SIM secundaria

- **Elemento web:** `IDENTITY2_IMEI`
- **Macros:** `${ device.IDENTITY2_IMEI }`

Nombre simplificado: IMSI de SIM secundaria

- **Elemento web:** `IDENTITY2_IMSI`
- **Macros:** `${ device.IDENTITY2_IMSI }`

Nombre simplificado: Itinerancia de SIM secundaria

- **Elemento web:** `IDENTITY2_ROAMING`
- **Macros:** `${ device.IDENTITY2_ROAMING }`

Nombre simplificado: Conformidad de itinerancia de SIM secundaria

- **Elemento web:** `IDENTITY2_ROAMING_COMPLIANCE`
- **Macros:** `${ device.IDENTITY2_ROAMING_COMPLIANCE }`

Nombre simplificado: Secure Boot Enabled?

- **Elemento web:** `WINDOWS_HAS_SECURE_BOOT_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_SECURE_BOOT_ENABLED }`

Nombre simplificado: Estado de Arranque seguro

- **Elemento web:** `SECURE_BOOT_STATE`
- **Macros:** `${ device.SECURE_BOOT_STATE }`

Nombre simplificado: Contenedor seguro habilitado

- **Elemento web:** `DLP_ACTIVE`
- **Macros:** `${ device.DLP_ACTIVE }`

Nombre simplificado: Nivel de parche de seguridad

- **Elemento web:** `SYSTEM_SECURITY_PATCH_LEVEL`
- **Macros:** `${ device.SYSTEM_SECURITY_PATCH_LEVEL }`

Nombre simplificado: Número de serie

- **Elemento web:** `SERIAL_NUMBER`
- **Macros:** `${ device.SERIAL_NUMBER }`

Nombre simplificado: Capacidad para SMS

- **Elemento web:** `IS_SMS_CAPABLE`
- **Macros:** `${ device.IS_SMS_CAPABLE }`

Nombre simplificado: Supervisado

- **Elemento web:** `SUPERVISED`
- **Macros:** `${ device.SUPERVISED }`

Nombre simplificado: Motivo de suspensión

- **Elemento web:** `GOOGLE_AW_DIRECTORY_SUSPENTION_REASON`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON }`

Nombre simplificado: Estado manipulado

- **Elemento web:** `TAMPERED_STATUS`
- **Macros:** `${ device.TAMPERED_STATUS }`

Nombre simplificado: Términos y condiciones

- **Elemento web:** `TERMS_AND_CONDITIONS`
- **Macros:** `${ device.TERMS_AND_CONDITIONS }`

Nombre simplificado: ¿Se aceptaron los términos de uso y el contrato?

- **Elemento web:** `GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS`
- **Macros:** `${ device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS }`

Nombre simplificado: Test Signing Enabled?

- **Elemento web:** `WINDOWS_HAS_TEST_SIGNING_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_TEST_SIGNING_ENABLED }`

Nombre simplificado: Total de RAM

- **Elemento web:** `MEMORY`
- **Macros:** `${ device.MEMORY }`

Nombre simplificado: Total de espacio de almacenamiento

- **Elemento web:** `TOTAL_DISK_SPACE`
- **Macros:** `${ device.TOTAL_DISK_SPACE }`

Nombre simplificado: Versión de TPM

- **Elemento web:** `TPM_VERSION`
- **Macros:** `${ device.TPM_VERSION }`

Nombre simplificado: UDID

- **Elemento web:** `UDID`
- **Macros:** `${ device.UDID }`

Nombre simplificado: Estado del control de cuentas de usuario

- **Elemento web:** `UAC_STATUS`
- **Macros:** `${ device.UAC_STATUS }`

Nombre simplificado: Agente de usuario

- **Elemento web:** `USER_AGENT`
- **Macros:** `${ device.USER_AGENT }`

Nombre simplificado: Definido por el usuario #1

- **Elemento web:** `USER_DEFINED_1`
- **Macros:** `${ device.USER_DEFINED_1 }`

Nombre simplificado: Definido por el usuario #2

- **Elemento web:** `USER_DEFINED_2`
- **Macros:** `${ device.USER_DEFINED_2 }`

Nombre simplificado: Definido por el usuario #3

- **Elemento web:** `USER_DEFINED_3`
- **Macros:** `${ device.USER_DEFINED_3 }`

Nombre simplificado: Idioma del usuario (configuración regional)

- **Elemento web:** `USER_LANGUAGE`
- **Macros:** `${ device.USER_LANGUAGE }`

Nombre simplificado: Proveedor

- **Elemento web:** `VENDOR`
- **Macros:** `${ device.VENDOR }`

Nombre simplificado: Capacidad para voz

- **Elemento web:** `IS_VOICE_CAPABLE`
- **Macros:** `${ device.IS_VOICE_CAPABLE }`

Nombre simplificado: Itinerancia de voz permitida

- **Elemento web:** `VOICE_ROAMING_ENABLED`
- **Macros:** `${ device.VOICE_ROAMING_ENABLED }`

Nombre simplificado: VSM Enabled?

- **Elemento web:** `WINDOWS_HAS_VSM_ENABLED`
- **Macros:** `${ device.WINDOWS_HAS_VSM_ENABLED }`

Nombre simplificado: Dirección MAC de Wi-Fi

- **Elemento web:** `WIFI_MAC`
- **Macros:** `${ device.WIFI_MAC }`

Nombre simplificado: `WINDOWS_ENROLLMENT_KEY`

- **Elemento web:** `WINDOWS_ENROLLMENT_KEY`
- **Macros:** `${ device.WINDOWS_ENROLLMENT_KEY }`

Nombre simplificado: WinPE Enabled?

- **Elemento web:** `WINDOWS_HAS_WINPE`
- **Macros:** `${ device.WINDOWS_HAS_WINPE }`

Nombre simplificado: Estado de notificación WNS

- **Elemento web:** `PROPERTY_WNS_PUSH_STATUS`
- **Macros:** `${ device.PROPERTY_WNS_PUSH_STATUS }`

Nombre simplificado: URL de notificación WNS

- **Elemento web:** `PROPERTY_WNS_PUSH_URL`
- **Macros:** `${ device.PROPERTY_WNS_PUSH_URL }`

Nombre simplificado: Fecha de caducidad de URL de notificación WNS

- **Elemento web:** `PROPERTY_WNS_PUSH_URL_EXPIRY`
- **Macros:** `${ device.PROPERTY_WNS_PUSH_URL_EXPIRY }`

Nombre simplificado: ID del agente de Citrix Endpoint Management

- **Elemento web:** `ENROLLMENT_AGENT_ID`
- **Macros:** `{device.ENROLLMENT_AGENT_ID}'`

Nombre simplificado: Revisión del agente de Citrix Endpoint Management

- **Elemento web:** `EW_REVISION`
- **Macros:** `${ device.EW_REVISION }`

Nombre simplificado: Versión del agente de Citrix Endpoint Management

- **Elemento web:** `EW_VERSION`
- **Macros:** `${ device.EW_VERSION }`

Nombre simplificado: API de Zebra disponible

- **Elemento web:** `ZEBRA_MDM`
- **Macros:** `${ device.ZEBRA_MDM }`

Nombre simplificado: Versión de Zebra MXMF

- **Elemento web:** `ZEBRA_MDM_VERSION`
- **Macros:** `${ device.ZEBRA_MDM_VERSION }`

Nombre simplificado: Versión del parche de Zebra

- **Elemento web:** `ZEBRA_PATCH_VERSION`
- **Macros:** `${ device.ZEBRA_PATCH_VERSION }`

Macros para obtener propiedades integradas de usuario

Nombre simplificado	Macros
<code>domainname</code> (nombre de dominio; dominio predeterminado)	<code>\${ user.domainname }</code>
<code>loginname</code> (nombre de usuario más nombre de dominio)	<code>\${ user.loginname }</code>
<code>username</code> (nombre de inicio de sesión menos el dominio, si existe alguno)	<code>\${ user.username }</code>

Macros para todas las propiedades de usuario

Nombre simplificado	Elemento web	Macros
Intentos fallidos de inicio de sesión en Active Directory	<code>badpwdcount</code>	<code>\${ user.badpwdcount }</code>
Correo electrónico de usuario de ActiveSync	<code>asuseremail</code>	<code>\${ user.asuseremail }</code>
Origen de datos de ASM	<code>asmpersonsource</code>	<code>\${ user.asmpersonsource }</code>
Nombre de cuenta del Programa de implementación de ASM	<code>asmdepaccount</code>	<code>\${ user.asmdepaccount }</code>
ID de Apple administrado por ASM	<code>asmpersonmanagedappleid</code>	<code>\${ user.asmpersonmanagedappleid }</code>
Tipo de código de acceso de ASM	<code>asmpersonpasscodetype</code>	<code>\${ user.asmpersonpasscodetype }</code>
ID personal de ASM	<code>asmpersonid</code>	<code>\${ user.asmpersonid }</code>
Estado personal de ASM	<code>asmpersonstatus</code>	<code>\${ user.asmpersonstatus }</code>
Título personal de ASM	<code>asmpersontitle</code>	<code>\${ user.asmpersontitle }</code>
ID personal único de ASM	<code>asmpersonuniqueid</code>	<code>\${ user.asmpersonuniqueid }</code>

Nombre simplificado	Elemento web	Macros
ID del sistema de origen de ASM	<code>asmpersonsourcesystemid</code>	<code>\${ user. asmpersonsourcesystemid }</code>
Curso del estudiante de ASM	<code>asmpersongrade</code>	<code>\${ user. asmpersongrade }</code>
Correo electrónico de usuario de BES	<code>besuseremail</code>	<code>\${ user.besuseremail }</code>
Empresa	<code>company</code>	<code>\${ user.company }</code>
Nombre de la empresa	<code>companyname</code>	<code>\${ user.companyname }</code>
País	<code>c</code>	<code>\${ user.c }</code>
Departamento	<code>department</code>	<code>\${ user.department }</code>
Descripción	<code>description</code>	<code>\${ user.description }</code>
Usuario inhabilitado	<code>disableduser</code>	<code>\${ user.disableduser }</code>
Nombre simplificado	<code>displayname</code>	<code>\${ user.displayname }</code>
Nombre distintivo	<code>distinguishedname</code>	<code>\${ user. distinguishedname }</code>
Nombre del dominio	<code>domainname</code>	<code>\${ user.domainname }</code>
Correo electrónico	<code>mail</code>	<code>\${ user.mail }</code>
Nombre de pila	<code>givenname</code>	<code>\${ user.givenname }</code>
Dirección del domicilio	<code>homestreetaddress</code>	<code>\${ user. homestreetaddress }</code>
Ciudad del domicilio	<code>homecity</code>	<code>\${ user.homecity }</code>
País del domicilio	<code>homecountry</code>	<code>\${ user.homecountry }</code>
Fax del domicilio	<code>homefax</code>	<code>\${ user.homefax }</code>
Teléfono del domicilio	<code>homephone</code>	<code>\${ user.homephone }</code>
Estado/región del domicilio	<code>homestate</code>	<code>\${ user.homestate }</code>
Código postal del domicilio	<code>homezip</code>	<code>\${ user.homezip }</code>
Teléfono IP	<code>iphone</code>	<code>\${ user.iphone }</code>
Iniciales	<code>middleinitial</code>	<code>\${ user.middleinitial }</code>

Nombre simplificado	Elemento web	Macros
Segundo nombre	<code>middlename</code>	<code>\${ user.middlename }</code>
Móvil	<code>mobile</code>	<code>\${ user.mobile }</code>
Nombre	<code>cn</code>	<code>\${ user.cn }</code>
Dirección de la oficina	<code>physicaldeliveryofficename</code>	<code>\${ user. physicaldeliveryofficename }</code>
Ciudad de la oficina	<code>l</code>	<code>\${ user.l }</code>
Fax de la oficina	<code>facsimiletelephonenumber</code>	<code>\${ user. facsimiletelephonenumber }</code>
Estado/provincia de la oficina	<code>st</code>	<code>\${ user.st }</code>
Calle de la oficina	<code>officestreetaddress</code>	<code>\${ user. officestreetaddress }</code>
Teléfono de la oficina	<code>telephonenumber</code>	<code>\${ user. telephonenumber }</code>
Código postal de la oficina	<code>postalcode</code>	<code>\${ user.postalcode }</code>
Apartado de correos	<code>postofficebox</code>	<code>\${ user.postofficebox }</code>
Buscapersonas	<code>pager</code>	<code>\${ user.pager }</code>
ID de grupo principal	<code>primarygroupid</code>	<code>\${ user. primarygroupid }</code>
Cuenta SAM	<code>samaccountname</code>	<code>\${ user. samaccountname }</code>
Calle	<code>streetaddress</code>	<code>\${ user.streetaddress }</code>
Surname	<code>sn</code>	<code>\${ user.sn }</code>
Título	<code>title</code>	<code>\${ user.title }</code>
Nombre de inicio de sesión del usuario	<code>userprincipalname</code>	<code>\${ user. userprincipalname }</code>

Acciones automatizadas

March 1, 2024

En Citrix Endpoint Management, puede crear acciones automatizadas para programar una reacción a:

- Eventos
- Propiedades de usuario o dispositivo
- La presencia de aplicaciones en los dispositivos de usuario

Cuando crea una acción automatizada, los desencadenantes definidos para la acción determinan qué sucede en el dispositivo del usuario cuando este se conecta a Citrix Endpoint Management. Cuando un evento tiene lugar, usted puede enviar una notificación al usuario para que este corrija el problema antes de tomar medidas más terminantes.

Los efectos automáticos que establezca varían entre:

- Borrar totalmente o de forma selectiva el dispositivo.
- Establecer el dispositivo como dispositivo que no cumple los requisitos.
- Revocar el dispositivo.
- Enviar una notificación al usuario para corregir el problema antes de tomar medidas más terminantes.

Las acciones de bloqueo y borrado de aplicaciones solo se pueden configurar en el modo de solo MAM.

Puede utilizar acciones automatizadas para marcar dispositivos con Windows 10 o Windows 11 unidos a Azure Active Directory como no conformes en Azure AD.

Nota:

Para poder notificar a los usuarios, primero debe configurar servidores de notificaciones en los parámetros 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 notificaciones que vaya a utilizar antes de continuar. Para obtener más información, consulte [Notificaciones](#). Consulte [Crear y actualizar plantillas de notificaciones](#).

Acciones de ejemplo

Estos son algunos ejemplos del uso de acciones automatizadas:

Ejemplo 1

- Quiere detectar una aplicación que ha bloqueado previamente (por ejemplo, “Words with Friends”). Puedes especificar un desencadenador que marcar el dispositivo del usuario como no conforme tras detectar la aplicación “Words with Friends”. Luego, la acción notifica a los usuarios de que quitar eliminar la aplicación para que su dispositivo vuelva a marcarse como conforme. También puede establecer un límite de tiempo de espera para que los usuarios realicen las acciones correctivas pertinentes. Después de ese límite de tiempo, se produce la acción definida (como borrar selectivamente el dispositivo).

Ejemplo 2

- Quiere verificar si los clientes están utilizando el firmware más reciente y bloquear el acceso a los recursos si los usuarios no tienen sus dispositivos actualizados. Puede especificar un desencadenante que establezca el dispositivo de usuario como no conforme cuando este no tenga la versión más reciente. Utilice las acciones automatizadas para bloquear recursos y notificar a los clientes.

Ejemplo tres

- Un dispositivo de usuario se establece en el estado no conforme y el usuario corrige el problema con el dispositivo. Puede configurar una directiva para implementar un paquete que restablezca el dispositivo al estado conforme.

Ejemplo cuatro

- Quiere marcar como no conformes los dispositivos de usuario que han estado inactivos durante un período de tiempo determinado. Puede crear una acción automatizada para dispositivos inactivos de la siguiente manera:
 1. En la consola de Citrix Endpoint Management, vaya a **Parámetros > Control de acceso de red** y, a continuación, seleccione **Dispositivos inactivos**. Para obtener información sobre el parámetro **Dispositivos inactivos**, consulte [Control de acceso de red](#).
 2. Siga los pasos para agregar una acción, tal y como se describe en [Agregar y administrar acciones](#). La única diferencia es que configura los parámetros siguientes en la página **Detalles de la acción**:
 - **Desencadenante**. Seleccione **Propiedad del dispositivo, No conforme y Verdadero**.
 - **Acción**. Seleccione **Enviar notificación** y, a continuación, una plantilla que haya creado con **Plantilla de notificación** en **Parámetros**. A continuación, establezca la demora en días, horas o minutos antes de realizar la acción. Establezca el intervalo durante el que se repite la acción hasta que el usuario solucione el problema que ha provocado la activación del desencadenante.

Consejo:

Para eliminar dispositivos inactivos en bloque, use la [API de REST pública de Citrix Endpoint Management](#). Obtenga, en primer lugar, el ID de dispositivo de los dispositivos inactivos que quiere eliminar y, a continuación, ejecute la API de eliminación para eliminarlos en bloque.

Agregar y administrar acciones

Para agregar, modificar y filtrar acciones automatizadas:

1. En la consola de Citrix Endpoint Management, haga clic en **Configurar > Acciones**. Aparecerá la página **Acciones**.
2. En la página **Acciones**, lleve a cabo alguna de estas acciones:
 - Haga clic en **Agregar** para agregar una acción.
 - Seleccione una acción existente para modificarla o eliminarla. Haga clic en la opción pertinente.
3. Aparecerá la página **Información de la acción**.
4. En la página **Información de la acción**, escriba o modifique la información siguiente:
 - **Nombre:** Escriba un nombre para identificar la acción. Este campo es obligatorio.
 - **Descripción:** Describa qué debe hacer la acción.
5. Haga clic en **Siguiente**. Aparecerá la página **Detalles de la acción**.

En el siguiente ejemplo, se muestra cómo configurar un desencadenante de **eventos**. Si selecciona otro desencadenante, las opciones resultantes difieren de las mostradas aquí.

6. En la página **Detalles de la acción**, escriba o modifique la información siguiente:

En la lista **Desencadenante**, haga clic en el tipo de desencadenante de eventos para esta acción. Seleccione uno de los siguientes desencadenantes:

- **Evento:** Comprueba si el estado del dispositivo coincide con el evento de incumplimiento seleccionado y, a continuación, reacciona a él.
- **Propiedad del dispositivo:** Consulta un atributo en un dispositivo administrado por MDM y, a continuación, reacciona a él. Para obtener más información, consulte el documento PDF [Valores y nombres de propiedades de dispositivo](#).
- **Propiedad del usuario:** Reacciona a un valor concreto del atributo de usuario, generalmente de Active Directory.
- **Nombre de la aplicación instalada:** Reacciona ante una aplicación instalada. No se aplica al modo solo MAM. Requiere que la directiva “Inventario de aplicaciones” esté habilitada en el dispositivo. De forma predeterminada, la directiva “Inventario de aplicaciones” está habilitada en todas las plataformas. Para obtener más información, consulte [Directiva de inventario de aplicaciones](#).
- **Valor devuelto por la directiva:** Comprueba si el valor devuelto por los scripts de PowerShell cumple determinados criterios lógicos. La directiva de Agente de Windows debe estar habilitada y configurada. Para obtener más información acerca de la directiva Agente Windows, consulte [Directiva de Agente de Windows](#).

7. En la siguiente lista, haga clic en la respuesta del desencadenante.

8. En la lista **Acción**, haga clic en la acción que se debe realizar cuando se cumplan los criterios del desencadenante. A excepción de la acción **Enviar notificación**, puede elegir un intervalo de tiempo en que los usuarios puedan resolver el problema que haya activado el desencadenante.

Si el problema no se resuelve en ese período de tiempo, se llevará a cabo la acción seleccionada. Para ver la definición de las acciones, consulte [Acciones de seguridad](#).

Si elige **Enviar notificación**, use los siguientes pasos para enviar una acción de notificación.

9. En la siguiente lista, seleccione la plantilla a utilizar para la notificación. Aparecerán las plantillas de las notificaciones pertinentes para el evento seleccionado. Si no hay plantilla para el tipo de notificación, se le solicitará que configure una plantilla con el mensaje: “No hay ninguna plantilla para este tipo de evento”. Cree una plantilla en **Plantilla de notificación**, en **Parámetros**.

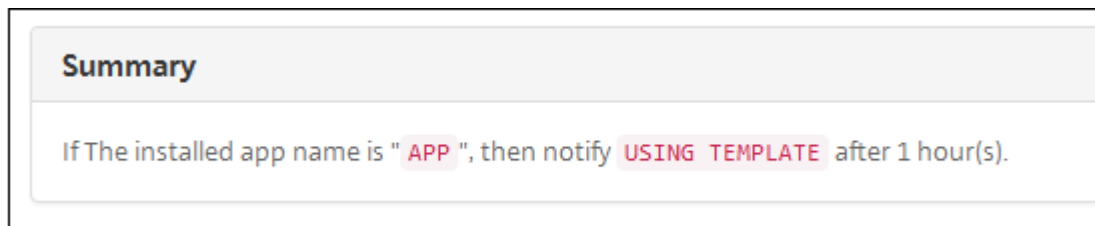
Para poder notificar a los usuarios, utilice **Parámetros > Servidor de notificaciones** para definir la configuración de SMTP de modo que Citrix Endpoint Management pueda enviar los mensajes. Consulte [Notificaciones](#). Además, antes de continuar, utilice **Parámetros > Plantilla de notificaciones** para configurar las plantillas que va a usar. Consulte [Crear y actualizar plantillas de notificaciones](#).

Después de seleccionar la plantilla, haga clic en **Vista previa del mensaje de notificación**.

10. En los siguientes campos, configure la demora en días, horas o minutos antes de realizar la acción. Establezca el intervalo durante el que se repite la acción hasta que el usuario solucione el problema que ha provocado la activación del desencadenante.



11. En **Resumen**, verifique que la acción automatizada que ha creado es la acción esperada.



12. Después de configurar los datos de la acción, puede configurar las reglas de implementación para cada plataforma individualmente. Para ello, siga el paso 13 para cada plataforma seleccionada.
13. Configure las reglas de implementación. Para obtener más información sobre cómo configurar las reglas de implementación, consulte [Implementar recursos](#).

Para este ejemplo:

- La propiedad del dispositivo debe ser **BYOD**.
 - El dispositivo debe ser conforme con el código de acceso.
 - El código de país móvil del dispositivo no puede ser solo Andorra.
14. Tras configurar las reglas de implementación de las plataformas para la acción, haga clic en **Siguiente**. Aparecerá la página de **asignaciones de acciones**, en la que puede asignar la acción a un grupo o grupos de entrega. Este paso es opcional.
15. Junto a **Elegir grupos de entrega**, escriba el nombre de un grupo de entrega para buscarlo, o bien seleccione grupos de la lista. Los grupos que seleccione aparecerán en la lista **Grupos de entrega a recibir asignaciones de aplicaciones**.
16. Expanda **Programación de implementación** y, a continuación, configure estos parámetros:
- Junto a **Implementar**, haga clic en **Sí** para programar la implementación, o bien, haga clic en **No** para cancelarla. De forma predeterminada, está **activado**. Si elige **No**, no habrá ninguna otra opción que configurar.
 - Junto a **Programación de implementación**, haga clic en **Ahora** o en **Más tarde**. La opción predeterminada es **Now**.
 - Si hace clic en **Más tarde**, haga clic en el icono de calendario y seleccione la fecha y la hora previstas para la implementación.

- Junto a **Condición de implementación**, puede hacer clic en **En cada conexión** o en **Solo cuando haya fallado la implementación anterior**. La opción predeterminada es **En cada conexión**.
- Junto a **Implementar para conexiones permanentes**, haga clic en **Sí** o **No**. De forma predeterminada, está **desactivado**.

Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Parámetros > Propiedades de servidor**.

Nota:

Esta opción se aplica cuando se ha configurado la clave de implementación en segundo plano para la programación. Esta opción se configura en **Parámetros > Propiedades de servidor**.

La opción permanente:

- No está disponible para dispositivos iOS
- No está disponible para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management a partir de la versión 10.18.19 o una posterior
- No se recomienda para Android y Android Enterprise cuando se trata de clientes que comenzaron a usar Citrix Endpoint Management antes de la versión 10.18.19

La programación de implementaciones que configure es la misma para todas las plataformas. Todos los cambios que se realicen se aplicarán a todas las plataformas, excepto la opción **Implementar para conexiones permanentes**.

17. Haga clic en **Siguiente**. Aparecerá la página **Resumen**, donde puede comprobar la configuración de la acción.
18. Haga clic en **Guardar** para guardar la acción.

Acciones de bloqueo y borrado de aplicaciones en el modo de solo MAM

Puede bloquear o borrar las aplicaciones de un dispositivo en respuesta a las cuatro categorías de desencadenantes que se enumeran en la consola de Citrix Endpoint Management: evento, propiedad de dispositivo, propiedad de usuario y nombre de aplicación instalada.

Para configurar el 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**, escriba un nombre para la acción y una descripción opcional.
4. En la página **Detalles de la acción**, seleccione el desencadenante pertinente.
5. En **Acción**, seleccione una acción.

Para este paso, no olvide las siguientes condiciones:

Si el tipo de desencadenante es **Evento**, pero el valor no es **Usuario de Active Directory inhabilitado**, las acciones **Borrado de aplicaciones** y **Bloqueo de aplicaciones** no aparecerán.

Si el tipo de desencadenante es **Propiedad del dispositivo** y el valor es **Modo perdido de MDM habilitado**, aparecerán las siguientes acciones:

- Borrar datos selectivamente del dispositivo
- Borrar datos completamente del dispositivo
- Revocar el dispositivo

Para cada opción, se establece una demora de 1 hora automáticamente, pero se puede seleccionar el periodo de demora en minutos, horas o días. La intención de la demora es dar tiempo a los usuarios para solucionar el problema antes de que ocurra la acción. Para obtener más información sobre las acciones Borrado de aplicaciones y Bloqueo de aplicaciones, consulte [Acciones de seguridad](#).

Nota:

Si establece el desencadenante en **Evento**, el intervalo de repetición es automáticamente 1 hora como mínimo. Para recibir la notificación en el dispositivo, deben actualizarse las directivas en él, es decir, debe estar sincronizado con el servidor. Por lo general, un dispositivo se sincroniza con el servidor cuando los usuarios inician sesión o actualizan manualmente sus directivas a través de Citrix Secure Hub.

También es posible que exista una demora de aproximadamente una hora antes de que la acción se lleve a cabo, para permitir que la base de datos de Active Directory se sincronice con Citrix Endpoint Management.

Device Policies Apps Media **Actions** ShareFile Enrollment Profiles Delivery Groups

Actions

- 1 Action Info
- 2 Details**
- 3 Assignment (optional)
- 4 Summary

Action details ×

Choose a trigger event and the associated action for that event.

Trigger*

Device property

Out of compliance

Is

True

Action*

App wipe

1

Hours

Summary

If device has been marked as Out of Compliance, then app wipe the device after 1 hour(s).

6. Configure las reglas de implementación y, a continuación, haga clic en **Siguiente**.
7. Configure las asignaciones de los grupos de entrega y una programación de la implementación. A continuación, haga clic en **Siguiente**.
8. Haga clic en **Guardar**.

Para comprobar el estado del bloqueo o borrado de las aplicaciones

1. Vaya a **Administrar > Dispositivos**, haga clic en un dispositivo y haga clic en **Mostrar más**.

Samsung_S5 04/14/2016 10:47:08 am 1 days

Edit Deploy Secure Notify Delete

XME Device Managed

Delivery Groups	1		Policies	0	
Actions	0		Apps	0	

Show more >

2. Vaya a **Borrado de aplicaciones de dispositivo** y **Bloqueo de aplicaciones de dispositivo**.

DevicesUsersEnrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Assigned Policies

5 Apps

6 Actions

7 Delivery Groups

8 Certificates

9 Connections

10 TouchDown

WiFi MAC Address

NONE

Bluetooth MAC Address

NONE

Device Ownership

Corporate

BYOD

Security

Strong ID

YEMXRMSG

Full Wipe of Device

No device wipe.

Selective Wipe of Device

No device selective wipe.

Lock Device

No device lock.

Device locate

No device locate.

Device App Wipe

No device App Wipe.

Device App Lock

App Lock was requested at 04/15/2016 01:59:47 pm.

Next >

Después de borrarse un dispositivo, se solicita al usuario que introduzca un código PIN. Si el usuario no consigue recordar el código, usted puede buscarlo en “Detalles del dispositivo”.

DevicesUsersEnrollment Invitations

Device details

1 General

2 Properties

3 User Properties

4 Assigned Policies

5 Apps

6 Media

7 Actions

8 Delivery Groups

9 Certificates

10 Connections

tgu3@testprise.net

General

Identifiers

Serial Number

CZVMXG8AG085

IMEI/MEID

NONE

ActiveSync ID

NONE

WiFi MAC Address

NONE

Bluetooth MAC Address

NONE

Device Ownership

Corporate

BYOD

Security

Strong ID

55S29M9B

Full Wipe of Device

Wipe was requested at 06/28/2017 02:45:01 pm with the PIN code 009634.

Selective Wipe of Device

No device selective wipe.

Lock Device

No device lock.

Marcar dispositivos con Windows 10 o Windows 11 como no conformes en Azure AD

Cuando Citrix Endpoint Management marca como no conformes dispositivos con Windows 10 o Windows 11 unidos a Azure AD, estos dispositivos también se pueden marcar como no conformes en Azure AD. Para habilitar esta función, conceda permisos para que la aplicación MDM local acceda 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 **Configuración de la aplicación MDM local**.
3. Haga clic en **Configuración de la aplicación MDM local > Permisos necesarios > Agregar > Seleccionar una API > Microsoft Graph**. Haga clic en **Seleccionar** y guarde la configuración.
4. En **Permisos necesarios**, seleccione **Microsoft Graph**. En **Habilitar acceso**, seleccione **Leer y escribir en datos de directorio**.
5. En **Permisos necesarios**, seleccione **Microsoft Graph**. Haga clic en **Conceder permisos**.
6. Haga clic en **Sí** para conceder los permisos.

Cuando un dispositivo inscrito de Azure AD con Windows 10 o Windows 11 no es conforme, Citrix Endpoint Management también lo marca como no conforme en Azure AD.

Crear una acción automatizada basada en un resultado de la directiva de Agente de Windows

Utilice la directiva “Agente Windows” para implementar scripts que supervisan los valores de Registro en escritorios y tabletas Windows administrados. Puede definir que una acción automatizada se ejecute o no en función de los valores que devuelva un script.

1. Configure una directiva de Agente de Windows y consulte los valores que devuelva el script. Para obtener más información acerca de la directiva Agente Windows, consulte [Directiva de Agente de Windows](#).

En ese artículo y en esta sección, se incluye un ejemplo basado en un script llamado `EntApp_2019_checkFirewall`. La directiva de Agente de Windows relacionada define una configuración denominada `cName_checkFirewall`. Esa configuración ejecuta el script de ejemplo.

Una vez ejecutado el script en un dispositivo, obtendrá la información necesaria para crear una acción, como se describe en [Directiva de Agente de Windows](#).

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**, escriba un nombre para la acción y una descripción opcional.
5. En la página **Detalles de la acción**, seleccione el desencadenante **Valor devuelto por la directiva**.

Action details

Choose a trigger event and the associated action for that event.

Trigger *

Policy returned value

Windows Agent

eg. policyName,configName,keyName

Is

Enter a string

6. En los campos que aparecen, defina el desencadenante y la acción:
- **Parámetros del Agente Windows:** Escriba el nombre de la directiva, el nombre de configuración y el nombre de la clave para el Agente Windows que ha creado.
 - **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 desencadene si se aplica la lógica.
 - **Introduzca una cadena:** Escriba la cadena resultante de ejecutar el script de PowerShell cargado en la directiva. Para obtener información sobre cómo localizar esa cadena, consulte [Directiva de Agente de Windows](#).
 - **Acción:** Seleccione una acción, un valor para la acción y elija una franja de tiempo para llevarla a cabo.

En nuestro ejemplo, si la clave de nombre `firewallEnabled` devuelve el valor `true`, la siguiente acción marca el dispositivo como conforme.

Actions

1 Action Info

2 Details

3 Assignment (optional)

4 Summary

Action details

Choose a trigger event and the associated action for that event.

Trigger *

Policy returned value

Windows Agent

WinAgent_2019_checkFirewall.cName_checkFirewall.firewallEnabled

Is

true

Action *

Mark the device as out of compliance

Is

False

0

Minutes

Si la clave de nombre `firewallEnabled` devuelve el valor `false`, la siguiente acción marca el dispositivo como no conforme.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

1128

Actions

1 Action Info

2 Details

3 Assignment (optional)

4 Summary

Action details

Choose a trigger event and the associated action for that event.

Trigger *

Policy returned value

Windows Agent

WinAgent_2019_checkFirewall.cName_checkFirewall.firewallEnabled

Is

false

Action *

Mark the device as out of compliance

Is

True

0

Minutes

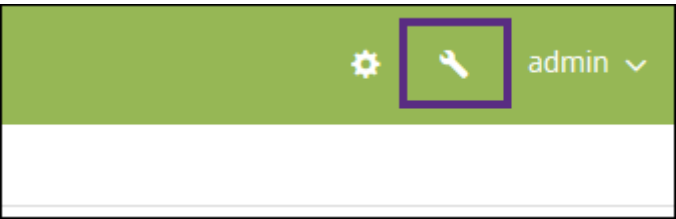
7. Si es necesario, establezca una programación de implementación y elija los grupos de entrega.

Supervisar y ofrecer asistencia

March 1, 2024

Puede utilizar el panel de mandos de Citrix Endpoint Management y la página “Asistencia” de Citrix Endpoint Management para supervisar y solucionar los problemas que presente su servidor Citrix Endpoint Management. Use la página “Asistencia” de Citrix Endpoint Management para acceder a un repertorio de datos y herramientas relacionadas con la asistencia.

En la consola de Citrix Endpoint Management, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha.



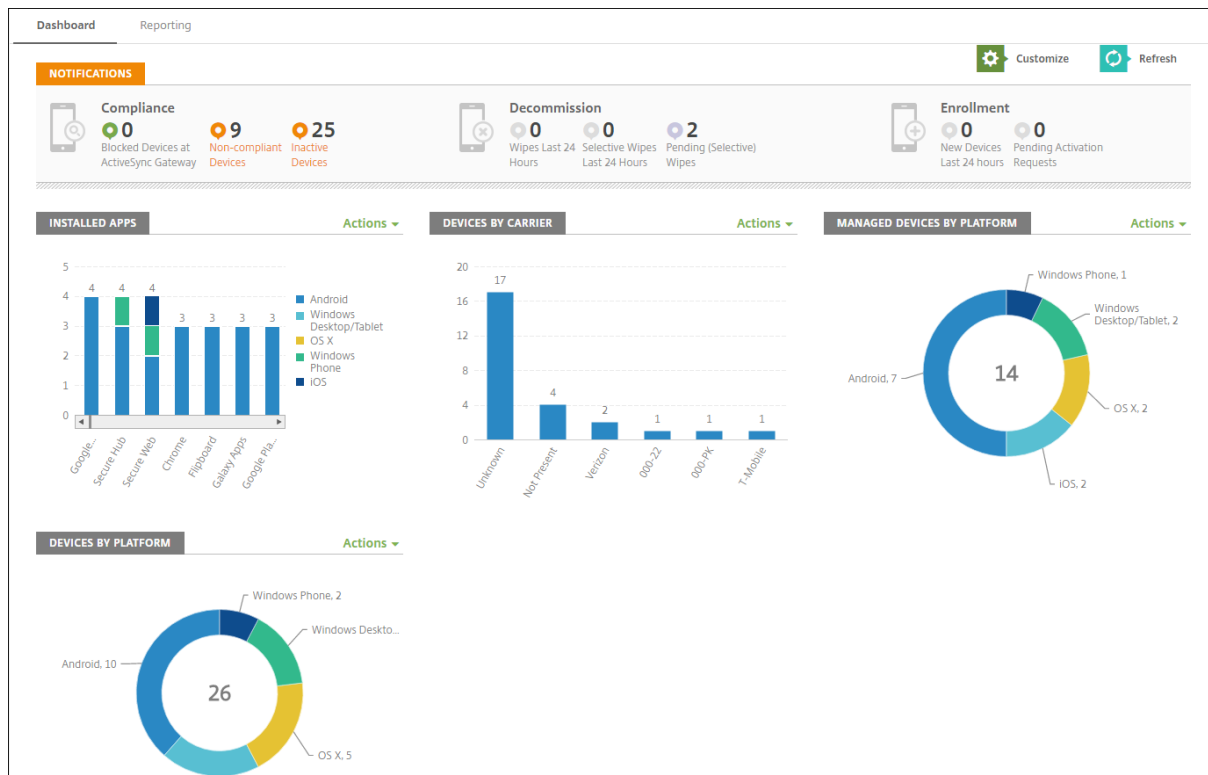
Aparece la página **Solución de problemas y asistencia**.

Use la página **Solución de problemas y asistencia** de Citrix Endpoint Management para:

- Acceder a datos de diagnóstico.
- Acceder a enlaces que llevan a la documentación de productos y al Knowledge Center de Citrix.
- Acceder a operaciones con registros.

- Utilizar las opciones de configuración avanzada.
- Acceder a un conjunto de herramientas y utilidades

Asimismo, puede ver toda la información de un vistazo desde su panel de mandos en la consola de Citrix Endpoint Management. En esta información, puede utilizar widgets para ver rápidamente los problemas y las operaciones correctas que se hayan producido.

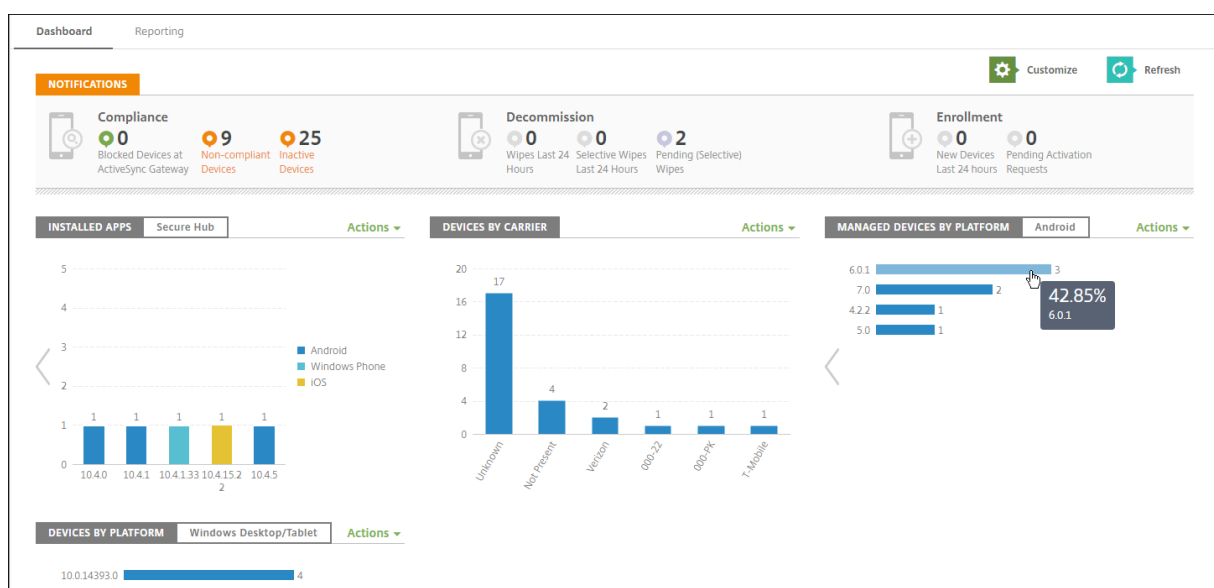


Por regla general, el panel de mandos es la página que aparece primero al iniciar sesión en la consola de Citrix Endpoint Management. Para acceder al panel de mandos desde cualquier otro sitio de la consola, haga clic en **Analizar**. Haga clic en **Personalizar** en el panel de mandos para modificar el diseño de la página y para modificar los widgets que aparecen.

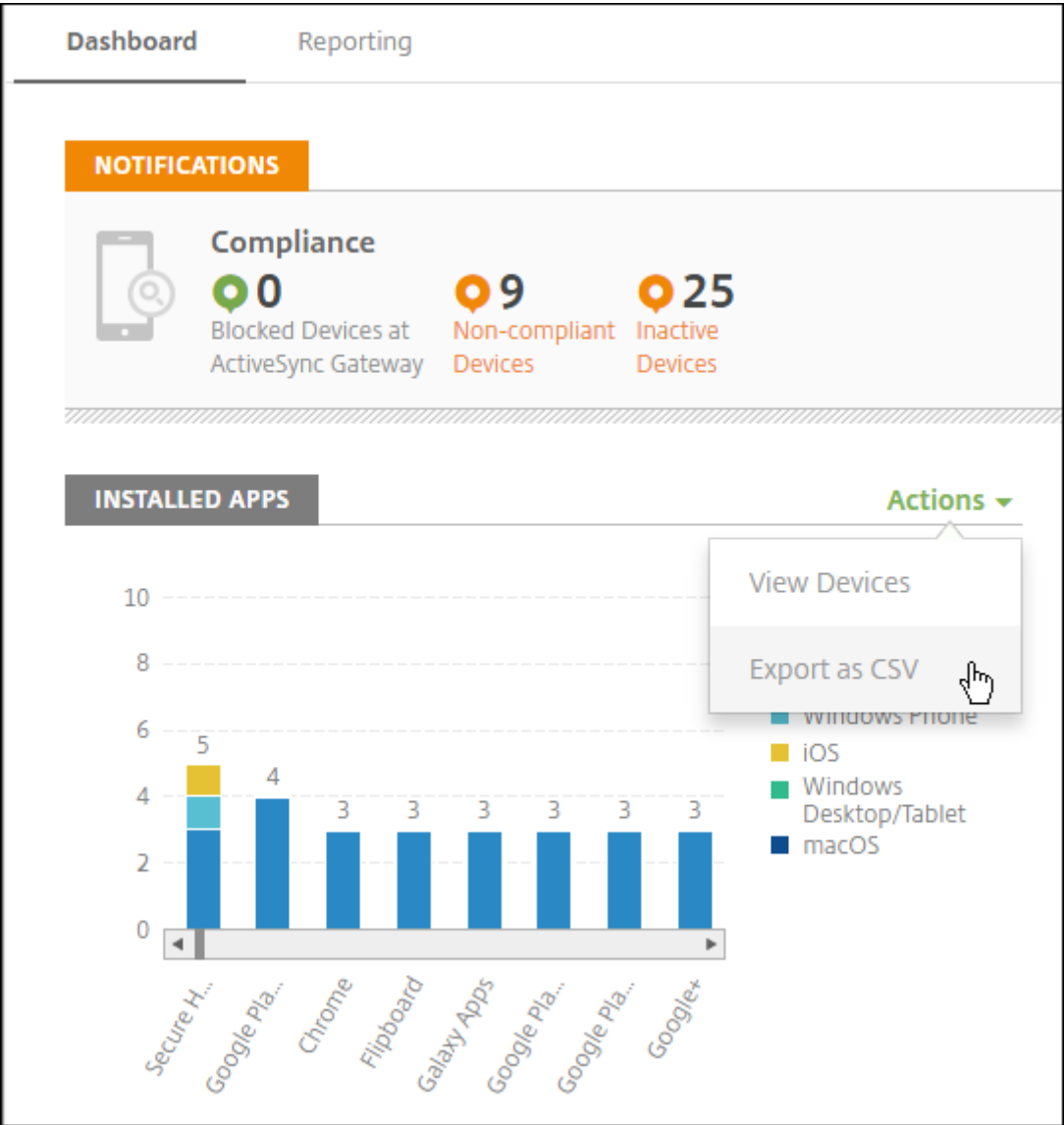
- **Mis paneles de mandos:** Puede guardar hasta cuatro paneles de mandos diferentes. Puede seleccionar cada panel guardado para verlo y modificarlo por separado.
- **Estilo de diseño:** En esta fila, puede seleccionar la cantidad de widgets que aparecerán en el panel de mandos y cómo se etiquetarán.
- **Selección de widget:** Puede elegir qué información se mostrará en el panel de mandos.
 - **Notificaciones:** Marque la casilla situada encima de los números en la parte izquierda para agregar una barra de notificaciones encima de los widgets. Esta barra muestra la cantidad de dispositivos conformes, dispositivos inactivos, dispositivos borrados o dispositivos inscritos en las últimas 24 horas.
 - **Dispositivos por plataforma:** Muestra la cantidad de dispositivos administrados y no administrados por plataforma.

- **Dispositivos por operador:** Muestra la cantidad de dispositivos administrados y no administrados por operador. Haga clic en cada barra para ver un desglose por plataforma.
- **Dispositivos administrados por plataforma:** Muestra la cantidad de dispositivos administrados por plataforma.
- **Dispositivos no administrados por plataforma:** Muestra la cantidad de dispositivos no administrados por plataforma. Los dispositivos que aparecen en este gráfico pueden tener un agente instalado, pero se podrían haber revocado sus privilegios, o el dispositivo podría haber sido borrado.
- **Dispositivos por estado de ActiveSync Gateway:** Muestra la cantidad de dispositivos agrupados por estado de ActiveSync Gateway. La información se muestra como estado Bloqueado, Permitido o Desconocido. Puede hacer clic en cada barra para desglosar los datos por plataforma.
- **Dispositivos por propietario:** Muestra la cantidad de dispositivos agrupados por propietario. La información se muestra como propiedad de la empresa, del empleado o propietario desconocido.
- **Implementaciones fallidas de grupos de entrega:** Muestra la cantidad total de implementaciones fallidas desglosadas por paquete. Solo se muestran los paquetes de implementaciones con errores.
- **Dispositivos por motivo de bloqueo:** Muestra la cantidad de dispositivos bloqueados por ActiveSync.
- **Aplicaciones instaladas:** Escriba un nombre de aplicación para ver un gráfico de información de esta.
- **Uso de licencias de aplicaciones de compras por volumen:** Muestra estadísticas sobre el uso de licencias por parte de las aplicaciones de compras por volumen de Apple.

En cada widget, puede hacer clic en partes individuales para ampliar la información mostrada.



También puede exportar la información como archivo CSV. Para ello, haga clic en el menú **Acciones**.



Página “Supervisar” para administradores de asistencia

Puede supervisar y solucionar problemas de Citrix Endpoint Management desde la página **Supervisar**. Esa interfaz está personalizada para que los administradores del servicio de ayuda puedan solucionar eficientemente los problemas de los usuarios.

Los administradores de asistencia técnica (Help Desk) deben tener los siguientes permisos para acceder a la página **Supervisar** y a todos los flujos de trabajo disponibles:

- Acceso autorizado
 - Acceso de administrador a la consola

- Acceso a API públicas
- Funciones de la consola
 - Supervisar
 - Dispositivos
 - Borrado completo de dispositivo
 - Ver ubicaciones
 - ★ Localizar dispositivos
 - ★ Seguimiento de dispositivos
 - Bloquear dispositivo
 - Desbloquear dispositivo
 - Bloqueo de aplicaciones
 - Borrado de aplicaciones
 - Aplicación

La página **Supervisar** ofrece una vista combinada de la configuración y las directivas de dispositivo. La vista incluye acciones para solucionar problemas (como bloqueo o desbloqueo de aplicaciones, borrado de aplicaciones, bloqueo o desbloqueo de dispositivos y borrado de dispositivos).

The screenshot displays the 'Device Details' page for a user named 'test user1'. The page is divided into two main sections: 'Policies' and 'Configuration'. The 'Policies' section shows a table with columns for Policy Name, Policy Status, and Resource Type. The 'Configuration' section shows a table with columns for Display Name, Operating System, RAM, Storage, External Storage, Battery, and Location. Below these sections is a 'Provisioned Applications' table with columns for Name, Created on, Last Update, Status, and Type.

Policy Name	Policy Status	Resource Type
Location Tracking	SUCCESS	LOCATIONSERVICES

Display Name	Operating System	RAM	Storage	External Storage	Battery	Location
Test User1's Iphone	iOS	0	24.82GB available of total 26.65GB	n/a	66%	

Name	Created on	Last Update	Status	Type
Work Notes	11/16/2017 2:09 PM	11/16/2017 2:09 PM	FAILURE	MDX
Secure Mail	11/21/2017 12:25 PM	11/21/2017 12:25 PM	FAILURE	MDX
Secure Web	11/21/2017 12:28 PM	11/21/2017 12:28 PM	FAILURE	MDX

Use la página **Supervisar** para:

- Buscar el usuario de Active Directory (AD) y el dispositivo que presenten problemas.
- Analice la página **Detalles del dispositivo**, que contiene lo siguiente:
 - **Directivas:** Muestra las directivas de dispositivo y aplicación relativas al 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 contiene iconos que indican si el dispositivo tiene habilitados los servicios de localización geográfica, está liberado por jailbreak o está administrado por MDM o MAM. El panel muestra también el estado de cifrado del almacenamiento.
- **Tabla de Aplicaciones en ejecución:** Muestra los datos de las aplicaciones activas en el dispositivo.
- Solucionar los problemas del dispositivo. Las acciones de seguridad disponibles en esta página se basan en la inscripción del dispositivo y los permisos disponibles para el administrador que inició sesión:
 - Bloquear o desbloquear dispositivo
 - Borrar dispositivo
 - Bloquear o desbloquear aplicación (disponible si el dispositivo está inscrito como dispositivo MAM)
 - Borrar aplicación (disponible si el dispositivo está inscrito como dispositivo MAM)

Para obtener información acerca de las acciones de que dispone, consulte [Acciones de seguridad](#).

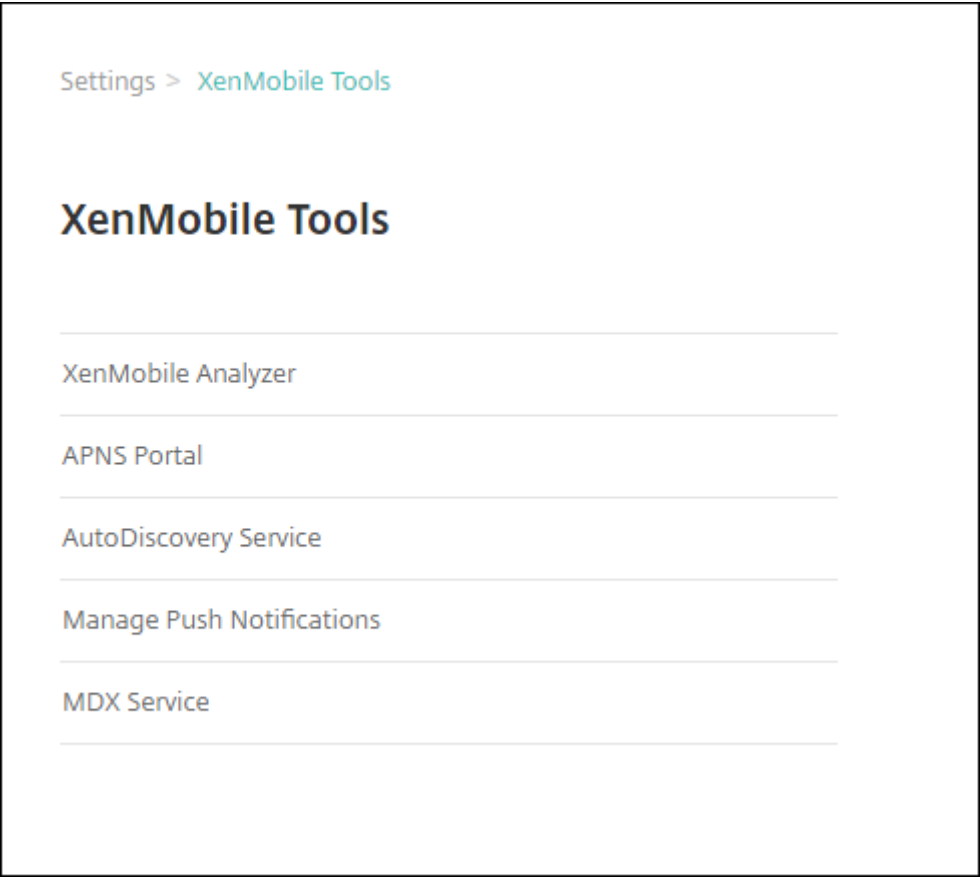
Es posible que la página “Supervisar” no funcione según lo esperado durante los 60 minutos posteriores a su última carga, ya que no gestiona las actualizaciones del token de inicio de sesión. Como solución temporal, puede actualizar el token. Para ello, vuelva a cargar la página: haga clic en el enlace **Citrix Cloud** ubicado en la consola del servicio y, a continuación, haga clic en **Citrix Endpoint Management > Administrar > Supervisar**.

Acceder 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:

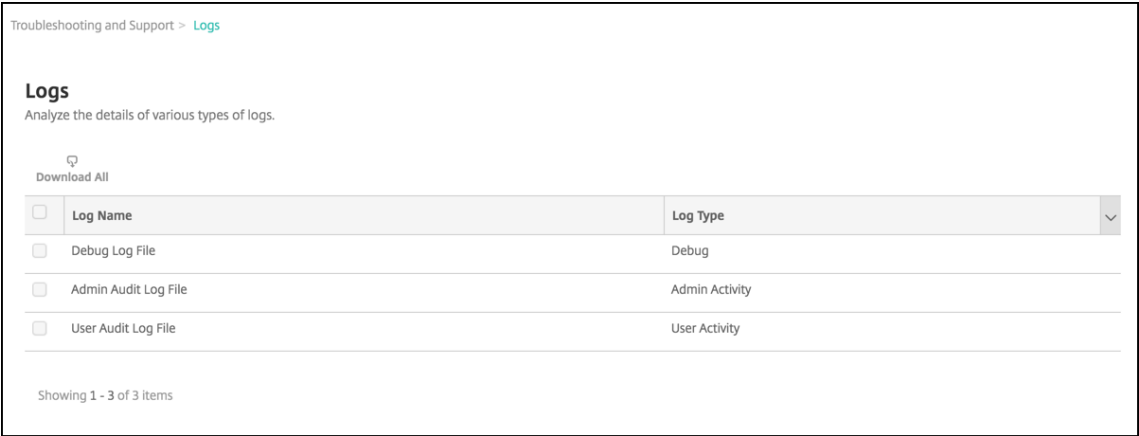
- **Portal APNs:** Con esta herramienta, puede enviar una solicitud a Citrix para que firme un certificado APNs que, a continuación, enviará a Apple.
- **Servicio de detección automática:** Con esta herramienta puede solicitar y configurar la detección automática de Citrix Endpoint Management en su dominio.
- **Administrar notificaciones push:** Con esta herramienta, puede administrar las notificaciones push de las aplicaciones para iOS y Windows.

Para acceder a estas herramientas, vaya a **Parámetros > Citrix Endpoint Management Tools**. Esta página está disponible para los usuarios con el rol de administrador de Cloud o administrador de clientes de Cloud.



Ver y analizar archivos de registros en Citrix Endpoint Management

- 1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha de la consola. Se abrirá la página **Solución de problemas y asistencia**.
- 2. En **Operaciones con registros**, haga clic en **Registros**. Aparecerá la página **Registros**. Los registros individuales se muestran en una tabla.



3. Seleccione el registro que quiera ver:

- Los archivos de registros de depuración (Debug Log File) contienen información muy útil para el servicio de asistencia Citrix Support, tal como mensajes de error y acciones relacionadas con el servidor.
- Los archivos de registros de auditoría de administración (Admin Audit Log File) contienen información de auditoría sobre actividad en la consola de Citrix Endpoint Management.
- Los archivos de registros de auditoría de usuarios (User Audit Log File) contienen información relacionada con los usuarios configurados.

4. Use las acciones de la parte superior de la tabla para descargar uno o todos los registros o simplemente verlos.

Download All View Download		
<input type="checkbox"/>	Log Name	Log Type
<input checked="" type="checkbox"/>	Debug Log File	Debug
<input type="checkbox"/>	Admin Audit Log File	Admin Activity
<input type="checkbox"/>	User Audit Log File	User Activity

Nota:

Si selecciona varios archivos de registro, solo estará disponible la opción **Descargar todo**.

5. Lleve a cabo una de las siguientes acciones:

- **Descargar todo:** La consola descarga todos los registros presentes en el sistema (incluidos los registros de depuración, auditoría de administración, auditoría de usuarios, registros del servidor, etcétera).
- **Ver:** Muestra, debajo de la tabla, el contenido de los registros seleccionados.
- **Descargar:** La consola descarga solo el tipo de archivo de registros seleccionado. La consola también descarga los registros archivados de ese mismo tipo.

Log contents for Debug Log File		
2018-11-15T06:49:40.7+0000	INFO	localhost-startStop-1 com.citrix.xmls.util.CloudUtil This is a cloud build.
2018-11-15T06:49:40.44+0000	INFO	localhost-startStop-1 com.citrix.xmls.util.CloudUtil *** Initializing Anonymization Configuration ***
2018-11-15T06:49:40.46+0000	INFO	localhost-startStop-1 com.citrix.xmls.util.CloudUtil Not generating anonymize.properties for cloud servers.
2018-11-15T06:49:40.46+0000	INFO	localhost-startStop-1 com.citrix.xmls.util.CloudUtil **** Inside EwConfig Initialize Method ****
2018-11-15T06:49:40.46+0000	INFO	localhost-startStop-1 com.citrix.xmls.util.CloudUtil Not generating ew.config.properties for cloud servers.
2018-11-15T06:49:54.463+0000	INFO	localhost-startStop-1 com.citrix.xmls.util.CloudUtil FirstBeanInitialization: Adding [redacted] to Java Security Providers.
2018-11-15T06:49:54.584+0000	INFO	localhost-startStop-1 com.citrix.xmls.util.CloudUtil Standard(Non-FIPS) BC lib registered
2018-11-15T06:49:54.585+0000	INFO	localhost-startStop-1 com.citrix.xmls.util.CloudUtil Setting CloudSecurity to MultiTenant mode.

Citrix Endpoint Management utiliza el appender log4j de syslog para enviar mensajes de syslog con el formato RFC5424. Los datos del mensaje syslog no tienen ningún formato específico.

Comprobaciones de conectividad

March 1, 2024

En la página **Solución de problemas y asistencia** de Citrix Endpoint Management, puede comprobar la conexión de Citrix Endpoint Management con NetScaler Gateway y con otros servidores y ubicaciones. Para realizar comprobaciones de conectividad de Citrix Endpoint Management, necesita el rol de asistencia o de administrador. Establezca este rol mediante el control de acceso por roles (RBAC). Para obtener información sobre cómo asignar roles, consulte [Configurar roles con RBAC](#).

Realizar comprobaciones sobre la conectividad de Citrix Endpoint Management

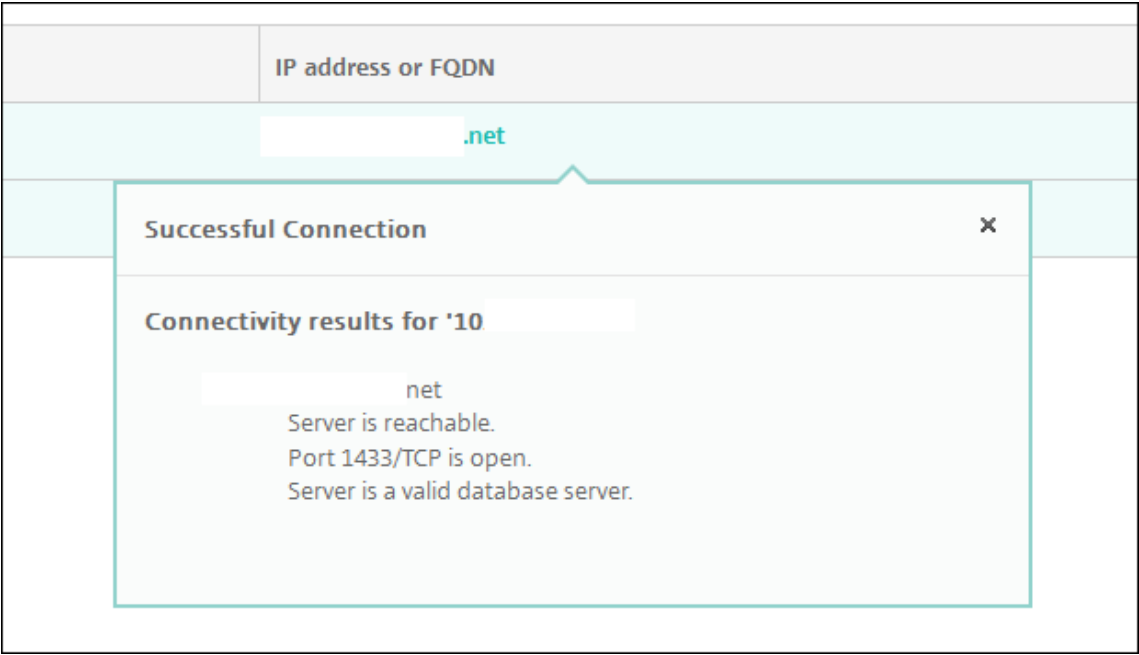
1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de llave inglesa situado en la esquina superior derecha de la consola. Aparece la página **Solución de problemas y asistencia**.
2. En **Diagnósticos**, haga clic en **Citrix Endpoint Management Connectivity Checks**. Aparecerá la página **Citrix Endpoint Management Connectivity Checks**. Si su entorno de Citrix Endpoint Management contiene nodos en clúster, se muestran todos los nodos.

<input type="checkbox"/>	Connectivity to	IP address or FQDN
<input type="checkbox"/>	Windows Phone Store	windowsphone.com
<input type="checkbox"/>	Databasenet
<input type="checkbox"/>	Apple Feedback Push Notification Server	feedback.push.apple.com
<input type="checkbox"/>	LDAPnet
<input type="checkbox"/>	Domain Name System (DNS)
<input type="checkbox"/>	Nexmo Gateway	-
<input type="checkbox"/>	Apple Push Notification Server	gateway.push.apple.com
<input type="checkbox"/>	iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
<input type="checkbox"/>	Google Play	play.google.com
<input type="checkbox"/>	Windows Security Token Service	login.live.com

3. Seleccione los servidores a incluir en la prueba de conectividad y, a continuación, haga clic en **Probar conectividad**. Aparecerá la página de resultados de pruebas.

<input type="checkbox"/>	Connectivity to	IP address or FQDN	
<input type="checkbox"/>	Database	net	✓
<input type="checkbox"/>	Windows Phone Store	windowsphone.com	✓

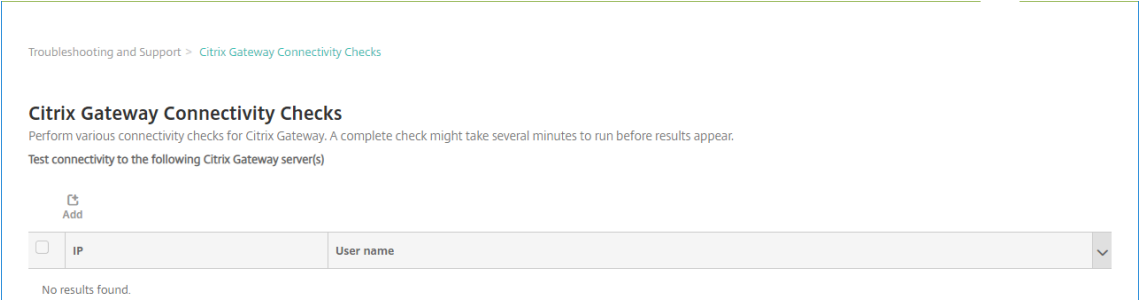
4. Seleccione un servidor de la tabla para ver los resultados detallados de dicho servidor.



Para obtener información sobre las comprobaciones de conectividad que Citrix Endpoint Management puede realizar y sus detalles, consulte Detalles de comprobación de la conectividad.

Comprobaciones de conectividad de NetScaler Gateway

- 1. En la página **Solución de problemas y asistencia**, en **Diagnósticos**, haga clic en **Comprobaciones de conectividad de NetScaler Gateway**. Aparecerá 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**. Aparecerá el cuadro de diálogo **Agregar servidor NetScaler Gateway**.

Add Citrix Gateway Server

Citrix Gateway Management IP *

User name *

administrator

Password *

.....

CancelAdd

3. En **IP de administración de NetScaler Gateway**, escriba la dirección IP de administración del servidor con NetScaler Gateway que quiere probar.

Si está llevando a cabo la comprobación de conectividad de un servidor NetScaler Gateway que ya se ha agregado, se proporciona la dirección IP.
4. Escriba las credenciales de administrador de este servidor NetScaler Gateway.

Si está llevando a cabo la comprobación de conectividad de un servidor NetScaler Gateway que ya se ha agregado, se proporciona el nombre de usuario.
5. Haga clic en **Agregar**. El servidor NetScaler Gateway se agrega a la tabla en la página **Comprobaciones de conectividad de NetScaler Gateway**.
6. Seleccione el servidor NetScaler Gateway y, a continuación, haga clic en **Probar conectividad**. Los resultados aparecerán en la tabla “Resultados de la prueba”.
7. Seleccione un servidor de la tabla para ver los resultados detallados de dicho servidor.

Detalles de comprobación de la conectividad

En la tabla siguiente, se indican las varias comprobaciones de conectividad que Citrix Endpoint Management puede realizar y se incluyen detalles sobre cada comprobación.

Conectividad con	Dirección IP o nombre de dominio completo	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 Management. El servidor de notificaciones push de Apple es necesario para enviar mensajes a dispositivos iOS y macOS.
Servidor de comentarios sobre notificaciones push 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 comentarios sobre notificaciones push de Apple proporciona información sobre notificaciones remotas fallidas enviadas a dispositivos iOS y macOS.
Citrix License Server	Dirección IP del servidor de licencias	Comprueba la conectividad entre Citrix License Server y el nodo de Citrix Endpoint Management. Los servidores con productos Citrix se comunican con Citrix License Server 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 y acceder a redes internas.

Conectividad con	Dirección IP o nombre de dominio completo	Detalles
Base de datos	Dirección IP o FQDN del servidor de base 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	localhost	Comprueba la conexión del nodo de Citrix Endpoint Management con 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 de FCM y el nodo de Citrix Endpoint Management. Con FCM, puede notificar a una aplicación cliente que un nuevo correo electrónico u otros datos están disponibles para sincronizar. Puede enviar mensajes de notificación para mantener a los usuarios interesados. FCM reemplaza a Google Cloud Messaging (GCM).
Google Play	play.google.com	Comprueba la conectividad entre Google Store Server y el nodo de Citrix Endpoint Management. Google Play se utiliza para ofrecer servicios que incluyen una tienda de entrega de aplicaciones de empresa privadas administradas.

Conectividad con	Dirección IP o nombre de dominio completo	Detalles
Compras por volumen o en el iTunes Store	vpp.itunes.apple.com	Comprueba la conectividad entre el servidor de la Apple Store y el nodo de Citrix Endpoint Management. Apple Store se utiliza para ofrecer servicios, incluida una tienda de entrega de aplicaciones de empresa administradas y privadas.
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 dispositivos Windows.
Servicio ShareFile	Dirección IP o FQDN del servicio ShareFile configurado en Citrix Endpoint Management	Comprueba la conectividad entre ShareFile Service y Citrix Endpoint Management. ShareFile Service es una plataforma segura basada en la nube para que las empresas almacenen y compartan archivos de gran tamaño.

Conectividad con	Dirección IP o nombre de dominio completo	Detalles
Tienda de escritorios o tabletas Windows	windows.microsoft.com	Comprueba la conectividad entre la tienda de escritorios o tabletas de Windows y el nodo de Citrix Endpoint Management. La tienda de tabletas y escritorios de Windows se utiliza para ofrecer servicios, incluida una tienda de entrega de aplicaciones de empresa privadas administradas.
Servicio de token de seguridad de Windows	login.live.com	Comprueba la conectividad entre el servidor de token de seguridad de Windows y el nodo de Citrix Endpoint Management. El servicio de token de seguridad de Windows admite la autenticación de dos factores (dominio más token de seguridad) para dispositivos Windows.

Proveedor de servicios móviles

November 29, 2023

Puede habilitar Citrix Endpoint Management para que utilice la interfaz del proveedor de servicios móviles, para enviar consultas a dispositivos BlackBerry y Exchange ActiveSync y emitir operaciones.

Por ejemplo, supongamos que su organización tiene 1000 usuarios y que cada usuario utiliza uno o más dispositivos. Después de indicar a todos los usuarios que inscriban sus dispositivos con Citrix Endpoint Management, la consola de Citrix Endpoint Management indica la cantidad de dispositivos que los usuarios inscriben. Mediante la configuración de este parámetro, puede determinar la cantidad de dispositivos que se conectan a Exchange Server. De este modo, puede hacer lo siguiente:

- Determinar si los usuarios aún tienen que inscribir sus dispositivos.
 - Emitir comandos para los dispositivos de usuario que se conectan a un servidor Exchange Server; por ejemplo, un comando de borrado de datos.
1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
 2. En **Servidor**, haga clic en **Proveedor de servicios móviles**. Aparece la página **Proveedor de servicios móviles**.

The screenshot shows the 'Mobile Service Provider' configuration page. At the top, it says 'Settings > Mobile Service Provider'. Below this is the title 'Mobile Service Provider' and a description: 'Allows XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and issue operations.' There are three input fields: 'Web service URL*' with the value 'http://XmmServer/services/zdm', 'User name*' with the value 'domain\admin', and 'Password*' which is empty. Below these is a toggle switch for 'Automatically update BlackBerry and ActiveSync device connections' which is currently 'OFF'. At the bottom center is a green 'Test Connection' button. In the bottom right corner are 'Cancel' and 'Save' buttons.

3. Configure estos parámetros:
 - **URL del servicio web:** Escriba la dirección URL del servicio web. Por ejemplo: <https://XmmServer/services/xdmservice>.
 - **Nombre de usuario:** Escriba el nombre de usuario con el formato `domain\admin`.
 - **Contraseña:** Escriba la contraseña.
 - **Habilitar la actualización automática de conexiones de dispositivos BlackBerry y ActiveSync:** Seleccione si quiere actualizar automáticamente las conexiones de los dispositivos. Está **desactivado** de forma predeterminada.
 - Haga clic en **Probar conexión** para comprobar la conexión.
4. Haga clic en **Guardar**.

Informes

March 1, 2024

Citrix Endpoint Management ofrece los siguientes informes predefinidos que permiten analizar las implementaciones de dispositivos y aplicaciones. Cada informe aparece como un gráfico y una tabla.

Puede ordenar y filtrar las tablas en función de cualquier columna. También puede seleccionar elementos de los gráficos para obtener información más detallada.

- **Total de intentos de implementación de la aplicación:** Ofrece una lista de las aplicaciones implementadas que los usuarios han intentado instalar en los dispositivos.
- **Aplicaciones por plataforma:** Ofrece una lista de las aplicaciones y sus versiones según la plataforma y la versión del dispositivo.
- **Aplicaciones por tipo:** Ofrece una lista de las aplicaciones según su versión, tipo o categoría.
- **Inscripción de dispositivos:** Ofrece una lista de todos los dispositivos inscritos.
- **Dispositivos y aplicaciones:** Ofrece una lista de los dispositivos que ejecutan aplicaciones administradas.
- **Dispositivos inactivos:** Ofrece una lista de los dispositivos que no hayan tenido ninguna actividad durante la cantidad de días que especifique la propiedad `device.inactivity.days.threshold` del servidor de Citrix Endpoint Management.
- **Dispositivos liberados por jailbreak/root:** Ofrece una lista de los dispositivos iOS liberados por jailbreak y de los dispositivos Android liberados por root.
- **Términos y condiciones:** Ofrece una lista de los usuarios que hayan aceptado o rechazado los contratos de términos y condiciones. Puede seleccionar áreas del gráfico para ver más detalles.
- **Las 10 primeras implementaciones fallidas:** Ofrece una lista de hasta 10 aplicaciones que no se pudieron implementar.
- **Aplicaciones bloqueadas por dispositivo y usuario:** Ofrece una lista de las aplicaciones incluidas en la lista de bloqueados que los usuarios tienen en sus dispositivos.
- **Dispositivos no conformes:** Ofrece una lista de los dispositivos que no cumplen los criterios de cumplimiento. Los criterios incluyen si el dispositivo está liberado por jailbreak, la versión del sistema operativo en ejecución y si el dispositivo tiene un código de acceso o no. El informe también muestra el nombre de usuario asociado al dispositivo y si el dispositivo está cifrado. Para dispositivos iOS, la columna de cifrado muestra N/D.

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 datos del dispositivo (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, consulte la página **Detalles del dispositivo**. La página **Detalles del dispositivo** muestra 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 que contiene **Detalles del dispositivo**, consulte [Obtener información acerca de dispositivos](#).

Los siguientes aspectos determinan cómo Citrix Endpoint Management recopila información sobre las aplicaciones implementadas o instaladas en dispositivos administrados:

- Tipo de dispositivo

- Método de inscripción
- Si la [directiva de inventario de aplicaciones](#) está implementada

Para los dispositivos Android, el comportamiento es diferente según el tipo de dispositivo y el método de inscripción. La tabla siguiente indica dónde se muestran las aplicaciones de **Android Enterprise** (página **Detalles del dispositivo**, informes o N/D). 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 Detalles del dispositivo e informes
Aplicaciones opcionales (la directiva de inventario de aplicaciones está implementada)	Aplicaciones de empresa, MDX, públicas y de enlaces web; informes	Página Detalles del dispositivo e informes

La siguiente tabla indica dónde se muestran las aplicaciones para **Android (AD heredado)** (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 (aplicaciones públicas y de empresa)	MAM
Aplicaciones obligatorias (la directiva de inventario de aplicaciones no está implementada)	Página Detalles del dispositivo e informes	Página Detalles del dispositivo e informes	N/D

	MDM+MAM (todas las aplicaciones)	MDM (aplicaciones públicas y de empresa)	MAM
Aplicaciones opcionales (la directiva de inventario de aplicaciones no está implementada)	Página Detalles del dispositivo e informes	Página Detalles del dispositivo e informes	No disponible
Aplicaciones obligatorias (la directiva de inventario de aplicaciones está implementada)	Página Detalles del dispositivo e informes	Página Detalles del dispositivo e informes	N/D
Aplicaciones opcionales (la directiva de inventario de aplicaciones está implementada)	Página Detalles del dispositivo e informes	Página Detalles del dispositivo e informes	No disponible

Para los dispositivos iOS, el comportamiento es diferente según el método de inscripción. La tabla siguiente indica dónde se muestran las aplicaciones (página **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 de empresa)	MAM (todas las aplicaciones)
Aplicaciones obligatorias (la directiva de inventario de aplicaciones no está implementada)	Página Detalles del dispositivo e informes	Página Detalles del dispositivo e informes	Página Detalles del dispositivo e informes; esas aplicaciones se muestran con el estado pendiente (incluso aunque no estén instaladas) o permanecen en estado pendiente después de instalarse manualmente.

	MDM+MAM (todas las aplicaciones)	MDM (aplicaciones públicas y de empresa)	MAM (todas las aplicaciones)
Aplicaciones opcionales (la directiva de inventario de aplicaciones no está implementada)	Página Detalles del dispositivo e informes	Página Detalles del dispositivo e informes	Las aplicaciones web, SaaS y de enlaces web aparecen en la página Detalles del dispositivo como aplicaciones instaladas; no aparecen en los informes. Las aplicaciones de empresa, MDX y públicas no aparecen en la página Detalles del dispositivo después de instalarse manualmente. Las aplicaciones no aparecen en los informes después de instalarse manualmente.

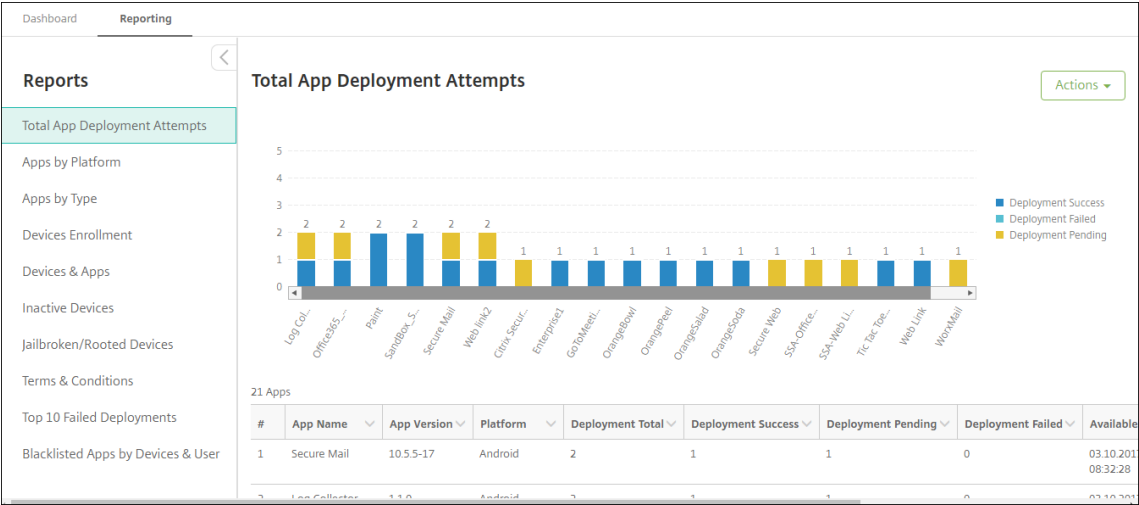
	MDM+MAM (todas las aplicaciones)	MDM (aplicaciones públicas y de empresa)	MAM (todas las aplicaciones)
Aplicaciones obligatorias (la directiva de inventario de aplicaciones está implementada)	Página Detalles del dispositivo e informes	Página Detalles del dispositivo e informes	La directiva de inventario de aplicaciones no se puede implementar en los dispositivos. Las aplicaciones aparecen en la página Detalles del dispositivo y en los informes. Estas aplicaciones se muestran en estado pendiente (incluso aunque no estén instaladas) o permanecen en estado pendiente después de instalarlas manualmente.

	MDM+MAM (todas las aplicaciones)	MDM (aplicaciones públicas y de empresa)	MAM (todas las aplicaciones)
Aplicaciones opcionales (la directiva de inventario de aplicaciones está implementada)	Página Detalles del dispositivo e informes	Página Detalles del dispositivo e informes	La directiva de inventario de aplicaciones no se puede implementar en los dispositivos. Las aplicaciones web, SaaS y de enlaces web aparecen en la página Detalles del dispositivo como aplicaciones instaladas; no aparecen en los informes. Las aplicaciones de empresa, MDX y públicas no aparecen en la página Detalles del dispositivo después de instalarse manualmente. Las aplicaciones no aparecen en los informes después de instalarse manualmente.

En el caso de dispositivos macOS y Windows, Citrix Endpoint Management recopila un inventario de aplicaciones *solo* cuando se implementa la directiva de inventario de aplicaciones.

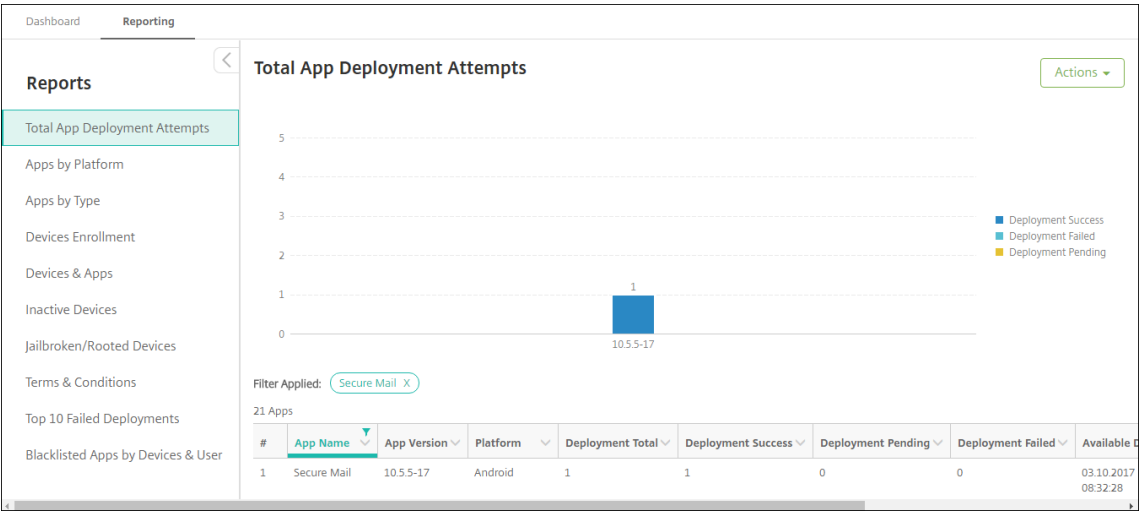
Para generar un informe

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 datos de un informe

1. Haga clic en las áreas del gráfico para profundizar y ver información más detallada.



Para ordenar, filtrar o buscar en una columna de la tabla, haga clic en el encabezado de dicha columna

DashboardReporting

Reports

Total App Deployment Attempts

Apps by PlatformApps by TypeDevices EnrollmentDevices & AppsInactive DevicesJailbroken/Rooted DevicesTerms & ConditionsTop 10 Failed DeploymentsBlacklisted Apps by Devices & User

22 Apps

#	App Name	App Version	Platform	Deployment Total	Deployment Success	Deployment Pending	Deployment Failed	Available
1	Enterprise1	↑ Sort Ascending		1	1	0	0	03.10.2019 09:10:10
2	SandBox_S	↓ Sort Descending		1	1	0	0	03.10.2019 08:38:40
3	Fonts	Filter with secure		1	0	1	0	03.10.2019 09:45:07
4	SandBox_S	<input type="checkbox"/> Secure Web		1	1	0	0	03.10.2019 08:38:40
5	GoToMeeti	Filter		1	1	0	0	03.10.2019 12:34:35
6	Secure Mail	10.5.5-17	Android	1	1	0	0	03.10.2019 08:32:28
7	GreedyPenguins		Windows Mobile	1	1	0	0	03.10.2019 13:01:50

Para filtrar el informe por fecha

1. Haga clic en el encabezado de una columna para ver los parámetros de filtro.

DashboardReporting

Reports

Total App Deployment Attempts

Apps by PlatformApps by TypeDevices EnrollmentDevices & AppsInactive DevicesJailbroken/Rooted DevicesTerms & ConditionsTop 10 Failed DeploymentsBlacklisted Apps by Devices & User

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:07	↑ Sort Ascending		03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_SAF
Compliance	03.27.2017 09:29:07	↓ Sort Descending		03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Editor
Compliance	03.27.2017 09:29:07	Filter Condition is on		03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:08	Value * MM / DD / YYYY		03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27	Filter	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_SAF

2. En **Condición de filtro**, elija cómo quiere restringir las fechas relevantes.

Dashboard **Reporting**

Reports

Total App Deployment Attempts

Apps by Platform

Apps by Type

Devices Enrollment

Devices & Apps

Inactive Devices

Jailbroken/Rooted Devices

Terms & Conditions

Top 10 Failed Deployments

Blacklisted Apps by Devices & User

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:08	Sort Ascending Sort Descending		03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:29:08	Filter Condition is on is on or before is on or after between		03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edit
Compliance	03.27.2017 09:29:08			03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27	03.27.2017 09:55:27	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_S

3. Use el selector de fecha para especificar las fechas.

Dashboard **Reporting**

Reports

Total App Deployment Attempts

Apps by Platform

Apps by Type

Devices Enrollment

Devices & Apps

Inactive Devices

Jailbroken/Rooted Devices

Terms & Conditions

Top 10 Failed Deployments

Blacklisted Apps by Devices & User

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:08	Sort Ascending Sort Descending		03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:29:08	Filter Condition is on or before		03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edit
Compliance	03.27.2017 09:29:08	Value MM/DD/YYYY		03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:08			03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27			09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:55:27			09.27.2016 04:48:39	Unknown		SUCCESS	Jota Text Edit

4. Como se muestra el siguiente ejemplo, aparecerá una columna con un filtro de fecha.

Dashboard **Reporting**

Reports

Total App Deployment Attempts

Apps by Platform

Apps by Type

Devices Enrollment

Devices & Apps

Inactive Devices

Jailbroken/Rooted Devices

Terms & Conditions

Top 10 Failed Deployments

Blacklisted Apps by Devices & User

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edit

5. Para quitar un filtro, haga clic en el encabezado de la columna y, a continuación, haga clic en **Quitar filtro**.

Dashboard

Reporting

Reports

Total App Deployment Attempts

Apps by Platform

Apps by Type

Devices Enrollment

Devices & Apps

Inactive Devices

Jailbroken/Rooted Devices

Terms & Conditions

Top 10 Failed Deployments

Blacklisted Apps by Devices & User

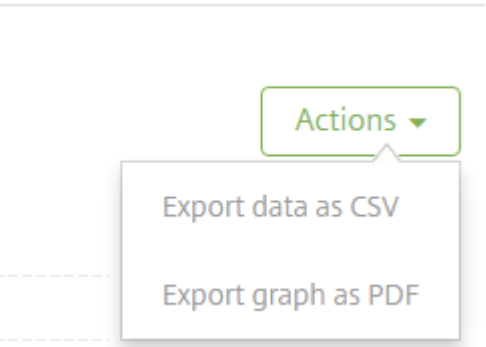
Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:00	↑ Sort Ascending ↓ Sort Descending		03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:29:00	Filter Condition between		03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edit
Compliance	03.27.2017 09:29:00	Value 1 * 12.31.2016		03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:00	Value 2 * 03.27.2017		03.27.2017 07:33:27	Unknown		SUCCESS	Web Link

Filter

Remove Filter

Para exportar un gráfico o una tabla

- Para exportar el gráfico en formato PDF, haga clic en **Acciones > Exportar gráfico como PDF**.
- Para exportar los datos de la tabla en formato CSV, haga clic en **Acciones > Exportar datos como CSV**.



API de REST

March 1, 2024

Con la API de REST de Citrix Endpoint Management, puede:

- Servicios de llamadas que aparecen en la consola de Citrix Endpoint Management
- Invocar servicios de REST desde cualquier cliente REST

La API no requiere el inicio de sesión en la consola de Citrix Endpoint Management para llamar a los servicios.

Para ver todo el conjunto actual de interfaces API disponibles, descargue el archivo PDF [Public API for REST Services](#).

Hay API disponibles para administrar sus dispositivos de punto final móviles y de escritorio y configurar los parámetros de sus aplicaciones de Workspace. En <https://developer.cloud.com/citrixworkspace>, vaya a **Citrix Endpoint Management > Mobile Application Integration**.

Permisos necesarios para acceder a la API de REST

Para acceder a la API de REST, necesita uno de los siguientes permisos:

- Administrador de Citrix Cloud
- Permiso de acceso a las API públicas establecido como parte de la configuración del acceso basado en roles. Para obtener información, consulte [Configuración de roles con RBAC](#).
- Permiso de superusuario

Para acceder a la API de REST mediante su cuenta de Citrix Cloud, genere las claves de **API**:

1. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
2. Seleccione **Acceso a API > Clientes seguros**.
3. Escriba un nombre de cliente seguro y, a continuación, haga clic en **Crear cliente**.

A continuación, Citrix Cloud crea el ID de cliente seguro y el secreto del cliente. Descargue una copia de esta información y guárdela de forma local y segura como referencia. Citrix Cloud no almacena los identificadores únicos después de cerrar el cuadro de diálogo.

Para invocar servicios de la API de REST

Puede llamar a servicios de la API de REST mediante comandos de cURL o el cliente REST. Los ejemplos siguientes usan el cliente Advanced REST para Chrome.

Nota:

En los siguientes ejemplos, deberá cambiar el nombre de host y el número de puerto para que coincidan con su entorno.

Inicio de sesión

El ejemplo que se muestra aquí cubre el inicio de sesión con un token obtenido 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:

```
1 {
2
3   "bearerToken": "eyJ0e0iJSUzJiibGcI1AiONiJ9.
   eyJkIjoMDExN1c2VlXmZNDc1OTk4...qf0iQ"
4 }
5
6 <!--NeedCopy-->
```

Debe obtener el token de portador mediante la API de Citrix Cloud <https://trust.citrixworkspacesapi.net/Help/Api/POST-customer-tokens-clients>. Para obtener información, consulte la [documentación para desarrolladores](#).

Ejemplo de respuesta:

```
1 {
2
3   "auth_token": "q483409eu82mkfrcdiV90iv0gc:q483409eu82mkfrcdiV90iv0gc"
4 }
5
6 <!--NeedCopy-->
```

Información relacionada

- [API de REST en Citrix Endpoint Management](#)

ActiveSync Gateway

November 29, 2023

ActiveSync es un protocolo de sincronización de datos móviles desarrollado por Microsoft. ActiveSync sincroniza datos entre dispositivos móviles y equipos de escritorio (o portátiles).

Puede configurar reglas de ActiveSync Gateway en Citrix Endpoint Management. La puerta de enlace conserva una lista de ID de ActiveSync para todos los dispositivos configurados en Citrix Endpoint Management. En función de las reglas que configure, se puede permitir o denegar el acceso de los dispositivos a datos ActiveSync tomando como referencia esos ID. Por ejemplo, si activa la regla **Aplicaciones obligatorias que faltan**, Citrix Endpoint Management consulta la directiva Acceso a aplicaciones para ver cuáles son las aplicaciones obligatorias y deniega el acceso a los datos de ActiveSync si faltan esas aplicaciones. Si faltan las aplicaciones obligatorias, la directiva deniega el acceso a los

datos de ActiveSync. Para cada regla, puede elegir **Permitir** o **Denegar**. El valor predeterminado es **Permitir**.

Para obtener más información acerca de la directiva Acceso a aplicaciones, consulte [Directiva 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 reconectar.

Aplicaciones prohibidas: Comprueba si un dispositivo tiene aplicaciones prohibidas, según se definen en la directiva Acceso a aplicaciones.

Permiso y denegación implícitos: Esta acción es la predeterminada de ActiveSync Gateway. La puerta de enlace crea una lista de todos los dispositivos que no cumplen alguno de los demás criterios de regla o filtro. A continuación, la puerta de enlace permite o deniega las conexiones en función de esa lista. Si no coincide ninguna regla, el valor predeterminado es **Permiso implícito**.

Dispositivos inactivos: Comprueba si un dispositivo está inactivo según se define en el parámetro **Umbral de días de inactividad** en **Propiedades de servidor**.

Aplicaciones obligatorias que faltan: Comprueba si en un dispositivo faltan aplicaciones obligatorias, según se definen en la directiva Acceso a aplicaciones.

Aplicaciones no sugeridas: Comprueba si un dispositivo tiene aplicaciones no sugeridas, según se definen en la directiva Acceso a aplicaciones.

Contraseña no conforme: Comprueba si la contraseña del usuario cumple los requisitos de conformidad. En dispositivos iOS y Android, Citrix Endpoint Management puede determinar si la contraseña actual del dispositivo cumple los requisitos de conformidad con la directiva Código de acceso enviada al dispositivo. Por ejemplo, en iOS, el usuario tiene 60 minutos para definir una contraseña si Citrix Endpoint Management envía una directiva Código de acceso al dispositivo. Antes de que el usuario defina la contraseña, el código de acceso podría no cumplir los requisitos de conformidad.

Dispositivos no conformes: Comprueba si un dispositivo ya no es conforme, según lo definido en la propiedad de dispositivo No conforme. Por regla general, las acciones automatizadas o el uso que terceros hacen de las API de Citrix Endpoint Management modifican esa propiedad.

Estado revocado: Comprueba si el certificado del dispositivo fue revocado. Un dispositivo revocado no se puede volver a inscribir hasta que se autorice de nuevo.

Dispositivos Android o iOS liberados por root/jailbreak: Comprueba si un dispositivo iOS está liberado por jailbreak o un dispositivo Android está liberado por rooting.

Dispositivos no administrados: Comprueba si un dispositivo aún está en estado administrado, bajo el control de Citrix Endpoint Management. Por ejemplo, un dispositivo inscrito en MAM o que se haya

desinscrito no es un dispositivo administrado.

Enviar usuarios de dominio de Android a ActiveSync Gateway: Haga clic en **SÍ** 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 antigua. 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 figure 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 con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En **Servidor**, haga clic en **ActiveSync Gateway**. Aparecerá la página **ActiveSync Gateway**.

Settings > ActiveSync Gateway

ActiveSync Gateway

Allows or denies access to devices and users based on rules and properties.

All devices

Activate the following rule(s)

- ☐ Anonymous Devices
- ☐ Failed Samsung KNOX attestation
- ☐ Forbidden Apps
- ☐ Implicit Allow and Deny
- ☐ Inactive Devices
- ☐ Missing Required Apps
- ☐ Non-Suggested Apps
- ☐ Noncompliant Password
- ☐ Out of Compliance Devices
- ☐ Revoked Status
- ☐ Rooted Android and jailbroken iOS Devices
- ☐ Unmanaged Devices

Android only

Send Android domain users to ActiveSync Gateway **YES** ?

Cancel Save

1. En **Activar las reglas siguientes**, seleccione las reglas que quiera activar.

2. En **Solo Android**, en **Enviar usuarios de dominio Android a ActiveSync Gateway**, haga clic en **SÍ** para que Citrix Endpoint Management envíe la información de los dispositivos Android a ActiveSync Gateway.
3. Haga clic en **Guardar**.

Conector de Citrix Endpoint Management para Exchange ActiveSync

March 1, 2024

XenMobile Mail Manager ha pasado a ser el conector de Citrix Endpoint Management para Exchange ActiveSync. Para obtener detalles sobre los productos unificados de Citrix, consulte la [guía de productos de Citrix](#).

El conector amplía la capacidad de Citrix Endpoint Management de este modo:

- Control de acceso dinámico para dispositivos Exchange ActiveSync (EAS). Se puede bloquear o permitir inmediatamente el acceso de dispositivos EAS a servicios de Exchange.
- Proporciona a Citrix Endpoint Management la capacidad de acceder a la información de asociación del dispositivo EAS, facilitada por Exchange.
- Proporciona a Citrix Endpoint Management la capacidad de borrar un dispositivo móvil según el estado EAS.
- Proporciona a Citrix Endpoint Management la capacidad de acceder a la información acerca de dispositivos BlackBerry y realizar operaciones de control tales como un borrado (Wipe) y un restablecimiento de contraseña (ResetPassword).

Para borrar un dispositivo según el estado EAS, configure una acción automatizada con un desencadenante 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 admitirán Exchange Online debido a los cambios de autenticación anunciados por Microsoft [aquí](#). El conector de Citrix Endpoint Management para Exchange seguirá funcionando con Microsoft Exchange Server (local).

Novedades en la versión 10.1.10

Se han corregido los siguientes problemas en la versión 10.1.10:

- Es posible que los clientes que sufren problemas frecuentes de red no puedan completar una instantánea en los tres intentos que se ofrecen. Con esta versión, un administrador puede

configurar el máximo de intentos (1-10). Esta corrección permite que una instantánea pueda sufrir varias interrupciones de la comunicación sin abandonar completamente el proceso de generación de la instantánea. [CXM-70837]

The screenshot shows the 'Configuration' window with the following settings:

- Type: On Premise
- Exchange Server: [Empty]
- User: [Empty]
- Password: [Empty]
- Major snapshot: Every 4 Hours
- Minor snapshot: Every 5 Minutes
- Snapshot Type: Shallow
- Default Access: Unchanged
- Command Mode: Powershell
- Connection Expiration: Every 00 Hours 30 Minutes
- Enable Diagnostics: ☐
- Days to Keep Snapshot Data: 00
- Snapshot Maximum Attempts: 03
- View Entire Forest: ☐
- Authentication: Kerberos
- Allow Redirection: ☐

Buttons: Test Connectivity, Save, Cancel.

- En versiones anteriores, el tipo Instantánea no aparecía en la lista de configuraciones de Exchange. Ahora sí aparece el tipo Instantánea. [CXM-70846]
- La excepción PSRemotingTransport notificada por PowerShell indica que la sesión con Exchange ya no es viable. El estado se agrega de forma predeterminada a la lista Errores críticos del archivo de configuración. Al hacerlo, cuando se detecta PSRemotingTransportException, la conexión se marca como Error para eliminarla luego. La siguiente comunicación emplea una conexión válida o crea una conexión. [XMHELP-2184, CXM-70836]
- Al guardar un cambio en la configuración, es posible que no todos los componentes internos previamente configurados se eliminaran correctamente antes de cargar la nueva configuración. Este problema puede provocar un comportamiento impredecible. Dicho comportamiento depende del cambio concreto y si el cambio entra en conflicto con la configuración anterior. En esta versión se eliminan todos los componentes internos antes de cargar la nueva configuración. [XMHELP-2259, CXM-71388]

Novedades en la versión 10.1.9

Se han corregido los siguientes problemas en la versión 10.1.9:

- Ahora los cambios de configuración se gestionan de manera 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 se inician de nuevo los subsistemas, por lo que todas las programaciones y otras infraestructuras internas se restablecen con parámetros nuevos. Esto corrige un problema conocido de la versión 10.1.8. [CXM-47709, CXM-61330]
- Durante la actualización de una versión, la configuración de la base de datos existente no se integraba en el nuevo archivo de configuración. Ahora la configuración de la base de datos se integra en el archivo de configuración actualizado. [CXM-49326]
- En los archivos de diagnóstico relacionados con la instantánea, faltaban los encabezados de columna. Los encabezados se han restaurado. [CXM-62680]
- Al actualizar una versión anterior, la sección de valores predeterminados del archivo de configuración quedaba sobrescrita por la sección análoga del archivo de configuración en uso. Este problema impedía que, tras la actualización, el servicio cargara aspectos agregados o mejorados de la sección de valores predeterminados. A partir de esta versión, la sección de valores predeterminados siempre refleja la configuración más reciente. [CXM-62681]
- Al ejecutar la aplicación, los administradores ya no pueden acceder a ciertas opciones al presionar Mayús. Antes estas opciones estaban disponibles con el permiso de Citrix. Ahora algunas opciones están totalmente disponibles, como Permitir redirección, y otras, como Detección de bloqueo y Corrección de recuento, se han retirado. [CXM-62767]

The screenshot shows the 'Configuration' window for Citrix Endpoint Management. It contains the following settings:

- Type: On Premise
- Exchange Server: [Empty text box]
- User: [Empty text box]
- Password: [Empty text box]
- Major snapshot: Every 4 Hours
- Minor snapshot: Every 5 Minutes
- Snapshot Type: Shallow
- Default Access: Unchanged
- Command Mode: Powershell
- Connection Expiration: Every 00 Hours 30 Minutes
- Enable Diagnostics: [Unchecked checkbox]
- Days to Keep Snapshot Data: 00
- View Entire Forest: [Unchecked checkbox]
- Authentication: Kerberos
- Allow Redirection: [Unchecked checkbox]

At the bottom, there is a 'Test Connectivity' button, a large empty text area, and 'Save' and 'Cancel' buttons.

Novedades en versiones anteriores

En la siguiente sección, se indican las nuevas funciones y los problemas resueltos en versiones anteriores del conector de Citrix Endpoint Management para Exchange ActiveSync.

Novedades en la versión 10.1.8

- Es posible que Exchange limite la emisión demasiado frecuente de comandos por parte del servicio del conector de Citrix Endpoint Management para Exchange ActiveSync. Este problema es habitual en las conexiones a Office 365. El efecto de la limitación requiere que el servicio se detenga durante un período de tiempo especificado antes de enviar el siguiente comando. Ahora, en el apartado “Configurar” de la consola, se muestra la cantidad de tiempo restante de pausa. [CXM-48044]
- 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. [CXM-52523]

- Se han agregado más detalles a los análisis enviados a Google Analytics, especialmente en lo que respecta a las instantáneas. [CXM-56691]
- La función para probar la conectividad de Exchange intentaría inicializar la conexión solo una vez. Debido a que las conexiones de Office 365 se pueden limitar, era posible que una prueba de conectividad pareciera fallida cuando se limitaba. Ahora, el conector de Citrix Endpoint Management para Exchange ActiveSync intenta iniciar una conexión hasta tres veces. [CXM-58180]
- Para aplicar directivas en Exchange, el conector de Citrix Endpoint Management para Exchange ActiveSync debe compilar un comando **Set-CASMailbox** que incluya todos los dispositivos correspondientes a cada buzón en dos listas: permitir y bloquear. Si un dispositivo no está incluido en ninguna de las listas, Exchange vuelve a su estado de acceso predeterminado. Si ese estado de acceso predeterminado es diferente del estado deseado para un dispositivo, ese dispositivo queda como no conforme. Por lo tanto, un usuario puede perder el acceso a su correo electrónico si el estado de acceso predeterminado de Exchange está bloqueado, y se debería permitir. O bien, un usuario cuyo acceso al correo electrónico debería estar bloqueado puede tener acceso a él. Ahora, el conector de Citrix Endpoint Management para Exchange ActiveSync garantiza que todos los dispositivos con un estado deseado válido se incluyan en cada comando **Set-CasMailbox**. [CXM-61251]

El siguiente problema es un problema conocido en la versión 10.1.8:

Si un administrador realiza un cambio en la aplicación de configuración que modifica los datos de configuración mientras el servicio realiza operaciones de larga duración (como una instantánea o evaluación de directiva), el servicio puede entrar en un estado indeterminado. Un posible síntoma puede ser que los cambios de directiva no se procesen o que las instantáneas no se inicien. Para que el servicio vuelva a un estado de funcionamiento, el servicio debe reiniciarse. Es posible que tenga que utilizar el administrador de servicios de Windows para finalizar el proceso del servicio antes de iniciar el servicio. [CXM-61330]

Novedades en la versión 10.1.7

- XenMobile Mail Manager ha pasado a ser el conector de Citrix Endpoint Management para Exchange ActiveSync.
- La opción **Disable Pipelining** ha dejado de usarse en el cuadro de diálogo de configuración de Exchange. Se obtiene el mismo resultado configurando varios pasos para cada comando en el archivo config.xml. [CXM-54593]

Se han corregido los siguientes problemas en la versión 10.1.7:

- En la ventana Snapshot History (historial de instantáneas), los mensajes de error pueden mostrarse con poco contexto. Ahora, los mensajes de error incluyen un prefijo con el contexto sobre el lugar donde se produjeron. [CXM-49157]

- El archivo XmmGoogleAnalytics.dll no tenía la versión de archivo correspondiente para esta versión. [CXM-52518]
- Para mejorar los diagnósticos, hemos cambiado recientemente el formato de cadena para una lista de ID de dispositivo que se utilizan para establecer un estado de buzón como permitido o bloqueado. Sin embargo, ante una indicación de demasiados dispositivos, excedía el tamaño máximo de la cadena. Ahora, usamos una estructura de datos de matriz interna. Esta estructura no tiene límite de tamaño y da a los datos el formato apropiado para los diagnósticos. [CXM-52610]
- Cuando se detectan directivas de dispositivo que no están sincronizadas con Exchange, los comandos de estas directivas pueden incluir dispositivos que no pertenecen al buzón correspondiente. Ahora el conector de Citrix Endpoint Management para Exchange ActiveSync garantiza que los comandos a Exchange representen solo los dispositivos que pertenezcan a los buzones respectivos. [CXM-54842]
- En algunos entornos, no está disponible el ensamblado de Microsoft. Ahora el ensamblado requerido se instala explícitamente con la aplicación. [CXM-55439]
- Si los nombres distintivos de dispositivos o buzones contienen espacios entre el nombre del atributo y los signos igual (=) o espacios después de los signos igual y antes del valor, el conector de Citrix Endpoint Management para Exchange ActiveSync puede no asociar correctamente un dispositivo a su buzón ni viceversa. Como resultado, es posible que algunos dispositivos y/o buzones de correo se rechacen durante la conciliación de instantáneas. [CXM-56088]

Nota:

En las siguientes secciones de Novedades se hace referencia al conector de Citrix Endpoint Management para Exchange ActiveSync por su nombre anterior, 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 10.1.6 contiene la siguiente corrección en la versión 10.1.6.20:

- Cuando se detectan directivas de dispositivo que no están sincronizadas con Exchange, los comandos de estas directivas pueden incluir dispositivos que no pertenecen al buzón correspondiente. Ahora XenMobile Mail Manager garantiza que los comandos a Exchange representen solo los dispositivos que pertenezcan a los buzones respectivos. [CXM-54842]

Novedades en la versión 10.1.6

XenMobile Mail Manager 10.1.6 contiene los siguientes problemas resueltos y las siguientes mejoras:

- La ventana de historial de instantáneas entra a veces en un estado en que deja de actualizarse. El mecanismo de actualización de la ventana se ha mejorado y ahora es más fiable. [CXM-47983]
- Se han usado dos modos y rutas de código diferentes para instantáneas con particiones y sin particiones. Debido a que las instantáneas sin particiones equivalen a las instantáneas con particiones que tienen una configuración con una sola partición “*”, se ha eliminado el modo de instantánea sin particiones. Ahora el modo de instantánea predeterminado son instantáneas con 36 particiones (de 0 a 9, de A a Z). [CXM-49093]
- En la ventana “Historial de instantáneas”, los mensajes de estado sobrescriben los mensajes de error. Ahora, XenMobile Mail Manager ofrece dos campos separados para que los usuarios puedan ver el estado y los errores simultáneamente. [CXM-51942]
- Al conectarse a Exchange Online (Office 365), es posible que haya consultas relacionadas con las instantáneas que den como resultado un conjunto de datos truncados. Este problema puede ocurrir cuando XenMobile Mail Manager ejecuta un script canalizado con comandos múltiples. Un comando no puede pasar los datos lo suficientemente rápido al comando siguiente, con lo que la función se completa antes de tiempo. Como resultado, se producen datos incompletos. Ahora XenMobile Mail Manager puede imitar el proceso y esperar hasta que un comando esté listo antes de invocar el siguiente comando en sentido descendente. Este cambio debería dar como resultado que se procesen y se capturen todos los datos. [CXM-52280]
- Si se produce un error irresoluble en un comando de actualización de directiva en Exchange, ese comando se devuelve a la cola de tareas repetidamente durante un largo período de tiempo. Esta situación provocaba que el comando se enviara muchas veces a Exchange. En esta versión de XenMobile Mail Manager, un comando que genera un error solo se devuelve a la cola de tareas una cantidad determinada de veces. [CXM-52633]
- Si una actualización de directiva para un buzón específico implicaba permitir o bloquear todos los dispositivos, el comando **Set-CASMailbox** emitido fallaba debido a que la lista vacía se convertía en una cadena vacía en lugar de **NULL**. Ahora se envían los datos correctos. [CXM-53759]
- Al procesar un nuevo dispositivo, Exchange puede devolver el estado “DeviceDiscovery” durante un tiempo (generalmente 15 minutos). XenMobile Mail Manager no gestionaba específicamente este estado. Ahora XenMobile Mail Manager gestiona ese estado. En la ficha “Monitor” de la interfaz de usuario, los usuarios pueden filtrar por dispositivos en ese estado. [CXM-53840]
- XenMobile Mail Manager no verificaba la capacidad de escribir en la base de datos de XenMobile Mail Manager. Por lo tanto, si se restringieron los permisos, es posible que no se puede predecir el comportamiento. Ahora XenMobile Mail Manager captura y valida los permisos necesarios de la base de datos. XenMobile Mail Manager indica los permisos reducidos cuando se prueba la conexión (aparece un mensaje) o en el indicador “Database”(pase el puntero para ver el mensaje) en la parte inferior de la ventana principal “Configure”. [CXM-54219]
- Dependiendo de la carga de trabajo actual, cuando se dirige a XenMobile Mail Manager, es posible que el servicio no se detenga rápidamente. Por lo tanto, el servicio parece estar en un estado que no responde. Las mejoras permiten interrumpir las tareas en curso, lo que permite un apa-

gado más fácil. [CXM-54282]

Novedades en la versión 10.1.5

XenMobile Mail Manager 10.1.5 contiene los siguientes problemas resueltos:

- Cuando Exchange aplica limitaciones a la actividad de XenMobile Mail Manager, no hay ninguna indicación de ello (solo se indica en los registros). Con esta versión, un usuario puede colocar el puntero sobre la instantánea activa y aparece el estado “throttling”(limitación). Además, mientras se aplican limitaciones a XenMobile Mail Manager, se prohíbe el inicio de una instantánea principal hasta que Exchange deje de aplicarlas. [CXM-49617]
- Si Exchange aplica limitaciones a XenMobile Mail Manager durante una instantánea principal, puede que transcurra un tiempo insuficiente antes de ejecutar el siguiente intento de instantánea. Este problema resulta en más limitaciones y una instantánea fallida. Ahora XenMobile Mail Manager espera un mínimo del tiempo que Exchange especifica que debe esperar entre intentos de instantáneas. [CXM-49618]
- Cuando el diagnóstico está habilitado, el archivo de comandos muestra los comandos **Set-CasMailbox** con guiones que faltan antes de cada nombre de propiedad. Este problema solo ocurre en el formato del archivo de diagnóstico, no en el comando real de Exchange. El guión que falta impide que un usuario corte el comando y lo pegue directamente en una ventana de PowerShell para probarlo o validarlo. Los guiones se han agregado. [CXM-52520]
- Si la identidad de un buzón tiene el formato `lastname, firstname`, Exchange agrega una barra diagonal inversa antes de la coma cuando devuelve datos de una consulta. Esta barra invertida se debe quitar cuando XenMobile Mail Manager usa la identidad para consultar más datos. [CXM-52635]

Limitación conocida

Nota:

Se ha resuelto la siguiente limitación en la versión 10.1.6.

XenMobile Mail Manager presenta una limitación conocida que puede hacer que fallen los comandos de Exchange. Para aplicar cambios de directiva a Exchange, XenMobile Mail Manager emite un comando **Set-CASMailbox**. Este comando puede tener en cuenta dos listas de dispositivos: una para Permitir y otra para Bloquear. El comando se aplica a los dispositivos asociados a un buzón.

Estas listas están limitadas a 256 caracteres cada una por la API de Microsoft. Si una de esas listas supera la limitación, todo el comando falla y no se define ninguna de las directivas para esos dispositivos del buzón. El error que se informa, que aparece en los registros de XenMobile Mail Manager, es similar a lo siguiente. El ejemplo es para la lista bloqueada.

“Message:’Cannot bind parameter ‘ActiveSyncBlockedDeviceIDs’to the target. Exception setting “ActiveSyncBlockedDeviceIDs”: “The length of the property is too long. The maximum length is 256 and the length of the value provided is ...”

La longitud de los ID de dispositivo puede variar, pero una buena regla es que unos 10 dispositivos o más permitidos o bloqueados simultáneamente podrían sobrepasar el límite. Aunque tener tantos dispositivos asociados a un buzón específico es raro, existe esa posibilidad. Hasta que XenMobile Mail Manager se mejore para gestionar este caso, le recomendamos que limite la cantidad de dispositivos asociados al usuario y al buzón a 10 o menos. [CXM-52633]

Novedades en la versión 10.1.4

XenMobile Mail Manager 10.1.4 contiene los siguientes problemas resueltos:

- Debido a la poca seguridad que ofrecen, PCI Council va a retirar TLS 1.0 y TLS 1.1. Se agregó la funcionalidad TLS 1.2 a XenMobile Mail Manager. [CXM-38573, CXM-32560]
- XenMobile Mail Manager incluye un nuevo archivo de diagnóstico. Cuando se selecciona **Enable Diagnostics** en la especificación de Exchange, se genera un nuevo archivo de historial de instantáneas. Con cada intento de instantánea, se agrega una línea al archivo con los resultados de la instantánea. [CXM-49631]
- En el archivo de diagnóstico de comandos, la lista de dispositivos permitidos o bloqueados no aparecía para el comando **Set-CASMailbox**. En cambio, el nombre de la clase interna se muestra en el archivo para los argumentos relacionados. Ahora, XenMobile Mail Manager muestra la lista de identificadores de dispositivo como una lista separada con comas. [CXM-50693]
- Cuando falla un intento de establecer conexión con Exchange debido a una especificación incorrecta, un mensaje incorrecto sobrescribe el mensaje de error: “All connections in use”(Todas las conexiones están en uso). Ahora, aparecen mensajes más descriptivos, como “All connections are inoperable”(Todas las conexiones están inoperativas), “Connection pool is empty”(El grupo de conexiones está vacío), “All connections are throttled”(Todas las conexiones están limitadas) y “No available connections”(No hay conexiones disponibles). [CXM-50783]
- A veces, los comandos Allow, Block o Wipe se ponen en cola varias veces en la caché interna de XenMobile Mail Manager. Este problema provoca un retraso en el envío del comando a Exchange. Ahora, XenMobile Mail Manager solo pone en cola una instancia de cada comando. [CXM-51524]

Novedades en la versión 10.1.3

- **Compatibilidad con Google Analytics:** Nos gustaría saber cómo usa XenMobile Mail Manager para centrarnos en dónde mejorar el producto.
- **Parámetro para habilitar diagnósticos:** Aparece una casilla **Enable Diagnostics** en el cuadro de diálogo **Configuration** de la consola.

Configuration

Type: On Premise

Exchange Server:

User:

Password:

Major snapshot: Every 4 Hours

Minor snapshot: Every 5 Minutes

Snapshot Type: Shallow

Default Access: Unchanged

Command Mode: Powershell

Connection Expiration: Every 00 Hours 00 Minutes

Enable Diagnostics: ☐

View Entire Forest: ☐

Authentication: Kerberos

Test Connectivity

Save Cancel

Problemas resueltos en la versión 10.1.3

- En la ventana **Snapshot History**, la información que muestra el estado actual de la instantánea no refleja el estado real. [CXM-5570]
A veces, XenMobile Mail Manager no puede escribir en el archivo de diagnósticos de comandos. Cuando eso ocurre, el historial de comandos no se registra en su totalidad. [CXM-49217]
- Cuando ocurre un error con una conexión, la conexión puede no marcarse como “errored”(con errores). Como resultado, un comando posterior puede intentar usar la conexión y provocar otro error. [CXM-49495]
- Cuando se limita una acción desde Exchange Server, se puede iniciar una excepción en la rutina de comprobación de estado. Como resultado, puede que no se eliminen las conexiones con errores o las que han caducado. Además, XenMobile Mail Manager podría no crear conexiones hasta que se agote el tiempo de la limitación. [CXM-49794].
- Cuando se supera el recuento máximo de sesiones para Exchange, XenMobile Mail Manager informa del error “Device Capture Failed”(Fallo en la captura de dispositivos), que no es un mensaje preciso. En vez de este motivo, el mensaje debe indicar que las dos sesiones que suele usar XenMobile Mail Manager para la comunicación con Exchange ya están en uso. [CXM-49994]

Novedades en la versión 10.1.2

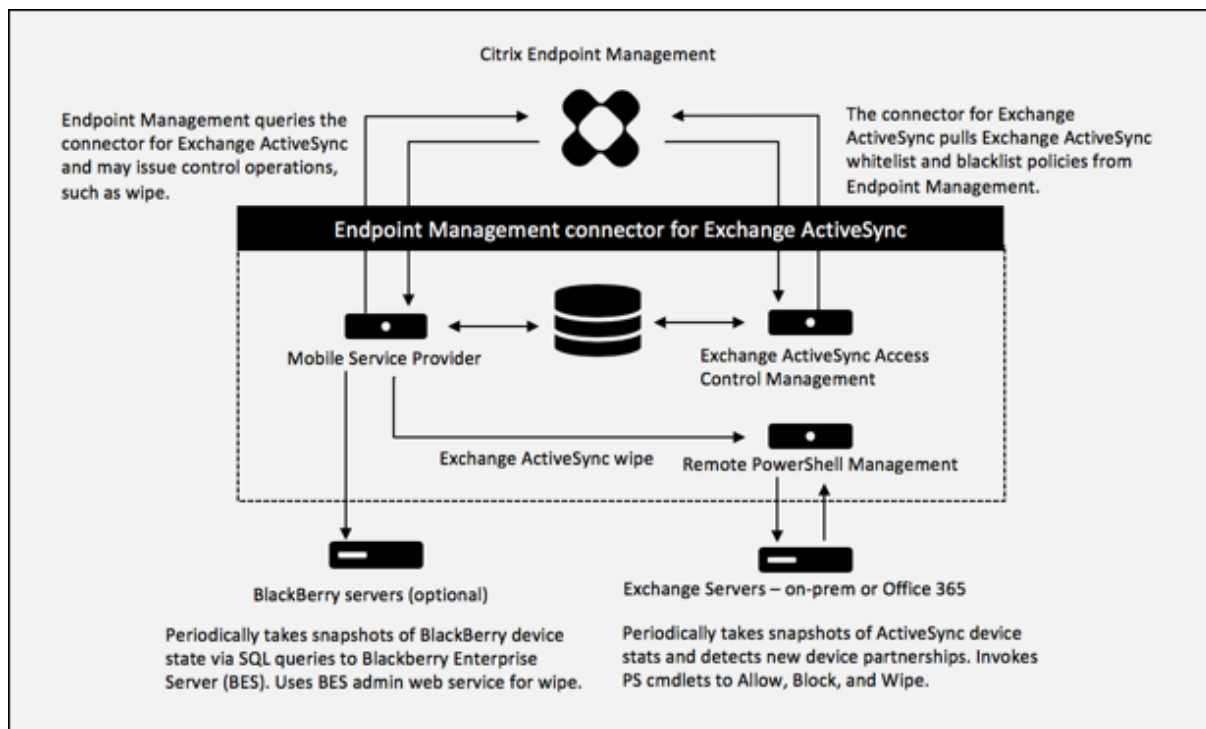
- **Conexión con Exchange mejorada:** XenMobile Mail Manager usa sesiones de PowerShell para comunicarse con Exchange. Una sesión de PowerShell, especialmente cuando se trata de Office 365, puede volverse inestable después de un tiempo, bloqueando el funcionamiento correcto de los siguientes comandos. XenMobile Mail Manager ahora puede establecer un período de caducidad para las conexiones. Cuando se agota el tiempo de la conexión, XenMobile Mail Manager cierra la sesión de PowerShell y crea una sesión. Al hacerlo, es menos probable que la sesión de PowerShell se vuelva inestable, lo que reduce significativamente la posibilidad de fallos en la instantánea.
- **Flujo de trabajo mejorado para las instantáneas:** Las instantáneas principales consumen mucho tiempo y requieren muchos recursos. Si se produce un error durante una instantánea, ahora XenMobile Mail Manager intenta completarla un máximo de tres veces. Los intentos posteriores no comienzan desde el principio. XenMobile Mail Manager continúa desde donde se quedó. Esta mejora aumenta la tasa general de instantáneas correctas, ya que permite errores transitorios mientras hay una instantánea en curso.
- **Diagnósticos mejorados:** Ahora las operaciones para solucionar problemas relacionadas con instantáneas son más fáciles, gracias a tres nuevos archivos de diagnóstico que se pueden generar durante una instantánea. Esos archivos ayudan a identificar problemas de comandos de PowerShell, buzones de correo con información incompleta y dispositivos que no se pueden relacionar a un buzón. Un administrador puede usar esos archivos para identificar datos que pueden no ser correctos en Exchange.
- **Uso mejorado de la memoria:** Ahora XenMobile Mail Manager es más eficiente en el consumo de la memoria. Los administradores pueden programar XenMobile Mail Manager para que se reinicie automáticamente y ofrezca un punto de partida raso al sistema.
- **Requisito previo de Microsoft .NET Framework 4.6:** El requisito previo para Microsoft .NET Framework ahora es la versión 4.6.

Problemas resueltos

- Error de solicitud de credenciales: La inestabilidad de las sesiones de Office 365 causa a menudo este error. Con la conexión mejorada con Exchange, se soluciona este problema. (XMHELP-293, XMHELP-311, XMHELP-801)
- Incoherencias de recuento entre buzones y dispositivos: XenMobile Mail Manager presenta un algoritmo mejorado para la asociación de buzones a dispositivos. La función de diagnósticos mejorados ayuda a identificar buzones y dispositivos que XenMobile Mail Manager considera fuera de su ámbito de responsabilidad. (XMHELP-623)
- No se reconocen los comandos Allow, Block ni Wipe: Se ha corregido un error donde, a veces, no se reconocen esos comandos de XenMobile Mail Manager. (XMHELP-489)
- Gestión de memoria: Mejor mitigación y gestión de memoria. (XMHELP-419)

Arquitectura

En el siguiente diagrama se muestran los componentes principales del conector de Citrix Endpoint Management para Exchange ActiveSync. Para obtener un diagrama detallado con una arquitectura como referencia, consulte [Arquitectura](#).



Los dos componentes principales son:

- **Administración del control de acceso de Exchange ActiveSync:** Se comunica con Citrix Endpoint Management para recuperar una directiva de Exchange ActiveSync, y combina esta directiva con cualquier directiva definida localmente para determinar los dispositivos Exchange ActiveSync a los que se debe permitir o denegar el acceso a Exchange. Las directivas definidas localmente amplían las reglas de directivas para permitir el control de acceso en función del grupo de Active Directory, del usuario, del tipo de dispositivo o del agente del dispositivo de usuario (por lo general, la versión de la plataforma móvil).
- **Administración remota de PowerShell:** Este componente se encarga de programar e invocar comandos de PowerShell remotos para aprobar la directiva compilada por la administración del control de acceso de Exchange ActiveSync. El componente crea, de forma periódica, una instantánea de la base de datos de Exchange ActiveSync para detectar dispositivos nuevos o modificados de Exchange ActiveSync.

Requisitos del sistema y requisitos previos

Para usar el conector de Citrix Endpoint Management para Exchange ActiveSync, se deben cumplir los siguientes requisitos mínimos del sistema:

- Windows Server 2016, Windows Server 2012 R2 o Windows Server 2008 R2 Service Pack 1. Debe ser un servidor en inglés. La compatibilidad para Windows Server 2008 R2 Service Pack 1 finaliza el 14 de enero de 2020 y la compatibilidad para Windows Server 2012 R2 finaliza el 10 de octubre de 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 (optativo).

Versiones mínimas admitidas de Microsoft Exchange Server:

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013 (dejará de ser compatible el 11 de abril de 2023)
- Exchange Server 2010 Service Pack 3 (dejará de ser compatible el 14 de enero de 2020)

Requisitos previos

- Windows Management Framework debe estar instalado.
 - PowerShell 5, 4 y 3
- La directiva de ejecución de PowerShell se debe establecer en RemoteSigned mediante Set-ExecutionPolicy RemoteSigned.
- El puerto TCP 80 debe estar abierto entre el equipo con el conector para Exchange ActiveSync y el Exchange Server remoto.

Clientes de correo electrónico del dispositivo: No todos los clientes de correo electrónico devuelven el mismo ID de ActiveSync para el mismo dispositivo. Debido a 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 constantemente el mismo y único ID de ActiveSync para cada dispositivo. Citrix ha realizado pruebas sin errores con estos clientes de correo electrónico:

- Cliente de correo electrónico nativo de Samsung
- Cliente de correo electrónico nativo de iOS

Exchange: A continuación, se indican los requisitos para un equipo local con Exchange:

Las credenciales especificadas en la interfaz de usuario de configuración de Exchange deben permitir la conexión al servidor de Exchange y deben 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 el servidor de 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 suministradas deben contar con derecho a conectarse al servidor de Exchange mediante el shell remoto. De forma predeterminada, el usuario que haya instalado Exchange tiene ese 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 usar `Set-PSSessionConfiguration` para eliminar el requisito administrativo, pero en este documento no se describe ese comando. Para obtener más información, consulte el artículo [About Session Configurations](#) de Microsoft.
 - El servidor Exchange debe estar configurado para admitir solicitudes remotas de PowerShell a través de HTTP. Por regla general, lo único que se necesita es que un administrador ejecute el siguiente comando de PowerShell en el servidor de Exchange: `WinRM QuickConfig`.
 - Exchange tiene muchas directivas de limitación de peticiones. Una de ellas controla la cantidad de conexiones simultáneas de PowerShell que se permiten por usuario. La cantidad predeter-

minada de conexiones simultáneas permitidas a un usuario es de 18 en Exchange 2010. Cuando se alcanza el límite de conexiones, el conector para Exchange ActiveSync no se puede conectar al Exchange Server. Hay maneras de cambiar la cantidad máxima de conexiones simultáneas permitidas a través de PowerShell, pero no se tratarán en esta documentación. Si le interesa, consulte las directivas de limitación de Exchange que estén relacionadas con la administración remota con PowerShell.

Requisitos para Office 365 Exchange

- **Permisos:** Las credenciales especificadas en la interfaz de usuario de la configuración de Exchange deben permitir la conexión a Office 365 y deben tener acceso total 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 suministradas deben contar con el derecho a conectarse al servidor de Office 365 a través del shell remoto. De forma predeterminada, el administrador conectado de Office 365 tiene los privilegios requeridos.
- **Directivas de limitaciones:** Exchange tiene muchas directivas de limitación de peticiones. Una de ellas controla la cantidad de conexiones simultáneas de PowerShell que se permiten por usuario. La cantidad predeterminada de conexiones simultáneas permitidas a un usuario es de tres en Office 365. Cuando se alcanza el límite de conexiones, el conector para Exchange ActiveSync no se puede conectar al Exchange Server. Hay maneras de cambiar la cantidad máxima de conexiones simultáneas permitidas a través de PowerShell, pero no se tratarán en esta documentación. Si le interesa, consulte las directivas de limitación de Exchange que estén relacionadas con la administración remota con PowerShell.

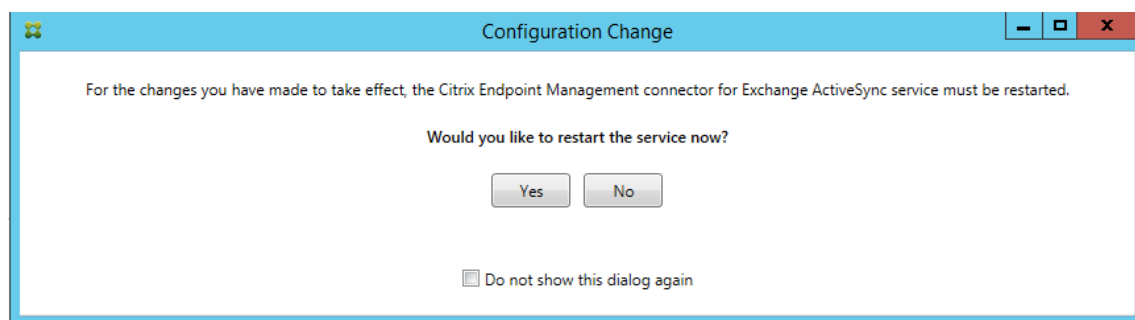
Instalación y configuración

1. Haga clic en el archivo XmmSetup.msi y, a continuación, siga las instrucciones del instalador para instalar el conector de Citrix Endpoint Management para Exchange ActiveSync.

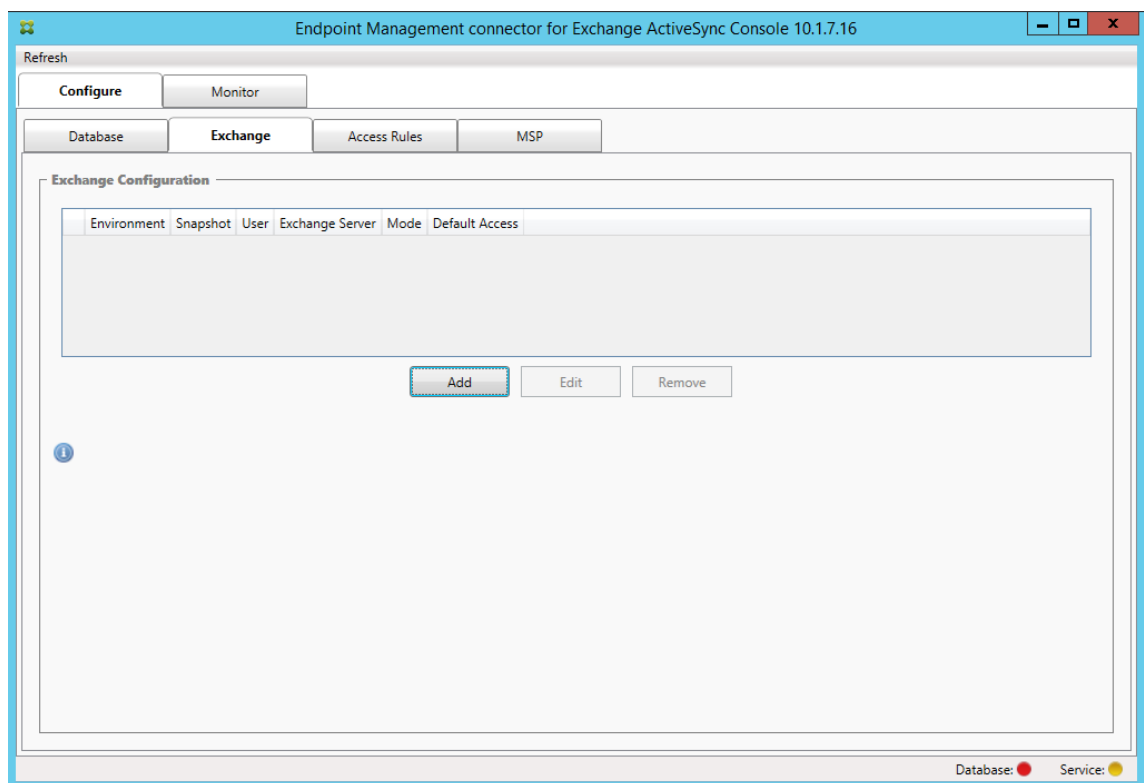
2. Deje **Launch the Configure utility** marcado en la última pantalla del Asistente de configuración. O bien desde el menú **Inicio**, abra el conector para Exchange ActiveSync.
3. Configure las siguientes propiedades de base de datos:
 - Seleccione la ficha **Configure > Database**.
 - Escriba el nombre del servidor SQL (el valor predeterminado es localhost).
 - Conserve la opción predeterminada de la base de datos, **CitrixXmm**.
4. Seleccione uno de los siguientes modos de autenticación para SQL:
 - **SQL:** Escriba el nombre de usuario y la contraseña de un usuario de SQL válido.
 - **Windows Integrated:** Si elige esta opción, las credenciales de inicio de sesión del servicio de XenMobile Mail Manager se deben cambiar a una cuenta de Windows que tenga permisos para acceder al servidor SQL Server. Para ello, abra **Panel de control > Herramientas administrativas > Servicios**, haga clic con el botón secundario en la entrada del servicio de XenMobile Mail Manager y, a continuación, haga clic en la ficha **Iniciar sesión**.

Si para la conexión de base de datos de BlackBerry también se selecciona la seguridad integrada de Windows, la cuenta de Windows que se especifique aquí también debe tener acceso a la base de datos de BlackBerry.

5. Haga clic en **Test Connectivity** para comprobar que se puede establecer conexión con el servidor SQL Server y, a continuación, haga clic en **Save**.
6. Un mensaje le solicitará que reinicie el servicio. Haga clic en **Sí**.



7. Configure uno o varios servidores Exchange:
 - Si administra un solo entorno de Exchange, solo deberá especificar un servidor. Si administra varios entornos de Exchange, deberá especificar un servidor de Exchange por cada entorno de Exchange.
 - Haga clic en la ficha **Configure > Exchange** y seleccione **Add**.

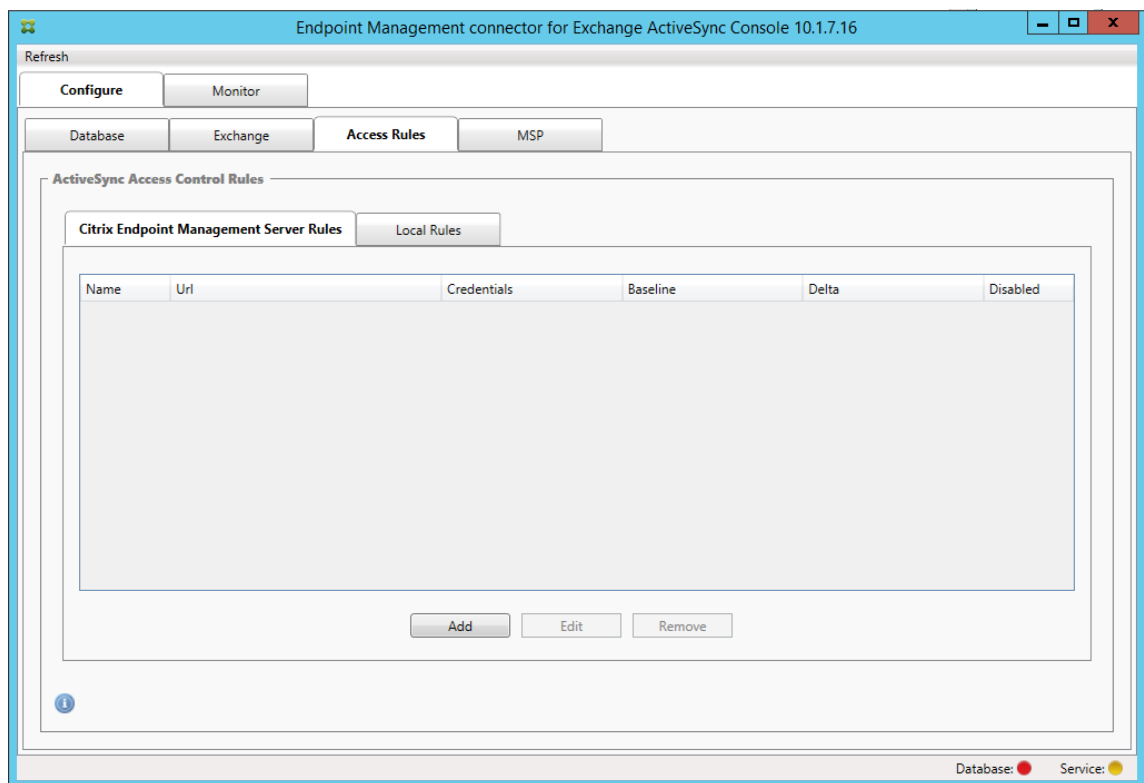


8. Seleccione el tipo de entorno de Exchange Server: **On Premise** u **Office 365**.

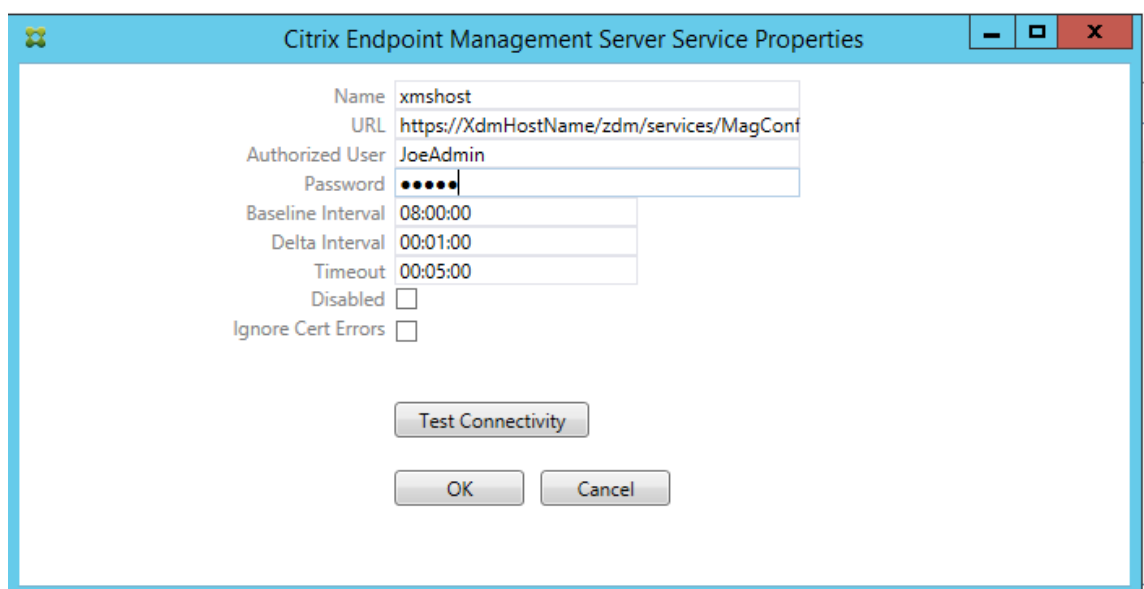
- Si selecciona **On Premise**, escriba el nombre del servidor de Exchange que se usará para los comandos remotos de PowerShell.
- Escriba el **nombre de usuario** de una identidad de Windows que tenga los permisos apropiados en el servidor de Exchange, como se especifica en el apartado “Requisitos”. A continuación, escriba la **contraseña** del usuario.
- Seleccione un horario para ejecutar las instantáneas principales. Una instantánea principal detecta cada asociación de Exchange ActiveSync.
- Seleccione un horario para ejecutar las instantáneas secundarias. Una instantánea secundaria detecta asociaciones recién creadas de Exchange ActiveSync.
- Seleccione el tipo de instantánea: **Deep** o **Shallow**. Las instantáneas superficiales (Shallow) son más rápidas y, con ellas, es suficiente para llevar a cabo todas las funciones de control de acceso del conector para Exchange ActiveSync.
- Seleccione el acceso predeterminado: **Allow**, **Block** o **Unchanged**. Este parámetro controla cómo se tratan todos los dispositivos, excepto aquellos que Citrix Endpoint Management o las reglas locales identifiquen de forma explícita. Si selecciona **Allow**, todos esos dispositivos pueden acceder a ActiveSync. Si selecciona **Block**, se deniega el acceso. Si selecciona **Unchanged**, no se realiza ningún cambio.
- Seleccione el modo de comandos de ActiveSync: **PowerShell** o **Simulation**.
- En el modo **PowerShell**, el conector para Exchange ActiveSync emite comandos de Power-

Shell para permitir el control de acceso pertinente. En el modo “Simulation”, el conector para Exchange ActiveSync no emite comandos de PowerShell, pero registra en la base de datos el comando en cuestión, así como los resultados esperados. En el modo Simulation, el usuario puede usar la ficha **Monitor** para ver lo que podría haber ocurrido si se hubiera habilitado el modo PowerShell.

- En **Connection Expiration**, configure las horas y los minutos de que dispondrá una conexión. Cuando una conexión alcanza la antigüedad especificada, se marca como caducada para que no se vuelva a usar. Cuando la conexión caducada ya no se usa, el conector para Exchange ActiveSync la cierra. Cuando se necesita de nuevo una conexión, se inicializa otra conexión si no hay ninguna disponible. Si no se especifica ningún valor, se usa el valor predeterminado de 30 minutos.
 - Seleccione **View Entire Forest** para configurar el conector para Exchange ActiveSync y ver 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 en implementaciones locales. De este modo, se puede utilizar el conector cuando su servidor no pertenece al dominio en el que reside el servidor de Exchange.
 - Haga clic en **Test Connectivity** para comprobar que se puede establecer conexión con el servidor de Exchange y, a continuación, haga clic en **Save**.
 - Un mensaje le solicitará que reinicie el servicio. Haga clic en **Sí**.
9. Configure las reglas de acceso: seleccione la ficha **Configuration > Access Rules**, haga clic en la ficha **Citrix Endpoint Management Rules** y luego haga clic en **Add**.



10. En la página **Citrix Endpoint Management Server Service Properties**, modifique la cadena de URL para que apunte al servidor de Citrix Endpoint Management. Por ejemplo, si el nombre de la instancia es **zdm**, escriba `https://<XdmHostName>/zdm/services/MagConfigService`. En el ejemplo, reemplace **XdmHostName** por la dirección IP o DNS del servidor de Citrix Endpoint Management.

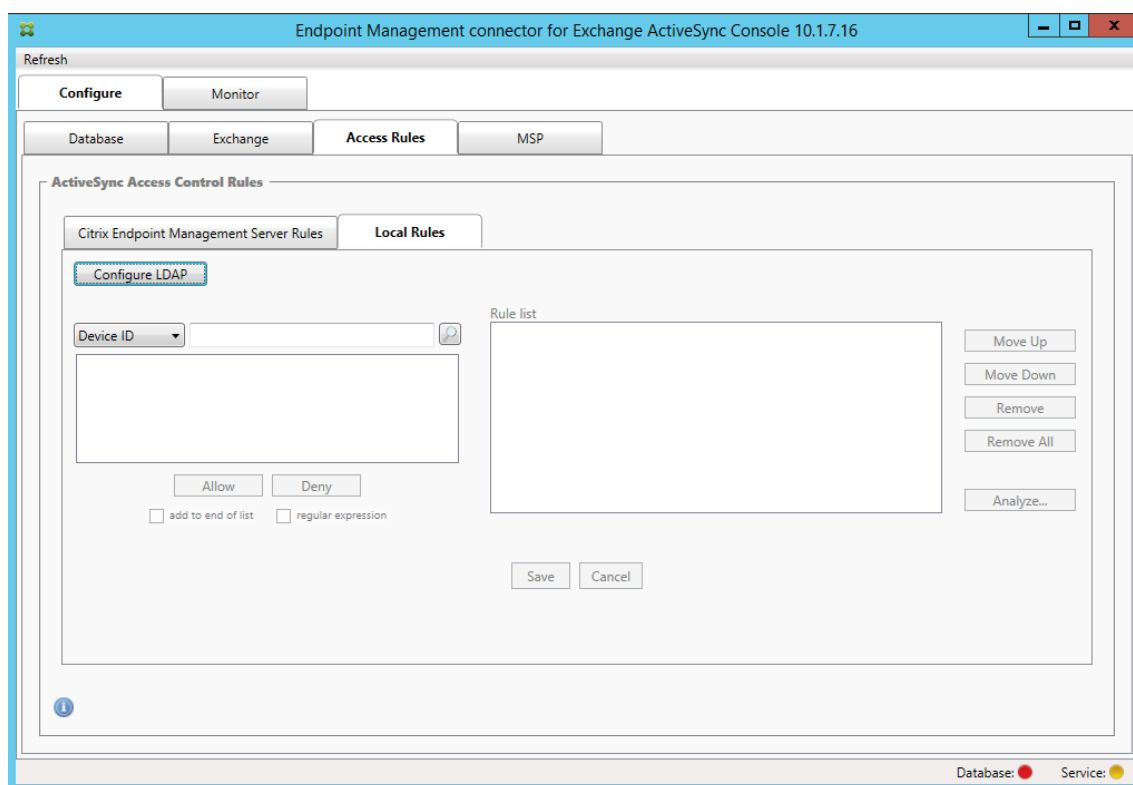


- Especifique un usuario autorizado del servidor.

- Escriba la contraseña del usuario.
- Conserve los valores predeterminados de **Baseline Interval**, **Delta Interval** y **Timeout**.
- Haga clic en **Test Connectivity** para probar la conexión con el servidor y haga clic en **OK**.

Si la casilla **Disabled** está marcada, el servicio de Citrix Endpoint Management Mail no recopila directivas de Citrix Endpoint Management.

11. Haga clic en la ficha **Local Rules**.



- Puede agregar reglas locales en función de: ActiveSync Device ID (el ID de dispositivo de ActiveSync), Device Type (el tipo de dispositivo), AD Group (el grupo de Active Directory), User (el usuario) o UserAgent (el agente del usuario del dispositivo). En la lista, seleccione el tipo adecuado.
- Escriba texto o fragmentos de texto en el cuadro de texto. Si quiere, haga clic en el botón de consulta para ver las entidades que se corresponden con el fragmento.

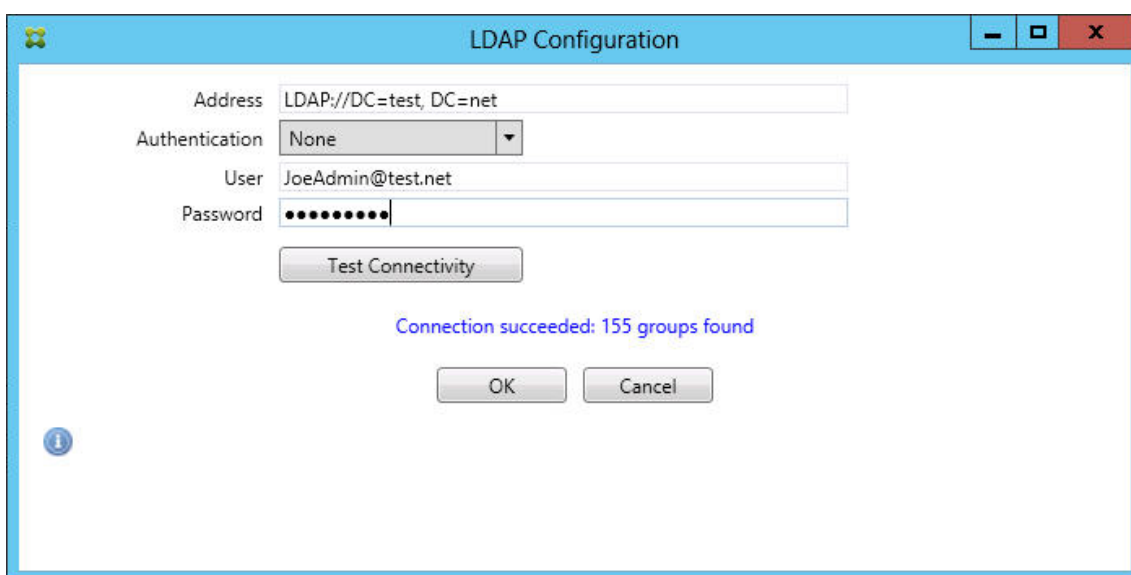
Para todos los criterios aparte de Group, el sistema se basa en los dispositivos que se han encontrado en una instantánea. Por lo tanto, si acaba de empezar y aún no ha completado ninguna instantánea, no habrá entidades disponibles.

- Seleccione un valor de texto y, a continuación, haga clic en **Allow** o en **Deny** para agregarlo a **Rule List** en el lado derecho. Puede quitar reglas o cambiar su orden mediante los botones situados a la derecha del panel **Rule List**. El orden es importante porque las reglas se cotejan en el orden mostrado con un usuario y un dispositivo determinados. Por

tanto, una correspondencia en una regla que se encuentre más arriba significa que las siguientes reglas no tendrán ningún efecto. Por ejemplo, si tiene una regla que permite todos los dispositivos iPad y otra regla posterior que bloquee al usuario “Sergio”, el iPad de Sergio aún tendrá permiso porque la regla “iPad” tiene una prioridad mayor (se coteja antes) que la regla “Sergio”.

- Para llevar a cabo un análisis de las reglas de la lista con el fin de buscar posibles conflictos, invalidaciones o complementaciones, haga clic en **Analyze** y, a continuación, en **Save**.

12. Si quiere crear reglas locales que operen en grupos de Active Directory, haga clic en **Configure LDAP** y, a continuación, configure las propiedades de conexión de LDAP.



13. Si quiere, configure una o varias instancias de BlackBerry Enterprise Server (BES). Para ello, haga clic en **Add** y escriba el nombre del servidor SQL de BES.

BES Properties

BES Sql Server

Server: BesServer

Database: BesMgmt

Authentication: Sql

User name: JoeAdmin

Password: •••••

Test Connectivity

Sync Schedule: Every 30 Minutes

Blackberry Device Administration from XMS

Enabled: ☒

BAS Server: BAServer

BAS Port: 443

Domain\User: ServerName\JoeAdmin

Password: •••••

Test Connectivity

Save Cancel

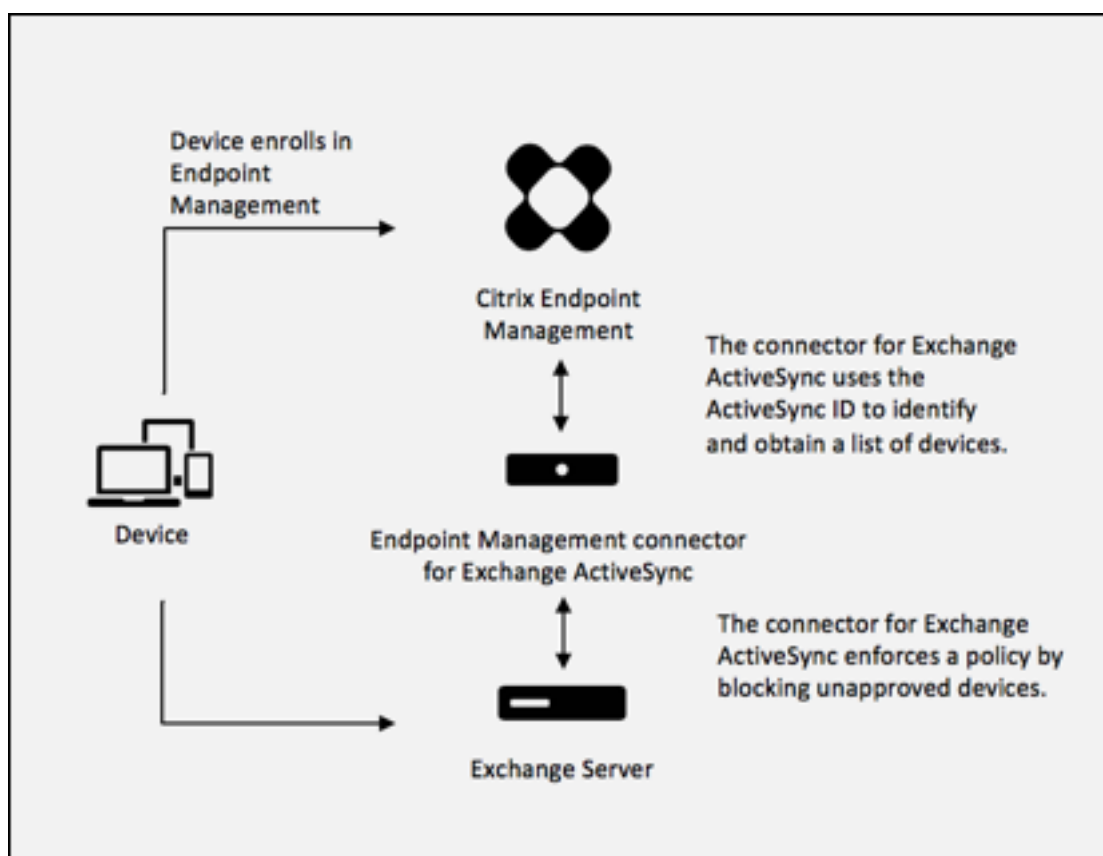
- Escriba el nombre de la base de datos de administración de BES.
- Seleccione el modo de **autenticación**. Si se selecciona la autenticación integrada de Windows, la cuenta de usuario del servicio del conector para Exchange ActiveSync será la cuenta utilizada para conectarse al servidor SQL Server para BES. Si también selecciona la seguridad integrada de Windows para la conexión de base de datos del conector, la cuenta de Windows especificada aquí también debe tener acceso a la base de datos del conector.
- Si selecciona **SQL authentication**, especifique el nombre de usuario y la contraseña.
- Configure la programación de sincronización en **Sync Schedule**. Esta es la programación usada para conectarse al servidor SQL Server para BES y buscar actualizaciones de dispositivo.
- Haga clic en **Test Connectivity** para comprobar la conectividad con el servidor SQL. Si se selecciona la seguridad integrada de Windows, esta prueba utiliza el usuario actual que ha iniciado sesión, no el usuario del servicio del conector; por lo tanto, la prueba de autenticación de SQL no es precisa.

- Si quiere admitir el borrado (Wipe) o el restablecimiento de contraseña (ResetPassword) remotos para los dispositivos BlackBerry desde Citrix Endpoint Management, marque la casilla **Enabled**.
- Introduzca el nombre de dominio completo (FQDN) de BES.
- Introduzca el puerto BES utilizado para el servicio web de admin.
- Escriba el nombre del usuario y la contraseña completos requeridos por el servicio de BES.
- Haga clic en **Test Connectivity** para probar la conexión al servidor BES y, luego, haga clic en **Save**.

Aplicar directivas de correo electrónico con los ID de ActiveSync

Es posible que una directiva de correo electrónico de la empresa indique que ciertos dispositivos no tienen la aprobación para usar el correo electrónico de la empresa. Para cumplir con esta directiva, asegúrese de que los usuarios no pueden tener acceso al correo electrónico de la empresa desde dichos dispositivos. El conector de Citrix Endpoint Management para Exchange ActiveSync y Citrix Endpoint Management operan juntos para aplicar este tipo de directiva de correo electrónico. Citrix Endpoint Management establece la directiva para acceder a correos electrónicos corporativos. Cuando un dispositivo no aprobado se inscribe con Citrix Endpoint Management, el conector para Exchange ActiveSync aplica la directiva.

El cliente de correo electrónico en un dispositivo se anuncia a Exchange Server (u Office 365) mediante el ID del dispositivo, también conocido como el ID de ActiveSync, que se usa para identificar el dispositivo de manera exclusiva. Citrix Secure Hub obtiene un identificador similar y envía el identificador a Citrix Endpoint Management cuando se inscribe el dispositivo. Comparando los dos ID de dispositivo, el conector para Exchange ActiveSync puede determinar si un dispositivo en concreto debe tener acceso al correo electrónico de la empresa. En la siguiente ilustración se muestra este concepto.



Si Citrix Endpoint Management envía al conector para Exchange ActiveSync un ID de ActiveSync distinto del ID publicado por el dispositivo en Exchange, el conector no podrá indicar a Exchange cómo debe proceder con respecto a dicho dispositivo.

Los ID de ActiveSync coincidentes funcionan con fiabilidad en la mayoría de las plataformas. Sin embargo, Citrix ha detectado que, en algunas implementaciones de Android, el ID de ActiveSync enviado desde el dispositivo es diferente del ID que el cliente de correo anuncia en Exchange. Para evitar 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 empresarial se aplica correctamente, puede adoptar una seguridad defensiva. Configure el conector de Citrix Endpoint Management para Exchange ActiveSync para bloquear correos electrónicos. Para ello, establezca la directiva estática en **Denegar** de forma predeterminada. Así, si un empleado configura otro cliente de correo electrónico en un dispositivo Android y la detección de ID de ActiveSync no funciona, ese empleado no podrá acceder al correo electrónico empresarial.

Reglas de control de acceso

El conector de Citrix Endpoint Management para Exchange ActiveSync ofrece un enfoque basado en reglas para controlar de forma dinámica el acceso a los dispositivos Exchange ActiveSync. Una regla de control de acceso del conector se compone de dos partes: una expresión correspondiente y un estado de acceso deseado (Permitir o Bloquear). Una regla se puede cotejar con un dispositivo Exchange ActiveSync concreto para determinar si se le puede aplicar (es decir, si corresponde al dispositivo). Hay varios tipos de expresiones correspondientes. Por ejemplo: una regla puede corresponderse con todos los dispositivos de un determinado tipo o un ID de Exchange ActiveSync o todos los dispositivos de un usuario concreto, entre otros.

En cualquier momento durante el proceso de agregar, quitar o cambiar el orden de las reglas en la lista de reglas, puede hacer clic en el botón **Cancel** para revertir la lista de reglas al estado en que estaba al abrirla. A menos que haga clic en **Save**, los cambios realizados en esta ventana se perderán si cierra la herramienta de configuración.

El conector de Citrix Endpoint Management para Exchange ActiveSync contiene tres tipos de reglas: reglas locales, reglas del servidor de Citrix Endpoint Management (también conocidas como reglas de Device Manager) y la regla del acceso predeterminado.

Reglas locales: Las reglas locales tienen la prioridad más alta. Si un dispositivo coincide con una regla local, el proceso de cotejo de reglas se detiene. No se consultarán ni las reglas del servidor de Citrix Endpoint Management ni la regla del acceso predeterminado. Las reglas locales se configuran localmente en el conector para Exchange ActiveSync, desde la ficha **Configure > Access Rules > Local Rules**. La correspondencia de compatibilidad se basa en la pertenencia de un usuario a un grupo determinado de Active Directory. La correspondencia de compatibilidad se basa en expresiones regulares de los siguientes campos:

- ID del dispositivo ActiveSync
- Tipo de dispositivo ActiveSync
- Nombre principal de usuario (UPN)
- Agente del usuario de ActiveSync (normalmente, la plataforma del dispositivo o el cliente de correo electrónico)

Mientras una instantánea principal se complete y encuentre dispositivos, podrá agregar reglas, ya sean de expresión regular o normal. Si no se completa ninguna instantánea principal, solo podrá agregar reglas de expresión regular.

Reglas del servidor de Citrix Endpoint Management: Las reglas del servidor de Citrix Endpoint Management hacen referencia a un servidor externo de Citrix Endpoint Management que proporciona reglas de dispositivos administrados. El servidor de Citrix Endpoint Management se puede configurar con sus propias reglas de alto nivel, que identifican aquellos dispositivos que se van a permitir o bloquear en función de las propiedades que conozca Citrix Endpoint Management (por ejemplo,

si el dispositivo se ha liberado por jailbreak o si contiene aplicaciones prohibidas). Citrix Endpoint Management coteja las reglas de alto nivel y genera un conjunto de identificadores de dispositivos ActiveSync permitidos o bloqueados. Después, estos ID se entregan a XenMobile Mail Manager.

Regla del acceso predeterminado: La regla del acceso predeterminado es única en que es una correspondencia potencial con todos los dispositivos y siempre se coteja la última. Esta es una regla comodín, lo que significa que, si un dispositivo determinado no coincide con ninguna regla local o del servidor de Citrix Endpoint Management, el estado del acceso al dispositivo lo determina el estado de la regla del acceso predeterminado.

- **Default Access –Allow (Acceso predeterminado: Permitir):** Se permitirá el acceso de cualquier dispositivo que no coincida con una regla local o del servidor de Citrix Endpoint Management.
- **Default Access –Block (Acceso predeterminado: Bloquear):** Se bloqueará el acceso de cualquier dispositivo que no coincida con una regla local o del servidor de Citrix Endpoint Management.
- **Default Access - Unchanged (Acceso predeterminado: Sin cambios):** el conector para Exchange ActiveSync no modificará el estado de acceso de un dispositivo que no coincida con ninguna regla local o del servidor de Citrix Endpoint Management. Si Exchange ha puesto un dispositivo en el modo de cuarentena, no se realiza ninguna acción; por ejemplo, la única forma de quitar un dispositivo del modo de cuarentena es tener una regla local o una regla de Device Manager que ignore explícitamente la cuarentena.

Acerca de los cotejos de reglas

Las reglas se cotejan siguiendo un orden (de mayor a menor prioridad) con cada dispositivo sobre el que Exchange informa al conector para Exchange ActiveSync:

- Reglas locales
- Reglas del servidor de Citrix Endpoint Management
- Regla del acceso predeterminado

Cuando se encuentra una correspondencia, el cotejo se detiene. Por ejemplo: si una regla local coincide con un dispositivo determinado, este no se cotejará con ninguna regla del servidor de Citrix Endpoint Management ni con la regla del acceso predeterminado. Esto también se da en el caso de un tipo concreto de regla. Por ejemplo, si hay más de una correspondencia en la lista de reglas de un dispositivo concreto, el cotejo se detiene tan pronto como se encuentre la primera correspondencia.

El conector para Exchange ActiveSync vuelve a cotejar el conjunto de reglas definido en cada momento cuando cambian las propiedades del dispositivo, cuando se agregan o quitan dispositivos,

o cuando cambian las propias reglas. Las instantáneas principales pueden elegir cambios y eliminaciones de las propiedades de dispositivo a intervalos que se pueden configurar. Las instantáneas secundarias eligen dispositivos nuevos a intervalos que se pueden configurar.

Exchange ActiveSync también tiene reglas que controlan el acceso. Es importante comprender el funcionamiento de estas reglas en el contexto del conector para Exchange ActiveSync. Exchange se puede configurar con tres niveles de reglas: exenciones personales, reglas de dispositivos y parámetros de organización. El conector para Exchange ActiveSync automatiza el control del acceso por la emisión, mediante programación, de solicitudes remotas de PowerShell que afectan a las listas de excepciones personales. Se trata de listas de identificadores de dispositivos Exchange ActiveSync permitidos o bloqueados asociados a un buzón de correo determinado. Cuando el conector Exchange ActiveSync se implementa, asume la capacidad de administración de las listas de exención en Exchange. Consulte el artículo [Device management with Exchange and Configuration Manager](#) de Microsoft.

El análisis es especialmente útil en situaciones en que se han definido varias reglas para el mismo campo. Puede detectar problemas potenciales de las relaciones entre las reglas. El análisis se realiza con respecto a los campos de reglas; por ejemplo, las reglas se analizan por grupos con el campo que se coteja (como el ID del dispositivo ActiveSync, el tipo de dispositivo ActiveSync, el usuario y el agente de usuario, entre otros).

Terminología referente a las reglas

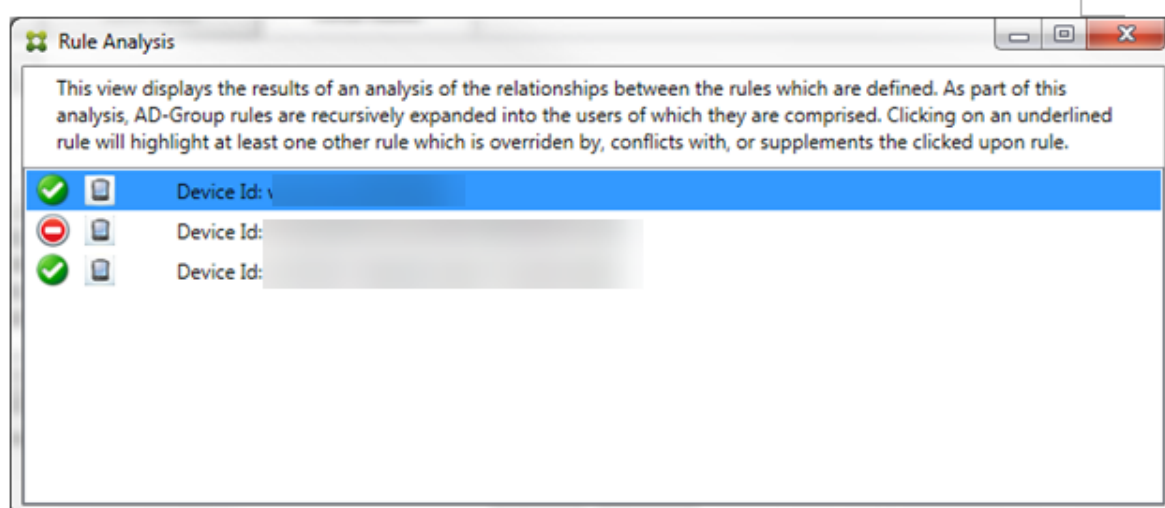
- **Overriding rule (Regla de invalidación):** Se produce una invalidación cuando hay más de una regla que se podría aplicar al mismo dispositivo. Como las reglas se cotejan por prioridad en la lista, es posible que las últimas instancias de reglas que se podrían aplicar nunca se cotejen.
- **Conflicting rule (Regla en conflicto):** El conflicto se produce cuando hay más de una regla que se podría aplicar al mismo dispositivo, pero cada regla tiene estipulado un acceso (permitir o bloquear) diferente. Si las reglas en conflicto no son de expresión regular, un conflicto siempre tiene la connotación implícita de una invalidación.
- **Supplemental rule (Regla adicional):** Se produce una adición cuando hay varias reglas de expresión regular y, por lo tanto, es posible que necesite comprobar que las dos (o más) expresiones regulares se pueden combinar en una sola regla de expresión regular, o bien deberá comprobar que no dupliquen la funcionalidad. Una regla adicional también puede entrar en conflicto en el acceso (permitir o bloquear).
- **Primary rule (Regla primaria):** La regla primaria es aquella sobre la que se ha hecho clic en el cuadro de diálogo. La regla está indicada visualmente por una línea de borde sólido que la rodea. La regla también tiene 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 la regla primaria. Si una flecha apunta hacia abajo, indica que hay reglas auxiliares que siguen a la regla primaria. Solo una regla primaria puede estar activa en un momento dado.

- **Ancillary rule (Regla auxiliar):** Una regla auxiliar está relacionada con la regla primaria, ya sea por invalidación, por conflicto o por reglas adicionales. Las reglas se indican visualmente con un borde discontinuo que las rodea. Puede haber entre una y varias reglas auxiliares por cada regla primaria. Al hacer clic en una entrada subrayada, las reglas auxiliares marcadas siempre se marcan con respecto a la regla primaria. Por ejemplo: la regla primaria invalida la regla auxiliar, o la regla auxiliar entra en conflicto en el acceso con la regla primaria, o la regla auxiliar complementa la regla primaria.

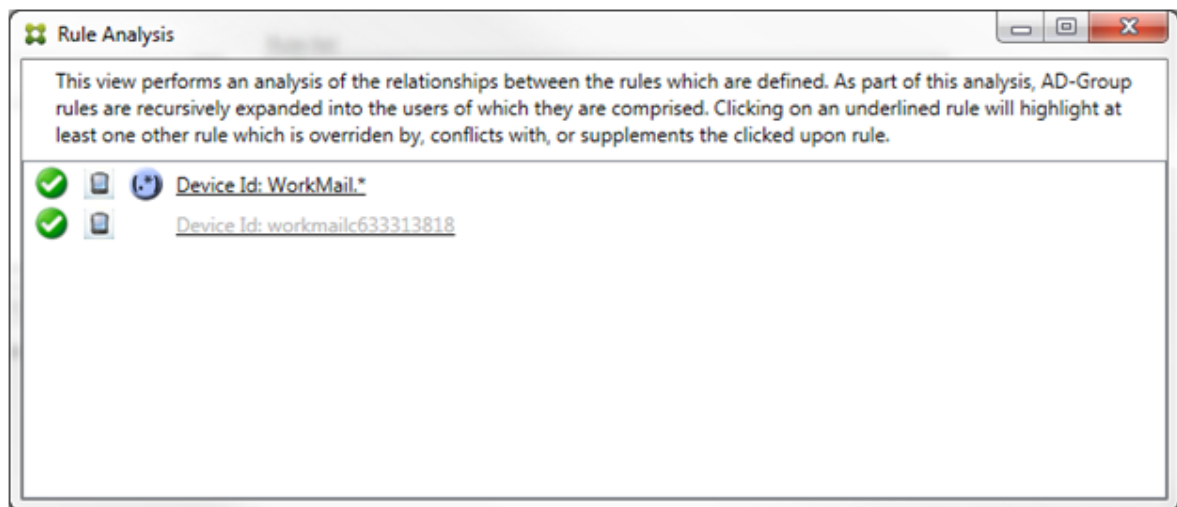
Cómo aparecen los tipos de reglas en el cuadro de diálogo Rule Analysis

Cuando no haya conflictos, invalidaciones ni complementaciones, el cuadro “Rule Analysis” no contendrá entradas subrayadas. Hacer clic en alguno de los elementos no tiene ningún efecto: solo se habrá seleccionado el elemento de la manera habitual.

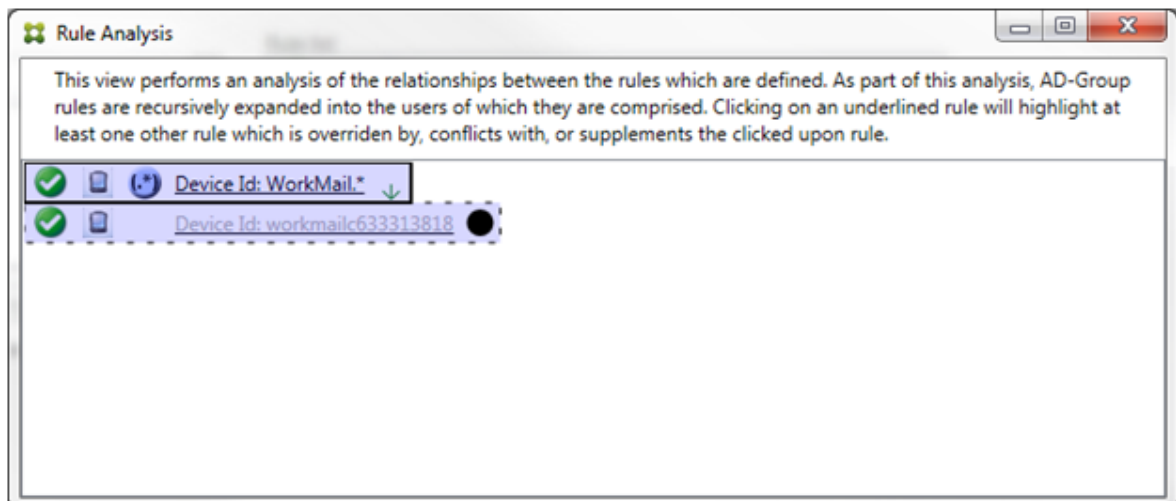
La ventana “Rule Analysis” tiene una casilla de verificación que, marcada, muestra únicamente las reglas con conflictos, invalidaciones, redundancias y complementaciones.



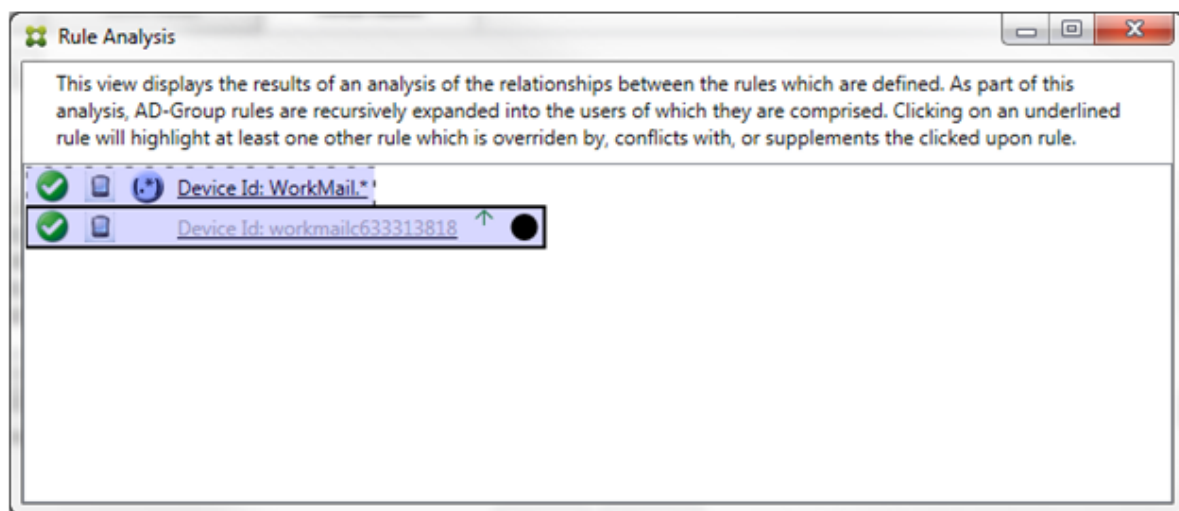
Cuando se produzca una invalidación, se subrayarán al menos dos reglas: la primaria y las auxiliares. Al menos una regla auxiliar aparece con una fuente más atenuada para indicar que se ha reemplazado por otra regla de mayor prioridad. Puede hacer clic en la regla invalidada para averiguar qué regla o reglas la han invalidado. Cada vez que se marque una regla como invalidada, ya sea porque es la primaria o porque es la auxiliar, aparecerá un círculo negro junto a ella, a modo de indicación visual de que la regla está inactiva. Por ejemplo, antes de hacer clic en la regla, el cuadro aparece de la siguiente manera:



Cuando haga clic en la regla de mayor prioridad, el cuadro aparecerá de la siguiente manera:

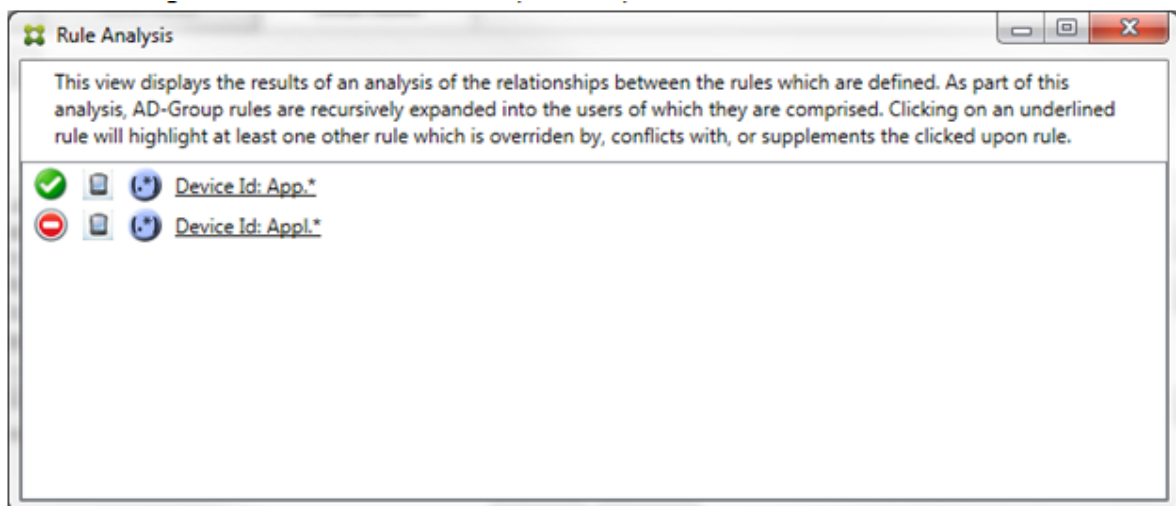


En este ejemplo, la regla de expresión regular `WorkMail.*` es la regla primaria (indicada con el borde sólido) y la regla normal `workmailc633313818` es una regla auxiliar (indicada con el borde discontinuo). El punto negro junto a la regla auxiliar es una indicación visual de que la regla está inactiva (nunca se cotejará) debido a la regla de expresión regular de mayor prioridad que la precede. Después de hacer clic en la regla invalidada, el cuadro aparecerá de la siguiente manera:



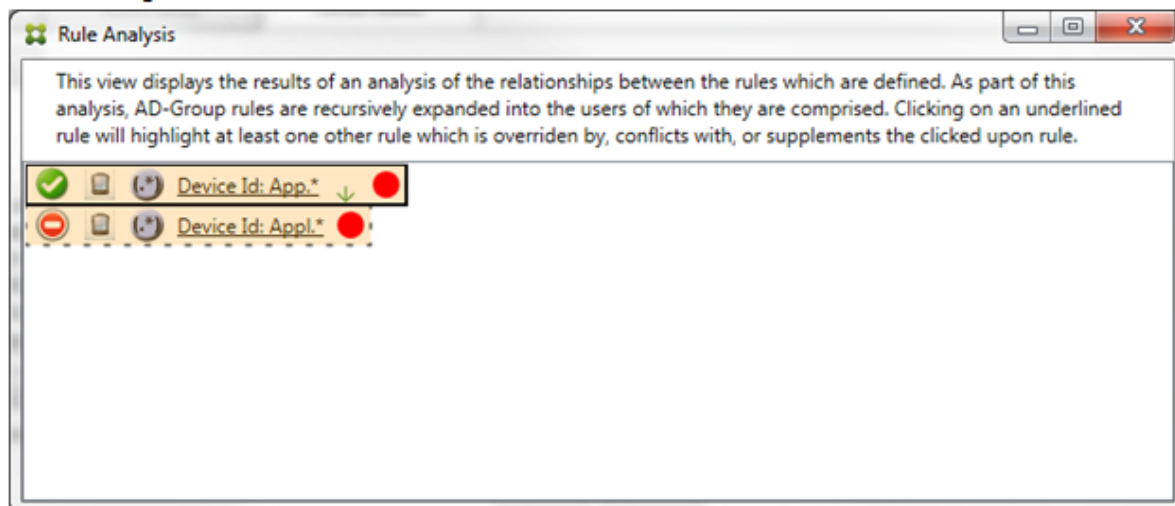
En el ejemplo anterior, la regla de expresión regular `WorkMail.*` es la regla auxiliar (indicada con el borde discontinuo) y la regla normal `workmailc633313818` es la regla primaria (indicada con el borde sólido). En este sencillo ejemplo, no hay mucha diferencia. Para un ejemplo más complejo, consulte el ejemplo de expresión compleja más adelante en este apartado. En un entorno con varias reglas definidas, hacer clic en la regla invalidada identificaría rápidamente las reglas que la han invalidado.

Cuando se produzca un conflicto, se subrayarán al menos dos reglas: la primaria y la(s) auxiliar(es). Las reglas en conflicto se indican con un punto de color rojo. Aquellas reglas que solo entren en conflicto una con otra solo se dan cuando hay dos o más reglas de expresión regular definidas. En todos los demás casos de conflictos, no solo hay un conflicto, sino también una invalidación. Antes de hacer clic en las reglas, en un ejemplo sencillo, el cuadro aparece de la siguiente manera:



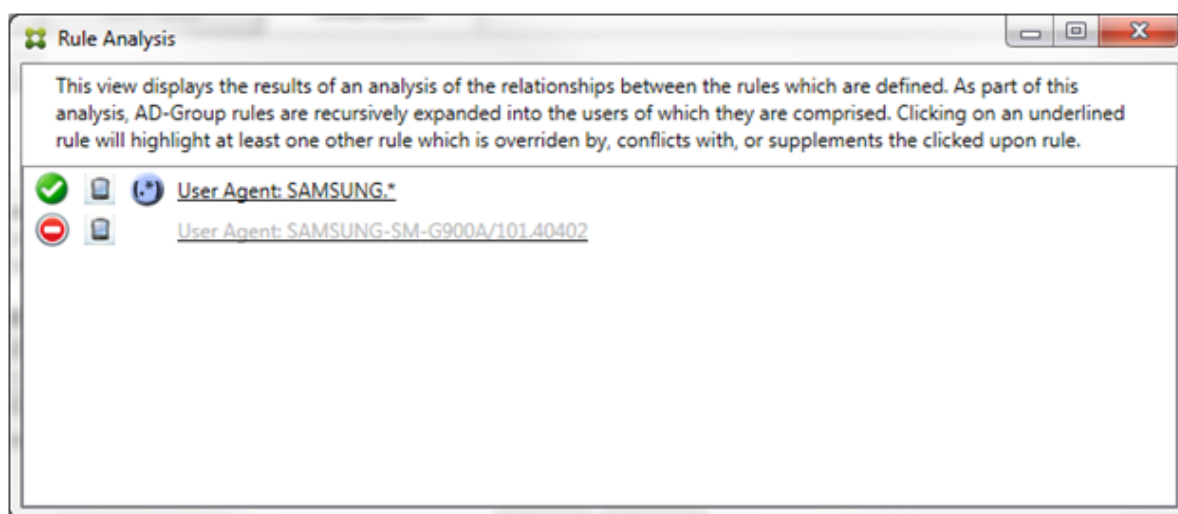
Tras examinar las dos reglas de expresiones regulares, es evidente que la primera regla permite el acceso a todos aquellos dispositivos con un ID de dispositivo que contenga "App" y la segunda regla niega el acceso a todos aquellos dispositivos con un ID de dispositivo que contenga `Appl`. Además,

aunque la segunda regla rechaza todos los dispositivos con un ID de dispositivo que contenga `App1`, no se negará el acceso a ningún dispositivo que se corresponda con ese criterio por la prioridad más alta de la regla que permite el acceso. Después de hacer clic en la primera regla, el cuadro aparece de la siguiente manera:



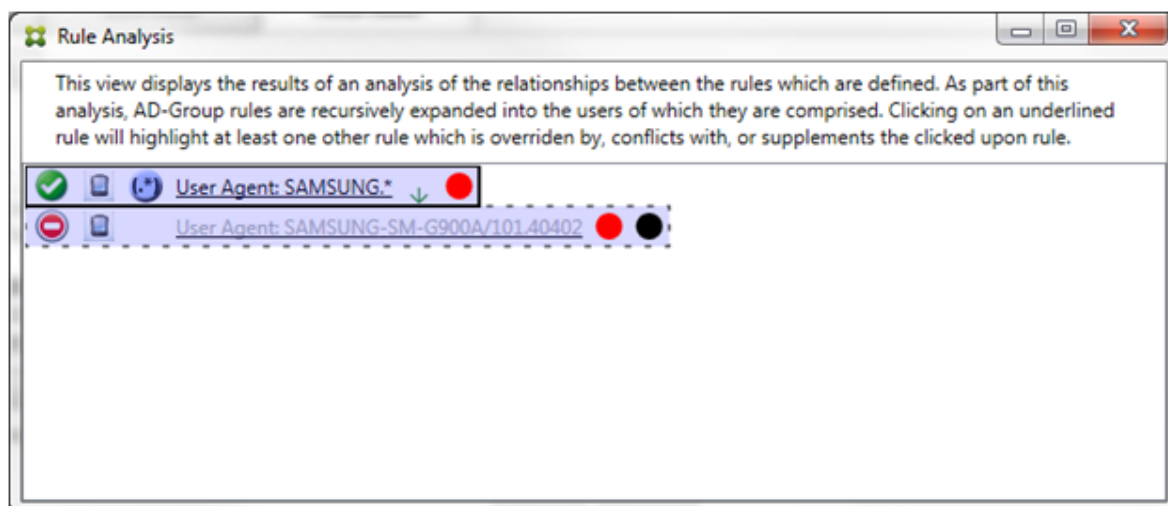
En este caso, tanto la regla primaria (la regla de expresión regular `App.*`) como la regla auxiliar (la regla de expresión regular `App1.*`) se resaltan en amarillo. Este es simplemente un elemento visual que sirve para advertirle de que ha aplicado más de una regla de expresión regular a un único campo correspondiente, lo que puede derivar en un problema de redundancia o algo más grave.

En un caso de conflicto e invalidación, la regla primaria (regla de expresión regular `App.*`) y la regla auxiliar (regla de expresión regular `App1.*`) se resaltan en amarillo. Este es simplemente un elemento visual que sirve para advertirle de que ha aplicado más de una regla de expresión regular a un único campo correspondiente, lo que puede derivar en un problema de redundancia o algo más grave.



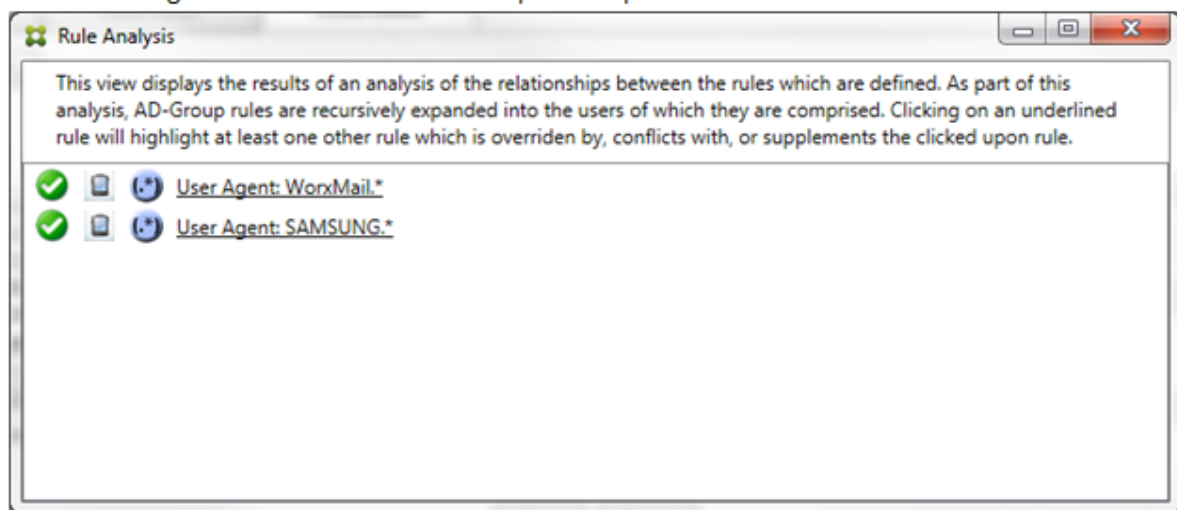
En el ejemplo anterior, es fácil observar que la primera regla (regla de expresión regular `SAMSUNG.*`) no solo invalida la siguiente regla (regla normal `SAMSUNG-SM-G900A/101.40402`), sino que las dos reglas se diferencian en su acceso (la primaria especifica Permitir, mientras que la auxiliar especifica Bloquear). La segunda regla (regla normal `SAMSUNG-SM-G900A/101.40402`) aparece con un texto más atenuado para indicar que se ha invalidado y está, por lo tanto, inactiva.

Después de hacer clic en la regla de expresión regular, el cuadro aparece de la siguiente manera:

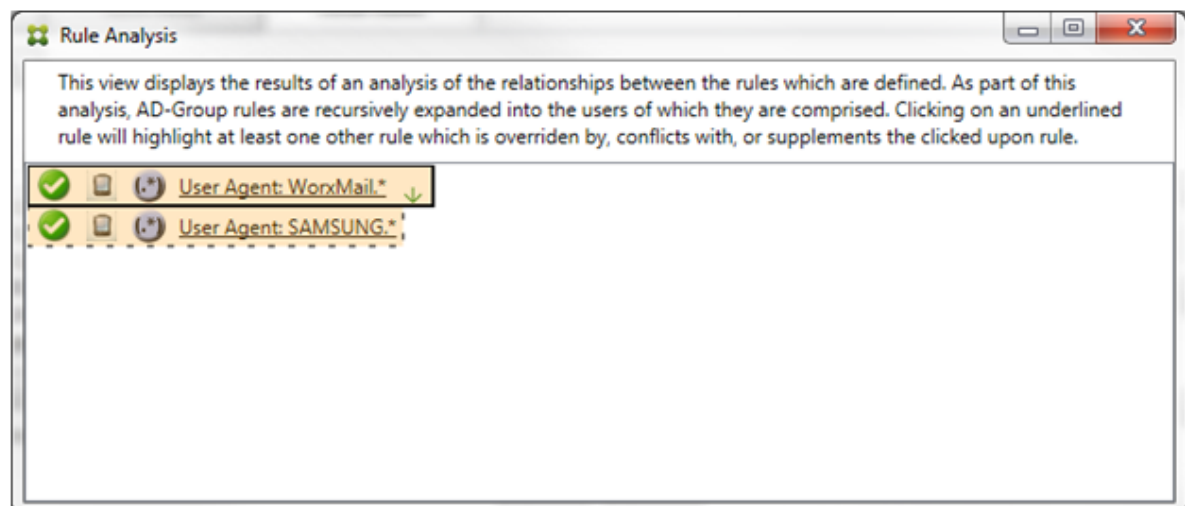


La regla primaria (regla de expresión regular `SAMSUNG.*`) va seguida de un punto rojo para indicar que su estado de acceso está en conflicto con una o varias reglas auxiliares. La regla auxiliar (regla normal `SAMSUNG-SM-G900A/101.40402`) va seguida de un punto rojo para indicar que su estado de acceso está en conflicto con la regla primaria. Esa regla también va seguida de un punto negro para indicar que está invalidada y, por lo tanto, inactiva.

Se subrayan al menos dos reglas: la primaria y la(s) auxiliar(es). Las reglas que solo se complementan entre ellas solo pueden ser reglas de expresión regular. Cuando las reglas se complementan entre ellas, se indican con una capa de color amarillo. Antes de hacer clic en las reglas, en un ejemplo sencillo, el cuadro aparece de la siguiente manera:




Tras echar un vistazo, es evidente que ambas reglas son de expresión regular y que se han aplicado al campo de ID de dispositivo ActiveSync en el conector de Citrix Endpoint Management para Exchange ActiveSync. Después de hacer clic en la primera regla, el cuadro aparece de la siguiente manera:

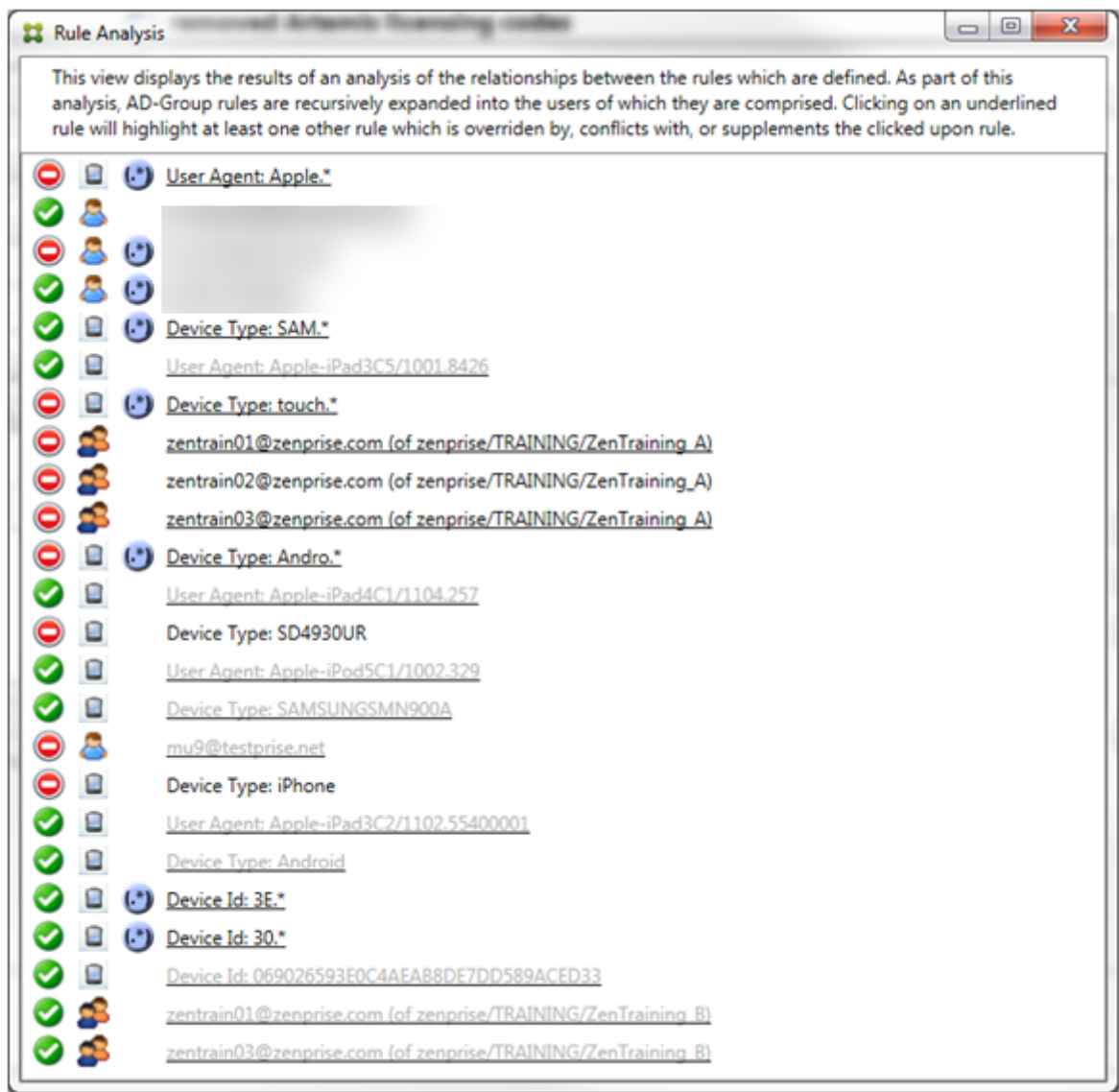


La regla primaria (regla de expresión regular `WorkMail.*`) está resaltada con una capa amarilla para indicar que hay al menos una regla auxiliar adicional que es una expresión regular. La regla auxiliar (regla de expresión regular `SAMSUNG.*`) está resaltada en amarillo para indicar que ella y la regla primaria son reglas de expresión regular que se aplican al mismo campo en el conector para Exchange ActiveSync. En este caso, ese campo es el ID del dispositivo ActiveSync. Las expresiones regulares pueden superponerse. Le corresponde a usted decidir si sus expresiones regulares se han elaborado correctamente.

Ejemplo de una expresión compleja

Se pueden producir tantos conflictos, invalidaciones o complementaciones que no se puede ofrecer un ejemplo para todos los casos posibles. En el siguiente ejemplo, se describe lo que no se recomienda hacer y también se ilustra el true potencial de la construcción visual del análisis de reglas. En la siguiente imagen, la mayoría de los elementos están subrayados. Muchos de los elementos se representan con una fuente más atenuada que otras, lo que indica que la regla en cuestión se ha invalidado por una regla de mayor prioridad. También se han incluido en la lista reglas de expresión

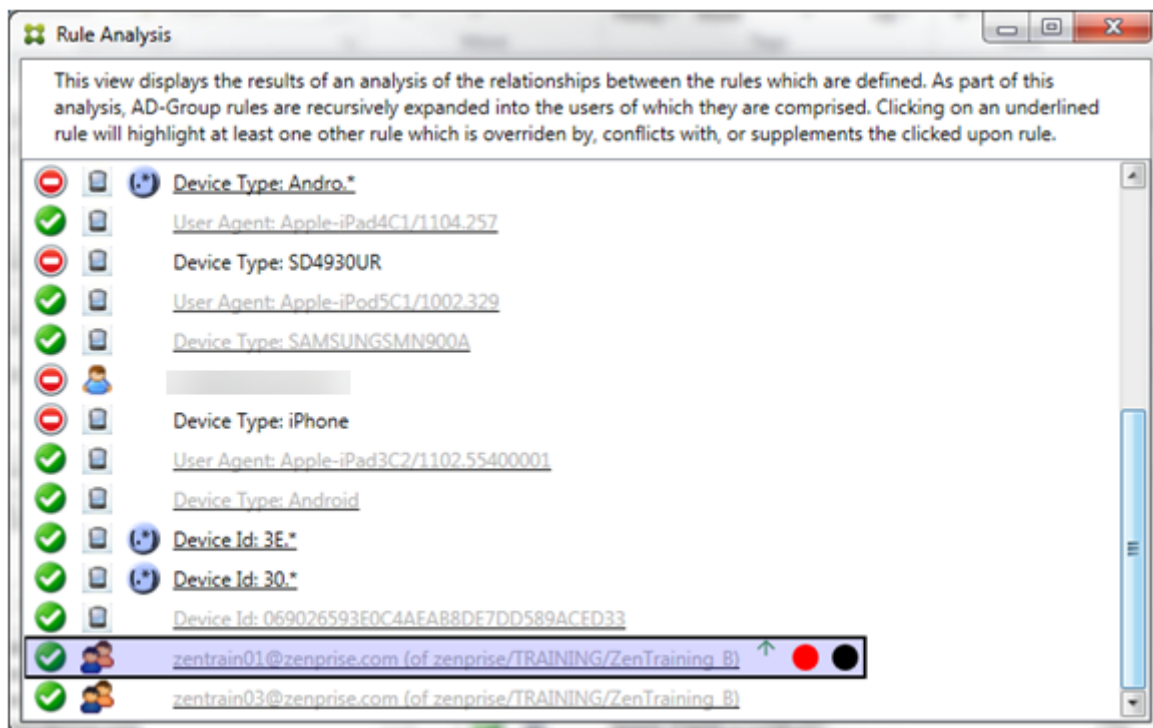
regular, indicadas con el icono .



Cómo analizar una invalidación

Para ver qué regla o reglas han invalidado una regla determinada, haga clic en la regla.

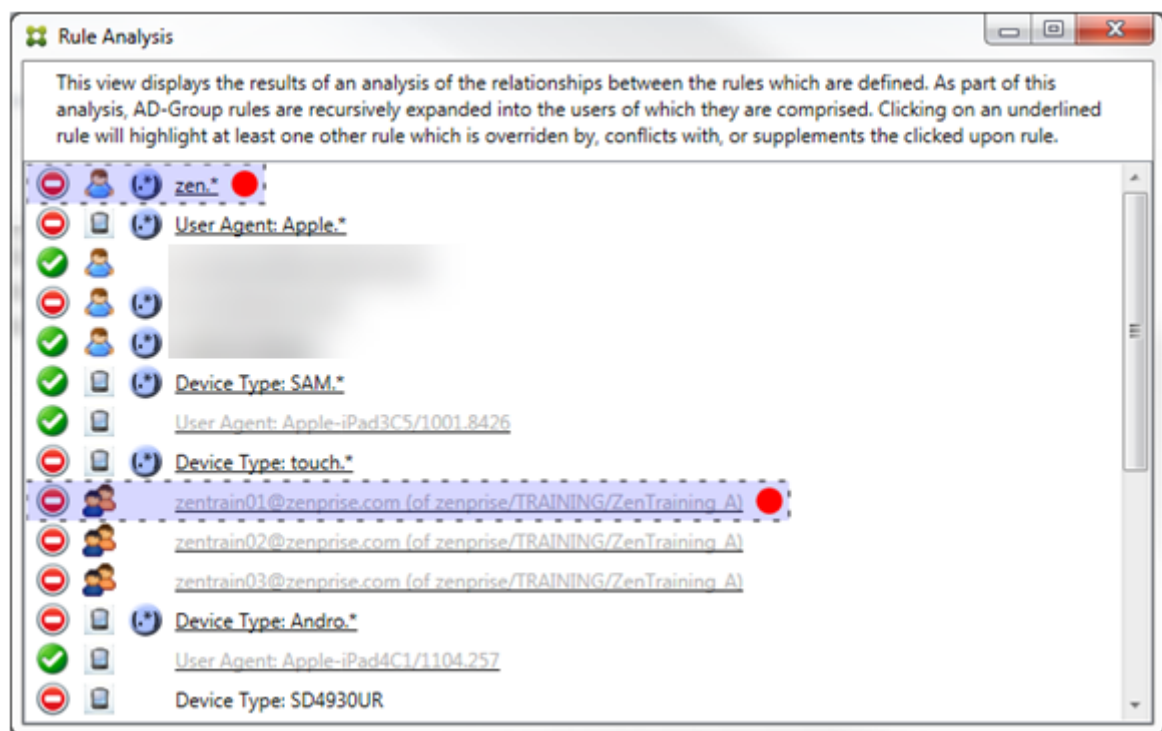
Ejemplo 1: En este ejemplo, se examina por qué zentrain01@zenprise.com se ha invalidado.



La regla primaria (regla del grupo AD [zenprise/TRAINING/ZenTraining B](#), donde zentrain01@zenprise.com es miembro) tiene las siguientes características:

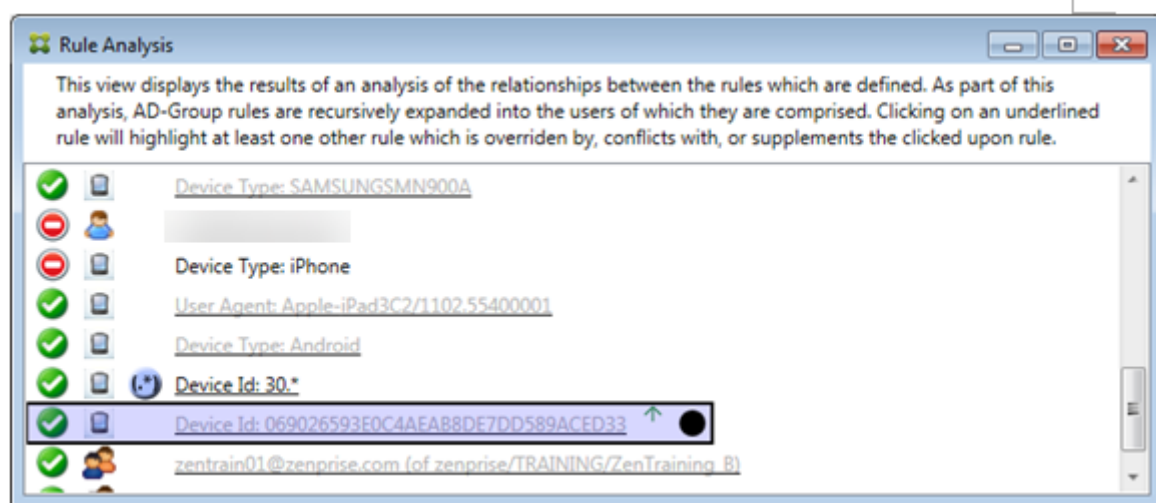
- Está resaltada en azul y tiene un borde sólido.
- Tiene una flecha verde que apunta hacia arriba (para indicar que las reglas auxiliares están todas encima de ella).
- Va seguida de un círculo rojo y uno negro para indicar, respectivamente, que una o más reglas están en conflicto con el acceso y que la regla primaria se ha invalidado y, por lo tanto, está inactiva.

Si se desplaza hacia arriba, verá lo siguiente:



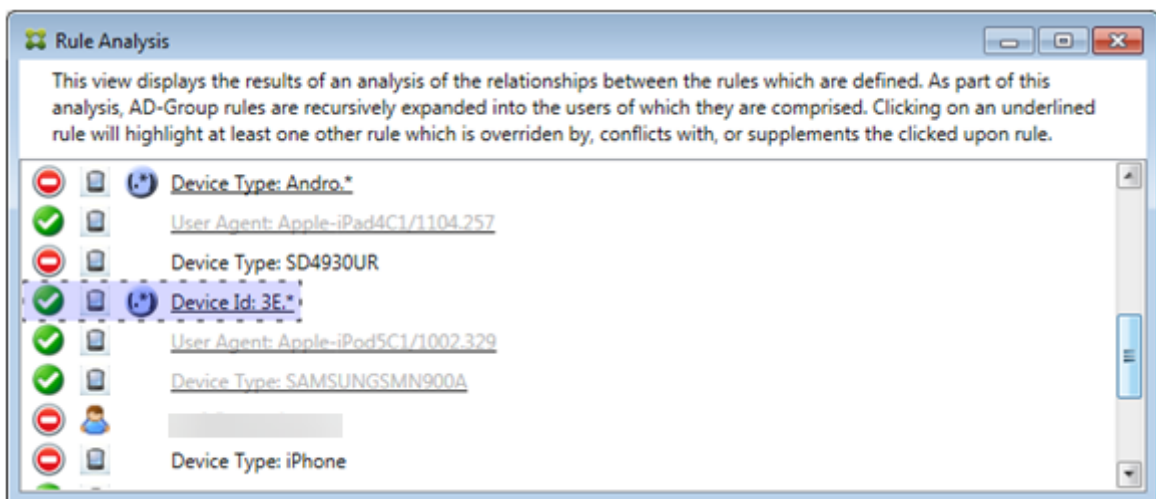
En este caso, hay dos reglas auxiliares que invalidan la regla primaria: la regla de expresión regular `zen.*` y la regla normal `zentrain01@zenprise.com` (de `zenprise/TRAINING/ZenTraining A`). En el caso de la última regla auxiliar, lo que ha ocurrido es que la regla del grupo de Active Directory `ZenTraining A` contiene el usuario `zentrain01@zenprise.com` y la regla del grupo de Active Directory `ZenTraining B` también contiene el usuario `zentrain01@zenprise.com`. La regla auxiliar, por tener una prioridad mayor, ha invalidado la regla primaria. El acceso de la regla primaria es Permitir y, como el acceso de ambas reglas auxiliares es Bloquear, todas van seguidas de un círculo rojo para indicar un conflicto de acceso.

Ejemplo 2: En este ejemplo, se muestra por qué se ha invalidado el dispositivo con el ID de dispositivo ActiveSync `069026593E0C4AEAB8DE7DD589ACED33`:



La regla primaria (regla normal de ID de dispositivo 069026593E0C4AEAB8DE7DD589ACED33) tiene las siguientes características:

- Está resaltada en azul y tiene un borde sólido.
- Tiene una flecha verde que apunta hacia arriba (para indicar que la regla auxiliar está encima de ella).
- Va seguida de un círculo negro para indicar que una regla auxiliar ha invalidado la primaria y, por lo tanto, está inactiva.

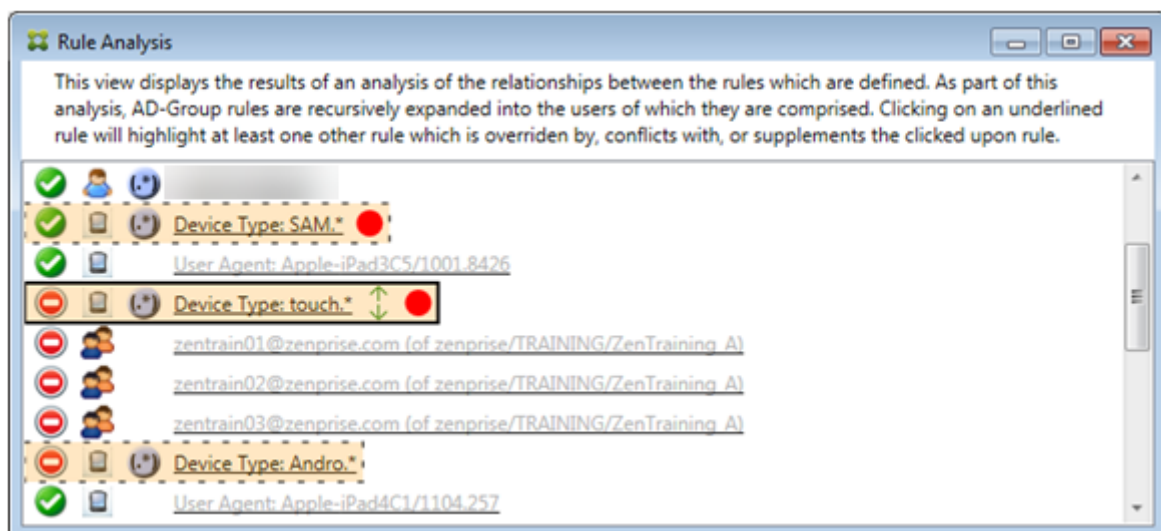


En este caso, una sola regla auxiliar invalida la regla primaria: la regla de expresión regular de ID de dispositivo ActiveSync es 3E . *. Como la expresión regular 3E . * se correspondería con 069026593E0C4AEAB8DE7DD589ACED33, la regla primaria no se cotejará nunca.

Cómo analizar una complementación y un conflicto

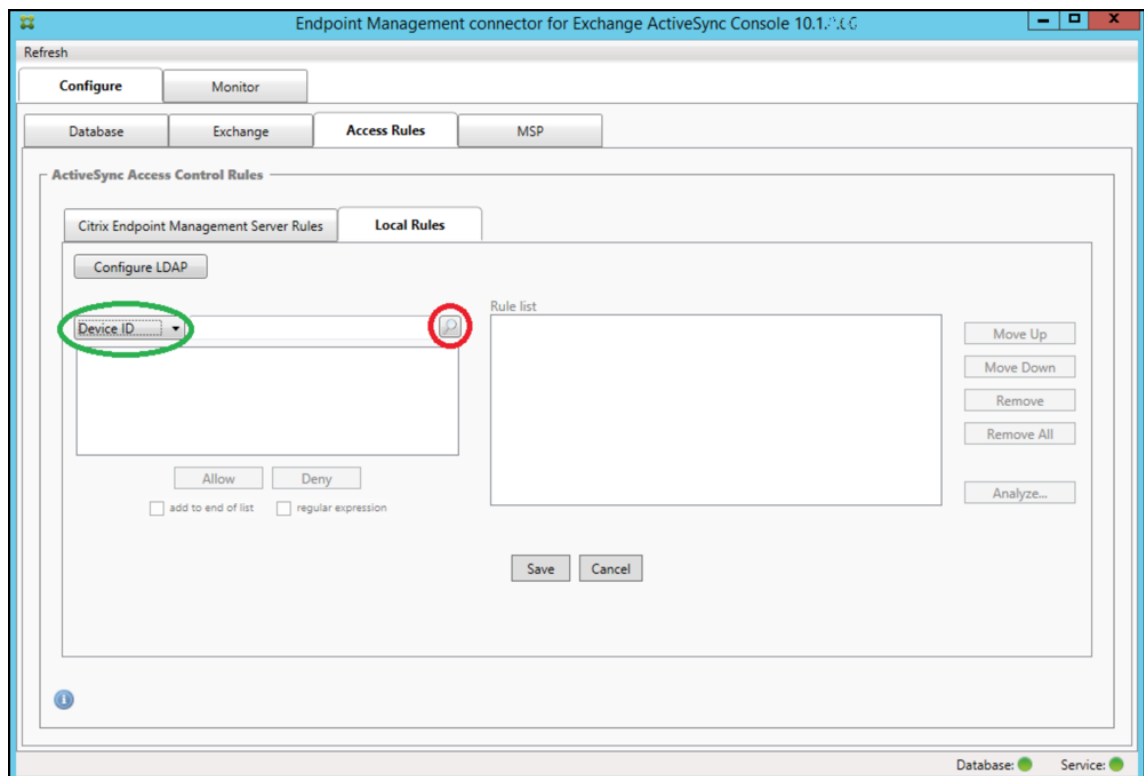
En este caso, la regla primaria es la regla en forma de expresión regular del tipo de dispositivo ActiveSync `touch.*`. Las características son las siguientes:

- Está indicada con un borde sólido y una capa amarilla a modo de advertencia de que hay más de una regla de expresión regular y solo un campo de regla concreto (en este caso: tipo de dispositivo ActiveSync).
- Una flecha que apunta hacia arriba y otra que apunta hacia abajo, 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 situado junto a ella indica que hay al menos una regla auxiliar con el acceso establecido en **Permitir**, lo que entra en conflicto con la regla primaria, cuyo acceso está **bloqueado**.
- Hay dos reglas auxiliares: la regla de expresión regular de tipo de dispositivo ActiveSync `SAM.*` y la regla de expresión regular de tipo de dispositivo ActiveSync `Andro.*`.
- Ambas reglas tienen bordes discontinuos para indicar que son auxiliares.
- Ambas reglas auxiliares tienen una capa amarilla para indicar que también se aplican al campo de regla de tipo de dispositivo ActiveSync.
- Debe comprobar, en estos casos, que las reglas de expresión regular no sean redundantes.

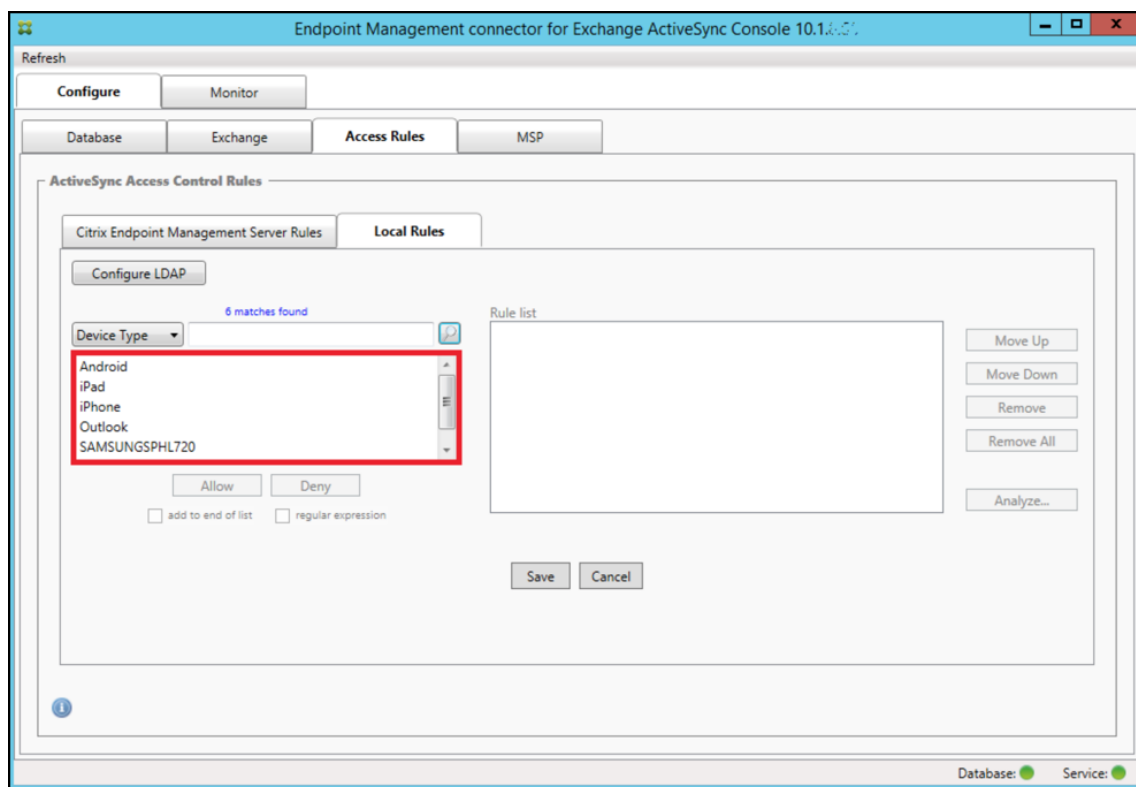


Cómo analizar las reglas al detalle

En este ejemplo, se describe cómo las relaciones entre reglas se dan siempre con respecto a la regla primaria. En el ejemplo anterior, se ha mostrado cómo un clic en la regla de expresión regular se aplicaba al campo de regla de tipo de dispositivo con el valor `touch.*`. Al hacer clic en la regla auxiliar `Andro.*`, se muestra un conjunto diferente de reglas auxiliares resaltadas.



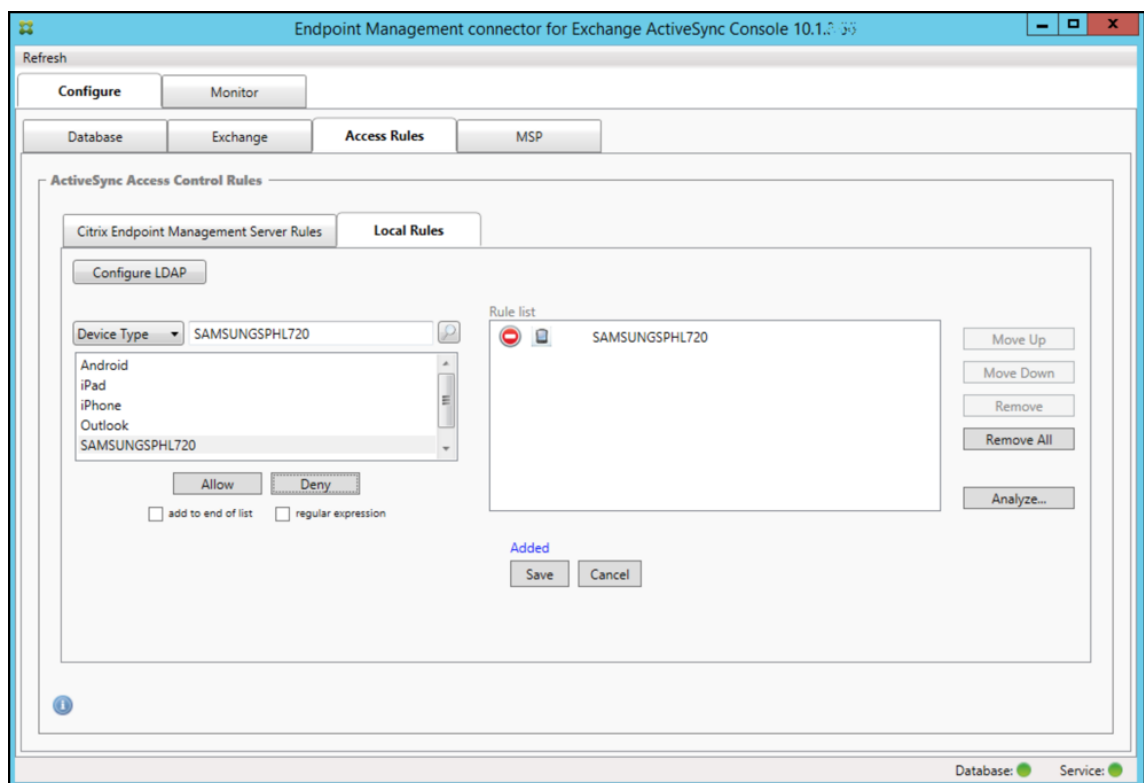
2. En la lista **Device ID**, seleccione el campo para el que quiere crear una regla local.
3. Haga clic en el icono de lupa para ver todas las correspondencias únicas con el campo seleccionado. En este ejemplo, se ha seleccionado el campo **Device Type**, y las opciones se muestran a continuación, en el cuadro de lista.



4. Haga clic en uno de los elementos de la lista de resultados y, a continuación, haga clic en una de las siguientes opciones:

- **Allow** significa que Exchange se configurará para permitir el tráfico de ActiveSync en todos los dispositivos que se correspondan.
- **Deny** significa que Exchange se configurará para denegar el tráfico de ActiveSync en todos los dispositivos que se correspondan.

En este ejemplo, se ha denegado el acceso a todos los dispositivos que tienen un tipo de dispositivo SamsungSPHL720.



Para agregar una expresión regular

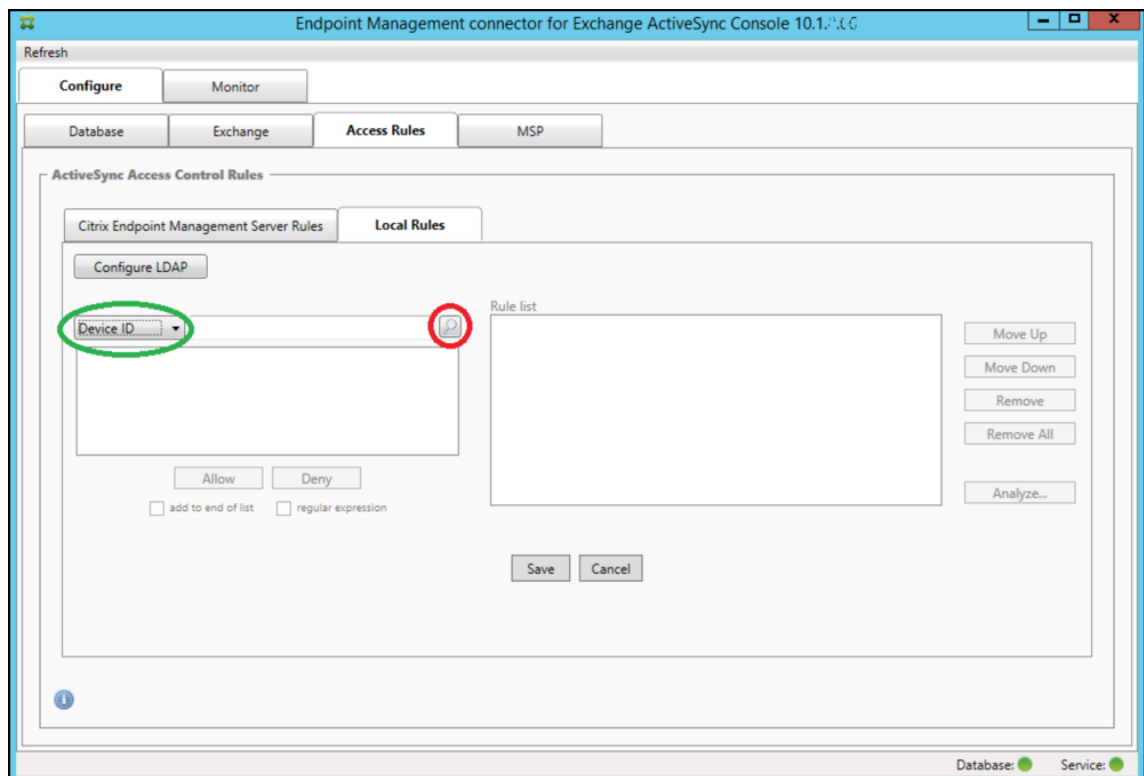
Las reglas locales de expresión regular se distinguen por el icono que aparece junto a ellas:



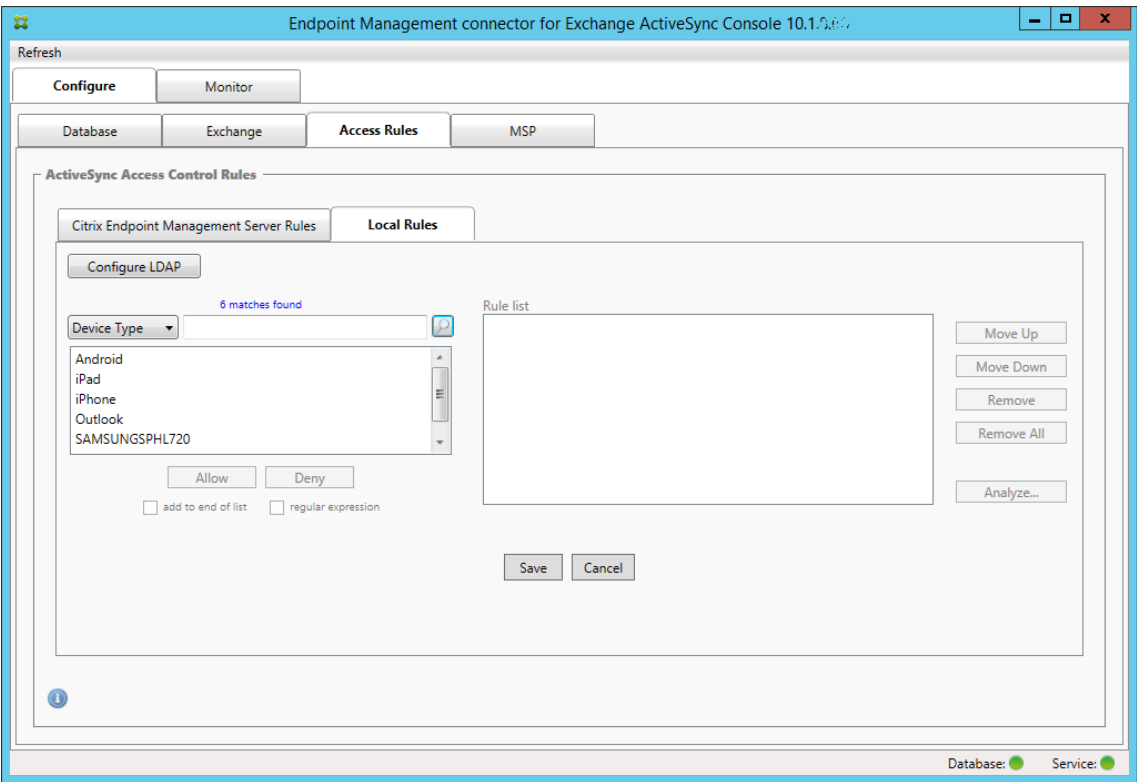
Para agregar una regla de expresión regular, puede crear una regla de expresión regular a partir de un valor existente de la lista de resultados de un campo determinado (siempre que se haya completado una instantánea principal), o bien puede, simplemente, escribir la expresión regular que quiera.

Para crear una expresión regular a partir de un valor de campo existente

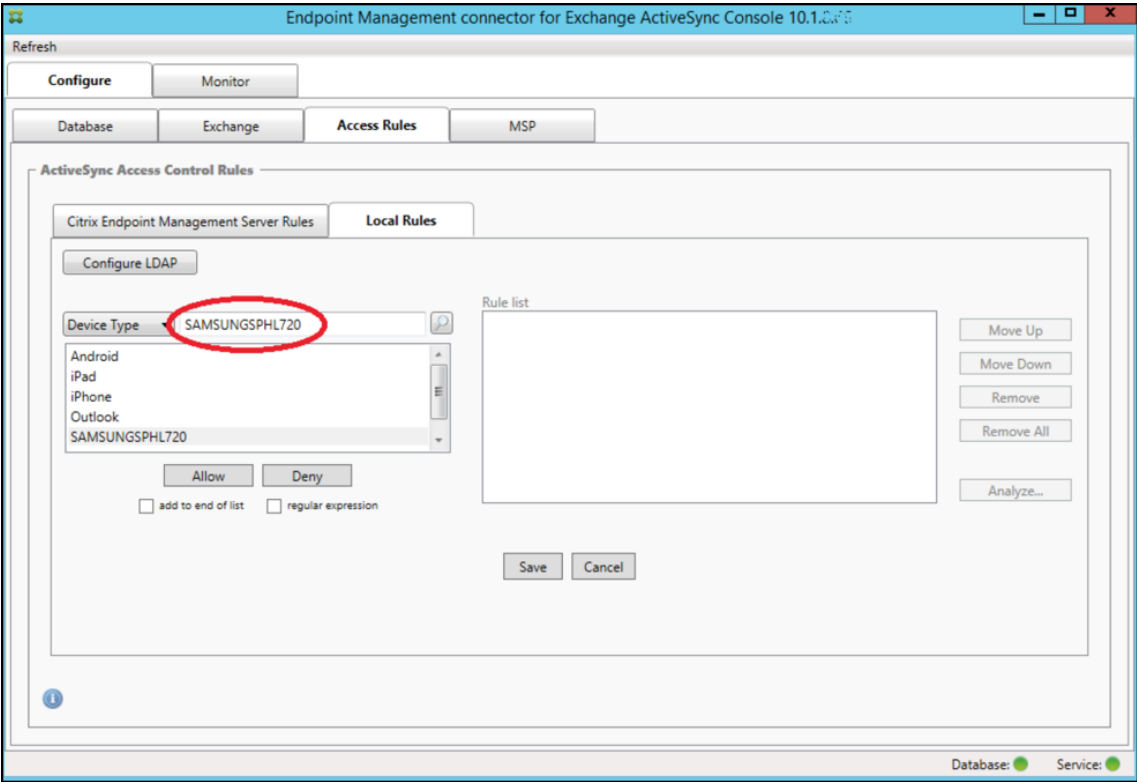
1. Haga clic en la ficha **Access Rules**.



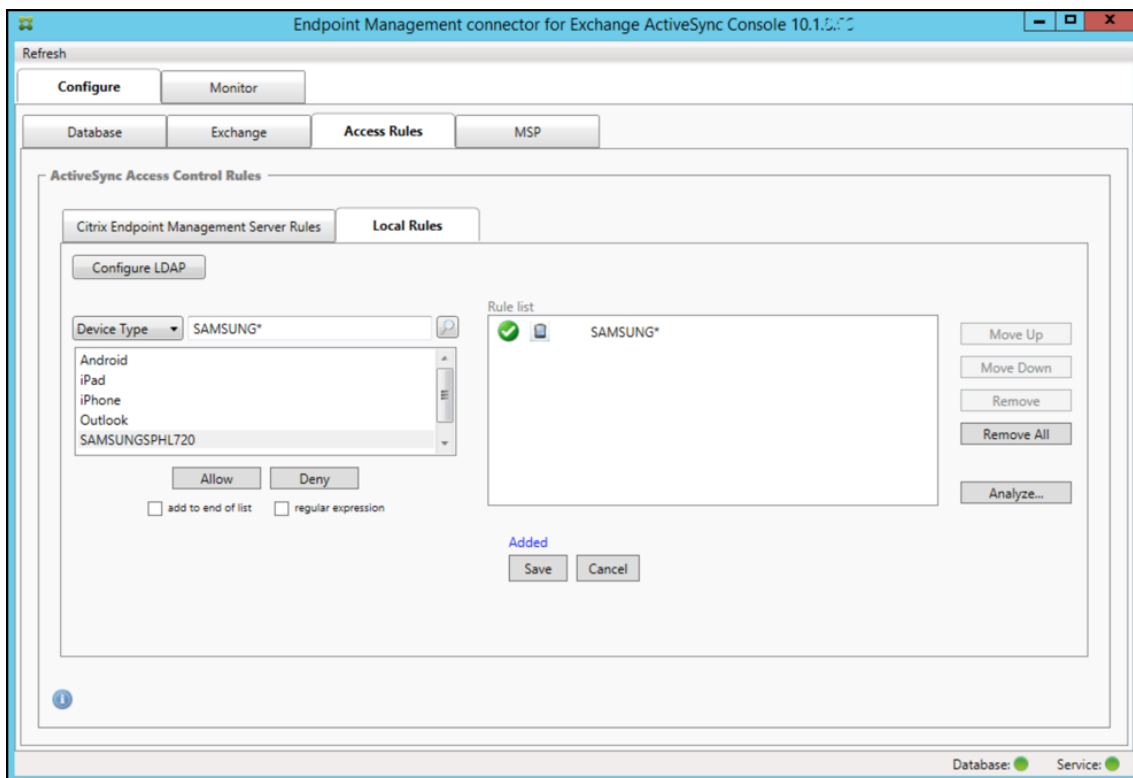
2. En la lista **Device ID**, seleccione el campo para el que quiere crear una regla local de expresión regular.
3. Haga clic en el icono de lupa para ver todas las correspondencias únicas con el campo seleccionado. En este ejemplo, se ha seleccionado el campo **Device Type**, y las opciones se muestran a continuación, en el cuadro de lista.



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 adyacente a **Device Type**.

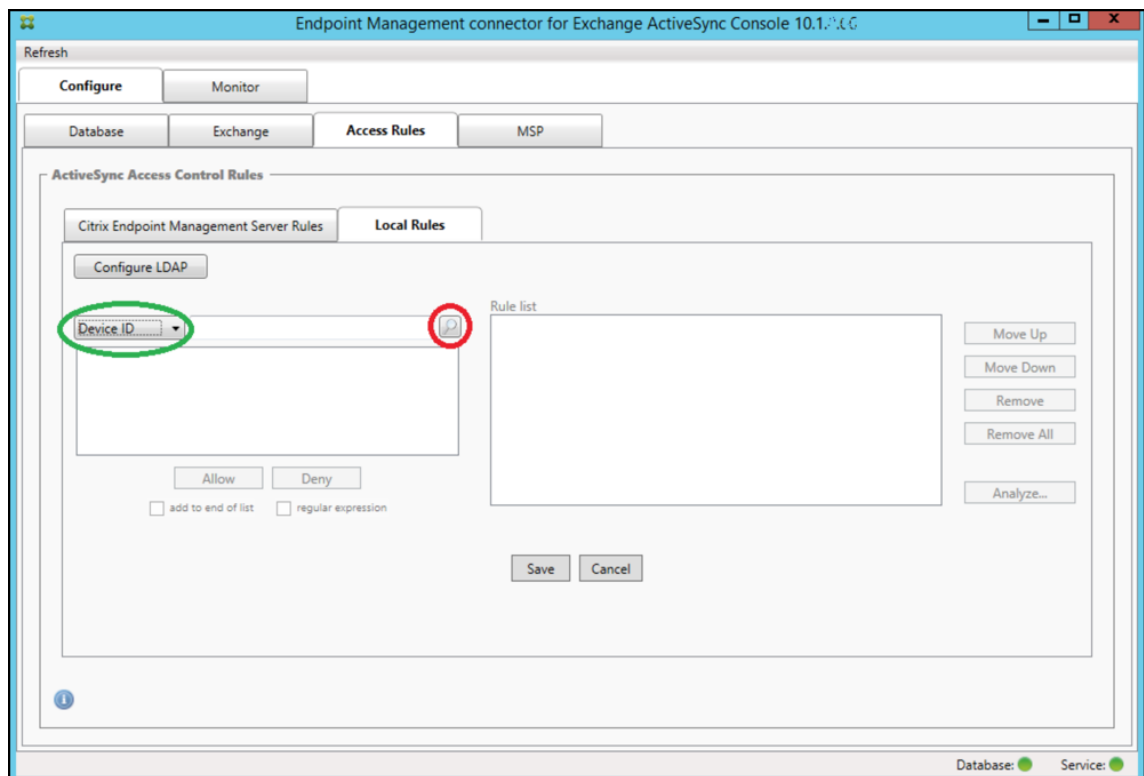


5. Para permitir el acceso a todos los tipos de dispositivos que contengan “Samsung” en su valor de tipo de dispositivo, siga estos pasos para agregar una regla de expresión regular:
 - a. Haga clic en el cuadro de texto del elemento seleccionado.
 - b. Cambie el texto de **SAMUNGSPHL720** a **SAMSUNG.***.
 - c. Compruebe que la casilla “regular expression” está marcada.
 - d. Haga clic en **Allow**.

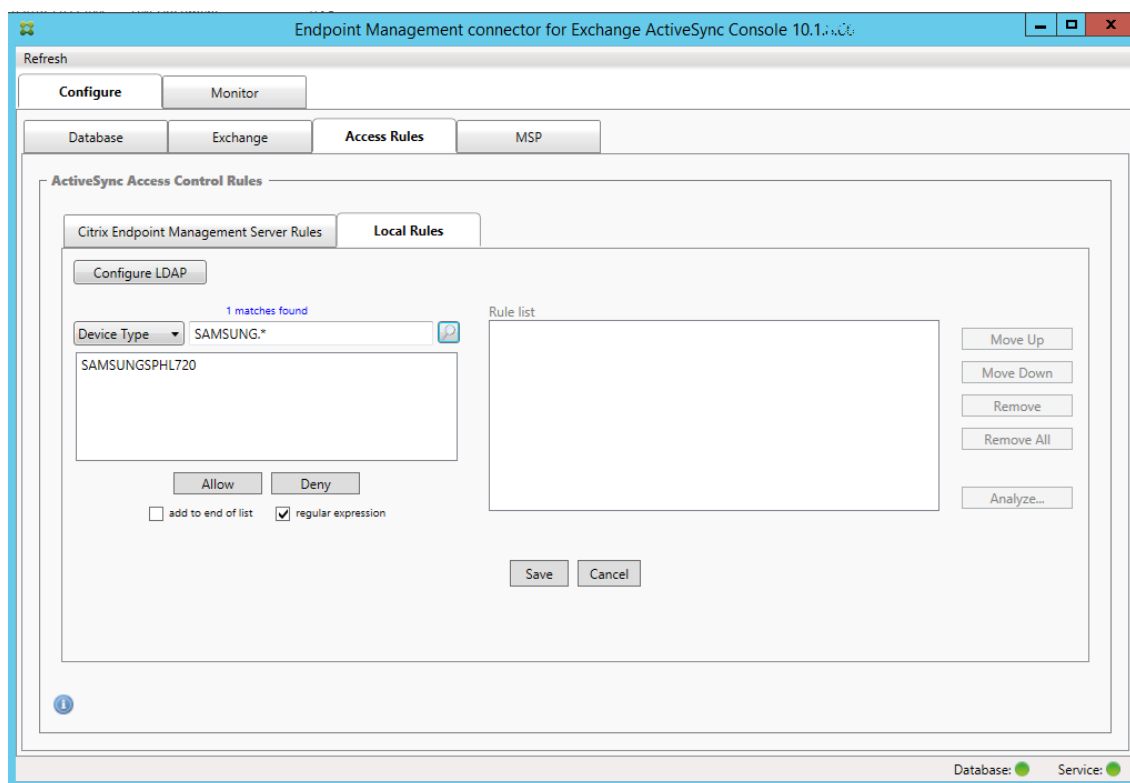


Para crear una regla de acceso

1. Haga clic en la ficha **Local Rules**.
2. Para escribir la expresión regular, deberá usar la lista Device ID y el cuadro de texto del elemento seleccionado.



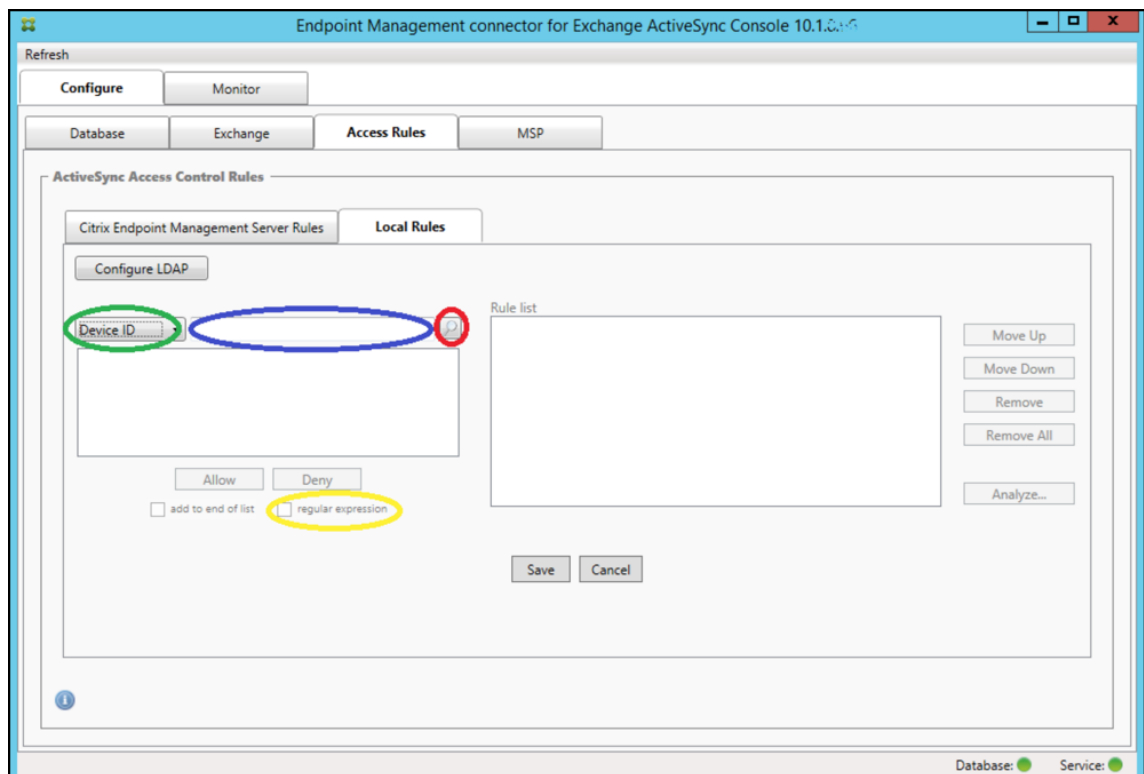
3. Seleccione el campo con el que corresponderse. En este ejemplo, se usa **Tipo de dispositivo**.
4. Escriba la expresión regular. En este ejemplo se usa `samsung.*`
5. Compruebe que la casilla “regular expression” está marcada y, a continuación, haga clic en **Allow** o **Deny**. En este ejemplo, se ha elegido **Allow**. El resultado final es el siguiente:



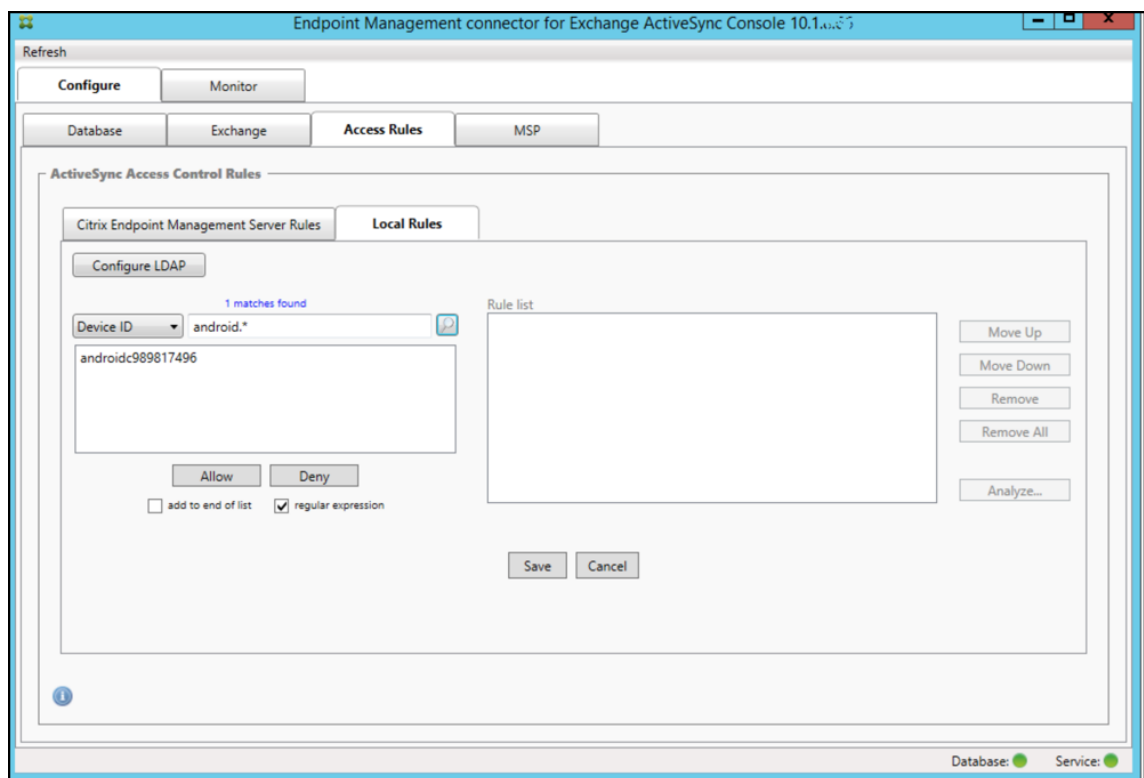
Para buscar dispositivos

Al marcar la casilla de expresión regular, puede realizar búsquedas de dispositivos específicos que se corresponden con la expresión indicada. Esta función solo está disponible si una instantánea principal se ha completado correctamente. Puede usar esta función incluso si no planea utilizar reglas de expresión regular. Por ejemplo, supongamos que quiere buscar todos los dispositivos que contienen el texto `workmail` en el ID de sus dispositivos ActiveSync. Para ello, siga este procedimiento.

1. Haga clic en la ficha **Access Rules**.
2. Compruebe que el selector del campo de correspondencia del dispositivo es Device ID (opción predeterminada).



3. Haga clic en el cuadro de texto del elemento seleccionado (como se muestra en azul en la imagen anterior) y escriba `workmail.*`.
4. Compruebe que la casilla “regular expression” está marcada y, a continuación, haga clic en el icono de lupa para ver los resultados, tal y como se muestra en la siguiente imagen.

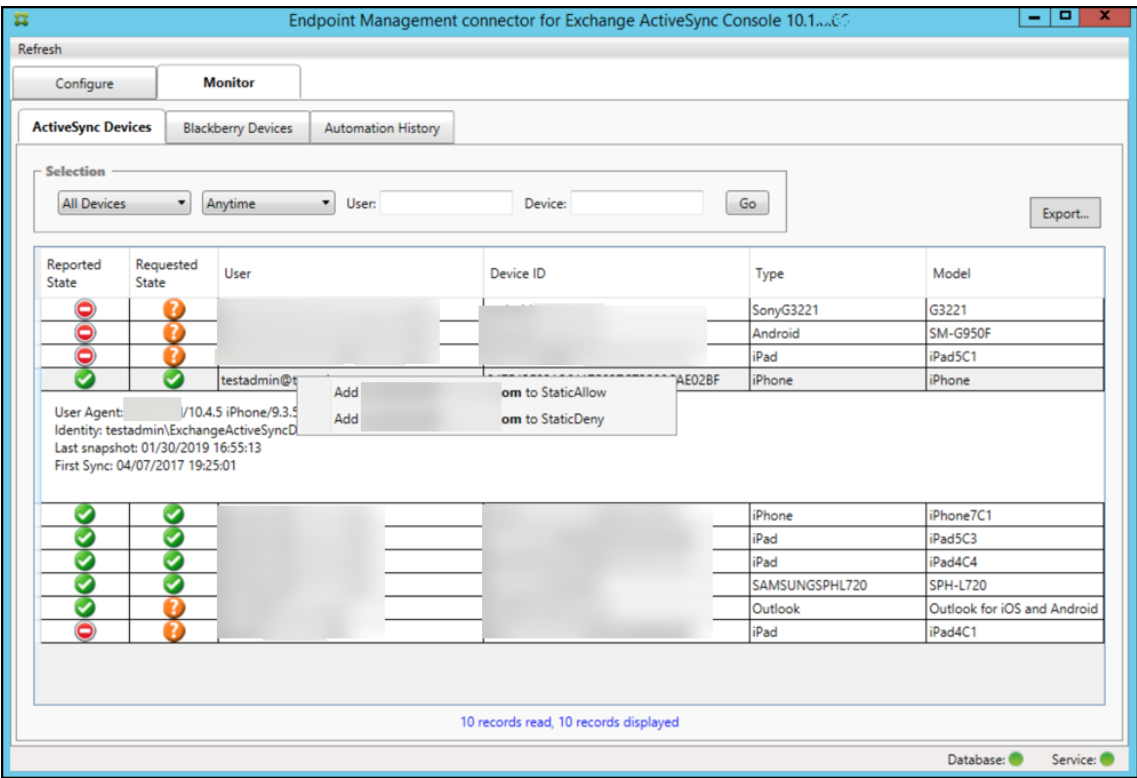


Para agregar un usuario individual, un dispositivo o un tipo de dispositivo a una regla

Puede agregar reglas estáticas basadas en el usuario, el ID de dispositivo o el tipo de dispositivo en la ficha ActiveSync Devices.

1. Haga clic en la ficha **ActiveSync Devices**.
2. En la lista, haga clic con el botón secundario en un usuario, un dispositivo o un tipo de dispositivo, y seleccione si permitir o denegar la selección.

En la imagen siguiente, se muestra la opción de permitir o denegar cuando el usuario1 está seleccionado.



Supervisión de dispositivos

En el conector de Citrix Endpoint Management para Exchange ActiveSync, la ficha **Monitor** permite explorar los dispositivos Exchange ActiveSync y BlackBerry que se hayan detectado y el historial de los comandos de PowerShell automatizados que se hayan emitido. La ficha **Monitor** contiene a su vez las siguientes tres fichas:

- **ActiveSync Devices:**
 - Para exportar las asociaciones de dispositivo ActiveSync mostradas, haga clic en el botón **Export**.
 - Para agregar reglas locales (estáticas), haga clic con el botón secundario en las columnas **User**, **Device ID** o **Type** y seleccione el tipo de regla apropiado, ya sea permitir o bloquear.
 - Para contraer una fila expandida, presione Ctrl y haga clic en la fila expandida.
- **BlackBerry Devices**
- **Automation History**

En la ficha **Configure** se muestra el historial de todas las instantáneas. La información que muestra el historial de instantáneas es: cuándo se realizó la instantánea, cuánto tiempo duró el proceso, cuántos dispositivos se detectaron y los errores que se produjeran.

- En la ficha **Exchange**, haga clic en el icono de información del servidor de Exchange pertinente.

Solución de problemas y diagnósticos

El conector de Citrix Endpoint Management para Exchange ActiveSync registra errores y demás información operativa en el archivo de registro: *Carpeta de instalación\log\XmmWindowsService.log*. El conector para Exchange ActiveSync también registra los eventos significativos en el registro de eventos de Windows.

Para cambiar el nivel de registro

El conector de Citrix Endpoint Management para Exchange ActiveSync ofrece estos niveles de registro: error, información, advertencia, depuración y seguimiento.

Nota:

Cada nivel sucesivo genera más detalles (más datos). Por ejemplo, el nivel Error ofrece el menor detalle, mientras que el nivel de seguimiento proporciona el mayor detalle.

Para cambiar el nivel de registro, lleve a cabo lo siguiente:

1. En `C:\Program Files\Citrix\Citrix` Citrix Endpoint Management connector, abra el archivo `nlog.config`.
2. En la sección `<rules>`, cambie el parámetro `minilevel` al nivel de registro que prefiera. Por ejemplo:

```
1      <rules >
2
3      <logger name="*" writeTo="file" minlevel="Debug" />
4
5      </rules>
6  <!--NeedCopy-->
```

3. Guarde el archivo.

Los cambios surten efecto de inmediato. No es necesario reiniciar el conector para Exchange ActiveSync.

Errores comunes

En la lista siguiente, se incluyen errores frecuentes:

- El servicio del conector para Exchange ActiveSync no se inicia

Compruebe si se han registrado errores en el archivo de registro y el registro de eventos de Windows. Las causas habituales son las siguientes:

- El servicio del conector para 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 servicio del conector para Exchange ActiveSync debe tener permitido el inicio de sesión en SQL. La cuenta del servicio del conector para Exchange ActiveSync es, de forma predeterminada, el sistema local, pero se puede cambiar a una cuenta que tenga privilegios de administrador local. Si se configura la autenticación de SQL, el inicio de sesión de SQL debe estar correctamente configurado en SQL.

Herramientas para solucionar problemas

En la carpeta Support\PowerShell, dispone de un conjunto de utilidades de PowerShell para la solución de problemas.

Una herramienta de solución de problemas realiza un análisis exhaustivo de los dispositivos y los buzones de correo de los usuarios para detectar condiciones de error y problemas potenciales, además de un detallado análisis de RBAC de los usuarios. Puede guardar sin formato los resultados de todos los cmdlets en un archivo de texto.

Conector de NetScaler Gateway para Exchange ActiveSync

March 1, 2024

Ahora XenMobile NetScaler Connector es el conector de NetScaler Gateway para Exchange ActiveSync. Para obtener más detalles sobre los productos unificados de Citrix, consulte la [guía de productos de Citrix](#).

El conector para ActiveSync ofrece un servicio de autorización a NetScaler Gateway en el nivel de dispositivos de los clientes ActiveSync, por lo que actúa como proxy inverso para el protocolo de Exchange ActiveSync. Puede controlar 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 obtener un diagrama detallado con una arquitectura como referencia, consulte [Arquitectura](#).

La versión actual del conector de NetScaler Gateway para Exchange ActiveSync es 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) > Software de producto > XenMobile Server 10 > Componentes de servidor**.
3. En el icono **NetScaler Gateway Connector**, haga clic en **Descargar archivo**.

To install the connector, see [Installing the NetScaler Gateway connector for Exchange ActiveSync](#)).

Importante:

A partir de octubre de 2022, los conectores de Citrix Endpoint Management y NetScaler Gateway para Exchange ActiveSync ya no admitirán Exchange Online debido a los cambios de autenticación anunciados por Microsoft [aquí](#). El conector de Citrix Endpoint Management para Exchange seguirá funcionando con Microsoft Exchange Server (local).

Novedades en la versión 8.5.3

- Esta versión funciona con los protocolos ActiveSync 16.0 y 16.1.
- Se han agregado más detalles a los análisis enviados a Google Analytics, especialmente en lo que respecta a las instantáneas. [CXM-52261]

Novedades en versiones anteriores

Nota:

En la siguiente sección de novedades, se hace referencia al conector de NetScaler Gateway para Exchange ActiveSync por su nombre anterior, XenMobile NetScaler Connector. El nombre cambió a partir de la versión 8.5.2.

Novedades en la versión 8.5.2

- Ahora XenMobile NetScaler Connector es el conector de NetScaler Gateway para Exchange ActiveSync.

Se han solucionado los problemas siguientes en esta versión:

- Si se usa más de un criterio para definir una regla de directiva y un criterio tiene que ver con el ID del usuario, puede dar el problema siguiente: si un usuario tiene más de un alias, los alias no se verifican al aplicar la regla. [CXM-55355]

Novedades en 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:** Nos gustaría saber cómo usa el Connector para centrarnos en dónde mejorar el producto.
- **Disponibilidad de TLS 1.1 y 1.2:** Debido a la poca seguridad que ofrecen, PCI Council va a retirar TLS 1.0 y TLS 1.1. TLS 1.2 ya está disponible en XenMobile NetScaler Connector.

Supervisar el conector de NetScaler Gateway para Exchange ActiveSync

La utilidad de configuración del conector de NetScaler Gateway para Exchange ActiveSync ofrece un registro detallado. Utilice los registros para ver todo el tráfico que pasa a través de Exchange Server que Secure Mobile Gateway permite o bloquea.

Use la ficha **Log** para ver el historial de las solicitudes de ActiveSync que se han reenviado al conector de Exchange ActiveSync para la autorización.

Además, para comprobar que el servicio web del conector para Exchange ActiveSync se está ejecutando, cargue la siguiente URL en un explorador web presente en el servidor del conector <https://<host:port>/services/ActiveSync/Version>. Si la dirección URL devuelve la versión de producto como una cadena, el servicio web funciona.

Para simular el tráfico de ActiveSync con el conector para Exchange ActiveSync

Puede utilizar el conector de NetScaler Gateway para Exchange ActiveSync para hacer una simulación del tráfico de ActiveSync con las directivas. En la herramienta de configuración del conector, haga clic en la ficha **Simulator**. Los resultados muestran la manera en que se aplicarán las directivas en función de las reglas que haya configurado.

Seleccionar filtros del conector para Exchange ActiveSync

Los filtros del conector de NetScaler Gateway para Exchange ActiveSync analizan un dispositivo para detectar la infracción de una directiva o un parámetro de propiedad concretos. Si el dispositivo cumple los criterios, se coloca en Device List. Esta lista de dispositivos, Device List, no es una lista de dispositivos permitidos ni bloqueados. Es una lista de los 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 aquellos dispositivos inscritos en Citrix Endpoint Management 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 basándose en la lista de dispositivos definida por las listas de aplicaciones bloqueadas en las directivas y la presencia de esas aplicaciones en esas listas.
- **Permitir / Denegar implícitamente:** Crea una lista de todos los dispositivos que no cumplen ninguno de los demás criterios de regla o filtro, y permite o deniega en función de esa lista. La opción “Permitir / Denegar implícitamente” garantiza que se habilite el estado del conector para Exchange ActiveSync en la ficha “Dispositivos”, y muestra el estado del conector para los dispositivos. La opción “Permitir / Denegar implícitamente” también controla todos los demás filtros que no se han seleccionado. Por ejemplo, el conector rechaza aquellas aplicaciones que estén presentes en la lista de aplicaciones bloqueadas. Sin embargo, el conector permite todos los demás filtros, porque la opción “Permitir / Denegar implícitamente” está establecida en **Permitir**.
- **Dispositivos inactivos:** Crea una lista de los dispositivos que no se han comunicado con Citrix Endpoint Management durante tiempo específico. Estos dispositivos se consideran inactivos. El filtro permite o niega esos dispositivos basándose en este filtro.
- **Aplicaciones obligatorias que faltan:** Cuando un usuario se inscribe, el usuario recibe una lista de las aplicaciones obligatorias que debe instalarse. El filtro “Aplicaciones obligatorias que faltan” indica que una o varias de esas 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 instalar. El filtro “Aplicaciones no sugeridas” examina el contenido del dispositivo en busca de las aplicaciones que no están en esa lista.
- **Contraseña no conforme:** Crea una lista de todos los dispositivos que no tienen código de acceso en el dispositivo.
- **Dispositivos no conformes:** Permite o deniega los dispositivos que cumplen los criterios propios del departamento interno de TI. La conformidad es un valor arbitrario definido por la propiedad de dispositivo denominada “No conforme”, un marcador booleano que puede ser **true** o **false**. (Puede crear esta propiedad manualmente y establecer el valor. O bien, puede utilizar acciones automatizadas para crear esta propiedad en un dispositivo, en función de si el dispositivo cumple criterios específicos.)
 - **No conforme = True:** Si el dispositivo no cumple los estándares de cumplimiento ni las definiciones de directivas establecidas por el departamento de TI, el dispositivo no cumple los requisitos.
 - **No conforme = False:** Si el dispositivo cumple los estándares de cumplimiento y las definiciones de directivas establecidas por el departamento de TI, se indica que el dispositivo

es conforme.

- **Estado revocado:** Crea una lista de todos los dispositivos y permite o prohíbe dispositivos según el estado de revocación.
- **Dispositivos Android o iOS liberados por jailbreak o root:** Crea una lista de todos los dispositivos marcados como liberados por rooting y permite o deniega el acceso en función de ese estado.
- **Dispositivos no administrados:** Crea una lista de todos los dispositivos de la base de datos de Citrix Endpoint Management. Implemente Mobile Application Gateway en un modo de bloqueo.

Para configurar una conexión con el conector de NetScaler Gateway para Exchange ActiveSync

El conector de NetScaler Gateway para Exchange ActiveSync se comunica con Citrix Endpoint Management y otros proveedores remotos de configuración a través de servicios Citrix Secure Web.

1. En la herramienta de configuración del conector para Exchange ActiveSync, haga clic en la ficha **Config Providers** y, a continuación, haga clic en **Add**.
2. En el cuadro de diálogo **Config Providers**, en **Name**, escriba un nombre de usuario que tenga privilegios de administrador. Este usuario se utilizará para la autorización HTTP básica en el servidor de Citrix Endpoint Management.
3. En **Url**, introduzca la dirección web del servicio GCS de Citrix Endpoint Management. Por norma general, en el formato: `https://<FQDN>/<instanceName>/services/<MagConfigService>`. En el nombre *MagConfigService* se distinguen mayúsculas de minúsculas.
4. En **Password**, introduzca la contraseña que se usará para la autorización básica de HTTP en el servidor de Citrix Endpoint Management.
5. En **Managing Host**, escriba el conector para el nombre del servidor de Exchange ActiveSync.
6. En **Baseline Interval**, especifique un período de tiempo para indicar cuándo se debe extraer, desde Citrix Endpoint Management, un conjunto de reglas dinámicas actualizadas.
7. En **Delta interval**, especifique un período de tiempo para la extracción de una actualización de reglas dinámicas.
8. En **Request Timeout**, especifique el intervalo de tiempo de espera para solicitudes del servidor.
9. En **Config Provider**, seleccione si la instancia de servidor del proveedor de configuración proporciona la configuración de directivas.
10. En **Events Enabled**, habilite esta opción si quiere que el conector para Exchange ActiveSync notifique a Citrix Endpoint Management cuando un dispositivo se bloquee. Se requiere esta opción si se utilizan reglas del conector en alguna de las acciones automatizadas de Citrix Endpoint Management.
11. Haga clic en **Save** y, a continuación, haga clic en **Test Connectivity** para probar la conectividad entre la puerta de enlace y el proveedor de configuración. Si se produce un error de conexión,

compruebe que la configuración del firewall local permite la conexión o póngase en contacto con el administrador.

12. Si la conexión se realiza correctamente, desmarque la casilla **Disabled** y, a continuación, haga clic en **Save**.

Al agregar un proveedor de configuraciones, el conector para Exchange ActiveSync crea automáticamente una o más directivas asociadas a ese proveedor. Una definición de plantilla contenida `config\policyTemplates.xml` de la sección `NewPolicyTemplate` define las directivas. Se crea una nueva directiva por cada elemento de Policy definido en esta sección.

El operador puede agregar, quitar o modificar los elementos de directiva si el elemento de Policy corresponde con la definición de esquema y las cadenas de sustitución estándar (entre llaves) no se modifican. Luego, agregue nuevos grupos para el proveedor y actualice la directiva para incluir los nuevos grupos.

Para importar una directiva desde Citrix Endpoint Management

1. En la herramienta de configuración del conector para Exchange ActiveSync, haga clic en la ficha **Config Providers** y, a continuación, haga clic en **Add**.
2. En el cuadro de diálogo **Config Providers**, en **Name**, escriba un nombre de usuario para la autorización HTTP básica en Citrix Endpoint Management. El usuario debe tener privilegios administrativos.
3. En **Url**, introduzca la dirección web del servicio Gateway Configuration Service de Citrix Endpoint Management. Por norma general, en el formato: `https://<xdmHost>/xdm/services/<MagConfigService>`. En el nombre `MagConfigService` se distinguen mayúsculas de minúsculas.
4. En **Password**, introduzca la contraseña que se usará para la autorización básica de HTTP en 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 se produce un error de conexión, compruebe que la configuración del firewall local permite la conexión o póngase en contacto con el administrador.
6. Cuando la conexión se realice correctamente, desmarque la casilla **Disabled** y, a continuación, haga clic en **Save**.
7. En **Managing Host**, deje el nombre DNS predeterminado del equipo host local. Este parámetro se utiliza para coordinar la comunicación con Citrix Endpoint Management cuando hay varios servidores de Forefront Threat Management Gateway (TMG) configurados en una matriz.

Después de guardar la configuración, abra GCS.

Configurar el modo de directiva en el conector de NetScaler Gateway para Exchange ActiveSync

El conector de NetScaler Gateway para Exchange ActiveSync se puede ejecutar en los seis modos siguientes:

- **Allow All:** Este modo de directiva concede acceso a todo el tráfico que pasa por el conector para Exchange ActiveSync. No se utiliza ninguna otra regla de filtrado.
- **Deny All:** Este modo de directiva bloquea el acceso a todo el tráfico que pasa por el conector para Exchange ActiveSync. No se utiliza ninguna otra regla de filtrado.
- **Static Rules: Block Mode:** Este modo de directiva ejecuta reglas estáticas con la instrucción implícita de denegación o bloqueo al final. El conector para Exchange ActiveSync bloquea aquellos dispositivos que otras reglas de filtrado no permitan.
- **Static Rules: Permit Mode:** Este modo de directiva ejecuta reglas estáticas con la instrucción implícita de permiso al final. El conector para Exchange ActiveSync permite aquellos dispositivos que otras reglas de filtrado no bloqueen o denieguen.
- **Static + ZDM Rules: Block Mode** (Modo de bloqueo). Este modo de directiva ejecuta primero las reglas estáticas, seguidas de las reglas dinámicas de Citrix Endpoint Management con una instrucción implícita de denegar o bloquear al final. Los dispositivos se permiten o deniegan según los filtros definidos y las reglas de Citrix Endpoint Management. Los dispositivos que no coincidan con las reglas y los filtros definidos se bloquean.
- **Static + ZDM Rules: Permit Mode** (Modo de permiso). Este modo de directiva ejecuta primero las reglas estáticas, luego las reglas dinámicas de Citrix Endpoint Management con una instrucción implícita de permitir al final. Los dispositivos se permiten o deniegan según los filtros definidos y las reglas de Citrix Endpoint Management. Los dispositivos que no coincidan con las reglas y los filtros definidos se permiten.

El proceso del conector para Exchange ActiveSync permite o bloquea reglas dinámicas en función de identificadores únicos de ActiveSync para dispositivos iOS y dispositivos móviles de Windows recibidos desde Citrix Endpoint Management. El comportamiento de los dispositivos Android difiere según el fabricante y algunos no exponen con facilidad un ID único de ActiveSync. Para compensar, Citrix Endpoint Management envía información acerca del ID del usuario de los dispositivos Android para la decisión de permitir o bloquear. Como resultado, si un usuario tiene un solo dispositivo Android, las acciones de permitir y bloquear funcionan de la manera habitual. En cambio, si el usuario dispone de varios dispositivos Android, se permiten todos los dispositivos porque los dispositivos Android no se pueden diferenciar. Puede configurar la puerta de enlace para bloquear estáticamente esos dispositivos en función de su ActiveSyncID, si este se conoce. Esta puerta también se puede configurar para bloquear según el tipo de dispositivo o el agente de usuario.

Para especificar el modo de directiva, en la herramienta de configuración del controlador SMG, realice lo siguiente:

1. Haga clic en la ficha **Path Filters** y, a continuación, haga clic en **Add**.
2. En el cuadro de diálogo **Path Properties**, seleccione un modo de directiva de la lista **Policy** y, a continuación, haga clic en **Save**.

Puede revisar las reglas en la ficha **Policies** de la herramienta de configuración. Las reglas se procesan en el conector para Exchange ActiveSync de arriba a abajo. Las directivas permitidas (Allow) se muestran con una marca de verificación verde. Las directivas denegadas (Deny) se muestran con un círculo rojo atravesado por una línea. Para actualizar la pantalla y ver las reglas actualizadas, 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 de los campos. Puede obtener los valores de los registros. Aparecerá un mensaje de resultados con la especificación Allow o Block.

Para configurar reglas estáticas

Introduzca reglas estáticas con valores que lean los filtros ISAPI de las solicitudes HTTP de conexión ActiveSync. Con las reglas estáticas, el conector para Exchange ActiveSync puede permitir o bloquear el tráfico mediante los criterios siguientes:

- **User:** El conector para Exchange ActiveSync usa la estructura del nombre y el valor del usuario autorizado capturado durante la inscripción del dispositivo. Generalmente, esa estructura se encuentra como `domain\username`, como consta en el servidor que ejecuta Citrix Endpoint Management conectado a Active Directory a través de LDAP. La ficha **Log** de la herramienta de configuración del conector mostrará los valores que pasan a través de este. Los valores se pasan si el conector debe determinar la estructura de valores o si la estructura difiere.
- **DeviceID (ActiveSyncID):** También conocido como ActiveSyncID del dispositivo conectado. Este valor se suele encontrar en la página de propiedades del dispositivo específico, en la consola de Citrix Endpoint Management. Este valor también se puede consultar desde la ficha **Log**, en la herramienta de configuración del conector para Exchange ActiveSync.
- **DeviceType:** El conector para Exchange ActiveSync puede determinar si el dispositivo es un iPhone, un iPad o cualquier otro tipo de dispositivo; puede permitirlos o bloquearlos en función de esos criterios. En cuanto a otros valores, la herramienta de configuración del conector puede revelar todos los tipos de dispositivos conectados que se están procesando para la conexión ActiveSync.
- **UserAgent:** Contiene información sobre el cliente de ActiveSync que se utiliza. Normalmente, el valor especificado corresponde a una versión y compilación determinadas de sistema operativo para la plataforma del dispositivo móvil.

La herramienta de configuración del conector para Exchange ActiveSync que se ejecuta en el servidor siempre administra las reglas estáticas.

1. En la herramienta de configuración del controlador SMG, haga clic en la ficha **Static Rules** y, a continuación, haga clic en **Add**.
2. En el cuadro de diálogo **Static Rule Properties**, especifique los valores a usar como criterios. Por ejemplo, puede indicar un usuario al que permitir el acceso si escribe el nombre del usuario (por ejemplo, AllowedUser) y si, a continuación, desmarca la casilla **Disabled**.
3. Haga clic en **Guardar**.

La regla estática está ahora activada. También puede usar expresiones regulares para definir los valores, pero debe habilitar el modo de procesamiento de reglas en el archivo config.xml.

Para configurar reglas dinámicas En Citrix Endpoint Management, las directivas y las propiedades de dispositivo definen las reglas dinámicas y pueden desencadenar un filtro dinámico para el conector para Exchange ActiveSync. La activación ocurre en caso de infracción de una directiva o un parámetro de propiedad. Los filtros del conector para Exchange ActiveSync analizan un dispositivo para detectar la infracción de una directiva concreta o un parámetro de propiedad. Si el dispositivo cumple los criterios, se coloca en Device List. Esta lista Device List no es una lista de dispositivos permitidos ni bloqueados. Es una lista de los dispositivos que cumplen los criterios definidos. Con las siguientes opciones de configuración, puede definir si quiere permitir o denegar los dispositivos de Device List mediante el conector para Exchange ActiveSync.

Nota:

Use la consola de Citrix Endpoint Management para configurar las reglas dinámicas.

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En **Servidor**, haga clic en **ActiveSync Gateway**. Aparecerá la página ActiveSync Gateway.
3. En **Activar las reglas siguientes**, seleccione las reglas que quiera activar.
4. En “Solo Android”, haga clic en **Sí** en **Enviar usuarios de dominio Android a ActiveSync Gateway** para que Citrix Endpoint Management envíe información de dispositivos 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 ActiveSync para el usuario del dispositivo.

Para configurar directivas personalizadas con la edición del archivo XML del conector para Exchange ActiveSync En la herramienta de configuración del conector para Exchange ActiveSync, puede ver las directivas básicas en la configuración predeterminada de la ficha **Políticas**. Si quiere

crear directivas personalizadas, puede modificar 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 (por ejemplo, otro grupo estático un grupo para admitir otro proveedor GCP), agregue el nuevo elemento **Group** a la sección **GroupList**.
3. Si quiere, puede cambiar el orden de los grupos dentro de una directiva existente. Para ello, reorganice los elementos de **GroupRef**.

Configurar el archivo XML del conector para Exchange ActiveSync El conector para Exchange ActiveSync utiliza un archivo de configuración XML para dictar las acciones del conector. Entre otras entradas, en el archivo se especifica el grupo de archivos y las acciones asociadas que el filtro tendrá en cuenta y realizará al evaluar solicitudes HTTP. De forma predeterminada, el archivo se denomina config.xml y se encuentra en la siguiente ubicación: ..\Archivos de programa\Citrix\XenMobile NetScaler Connector\config.

Nodos GroupRef

Los nodos de GroupRef definen los nombres de los grupos lógicos. Los valores predeterminados son AllowGroup y DenyGroup.

Nota:

Es importante el orden de aparición de los nodos GroupRef en el nodo GroupRefList.

El valor de ID de un nodo GroupRef identifica un contenedor lógico o una colección de miembros, que se utilizan para hacer coincidir dispositivos o cuentas de usuario específicos. Los atributos de la acción especifican cómo tratará el filtro a un miembro que coincida con una regla de la colección. Por ejemplo, un dispositivo o cuenta de usuario que coincida con una regla del conjunto AllowGroup “pasa”. En este caso, “pasar” significa que se le permitirá acceder a Exchange CAS. En cambio, un dispositivo o cuenta de usuario que coincida con una regla del conjunto DenyGroup será “rechazada”. En este caso, “rechazar” significa que no se le permitirá acceder a Exchange CAS.

Cuando un dispositivo o una cuenta de usuario determinados, o bien una combinación, cumplen las reglas de ambos grupos, se usa una convención de precedencia para dirigir el resultado de la solicitud. La precedencia se expresa en el orden de los nodos GroupRef en el archivo config.xml de arriba a abajo. Los nodos GroupRef están clasificados por orden de prioridad. Las reglas de una condición determinada del grupo Allow (Permitir) siempre prevalecerán sobre las reglas de la misma condición en el grupo Deny (Denegar).

Nodos Group

Además, el archivo config.xml define los nodos Group. Estos nodos enlazan los contenedores lógicos AllowGroup y DenyGroup a archivos XML. Las entradas almacenadas en los archivos externos forman la base de las reglas de filtrado.

Nota:

En esta versión, solo se admiten los archivos XML externos.

La instalación predeterminada implementa dos archivos XML en la configuración: allow.xml y deny.xml.

Configurar el conector de NetScaler Gateway para Exchange ActiveSync

Puede configurar el conector de NetScaler Gateway para Exchange ActiveSync de modo que este conector bloquee o permita solicitudes de ActiveSync de forma selectiva, en función de las propiedades **Active Sync Service ID**, **Device type**, **User Agent** (sistema operativo del dispositivo), **Authorized user** y **ActiveSync Command**.

La configuración predeterminada admite una combinación de grupos estáticos y dinámicos. Debe mantener grupos estáticos mediante la herramienta de configuración del controlador SMG. Los grupos estáticos pueden constar solo de las categorías conocidas de los dispositivos, como, por ejemplo, todos los dispositivos con un agente determinado de usuario.

Una fuente externa, llamada Gateway Configuration Provider (Proveedor de configuración de la puerta de enlace) mantiene los grupos dinámicos. El conector para Exchange ActiveSync conecta los grupos de forma periódica. Con Citrix Endpoint Management puede exportar grupos de dispositivos y usuarios permitidos y bloqueados al conector para Exchange ActiveSync.

Una fuente externa, llamada Gateway Configuration Provider (Proveedor de configuración de la puerta de enlace) mantiene los grupos dinámicos. El conector para Exchange ActiveSync recopila periódicamente grupos dinámicos. Con Citrix Endpoint Management puede exportar grupos de dispositivos y usuarios permitidos y bloqueados al conector.

Una directiva es una lista ordenada de grupos, donde cada grupo tiene asociada una acción (permitir o bloquear), además de una lista de los miembros del grupo. Una directiva puede tener una cantidad infinita de grupos. El orden de los grupos en una directiva es importante porque, cuando se encuentra una coincidencia, se realiza la acción del grupo, y los demás grupos no se evalúan.

Un miembro define la manera de coincidir con las propiedades de una solicitud. Se puede coincidir con una sola propiedad, como ID de dispositivo, o con varias propiedades, como el tipo de dispositivo y el agente de usuario.

Seleccionar un modelo de seguridad para el conector de NetScaler Gateway para Exchange ActiveSync

Establecer un modelo de seguridad es esencial para una buena implementación de dispositivos móviles en organizaciones de cualquier tamaño. Es frecuente utilizar un control de red protegida o en cuarentena para permitir el acceso a un usuario, un equipo o un dispositivo de forma predeterminada. Sin embargo, esta práctica no es siempre la más adecuada. Es posible que las organizaciones que administran la seguridad de TI tengan enfoques diferentes o adaptados a la seguridad de los dispositivos móviles.

La misma lógica se aplica a la seguridad de los dispositivos móviles. Utilizar un modelo permisivo es una mala elección debido a la gran cantidad de: dispositivos móviles y sus tipos, dispositivos móviles por usuario, así como aplicaciones y plataformas de sistemas operativos disponibles. En la mayoría de las organizaciones, el modelo restrictivo es la elección más lógica.

Los tipos de configuración que permite Citrix para integrar el conector para Exchange ActiveSync en Citrix Endpoint Management son:

Modelo permisivo (Permit mode)

El modelo de seguridad permisivo estipula que, de forma predeterminada, se permite o se concede acceso a todo. Solo se bloqueará el acceso a algo y se aplicará una restricción si existen reglas y filtros. El modelo de seguridad permisivo es una buena opción para organizaciones con un criterio de seguridad de dispositivos móviles relativamente laxo. Ese modelo solo aplica controles restrictivos para denegar el acceso cuando corresponda (si falla una regla de directiva).

Modelo restrictivo (Block Mode)

El modelo de seguridad restrictivo estipula que, de forma predeterminada, no se permite o no se concede acceso a nada. Todo lo que pasa por el punto de control de seguridad se filtra y se comprueba; se le deniega el acceso a menos que las reglas de acceso lo permitan. El modelo de seguridad restrictivo es una buena opción para organizaciones con un criterio de seguridad de dispositivos móviles relativamente estricto. Este modo solo concede acceso para uso y funciones con los servicios de red cuando todas las reglas de acceso lo permitan.

Administrar el conector de NetScaler Gateway para Exchange ActiveSync

Puede utilizar 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

provenientes de los dispositivos administrados. El acceso se concede en función del estado del dispositivo, las aplicaciones permitidas o prohibidas u otras condiciones de cumplimiento.

Con la herramienta de configuración del conector para Exchange ActiveSync, puede generar reglas dinámicas y estáticas que apliquen directivas de correo electrónico de empresa. Estas reglas y directivas permiten bloquear a los usuarios que infrinjan las normas de cumplimiento. También puede configurar el cifrado de datos adjuntos de correo electrónico, de modo que todos esos datos que pasen a través del servidor Exchange hacia los dispositivos administrados se cifren. En ese caso, solo los usuarios autorizados con dispositivos administrados podrán ver los datos adjuntos cifrados.

Para desinstalar XenMobile NetScaler Connector

1. Ejecute XncInstaller.exe con una cuenta de administrador.
2. Siga las instrucciones que aparecen en la 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 para permitir la actualización o la eliminación de un conector existente.
2. Siga las instrucciones en pantalla para completar la instalación, la actualización o la desinstalación.

Después de instalar el conector para Exchange ActiveSync, debe reiniciar manualmente el servicio de notificación y el servicio de configuración de Citrix Endpoint Management.

Instalar el conector de NetScaler Gateway para Exchange ActiveSync

Puede instalar el conector para Exchange ActiveSync en su propio servidor o en el mismo servidor donde se ha instalado Citrix Endpoint Management.

Puede plantearse instalar el conector para Exchange ActiveSync en su propio servidor (separado de Citrix Endpoint Management) por los siguientes motivos:

- Si el 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 todos los recursos del sistema de un servidor al conector para Exchange ActiveSync (rendimiento)

La carga de la CPU que pone el conector para Exchange ActiveSync en 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. En caso de una gran cantidad de dispositivos (más de 50 000), tal vez necesite aprovisionar más núcleos si no dispone de un entorno en clústeres. La superficie de memoria del conector no es lo suficientemente significativa como para garantizar una memoria adicional.

Requisitos del sistema para el 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. Ese puente permite al dispositivo pasar todo el tráfico seguro directamente a Citrix Endpoint Management. El conector para Exchange ActiveSync requiere la siguiente configuración mínima de sistema:

Componente	Requisito
Equipo y procesador	Procesador Pentium III de 733 MHz o más. Procesador Pentium III de 2,0 GHz o más (recomendado)
Citrix Gateway	Dispositivo Citrix Gateway con la versión 10 del software
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 en inglés. La compatibilidad para Windows Server 2008 R2 Service Pack 1 finaliza el 14 de enero de 2020 y la compatibilidad para Windows Server 2012 R2 finaliza el 10 de octubre de 2023.
Otros dispositivos	Un adaptador de red compatible con el sistema operativo del 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 del conector para Exchange ActiveSync requiere el siguiente espacio mínimo disponible en el disco duro:

- **Aplicación:** De 10 a 15 MB (se recomienda 100 MB)
- **Captura de registros:** 1 GB (se recomienda 20 GB)

Para obtener más información acerca de la compatibilidad de plataformas con el conector para Exchange ActiveSync, consulte [Sistemas operativos compatibles](#).

Clientes de correo electrónico del dispositivo

No todos los clientes de correo electrónico devuelven el mismo ID de ActiveSync para un dispositivo. Debido a 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 constantemente el mismo y único ID de ActiveSync para cada dispositivo. Citrix ha realizado pruebas sin errores con estos clientes de correo electrónico:

- Cliente de correo electrónico nativo de Samsung
- Cliente de correo electrónico nativo de iOS

Implementar el conector de NetScaler Gateway para Exchange ActiveSync

El conector de NetScaler Gateway para Exchange ActiveSync permite utilizar NetScaler Gateway para redirigir mediante proxy y equilibrar la carga de la comunicación entre el servidor y los dispositivos administrados de Citrix Endpoint Management. El conector para Exchange ActiveSync se comunica periódicamente con Citrix Endpoint Management para sincronizar directivas. Puede agrupar en un mismo clúster el conector para Exchange ActiveSync y Citrix Endpoint Management, juntos o de forma independiente.

Componentes del conector para Exchange ActiveSync

- **Servicio del conector para Exchange ActiveSync:** Este servicio ofrece una interfaz de servicio web de REST que NetScaler Gateway puede invocar para determinar si se autoriza una solicitud de ActiveSync desde un dispositivo.
- **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 a Citrix Endpoint Management acerca de accesos de dispositivos no autorizados. De esta forma, Citrix Endpoint Management puede tomar las medidas adecuadas, como notificar al usuario el motivo del bloqueo del dispositivo.
- **Herramienta 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 desde NetScaler Gateway para autorizar el tráfico de ActiveSync, debe: Especificar 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 la herramienta de configuración del conector para Exchange ActiveSync.
2. Haga clic en la ficha **Web Service** y, a continuación, escriba las direcciones de escucha para el servicio web del conector. Puede seleccionar **HTTP**, **HTTPS** o ambos. Si el conector para Exchange ActiveSync y Citrix Endpoint Management están instalados en el mismo servidor, seleccione puertos que no entren en conflicto con Citrix Endpoint Management.
3. Después de configurar los valores, haga clic en **Save** y, a continuación, haga clic en **Start Service** para iniciar el servicio web.

Para configurar las directivas de control de acceso del dispositivo en el conector de NetScaler Gateway para Exchange ActiveSync

Para configurar la directiva de control de acceso que quiere aplicar a los dispositivos administrados, haga lo siguiente:

1. En la herramienta de configuración del conector para Exchange ActiveSync, haga clic en la ficha **Path Filters**.
2. Seleccione la primera fila **Microsoft-Server-ActiveSync is for ActiveSync** y, a continuación, haga clic en **Edit**.
3. En la lista **Policy**, seleccione la directiva pertinente. Para una directiva que incluya las directivas de Citrix Endpoint Management, seleccione **Static + ZDM: Permit Mode** o **Static + ZDM: Block Mode**. Estas directivas combinan reglas locales (o estáticas) con las reglas de Citrix Endpoint Management. El modo Permit Mode significa que se permite el acceso a ActiveSync por parte de todos los dispositivos no identificados específicamente mediante reglas. En cambio, el modo Block Mode significa que todos esos dispositivos serán bloqueados.
4. Después de establecer las directivas, haga clic en **Save**.

Para configurar la comunicación con Citrix Endpoint Management

Especifique el nombre y las propiedades del servidor de Citrix Endpoint Management que quiere utilizar con el conector de NetScaler Gateway para Exchange ActiveSync y NetScaler Gateway.

Nota:

En esta tarea, se presupone que Citrix Endpoint Management ya está instalado y configurado. La utilidad de configuración de Exchange ActiveSync utiliza el término “Config Provider”(proveedor de configuraciones) para referirse a Citrix Endpoint Management.

1. En la herramienta de configuración del conector para Exchange ActiveSync, haga clic en la ficha **Config Providers** y, a continuación, haga clic en **Add**.
2. Indique el nombre y la dirección URL del servidor de Citrix Endpoint Management utilizado en esta implementación. Si dispone de varios servidores Citrix Endpoint Management implementados en una implementación multitarrendatario, este nombre debe ser único para cada instancia de servidor.
3. En **Url**, introduzca la dirección web de GlobalConfig Provider (GCP) de Citrix Endpoint Management. Por norma general, en el formato: `https://<FQDN>/<instanceName>/services/<MagConfigService>`. En el nombre *MagConfigService* se distinguen mayúsculas de minúsculas.
4. En **Password**, introduzca la contraseña que se usará para la autorización básica de HTTP en el servidor web de Citrix Endpoint Management.
5. En **Managing Host**, introduzca el nombre del servidor donde se instaló el conector para Exchange ActiveSync.
6. En **Baseline Interval**, especifique un período de tiempo para la extracción, desde Citrix Endpoint Management, de un conjunto de reglas dinámicas actualizadas.
7. En **Request Timeout**, especifique el intervalo de tiempo de espera para solicitudes del servidor.
8. En **Config Provider**, seleccione si la instancia de servidor de Config Provider proporciona la configuración de directivas.
9. Habilite la opción **Events Enabled** si quiere que Secure Mobile Gateway notifique a Citrix Endpoint Management cuando se bloquee un dispositivo. Se requiere esta opción si se utilizan las reglas de Secure Mobile Gateway en alguna de las acciones automatizadas de Citrix Endpoint Management.
10. Una vez configurado el servidor, haga clic en **Test Connectivity** para comprobar la conexión con Citrix Endpoint Management.
11. Cuando se haya establecido la conectividad, haga clic en **Save**.

Implementar el conector de NetScaler Gateway para Exchange ActiveSync para la redundancia y la escalabilidad

Si quiere ampliar 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 de conector deben apuntar a la misma instancia de Citrix Endpoint Management. Puede utilizar NetScaler Gateway para equilibrar la carga de los servidores.

La configuración del conector para Exchange ActiveSync cuenta con dos modos:

- En el modo no compartido (non-shared mode), cada instancia del conector para 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 del conector en cada servidor de Citrix Endpoint Management. Así, el conector obtiene directivas de parte de la instancia local de Citrix Endpoint Management.
- En modo compartido, un nodo del conector para Exchange ActiveSync es designado como nodo principal. El conector se comunica con Citrix Endpoint Management. Los demás nodos comparten la configuración resultante, ya sea mediante una replicación de Windows (o de terceros) o un recurso compartido de red Windows.

Toda la configuración del conector para Exchange ActiveSync se encuentra en una carpeta (de varios archivos XML). El proceso del conector detecta los cambios en los archivos de esta carpeta y vuelve a cargar automáticamente la configuración. No hay ninguna conmutación por error para el nodo principal en el 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 procesamiento del conector.

Conceptos avanzados

March 1, 2024

Los artículos de Conceptos avanzados de Citrix Endpoint Management ofrecen una información más exhaustiva sobre el producto Citrix Endpoint Management. El objetivo es ayudar a reducir el tiempo empleado en implementarlo, a través de técnicas de experto. Los expertos técnicos que hayan escrito el contenido se citan en los artículos.

Para ver puntos de decisión, recomendaciones, preguntas frecuentes y casos de uso de un entorno de Citrix Endpoint Management, consulte [Implementación de Citrix Endpoint Management](#) en esta sección.

Para buscar asistencia técnica en los foros de la comunidad de Citrix Endpoint Management, consulte [Citrix Discussions](#).

Implementar Citrix Endpoint Management

March 1, 2024

Hay muchos aspectos a tener en cuenta cuando se planifica una implementación de Citrix Endpoint Management. ¿Qué dispositivos elegir? ¿Cómo administrarlos? ¿Cómo asegurarse de que la red es segura y fácil de usar al mismo tiempo para los usuarios? ¿Qué hardware se necesita y cómo solucionar problemas en él? Los artículos de esta sección tienen como objetivo responder a estas preguntas. Se incluyen casos de uso y recomendaciones sobre temas que cubren sus dudas sobre la implementación.

Tenga en cuenta que una guía o recomendación podría no aplicarse a todos los entornos o casos de uso. Debe configurar un entorno de prueba antes de lanzar una implementación de Citrix Endpoint Management.

Los artículos de esta sección cubren las siguientes áreas:

- **Evaluar:** Casos de uso y preguntas frecuentes a plantearse durante la planificación de la implementación.
- **Diseñar y configurar:** Recomendaciones para diseñar y configurar el entorno
- **Operar y supervisar:** Asegurar el buen funcionamiento del entorno de ejecución.

Evaluación

Como con cualquier implementación, evaluar sus necesidades debe ser su primera prioridad. ¿Qué va a necesitar principalmente de Citrix Endpoint Management? ¿Necesita administrar 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 y preguntas frecuentes a considerar cuando planifique su implementación.

- [Modos de administración](#)
- [Requisitos de dispositivo](#)
- [Seguridad y experiencia del usuario](#)
- [Aplicaciones](#)
- [Comunidades de usuarios](#)
- [Estrategia de correo electrónico](#)
- [Integrar Citrix Endpoint Management](#)

Diseñar y configurar

Una vez que haya terminado de evaluar las necesidades de su implementación, puede decidir cómo diseñar y configurar su entorno. Los elementos que planificar son:

- Elegir el hardware para su servidor
- Configurar directivas para aplicaciones y dispositivos
- Hacer que los usuarios se inscriban

Esta sección incluye casos de uso y recomendaciones para cada uno de estos casos, entre otros.

- [Integración en NetScaler Gateway y Citrix ADC](#)
- [Consideraciones sobre SSO y proxies para aplicaciones MDX](#)
- [Autenticación](#)
- [Propiedades de servidor](#)
- [Directivas de aplicación y de dispositivo](#)
- [Opciones de inscripción de usuarios](#)

Operar y supervisar

Cuando su entorno de Citrix Endpoint Management esté en funcionamiento, querrá supervisarlos para garantizar un funcionamiento óptimo. En la sección de supervisión se describe dónde se encuentran los varios registros y mensajes que generan Citrix Endpoint Management y sus componentes, además de indicarle cómo interpretar esos registros. Esta sección también incluye una serie de pasos para solucionar problemas frecuentes, que puede seguir para reducir el tiempo de comunicación con los equipos de asistencia al cliente.

- [Aprovisionar y desaprovisionar aplicaciones](#)
- [Operaciones del panel de mandos](#)
- [Control de acceso basado en roles y asistencia de Citrix Endpoint Management](#)
- [Supervisar y ofrecer asistencia](#)
- [Proceso de asistencia de Citrix](#)

Modos de administración

March 1, 2024

Modos de administración es un término que incluye administración de dispositivos móviles (MDM) y 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 ofrecer a los usuarios la posibilidad de excluirse de MDM.
- Perfiles de inscripción para inscribir dispositivos con Windows 10 o Windows 11 en MDM.

Las opciones de inscripción se especifican en los perfiles de inscripción, que se asocian a los grupos de entrega. Para obtener información sobre las opciones de inscripción, consulte [Perfiles de inscripción](#). Las siguientes secciones se centran en consideraciones para administrar dispositivos y aplicaciones.

Administración de dispositivos móviles (MDM)

Con MDM, puede configurar, proteger y ofrecer soporte a dispositivos móviles. MDM permite proteger los dispositivos y los datos contenidos en esos dispositivos a nivel de sistema. Puede configurar directivas, acciones y funciones de seguridad. Por ejemplo, puede borrar un dispositivo de forma selectiva si el dispositivo se pierde, deja de cumplir la normativa o se lo roban.

Incluso si decide no administrar aplicaciones en dispositivos, puede entregar aplicaciones móviles, como las de tiendas públicas de aplicaciones y aplicaciones empresariales.

A continuación, se presentan los casos de uso más frecuentes para MDM:

- Vale la pena tener el modo MDM en cuenta cuando se trata de dispositivos propiedad de la empresa donde se requieren ciertas restricciones o directivas de administración a nivel de dispositivo. Estas restricciones incluyen borrado completo, borrado selectivo o geolocalización.
- Cuando los clientes requieren la administración de un dispositivo, pero no requieren directivas MDX.
- Cuando los usuarios solo necesitan que se entregue el correo electrónico a los clientes de correo nativos presentes en sus dispositivos móviles, y ya se puede acceder externamente a Exchange ActiveSync o al servidor de acceso de cliente. En este caso, se puede usar la administración MDM para configurar la entrega de correo electrónico.
- Cuando implementa aplicaciones empresariales nativas (no MDX), aplicaciones de tiendas públicas o aplicaciones MDX entregadas desde tiendas públicas. Tenga en cuenta que una solución MDM por sí sola no evita la filtración de información confidencial entre las aplicaciones presentes en el dispositivo. La filtración de datos puede ocurrir con las operaciones “Copiar”, “Pegar” o “Guardar como” en las aplicaciones Office 365.

Administración de aplicaciones móviles (MAM)

La administración MAM protege los datos de la aplicación y permite controlar el uso compartido de esos datos. MAM también permite administrar los datos y los recursos corporativos de manera separada de los datos personales. Con Citrix Endpoint Management configurado para MAM, puede usar aplicaciones móviles habilitadas para MDX para proporcionar el control y la contenedorización para cada aplicación.

Al utilizar las directivas MDX, Citrix Endpoint Management ofrece el control a nivel de aplicación sobre: el acceso a la red (por ejemplo, con una red micro VPN), la interacción de dispositivos y aplicaciones y el acceso a las aplicaciones.

MAM suele ser idóneo para dispositivos BYO porque, aunque el dispositivo no esté administrado, los datos corporativos permanecen protegidos. MDX tiene muchas directivas exclusivas de MAM que no requieren un control de MDM.

MAM también admite las aplicaciones móviles de productividad Citrix. Esto incluye:

- Entrega segura de correo electrónico a Citrix Secure Mail
- Uso compartido de datos entre las aplicaciones móviles de productividad seguras de Citrix
- Almacenamiento seguro de datos en Citrix Files.

Para obtener más información, consulte [Aplicaciones móviles de productividad](#).

A menudo, MAM conviene cuando:

- Entrega aplicaciones móviles, tales como aplicaciones MDX, administradas a nivel de aplicación.
- No necesita administrar dispositivos a nivel de sistema.

MDM+MAM

Citrix Endpoint Management le permite especificar si los usuarios pueden optar por no administrar los dispositivos. Esta flexibilidad es útil para entornos que incluyen una mezcla de casos de uso. Estos entornos pueden requerir la administración de un dispositivo a través de directivas MDM para acceder a los recursos MAM.

MDM+MAM conviene cuando:

- Dispone de un solo caso de uso donde se requieren MDM y MAM. Se necesita MDM para acceder a los 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 MDM

Un entorno de Citrix Endpoint Management Enterprise puede incluir una mezcla de casos de uso, donde algunos de ellos requieren la administración de dispositivos a través de directivas MDM para permitir el acceso a los recursos MAM.

Antes de implementar las aplicaciones móviles de productividad Citrix a los usuarios, debe evaluar de manera exhaustiva los casos de uso y decidir si requiere la inscripción MDM. Si más adelante decide cambiar el requisito de la inscripción 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 en NetScaler Gateway y Citrix ADC](#).

A continuación, dispone de un resumen de las ventajas y las desventajas (junto con las maneras de atenuarlas) de requerir la inscripción MDM.

Cuando la inscripción MDM es opcional

Ventajas

- Los usuarios pueden acceder a los recursos MAM sin que sus dispositivos se administren por MDM. Esta opción puede aumentar la cantidad de usuarios.
- Posibilidad de proteger el acceso a los recursos MAM para, a su vez, proteger los datos de empresa.
- Las directivas MDX, como **Código de acceso de aplicación**, pueden controlar el acceso a cada aplicación MDX.
- Si configura NetScaler Gateway, Citrix Endpoint Management y tiempos de espera para cada aplicación, junto con el PIN de Citrix, tendrá una capa extra de protección.
- Si bien las acciones de MDM no se aplican al dispositivo, dispone de determinadas directivas MDX para denegar el acceso a los recursos MAM. La denegación del acceso se basaría en la configuración del sistema, como dispositivos liberados por jailbreak o rooting.
- Los usuarios pueden elegir si inscribir sus dispositivos con MDM al primer uso.

Desventajas

- Los recursos MAM están disponibles para los dispositivos que no están inscritos con MDM.
- Las acciones y las directivas MDM solo están disponibles en los dispositivos inscritos con MDM.

Opciones de mitigación

- Haga que los usuarios acepten los términos y las condiciones de la empresa. Serán responsables frente a esta empresa si eligen dejar de cumplir las normas. Haga que los administradores supervisen los dispositivos no administrados.
- Administre la seguridad y el acceso a las aplicaciones a través de temporizadores de aplicación. Unos valores inferiores de tiempo de espera aumentan la seguridad, pero pueden afectar a la experiencia de usuario.

Cuando la inscripción MDM es obligatoria

Ventajas

- Posibilidad de restringir el acceso a los recursos MAM solo a los dispositivos administrados por MDM.
- Las acciones y las directivas MDM pueden aplicarse a todos los dispositivos del entorno como sea pertinente.
- Los usuarios no pueden optar por no inscribir su dispositivo.

Desventajas

- Requiere que todos los usuarios se inscriban con MDM.
- Puede reducir la cantidad de usuarios, ya que los usuarios que no estén de acuerdo con que la empresa administre sus dispositivos personales pueden no inscribirse.

Opciones de mitigación

- Informe a los usuarios sobre lo que Citrix Endpoint Management administra realmente en sus dispositivos e indíqueles a qué información pueden acceder los administradores.

Requisitos de dispositivo

November 29, 2023

Un punto importante a tener en cuenta en toda implementación es el conjunto de dispositivos que se va a utilizar. En las plataformas iOS, Android y Windows, existen varias opciones. Para ver la lista de los dispositivos que admiten Citrix Endpoint Management, consulte [Plataformas de dispositivos admitidos](#).

En un entorno BYOD, se puede dar una combinación de las plataformas compatibles. Sin embargo, tenga en cuenta las limitaciones descritas en el artículo “Plataformas de dispositivos admitidos” cuando informe a los usuarios sobre los dispositivos que pueden inscribir. Aunque solo permita uno o dos dispositivos en el entorno, el funcionamiento de Citrix Endpoint Management cambia ligeramente en dispositivos iOS, Android o Windows. En cada plataforma, están disponibles diferentes conjuntos de funciones.

Además, no todos los diseños de aplicaciones están orientados a tabletas y teléfonos a la vez. Antes de realizar cambios generalizados, pruebe las aplicaciones para asegurarse de que se ajustan a la pantalla del dispositivo donde quiere implementar el entorno.

También puede plantearse los factores de inscripción que va a utilizar. Apple y Google ofrecen programas de inscripción empresarial. A través del [Programa de implementación de Apple](#) y [Google Android Enterprise](#), puede adquirir dispositivos preconfigurados y listos para que los usen los empleados.

Para obtener más información acerca de la inscripción, consulte [Opciones de inscripción de usuarios](#).

Seguridad y experiencia del usuario

March 1, 2024

La seguridad es importante para cualquier organización, pero hay que encontrar el equilibrio entre la seguridad y la experiencia del usuario. Por ejemplo, es posible que tenga un entorno muy seguro que resulte difícil de usar para los usuarios. O, al contrario, es posible que su entorno resulte tan fácil de usar que el control del acceso no sea tan estricto como debiera. En las demás secciones de este manual virtual se tratan detalladamente las funciones de seguridad. El propósito de este artículo es ofrecer una visión general de los problemas 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 determinadas aplicaciones, todo el dispositivo o ambos?
- ¿Cómo quiere que los usuarios se autentiquen? ¿Quiere utilizar LDAP, la autenticación por certificado o una combinación de ambos?
- ¿Cuánto tiempo quiere que dure la sesión de un usuario antes de que se acabe el tiempo? Tenga en cuenta que existen valores de tiempo de espera diferentes para los servicios en segundo plano, Citrix ADC y para el acceso a aplicaciones sin conexión.
- ¿Quiere que los usuarios configuren una clave de acceso a nivel de dispositivo y aplicación? ¿Cuántos intentos de inicio de sesión quiere permitir? Tenga en cuenta los requisitos adicionales de autenticación por aplicación que se pueden implementar con MAM y cómo los pueden percibir los usuarios.
- ¿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 se ponga a su disposición y qué no pueden hacer? ¿Quiere implementar directivas de redes (Wi-Fi) en la empresa para impedir que se consuman planes de datos móviles en las oficinas?

Aplicación y dispositivo

Uno de los primeros aspectos a plantearse es si quiere proteger:

- Solo determinadas aplicaciones (administración de aplicaciones móviles o MAM)
- Todo el dispositivo (administración de dispositivos móviles o MDM).
- MDM+MAM

Lo más frecuente es que, si no requiere control a nivel de dispositivo, solo necesitará administrar aplicaciones móviles, sobre todo si la organización admite los dispositivos Bring Your Own Device (BYOD).

Los usuarios cuyos dispositivos no administre Citrix Endpoint Management pueden instalarse aplicaciones a través del almacén de aplicaciones. En lugar de controles a nivel de dispositivo (como el borrado completo o selectivo de datos), se puede controlar el acceso a las aplicaciones a través de directivas de aplicaciones. Según los valores que se establezcan, las directivas requieren que el dispositivo consulte periódicamente Citrix Endpoint Management para confirmar que las aplicaciones aún se pueden ejecutar.

MDM permite proteger un dispositivo completo, incluida la capacidad de realizar un inventario de todo el software presente en un dispositivo. MDM permite impedir la inscripción si el dispositivo está liberado por jailbreak, rooting o tiene instalado software no seguro. Sin embargo, asumir este nivel de control hace que los usuarios sean reacios a permitir tanto poder sobre sus dispositivos personales, con lo que puede que se reduzcan las tasas de inscripción.

Autenticación

La autenticación es donde se lleva a cabo una gran parte de la experiencia del usuario. Si la organización ya ejecuta Active Directory, usar Active Directory es la forma más sencilla de que los usuarios accedan al sistema.

Otra parte importante de la experiencia de autenticación de los usuarios son los tiempos de espera. Un entorno de alta seguridad puede hacer que los usuarios inicien sesión cada vez que accedan al sistema. Es posible que esa opción no sea ideal para todas las organizaciones o casos de uso.

Entropía de usuario

Para obtener una mayor seguridad, puede habilitar una función llamada *entropía de usuario*. Citrix Secure Hub y otras aplicaciones a menudo comparten datos comunes (como contraseñas, números PIN y certificados) para garantizar que todo funciona correctamente. Esta información se almacena en una caja fuerte genérica dentro de Citrix Secure Hub. Si habilita la entropía de usuario a través de la opción **Encrypt Secrets** (cifrar secretos), Citrix Endpoint Management crea una caja fuerte llamada “UserEntropy”. Citrix Endpoint Management traslada la información desde la caja fuerte genérica a esta nueva caja. Para que Citrix Secure Hub u otra aplicación accedan a los datos, los usuarios deben escribir una contraseña o PIN.

Habilitar la entropía de usuario agrega otra capa de autenticación en varios lugares. Por eso, siempre que una aplicación requiera acceso a datos compartidos en la caja fuerte “UserEntropy” (incluidas contraseñas, números PIN y certificados), los usuarios deben autenticarse.

Puede obtener más información sobre la entropía de usuario en [Acerca de MDX Toolkit](#). Para activar la entropía de usuario, dispone de la configuración relacionada en las [Propiedades del cliente](#).

Directivas

Las directivas MDX y MDM ofrecen una gran flexibilidad a las organizaciones, pero también pueden imponer restricciones a los usuarios. Puede que esa restricción le convenga en algunas situaciones, pero las directivas también pueden dar lugar a un sistema que no se pueda usar. Por ejemplo, puede que le interese bloquear el acceso a aplicaciones en la nube (como Siri o iCloud), con las que se pueden enviar datos confidenciales a destinos externos. 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

La administración de movilidad empresarial (EMM) se divide en la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM). Si bien MDM permite a las organizaciones proteger y controlar dispositivos móviles, MAM facilita la administración y la entrega de aplicaciones. Con el creciente uso de dispositivos BYOD, generalmente se puede implementar una solución MAM, como Citrix Endpoint Management, para lo siguiente:

- entrega de aplicaciones
- licencias de software
- configuración
- administración del ciclo de vida de las aplicaciones

Con Citrix Endpoint Management, puede agregar más seguridad a esas aplicaciones mediante directivas MAM y configuraciones de VPN específicas para evitar filtraciones de datos y otras amenazas a la seguridad. Citrix Endpoint Management proporciona a las organizaciones la flexibilidad necesaria para incluir la funcionalidad MDM y MAM en un mismo entorno.

Además de la capacidad de entregar aplicaciones a los dispositivos móviles, Citrix Endpoint Management ofrece la contenedorización de aplicaciones a través de la tecnología MDX. MDX protege las aplicaciones mediante un cifrado independiente del cifrado al nivel del dispositivo proporcionado por la plataforma. Puede borrar o bloquear aplicaciones. Las aplicaciones están sujetas a controles concisos basados en directivas. Los proveedores de software independientes (ISV) pueden aplicar estos controles mediante el Mobile Apps SDK.

En un entorno corporativo, los usuarios utilizan una variedad de aplicaciones móviles para desempeñar su trabajo. Las aplicaciones pueden ser: aplicaciones procedentes de la tienda pública, aplicaciones propias desarrolladas internamente o aplicaciones nativas. Citrix Endpoint Management clasifica estas aplicaciones de la siguiente manera:

Aplicaciones públicas: Este grupo contiene las aplicaciones, gratuitas o de pago, disponibles en una tienda pública de aplicaciones, como App Store de Apple o Google Play. Los proveedores externos a la

organización suelen poner sus aplicaciones disponibles en las tiendas públicas de aplicaciones. Esta opción permite a sus clientes descargar las aplicaciones directamente desde Internet. Puede utilizar varias aplicaciones públicas en su organización, según las necesidades de los usuarios. GoToMeeting, Salesforce y EpicCare son ejemplos de tales aplicaciones.

Citrix no admite la descarga de archivos binarios de aplicación directamente desde tiendas públicas de aplicaciones y, a continuación, su empaquetado con el MDX Toolkit para la distribución empresarial. Para habilitar para MDX aplicaciones de terceros, póngase en contacto con su proveedor de aplicaciones para obtener los binarios de aplicación. Puede empaquetar los binarios con MDX Toolkit o integrar el SDK de MAM con los binarios.

Aplicaciones internas: Muchas organizaciones tienen desarrolladores internos que crean aplicaciones con una funcionalidad específica y que se desarrollan y distribuyen de manera independiente dentro de la organización. En ciertos casos, algunas organizaciones también pueden tener aplicaciones proporcionadas por los ISV. Puede implementar esas aplicaciones como nativas, o puede colocarlas en un contenedor mediante una solución MAM, como Citrix Endpoint Management. Por ejemplo, una organización de asistencia sanitaria puede crear una aplicación interna que permita a los médicos ver la información del paciente en dispositivos móviles. En ese caso, la organización puede habilitar el SDK de MAM o empaquetar con MDM la aplicación a fin de proteger la información del paciente y permitir el acceso por VPN al servidor back-end de la base de datos de pacientes.

Aplicaciones web y SaaS: Este grupo incluye aquellas aplicaciones a las que se puede acceder a través de una red interna (aplicaciones web) o a través de una red pública (aplicaciones SaaS). Citrix Endpoint Management también permite crear aplicaciones web y SaaS personalizadas mediante una lista de conectores de aplicaciones. Esos conectores de aplicaciones pueden facilitar el inicio Single Sign-On (SSO) en las aplicaciones web existentes. Para obtener más información, consulte [Tipos de conectores de aplicaciones](#). Por ejemplo, puede usar Google Apps SAML para Single Sign-On basado en SAML (Security Assertion Markup Language) en aplicaciones de Google Apps.

Aplicaciones móviles de productividad: Se trata de aplicaciones desarrolladas por Citrix que se incluyen con la licencia de Citrix Endpoint Management. Para obtener más información, consulte [Acerca de las aplicaciones móviles de productividad](#). Citrix también ofrece otras [aplicaciones preparadas para empresas](#). Los ISV desarrollan aplicaciones de negocio con la ayuda de Mobile Apps SDK.

Aplicaciones HDX: Se trata de aplicaciones alojadas en Windows que se publican con StoreFront. Si dispone de un entorno de Citrix Virtual Apps and Desktops, puede integrar las aplicaciones en Citrix Endpoint Management para que estén disponibles a los usuarios inscritos.

La configuración y la arquitectura subyacentes varían según el tipo de aplicaciones móviles a implementar y administrar a través de Citrix Endpoint Management. Por ejemplo, varios grupos de usuarios con diferentes niveles de permisos utilizan una sola aplicación. En ese caso, puede crear grupos de entrega independientes para implementar dos versiones separadas de la misma aplicación. Además, deberá asegurarse de que la pertenencia a cada grupo de usuarios se excluya mutuamente, para evitar discrepancias entre las directivas que se apliquen a los dispositivos de los usuarios.

También sería conveniente administrar las licencias de las aplicaciones iOS a través de las compras por volumen de Apple. Esta opción requiere que se registre en el Programa de compras por volumen de Apple. Además, debe usar la consola de Citrix Endpoint Management para configurar las opciones de compra por volumen. Esta configuración permite distribuir las aplicaciones con las licencias de compras por volumen. Dada la variedad de estos casos de uso, es importante analizar y planificar la estrategia de MAM que va a seguir antes de implementar el entorno de Citrix Endpoint Management. Para comenzar a planificar su estrategia de MAM, defina lo siguiente:

Tipos de aplicaciones: Muestra los diferentes tipos de aplicaciones que estarán disponibles. A continuación, categorice las aplicaciones (web, públicas, nativas, móviles de productividad de Citrix, internas e ISV). Además, clasifique las aplicaciones según las diferentes plataformas de dispositivo (como iOS y Android). Esta categorización ayuda a alinear las configuraciones de Citrix Endpoint Management necesarias para cada tipo de aplicación. Por ejemplo, es posible que algunas aplicaciones no cumplan los requisitos para el empaquetado. O bien, algunas aplicaciones pueden requerir el uso del SDK de aplicaciones móviles para habilitar las API específicas para la interacción con otras aplicaciones.

Requisitos de red: Las aplicaciones que tengan requisitos específicos de acceso a la red deben configurarse con los parámetros adecuados. Por ejemplo, ciertas aplicaciones pueden necesitar acceder a la red interna por VPN. En cambio, otras aplicaciones pueden requerir que el acceso a Internet se enrute a través de la zona DMZ. Para permitir que esas aplicaciones se conecten a la red requerida, debe configurar varios parámetros según corresponda. Defina los requisitos de red por aplicación para adelantarse a la finalización de las decisiones de arquitectura. Esa tarea agiliza el proceso general de implementación.

Requisitos de seguridad: Defina los requisitos de seguridad que se aplicarán a aplicaciones individuales o a todas las aplicaciones. Las configuraciones, como las directivas MDX, se aplican a aplicaciones individuales. Las configuraciones de sesión y autenticación se aplican a todas las aplicaciones. Algunas aplicaciones pueden presentar requisitos específicos de cifrado, contenedorización, empaquetado, autenticación, geocercas, código de acceso o uso compartido de datos. Debe prever esos requisitos para facilitar la implementación.

Requisitos de implementación: Puede que le interese una implementación basada en directivas si quiere permitir que solo los usuarios conformes descarguen las aplicaciones publicadas. Por ejemplo, puede interesarle que ciertas aplicaciones requieran que:

- El cifrado por plataforma de dispositivos está habilitado
- El dispositivo está administrado
- El dispositivo tiene una versión mínima del sistema operativo
- Ciertas aplicaciones están disponibles solo para usuarios de empresa

Debe esbozar dichos requisitos con antelación para configurar las acciones o las reglas de implementación apropiadas.

Requisitos de licencia: Registre los requisitos de licencia relacionados con las aplicaciones. Estas notas le ayudarán a administrar de manera efectiva el uso de las licencias y a decidir si necesita configurar funciones específicas en Citrix Endpoint Management para optimizar la gestión de licencias. Por ejemplo, si implementa una aplicación iOS gratuita o de pago, Apple aplica requisitos de licencia a la aplicación porque obliga a los usuarios a iniciar sesión en su cuenta de App Store. Puede registrarse en el Programa de compras por volumen de Apple para distribuir y administrar esas aplicaciones a través de Citrix Endpoint Management. El Programa de compras por volumen permite a los usuarios descargar las aplicaciones sin tener que iniciar sesión en la cuenta del App Store. Además, las herramientas (como Samsung Knox) presentan requisitos especiales de licencia que debe cumplir antes de implementar esas funciones.

Requisitos de lista de bloqueados o lista de permitidos: Es probable que quiera impedir que los usuarios instalen o utilicen algunas aplicaciones. Cree una lista de aplicaciones bloqueadas que cambian el estado de un dispositivo a no conforme. A continuación, configure las directivas para que se activen cuando un dispositivo pase a ser no conforme. Por otro lado, puede que acepte el uso de una aplicación, pero esta se incluya en la lista de aplicaciones bloqueadas por una razón u otra. En ese caso, puede agregar la aplicación a una lista de aplicaciones permitidas e indicar que se puede usar, pero no es obligatoria. Además, tenga en cuenta que las aplicaciones ya instaladas en los dispositivos nuevos pueden incluir algunas aplicaciones de uso común que no forman parte del sistema operativo. Estas aplicaciones pueden entrar en conflicto con su estrategia de listas de aplicaciones bloqueadas.

Aplicaciones: caso de uso

Una organización de asistencia sanitaria quiere implementar Citrix Endpoint Management como solución MAM para sus aplicaciones móviles. Las aplicaciones móviles se entregan a usuarios de empresa y usuarios BYOD. El departamento de TI decide entregar y administrar las siguientes aplicaciones:

- **Aplicaciones móviles de productividad:** Aplicaciones iOS y Android que proporciona Citrix.
- **Citrix Files:** Aplicación para acceder a datos compartidos y para compartir, sincronizar y modificar archivos.

Tienda pública de aplicaciones

- **Citrix Secure Hub:** Cliente que utilizan todos los dispositivos móviles para comunicarse con Citrix Endpoint Management. El departamento de TI envía los parámetros de seguridad, las configuraciones y las aplicaciones móviles a los dispositivos móviles a través del cliente de Citrix Secure Hub. Los dispositivos Android y iOS se inscriben en Citrix Endpoint Management a través de Citrix Secure Hub.
- **Aplicación Citrix Workspace:** Aplicación móvil que permite a los usuarios abrir las aplicaciones para móviles alojadas en Citrix Virtual Apps.

- **GoToMeeting:** Un cliente de reuniones en línea, uso compartido de escritorios y videoconferencias que permite a los usuarios reunirse con clientes, colegas u otros usuarios de equipos a través de Internet en tiempo real.
- **SalesForce1:** Permite a los usuarios acceder a Salesforce desde dispositivos móviles, y reúne todos los procesos de negocio y las aplicaciones personalizadas, Chatter y CRM, en una experiencia unificada para cualquier usuario de Salesforce.
- **RSA SecurID:** Token basado en software para la autenticación de dos factores.
- **Aplicaciones EpicCare:** Estas aplicaciones ofrecen a los profesionales de la salud un acceso seguro y portátil a los gráficos de pacientes, las listas de pacientes, los horarios y los mensajes.
 - **Haiku:** Aplicación móvil para teléfonos Android y iPhone.
 - **Canto:** Aplicación móvil para el 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 administración electrónica de registros de salud.

ISV

- **Vocera:** Aplicación móvil de mensajería y VoIP compatible con HIPAA, que extiende las ventajas de la tecnología de voz de Vocera para poder aprovecharlas en cualquier momento y cualquier lugar desde smartphones iPhone y Android.

Aplicaciones internas

- **HCMail:** Aplicación que ayuda a redactar mensajes cifrados, buscar en las libretas de direcciones en servidores de correo interno y enviar los mensajes cifrados a los contactos mediante un cliente de correo electrónico.

Aplicaciones web internas

- **PatientRounding:** Aplicación web utilizada para registrar la información sanitaria del paciente por diferentes departamentos.
- **Outlook Web Access:** Permite el acceso al correo electrónico a través de un explorador web.
- **SharePoint:** Se usa para compartir archivos y datos por toda la organización.

En la tabla siguiente, se muestra la información básica necesaria para la configuración de MAM.

Nombre de la aplicación	Tipo de aplicación	Empaquetado MDX	iOS	Android
Citrix Secure Mail	Aplicación móvil de productividad	No a partir de la versión 10.4.1	Sí	Sí
Citrix Secure Web	Aplicación móvil de productividad	No a partir de la versión 10.4.1	Sí	Sí
Citrix Files	Aplicación móvil de productividad	No a partir de la versión 10.4.1	Sí	Sí
Citrix Secure Hub	Aplicación pública	NA	Sí	Sí
Aplicación Citrix Workspace	Aplicación pública	NA	Sí	Sí
GoToMeeting	Aplicación pública	NA	Sí	Sí
SalesForce1	Aplicación pública	NA	Sí	Sí
RSA SecurID	Aplicación pública	NA	Sí	Sí
Epic Haiku	Aplicación pública	NA	Sí	Sí
Epic Canto	Aplicación pública	NA	Sí	No
Epic Rover	Aplicación pública	NA	Sí	No
Epic Hyperspace	Aplicación HDX	NA	Sí	Sí
Vocera	Aplicación de ISV	Sí	Sí	Sí
HCMail	Aplicación interna	Sí	Sí	Sí
PatientRounding	Aplicación web	NA	Sí	Sí
Outlook Web Access	Aplicación web	NA	Sí	Sí
SharePoint	Aplicación web	NA	Sí	Sí

En la siguiente tabla, se ofrece una lista de los requisitos específicos que puede consultar para la configuración de directivas MAM en Citrix Endpoint Management.

Nombre de la aplicación	Se requiere VPN	Interacción (con aplicaciones fuera del contenedor)	Interacción (desde aplicaciones fuera del contenedor)	Cifrado por plataforma de dispositivos
Citrix Secure Mail	S	Se permite de manera selectiva	Se permite	No se requiere
Citrix Secure Web	S	Se permite	Se permite	No se requiere
Citrix Files	S	Se permite	Se permite	No se requiere
Citrix Secure Hub	S	N/D	N/D	N/D
Aplicación Citrix Workspace	S	N/D	N/D	N/D
GoToMeeting	N	N/D	N/D	N/D
SalesForce1	N	N/D	N/D	N/D
RSA SecurID	N	N/D	N/D	N/D
Epic Haiku	S	N/D	N/D	N/D
Epic Canto	S	N/D	N/D	N/D
Epic Rover	S	N/D	N/D	N/D
Epic Hyperspace	S	N/D	N/D	N/D
Vocera	S	Bloqueada	Bloqueada	No se requiere
HCMail	S	Bloqueada	Bloqueada	Si son necesarias
PatientRounding	S	N/D	N/D	Si son necesarias
Outlook Web Access	S	N/D	N/D	No se requiere
SharePoint	S	N/D	N/D	No se requiere

Nombre de la aplicación	Filtrado de proxy	Licencias	Geocerca	Mobile Apps SDK	Versión mínima del sistema operativo
Citrix Secure Mail	Si son necesarias	N/D	Se requiere de manera selectiva	N/D	Se aplica

Nombre de la aplicación	Filtrado de proxy	Licencias	Geocerca	Mobile Apps SDK	Versión mínima del sistema operativo
Citrix Secure Web	Si son necesarias	N/D	No se requiere	N/D	Se aplica
Secure Notes	Si son necesarias	N/D	No se requiere	N/D	Se aplica
Citrix Files	Si son necesarias	N/D	No se requiere	N/D	Se aplica
Citrix Secure Hub	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Aplicación Citrix Workspace	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
GoToMeeting	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
SalesForce1	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
RSA SecurID	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Haiku	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Canto	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Rover	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Hyperspace	No se requiere	N/D	No se requiere	N/D	No se aplica
Vocera	Si son necesarias	N/D	Si son necesarias	Si son necesarias	Se aplica
HCMail	Si son necesarias	N/D	Si son necesarias	Si son necesarias	Se aplica
PatientRounding	Si son necesarias	N/D	No se requiere	N/D	No se aplica
Outlook Web Access	Si son necesarias	N/D	No se requiere	N/D	No se aplica
SharePoint	Si son necesarias	N/D	No se requiere	N/D	No se aplica

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 mediante diversos recursos que usted proporciona a través de los dispositivos de usuario. Los usuarios pueden trabajar desde casa o en oficinas remotas mediante dispositivos móviles que usted proporcione. O bien, los usuarios pueden usar dispositivos móviles personales, lo que les permite acceder a herramientas que están sujetas a ciertas reglas de seguridad.

A medida que más comunidades de usuarios comienzan a utilizar dispositivos móviles en el trabajo, la administración de la movilidad empresarial (EMM) se vuelve vital para evitar la filtración de datos. EMM también es fundamental para hacer cumplir las restricciones de seguridad de una organización. Para una administración eficiente y más sofisticada de dispositivos móviles, puede categorizar las comunidades de los usuarios. Eso simplifica la asignación de los usuarios a los recursos y garantiza que se apliquen las directivas de seguridad correspondientes a los usuarios indicados.

El siguiente ejemplo ilustra cómo se clasifican para EMM las comunidades de usuarios de una organización de asistencia sanitaria.

Comunidades de usuarios: caso de uso

Esta organización sanitaria de ejemplo ofrece recursos tecnológicos y acceso a varios usuarios, incluidos los voluntarios, los empleados en la red y los empleados asociados. La organización ha decidido aplicar la solución EMM solo para usuarios no ejecutivos.

En esta organización, las funciones y los roles se pueden dividir en estos subgrupos: sanitarios, no sanitarios y contratistas. Unos usuarios concretos reciben dispositivos móviles de empresa, mientras que otras personas pueden acceder a recursos limitados de la empresa desde sus dispositivos personales. Para hacer cumplir el nivel apropiado de restricciones de seguridad y evitar la filtración de datos, la organización decidió que el departamento de TI corporativo administrara cada dispositivo inscrito. Estos dispositivos pueden ser propiedad de la empresa o Bring Your Own Device (BYOD). Además, los usuarios pueden inscribir un solo dispositivo.

La siguiente sección ofrece una descripción general de los roles y las funciones de cada subgrupo:

Sanitarios

- Enfermeros
- Médicos (doctores, cirujanos, etc.)
- Especialistas (dietistas, anestesiólogos, radiólogos, cardiólogos, oncólogos, etc.)
- Médicos externos (médicos que no son empleados y empleados de oficina que trabajan desde oficinas remotas)

- Servicios de cuidados a domicilio (empleados de oficina y móviles que desempeñan tareas de cuidado sanitario en visitas a domicilio de los pacientes)
- Especialista en investigación (trabajadores intelectuales y usuarios avanzados en seis institutos de investigación que realizan investigaciones clínicas para buscar respuestas a problemas en Medicina)
- Educación y formación (enfermeros, médicos y especialistas en educación y formación)

No sanitarios

- Servicios compartidos (empleados de oficina que realizan varias funciones administrativas, entre ellas: recursos humanos, nóminas, contabilidad y servicio de cadena de suministro)
- Servicios médicos (empleados de oficina que realizan diversos servicios de administración de cuidados médicos, servicios administrativos y procesos comerciales para proveedores, incluidos: servicios administrativos, análisis e inteligencia empresarial, sistemas de negocio, servicios al cliente, finanzas, gestión de cuidados realizados, soluciones de acceso a pacientes, soluciones de ciclo de ingresos, etc.)
- Servicios de asistencia técnica (empleados de oficina que realizan varias funciones no clínicas, por ejemplo: gestión de ganancias y beneficios, integración clínica, comunicaciones, compensación y gestión del rendimiento, servicios de instalaciones y propiedades, sistemas de tecnología de recursos humanos, servicios de información, auditoría interna y mejora de procesos, etc.)
- Programas filantrópicos (empleados de oficina y móviles que realizan diversas funciones en apoyo a programas filantrópicos)

Contratistas

- Socios de fabricantes y proveedores (in situ y conectados de forma remota a través de la VPN de sitio a sitio, ofrecen varias funciones de asistencia no sanitaria)

En función de la información anterior, la organización crea las siguientes entidades. Para obtener más información acerca de los grupos de entrega en Citrix Endpoint Management, consulte [Implementar recursos](#).

Grupos y unidades organizativas (OU) de Active Directory Como OU = Recursos de Citrix Endpoint Management:

- OU = Sanitarios; Groups =
 - XM-Enfermería
 - XM-Médicos
 - XM-Especialistas

- XM-Médicos externos
 - XM-Servicios de cuidados a domicilio
 - XM-Especialista en investigación
 - XM-Educación y formación
- OU = No sanitarios; Groups =
 - XM-Servicios compartidos
 - XM-Servicios médicos
 - XM-Servicios de asistencia técnica
 - XM-Programas filantrópicos

Grupos y usuarios locales de Citrix Endpoint Management Como Group= Contratistas, Users =

- Proveedor1
- Proveedor2
- Proveedor3
- ...Proveedor10

Grupos de entrega de Citrix Endpoint Management

- Sanitario-Enfermeros
- Sanitario-Médicos
- Sanitario-Especialistas
- Sanitario-Médicos externos
- Sanitario-Servicios de cuidados a domicilio
- Sanitario-Especialista en investigación
- Sanitario-Educación y formación
- No-Sanitario-Servicios compartidos
- No-Sanitario-Servicios médicos
- No-Sanitario-Servicios de asistencia técnica
- No-Sanitario-Programas filantrópicos

Asignación de grupos de usuario y grupos de entrega

Usar grupos de Active Directory	Grupos de entrega de Citrix Endpoint Management
XM-Enfermería	Sanitario-Enfermeros
XM-Médicos	Sanitario-Médicos

Usar grupos de Active Directory	Grupos de entrega de Citrix Endpoint Management
XM-Especialistas	Sanitario-Especialistas
XM-Médicos externos	Sanitario-Médicos externos
XM-Servicios de cuidados a domicilio	Sanitario-Servicios de cuidados a domicilio
XM-Especialista en investigación	Sanitario-Especialista en investigación
XM-Educación y formación	Sanitario-Educación y formación
XM-Servicios compartidos	No-Sanitario-Servicios compartidos
XM-Servicios médicos	No-Sanitario-Servicios médicos
XM-Servicios de asistencia técnica	No-Sanitario-Servicios de asistencia técnica
XM-Programas filantrópicos	No-Sanitario-Programas filantrópicos

Asignación de recursos y grupos de entrega En las siguientes tablas, se indican los recursos asignados a cada grupo de entrega en este caso de uso. La primera tabla contiene 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
Sanitario-Enfermeros	X		
Sanitario-Médicos			
Sanitario-Especialistas			
Sanitario-Médicos externos	X		
Sanitario-Servicios de cuidados a domicilio	X		
Sanitario-Especialista en investigación	X		
Sanitario-Educación y formación		X	X
No-Sanitario-Servicios compartidos		X	X
No-Sanitario-Servicios médicos		X	X

Grupos de entrega de

Citrix Endpoint Management	Aplicaciones móviles de Citrix	Aplicaciones móviles públicas	Aplicaciones móviles HDX
No-Sanitario-Servicios de asistencia técnica	X	X	X
No-Sanitario-Programas filantrópicos	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 Hyper-space	Directiva de código de acceso	Restricciones de dispositivo	Acciones automatizadas	Directiva de redes
Sanitario-Enfermeros							X
Sanitario-Médicos					X		
Sanitario-Especialistas							
Sanitario-Médicos externos							
Sanitario-Servicios de cuidados a domicilio							
Sanitario-Especialista en inversión							

Grupos de entrega de Citrix Endpoint Management	Aplicación pública:						
	RSA SecurID	Aplicación pública: EpicCare Haiku	Aplicación HDX: Epic Hyper-space	Directiva de código de acceso	Restricciones de dispos- itivo	Acciones automati- zadas	Directiva de redes
Sanitario- Educación y forma- ción		X	X				
No- Sanitario- Servicios compartidos		X	X				
No- Sanitario- Servicios médicos		X	X				
No- Sanitario- Servicios de asistencia técnica		X	X				

Notas y consideraciones

- Citrix Endpoint Management crea un grupo de entrega predeterminado llamado AllUsers (Todos los usuarios) durante la configuración inicial. Si no inhabilita este grupo de entrega, todos los usuarios de Active Directory tendrán derecho a inscribirse en Citrix Endpoint Management.
- Citrix Endpoint Management sincroniza los grupos y los usuarios de Active Directory a demanda mediante una conexión dinámica al servidor LDAP.
- Si un usuario forma parte de un grupo que no está asignado en Citrix Endpoint Management, dicho usuario no podrá inscribirse. Del mismo modo, si un usuario es miembro de varios grupos, Citrix Endpoint Management solo clasifica al usuario como perteneciente a los grupos asignados a Citrix Endpoint Management.

Requisitos de seguridad

La cantidad de consideraciones de seguridad al implementar un entorno de Citrix Endpoint Management puede convertirse rápidamente en abrumadora. Hay muchas piezas y parámetros interconectados. Por consiguiente, no es fácil saber por dónde empezar o qué elegir para garantizar un nivel aceptable de protección. Para simplificar estas opciones, Citrix ofrece recomendaciones para un nivel de seguridad alto, superior y máximo, como se describe en la siguiente tabla.

Las cuestiones de seguridad por sí solas no dictan el modo de inscribir los dispositivos: MAM, MDM+MAM con MDM optativo 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 el modo de administración.

Alto: Usar estas configuraciones proporciona una experiencia de usuario óptima, al mismo tiempo que se mantiene un nivel básico de seguridad aceptable para la mayoría de las organizaciones.

Superior: Estas configuraciones logran un mayor equilibrio entre seguridad y usabilidad.

Máximo: Seguir estas recomendaciones proporciona un alto nivel de seguridad a costa de la usabilidad y el aumento de la cantidad de usuarios.

Consideraciones sobre seguridad en el modo de administración

La siguiente tabla contiene los modos de administración para cada nivel de seguridad.

High Security (Nivel alto de seguridad)	Higher Security (Mayor nivel de seguridad)	Highest Security (El mayor nivel de seguridad)
MAM, MDM+MAM	MDM+MAM	MDM+MAM

Notas:

- Dependiendo del caso de uso, una implementación de solo MAM podría cumplir los requisitos de seguridad y proporcionar una buena experiencia de usuario.
- Para casos de uso como BYOD, donde todos los requisitos de empresa y de seguridad pueden cumplirse solo con contenedores de aplicaciones, Citrix recomienda el modo solo MAM.
- Para entornos de alta seguridad (y dispositivos que distribuyan las empresas), Citrix recomienda MDM+MAM para utilizar todas las capacidades de seguridad disponibles.

Consideraciones sobre la seguridad de Citrix ADC y NetScaler Gateway

La siguiente tabla contiene recomendaciones de Citrix ADC y NetScaler Gateway para cada nivel de seguridad.

High Security (Nivel alto de seguridad)	Higher Security (Mayor nivel de seguridad)	Highest Security (El mayor nivel de seguridad)
Se recomienda Citrix ADC. Se requiere NetScaler Gateway para MAM y MDM+MAM.	Configuración estándar del asistente de NetScaler para XenMobile con puente SSL si Citrix Endpoint Management está en la zona DMZ.	Descarga de SSL con cifrado de extremo a extremo

Notas:

- Exponer el servidor de Citrix Endpoint Management a Internet a través de NAT o proxies/equilibradores de carga de terceros 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 potencial para la seguridad.
- Para entornos de alta seguridad, NetScaler Gateway con la configuración predeterminada de Citrix Endpoint Management cumple o supera los requisitos de seguridad.
- Para inscripciones en MDM con las necesidades de seguridad máxima, la finalización de SSL en NetScaler Gateway permite inspeccionar el tráfico en el perímetro, al mismo tiempo que se mantiene el cifrado SSL de extremo a extremo.
- Opciones para definir cifrados SSL/TLS.
- Para obtener más información, consulte [Integrar en NetScaler Gateway y Citrix ADC](#).

Consideraciones sobre seguridad para la inscripción

La siguiente tabla contiene recomendaciones de Citrix ADC y NetScaler Gateway para cada nivel de seguridad.

High Security (Nivel alto de seguridad)	Higher Security (Mayor nivel de seguridad)	Highest Security (El mayor nivel de seguridad)
Solo miembros del grupo de Active Directory. Inhabilitado el grupo de entrega Todos los usuarios.	Modo de seguridad de inscripción solo por invitación. Solo miembros del grupo de Active Directory. Inhabilitado el grupo de entrega Todos los usuarios.	Modo de seguridad de inscripción vinculado al ID del dispositivo. Solo miembros del grupo de Active Directory. Inhabilitado el grupo de entrega Todos los usuarios.

Notas:

- Por regla general, Citrix recomienda que restrinja la inscripción a solamente aquellos usuarios que formen parte de los grupos predefinidos de Active Directory. Esta restricción requiere inhabilitar el grupo de entrega integrado Todos los usuarios.
- Puede utilizar las invitaciones de inscripción para restringir la inscripción a los usuarios que tengan 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 una solución de dos factores. Así también puede controlar la cantidad de dispositivos que un usuario puede inscribir (las invitaciones con OTP no están disponibles para dispositivos Windows).

Consideraciones sobre la seguridad de los códigos de acceso de dispositivo

Esta tabla contiene las recomendaciones para el código de acceso de dispositivo en cada nivel de seguridad.

High Security (Nivel alto de seguridad)	Higher Security (Mayor nivel de seguridad)	Highest Security (El mayor nivel de seguridad)
Recomendado. Se requiere un nivel alto de seguridad para el cifrado a nivel de dispositivo. Puede aplicarse con MDM. Se puede configurar como obligatorio solo para MAM mediante la directiva MDX Comportamiento de dispositivos no conformes.	Se aplica mediante una directiva MDM, MAM o MDM+MAM.	Aplicado mediante una directiva MDM y MDX. Directiva MDM “Código de acceso complejo”.

Notas:

- Citrix recomienda usar un código de acceso de dispositivo.
- Puede aplicar un código de acceso de dispositivo a través de una directiva MDM.
- Puede usar una directiva MDX para hacer que un código de acceso de 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 una mayor seguridad en las inscripciones con MDM+MAM.
- Para entornos con los requisitos máximos de seguridad, puede configurar directivas “Código de acceso complejo” y aplicarlas con MDM. Puede configurar acciones automáti-

cas que notifiquen a los administradores, o puede emitir borrados selectivos o completos cuando un dispositivo no sigue una directiva de código de acceso.

Aplicaciones

March 1, 2024

La administración de movilidad empresarial (EMM) se divide en la administración de dispositivos móviles (MDM) y la administración de aplicaciones móviles (MAM). Si bien MDM permite a las organizaciones proteger y controlar dispositivos móviles, MAM facilita la administración y la entrega de aplicaciones. Con el creciente uso de dispositivos BYOD, generalmente se puede implementar una solución MAM como Citrix Endpoint Management. Citrix Endpoint Management simplifica la entrega de aplicaciones, la gestión de licencias de software, la configuración y la administración del ciclo de vida de las aplicaciones. Puede requerir o permitir que los usuarios opten también por la administración MDM.

Con Citrix Endpoint Management, puede proteger aplicaciones mediante directivas MAM y configuraciones de VPN para evitar filtraciones de datos y otras amenazas a la seguridad. Citrix Endpoint Management ofrece a las organizaciones la flexibilidad de inscribir dispositivos como solo MAM o MDM+MAM.

Además de la capacidad de entregar aplicaciones a los dispositivos móviles, Citrix Endpoint Management ofrece la contenedorización de aplicaciones a través de la tecnología MDX. Las aplicaciones están sujetas a controles concisos basados en directivas. Los proveedores de software independientes (ISV) pueden aplicar estos controles mediante el Mobile Apps SDK.

En un entorno corporativo, los usuarios utilizan una variedad de aplicaciones móviles para desempeñar su trabajo. Las aplicaciones pueden ser: aplicaciones procedentes de la tienda pública, aplicaciones propias desarrolladas internamente o aplicaciones nativas. Citrix Endpoint Management clasifica estas aplicaciones de la siguiente manera:

- **Aplicaciones públicas:** Este grupo contiene las aplicaciones, gratuitas o de pago, disponibles en una tienda pública de aplicaciones, como App Store de Apple o Google Play. Los proveedores externos a la organización suelen poner sus aplicaciones disponibles en las tiendas públicas de aplicaciones. Esta opción permite a sus clientes descargar las aplicaciones directamente desde Internet. Puede utilizar varias aplicaciones públicas en su organización, según las necesidades de los usuarios. GoToMeeting, Salesforce y EpicCare son ejemplos de tales aplicaciones.
 - **Si utiliza el SDK de MAM:** Obtenga los binarios de aplicación de su proveedor de aplicaciones. A continuación, integre el SDK de MAM en la aplicación.

- **Si utiliza MDX Toolkit:** Citrix no admite la descarga de archivos binarios de aplicación directamente desde tiendas públicas de aplicaciones y, a continuación, su empaquetado con el MDX Toolkit para la distribución empresarial. Para empaquetar aplicaciones de terceros, debe colaborar con su proveedor de aplicaciones para obtener los archivos binarios de aplicación. A continuación, podrá empaquetar esos archivos binarios con MDX Toolkit.
- **Aplicaciones internas:** Muchas organizaciones tienen desarrolladores internos que crean aplicaciones con una funcionalidad específica y que se desarrollan y distribuyen de manera independiente dentro de la organización. En ciertos casos, algunas organizaciones también pueden tener aplicaciones proporcionadas por los ISV. Puede implementar esas aplicaciones como nativas, o puede colocarlas en un contenedor mediante una solución MAM, como Citrix Endpoint Management.

Por ejemplo, una organización de asistencia sanitaria puede crear una aplicación interna que permita a los médicos ver la información del paciente en dispositivos móviles. A continuación, esa organización puede proteger la información del paciente y habilitar el acceso por VPN a la base de datos de pacientes mediante uno de los siguientes procedimientos:

 - SDK de MAM
 - MDX Toolkit
- **Aplicaciones web y SaaS:** Este grupo incluye aquellas aplicaciones a las que se puede acceder a través de una red interna (aplicaciones web) o a través de una red pública (aplicaciones SaaS). Citrix Endpoint Management también permite crear aplicaciones web y SaaS personalizadas mediante una lista de conectores de aplicaciones. Esos conectores de aplicaciones pueden facilitar el inicio Single Sign-On (SSO) en las aplicaciones web existentes. Para obtener más información, consulte [Tipos de conectores de aplicaciones](#). Por ejemplo, puede usar Google Apps SAML para Single Sign-On basado en SAML (Security Assertion Markup Language) en aplicaciones de Google Apps.
- **Aplicaciones móviles de productividad:** Se trata de aplicaciones desarrolladas por Citrix que se incluyen con la licencia de Citrix Endpoint Management. Para obtener más información, consulte [Acerca de las aplicaciones móviles de productividad](#). Citrix también ofrece otras [aplicaciones de negocio](#) que los ISV desarrollan mediante el Mobile Apps SDK.
- **Aplicaciones HDX:** Se trata de 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.

La configuración subyacente varía según el tipo de aplicaciones móviles a implementar y administrar a través de Citrix Endpoint Management. Por ejemplo, varios grupos de usuarios con diferentes niveles de permisos utilizan una sola aplicación. En ese caso, puede crear grupos de entrega independientes para implementar dos versiones separadas de la misma aplicación. Además, deberá asegurarse

de que la pertenencia a cada grupo de usuarios se excluya mutuamente, para evitar discrepancias entre las directivas que se apliquen a los dispositivos de los usuarios.

También puede administrar las licencias de las aplicaciones iOS a través de las compras por volumen de Apple. Para poder utilizar esta opción, deberá registrarse en el Programa de compras por volumen y definir los parámetros de compras por volumen desde la consola de Citrix Endpoint Management. Esta configuración permite distribuir las aplicaciones con las licencias de compras por volumen. Dada la variedad de casos de uso, es importante analizar y planificar la estrategia de MAM que va a seguir antes de implementar el entorno de Citrix Endpoint Management. Para comenzar a planificar su estrategia de MAM, defina lo siguiente:

- **Tipos de aplicaciones:** Indique los diferentes tipos de aplicaciones que quiere admitir y clasifíquelas por categorías (por ejemplo, aplicaciones públicas, nativas, web, internas o ISV). Además, clasifique las aplicaciones según las diferentes plataformas de dispositivo (como iOS y Android). Esta categorización ayudará a encajar los distintos parámetros de Citrix Endpoint Management que se requieren para cada tipo de aplicación. Por ejemplo, algunas aplicaciones pueden requerir el uso del Mobile Apps SDK a fin de habilitar unas API especiales para la interacción con otras aplicaciones.
- **Requisitos de red:** Deberán configurarse los parámetros de las aplicaciones que tengan requisitos específicos de acceso a la red. Por ejemplo, ciertas aplicaciones pueden necesitar acceder a la red interna por VPN. En cambio, otras aplicaciones pueden requerir que el acceso a Internet se enrute a través de la zona DMZ. Para permitir que esas aplicaciones se conecten a la red requerida, debe configurar varios parámetros según corresponda. Definir unos requisitos de red por aplicación contribuye a precisar sus decisiones arquitectónicas desde el principio, lo que optimiza el proceso general de implementación.
- **Requisitos de seguridad:** Puede definir requisitos de seguridad que se aplicarán a aplicaciones individuales o a todas las aplicaciones.
 - Las configuraciones, como las directivas MDX, se aplican a aplicaciones individuales
 - Las configuraciones de sesión y autenticación se aplican a todas las aplicaciones
 - Algunas aplicaciones pueden presentar requisitos específicos de contenedorización, MDX, autenticación, geocercas, código de acceso o uso compartido de datos.

Debe prever esos requisitos para facilitar la implementación. Para obtener más información sobre la seguridad en Citrix Endpoint Management, consulte [Seguridad y experiencia de usuario](#).

- **Requisitos de implementación:** Puede que le interese una implementación basada en directivas si quiere permitir que solo los usuarios conformes descarguen las aplicaciones publicadas. Por ejemplo, aplicaciones determinadas pueden requerir que el dispositivo esté administrado o tenga instalada una versión mínima del sistema operativo. También puede interesarle que ciertas aplicaciones estén disponibles solo para usuarios de empresa. Debe esbozar dichos requisitos con antelación para configurar las acciones o las reglas de implementación apropiadas.

- **Requisitos de licencia:** Conserve un registro de los requisitos de licencia relacionados con las aplicaciones. Las notas pueden servirle de ayuda para administrar de manera efectiva el uso de las licencias y decidir si configurar funciones específicas en Citrix Endpoint Management para optimizar la gestión de licencias. Por ejemplo, si implementa una aplicación iOS gratuita o de pago, Apple aplica requisitos de licencia a la aplicación, lo que obliga a los usuarios a iniciar sesión en su cuenta de App Store.

Sin embargo, puede registrarse en el Programa de compras por volumen de Apple para distribuir y administrar esas aplicaciones a través de Citrix Endpoint Management. El Programa de compras por volumen permite a los usuarios descargar las aplicaciones sin tener que iniciar sesión en la cuenta del App Store.

Algunas plataformas presentan requisitos especiales de licencia que debe cumplir antes de implementar esas funciones.

- **Requisitos de lista de aplicaciones permitidas o bloqueadas:** Puede identificar las aplicaciones que no quiere que los usuarios se instalen o usen. Para empezar, cree una lista donde defina un evento de incumplimiento que será motivo de bloqueo. A continuación, configure directivas para que se activen cuando se produzca el evento. Por otro lado, puede que acepte el uso de una aplicación, pero esta se incluya en la lista de bloqueo por alguna razón. En ese caso, puede agregar la aplicación a una lista de aplicaciones permitidas e indicar que se puede usar, pero no es obligatoria. Además, tenga en cuenta que las aplicaciones ya instaladas en los dispositivos nuevos pueden incluir algunas aplicaciones de uso común que no forman parte del sistema operativo. Estas aplicaciones pueden entrar en conflicto con su estrategia de listas de aplicaciones bloqueadas.

Caso de uso

Una organización de asistencia sanitaria quiere implementar Citrix Endpoint Management como solución MAM para sus aplicaciones móviles. Las aplicaciones móviles se entregan a usuarios de empresa y usuarios BYOD. El departamento de TI decide entregar y administrar las siguientes aplicaciones:

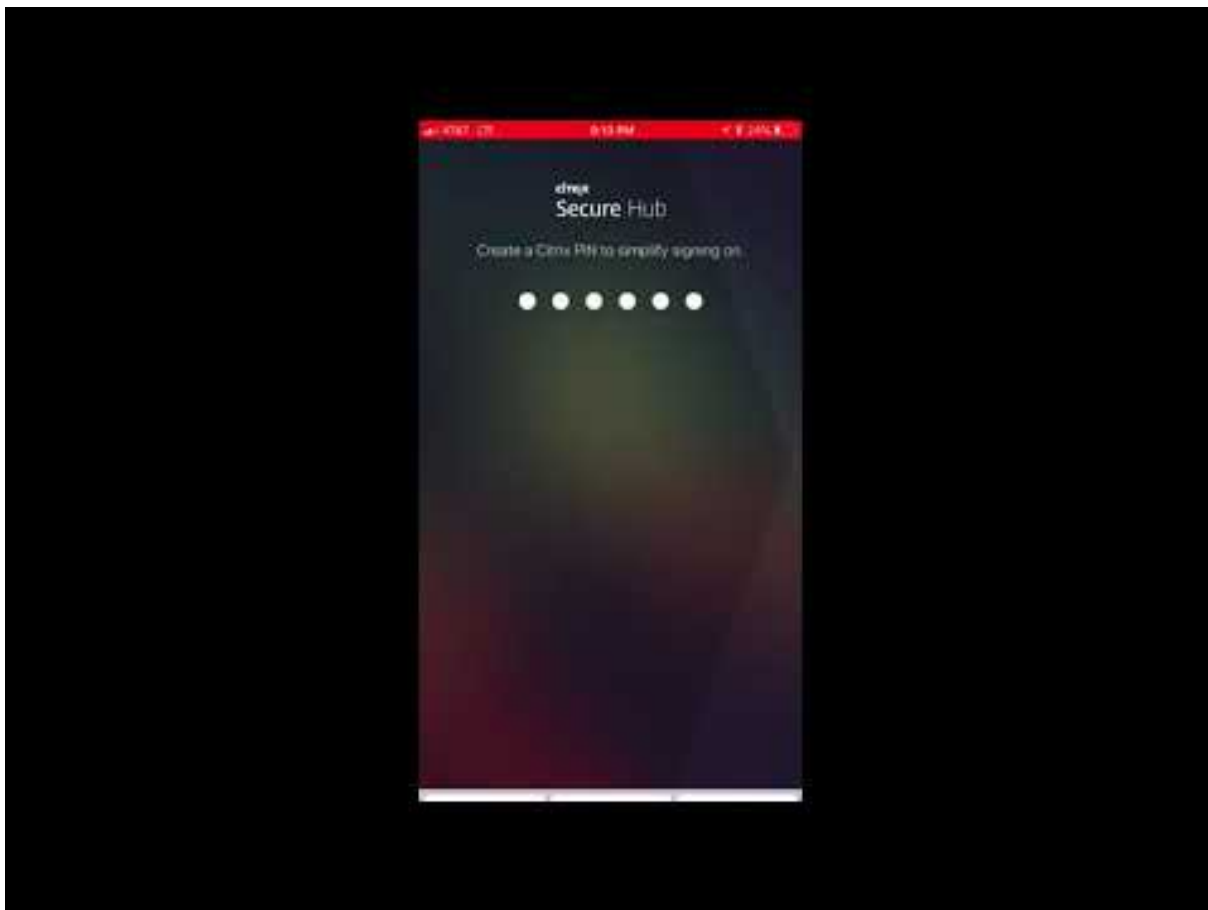
Aplicaciones móviles de productividad: Aplicaciones iOS y Android que proporciona Citrix. Para obtener más información, consulte [Aplicaciones móviles de productividad](#).

Citrix Secure Hub: Para los clientes anteriores a Citrix Endpoint Management 10.18.14, usted envía los parámetros de seguridad, las configuraciones y las aplicaciones móviles a los dispositivos móviles a través de Citrix Secure Hub. Los dispositivos Android y iOS se inscriben en Citrix Endpoint Management a través de Citrix Secure Hub.

Para los clientes nuevos (a partir de Citrix Endpoint Management 10.18.14), Citrix Secure Hub admite el uso del almacén de aplicaciones de Workspace. Al abrir Citrix Secure Hub, los usuarios ya no ven el

almacén de Citrix Secure Hub. Ahora, un botón “Agregar aplicaciones” lleva a los usuarios al almacén de aplicaciones de Workspace.

A continuación dispone de un vídeo donde un dispositivo iOS realiza una inscripción en Citrix Endpoint Management a través de la aplicación Citrix Workspace.



Aplicación Citrix Workspace: 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 ofrece a los usuarios finales una experiencia contextual unificada.

GoToMeeting: Un cliente de reuniones en línea, uso compartido de escritorios y videoconferencias que permite a los usuarios reunirse con clientes, colegas u otros usuarios de equipos a través de Internet en tiempo real.

SalesForce1: Permite a los usuarios acceder a Salesforce desde dispositivos móviles, y reúne todos los procesos de negocio y las aplicaciones personalizadas, Chatter y CRM, en una experiencia unificada para cualquier usuario de Salesforce.

RSA SecurID: Token basado en software para la autenticación de dos factores.

Aplicaciones EpicCare: Estas aplicaciones ofrecen a los profesionales de la salud un acceso seguro y portátil a los gráficos de pacientes, las listas de pacientes, los horarios y los mensajes.

Haiku: Aplicación móvil para teléfonos Android y iPhone.

Canto: Aplicación móvil para el 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 administración electrónica de registros de salud.

ISV:

- **Vocera:** Aplicación móvil de mensajería y VoIP compatible con HIPAA, que extiende las ventajas de la tecnología de voz de Vocera para poder aprovecharlas en cualquier momento y cualquier lugar desde smartphones iPhone y Android.

Aplicaciones internas:

- **HCMail:** Aplicación que ayuda a redactar mensajes cifrados, buscar en las libretas de direcciones en servidores de correo interno y enviar los mensajes cifrados a los contactos mediante un cliente de correo electrónico.

Aplicaciones web internas:

- **PatientRounding:** Aplicación web utilizada para registrar la información sanitaria del paciente por diferentes departamentos.
- **Outlook Web Access:** Permite el acceso al correo electrónico a través de un explorador web.
- **SharePoint:** Se usa para compartir archivos y datos por toda la organización.

En la tabla siguiente, se muestra la información básica necesaria para la configuración de MAM.

Nombre de la aplicación	Tipo de aplicación	Habilitada para		
		MDX	iOS	Android
Citrix Secure Mail	Aplicación móvil de productividad	No	Sí	Sí
Citrix Secure Web	Aplicación móvil de productividad	No	Sí	Sí
Citrix Files	Aplicación móvil de productividad	No	Sí	Sí
Citrix Secure Hub	Aplicación pública	N/D	Sí	Sí
Aplicación Citrix Workspace	Aplicación pública	N/D	Sí	Sí

Nombre de la aplicación	Tipo de aplicación	Habilitada para		
		MDX	iOS	Android
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 de ISV	Sí	Sí	Sí
HCMail	Aplicación interna	Sí	Sí	Sí
PatientRounding	Aplicación web	N/D	Sí	Sí
Outlook Web Access	Aplicación web	N/D	Sí	Sí
SharePoint	Aplicación web	N/D	Sí	Sí

En la siguiente tabla, se ofrece una lista de los requisitos específicos que puede consultar para configurar directivas MAM en Citrix Endpoint Management.

Nombre de la aplicación	Se requiere VPN	Interacción		Filtrado de proxy	Licencias	Geocerca	Mobile Apps SDK	Versión mínima del sistema operativo
		(con aplicaciones fuera del contenedor)	(desde aplicaciones fuera del contenedor)					
Citrix Secure Mail	S	Se permite de manera selectiva	Se permite	Si son necesarias	N/D	Se requiere de manera selectiva	N/D	Se aplica
Citrix Secure Web	S	Se permite	Se permite	Si son necesarias	N/D	No se requiere	N/D	Se aplica
Citrix Files	S	Se permite	Se permite	Si son necesarias	N/D	No se requiere	N/D	Se aplica
Citrix Secure Hub	S	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Aplicación Citrix Workspace	S	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
GoToMeeting	N	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
SalesForce	N	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
RSA SecurID	N	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Haiku	S	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica

Nombre de la aplicación	Se requiere VPN	Interacción		Filtrado de proxy	Licencias	Geocerca	Mobile Apps SDK	Versión mínima del sistema operativo
		(con aplicaciones fuera del contenedor)	(desde aplicaciones fuera del contenedor)					
Epic Canto	S	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Rover	S	N/D	N/D	No se requiere	Compras por volumen	No se requiere	N/D	No se aplica
Epic Hyper-space	S	N/D	N/D	No se requiere	N/D	No se requiere	N/D	No se aplica
Vocera	S	Bloqueada	Bloqueada	Si son necesarias	N/D	Si son necesarias	Si son necesarias	Se aplica
HCMail	S	Bloqueada	Bloqueada	Si son necesarias	N/D	Si son necesarias	Si son necesarias	Se aplica
PatientRound	S	N/D	N/D	Si son necesarias	N/D	No se requiere	N/D	No se aplica
Outlook Web Access	S	N/D	N/D	Si son necesarias	N/D	No se requiere	N/D	No se aplica
SharePoint	S	N/D	N/D	Si son necesarias	N/D	No se requiere	N/D	No se aplica

Comunidades de usuarios

March 1, 2024

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 mediante diversos recursos que usted proporciona a través de los dispositivos móviles de esos usuarios. Los usuarios pueden trabajar desde casa o en oficinas remotas mediante dispositivos móviles que usted proporcione. O bien, los usuarios pueden usar dispositivos móviles personales, lo que les permite acceder a herramientas que están sujetas a ciertas reglas de seguridad.

Con la cantidad creciente de comunidades de usuarios que usan dispositivos móviles, la administración Enterprise Mobility Management (EMM) se ha convertido en un elemento vital para evitar la filtración de datos y para hacer cumplir las restricciones de seguridad de la organización. Para una administración eficiente y más sofisticada de dispositivos móviles, puede categorizar las comunidades de los usuarios. Al hacerlo, se simplifica la asignación de usuarios a los recursos y se garantiza que se apliquen las directivas de seguridad correspondientes a los usuarios indicados.

La categorización de las comunidades de usuarios puede incluir el uso de los siguientes componentes:

- Grupos y unidades organizativas (OU) de Active Directory

Los usuarios agregados a grupos de seguridad de Active Directory específicos pueden recibir recursos tales como aplicaciones y directivas. Quitar usuarios de los grupos de seguridad de Active Directory, elimina el acceso que tenían esos usuarios a los recursos de Citrix Endpoint Management previamente permitidos.

- Grupos y usuarios locales de Citrix Endpoint Management

Para los usuarios que no tienen cuenta de 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 varios grupos de usuarios con diferentes niveles de permisos utilizan una sola aplicación, puede que le interese crear grupos de entrega independientes. Con grupos de entrega independientes, 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 usuario y grupos de entrega

Las asignaciones de grupos de entrega a grupos de Active Directory pueden ser uno a uno, o uno a varios. Asigne aplicaciones y directivas base a grupos de entrega. La asignación puede ser de tipo “de uno a varios”, es decir una aplicación y directiva base se pueden asignar a varios grupos de entrega. Asigne aplicaciones y directivas específicas por función a las asignaciones uno a uno de grupos de entrega.

- Asignación de aplicaciones por recursos y grupos de entrega

Asigne aplicaciones específicas a cada grupo de entrega.

- Asignación de recursos MDM por recursos y grupos de entrega

Asigne aplicaciones y recursos de administración de dispositivos específicos a cada grupo de entrega. Por ejemplo: Configure un grupo de entrega con cualquier combinación de las siguientes acciones: 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 para EMM las comunidades de usuarios de una organización de asistencia sanitaria.

Caso de uso

Esta organización sanitaria de ejemplo ofrece recursos tecnológicos y acceso a varios usuarios, incluidos los voluntarios, los empleados en la red y los empleados asociados. La organización ha decidido aplicar la solución EMM solo para usuarios no ejecutivos.

En esta organización, las funciones y los roles se pueden dividir en estos subgrupos: sanitarios, no sanitarios y contratistas. Un conjunto seleccionado de los usuarios recibe dispositivos móviles de empresa, mientras que otras personas pueden acceder a recursos limitados de la empresa desde sus dispositivos personales (BYOD). Para hacer cumplir el nivel apropiado de restricciones de seguridad y evitar la filtración de datos, la organización decidió que el departamento de TI corporativo administrara cada dispositivo inscrito. Además, los usuarios pueden inscribir un solo dispositivo.

Las siguientes secciones ofrecen una descripción general de los roles y las funciones de cada subgrupo:

Sanitarios

- Enfermeros
- Médicos (doctores, cirujanos, etc.)
- Especialistas (dietistas, anestesiólogos, radiólogos, cardiólogos, oncólogos, etc.)
- Médicos externos (médicos que no son empleados y empleados de oficina que trabajan desde oficinas remotas)
- Servicios de cuidados a domicilio (empleados de oficina y móviles que desempeñan tareas de cuidado sanitario en visitas a domicilio de los pacientes)
- Especialista en investigación (trabajadores intelectuales y usuarios avanzados en seis institutos de investigación que realizan investigaciones clínicas para buscar respuestas a problemas en Medicina)
- Educación y formación (enfermeros, médicos y especialistas en educación y formación)

No sanitarios

- Servicios compartidos (empleados de oficina que realizan varias funciones administrativas, entre ellas: recursos humanos, nóminas, contabilidad, servicio de cadena de suministro, etc.)
- Servicios médicos (empleados de oficina que realizan diversos servicios de administración de cuidados médicos, servicios administrativos y procesos comerciales para proveedores, incluidos: servicios administrativos, análisis e inteligencia empresarial, sistemas de negocio, servicios al cliente, finanzas, gestión de cuidados realizados, soluciones de acceso a pacientes, soluciones de ciclo de ingresos, etc.)
- Servicios de asistencia técnica (empleados de oficina que realizan varias funciones no clínicas, por ejemplo: gestión de ganancias y beneficios, integración clínica, comunicaciones, compensación y gestión del rendimiento, servicios de instalaciones y propiedades, sistemas de tecnología de recursos humanos, servicios de información, auditoría interna y mejora de procesos, etc.)
- Programas filantrópicos (empleados de oficina y móviles que realizan diversas funciones en apoyo a programas filantrópicos)

Contratistas

- Socios de fabricantes y proveedores (in situ y conectados de forma remota a través de la VPN de sitio a sitio, ofrecen varias funciones de asistencia no sanitaria)

En función de la información anterior, la organización crea las siguientes entidades. Para obtener más información acerca de los grupos de entrega en Citrix Endpoint Management, consulte [Implementar recursos](#) en la documentación de producto de Citrix Endpoint Management.

Grupos y unidades organizativas (OU) de Active Directory

Como OU = Recursos de Citrix Endpoint Management:

- OU = Sanitarios; Groups =
 - XM-Enfermería
 - XM-Médicos
 - XM-Especialistas
 - XM-Médicos externos
 - XM-Servicios de cuidados a domicilio
 - XM-Especialista en investigación
 - XM-Educación y formación
- OU = No sanitarios; Groups =

- XM-Servicios compartidos
- XM-Servicios médicos
- XM-Servicios de asistencia técnica
- XM-Programas filantrópicos

Grupos y usuarios locales de Citrix Endpoint Management

Como Group= Contratistas, Users =

- Proveedor1
- Proveedor2
- Proveedor3
- ...Proveedor10

Grupos de entrega de Citrix Endpoint Management

- Sanitario-Enfermeros
- Sanitario-Médicos
- Sanitario-Especialistas
- Sanitario-Médicos externos
- Sanitario-Servicios de cuidados a domicilio
- Sanitario-Especialista en investigación
- Sanitario-Educación y formación
- No-Sanitario-Servicios compartidos
- No-Sanitario-Servicios médicos
- No-Sanitario-Servicios de asistencia técnica
- No-Sanitario-Programas filantrópicos

Asignación de grupos de usuario y grupos de entrega

	Grupos de entrega de Citrix Endpoint Management
Usar grupos de Active Directory	
XM-Enfermería	Sanitario-Enfermeros
XM-Médicos	Sanitario-Médicos
XM-Especialistas	Sanitario-Especialistas
XM-Médicos externos	Sanitario-Médicos externos
XM-Servicios de cuidados a domicilio	Sanitario-Servicios de cuidados a domicilio

Usar grupos de Active Directory	Grupos de entrega de Citrix Endpoint Management
XM-Especialista en investigación	Sanitario-Especialista en investigación
XM-Educación y formación	Sanitario-Educación y formación
XM-Servicios compartidos	No-Sanitario-Servicios compartidos
XM-Servicios médicos	No-Sanitario-Servicios médicos
XM-Servicios de asistencia técnica	No-Sanitario-Servicios de asistencia técnica
XM-Programas filantrópicos	No-Sanitario-Programas filantrópicos

Asignación de aplicaciones por recursos y grupos de entrega

	Secure Mail	Secure Web	Citrix Files	Aplicación Work-space	RSA SecurID SalesForce	EpicCare Haiku	Epic Hyper-space
Sanitario- Enfermeros	X	X	X				
Sanitario- Médicos							
Sanitario- Especialistas							
Sanitario- Médicos externos	X		X				
Sanitario- Servicios de cuida- dos a domi- cilio	X		X				
Sanitario- Especialista en inves- tigación	X		X				

	Secure Mail	Secure Web	Citrix Files	Aplicación Work-space	SalesForce	RSA SecurID	EpicCare Haiku	Epic Hyper-space
Sanitario-Educación y forma-ción							X	X
No-Sanitario-Servicios compa-rtidos							X	X
No-Sanitario-Servicios médicos							X	X
No-Sanitario-Servicios de asis-tencia técnica	X		X				X	X
No-Sanitario-Programas fi-lantrópi-cos	X		X				X	X
Contratista	X		X	X	X		X	X

Asignación de recursos MDM por recursos y grupos de entrega

	MDM: Directiva de código de acceso	MDM: Restricciones de dispositivo	MDM: Acciones automatizadas	MDM: Directiva de redes
Sanitario-Enfermeros				X

	MDM: Directiva de código de acceso	MDM: Restricciones de dispositivo	MDM: Acciones automatizadas	MDM: Directiva de redes
Sanitario- Médicos Sanitario- Especialistas Sanitario- Médicos externos Sanitario- Servicios de cuidados a domicilio Sanitario- Especialista en investigación Sanitario- Educación y formación No-Sanitario- Servicios compartidos No-Sanitario- Servicios médicos No-Sanitario- Servicios de asistencia técnica No-Sanitario- Programas filantrópicos Contratistas		X		X

Notas y consideraciones

- Citrix Endpoint Management crea un grupo de entrega predeterminado llamado AllUsers (Todos los usuarios) durante la configuración inicial. Si no inhabilita este grupo de entrega, todos los usuarios de Active Directory tendrán derecho a inscribirse en Citrix Endpoint Management.

- Citrix Endpoint Management sincroniza los grupos y los usuarios de Active Directory a demanda mediante una conexión dinámica al servidor LDAP.
- Si un usuario forma parte de un grupo que no está asignado en Citrix Endpoint Management, dicho usuario no podrá inscribirse. Del mismo modo, si un usuario es miembro de varios grupos, Citrix Endpoint Management solo clasifica al usuario como perteneciente a los grupos asignados a Citrix Endpoint Management.

Estrategia de correo electrónico

March 1, 2024

El acceso seguro al correo electrónico desde dispositivos móviles es uno de los motivos principales detrás de una iniciativa de administración de la movilidad en todas las organizaciones. Decidir la estrategia de correo electrónico adecuada suele ser un componente clave a la hora de diseñar elementos en Citrix Endpoint Management. Citrix Endpoint Management ofrece varias opciones para adaptarse a diferentes casos de uso, en función de la seguridad, la experiencia de usuario y los requisitos de integración. En este artículo se documenta el proceso de toma de decisiones sobre un diseño típico y se indican criterios para elegir la solución adecuada, desde la selección del cliente hasta el flujo del tráfico de correo.

Elegir los clientes de correo electrónico

Generalmente, la elección de un cliente encabeza la lista a la hora de diseñar la estrategia a seguir para el correo electrónico. Puede elegir entre varios clientes: Citrix Secure Mail, el correo nativo que se incluye con el sistema operativo de la plataforma móvil en cuestión, o bien otros clientes de terceros, disponibles a través de las tiendas públicas de aplicaciones. En función de sus necesidades, puede ofrecer soporte a comunidades de usuarios con un solo cliente (estándar) o puede que necesite usar una combinación de clientes.

En la siguiente tabla se describen algunos criterios de diseño para las diferentes opciones de cliente disponibles:

Temática	Citrix Secure Mail	Nativo (por ejemplo, iOS Mail)	Correo de terceros
----------	--------------------	--------------------------------	--------------------

Configuración	Perfiles de cuentas de Exchange configurados a través de una directiva MDX.	Perfiles de cuenta de Exchange configurados a través de una directiva MDM. La compatibilidad con Android está limitada a: Android Enterprise. Todos los demás clientes se consideran clientes de terceros.	Generalmente requiere una configuración manual por parte del usuario.
Seguridad	Seguro gracias a su diseño, con lo que proporciona la seguridad más alta. Utiliza directivas MDX con niveles agregados de cifrado de datos. Citrix Secure Mail es una aplicación administrada totalmente a través de una directiva MDX. Capa agregada de autenticación con el PIN de Citrix.	Según el conjunto de funciones del proveedor o la aplicación. Proporciona más seguridad. Utiliza los parámetros de cifrado de dispositivos. Se basa en la autenticación a nivel de dispositivo para acceder a la aplicación.	Según el conjunto de funciones del proveedor o la aplicación. Proporciona alta seguridad.

Integración	Permite la interacción con aplicaciones administradas (MDX) de forma predeterminada. Permite abrir direcciones URL con Citrix Secure Web. Guardar archivos y adjuntarlos desde Citrix Files. Unirse directamente o acceder por teléfono a reuniones en GoToMeeting.	Solo puede interactuar con otras aplicaciones no administradas (que no sean MDX) de forma predeterminada.	Solo puede interactuar con otras aplicaciones no administradas (que no sean MDX) de forma predeterminada.
Implementación o Licencias	Puede enviar Citrix Secure Mail a través de MDM, directamente desde las tiendas públicas de aplicaciones. Incluido con las licencias Citrix Endpoint Management Advanced y Enterprise.	La aplicación del cliente, incluida con el sistema operativo de la plataforma. Sin requisitos de licencia adicionales.	Puede enviarse a través de MDM, como una aplicación de empresa o directamente desde las tiendas públicas de aplicaciones. Costes o modelos de licencia asociados según el proveedor de la aplicación.

Asistencia	Soporte del proveedor único para el cliente y la solución de EMM (Citrix). Información de contacto de asistencia integrada en las capacidades del registro de depuración en Citrix Secure Hub o la aplicación. Un cliente al que ofrecer soporte.	Soporte definido por el proveedor (Apple o Google). Puede que necesite ofrecer soporte a diferentes clientes, según la plataforma del dispositivo.	Soporte definido por el proveedor. Un cliente al que ofrecer soporte, suponiendo que el cliente de terceros es compatible con todas las plataformas de los dispositivos administrados.
------------	---	--	--

Consideraciones sobre el filtrado y el flujo del tráfico de correo

En esta sección se tratan los tres casos principales y las consideraciones sobre el diseño con respecto al flujo del tráfico de correo (ActiveSync) en el contexto de Citrix Endpoint Management.

Caso 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 por esta ruta externa a través de un proxy inverso (por ejemplo, NetScaler Gateway) o a través de un servidor perimetral. Esta opción es necesaria para usar clientes de correo nativos o de terceros, con lo que estos clientes se convierten en la elección típica en este caso. Aunque sea poco frecuente, también puede usar el cliente de Citrix Secure Mail en este caso. Al hacerlo, aprovecha las funciones de seguridad que ofrecen el uso de las directivas MDX y la administración de la aplicación.

Caso 2: Túnel a través de NetScaler Gateway (micro VPN y STA)

Este es el caso predeterminado cuando se utiliza el cliente de Citrix Secure Mail, debido a sus capacidades de micro VPN. En este caso, el cliente de Citrix Secure Mail establece una conexión segura con ActiveSync a través de NetScaler Gateway. Básicamente, puede considerar Citrix Secure Mail como el cliente que se conecta directamente a ActiveSync desde la red interna. Los clientes de Citrix suelen usar Citrix Secure Mail como el cliente móvil preferido para ActiveSync. Esa decisión forma parte de

una iniciativa para evitar exponer los servicios de ActiveSync a Internet en un servidor Exchange ya expuesto (primer caso descrito).

Solo las aplicaciones habilitadas para el SDK de MAM o empaquetadas con MDX pueden usar la función micro VPN. Este supuesto no es aplicable a los clientes nativos si se utiliza el empaquetado con MDX. Aunque es posible empaquetar clientes de terceros con el MDX Toolkit, no es frecuente. El uso de clientes VPN a nivel de dispositivo para permitir el acceso por túnel a clientes nativos o de terceros ha resultado ser engorroso y no es una solución viable.

Caso 3: Servicios de Exchange alojados en la nube

El uso de los servicios de Exchange alojados en la nube, como Microsoft Office 365, está cada vez más extendido. En el contexto de Citrix Endpoint Management, este caso se puede tratar de la misma manera que el primero, porque aquí el servicio ActiveSync también está expuesto a Internet. En este caso, los requisitos del proveedor de servicios en la nube dictan las opciones del cliente. Las opciones suelen ser compatibles con la mayoría de los clientes ActiveSync, como Citrix Secure Mail y otros clientes nativos o de terceros.

Citrix Endpoint Management puede agregar valor en tres áreas de este caso:

- Clientes con directivas MDX y administración de aplicaciones con Citrix Secure Mail
- Configuración de clientes con una directiva MDM en clientes de correo nativos admitidos
- Opciones de filtrado de ActiveSync mediante el conector de Citrix Endpoint Management para Exchange ActiveSync

Consideraciones sobre el filtrado del tráfico de correo

Al igual que con la mayoría de los servicios expuestos a Internet, debe proteger la ruta y proporcionar filtros para el acceso autorizado. La solución Citrix Endpoint Management incluye dos componentes diseñados específicamente para proporcionar las capacidades de filtrado de ActiveSync a 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 ofrece el filtrado de ActiveSync en el perímetro, mediante NetScaler Gateway como proxy para el tráfico de ActiveSync. Así, el componente de filtrado se encuentra en la ruta de tráfico del correo: lo intercepta 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 servicio de connector for Exchange ActiveSync. Ese servicio verifica el estado del dispositivo a través de Citrix Endpoint Management. El componente connector for Exchange ActiveSync responde a NetScaler Gateway en función del estado del dispositivo, para permitir o denegar la conexión. También se pueden configurar reglas estáticas para filtrar el acceso en función del usuario, el agente, el ID o el tipo de dispositivo.

Esta configuración permite que los servicios Exchange ActiveSync se expongan a Internet con una capa adicional de seguridad para evitar el acceso no autorizado. En las consideraciones sobre el diseño se incluye:

- **Servidor de Windows:** El componente del conector para Exchange ActiveSync requiere un servidor de 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 un grupo de Active Directory, por ejemplo. Si hay un requisito para el filtrado por grupos de Active Directory, puede usar el conector de Citrix Endpoint Management para Exchange ActiveSync en su lugar.
- **Escalabilidad de NetScaler Gateway:** Dado el requisito de proxy para el tráfico de ActiveSync a través de NetScaler Gateway, un tamaño adecuado de la instancia de NetScaler Gateway es fundamental para admitir la carga de trabajo adicional de todas las conexiones SSL de ActiveSync.
- **Almacenamiento en caché integrado de NetScaler Gateway:** La configuración del conector para Exchange ActiveSync en NetScaler Gateway utiliza la función “Almacenamiento en caché integrado” para almacenar en caché las respuestas del conector. Como resultado de esa configuración, NetScaler Gateway no necesita emitir una solicitud al conector para cada transacción de ActiveSync en una sesión determinada. Esa configuración también es vital para un rendimiento y una escala adecuados. El almacenamiento en caché integrado está disponible con la edición NetScaler Gateway Platinum.
- **Directivas de filtrado personalizadas:** Puede que necesite crear directivas personalizadas de NetScaler Gateway para restringir algunos clientes de ActiveSync que no sean los clientes móviles nativos estándar. Esta configuración requiere conocimiento sobre las solicitudes HTTP de ActiveSync y la creación de directivas del respondedor de NetScaler Gateway.
- **Clientes de Citrix Secure Mail:** Citrix Secure Mail ofrece redes micro VPN, que eliminan la necesidad de filtros en el perímetro. Por regla general, el cliente de Citrix Secure Mail se trataría 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 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 ofrece el filtrado de ActiveSync en el nivel de servicio de Exchange. Así, el filtrado solo se produce una vez que el correo haya llegado al servicio de intercambio, en lugar de en cuanto entre en el entorno de Citrix Endpoint Management. Mail Manager utiliza PowerShell para consultar Exchange ActiveSync cuando busca información de asociación de dispositivos y para controlar el acceso a través de acciones de cuarentena de dispositivos. Estas acciones ponen los dispositivos en cuarentena, y los sacan de ella, en función de 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 en función de la conformidad del dispositivo. También se pueden configurar reglas estáticas para filtrar el acceso en función del ID o el tipo de dispositivo, la versión del agente y la pertenencia al grupo de Active Directory.

Esta solución no requiere el uso de NetScaler Gateway. Puede implementar el conector para Exchange ActiveSync sin cambiar el enrutamiento para el tráfico de ActiveSync existente. En las consideraciones sobre el diseño se incluye:

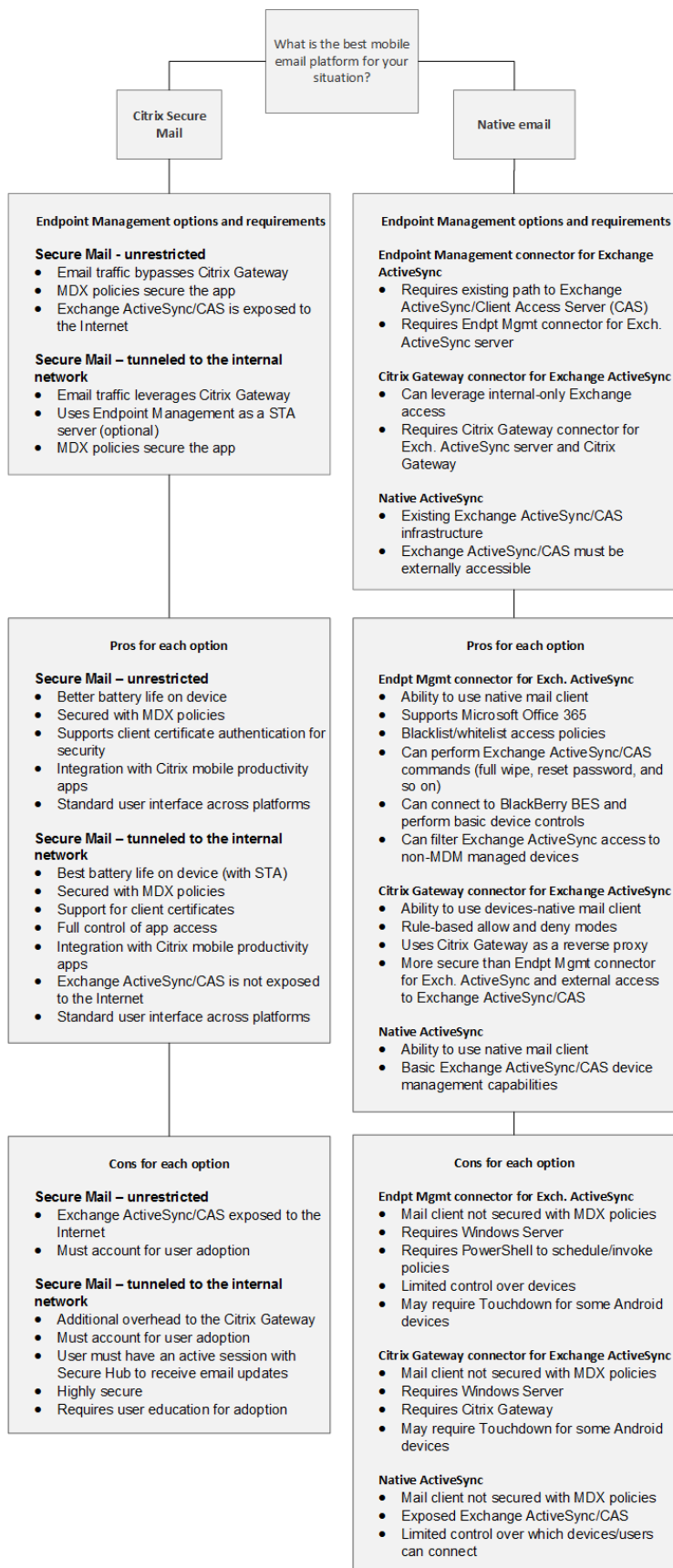
- **Servidor Windows:** El conector para Exchange ActiveSync requiere la implementación de un servidor Windows Server.
- **Conjunto de reglas de filtrado:** Al igual que el conector de NetScaler Gateway para Exchange ActiveSync, el conector para Exchange ActiveSync incluye reglas de filtrado para evaluar el estado del dispositivo. Además, el conector para Exchange ActiveSync también admite reglas estáticas para filtrar según la pertenencia al grupo de Active Directory.
- **Integración en Exchange:** El conector para Exchange ActiveSync requiere acceso directo al servidor de acceso de cliente (CAS) de Exchange que aloja el rol de ActiveSync y controla las acciones de cuarentena del dispositivo. Este requisito puede ser un problema dependiendo de la arquitectura del entorno y las indicaciones de seguridad. Es fundamental que evalúe este requisito técnico por adelantado.
- **Otros clientes de ActiveSync:** Como el conector para Exchange ActiveSync filtra en el nivel de servicio de ActiveSync, tenga en cuenta otros clientes de ActiveSync fuera del entorno de Citrix Endpoint Management. Puede configurar reglas estáticas del conector para Exchange ActiveSync si quiere evitar un impacto involuntario sobre otros clientes de ActiveSync.
- **Funciones extendidas de Exchange:** A través de la integración directa en Exchange ActiveSync, el conector para Exchange ActiveSync ofrece la capacidad de que Citrix Endpoint Management

borre los datos de Exchange ActiveSync que haya en un dispositivo móvil. El conector para Exchange ActiveSync también permite que Citrix Endpoint Management acceda a información sobre dispositivos BlackBerry y realice 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 decisiones sobre la plataforma de correo electrónico

La siguiente imagen tiene por objetivo facilitar la distinción entre las ventajas y las desventajas que ofrecen las soluciones de correo electrónico nativas o Citrix Secure Mail en su implementación de Citrix Endpoint Management. Cada opción implica que las opciones y los requisitos de Citrix Endpoint Management asociados permitan el acceso al servidor, la red y la base de datos. En los criterios de pros y contras se incluyen detalles sobre seguridad, directivas e interfaz de usuario.



Integrar Citrix Endpoint Management

March 1, 2024

En este artículo se describen los elementos a tener en cuenta al planificar cómo se integra Citrix Endpoint Management en su red y sus soluciones existentes. Por ejemplo, si ya está utilizando NetScaler Gateway para Citrix Virtual Apps and Desktops:

- ¿Quiere utilizar la instancia existente de NetScaler Gateway o una nueva instancia dedicada?
- ¿Quiere integrar en Citrix Endpoint Management las aplicaciones HDX que se han publicado mediante StoreFront?
- ¿Va a 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

Se necesita NetScaler Gateway para Citrix Endpoint Management. NetScaler Gateway proporciona una ruta de red micro VPN para acceder a todos los recursos de empresa. Asimismo, ofrece un respaldo sólido a la autenticación de varios factores.

Puede usar instancias existentes de NetScaler Gateway o configurar nuevas para Citrix Endpoint Management. En las secciones siguientes se indican las ventajas y las desventajas de utilizar las instancias de NetScaler Gateway existentes o unas instancias nuevas dedicadas.

NetScaler Gateway MPX compartido con una dirección IP virtual de NetScaler Gateway creada 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; por ejemplo, para la autenticación con certificados y para acceder a servicios como DNS, LDAP y NTP.
- Utiliza una sola licencia de plataforma NetScaler Gateway.

Desventajas:

- Es más difícil planificar la escalabilidad cuando se enfrenta a dos casos de uso diferentes en el mismo NetScaler Gateway.

- A veces necesita una versión concreta de NetScaler Gateway para un caso de uso de Citrix Virtual Apps. Sin embargo, esa misma versión podría presentar problemas conocidos en Citrix Endpoint Management. O Citrix Endpoint Management podría presentar problemas conocidos para la versión de NetScaler Gateway.
- Si ya existe un NetScaler Gateway, no puede ejecutar el asistente de NetScaler para XenMobile por segunda vez para crear la configuración de NetScaler Gateway para Citrix Endpoint Management.
- Excepto cuando se usan licencias Platinum para NetScaler Gateway 11.1 o posterior, se agrupan las licencias de acceso de usuario instaladas en NetScaler Gateway, necesarias para la conectividad VPN. Puesto que esas licencias están disponibles para todos los servidores virtuales de NetScaler Gateway, unos servicios que no sean de Citrix Endpoint Management pueden potencialmente consumirlas.

Instancia dedicada de NetScaler Gateway VPX o MPX

Ventajas:

Citrix recomienda usar una instancia dedicada de NetScaler Gateway.

- Es más fácil planear la escalabilidad en ella. Además, así el tráfico de Citrix Endpoint Management se separa de una instancia de NetScaler Gateway que podría ya tener restricciones de recursos.
- Evita los problemas que pueden surgir cuando Citrix Endpoint Management y Citrix Virtual Apps necesitan diferentes versiones de software de NetScaler Gateway. Por lo general, es mejor utilizar la versión y la compilación más recientes de NetScaler Gateway compatibles con Citrix Endpoint Management.
- Permite configurar NetScaler Gateway para Citrix Endpoint Management gracias al asistente integrado de NetScaler para XenMobile.
- Separación virtual y física de servicios.

Desventajas:

- Requiere la instalación y la configuración de servicios adicionales en NetScaler Gateway para admitir la configuración de Citrix Endpoint Management.
- Requiere otra licencia de plataforma de NetScaler Gateway. Cada instancia de NetScaler Gateway deberá disponer de una licencia para NetScaler Gateway.

Para obtener información sobre qué tener en cuenta a la hora de integrar NetScaler Gateway y Citrix ADC para los modos de administración de Citrix Endpoint Management, consulte [Integración en NetScaler Gateway y Citrix ADC](#).

StoreFront

Si tiene un entorno de Citrix Virtual Apps and Desktops, puede usar StoreFront para integrar aplicaciones HDX en Citrix Endpoint Management. Cuando integra aplicaciones HDX en Citrix Endpoint Management:

- Las aplicaciones están disponibles para los usuarios que están inscritos en Citrix Endpoint Management.
- Las aplicaciones se muestran en el almacén de aplicaciones junto con otras aplicaciones móviles.
- Citrix Endpoint Management utiliza Citrix Receiver en StoreFront.
- Si la aplicación Citrix Workspace está instalada en un dispositivo, las aplicaciones HDX comienzan a usarla.

StoreFront presenta una limitación de un sitio de servicio por instancia de StoreFront. Supongamos que tiene varios almacenes y quiere separarlos de otro uso de producción. En ese caso, Citrix recomienda generalmente que se plantee un nuevo sitio de servicios y una nueva instancia de StoreFront para Citrix Endpoint Management.

Plantéese lo siguiente:

- ¿Hay algún requisito de autenticación diferente para StoreFront? El sitio de servicios de StoreFront requiere credenciales de Active Directory para el inicio de sesión. Los clientes que solo usan la autenticación basada en certificados no pueden enumerar las aplicaciones a través de Citrix Endpoint Management mediante el mismo NetScaler Gateway.
- ¿Usar el mismo almacén o crear otro?
- ¿Usar el mismo servidor de StoreFront o no?

En las siguientes secciones se indican las ventajas y las desventajas de utilizar almacenes de StoreFront separados o combinados para Citrix Workspace y las aplicaciones móviles de productividad Citrix.

Integrar la instancia existente de StoreFront en Citrix Endpoint Management

Ventajas:

- Mismo almacén: No se requiere configuración adicional de StoreFront para Citrix Endpoint Management, suponiendo que utilice la misma dirección IP virtual de NetScaler Gateway para el acceso HDX. Supongamos que elige usar el mismo almacén y quiere dirigir el acceso de Citrix Workspace a una nueva dirección IP virtual de NetScaler Gateway. En ese caso, agregue la configuración apropiada de NetScaler Gateway a StoreFront.
- Mismo servidor de StoreFront: Utiliza la instalación y la configuración del StoreFront existente.

Desventajas:

- Mismo almacén: Cualquier cambio en la configuración de StoreFront para admitir las cargas de trabajo de Citrix Virtual Apps and Desktops puede afectar negativamente a Citrix Endpoint Management.
- Mismo servidor de StoreFront: En entornos grandes, tenga en cuenta la carga adicional que provocará el uso de Citrix Receiver por parte de Citrix Endpoint Management para la enumeración y el inicio de las aplicaciones.

Usar una instancia nueva y dedicada de StoreFront para la integración en Citrix Endpoint Management

Ventajas:

- Nuevo almacén: Ningún cambio en la configuración del almacén de StoreFront para Citrix Endpoint Management afecta a las cargas de trabajo existentes de Citrix Virtual Apps and Desktops.
- Nuevo servidor de StoreFront: Los cambios en la configuración del servidor no afectan a los flujos de trabajo de Citrix Virtual Apps and Desktops. Además, la carga no derivada del uso de Citrix Receiver por parte de Citrix Endpoint Management para la enumeración y el inicio de aplicaciones no afecta a la escalabilidad.

Desventajas:

- Nuevo almacén: Configuración del almacén StoreFront.
- Nuevo servidor de 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

ShareFile permite intercambiar documentos de forma fácil y segura, enviar documentos grandes por correo electrónico y manejar de forma segura 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 Single Sign-On para los usuarios de las aplicaciones móviles de productividad.
- Aprovisionamiento de cuentas de usuario basado en Active Directory.
- Directivas integrales para controlar el acceso.

Los usuarios móviles pueden aprovechar el conjunto completo de funciones de la cuenta Enterprise.

De forma alternativa, puede configurar Citrix Endpoint Management para que se integre solamente en conectores de zonas de almacenamiento. A través de conectores de zonas de almacenamiento, Citrix Files proporciona acceso a:

- Documentos y carpetas
- Recursos compartidos de red
- En sitios de SharePoint: Colecciones de sitios y bibliotecas de documentos.

Los recursos compartidos conectados pueden incluir las mismas unidades “home” de red utilizadas en entornos de Citrix Virtual Apps and Desktops. Puede utilizar la consola de Citrix Endpoint Management para configurar la integración en cuentas Enterprise o conectores de zonas de almacenamiento. Para obtener más información, consulte [Citrix Files para Citrix Endpoint Management](#).

En las siguientes secciones se indican las preguntas a contestar cuando se decide el diseño de Citrix Files.

Integrar en Citrix Files o solo en conectores de zonas de almacenamiento

Preguntas que debe hacer:

- ¿Necesita almacenar datos en las zonas de almacenamiento que administra Citrix?
- ¿Quiere ofrecer a los usuarios funciones de intercambio y sincronización de archivos?
- ¿Quiere que los usuarios puedan acceder a los archivos que se encuentran en el sitio web de Citrix Files? ¿O que puedan acceder al contenido de Office 365 y los conectores de nube personal desde dispositivos móviles?

Decisión de diseño:

- Si la respuesta a alguna de esas preguntas es «sí», integre en una cuenta Enterprise.
- Una integración en solo conectores de zonas de almacenamiento permite a los usuarios iOS un acceso móvil seguro a repositorios de almacenamiento locales existentes, como sitios de SharePoint y recursos compartidos de archivos de red. En esta configuración no se requiere configurar ningún subdominio de Citrix Files, aprovisionar usuarios a Citrix Files ni alojar datos de Citrix Files. El uso de conectores de zonas de almacenamiento con Citrix Endpoint Management cumple las restricciones de seguridad contra la filtración de datos del usuario fuera de la red corporativa.

Ubicación de los servidores de controladores de zonas de almacenamiento

Preguntas que debe hacer:

- ¿Necesita almacenamiento local o funciones como conectores de zonas de almacenamiento?
- Si usa las 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 de los controladores de las zonas de almacenamiento en la nube de Citrix Files, en su sistema local de almacenamiento de arrendatarios individuales o en un almacenamiento en la nube de terceros compatible.
- Los controladores de zonas de almacenamiento requieren acceso a Internet para comunicarse con el plano de control de Citrix Files. Puede conectarse de varias formas, incluido el acceso directo o las configuraciones NAT/PAT.

Conectores de zonas de almacenamiento

Preguntas que debe hacer:

- ¿Cuáles son las rutas a recursos CIFS?
- ¿Cuáles son las URL de SharePoint?

Decisión de diseño:

- Determine si son necesarios unos controladores de zonas de almacenamiento locales para acceder a esas ubicaciones.
- Debido a la comunicación del controlador de zonas de almacenamiento con recursos internos (como repositorios de archivos, recursos CIFS y SharePoint), Citrix recomienda que esos controladores residan en la red interna, detrás de los firewalls DMZ y de NetScaler Gateway.

Integrar SAML en Citrix Endpoint Management

Preguntas que debe hacer:

- ¿Se requiere la autenticación de Active Directory para Citrix Files?
- ¿Usar la aplicación Citrix Files por primera vez para Citrix Endpoint Management requiere SSO?
- ¿Hay un proveedor de identidades estándar en el entorno actual?
- ¿Cuántos dominios se requieren para usar SAML?
- ¿Hay varios alias de correo electrónico para los usuarios de Active Directory?
- ¿Hay alguna migración de dominio de Active Directory en curso o programada próximamente?

Decisión de diseño:

Puede elegir utilizar SAML como mecanismo de autenticación para Citrix Files. Las opciones de autenticación son:

- Utilizar el servidor Citrix Endpoint Management como el 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 Single Sign-On para las aplicaciones móviles.

El servidor Citrix Endpoint Management se ha mejorado para este proceso, ya que no requiere la sincronización con Active Directory.

Usar la herramienta Citrix Files User Management Tool para el aprovisionamiento de usuarios.

- Usar un proveedor de terceros compatible en calidad de IdP para SAML

Si tiene un IdP existente compatible y no requiere capacidades SSO para aplicaciones móviles, esta puede ser la opción más adecuada. Esta opción también requiere la herramienta Citrix Files User Management Tool para el aprovisionamiento de cuentas.

Usar soluciones IdP de terceros, como ADFS, también puede proporcionar SSO en el lado del cliente Windows. Debe valorar los casos de uso antes de elegir su IdP SAML para Citrix Files.

- O bien, para satisfacer ambos casos de uso, consulte la [ShareFile single sign-on configuration guide for dual identity providers](#).

Aplicaciones móviles

Preguntas que debe hacer:

- ¿Qué aplicación móvil de Citrix Files va a usar (pública, MDM, MDX)?

Decisión de diseño:

- Puede distribuir las aplicaciones móviles de productividad Citrix desde Apple App Store y la tienda de Google Play. Con esa distribución desde el tienda pública de aplicaciones, se obtienen aplicaciones empaquetadas desde la página Descargas de Citrix.
- Si sus requisitos de seguridad son bajos y no necesita utilizar contenedores, puede que la aplicación pública Citrix Files no sea la adecuada.
- Para obtener más información, consulte [Aplicaciones y Citrix Files para Citrix Endpoint Management](#).

Seguridad, directivas y control de acceso

Preguntas que debe hacer:

- ¿Qué restricciones necesita para usuarios móviles, Web y de escritorio?

- ¿Qué configuración estándar quiere para controlar el acceso de los usuarios?
- ¿Qué directiva de retención de archivos va a usar?

Decisión de diseño:

- Citrix Files le permite administrar los permisos de los empleados. Para obtener más información, consulte [Employee Permissions](#).
- Determinadas directivas MDX y configuraciones de Citrix Files para la seguridad del dispositivo controlan las mismas funciones. En esos casos, tienen prioridad las directivas de Citrix Endpoint Management, seguidas de las configuraciones de Citrix Files para la seguridad de los dispositivos. Ejemplos: Si inhabilita aplicaciones externas en Citrix Files, pero las habilita en Citrix Endpoint Management, las aplicaciones externas se inhabilitan en Citrix Files. Puede configurar las aplicaciones para que Citrix Endpoint Management no requiera PIN o código de acceso, pero la aplicación Citrix Files los requiere.

Zonas de almacenamiento estándar o restringidas

Preguntas que debe hacer:

- ¿Necesita zonas de almacenamiento restringidas?

Decisión de diseño:

- Una zona de almacenamiento estándar está diseñada para almacenar datos no confidenciales, y permite a los empleados compartir datos con otras personas ajenas a la empresa. En esta opción se admiten flujos de trabajo que implican compartir datos fuera del dominio.
- Una zona de almacenamiento restringida protege datos confidenciales, por lo que solo los usuarios de dominio autenticados pueden acceder a los datos almacenados en estas zonas.

Control de acceso

Las empresas pueden administrar dispositivos móviles dentro y fuera de las redes. Las soluciones de administración de la movilidad empresarial (como Citrix Endpoint Management) son excelentes para proporcionar la seguridad de los dispositivos móviles y control sobre ellos, independientemente de dónde estén ubicados. Sin embargo, cuando esas soluciones se combinan con una solución de control de acceso a la red (NAC), puede agregar QoS y un control más preciso a los dispositivos internos de su red. Esa combinación permite extender la evaluación de la seguridad de los dispositivos Citrix Endpoint Management a través de la solución NAC. La solución NAC puede usar la evaluación de seguridad de Citrix Endpoint Management para facilitar y gestionar las decisiones de autenticación.

Puede utilizar cualquiera de estas soluciones para aplicar directivas de NAC:

- NetScaler Gateway

- ForeScout

Citrix no garantiza la integración de otras soluciones NAC.

Ventajas de integrar una solución NAC en Citrix Endpoint Management:

- Una seguridad, conformidad y control mejores para todos los dispositivos de punto final en una red empresarial.
- Una solución NAC puede:
 - Detectar dispositivos en el instante en que intentan conectarse a la red.
 - Enviar consultas a Citrix Endpoint Management sobre los atributos de los dispositivos.
 - Luego, usar esa información para determinar si permitir, bloquear, limitar o redirigir esos dispositivos. Esas decisiones dependen de las directivas de seguridad que elija aplicar.
- Una solución NAC ofrece a los administradores de TI una visión que engloba dispositivos no administrados y no conformes.

Para obtener una descripción de los filtros de conformidad de NAC que admite Citrix Endpoint Management y una introducción a la configuración, consulte [Control de acceso de red](#).

Integración en NetScaler Gateway y Citrix ADC

March 1, 2024

Cuando se integra en Citrix Endpoint Management, NetScaler Gateway ofrece un mecanismo de autenticación para que dispositivos MAM remotos accedan a la red interna. Esta integración permite a las aplicaciones móviles de productividad Citrix conectarse a los servidores de empresa ubicados en la intranet a través de una red micro VPN. Porque Citrix Endpoint Management crea una micro VPN que se extiende desde las aplicaciones presentes en el dispositivo hasta NetScaler Gateway. NetScaler Gateway proporciona una ruta de red micro VPN para acceder a todos los recursos de empresa. Asimismo, ofrece un respaldo sólido a la autenticación de varios factores.

Cuando un usuario abandona la inscripción MDM, los dispositivos se inscriben mediante el FQDN de NetScaler Gateway.

Citrix Cloud Operations administra el equilibrio de carga de Citrix ADC.

Decisiones en cuanto a diseño

En las secciones siguientes, se resumen las diversas decisiones de diseño a considerar durante la planificación de una integración de NetScaler Gateway en Citrix Endpoint Management.

Certificados

Detalles de la decisión:

- ¿Necesita mayor grado de seguridad para la inscripción y el acceso al entorno de Citrix Endpoint Management?
- ¿LDAP no es una opción?

Guía de diseño:

En Citrix Endpoint Management, la autenticación predeterminada es el nombre de usuario y la contraseña. Para agregar otra capa de seguridad para la inscripción y el acceso al entorno de Citrix Endpoint Management, considere la posibilidad de usar la autenticación basada en certificados. Puede usar certificados con LDAP para la autenticación de dos factores, lo que proporciona un grado mayor de seguridad sin necesidad de un servidor RSA.

Si no permite LDAP y usa tarjetas inteligentes o métodos similares, la configuración de los certificados permite representar una tarjeta inteligente en Citrix Endpoint Management. Los usuarios se inscriben mediante un PIN único que Citrix Endpoint Management genera para ellos. Una vez que el usuario haya obtenido acceso, Citrix Endpoint Management crea e implementa el certificado utilizado más adelante a partir de entonces para autenticarse en el entorno de Citrix Endpoint Management.

Citrix Endpoint Management solo admite la lista de revocación de certificados (CRL) cuando se trata de una entidad de certificación (CA) de terceros. Si dispone de una entidad de certificación de Microsoft configurada, Citrix Endpoint Management utiliza NetScaler Gateway para administrar la revocación. Al configurar la autenticación por certificados de cliente, plantéese si es necesario configurar el parámetro de lista de revocación de certificados (CRL) de NetScaler Gateway, **Enable CRL Auto Refresh**. Este paso garantiza que el usuario de un dispositivo inscrito en MAM solo no pueda autenticarse con un certificado existente en el dispositivo. Citrix Endpoint Management vuelve a emitir un certificado nuevo, porque no impide que un usuario genere otro certificado de usuario si uno se revoca. Este parámetro aumenta la seguridad de las entidades PKI cuando la lista de revocación de certificados comprueba si hay entidades PKI caducadas.

VIP dedicadas o compartidas de NetScaler Gateway

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 el entorno de Citrix incluye Citrix Endpoint Management junto con Citrix Virtual Apps and Desktops, se puede usar el mismo servidor virtual de NetScaler Gateway para ambos. Debido a posibles conflictos de versiones y al aislamiento del entorno, se recomienda un NetScaler Gateway dedicado para cada entorno de Citrix Endpoint Management.

Si usa la autenticación LDAP, Citrix Secure Hub pueden autenticarse en el mismo NetScaler Gateway sin problemas. Si usa la autenticación basada en certificados, Citrix Endpoint Management envía un certificado al contenedor MDX y Citrix Secure Hub utiliza ese certificado para autenticarse en NetScaler Gateway.

Puede plantearse esta solución temporal, que permite usar un mismo FQDN para dos direcciones IP virtuales de NetScaler Gateway. Puede crear dos direcciones IP virtuales de NetScaler Gateway con la misma dirección IP. La de Citrix Secure Hub utilizará el puerto 443 estándar y la de Citrix Virtual Apps and Desktops (que implementan la aplicación Citrix Workspace) utilizará el puerto 444. Así, un solo nombre de dominio completo se resuelve en la misma dirección IP. Para esta solución temporal, quizá deba configurar StoreFront para devolver un archivo ICA para el puerto 444, en lugar de la opción predeterminada, el puerto 443. Esta solución temporal no requiere que los usuarios introduzcan ningún número de puerto.

Tiempos de espera de NetScaler Gateway

Detalles de la decisión:

- ¿Cómo quiere configurar los tiempos de espera de NetScaler Gateway para el tráfico de Citrix Endpoint Management?

Guía de diseño:

NetScaler Gateway contiene los parámetros Session time-out (Tiempo de espera de la sesión) y Forced time-out (Tiempo de espera forzado). Para obtener más información, consulte [Configuraciones recomendadas](#). Tenga en cuenta que existen valores de tiempo de espera diferentes para los servicios en segundo plano, NetScaler Gateway y para el acceso a aplicaciones sin conexión.

FQDN de inscripción

Importante:

Para cambiar el FQDN de inscripción, se necesita una nueva base de datos de SQL Server y una recompilación del servidor de Citrix Endpoint Management.

Tráfico de Citrix Secure Web

Detalles de la decisión:

- ¿Restringirá Citrix Secure Web a la navegación web interna solamente?
- ¿Habilitará Citrix Secure Web para la navegación web interna y externa?

Guía de diseño:

Si utiliza Citrix Secure Web únicamente para la navegación web en interno, la configuración de NetScaler Gateway es sencilla. Sin embargo, si Citrix Secure Web no puede llegar a todos los sitios internos de forma predeterminada, es posible que tenga que configurar firewalls y servidores proxy.

Si va a utilizar Citrix Secure Web para la navegación interna y externa, debe habilitar la dirección IP de subred (SNIP) para tener acceso saliente a Internet. El departamento de TI suele considerar los dispositivos inscritos (mediante el contenedor MDX) una extensión de la red corporativa. Por lo tanto, TI normalmente quiere que las conexiones de Citrix Secure Web vuelvan a NetScaler Gateway, pasen por un servidor proxy y, a continuación, salgan a Internet. De forma predeterminada, el acceso de Citrix Secure Web se lleva a cabo por túnel a la red interna. Citrix Secure Web usa un túnel VPN por aplicación hacia la red interna para todo el acceso de red y NetScaler Gateway usa los parámetros de túnel dividido.

Para obtener información sobre las conexiones de Citrix Secure Web, consulte [Configurar conexiones de usuario](#).

Notificaciones push para Citrix Secure Mail

Detalles de la decisión:

- ¿Usará 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 desde Citrix Secure Mail hacia las direcciones URL del servicio de escucha de Citrix. Esas URL se especifican en las notificaciones push de Citrix Secure Mail para iOS.

Guía de diseño para Android:

Utilice Firebase Cloud Messaging (FCM) para controlar cómo y cuándo los dispositivos Android se conectan a Citrix Endpoint Management. Con FCM configurado, toda acción de seguridad o comando de implementación desencadena una notificación push en Citrix Secure Hub para pedir al usuario que se reconecte al servidor de Citrix Endpoint Management.

STA HDX

Detalles de la decisión:

- ¿Qué STA usar si quiere integrar el acceso a aplicaciones HDX?

Guía de diseño:

Los STA de HDX deben coincidir con los STA en 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 las zonas de almacenamiento en el entorno?
- ¿Qué URL de dirección IP virtual de Citrix Files usará?

Guía de diseño:

Si incluye controladores de zonas de almacenamiento en el entorno, debe configurar correctamente lo siguiente:

- Dirección IP virtual de conmutación de contenido de Citrix Files (utilizada por el plano de control de Citrix Files para comunicarse con los servidores de los controladores de las zonas de almacenamiento)
- Direcciones IP virtuales del equilibrio de carga de Citrix Files
- Todas las directivas y perfiles necesarios

Para obtener información, consulte la documentación de [Storage zones controller](#).

Proveedor de identidades SAML

Detalles de la decisión:

- Si necesita SAML para Citrix Files, ¿quiere usar Citrix Endpoint Management como proveedor de identidades SAML?

Guía de diseño:

Se recomienda integrar Citrix Files en Citrix Endpoint Management, ya que es una alternativa más sencilla a configurar la federación basada en SAML. Citrix Endpoint Management proporciona a Citrix Files lo siguiente:

- Autenticación Single Sign-On (SSO) de los usuarios de aplicaciones móviles Citrix de productividad
- Aprovisionamiento de cuentas de usuario basado en Active Directory
- Directivas integrales para controlar el acceso.

La consola de Citrix Endpoint Management permite configurar Citrix Files y supervisar los niveles de servicio y uso de licencias.

Hay dos tipos de clientes de Citrix Files: Citrix Files para Citrix Endpoint Management (también conocidos como Citrix Files empaquetados) y clientes móviles de Citrix Files (también conocidos como Citrix Files sin empaquetar). Para obtener más información sobre las diferencias, consulte [En qué 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 que utilicen SAML con el fin de ofrecer acceso SSO a:

- Aplicaciones de Citrix Files que están habilitadas para el SDK de MAM o empaquetadas con MDX Toolkit
- Clientes de Citrix Files no empaquetados, como el sitio web, Outlook Plug-in o clientes de sincronización

Si quiere usar Citrix Endpoint Management como proveedor de identidades SAML para Citrix Files, compruebe que estén definidas las configuraciones adecuadas. Para obtener más información, consulte [SAML para SSO en Citrix Files](#).

Conexiones directas con ShareConnect

Detalles de la decisión:

- ¿Los usuarios accederán a un equipo host desde un equipo o dispositivo móvil que ejecuta ShareConnect con conexiones directas?

Guía de diseño:

ShareConnect permite a los usuarios conectarse a sus equipos de forma segura a través de iPads, tabletas y teléfonos Android para el acceso a sus archivos y aplicaciones. Para las conexiones directas, Citrix Endpoint Management utiliza NetScaler Gateway para proporcionar acceso seguro a los recursos de fuera de la red local. Para obtener más información 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

Modo de administración	FQDN de inscripción
MDM+MAM con inscripción MDM opcional	FQDN del servidor de Citrix Endpoint Management o FQDN de NetScaler Gateway
Solo MAM	FQDN del servidor de Citrix Endpoint Management
Solo MAM (antiguo)	FQDN de NetScaler Gateway

Resumen de implementación

Si tiene varias instancias de Citrix Endpoint Management (por ejemplo, para entornos de prueba, desarrollo y producción) debe configurar manualmente NetScaler Gateway para los entornos adicionales. Si dispone de un entorno de trabajo, tome nota de la configuración antes de intentar configurar NetScaler Gateway manualmente para Citrix Endpoint Management.

Una decisión clave es si utilizar HTTPS o HTTP para la comunicación con el servidor de Citrix Endpoint Management. HTTPS ofrece una comunicación back-end segura, ya que se cifra el tráfico entre NetScaler Gateway y Citrix Endpoint Management. El recifrado afecta el rendimiento del servidor de Citrix Endpoint Management. HTTP ofrece un mejor rendimiento del servidor de Citrix Endpoint Management. El tráfico entre NetScaler Gateway y Citrix Endpoint Management no está cifrado. En las siguientes tablas, se muestran los requisitos de puertos HTTP y HTTPS para NetScaler Gateway y Citrix Endpoint Management.

HTTPS

Por regla general, Citrix recomienda el puente SSL para los parámetros del servidor virtual MDM de NetScaler Gateway. Para usar la descarga de SSL de NetScaler Gateway con servidores virtuales MDM, Citrix Endpoint Management admite solo el puerto 80 como servicio back-end.

Modo de administración	Método de equilibrio de carga de NetScaler Gateway	Recifrado SSL	Puerto del servidor de Citrix Endpoint Management
MAM	Descarga de SSL	Habilitado	8443
MDM+MAM	MDM: Puente SSL	N/D	443, 8443
MDM+MAM	MAM: Descarga de SSL	Habilitado	8443

HTTP

Modo de administración	Método de equilibrio de carga de NetScaler Gateway		Puerto del servidor de Citrix Endpoint Management
		Recifrado SSL	
MAM	Descarga de SSL	Habilitado	8443
MDM+MAM	MDM: Descarga de SSL	No compatible	80
MDM+MAM	MAM: Descarga de SSL	Habilitado	8443

Para obtener diagramas de NetScaler Gateway en las implementaciones de Citrix Endpoint Management, consulte [Arquitectura](#).

Consideraciones sobre SSO y proxies para aplicaciones MDX

March 1, 2024

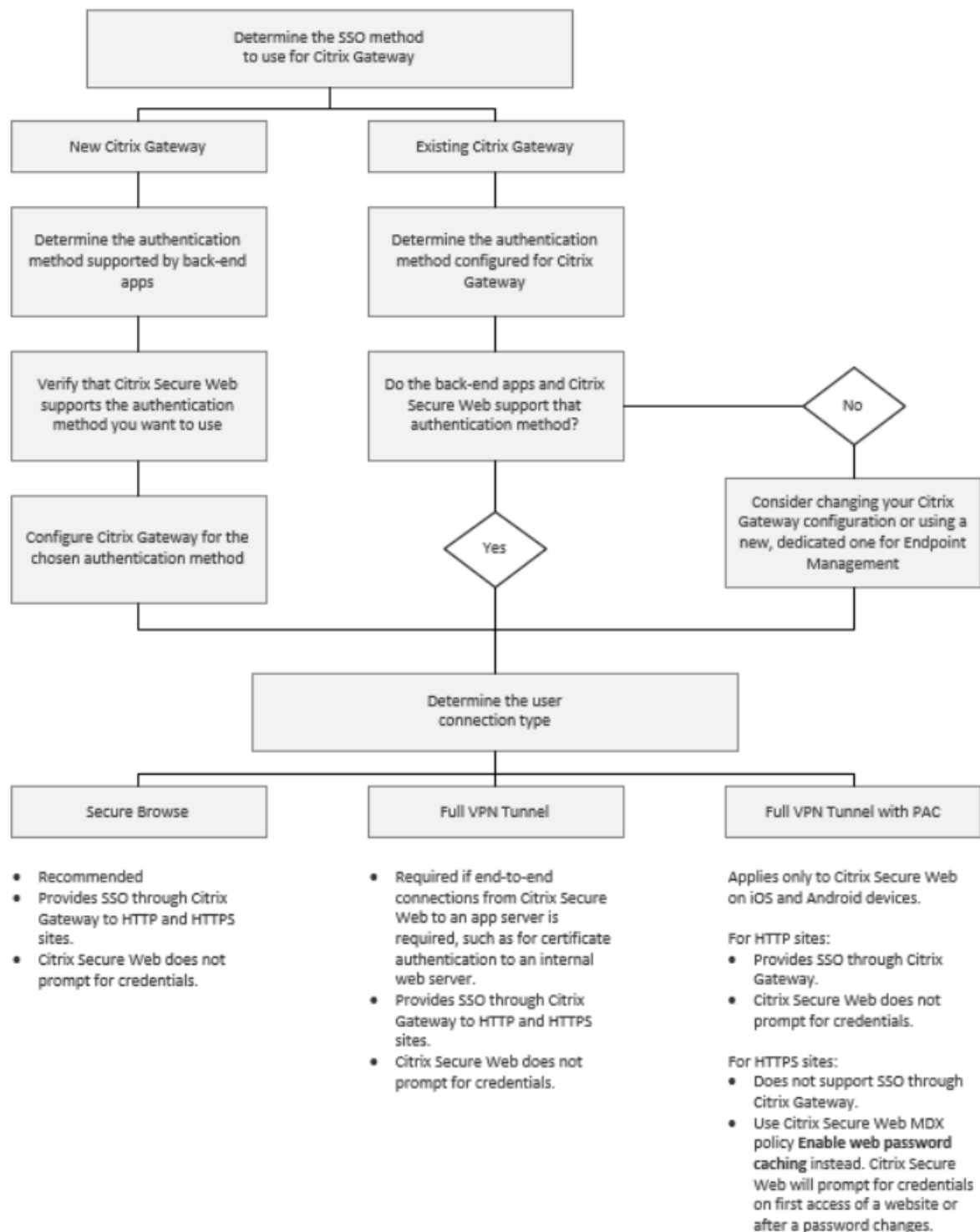
La integración de Citrix Endpoint Management en NetScaler Gateway permite ofrecer a los usuarios un inicio de sesión único (SSO) en todos los recursos back-end HTTP o HTTPS. Dependiendo de sus requisitos de autenticación para SSO, configure las conexiones de usuario para que una aplicación MDX utilice Secure Browse (SSO web en túnel), que es un tipo de VPN sin cliente.

Importante:

Citrix ha retirado el archivo de configuración automática de proxy (PAC) con una implementación de túnel completo de VPN para los dispositivos iOS y Android. Para obtener más información, consulte [Elementos retirados](#).

Si NetScaler Gateway no es el mejor medio para ofrecer SSO en el entorno, puede configurar directivas para que las aplicaciones MDX almacenen las contraseñas en caché local. En este artículo se exploran las diversas opciones SSO y proxy, centrándose sobre todo en Citrix Secure Web. Los conceptos se aplican a otras aplicaciones MDX.

En el siguiente diagrama de flujo, se resume el recorrido de decisiones para SSO y las conexiones de usuario.



Métodos de autenticación de NetScaler Gateway

En esta sección se ofrece información general sobre los métodos de autenticación que admite NetScaler Gateway.

Autenticación SAML

Cuando configura NetScaler Gateway para SAML (Security Assertion Markup Language), los usuarios pueden conectarse a las aplicaciones Web que admiten el protocolo SAML para el inicio SSO. NetScaler Gateway admite el inicio SSO del proveedor de identidades (IdP) para aplicaciones Web SAML.

Configuración requerida:

- Configure SSO con SAML en el perfil de tráfico de NetScaler Gateway.
- Configure un proveedor de identidades con SAML para el servicio solicitado.

Autenticación NTLM

Si el inicio SSO para las aplicaciones Web está habilitado en el perfil de la sesión, NetScaler Gateway realiza automáticamente la autenticación NTLM.

Configuración requerida:

- Habilite SSO en la sesión o el perfil de tráfico de NetScaler Gateway.

Suplantación Kerberos

Citrix Endpoint Management solo admite Kerberos para Citrix Secure Web. Cuando configura NetScaler Gateway para el inicio SSO con Kerberos, NetScaler Gateway utiliza la suplantación cuando NetScaler Gateway dispone de una contraseña de usuario. La suplantación significa que NetScaler Gateway usa credenciales de usuario para obtener el tíquet necesario y acceder a servicios como Citrix Secure Web.

Configuración requerida:

- Configure la directiva de sesión [Worx](#) de NetScaler Gateway para que pueda identificar el territorio Kerberos en la conexión.
- Configure una cuenta de delegación limitada de Kerberos (KCD) en NetScaler Gateway. Configure esa cuenta sin contraseña y vincúlela a una directiva de tráfico en la puerta de enlace de Citrix Endpoint Management.
- Para conocer esos y otros detalles de configuración, consulte el blog de Citrix: [WorxWeb and Kerberos Impersonation SSO](#).

Delegación limitada de Kerberos

Citrix Endpoint Management solo admite Kerberos para Citrix Secure Web. Cuando configura NetScaler Gateway para el inicio SSO con Kerberos, NetScaler Gateway utiliza la delegación limitada cuando NetScaler Gateway no dispone de la contraseña de usuario.

Con la delegación limitada, NetScaler Gateway usa una cuenta de administrador específica para obtener tíquets para usuarios y servicios.

Configuración requerida:

- Configure una cuenta KCD en Active Directory con los permisos necesarios y una cuenta KDC en NetScaler Gateway.
- Habilite SSO en el perfil de tráfico de NetScaler Gateway.
- Configure el sitio web back-end para la autenticación Kerberos.

Autenticación con rellenado de formularios

Cuando configura NetScaler Gateway para el inicio SSO basado en formularios, los usuarios pueden iniciar sesión una vez para acceder a todas las aplicaciones protegidas de la red. Este método de autenticación es aplicable a las aplicaciones que usan el modo SSO web en túnel.

Configuración requerida:

- Configure el inicio SSO basado en formularios en el perfil de tráfico de NetScaler Gateway.

Autenticación HTTP implícita

Si habilita el inicio SSO para las aplicaciones Web en el perfil de la sesión, NetScaler Gateway realiza automáticamente la autenticación HTTP implícita. Este método de autenticación es aplicable a las aplicaciones que usan el modo SSO web en túnel.

Configuración requerida:

- Habilite SSO en la sesión o el perfil de tráfico de NetScaler Gateway.

Autenticación HTTP básica

Si habilita el inicio SSO para las aplicaciones Web en el perfil de la sesión, NetScaler Gateway realiza automáticamente la autenticación HTTP básica. Este método de autenticación es aplicable a las aplicaciones que usan el modo SSO web en túnel.

Configuración requerida:

- Habilite SSO en la sesión o el perfil de tráfico de NetScaler Gateway.

SSO web en túnel seguro

En esta sección se describen los tipos de conexión de usuario **SSO web en túnel** para Citrix Secure Web.

Las conexiones por túnel con la red interna pueden utilizar una variante de VPN sin cliente, conocida como SSO web en túnel. SSO web en túnel es la configuración predeterminada para la directiva **Modo preferido de VPN** de Citrix Secure Web. Citrix recomienda el valor Túnel - SSO web para conexiones que requieren Single Sign-On (SSO).

En el modo “SSO web en túnel”, NetScaler Gateway divide la sesión HTTPS en dos partes:

- Del cliente a NetScaler Gateway
- Desde NetScaler Gateway hasta el servidor back-end de recursos.

De esta manera, NetScaler Gateway tiene una visibilidad total de todas las transacciones entre el cliente y el servidor, lo que le permite ofrecer SSO.

También puede configurar los servidores proxy de Citrix Secure Web cuando se usa el modo “SSO web en túnel”. Para obtener más información, consulte la entrada de blog [XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode](#).

Nota:

Citrix anunció la retirada del túnel VPN completo con PAC. Consulte [Elementos retirados](#).

Citrix Endpoint Management admite la autenticación de proxy suministrada por NetScaler Gateway. Un archivo PAC contiene reglas que definen el modo en que los exploradores web seleccionan un proxy para acceder a una dirección URL especificada. Las reglas del archivo PAC pueden especificar cómo gestionar tanto sitios internos como sitios externos. Citrix Secure Web analiza las reglas del archivo PAC y envía la información del servidor proxy a NetScaler Gateway. NetScaler Gateway no detecta el archivo PAC ni el servidor proxy.

Para la autenticación en sitios web HTTPS, la directiva MDX **Habilitar caché de contraseñas Web** permite a Citrix Secure Web autenticarse y ofrecer SSO en el servidor proxy a través de MDX.

Túnel dividido de NetScaler Gateway

Cuando planifique la configuración de SSO y proxy, también debe decidir si usar el túnel dividido de NetScaler Gateway o no. Citrix recomienda que utilice el túnel dividido de NetScaler Gateway solo si es necesario. En esta sección se ofrece una vista de alto nivel sobre cómo funciona el túnel dividido: NetScaler Gateway determina la ruta del tráfico en función de su tabla de enrutamiento. Cuando el túnel dividido de NetScaler Gateway está activado, Citrix Secure Hub distingue el tráfico de red interno (protegido) del tráfico de Internet. Citrix Secure Hub realiza esa distinción en función del sufijo DNS y

las aplicaciones de la intranet. A continuación, Citrix Secure Hub envía por el túnel VPN solo el tráfico de la red interna. Cuando el túnel dividido de NetScaler Gateway está desactivado, todo el tráfico pasa por el túnel VPN.

Si, por motivos de seguridad, prefiere supervisar todo el tráfico, desactive el túnel dividido de NetScaler Gateway. Como resultado, todo el tráfico pasará por el túnel VPN.

NetScaler Gateway también tiene un modo de túnel dividido inverso de micro VPN. Esta configuración admite una lista de exclusión de direcciones IP que no se envían por el túnel de NetScaler Gateway. En vez de ello, esas direcciones se envían mediante la conexión a Internet del dispositivo. Para obtener más información sobre el túnel dividido inverso, consulte la documentación de NetScaler Gateway.

Citrix Endpoint Management incluye una **Lista de exclusión para revertir túnel dividido**. Para impedir que determinados sitios web usen el túnel a través de NetScaler Gateway, agregue una lista de nombres de dominio completo (FQDN) o sufijos DNS, separados por comas, para que se conecten a través de la red LAN en lugar del túnel. Esta lista se aplica solamente al modo “SSO web en túnel” cuando NetScaler Gateway está configurado en el modo túnel dividido revertido.

Autenticación

March 1, 2024

En una implementación de Citrix Endpoint Management, entran varias consideraciones en juego a la hora de decidir cómo configurar la autenticación. En esta sección se describen los diversos factores que afectan a la autenticación:

- Las principales directivas MDX, las propiedades del cliente de Citrix Endpoint Management y las configuraciones de NetScaler Gateway relacionadas con la autenticación.
- Las formas en que interactúan estas directivas, parámetros y propiedades de cliente.
- Los pros y contras de cada elección.

Este artículo también contiene tres ejemplos de configuraciones recomendadas para aumentar los grados de seguridad.

En términos generales, una seguridad más alta empobrece la experiencia del usuario, ya que los usuarios deben autenticarse más a menudo. La forma de equilibrar estos aspectos, la seguridad y la fluidez de la experiencia del usuario depende de las necesidades y las prioridades de su organización. Revise las tres configuraciones recomendadas para comprender la interacción de las distintas opciones de autenticación.

Modos de autenticación

Autenticación con conexión: Permite a los usuarios conectarse a la red de Citrix Endpoint Management. Requiere una conexión a Internet.

Autenticación sin conexión: Ocurre en el dispositivo. Los usuarios desbloquean la caja fuerte segura y tienen acceso sin conexión a elementos (como el correo descargado, los sitios web almacenados en caché y las notas).

Métodos de autenticación

Factor único LDAP: En Citrix Endpoint Management, puede configurar una conexión a varios directorios compatibles con el protocolo ligero de acceso a directorios (LDAP). Este es un método frecuente para ofrecer el inicio Single Sign-On (SSO) en entornos de empresa. Puede optar por el PIN de Citrix con 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 información detallada, consulte [Autenticación con dominio o dominio y token de seguridad](#).

Certificado de cliente: Citrix Endpoint Management puede integrarse en entidades de certificación estándar del sector para usar certificados como método único de la autenticación en línea. Citrix Endpoint Management ofrece este certificado una vez los usuarios se han inscrito, lo que requiere una contraseña de un solo uso, una URL de invitación o credenciales LDAP. Cuando se usa un certificado de cliente como el método principal de autenticación, se necesita 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) cuando se trata de una entidad de certificación (CA) de terceros. Si dispone de una entidad de certificación de Microsoft configurada, Citrix Endpoint Management utiliza NetScaler Gateway para administrar la revocación. Al configurar la autenticación por certificados de cliente, plantéese si es necesario configurar el parámetro de lista de revocación de certificados (CRL) de NetScaler Gateway, Enable CRL Auto Refresh. Este paso garantiza que un dispositivo inscrito en MAM solo no pueda autenticarse mediante un certificado existente en el dispositivo. Citrix Endpoint Management vuelve a emitir un certificado nuevo, porque no impide que un usuario genere otro certificado de usuario si uno se revoca. Este parámetro aumenta la seguridad de las entidades PKI cuando la lista de revocación de certificados comprueba si hay entidades PKI caducadas.

Para obtener un diagrama que muestra la implementación necesaria para la autenticación basada en certificados o el uso de la entidad de certificación (CA) de empresa para emitir certificados de dispositivo, consulte [Arquitectura](#).

Autenticación de dos factores Certificado de cliente + LDAP: Esta configuración es la mejor combinación de seguridad y experiencia de usuario para Citrix Endpoint Management. Usar LDAP y la autenticación de certificados de cliente:

- Tiene las mejores posibilidades de SSO, junto con la seguridad que proporciona la autenticación de dos factores en NetScaler Gateway.
- Ofrece seguridad con algo que los usuarios conocen (sus contraseñas de Active Directory) y algo que poseen (certificados de cliente en sus dispositivos).

Citrix Secure Mail puede configurar automáticamente y ofrecer una primera experiencia de usuario fluida con la autenticación de certificados de cliente. Esta función requiere un entorno de servidor de acceso de cliente Exchange configurado correctamente.

Para una experiencia de uso óptima, puede combinar la autenticación por certificado y dominio, junto 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 y una contraseña de un solo uso, mediante el protocolo RADIUS. Para una experiencia de uso 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 propiedades de cliente, configuraciones y directivas intervienen en las tres configuraciones recomendadas indicadas más adelante:

Directivas MDX

Código de acceso de aplicación: Cuando se establece en **Sí**, se requiere un PIN o un código de acceso de Citrix para desbloquear la aplicación cuando ésta se inicia o se reanuda después de un período de inactividad. De forma predeterminada, está **activado**.

Para configurar el temporizador de inactividad para todas las aplicaciones, establezca el valor de INACTIVITY_TIMER en minutos, en la consola de Citrix Endpoint Management, desde la ficha **Parámetros**, en **Propiedades de cliente**. El valor predeterminado es 15 minutos. Para inhabilitar el temporizador de inactividad, de modo que la petición de PIN o código de acceso aparezca solo cuando se inicie la aplicación, establezca un valor de cero.

Sesión Micro VPN requerida: Cuando se **activa**, el usuario debe contar con una sesión activa y una conexión a la red de la empresa para poder acceder a la aplicación presente en el dispositivo. Cuando se establece en **No**, no se requiere una sesión activa para poder acceder a la aplicación presente en el dispositivo. El valor predeterminado es **Desactivado**.

Período máximo sin conexión (horas): Define el período de tiempo máximo que una aplicación puede ejecutarse sin tener que volver a confirmar los derechos a utilizarla ni actualizar las directivas desde Citrix Endpoint Management. Una aplicación de iOS recupera nuevas directivas para aplicaciones MDX desde Citrix Endpoint Management sin interrupciones para los usuarios cuando se cumplen estas condiciones:

- Se establece el período máximo sin conexión y
- Citrix Secure Hub para iOS tiene un token de NetScaler Gateway válido.

En cambio, si Citrix Secure Hub no tiene un token válido de NetScaler Gateway, los usuarios deben autenticarse en Citrix Secure Hub para que se actualicen las directivas de las aplicaciones. El token de NetScaler Gateway puede dejar de ser válido debido a la inactividad en la sesión de NetScaler Gateway o a alguna directiva de tiempo de espera forzado para la sesión. Cuando los usuarios vuelvan a iniciar sesión en Citrix Secure Hub, podrán continuar ejecutando la aplicación.

Los usuarios reciben un recordatorio para que inicien sesión 30, 15 y 5 minutos antes de que acabe el período. Una vez se acabe el período, la aplicación se bloquea hasta que los usuarios inicien sesión. El valor predeterminado es **72 horas (3 días)**. El período mínimo de tiempo es 1 hora.

Nota:

Tenga en cuenta que, cuando los usuarios viajan con frecuencia y usan la itinerancia internacional, el valor predeterminado de 72 horas (3 días) puede ser demasiado corto.

Caducidad del tíquet de servicios en segundo plano: El período de validez que tiene un tíquet del servicio de red en segundo plano. Cuando Citrix Secure Mail se conecta a través de NetScaler Gateway a un Exchange Server que ejecuta ActiveSync, Citrix Endpoint Management emite un token. Citrix Secure Mail usa ese token para conectarse al servidor interno de Exchange. Esta propiedad determina cuánto tiempo Citrix Secure Mail puede usar el token sin necesidad de uno nuevo para la autenticación y la conexión con Exchange Server. Cuando se alcanza el límite de tiempo, los usuarios deben volver a iniciar sesión para generar un nuevo token. El valor predeterminado es **168 horas (7 días)**. Cuando se agota este tiempo de espera, se detienen las notificaciones por correo.

Período de gracia para requerir una sesión de micro VPN: Determina cuántos minutos puede un usuario utilizar una aplicación sin conexión hasta de que la sesión con conexión sea validada. El valor predeterminado es **0** (no hay período de gracia).

Para obtener información acerca de las directivas de autenticación, consulte:

- Si utiliza el SDK de MAM: [Introducción al SDK de MAM](#)
- Si utiliza 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 sencilla de inicio de sesión, puede optar por habilitar el PIN de Citrix. Con el PIN, los usuarios no tienen que introducir repetidamente otras credenciales (como los nombres de usuario y las contraseñas de Active Directory). Puede configurar el PIN de Citrix como una autenticación independiente que solo funciona sin conexión. También puede combinar el PIN con el almacenamiento en caché de contraseñas de Active Directory para una usabilidad óptima y fluida. Configure el PIN de Citrix en **Parámetros > Cliente > Propiedades de cliente** en la consola de Citrix Endpoint Management.

A continuación dispone de un resumen con algunas propiedades importantes. Para obtener más información, consulte [Propiedades de cliente](#).

ENABLE_PASSCODE_AUTH

Nombre simplificado: Enable Citrix PIN Authentication

Esta clave permite activar la función de PIN de Citrix. Si se activa la función de PIN o código de acceso de Citrix, se solicita a los usuarios que definan un número PIN que se usará en lugar de su contraseña de Active Directory. Habilite esta configuración si la propiedad **ENABLE_PASSWORD_CACHING** está habilitada o si Citrix Endpoint Management usa la autenticación por certificado.

Valores posibles: true o false

Valor predeterminado: false

ENABLE_PASSWORD_CACHING

Nombre simplificado: Enable User Password Caching

Esta clave permite que la contraseña de Active Directory de los usuarios se almacene en la memoria caché local del dispositivo móvil. Al establecer esta clave en true, se solicita a los usuarios que establezcan un PIN o un código de acceso de Citrix. El valor de la clave **ENABLE_PASSCODE_AUTH** debe establecerse en true cuando esta clave se establece en **true**.

Valores posibles: true o false

Valor predeterminado: false

PASSCODE_STRENGTH

Nombre simplificado: PIN Strength Requirement

Esta clave define la seguridad del PIN o código de acceso de Citrix. Si cambia este parámetro, se solicitará a los usuarios que establezcan un nuevo PIN o código de acceso de Citrix la próxima vez que deban autenticarse.

Valores posibles: Low, Medium o Strong

Valor predeterminado: Medium

INACTIVITY_TIMER

Nombre simplificado: Inactivity Timer

Esta clave define el tiempo en minutos que los usuarios pueden dejar su dispositivo inactivo y luego acceder a una aplicación sin que se solicite un PIN o un código de acceso de Citrix. Si quiere habilitar esta configuración para una aplicación MDX, debe **activar** la configuración **Código de acceso de aplicación**. Si el parámetro **Código de acceso de aplicación** está **desactivado**, se redirige a los usuarios a Citrix Secure Hub para realizar una autenticación completa. Al cambiar este parámetro, el valor se aplicará la próxima vez que los usuarios deban autenticarse. El valor predeterminado es 15 minutos.

ENABLE_TOUCH_ID_AUTH

Nombre simplificado: Enable Touch ID Authentication

Permite el uso del lector de huellas dactilares (solo en iOS) para la autenticación sin conexión. La autenticación en línea aún requerirá el método de autenticación principal.

ENCRYPT_SECRETS_USING_PASSCODE

Nombre simplificado: Encrypt secrets using Passcode

Esta clave permite que los datos confidenciales se almacenen en el dispositivo móvil, en un almacén secreto, en lugar de guardarse en un almacén nativo basado en la plataforma, como el llavero de iOS. Esta clave de configuración permite un cifrado seguro de los objetos clave, pero también agrega la entropía de usuario (un código PIN aleatorio generado por el usuario y que solo el usuario conoce).

Valores posibles: true o false

Valor predeterminado: false

Parámetros de NetScaler Gateway

Tiempo de desconexión de la sesión: Si se habilita esta configuración, NetScaler Gateway desconecta la sesión si no detecta ninguna actividad de red durante un intervalo especificado. Esta configuración se aplica a los usuarios que se conectan con NetScaler Gateway Plug-in, Citrix Secure Hub o mediante un explorador web. El valor predeterminado es **1440 minutos**. Si se establece este valor en cero, el parámetro queda inhabilitado.

Tiempo de espera forzado: Si habilita esta configuración, NetScaler Gateway desconecta la sesión una vez transcurrido el intervalo del tiempo de espera, independientemente de la actividad del usuario. No existe ninguna acción que el usuario pueda realizar para evitar que se produzca la desconexión cuando se agota el tiempo de espera. Esta configuración se aplica a los usuarios que

se conectan con NetScaler Gateway Plug-in, Citrix Secure Hub o mediante un explorador web. Si Citrix Secure Mail usa STA, un modo especial de NetScaler Gateway, este parámetro no se aplica a las sesiones de Citrix Secure Mail. El valor predeterminado no es ningún valor, lo que significa que las sesiones se extienden si hay alguna actividad.

Para obtener más información acerca de los tiempos de espera para NetScaler Gateway, consulte la documentación de NetScaler Gateway.

Para obtener más información acerca de los casos en que se solicita a los usuarios que se autenticuen en Citrix Endpoint Management con credenciales en sus dispositivos, consulte [Situaciones de petición de credenciales](#).

Parámetros predeterminados de configuración

Estos parámetros son los valores predeterminados proporcionados por:

- Asistente de NetScaler para XenMobile
- SDK de MAM o MDX Toolkit
- Consola de Citrix Endpoint Management

Parámetro	Dónde encontrar el parámetro	Configuración predeterminada
Tiempo de desconexión 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	No
Período de gracia de sesión de Micro VPN requerida	Directivas MDX	0
Código de acceso de aplicación	Directivas MDX	Sí
Cifrar secretos mediante un código de acceso	Propiedades de cliente de Citrix Endpoint Management	false
Enable Citrix PIN Authentication	Propiedades de cliente de Citrix Endpoint Management	false
Requisito de seguridad de código PIN	Propiedades de cliente de Citrix Endpoint Management	Medio

Parámetro	Dónde encontrar el parámetro	Configuración predeterminada
Tipo de código PIN	Propiedades de cliente de Citrix Endpoint Management	Numérico
Enable User Password Caching (Habilitar almacenamiento en caché de la contraseña del usuario)	Propiedades de cliente de Citrix Endpoint Management	false
Inactivity Timer (Temporizador de inactividad)	Propiedades de cliente de Citrix Endpoint Management	15
Enable Touch ID Authentication	Propiedades de cliente de Citrix Endpoint Management	false

Configuraciones recomendadas

En esta sección, se ofrecen ejemplos de tres configuraciones de Citrix Endpoint Management: desde la configuración de seguridad más baja y la experiencia de usuario óptima, hasta la configuración de mayor seguridad y experiencia de usuario más intrusiva. El objetivo de estos ejemplos es proporcionarle puntos de referencia para decidir a qué altura de la escala quiere colocar su propia configuración. Tenga en cuenta que modificar estas configuraciones puede requerir que modifique otras configuraciones también. Por ejemplo, el período máximo sin conexión no debe exceder el tiempo de espera de la sesión.

Highest Security (El mayor nivel de seguridad)

Esta configuración ofrece el nivel más alto de seguridad, pero tiene inconvenientes significativos para la facilidad de uso.

Parámetro	Dónde encontrar el parámetro	Configuración recomendada	Impacto en el comportamiento
-----------	------------------------------	---------------------------	------------------------------

Tiempo de desconexión de la sesión	NetScaler Gateway	1440	Los usuarios introducen sus credenciales de Citrix Secure Hub solo cuando se necesita la autenticación en línea (cada 24 horas)
Tiempo de espera forzado	NetScaler Gateway	Ningún 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, lo que permite sesiones duraderas sin 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 se detengan las notificaciones de correo. En ese caso, Citrix Secure Mail no preguntará al usuario si este no abre la aplicación antes de que caduque la sesión.
Sesión de micro VPN requerida	Directivas MDX	No	Ofrece una conexión de red válida y una sesión de NetScaler Gateway para usar aplicaciones.

Período de gracia de sesión de Micro VPN requerida	Directivas MDX	0	Sin período de gracia (si habilitó “Sesión de Micro VPN requerida”).
Código de acceso de aplicación	Directivas MDX	Sí	Requerir código de acceso para una aplicación.
Cifrar secretos mediante un código de acceso	Propiedades de cliente de Citrix Endpoint Management	true	Una clave derivada de la entropía del usuario protege la caja fuerte.
Enable Citrix PIN Authentication	Propiedades de cliente de Citrix Endpoint Management	true	El PIN de Citrix simplifica la experiencia de autenticación del usuario.
Requisito de seguridad de código PIN	Propiedades de cliente de Citrix Endpoint Management	Fuerte	Altos requisitos de complejidad para la contraseña.
Tipo de código PIN	Propiedades de cliente de Citrix Endpoint Management	Alfanumérico	El PIN es una secuencia alfanumérica.
Habilitar	Propiedades de cliente de Citrix Endpoint Management	false	La contraseña de Active Directory no se almacena en caché y el PIN de Citrix se usará para las autenticaciones sin conexión.
Inactivity Timer (Temporizador de inactividad)	Propiedades de cliente de Citrix Endpoint Management	15	Si el usuario no usa Citrix Secure Hub o las aplicaciones MDX durante este período de tiempo, se pide la autenticación sin conexión.

Enable Touch ID Authentication	Propiedades de cliente de Citrix Endpoint Management	false	Inhabilita Touch ID para casos de autenticación sin conexión en iOS.
--------------------------------	--	-------	--

Higher Security (Mayor nivel de seguridad)

Con un enfoque más intermedio, esta configuración requiere que los usuarios se autenticen más a menudo, cada 3 días a lo sumo (en lugar de 7), y ofrece una mayor seguridad. Esta mayor cantidad de autenticaciones bloquea el contenedor de datos más a menudo, lo que ofrece la seguridad de los datos cuando los dispositivos no se están usando.

Parámetro	Dónde encontrar el parámetro	Configuración recomendada	Impacto en el comportamiento
Tiempo de desconexión de la sesión	NetScaler Gateway	4320	Los usuarios introducen sus credenciales de Citrix Secure Hub solo cuando se necesita la autenticación en línea (cada 3 días)
Tiempo de espera forzado	NetScaler Gateway	Ningún 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 hora es para permitir la actualización antes de que se agote el Tiempo de desconexión de la sesión (Session time-out).

Caducidad del tíquet de servicios en segundo plano	Directivas MDX	168 horas	Tiempo de espera para STA, lo que permite sesiones duraderas sin 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 se detengan las notificaciones de correo sin preguntar al usuario.
Sesión de micro VPN requerida	Directivas MDX	No	Ofrece una conexión de red válida y una sesión de NetScaler Gateway para usar aplicaciones.
Período de gracia de sesión de Micro VPN requerida	Directivas MDX	0	Sin período de gracia (si habilitó “Sesión de Micro VPN requerida”).
Código de acceso de aplicación	Directivas MDX	Sí	Requerir código de acceso para una aplicación.
Cifrar secretos mediante un código de acceso	Propiedades de cliente de Citrix Endpoint Management	false	No se requiere entropía de usuario para cifrar la caja fuerte.
Enable Citrix PIN Authentication	Propiedades de cliente de Citrix Endpoint Management	true	El PIN de Citrix simplifica la experiencia de autenticación del usuario.
Requisito de seguridad de código PIN	Propiedades de cliente de Citrix Endpoint Management	Medio	Aplica reglas de complejidad media a la contraseña.

Tipo de código PIN	Propiedades de cliente de Citrix Endpoint Management	Numérico	Un PIN es una secuencia numérica.
Habilitar	Propiedades de cliente de Citrix Endpoint Management	true	El PIN del usuario se almacena en caché y protege la contraseña de Active Directory.
Inactivity Timer (Temporizador de inactividad)	Propiedades de cliente de Citrix Endpoint Management	30	Si el usuario no usa Citrix Secure Hub o las aplicaciones MDX durante este período de tiempo, se pide la autenticación sin conexión.
Enable Touch ID Authentication	Propiedades de cliente de Citrix Endpoint Management	true	Permite Touch ID para casos de autenticación sin conexión en iOS.

High Security (Nivel alto de seguridad)

Esta configuración, la más conveniente para los usuarios, proporciona una seguridad base.

Parámetro	Dónde encontrar el parámetro	Configuración recomendada	Impacto en el comportamiento
Tiempo de desconexión de la sesión	NetScaler Gateway	10080	Los usuarios introducen sus credenciales de Citrix Secure Hub solo cuando se necesita la autenticación en línea (cada 7 días)
Tiempo de espera forzado	NetScaler Gateway	Ningún valor	Las sesiones se extienden si hay alguna actividad.

Período máximo sin conexión	Directivas MDX	167	Requiere una actualización de directivas por semana (cada 7 días). La diferencia de hora es para permitir la actualización antes de que se agote el Tiempo de desconexión de la sesión (Session time-out).
Caducidad del tíquet de servicios en segundo plano	Directivas MDX	240	Tiempo de espera para STA, lo que permite sesiones duraderas sin 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 se detengan las notificaciones de correo. En ese caso, Citrix Secure Mail no preguntará al usuario si este no abre la aplicación antes de que caduque la sesión.
Sesión de micro VPN requerida	Directivas MDX	No	Ofrece una conexión de red válida y una sesión de NetScaler Gateway para usar aplicaciones.
Período de gracia de sesión de Micro VPN requerida	Directivas MDX	0	Sin período de gracia (si habilitó “Sesión de Micro VPN requerida”).

Código de acceso de aplicación	Directivas MDX	Sí	Requerir código de acceso para una aplicación.
Cifrar secretos mediante un código de acceso	Propiedades de cliente de Citrix Endpoint Management	false	No se requiere entropía de usuario para cifrar la caja fuerte.
Enable Citrix PIN Authentication	Propiedades de cliente de Citrix Endpoint Management	true	El PIN de Citrix simplifica la experiencia de autenticación del usuario.
Requisito de seguridad de código PIN	Propiedades de cliente de Citrix Endpoint Management	Bajo	Sin requisitos de complejidad para la contraseña
Tipo de código PIN	Propiedades de cliente de Citrix Endpoint Management	Numérico	Un PIN es una secuencia numérica.
Habilitar	Propiedades de cliente de Citrix Endpoint Management	true	El PIN del usuario se almacena en caché y protege la contraseña de Active Directory.
Inactivity Timer (Temporizador de inactividad)	Propiedades de cliente de Citrix Endpoint Management	90	Si el usuario no usa Citrix Secure Hub o las aplicaciones MDX durante este período de tiempo, se pide la autenticación sin conexión.
Enable Touch ID Authentication	Propiedades de cliente de Citrix Endpoint Management	true	Permite Touch ID para casos de autenticación sin conexión en iOS.

Usar una autenticación de nivel superior

Puede que algunas aplicaciones requieran una autenticación mejorada. Por ejemplo, un factor de autenticación secundario, como un token o tiempos de espera de sesión agresivos. Se puede controlar

este método de autenticación a través de una directiva MDX. El método también requiere un servidor virtual independiente para controlar los métodos de autenticación (en el mismo dispositivo NetScaler Gateway o en varios).

Parámetro	Dónde encontrar el parámetro	Configuración recomendada	Impacto en el comportamiento
NetScaler Gateway alternativo	Directivas MDX	Requiere el FQDN y el puerto del dispositivo NetScaler Gateway secundario.	Permite la autenticación mejorada, controlada por las directivas de sesión y autenticación del dispositivo secundario de NetScaler Gateway.

Si un usuario abre una aplicación que utiliza NetScaler Gateway alternativo, todas las demás aplicaciones utilizarán esa instancia de NetScaler Gateway para comunicarse con la red interna. La sesión solo vuelve a la instancia de menor seguridad de NetScaler Gateway cuando se agota su tiempo de espera en la instancia de NetScaler Gateway con seguridad mejorada.

Utilizar “sesión de Micro VPN requerida”

Para determinadas aplicaciones, como Citrix Secure Web, puede asegurarse de que los usuarios ejecuten una aplicación solo cuando tengan una sesión autenticada. Esta directiva aplica esa opción y permite un período de gracia para que los usuarios puedan finalizar su trabajo.

Parámetro	Dónde encontrar el parámetro	Configuración recomendada	Impacto en el comportamiento
Sesión de micro VPN requerida	Directivas MDX	Sí	Garantiza que el dispositivo está conectado y tiene 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 de servidor

March 1, 2024

Las propiedades de servidor son aquellas propiedades globales que se aplican globalmente a operaciones, usuarios y dispositivos en toda la instancia de Citrix Endpoint Management. Citrix recomienda que evalúe si son útiles para su entorno las propiedades de servidor descritas en este artículo. Debe consultar con Citrix antes de cambiar otras propiedades de servidor.

Para actualizar las propiedades del servidor, vaya a **Parámetros > Propiedades del servidor**.

Agregar, modificar o eliminar propiedades de servidor


En Citrix Endpoint Management, se pueden aplicar propiedades al servidor.

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En **Servidor**, haga clic en **Propiedades de servidor**. Aparecerá la página **Propiedades de servidor**. Puede agregar, modificar o eliminar propiedades de servidor desde esta página.

Settings > [Server Properties](#)

Server Properties

You must restart XenMobile on all nodes to commit and activate your changes to the server properties. To restart XenMobile, use the command prompt through your hypervisor.

 Add

<input type="checkbox"/>	Display name	Key	Value	Default value	Description	
<input type="checkbox"/>	NetScaler Gateway Client Cert Issuing Throttling Interval	ag.client.cert.throttling.minutes	30	30	Throttling interval for issuance of NetScaler Gateway client certificates.	
<input type="checkbox"/>	Number of consecutive failed uploads.	ceip.consecutive.upload.failures	0	0		
<input type="checkbox"/>	Sharefile byPath API fields	com.citrix.sharefile.bypath.fields	odata.metadata.id, url	odata.metadata, id, url	Comma separated set of fields (case-sensitive) that need to be extracted from the complete sharefile byPath API response	
<input type="checkbox"/>	Sharefile configuration type : ENTERPRISE/CONNECTORS/NONE	com.citrix.sharefile.config.type	ENTERPRISE	NONE	Sharefile configuration type . Possible values being ENTERPRISE or CONNECTORS or NONE	
<input type="checkbox"/>	Connection Timeout	CONNECTION_TIMEOUT	5	5	Session inactivity timeout, in minutes, after which the TCP connection to a device will be closed (by default 5 minutes).	
<input type="checkbox"/>	Identifies if telemetry is enabled or not.	console.ceip.participate	true	false		
<input type="checkbox"/>	Length of Inactivity Before Device Is Disconnected	device.inactivity.days.threshold	7	7	Length of inactivity (in days) before the device is disconnected.	
<input type="checkbox"/>	User-Defined Device Properties 1	device.properties.userDefined1			User-defined device properties.	
<input type="checkbox"/>	User-Defined Device Properties 2	device.properties.userDefined2			User-defined device properties.	
<input type="checkbox"/>	User-Defined Device Properties 3	device.properties.userDefined3			User-defined device properties.	

Showing 1 - 10 of 111 items

Showing 1 of 12

Para agregar una propiedad de servidor

1. Haga clic en **Agregar**. Aparecerá la página **Agregar nueva propiedad de servidor**.

Settings > Server Properties > Add New Server Property

Add New Server Property

Key ?

Value*

Display name*

Description

2. Configure estos parámetros:

- **Clave:** En la lista, seleccione la clave apropiada. Las claves distinguen mayúsculas y minúsculas. Póngase en contacto con la asistencia de Citrix antes de modificar los valores de propiedad o para solicitar una clave especial.
- **Valor:** Escriba un valor en función de la clave seleccionada.
- **Nombre simplificado:** Especifique el nombre del nuevo valor de propiedad que aparece en la tabla **Propiedades de servidor**.
- **Descripción:** Escriba una descripción opcional de la nueva propiedad de servidor.

3. Haga clic en **Guardar**.

Para modificar una propiedad de servidor

1. En la tabla **Propiedades de servidor**, seleccione la propiedad de servidor que quiere modificar.
Si marca la casilla situada junto a una propiedad de servidor, el menú de opciones aparece encima de la lista de propiedades de servidor. Haga clic en cualquier lugar de la lista para que el menú de opciones aparezca a la derecha de la lista.
2. Haga clic en **Edit**. Aparecerá la página **Modificar nueva propiedad de servidor**.

Settings > Server Properties > Edit New Server Property

Edit New Server Property

Key	ag.client.cert.throttling.mi
Value*	30
Display name*	NetScaler Gateway Client
Description	Throttling interval for issuance of NetScaler Gateway client certificates.

Cancel Save

3. Cambie la siguiente información como corresponda:

- Clave: Este campo no puede cambiarse.
- Valor: El valor de la propiedad.
- Nombre simplificado: El nombre de la propiedad.
- Descripción: La descripción de la propiedad.

4. Haga clic en **Guardar** para guardar los cambios o en **Cancelar** para descartarlos.

Para eliminar una propiedad de servidor

1. En la tabla **Propiedades de servidor**, seleccione las propiedades de servidor que quiere eliminar.
2. Haga clic en **Eliminar**. Aparecerá un cuadro de diálogo de confirmación. Vuelva a hacer clic en **Eliminar**.

Definiciones de las propiedades de servidor

Acceder a todas las aplicaciones en la tienda administrada de Google Play

- Si es **true**, Citrix Endpoint Management hace que todas las aplicaciones de la tienda pública de Google Play sean accesibles desde la tienda administrada de Google Play. Puede usar la [directiva Restricciones](#) para controlar el acceso a estas aplicaciones. El valor predeterminado es **false**.

Agregar dispositivo siempre

- Si tiene el valor **true**, Citrix Endpoint Management agrega un dispositivo a la consola de Citrix Endpoint Management, incluso aunque falle la inscripción. Como resultado, puede ver qué dispositivos intentaron inscribirse. El valor predeterminado es **false**.

Intervalo de limitación de emisión de certificados cliente de AG

- El período de gracia entre la generación de certificados. Este intervalo evita que Citrix Endpoint Management genere varios certificados para un dispositivo en un período corto de tiempo. Citrix recomienda no modificar este valor. El valor predeterminado es **30** minutos.

Permitir quitar dispositivos marcados como inactivos durante un período de tiempo específico

- Si el valor es **true**, los dispositivos que hayan estado inactivos durante un tiempo específico (en días) se quitan y se eliminan de Citrix Endpoint Management. El período de actividad lo establece la propiedad del 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, consúltelo con un representante de Citrix.

Registrador de auditoría

- Si es **false**, no registra eventos de interfaz de usuario (UI). El valor predeterminado es **False**.

Bloquear inscripción de dispositivos iOS y Android liberados por jailbreak o rooting

Cuando esta propiedad tiene el valor **true**, Citrix Endpoint Management bloquea las inscripciones de dispositivos Android liberados por rooting y dispositivos iOS liberados por jailbreak. El valor recomendado es **true** para todos los niveles de seguridad. El valor predeterminado es **true**.

cdn.s3.retry.interval y cdn.s3.max.retry

Las propiedades `cdn.s3.retry.interval` y `cdn.s3.max.retry` del servidor funcionan juntas para establecer el límite de tiempo máximo de cada carga de archivos PKG en macOS. De forma predeterminada, Citrix Endpoint Management limita los tiempos de carga de archivos a 100 segundos. Si la carga de un archivo supera ese límite, el proceso 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 comprueba si una carga de archivos se completa correctamente. El valor predeterminado es 10000.
- `cdn.s3.max.retry`. Permite definir la cantidad máxima de reintentos de verificación tras los cuales la carga falla. El valor predeterminado es 10.

Las dos claves funcionan juntas para limitar los tiempos de carga de archivos. De forma predeterminada, el límite de tiempo es de 100 segundos (10000*10 milisegundos).

Renovación de certificado (en segundos)

- Especifica con cuántos segundos de antelación Citrix Endpoint Management empieza a renovar certificados previamente a su caducidad. 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 de diciembre y el 30 de diciembre, Citrix Endpoint Management intenta renovar el certificado. El valor predeterminado es **2 592 000** segundos (30 días).

Tiempo de espera de la conexión

- El tiempo de espera de la sesión inactiva, en minutos, transcurrido el cual Citrix Endpoint Management cierra la conexión TCP con un dispositivo. La sesión permanece abierta. Se aplica a dispositivos Android. El valor predeterminado es **5** minutos.

Canal de implementación predeterminado

- Determina la forma en que 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**.

Retirar proveedor de servicios móviles

- Retira la interfaz del proveedor de servicios móviles que se utiliza para enviar consultas a dispositivos BlackBerry y otros dispositivos Exchange ActiveSync. Mientras se habilite, la interfaz del **proveedor de servicios móviles** se oculta de la consola. El valor predeterminado es **true**.

Etiquetado de dispositivos

- Si establece `enable.device.tagging` en **true**, Citrix Endpoint Management etiqueta los dispositivos por tipo de dispositivo automáticamente. Puede utilizar etiquetas de dispositivo

para implementar directivas y aplicaciones o configurar grupos de entrega. Citrix Endpoint Management aplica etiquetas a los dispositivos para esto:

- Etiquetas BYOD
 - * Inscripción de usuarios de iOS
 - * Perfil de trabajo de Android Enterprise
- Etiquetas corporativas
 - * Dispositivos Android Enterprise corporativos totalmente administrados
 - * Inscripción en bloque
 - Dispositivos Apple Business Manager
 - Dispositivos Apple School Manager
 - Dispositivos Windows Autopilot
 - Inscripción en bloque de Android Enterprise

Inhabilitar la verificación del nombre de host

- De forma predeterminada, la verificación de nombres de host está habilitada en las conexiones salientes, excepto para el servidor PKI de Microsoft. Cuando se produce un error en la verificación de nombres de host, el registro del servidor contiene errores del tipo: “No se puede conectar con el servidor de compras por volumen: El nombre de host ‘192.0.2.0’ no coincide con el sujeto de certificado suministrado por el servidor homólogo”. Si la verificación de nombres de host deja inoperativa la implementación, cambie esta propiedad a **true**. El valor predeterminado es **false**.

Inhabilitar verificación del servidor SSL

- Si tiene el valor **true**, inhabilita la validación de certificados SSL de servidor cuando se cumplen todas las condiciones siguientes:
 - Ha habilitado la autenticación basada en certificados en Citrix Endpoint Management
 - El servidor de CA de Microsoft es el emisor del certificado
 - Ha firmado el certificado una CA interna en cuya raíz no confía Citrix Endpoint Management.

El valor predeterminado es **true**.

Enable Crash Reporting (Habilitar informes de errores)

- Si tiene el valor **true**, Citrix recopila informes de errores y diagnósticos para ayudar a solucionar problemas con Citrix Secure Hub para iOS y Android. Si el valor es **false**, no se recopilan datos. El valor predeterminado es **true**.

Habilitar/inhabilitar la captura de registros de estadísticas de Hibernate para diagnósticos

- Si tiene el valor **true**, se habilita la captura de estadísticas de Hibernate para ayudar a resolver problemas de rendimiento de aplicaciones. Hibernate es un componente que se utiliza para las conexiones de Citrix Endpoint Management a un servidor SQL de Microsoft. De forma predeterminada, esta captura de registros está inhabilitada porque tiene un impacto en el rendimiento de las aplicaciones. Habilite esta captura de registros solo durante un espacio corto de tiempo para evitar crear un archivo de registros demasiado grande. Citrix Endpoint Management escribe los registros en `/opt/sas/logs/hibernate_stats.log`. El valor predeterminado es **False**.

Enable macOS OTAE (Habilitar OTAE de macOS)

- Si tiene el valor **false**, impide que se use un enlace de inscripción para dispositivos macOS, lo que significa que los usuarios de macOS solo pueden inscribirse con una invitación de inscripción. El valor predeterminado es **true**.

Habilitar desencadenante de notificaciones

- Habilita o inhabilita las notificaciones de cliente de Citrix Secure Hub. El valor **true** habilita las notificaciones. El valor predeterminado es **true**.

Extracción completa de usuarios permitidos y prohibidos de ActiveSync

- El intervalo (en segundos) tras el que Citrix Endpoint Management extrae una lista completa (referencia) de los 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 Customer Experience Improvement Program (CEIP). Puede elegir si participar en CEIP al instalar o actualizar Citrix Endpoint Management. Si Citrix Endpoint Management experimenta 15 cargas fallidas consecutivas, se inhabilita la telemetría. El valor predeterminado es **false**.

Tiempo de espera por inactividad en minutos

- El número de minutos, transcurridos 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 una aplicación de terceros.

Un tiempo de espera de **0** significa que no se cerrará la sesión del usuario inactivo. Para las aplicaciones de terceros que acceden a la API, normalmente es necesario iniciar sesión. El valor predeterminado es **5**.

- Si la propiedad de servidor **WebServices timeout type** (Tipo de tiempo de espera de los servicios web) es **INACTIVITY_TIMEOUT**, esta propiedad define la cantidad de minutos tras los que Citrix Endpoint Management cierra la sesión de un administrador inactivo que haya hecho lo siguiente:
 - Ha utilizado la API pública para servicios de REST para acceder a la consola de Citrix Endpoint Management
 - Ha utilizado la API pública para servicios de REST para acceder a una aplicación de terceros.Un tiempo de espera de **0** significa que no se cierra la sesión de un usuario inactivo.

include.device.properties.during.search

- Incluye todas las propiedades del dispositivo en una búsqueda de dispositivos. Está **desactivado** de forma predeterminada, lo que limita el ámbito de búsqueda a estas propiedades de 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 está **activada**, las búsquedas de dispositivos pueden tardar más tiempo.

ios.delayBeforeDeclareUnreachable; macos.delayBeforeDeclareUnreachable

- Especifica la cantidad 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 consultar Citrix Endpoint Management. Ambas propiedades tienen un valor predeterminado de **45** días.

Inscripción en administración de dispositivos iOS: Instalar CA raíz si es necesario

- La propiedad de servidor **ios.mdm.enrollment.installRootCalfRequired** se establece 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 solo se utiliza para entornos locales).

Inscripción en administración de dispositivos iOS: Demora de la última etapa

- Durante la inscripción de dispositivos, este valor de propiedad especifica cuánto tiempo se espera entre la instalación del perfil de MDM y el inicio del agente en el dispositivo. Citrix recomienda no modificar esta propiedad a menos que haya mucha latencia o problemas de velocidad en la red. En ese caso, no configure un valor superior a 5000 milésimas de segundo (5 segundos). El valor predeterminado es **1000** milésimas de segundo (1 segundo).

Administración de dispositivos iOS: Modo de entrega de identidad

- Especifica si Citrix Endpoint Management distribuye el certificado MDM a los dispositivos que usan **SCEP** (recomendado por razones de seguridad) o **PKCS12**. En el modo de PKCS12, el par de claves se genera en el servidor y no se lleva a cabo ninguna negociación. El valor predeterminado es **SCEP**.

Administración de dispositivos iOS: Tamaño de clave de identidad

- Define el tamaño de las claves privadas para las identidades MDM, el servicio de perfiles de iOS y las identidades del agente iOS de Citrix Endpoint Management. El valor predeterminado es **2048**.

Administración de dispositivos iOS: Días de renovación de identidad

- Especifica con cuántos días de antelación Citrix Endpoint Management empieza a renovar certificados previamente a su fecha de caducidad. Por ejemplo, si un certificado caduca en 10 días y esta propiedad tiene un valor de **10** días, si un dispositivo se conecta 9 días antes de caducar el certificado, Citrix Endpoint Management emite uno nuevo. El valor predeterminado es **30** días.

Contraseña de clave privada de APNS de iOS MDM

- Esta propiedad contiene la contraseña de APNs, que Citrix Endpoint Management necesita para enviar notificaciones push a los servidores Apple.

Período de inactividad antes de desconectar el dispositivo

- Especifica el tiempo que un dispositivo puede permanecer inactivo, incluida la última autenticación, antes de que Citrix Endpoint Management lo desconecte. El valor predeterminado es **7** días.

Tiempo que el dispositivo puede estar inactivo antes de que se quite automáticamente de CEM

- El tiempo (en días) que un dispositivo puede estar inactivo antes de que se quite automáticamente de Citrix Endpoint Management. El mínimo es de **14** días y el valor predeterminado es de **30** días. La propiedad del 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 los minutos que debe esperar un usuario después de superar 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 consecutivos de inicio de sesión no válidos por usuario. Los valores admitidos son 0—999. El valor predeterminado se establece en **6**.

mac.dep.admin.passwd.rotate

Esta propiedad de servidor le permite configurar intervalos de rotación de contraseñas de administrador para dispositivos macOS inscritos a través del Programa de implementación de Apple. Citrix Endpoint Management comprueba si se debe rotar diariamente 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 este modo:

- Valor: *administrator-defined*
Intervalo, en minutos, en el que Citrix Endpoint Management rota la contraseña. Introduzca un valor igual o superior a 360 (6 horas). Citrix Endpoint Management ignora los valores menores que 360 y, en su lugar, rota la contraseña cada 360 minutos (6 horas).
- Nombre simplificado: *administrator-defined*
- Descripción: *administrator-defined*

MAM Only Device Max (Máximo de dispositivos administrados por MAM)

- Esta clave personalizada limita la cantidad de dispositivos de solo MAM que puede inscribir un usuario. Configure la clave de este modo. Un **valor** de **0** permite inscripciones ilimitadas de dispositivos.
- Clave = **number.of.mam.devices.per.user**
- Valor = **5**
- Nombre simplificado = **MAM Only Device Max**
- Descripción = **Limita la cantidad de dispositivos MAM que cada usuario puede inscribir.**

MaxNumberOfWorker

- La cantidad de subprocesos que se utilizan cuando se importa una gran cantidad de licencias de compras por volumen. El valor predeterminado es **3**. Si necesita mayor optimización, puede aumentar la cantidad de subprocesos. Sin embargo, una mayor cantidad de subprocesos se traduce en un uso elevado de la CPU.

Single Sign-On de NetScaler Gateway (NetScaler Gateway)

- Si el valor es **false**, se inhabilita la función de respuesta de Citrix Endpoint Management durante el inicio de sesión único Single Sign-On desde NetScaler Gateway a Citrix Endpoint Management. Citrix Endpoint Management usa la función de respuesta para verificar el ID de sesión de NetScaler Gateway si la configuración de NetScaler Gateway incluye una dirección URL de respuesta. El valor predeterminado es **False**.

Cantidad de cargas fallidas consecutivas

- Muestra la cantidad de fallos consecutivos durante cargas de Customer Experience Improvement Program (CEIP). Citrix Endpoint Management aumenta el valor cuando falla una carga. Después de 15 fallos de carga, Citrix Endpoint Management inhabilita el programa CEIP, también conocido como “telemetría”. Para obtener más información, consulte la propiedad de servidor **Identifica si la telemetría está habilitada o no**. Citrix Endpoint Management restablece el valor a **0** si una carga se realiza correctamente.

Cantidad de usuarios por dispositivo

- La cantidad máxima de usuarios que pueden inscribir el mismo dispositivo en MDM. El valor **0** significa que una cantidad ilimitada de usuarios puede inscribir el mismo dispositivo. El valor

predeterminado es **0**.

optional.user.identity.attributes

- Esta propiedad de servidor permite personalizar los atributos de usuario opcionales de Active Directory.

Cree la clave personalizada y, en el campo **Valores**, modifique los atributos de usuario para definir los atributos a los que 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 simplificado: **optional.user.identity.attributes**
- Descripción: **Atributos de usuario opcionales de Active Directory**

Nombre de la organización para los perfiles de inscripción de macOS e iOS/iPadOS

- El valor que introduzca para `apple.mdm.enrollment.profile.organization.name` corresponderá al nombre de la organización que proporciona el perfil de inscripción. El nombre aparece cuando los usuarios inscriben sus dispositivos en Citrix Endpoint Management. El nombre predeterminado que aparece es **Citrix Workspace**.

Extracción de cambios incrementales de usuarios permitidos y prohibidos

- Los segundos durante los que Citrix Endpoint Management espera una respuesta de parte del dominio tras ejecutar un comando de PowerShell para obtener la información nueva de dispositivos de ActiveSync. El valor predeterminado es **60** segundos.

Tiempo de espera de lectura de Microsoft Certification Server

- Los segundos durante los que Citrix Endpoint Management espera una respuesta del servidor de certificados al llevar a cabo una lectura. Si el servidor de certificados es lento y tiene una gran cantidad de tráfico, puede aumentar este valor a 60 segundos o más. Un servidor de certificados

que no responda al cabo de 120 segundos necesita mantenimiento. El valor predeterminado es **15000** milésimas de segundo (15 segundos).

REST Web Services (Servicios web de REST)

- Permite el servicio web de REST. El valor predeterminado es **true**.

Obtiene información de dispositivos en fragmentos de un tamaño especificado

- Este valor se usa internamente para subprocesamientos múltiples durante exportaciones de dispositivos. Si el valor es superior, un solo subproceso analiza varios dispositivos. Si el valor es inferior, varios subprocesos obtienen los dispositivos. Reducir el valor puede aumentar el rendimiento de exportaciones y la lista de dispositivos exportados, aunque puede reducir la memoria disponible. El valor predeterminado es **1000**.

shp.console.enable

- Si tiene el valor **false**, impide el acceso a Self Help Portal. Los usuarios que navegan al portal en el puerto 4443 reciben el mensaje “Acceso denegado”. Si tiene el valor **true**, ofrece acceso a Self-Help Portal a través del puerto 443.

El valor predeterminado es **False**.

enable.new.shp

- Si es **False**, impide que los usuarios puedan habilitar sus dispositivos desde Self-Help Portal. Si es **True**, los usuarios pueden habilitar sus dispositivos desde Self-Help Portal.

La función de clave de recuperación de BitLocker requiere que establezca esta propiedad en **False** y la propiedad `shp.console.enable` en **True**.

El valor predeterminado es **False**.

Limpieza de registros de sesiones (días)

- La cantidad de días que Citrix Endpoint Management conserva los registros 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** solo ofrece acceso a los conectores de zonas de almacenamiento que haya creado desde la consola de Citrix Endpoint Management. El valor predeterminado es **NONE**, lo que muestra la vista inicial de la pantalla **Configure > Citrix Files**, desde donde elige entre los conectores y Citrix Files Enterprise. 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 la cantidad de minutos tras los que Citrix Endpoint Management cierra la sesión de un administrador que haya utilizado:
 - La API pública para servicios de REST para acceder a la consola de Citrix Endpoint Management.
 - La API pública para servicios de REST para acceder a una aplicación de terceros.

El valor predeterminado es **60**.

Desencadenar supresión de mensajes del agente

- Habilita o inhabilita la mensajería de cliente de Citrix Secure Hub. El valor **false** habilita la mensajería. El valor predeterminado es **true**.

Desencadenar supresión de sonido del agente

- Habilita o inhabilita los sonidos de cliente de Citrix Secure Hub. El valor **false** habilita los sonidos. El valor predeterminado es **true**.

Descarga de aplicaciones no autenticada para dispositivos Android

- Si el valor es **True**, se pueden descargar aplicaciones autoalojadas en dispositivos Android que ejecutan Android Enterprise. Citrix Endpoint Management necesita esta propiedad si está habilitada la opción de Android Enterprise para suministrar una URL de descarga en la tienda de Google Play de forma estática. En ese caso, las direcciones URL de descarga no pueden incluir un tíquet de uso único (definido por la propiedad de servidor **Tíquet XAM de uso único**) que tiene el token de autenticación. El valor predeterminado es **False**.

Descarga de aplicaciones no autenticada para dispositivos Windows

- Solo se utiliza para versiones anteriores de Citrix Secure Hub que no validan los tíquets de un solo uso. Si el valor es **False**, puede descargar aplicaciones no autenticadas desde Citrix Endpoint Management en dispositivos Windows. El valor predeterminado es **False**.

Usar ID de ActiveSync para realizar un borrado de dispositivo ActiveSync

- Si el valor es **true**, el conector de Citrix Endpoint Management para Exchange ActiveSync usa el identificador de ActiveSync como argumento para el método **asWipeDevice**. El valor predeterminado es **false**.

Usuarios de Exchange solamente

- Si es **true**, inhabilita la autenticación de los usuarios de ActiveSync Exchange. El valor predeterminado es **false**.

Intervalo de referencia de compras por volumen

- El intervalo mínimo tras el que Citrix Endpoint Management vuelve a importar licencias de compras por volumen de Apple. Actualizar la información de las licencias garantiza que Citrix Endpoint Management refleja todos los cambios (por ejemplo, si elimina manualmente una aplicación importada del programa de compras por volumen). De forma predeterminada, Citrix Endpoint Management actualiza el punto de referencia para las licencias del programa de compras por volumen cada **1440** minutos como mínimo.
 - Si tiene una gran cantidad de licencias de compras por volumen instaladas (por ejemplo, más de 50 000), Citrix recomienda aumentar el intervalo del punto de referencia para reducir la frecuencia de la importación de licencias y el consumo de recursos que eso conlleva.
 - Si espera cambios frecuentes en las licencias de compras por volumen por parte de Apple, Citrix recomienda reducir el valor para mantener Citrix Endpoint Management actualizado con los cambios.
 - El intervalo mínimo entre dos puntos de referencia es de 60 minutos. Además, Citrix Endpoint Management lleva a cabo una importación delta cada 60 minutos, para obtener los cambios realizados desde la última importación. Por lo tanto, si el intervalo de referencia de compras por volumen es de 60 minutos, el intervalo entre los puntos de referencia puede retrasarse hasta 119 minutos.

Tipo de tiempo de espera de los servicios web

- Especifica cómo hacer caducar un token de autenticación obtenido desde la API pública.
 - Si es **STATIC_TIMEOUT**: Citrix Endpoint Management considera caducado un token basándose en el valor de la propiedad de servidor **Tiempo de espera estático en minutos**.
 - Si es **INACTIVITY_TIMEOUT**: Citrix Endpoint Management considera caducado un token basándose en el valor de la propiedad de servidor **Tiempo de espera por inactividad en minutos**. El valor predeterminado es **STATIC_TIMEOUT**.

Validez extendida de certificado MDM de tabletas Windows (5 años)

- El período de validez del certificado del dispositivo emitido por MDM para tabletas Windows. Los dispositivos usan un certificado de dispositivo para autenticarse en el servidor MDM durante la administración de dispositivos. Si tiene el valor **true**, el período de validez es de cinco años. Si el valor es **false**, el período de validez es de dos años. El valor predeterminado es **true**.

Windows WNS Channel - Number of Days Before Renewal (Canal Windows WNS: Cantidad de días antes de la renovación)

- La frecuencia de renovación de ChannelURI. El valor predeterminado es **10** días.

Windows WNS Heartbeat Interval (Intervalo de latido de Windows WNS)

- El tiempo que espera Citrix Endpoint Management antes de conectarse a un dispositivo tras haberse conectado a él cinco veces cada 3 minutos. El valor predeterminado es **6** horas.

Tíquet XAM de uso único

- El período de tiempo, en milisegundos, durante el cual un token de autenticación de un solo uso (OTT) se considera válido para descargar una aplicación. Esta propiedad se utiliza con las propiedades **Descarga de aplicaciones no autenticada para dispositivos Android** y **Descarga de aplicaciones no autenticada para dispositivos Windows**. Esas propiedades especifican si permitir descargas no autenticadas de aplicaciones. El valor predeterminado es **3600000**.

Citrix Endpoint Management MDM Self-Help Portal console max inactive interval (minutes)
[Intervalo máximo de inactividad para la consola de Citrix Endpoint Management MDM Self-Help Portal (en minutos)]

- Este nombre de propiedad refleja las versiones anteriores de Citrix Endpoint Management. La propiedad controla el intervalo máximo de inactividad en la consola de Citrix Endpoint Management. Ese intervalo es la cantidad de minutos, transcurridos 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 no se cierra la sesión del usuario inactivo. El valor predeterminado es **30**.

Directivas de aplicación y de dispositivo

March 1, 2024

Las directivas de dispositivo y aplicación de Citrix Endpoint Management permiten optimizar el equilibrio entre los siguientes factores:

- Seguridad de la empresa
- Protección de datos y activos de la empresa
- Privacidad de los usuarios
- Experiencias de usuario productivas y positivas

El equilibrio óptimo entre esos factores puede variar. Por ejemplo, las organizaciones altamente reguladas (como las del ámbito de finanzas), requieren controles de seguridad más estrictos que las empresas de otros sectores (como la educación y el comercio), donde la productividad del usuario es una consideración primordial.

Puede controlar y configurar de manera centralizada las directivas 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. En caso de pérdida o robo de un dispositivo, puede desactivar, bloquear o borrar las aplicaciones y los datos corporativos de forma remota. El resultado global es una solución que aumenta la satisfacción y la productividad de los empleados, al mismo tiempo que garantiza la seguridad y el control administrativo.

El enfoque principal de este artículo es la cantidad de directivas de dispositivo y aplicación relacionadas con la seguridad.

Directivas que abordan los riesgos de seguridad

Las directivas de dispositivo y aplicación de Citrix Endpoint Management abordan muchas situaciones que pueden poner en riesgo la seguridad, como cuando:

- Los usuarios intentan acceder a aplicaciones y datos desde dispositivos con los que no existe una relación de confianza y desde ubicaciones inesperadas
- Los usuarios pasan datos entre dispositivos
- Un usuario no autorizado trata de acceder a los datos
- Un usuario que usaba su propio dispositivo (BYOD) deja la empresa
- Un usuario pierde de vista un dispositivo
- Los usuarios siempre deben acceder a la red de forma segura
- Los usuarios tienen su propio dispositivo administrado y se necesita separar los datos de trabajo de los datos personales
- Un dispositivo está inactivo y se requiere la verificación de las credenciales de usuario de nuevo
- Los usuarios copian y pegan contenido confidencial en sistemas de correo electrónico no protegidos
- Los usuarios reciben datos adjuntos de correo electrónico o enlaces web con datos confidenciales en un dispositivo que contiene tanto cuentas personales como empresariales

Estas circunstancias están relacionadas con las dos áreas principales que adquieren importancia cuando se trata de proteger los datos de empresa, que se dan cuando los datos:

- Están en reposo
- En tránsito

Cómo protege Citrix Endpoint Management los datos en reposo

Los datos almacenados en dispositivos móviles se denominan datos en reposo. Citrix Endpoint Management utiliza el cifrado de dispositivo que proporcionan las plataformas iOS y Android. Citrix Endpoint Management complementa el cifrado por plataforma con funciones como los controles de conformidad, disponibles a través del SDK de Citrix MAM.

En Citrix Endpoint Management, las funciones de administración de aplicaciones móviles (MAM) permiten una administración, una seguridad y un control completos sobre las aplicaciones móviles de productividad de Citrix, las aplicaciones habilitadas para MDX y sus datos asociados.

Mobile Apps SDK permite la implementación de aplicaciones a Citrix Endpoint Management gracias a la tecnología de contenedor de aplicaciones Citrix MDX. La tecnología de contenedor separa las aplicaciones corporativas, los datos de las aplicaciones personales y los datos de un dispositivo de usuario. La separación de datos permite proteger cualquier aplicación móvil propia, de terceros o desarrollada a medida con la ayuda de controles exhaustivos basados en directivas.

Citrix Endpoint Management también incluye cifrado a nivel de aplicación. Citrix Endpoint Management cifra por separado los datos almacenados en una aplicación habilitada para MDX sin necesidad de un código de acceso de dispositivo y sin requerir que usted administre el dispositivo para aplicar la directiva.

- En dispositivos iOS, Citrix Endpoint Management utiliza bibliotecas y servicios criptográficos sólidos validados por FIPS, como llaveros.
- OpenSSL proporciona módulos validados por FIPS para distintas plataformas de dispositivos e intensifica la protección de los datos en movimiento y los certificados necesarios para administrar e inscribir los dispositivos.
- Citrix Endpoint Management utiliza la API de caja fuerte compartida del SDK de MAM para compartir contenido administrado entre las aplicaciones que tienen el mismo grupo de Acceso a Llaveros. Por ejemplo, puede compartir certificados de usuario a través de una aplicación inscrita, de modo que las aplicaciones pueden obtener un certificado de la caja fuerte segura.
- Citrix Endpoint Management utiliza el cifrado de dispositivo que proporcionan las plataformas.
- Los controles MAM de Citrix Endpoint Management a nivel de aplicación realizan una comprobación de conformidad para validar que el cifrado de dispositivos esté habilitado cada vez que se inicia una aplicación.

Cómo protege Citrix Endpoint Management los datos en tránsito

Los datos que se estén transfiriendo entre los dispositivos móviles del usuario y la red interna se conocen como datos en tránsito. La tecnología del contenedor de aplicaciones MDX ofrece el acceso VPN por aplicación a la red interna a través de NetScaler Gateway.

Tenga en cuenta los casos en que un empleado quiera acceder desde un dispositivo móvil a estos recursos que residen en la red empresarial segura:

- El servidor de correo electrónico corporativo
- Una aplicación web con SSL habilitado alojada en la intranet corporativa
- Documentos almacenados en un servidor de archivos o Microsoft SharePoint

MDX permite el acceso a todos esos recursos de la empresa desde dispositivos móviles a través de una micro VPN específica para cada aplicación. Cada dispositivo dispone de su propio túnel micro VPN dedicado.

La funcionalidad Micro VPN no requiere de una VPN para todo el dispositivo, lo que puede poner en peligro la seguridad en los dispositivos móviles que no son de confianza. Como resultado, la red interna no está expuesta al malware ni a ataques que podrían infectar todo el sistema corporativo. Las aplicaciones móviles de empresa y las aplicaciones móviles personales pueden coexistir en un solo dispositivo.

Para ofrecer niveles de seguridad más altos, puede configurar aplicaciones habilitadas para MDX con una directiva Dispositivo NetScaler Gateway alternativo. La directiva se utiliza para la autenticación y para sesiones de micro VPN con una aplicación. Puede utilizar la directiva “Dispositivo NetScaler Gateway alternativo” junto con la directiva “Sesión de micro VPN requerida” para obligar a las aplicaciones a volver a autenticarse en la puerta de enlace específica. Estas puertas de enlace suelen tener directivas de administración de tráfico y requisitos de autenticación diferentes (mayor nivel de control).

Además de las funciones de seguridad, la funcionalidad micro VPN también ofrece técnicas de optimización de datos, incluidos algoritmos de compresión. Los algoritmos de compresión garantizan que:

- Solo se transfieren datos mínimos.
- La transferencia se realiza en el tiempo más rápido posible. La velocidad mejora la experiencia del usuario, que es un factor clave de éxito en la adopción de dispositivos móviles.

Debe volver a evaluar las directivas de dispositivo periódicamente, como en estas situaciones:

- Cuando una nueva versión de Citrix Endpoint Management incluye directivas nuevas o actualizadas debido a la publicación de actualizaciones para el sistema operativo del dispositivo.
- Cuando agrega un tipo de dispositivo:

Aunque muchas directivas sean las mismas para todos los dispositivos, cada dispositivo tiene un conjunto específico de directivas para su sistema operativo. En consecuencia, se pueden encontrar muchas diferencias entre dispositivos iOS, Android y Windows, e incluso entre los dispositivos Android de diferentes fabricantes.

- Para mantener el funcionamiento de Citrix Endpoint Management sincronizado con los cambios empresariales o industriales, como nuevas directrices de seguridad o nuevas normativas corporativas.
- Cuando una nueva versión del SDK de MAM incluye directivas nuevas o actualizadas
- Cuando agrega o actualiza una aplicación.
- Cuando necesita integrar nuevos flujos de trabajo para sus usuarios debido a aplicaciones o requisitos nuevos.

Directivas de aplicación y casos de uso

Aunque puede elegir las aplicaciones que estarán disponibles a través de Citrix Secure Hub, puede que también le interese definir cómo interactúan esas aplicaciones con Citrix Endpoint Management. Use directivas de aplicación:

- Si quiere que los usuarios se autenticquen después de un determinado período de tiempo.

- Si quiere ofrecer a los usuarios acceso sin conexión a la 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 [Introducción al SDK de MAM](#).
- Para ver una lista de todas las directivas MDX desglosadas por plataforma, consulte [Directivas MDX](#).

Directivas de autenticación

- **Código de acceso de dispositivo**

Por qué usar esta directiva: Habilite la directiva “Código de acceso del dispositivo” para estipular que un usuario solo pueda acceder a una aplicación MDX si el dispositivo tiene un código de acceso de dispositivo habilitado. Esta función garantiza el uso del cifrado de iOS al nivel del dispositivo.

Ejemplo para el usuario: Habilitar esta directiva significa que el usuario debe definir un código de acceso en su dispositivo iOS para poder acceder a la aplicación MDX.

- **Código de acceso de aplicación**

Por qué usar esta directiva: Habilite la directiva “Código de acceso de aplicación” para que Citrix Secure Hub pida al usuario que se autentique en la aplicación administrada para poder abrirla y acceder a los datos. El usuario puede autenticarse con su contraseña de Active Directory, el PIN de Citrix o TouchID de iOS, dependiendo de 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 pida al usuario que se autentique en la aplicación administrada nuevamente hasta que el temporizador expire.

El código de acceso de la aplicación difiere del código de acceso de un dispositivo. Con una directiva de código de acceso de dispositivo presente en un dispositivo, Citrix Secure Hub solicita al usuario que configure un código de acceso o un PIN. El usuario debe desbloquear su dispositivo cuando lo encienda o cuando caduque el temporizador de inactividad. Para obtener más información, consulte [Autenticación en Citrix Endpoint Management](#).

Ejemplo para el usuario: Al abrir la aplicación Citrix Secure Web en el dispositivo, el usuario debe introducir su PIN de Citrix para poder navegar por sitios web si ha transcurrido el período de inactividad.

- **Sesión de micro VPN requerida**

Por qué utilizar esta directiva: Si una aplicación requiere acceso a una aplicación web (servicio web) para ejecutarse, habilite esta directiva. Citrix Endpoint Management pide al usuario que se conecte a la red empresarial o que tenga una sesión activa antes de usar la aplicación.

Ejemplo para el usuario: Cuando un usuario intenta abrir una aplicación MDX que tiene habilitada la directiva “Sesión de micro VPN requerida”, no puede utilizar 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 utilizar 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 que tienen derecho a usar esa aplicación y actualizar las directivas.

Ejemplo para el usuario: Si configura una aplicación MDX con un “Período máximo sin conexión”, los usuarios pueden abrir y utilizar la aplicación sin conectarse a la red hasta que caduque el período del temporizador sin conexión. En ese momento, el usuario debe volver a conectarse a la red a través del servicio móvil o Wi-Fi y volver a autenticarse, si se le solicita.

Otras directivas de acceso

- **Período de gracia de actualización de aplicación (horas)**

Por qué usar esta directiva: El período de gracia para la actualización de aplicaciones es el tiempo de que dispone el usuario para actualizar una aplicación que tenga una versión más reciente publicada en el almacén de aplicaciones. Transcurrido este período, el usuario debe actualizar la aplicación para poder acceder a los datos que esta contiene. Cuando establezca el valor de esta directiva, tenga en cuenta las necesidades de su personal móvil, en particular las necesidades de aquellos empleados que podrían verse expuestos a largos períodos sin conexión durante viajes internacionales.

Ejemplo para el usuario: Se carga una nueva versión de Citrix Secure Mail en el almacén de aplicaciones y, a continuación, se establece un período de gracia para la actualización de aplicaciones de 6 horas. Los usuarios de Citrix Secure Hub disponen de 6 horas para actualizar Citrix Secure Mail antes de que se enruten a la tienda de aplicaciones.

- **Período de sondeo activo (minutos)**

Por qué usar esta directiva: El período de sondeo activo es el intervalo durante el cual Citrix Endpoint Management examina las aplicaciones para realizar acciones de seguridad, tales como el bloqueo de aplicaciones y el borrado de aplicaciones.

Ejemplo para el usuario: Si establece la directiva “Período de sondeo activo” en 60 minutos y envía el comando “Bloqueo de aplicaciones”, el bloqueo se producirá durante los 60 minutos siguientes después del último sondeo.

Directivas de comportamiento de dispositivos no conformes

Cuando un dispositivo no cumple todos los requisitos mínimos de conformidad, la directiva Comportamiento de dispositivos no conformes le permite seleccionar qué hacer al respecto. Para obtener información, consulte [Comportamiento de dispositivos no conformes](#).

Directivas de interacción entre aplicaciones

Por qué usar estas directivas: Puede usar las directivas de interacción entre aplicaciones para controlar el flujo de documentos y datos desde las aplicaciones MDX a otras aplicaciones en el dispositivo. Por ejemplo, puede impedir que un usuario:

- mueva datos a sus aplicaciones personales fuera del contenedor
- pegue datos desde fuera del contenedor en las aplicaciones del contenedor

Ejemplo para el usuario: Usted establece la directiva “Interacción entre aplicaciones” en “Restringida”, lo que significa que un usuario puede copiar texto desde Citrix Secure Mail a Citrix Secure Web. Sin embargo, el usuario no puede copiar esos datos a su explorador personal Safari o Chrome que está fuera del contenedor. Además, un usuario puede abrir un documento adjunto desde Citrix Secure Mail en Citrix Files o QuickEdit. Sin embargo, el usuario no puede abrir el documento adjunto en sus propias aplicaciones de visualización de archivos personales que están fuera del contenedor.

Directivas de restricciones a aplicaciones

Por qué usar estas directivas: Puede usar las directivas de restricciones a aplicaciones para controlar a qué funciones pueden acceder los usuarios mientras está abierta una aplicación MDX. La restricción ayuda a garantizar que no haya actividades maliciosas mientras se ejecuta la aplicación. Las directivas de restricciones a aplicaciones varían ligeramente entre iOS y Android. Por ejemplo, en iOS puede bloquear el acceso a iCloud mientras se ejecuta la aplicación MDX. En Android, puede detener el uso de NFC mientras se ejecuta la aplicación MDX.

Ejemplo para el usuario: Si se habilita la directiva “Restricciones a aplicaciones” para bloquear el dictado en una aplicación MDX en iOS, el usuario no puede usar la función de dictado en el teclado iOS mientras se ejecuta la aplicación MDX. Por lo tanto, los datos que dictan los usuarios no se transfieren al servicio, no seguro, de dictado en la nube de terceros. Cuando el usuario abre sus aplicaciones personales fuera del contenedor, la opción de dictado permanece disponible para el usuario para las comunicaciones personales.

Directivas de acceso de las aplicaciones a la red

Por qué usar estas directivas: Puede utilizar las directivas del acceso de las aplicaciones a la red para proporcionar el acceso desde una aplicación MDX ubicada en el contenedor del dispositivo a los datos que se encuentran dentro de la red corporativa. La opción Túnel - SSO web solo permite el envío por túnel del tráfico HTTP y HTTPS. Esta opción proporciona Single Sign-On (SSO) para el tráfico HTTP y HTTPS y la autenticación PKINIT.

Ejemplo para el usuario: Cuando un usuario abre una aplicación MDX que tiene habilitado el túnel, el explorador web abre un sitio de intranet sin que el usuario tenga que iniciar una VPN. La aplicación accede automáticamente al sitio interno mediante la tecnología de red micro VPN.

Directivas de geocercas y geolocalización de aplicaciones

Por qué usar estas directivas: Las directivas que controlan las geocercas y la geolocalización de aplicaciones incluyen la longitud del punto central, la latitud del punto central y el radio. Esas directivas limitan el acceso a los datos en las aplicaciones MDX en función de un área geográfica específica. Las directivas definen un área geográfica por un radio y unas 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 para el usuario: Un usuario puede acceder a los datos de fusión y adquisición mientras se encuentra en su oficina. Cuando sale de su oficina, esos datos confidenciales dejan de estar accesibles.

Directivas de 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 usan Secure Ticket Authority (STA), que es a efectos prácticos un proxy SOCKS5 para conectarse a través de NetScaler Gateway. STA admite conexiones de larga duración y ofrece una mejor duración de la batería que una red micro VPN. Por lo tanto, STA es ideal para aplicaciones de correo, que se conectan constantemente. Citrix recomienda configurar estos parámetros para Citrix Secure Mail. El asistente de NetScaler para XenMobile establece automáticamente STA para Citrix Secure Mail.

Ejemplo para el usuario: Cuando STA no está habilitado y un usuario Android abre Citrix Secure Mail, se le solicita que abra una VPN, que permanece abierta en el dispositivo. Cuando STA está habilitado y el usuario Android abre Citrix Secure Mail, esta aplicación se conecta 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. Cuantos más datos haya que sincronizar, más dura el proceso de configuración para el usuario.

Ejemplo para el usuario: Por ejemplo, el intervalo de sincronización predeterminado se establece en tres días cuando el usuario configura Citrix Secure Mail por primera vez. Entonces, el usuario verá todos los correos electrónicos de su bandeja de entrada que ha recibido en los últimos tres días. Si el usuario quiere ver mensajes anteriores a tres días, puede buscarlos. Tras la búsqueda, Citrix Secure Mail muestra los mensajes anteriores almacenados en el servidor. Después de instalar Citrix Secure Mail, cada usuario puede cambiar este parámetro para adaptarlo mejor a sus necesidades.

Directivas de dispositivo y comportamiento de caso de uso

Las directivas de dispositivo, también conocidas como directivas MDM, determinan cómo Citrix Endpoint Management administra los dispositivos. Aunque muchas directivas sean las mismas para todos los dispositivos, cada dispositivo tiene un conjunto específico de directivas para su sistema operativo. En la siguiente lista se incluyen algunas de las directivas de dispositivo y se describe cómo se pueden usar. Para ver una lista de todas las directivas de dispositivo, consulte el artículo de [Directivas de dispositivo](#).

- **Directiva de inventario de aplicaciones**

Por qué usar esta directiva: Implemente la directiva “Inventario de aplicaciones” en un dispositivo si quiere ver las aplicaciones que haya instalado un usuario. Si no implementa la directiva, solo verá las aplicaciones que un usuario haya instalado desde la tienda de aplicaciones, no las aplicaciones que haya instalado personalmente. Use la directiva “Inventario de aplicaciones” si quiere prohibir la ejecución de determinadas aplicaciones en los dispositivos de empresa.

Ejemplo para el usuario: Un usuario con un dispositivo MDM administrado no puede inhabilitar esta funcionalidad. Los administradores de Citrix Endpoint Management pueden ver las aplicaciones que el usuario se haya instalado personalmente.

- **Directiva de bloqueo de aplicaciones**

Por qué usar esta directiva: En Android, la directiva “Bloqueo de aplicaciones” permite incluir las aplicaciones en una lista de aplicaciones permitidas o una lista de aplicaciones bloqueadas. Por ejemplo, con las aplicaciones permitidas, puede configurar un dispositivo como quiosco. Por lo general, la directiva “Bloqueo de aplicaciones” solo se implementa en dispositivos de

empresa, ya que limita las aplicaciones que los usuarios pueden instalar. Puede establecer una contraseña de anulación para ofrecer acceso a las aplicaciones bloqueadas.

Ejemplo para el usuario: Supongamos que implementa una directiva “Bloqueo de aplicaciones” que bloquea la aplicación Angry Birds. El usuario puede instalarse la aplicación Angry Birds desde Google Play, pero, cuando intenta abrirla, un mensaje le informa que el administrador ha bloqueado la aplicación.

- **Directiva de programación de conexiones**

Por qué usar esta directiva: La directiva “Programación de conexiones” permite que los dispositivos Windows Mobile se conecten a Citrix Endpoint Management para la implementación de directivas, el envío de aplicaciones y la administración MDM. Para dispositivos Android y Android Enterprise, use Google Firebase Cloud Messaging (FCM). FCM controla las conexiones a Citrix Endpoint Management. Las opciones de programación son:

- **Nunca:** Se conecta manualmente. Los usuarios deben iniciar la conexión desde la instancia de Citrix Endpoint Management presente en sus dispositivos. Citrix no recomienda esta opción para las implementaciones de producción, ya que le impide implementar directivas de seguridad en los dispositivos. Por lo tanto, los usuarios no reciben nunca aplicaciones ni directivas nuevas. La opción **Nunca** está habilitada de forma predeterminada.
- **Cada:** Se conecta en el intervalo elegido. Cuando se envía una directiva de seguridad (como un bloqueo o un borrado), Citrix Endpoint Management procesa la directiva en el dispositivo la próxima vez que el dispositivo se conecta.
- **Definir programación:** Citrix Endpoint Management intenta volver a conectar el dispositivo del usuario al servidor de Citrix Endpoint Management después de perder la conexión de red. Citrix Endpoint Management supervisa la conexión transmitiendo paquetes de control a intervalos periódicos durante la franja de tiempo que usted indique.

Ejemplo para el usuario: Quiere implementar una directiva “Código de acceso” en los dispositivos inscritos. La directiva de programación garantiza que los dispositivos se conecten al servidor en un intervalo periódico para recopilar la nueva directiva.

- **Directiva de credenciales**

Por qué usar esta directiva: A menudo se usa con una directiva de redes. La directiva Credenciales permite implementar certificados para la autenticación en recursos internos que requieren la autenticación por certificado.

Ejemplo para el usuario: Usted implementa una directiva de redes que configura una red inalámbrica en el dispositivo. La red Wi-Fi requiere un certificado para la autenticación. La directiva “Credenciales” implementa un certificado que se almacena en el almacén de claves del sistema operativo. El usuario puede seleccionar el certificado cuando está conectado al recurso interno.

- **Directiva de Exchange**

Por qué usar esta directiva: Con Citrix Endpoint Management, tiene dos opciones para entregar el correo electrónico de Microsoft Exchange ActiveSync.

- **La aplicación Citrix Secure Mail:** Puede entregar el correo electrónico a través de la aplicación Citrix Secure Mail, que usted distribuye desde el almacén de aplicaciones, público o no.
- **Aplicación nativa de correo:** Habilite el correo electrónico ActiveSync para el cliente de correo nativo del dispositivo. Puede usar macros para rellenar los datos de usuario desde sus atributos de Active Directory, por ejemplo, `${ user.username }` para rellenar el nombre de usuario y `${ user.domain }` para rellenar el dominio de usuario.

Ejemplo para el usuario: Cuando envía la directiva “Exchange”, envía también los detalles del servidor Exchange al dispositivo. A continuación, Citrix Secure Hub solicita al usuario que se autentique y el correo electrónico comienza a sincronizarse.

- **Directiva de localización geográfica**

Por qué usar esta directiva: La directiva “Localización geográfica” se puede usar para ubicar geográficamente los dispositivos en un mapa, siempre que el dispositivo tenga habilitado el GPS para Citrix Secure Hub. Tras implementar esta directiva, si envía un comando de localización geográfica desde Citrix Endpoint Management, y el dispositivo responde con las coordenadas de la ubicación.

Ejemplo para el usuario: Cuando implementa la directiva “Localización” y el GPS está habilitado en el dispositivo, si el usuario pierde su dispositivo, puede iniciar sesión en Citrix Endpoint Management Self Help Portal y elegir la opción de localización para ver la ubicación de su dispositivo en un mapa. Un usuario elige si permite que Citrix Secure Hub utilice los servicios de localización. Los servicios de localización geográfica no se pueden aplicar cuando los usuarios inscriben un dispositivo por sí mismos. Otra consideración a tener en cuenta a la hora de usar esta directiva es el efecto sobre la duración de la batería.

- **directiva de código de acceso**

Por qué usar esta directiva: La directiva “Código de acceso” permite imponer un código de acceso (PIN o contraseña) en un dispositivo administrado. Con esta directiva, se puede definir la complejidad y el tiempo de espera del código de acceso en el dispositivo.

Ejemplo para el usuario: Cuando implementa una directiva de código de acceso en un dispositivo administrado, Citrix Secure Hub solicita al usuario que configure un código de acceso o un PIN. El código de acceso o PIN proporciona al usuario acceso a su dispositivo durante el arranque o cuando caduca el temporizador de inactividad.

- **Directiva de eliminación de perfiles**

Por qué usar esta directiva: Supongamos que implementa una directiva a un grupo de usuarios y, más tarde, necesita quitar dicha directiva de un subconjunto de los usuarios. Puede quitar la directiva de los usuarios seleccionados mediante la creación de una directiva de eliminación de perfiles. A continuación, utilice las reglas de implementación para implementar la directiva de eliminación de perfiles solo para los usuarios especificados.

Ejemplo para el usuario: Tras implementar una directiva “Eliminación de perfiles” en los dispositivos de usuario, es posible que los usuarios no noten ningún cambio. Por ejemplo, si la directiva “Eliminación de perfiles” elimina una restricción que inhabilitaba la cámara del dispositivo, el usuario no sabrá que ahora se permite el uso de la cámara. Considere la posibilidad de avisar a los usuarios cuando se produzcan cambios que afecten a su experiencia.

- **Directiva de restricciones**

Por qué usar esta directiva: La directiva “Restricciones” le ofrece diversas opciones para bloquear y controlar las funciones y la funcionalidad de los dispositivos administrados. Puede habilitar cientos de opciones de restricción para dispositivos compatibles. Por ejemplo, puede inhabilitar la cámara o el micrófono de un dispositivo, aplicar reglas de itinerancia y aplicar el acceso a servicios de terceros, como tiendas de aplicaciones.

Ejemplo para el usuario: Si implementa una restricción en un dispositivo iOS, es posible que el usuario no pueda acceder a iCloud o al App Store.

- **Directiva de términos y condiciones**

Por qué usar esta directiva: Puede que necesite advertir a los usuarios de las implicaciones legales de tener su dispositivo administrado. Además, puede que quiera asegurarse de que los usuarios conocen los riesgos a la seguridad cuando se envían datos de empresa al dispositivo. El documento de términos y condiciones permite publicar reglas y avisos legales antes de que el usuario se inscriba.

Ejemplo para el usuario: El usuario ve la información de términos y condiciones durante el proceso de inscripción. Si no acepta las condiciones estipuladas, el proceso de inscripción finaliza y no puede acceder a los datos de empresa. Puede generar un informe que facilitar a los equipos jurídicos o de Recursos Humanos para que estos vean quién aceptó o rechazó los términos.

- **directiva de VPN**

Por qué usar esta directiva: Use la directiva “VPN” para proporcionar acceso a sistemas back-end con la ayuda de tecnología antigua de puerta de enlace VPN. La directiva admite varios proveedores de VPN, incluidos Cisco AnyConnect, Juniper y Citrix VPN. También es posible vincular esta directiva a una entidad de certificación (CA) y una VPN habilitada a demanda (siempre que la puerta de enlace VPN admita esta opción).

Ejemplo para el usuario: Con la directiva de red VPN habilitada, el dispositivo del usuario abre

una conexión VPN cuando el usuario accede a un dominio interno.

- **Directiva de clip web**

Por qué usar esta directiva: Use la directiva “Clip web” si quiere enviar a los dispositivos un icono que abra directamente un sitio web. Un clip web contiene un enlace a un sitio web y puede incluir un icono personalizado. En un dispositivo, un clip web parece un icono de aplicación.

Ejemplo para el usuario: Un usuario puede hacer clic en un icono de clip web para abrir un sitio de Internet que ofrezca los servicios que necesita. Usar un enlace web es más conveniente que escribir una dirección de enlace en un explorador web.

- **Directiva de redes**

Por qué usar esta directiva: La directiva de redes le permite implementar detalles de red inalámbrica (como el SSID, los datos de autenticación y los datos de configuración) en un dispositivo administrado.

Ejemplo para el usuario: Cuando implementa la directiva de redes, el dispositivo se conecta automáticamente a la red Wi-Fi y autentica al usuario para que este acceda a la red.

- **Directiva de almacenes de Endpoint Management**

Por qué usar esta directiva: Es un almacén de aplicaciones unificado donde los administradores pueden publicar todas las aplicaciones de empresa y todos los recursos de datos de empresa que los usuarios puedan necesitar. Un administrador puede agregar:

- Aplicaciones web, aplicaciones SaaS y aplicaciones habilitadas para el SDK de MAM o empaquetadas con MDX
- Aplicaciones móviles de productividad de Citrix
- Aplicaciones móviles nativas, como archivos .ipa o .apk
- Aplicaciones del App Store y Google Play
- Enlaces web
- Citrix Virtual Apps publicadas mediante Citrix StoreFront

Ejemplo para el usuario: Después de que un usuario inscriba el dispositivo en Citrix Endpoint Management, puede acceder al almacén de aplicaciones a través de la aplicación Citrix Secure Hub. Allí, el usuario verá todos los servicios y las aplicaciones de empresa que tiene disponibles. El usuario puede hacer clic en una aplicación para instalarla, evaluarla, revisarla y acceder a sus datos, así como descargar actualizaciones de la aplicación desde el almacén de aplicaciones.

Propiedades de cliente

March 1, 2024

En las propiedades de cliente, se ofrece información que se proporciona directamente a Citrix Secure Hub en los dispositivos de los usuarios. Puede usar estas propiedades para definir parámetros avanzados de configuración, como el PIN de Citrix. Las propiedades de cliente se pueden obtener del servicio de asistencia de Citrix.


Las propiedades de cliente están sujetas a cambios en cada versión de Citrix Secure Hub y, ocasionalmente, en las aplicaciones cliente. Para obtener información más detallada acerca de las propiedades de cliente más comunes a configurar, consulte Referencia de propiedades de cliente más adelante en este artículo.

1. En la consola de Citrix Endpoint Management, haga clic en el icono con forma de engranaje situado en la esquina superior derecha. Aparecerá la página **Parámetros**.
2. En **Cliente**, haga clic en **Propiedades de cliente**. Aparecerá la página **Propiedades de cliente**. Puede agregar, modificar y eliminar las propiedades de cliente desde esta página.

Settings > Client Properties

Client Properties

To change a property, select the property and then click Edit.

 Add

<input type="checkbox"/>	Name	Key	Value	Description	
<input type="checkbox"/>	Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	true	Enable Citrix PIN Authentication	
<input type="checkbox"/>	Enable User Password Caching	ENABLE_PASSWORD_CACHING	true	Enable User Password Caching	
<input type="checkbox"/>	Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password	
<input type="checkbox"/>	PIN Type	PASSCODE_TYPE	Numeric	PIN Type	
<input type="checkbox"/>	PIN Strength Requirement	PASSCODE_STRENGTH	Medium	PIN Strength Requirement	
<input type="checkbox"/>	PIN Length Requirement	PASSCODE_MIN_LENGTH	4	PIN Length Requirement	
<input type="checkbox"/>	PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement	
<input type="checkbox"/>	PIN History	PASSCODE_HISTORY	5	PIN History	
<input type="checkbox"/>	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**.

Settings > Client Properties > Add New Client Property

Add New Client Property

Key ?

Value *

Name *

Description *

2. Configure estos parámetros:

- **Clave:** En la lista desplegable, haga clic en la clave de propiedad que quiere agregar. **Importante:** Póngase en contacto con Citrix Support antes de actualizar los parámetros. Puede solicitar una clave especial.
- **Valor:** El valor de la propiedad seleccionada.
- **Nombre:** Introduzca un nombre para la propiedad.
- **Descripción:** Introduzca una descripción de la propiedad.

3. Haga clic en **Guardar**.

Para modificar una propiedad de cliente

1. En la tabla **Propiedades de cliente**, seleccione la propiedad de cliente que quiere modificar.

Al marcar la casilla situada junto a una propiedad de cliente, se abrirá el menú de opciones encima de la lista de propiedades de cliente. Haga clic en cualquier lugar de la lista para que el menú de opciones aparezca a la derecha de la lista.

2. Haga clic en **Edit**. Aparecerá la página **Modificar propiedad de cliente**.

Settings > Client Properties > Edit Client Property

Edit Client Property

Key	ENABLE_PASSCODE_AUTH
Value *	true
Name *	Enable Citrix PIN Authentication
Description *	Enable Citrix PIN Authentication

3. Cambie la siguiente información como corresponda:

- **Clave:** Este campo no puede cambiarse.
- **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 descartarlos.

Para eliminar una propiedad de cliente

1. En la tabla **Propiedades de cliente**, seleccione la propiedad de cliente que quiere eliminar.

Puede eliminar más de una propiedad. Para ello, marque la casilla de verificación situada 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

A continuación, se indican las propiedades de cliente predefinidas en Citrix Endpoint Management, así como sus valores predeterminados:

- **ALLOW_CLIENTSIDE_PROXY**

- Nombre simplificado: ALLOW_CLIENTSIDE_PROXY
- Si los usuarios necesitan usar un proxy que hayan configurado en sus teléfonos iOS, deje esta directiva personalizada en el valor **true**.

Es posible que algunos usuarios ya tengan un proxy configurado en **Ajustes > Wi-Fi > Configurar proxy** en sus dispositivos. Si Citrix Secure Hub no se abre para esos usuarios, lleve a cabo una de estas acciones:

- ★ Quite la configuración de proxy que haya en el 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** tiene el valor **false** y los usuarios configuran un proxy en sus dispositivos, Citrix Endpoint Management lo detectará. 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 habilitado un proxy, Citrix Endpoint Management no detecta el proxy. Por cuestiones de seguridad, le recomendamos que utilice fijación de certificados. Para obtener información sobre cómo habilitar la fijación de certificados para Citrix Secure Hub, consulte [Fijación de certificados](#).
- Para configurar esta directiva de cliente personalizada, vaya a **Parámetros > Propiedades de cliente**, agregue la clave personalizada **ALLOW_CLIENTSIDE_PROXY** y establezca el **Valor**.

• **CONTAINER_SELF_DESTRUCT_PERIOD**

- Nombre simplificado: MDX Container Self-Destruct Period (Período de autodestrucción del contenedor MDX)
- La propiedad Autodestrucción impide el acceso a Citrix Secure Hub y a aplicaciones administradas después de una cantidad determinada de días de inactividad. Transcurrido el límite de tiempo, las aplicaciones ya no pueden utilizarse. El borrado de datos consiste en borrar los datos de todas las aplicaciones instaladas, incluidos los datos de usuario y la memoria caché de la aplicación.

El período de inactividad se interpreta como el período durante el cual el servidor no recibe ninguna solicitud de autenticación para validar a un usuario. Supongamos que el valor de esta propiedad es 30 días. Si el usuario no usa una aplicación durante más de 30 días, entonces se aplica la directiva.

Esta directiva de seguridad global se aplica a las plataformas iOS y Android, y es una mejora de las directivas existentes de borrado y bloqueo de aplicaciones.

- Para agregar o configurar esta directiva global, vaya a **Parámetros > Propiedades de cliente**, y agregue la clave personalizada **CONTAINER_SELF_DESTRUCT_PERIOD**.
- Valor: Cantidad de días

• **DEVICE_LOGS_TO_IT_HELP_DESK**

- Nombre simplificado: Send device logs to IT help desk (Enviar registros del dispositivo al servicio de asistencia)
- Esta propiedad habilita o inhabilita la capacidad de enviar registros al servicio de asistencia de TI.
- Valores posibles: **true** o **false**
- Valor predeterminado: **false**

- **DISABLE_LOGGING**

- Nombre simplificado: Disable Logging
- Utilice esta propiedad para impedir que los usuarios recopilen y carguen registros desde sus dispositivos. Esta propiedad inhabilita la captura de registros de Citrix Secure Hub y todas las aplicaciones MDX instaladas. Los usuarios no pueden enviar registros de cualquier aplicación desde la página de asistencia. Aunque aparezca el cuadro de diálogo para redactar el correo, los registros no se adjuntan. Un mensaje indica que el registro está inhabilitado. Este parámetro también impide actualizar los parámetros 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 registrar eventos cuando se aplica la nueva directiva.

- Valores posibles: **true** o **false**
- Valor predeterminado: **false** (la captura de registros no está inhabilitada)

- **ENABLE_CRASH_REPORTING**

- Nombre simplificado: Enable Crash Reporting
- Si tiene el valor **true**, Citrix recopila informes de errores y diagnósticos para ayudar a solucionar problemas con Citrix Secure Hub para iOS y Android. Si el valor es **false**, no se recopilan datos.
- Valores posibles: **true** o **false**
- Valor predeterminado: **true**

- **ENABLE_CREDENTIAL_STORE**

- Nombre simplificado: Enable Credential Store
- Habilitar el almacén de credenciales significa que los usuarios de iOS o Android introducen su contraseña una vez cuando acceden a las aplicaciones móviles de productividad Citrix. Puede utilizar el almacén de credenciales independientemente de si habilita el PIN de Citrix. Si no habilita el PIN de Citrix, los usuarios deberán introducir su contraseña de Active

Directory. Citrix Endpoint Management admite contraseñas de Active Directory en el almacén de credenciales solo para Citrix Secure Hub y las aplicaciones de tiendas públicas. Citrix Endpoint Management no admite la autenticación con la infraestructura de clave pública si se utilizan contraseñas de Active Directory en el almacén de credenciales.

- La inscripción automática en Citrix Secure Mail requiere que esta propiedad se establezca en **true**.
- Para agregar o configurar esta directiva de cliente global, vaya a **Parámetros > Propiedades de cliente** y agregue la clave personalizada **ENABLE_CREDENTIAL_STORE** y defina el **Valor** en **true**.

- **ENABLE_PASSCODE_AUTH**

- Nombre simplificado: Enable Citrix PIN Authentication
- Esta propiedad permite activar la función de PIN de Citrix. Si se activa la función de PIN o código de acceso de Citrix, se solicita a los usuarios que definan un número PIN que se usará en lugar de su contraseña de Active Directory. Este parámetro se habilita automáticamente si la propiedad **ENABLE_PASSWORD_CACHING** está habilitada o si Citrix Endpoint Management usa la autenticación por 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 solicitado. Para la autenticación con conexión, se utiliza el PIN o el código de acceso de Citrix para desbloquear el certificado o la contraseña de Active Directory, enviados a continuación para realizar la autenticación en Citrix Endpoint Management.

Si **ENABLE_PASSCODE_AUTH** se establece en “true” y **ENABLE_PASSWORD_CACHING** se establece en “false”, la autenticación en línea siempre solicitará la contraseña debido a que Citrix Secure Hub no la guarda.

- Valores posibles: **true** o **false**
- Valor predeterminado: **false**

- **ENABLE_PASSWORD_CACHING**

- Nombre simplificado: Enable User Password Caching
- Esta propiedad permite que las contraseñas de Active Directory de los usuarios se almacenen en la memoria caché local del dispositivo móvil. Cuando establezca esta propiedad en **true**, también deberá establecer la propiedad **ENABLE_PASSCODE_AUTH** en **true**. Si se habilita el almacenamiento en caché de las contraseñas de usuario, Citrix Endpoint Management pide a los usuarios que definan un código de acceso o un PIN de Citrix.
- Valores posibles: **true** o **false**
- Valor predeterminado: **false**

- **ENABLE_TOUCH_ID_AUTH**

- Nombre simplificado: Enable Touch ID Authentication
- Para los dispositivos que admiten la autenticación Touch ID, esta propiedad habilita o inhabilita la autenticación Touch ID en el dispositivo. Requisitos:

Los dispositivos de usuario deben tener el PIN de Citrix o LDAP habilitado. Si la autenticación de LDAP está desactivada (por ejemplo, debido a que solo se usa la autenticación por certificados), los usuarios deben establecer un PIN de Citrix. En este caso, Citrix Endpoint Management pide el PIN de Citrix aunque la propiedad de cliente **ENABLE_PASSCODE_AUTH** esté establecida en **false**.

Establezca **ENABLE_PASSCODE_AUTH** en **false** de modo que, cuando los usuarios inicien una aplicación, deban responder a una solicitud de usar Touch ID.

- Valores posibles: **true** o **false**
- Valor predeterminado: **false**

- **ENABLE_WORXHOME_CEIP**

- Nombre simplificado: Enable Citrix Secure Hub CEIP
- Esta propiedad activa el programa CEIP de mejora de la experiencia del cliente. Esa función envía datos anónimos de uso y configuración a Citrix periódicamente. Esos datos ayudan a Citrix a mejorar la calidad, la fiabilidad y el rendimiento de Citrix Endpoint Management.
- Valor: **true** o **false**
- Valor predeterminado: **false**

- **ENCRYPT_SECRETS_USING_PASSCODE**

- Nombre simplificado: Encrypt secrets using Passcode
- Esta propiedad almacena datos confidenciales en el dispositivo móvil, en un almacén secreto, en lugar de guardarse en un almacén nativo basado en la plataforma, como el llavero de iOS. Esta propiedad permite un cifrado seguro de los artefactos de la clave, aunque también agrega la entropía de usuario. La entropía de usuario es un código PIN aleatorio generado por el usuario y que solo este conoce.

Citrix recomienda habilitar esta propiedad para una mayor seguridad en los dispositivos de usuario. En consecuencia, los usuarios ven más solicitudes de autenticación con el PIN de Citrix.

- Valores posibles: **true** o **false**
- Valor predeterminado: **false**

• INACTIVITY_TIMER

- Nombre simplificado: Inactivity Timer
- Esta propiedad define cuánto tiempo pueden dejar los usuarios su dispositivo inactivo y luego acceder a una aplicación sin que se les solicite un PIN o un código de acceso de Citrix. Si quiere habilitar este parámetro para una aplicación MDX, active el parámetro “Código de acceso de aplicación”. Si el parámetro Código de acceso de aplicación está desactivado, se redirige a los usuarios a Citrix Secure Hub para realizar una autenticación completa. Al cambiar esta configuración, el valor se aplicará la próxima vez que los usuarios deban autenticarse.

En iOS, el temporizador de inactividad también controla el acceso a Citrix Secure Hub, para aplicaciones MDX y aplicaciones que no son MDX.

- Valores posibles: Cualquier número entero positivo
- Valor predeterminado: **15** (minutos)

• ON_FAILURE_USE_EMAIL

- Nombre simplificado: On failure Use Email to Send device logs to IT help desk
- Esta propiedad habilita o inhabilita la capacidad de utilizar el correo electrónico para enviar registros del dispositivo al departamento de TI.
- Valores posibles: **true** o **false**
- Valor predeterminado: **true**

• PASSCODE_EXPIRY

- Nombre simplificado: PIN Change Requirement
- Esta clave define cuánto tiempo es válido el PIN o código de acceso de Citrix. Una vez transcurrido ese período, se obliga al usuario a cambiar su PIN o código de acceso de Citrix. Si cambia este parámetro, el nuevo valor se establece solamente cuando el PIN o el código de acceso de Citrix actuales caducan.
- Valores posibles: Se recomienda un valor entre **1** y **99**. Si quiere que los usuarios no tengan que restablecer nunca su PIN, defina un valor alto (por ejemplo 100.000.000.000). Si al principio define un período de caducidad de entre 1 y 99 días y luego lo cambia a uno mayor durante ese período, los PIN caducarán al final del período definido originalmente, pero ya no caducarán nunca más después de eso.
- Valor predeterminado: **90** (días)

• PASSCODE_HISTORY

- Nombre simplificado: PIN History
- Esta propiedad define la cantidad de números PIN o códigos de acceso de Citrix usados anteriormente que los usuarios no pueden volver a utilizar cuando cambien sus números

PIN o códigos de acceso de Citrix. Si cambia este parámetro, el nuevo valor se establece la próxima vez que el usuario restablezca su PIN o código de acceso a Citrix.

- Valores posibles: de **1** a **99**
- Valor predeterminado: **5**

• **PASSCODE_MAX_ATTEMPTS**

- Nombre simplificado: PIN Attempts
- Esta propiedad define cuántos números PIN o códigos de acceso de Citrix incorrectos pueden introducir los usuarios antes de que se les solicite una autenticación completa. Después de que los usuarios realicen correctamente una autenticación completa, se les solicita crear un PIN o código de acceso de Citrix.
- Valores posibles: Cualquier número entero positivo
- Valor predeterminado: **15**

• **PASSCODE_MIN_LENGTH**

- Nombre simplificado: PIN Length Requirement (Requisito de longitud de código PIN)
- Esta propiedad define la longitud mínima de los PIN de Citrix.
- Valores posibles: De **4** a **10**
- Valor predeterminado: **6**

• **PASSCODE_STRENGTH**

- Nombre simplificado: PIN Strength Requirement
- Esta propiedad define la seguridad del PIN o código de acceso de Citrix. Si cambia este parámetro, se solicitará a los usuarios que creen un PIN o código de acceso de Citrix la próxima vez que deban autenticarse.
- Valores posibles: **Low**, **Medium**, **High** o **Strong**
- Valor predeterminado: **Medium**
- En esta tabla se describen las reglas de contraseña para cada parámetro de nivel de seguridad, basadas en el parámetro PASSCODE_TYPE:

Reglas para códigos de acceso numéricos:

Nivel de seguridad de la contraseña	Reglas para el tipo de código de acceso numérico	Reglas para el tipo de código de acceso	
		Se permite	No se permite
Bajo	Se permiten todos los números y todas las secuencias	444444, 123456, 654321	

Nivel de seguridad de la contraseña	Reglas para el tipo de código de acceso numérico	Reglas para el tipo de código de acceso	
		Se permite	No se permite
Medio (configuración predeterminada)	Los números no pueden ser los mismos ni consecutivos.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
Alto	Los números adyacentes no pueden ser iguales.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
Fuerte	No use el mismo número más de dos veces. No use tres o más números consecutivos seguidos. No use tres o más números consecutivos en el orden inverso.	102983, 085085, 824673, 132312	132132, 131313, 902030

Reglas para códigos de acceso alfanuméricos:

Nivel de seguridad de la contraseña	Reglas para el tipo de código de acceso alfanumérico	Reglas para el tipo de código de acceso	
		Se permite	No se permite
Bajo	Debe contener al menos una letra y un número	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef
Medio (configuración predeterminada)	Además de las reglas de contraseñas con nivel bajo de seguridad, ni los números ni las letras pueden ser los mismos. Ni letras ni números pueden ser consecutivos.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa, or aaa111; abcd12, bcd123, 123abc, xy1234, xyz345 o cba123
Alto	Incluya al menos una letra mayúscula y una letra minúscula.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2

Nivel de seguridad de la contraseña	Reglas para el tipo de código de acceso		
	alfanumérico	Se permite	No se permite
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 simplificado: PIN Type
- Esta propiedad indica si el usuario puede definir un PIN numérico o un código de acceso alfanumérico de Citrix. Si selecciona **Numeric**, el usuario solo podrá definir un valor numérico para el PIN de Citrix. Si selecciona **Alphanumeric**, el usuario podrá utilizar una combinación de letras y números para el código de acceso.

Si cambia este parámetro, los usuarios deberán establecer un nuevo PIN o código de acceso de Citrix la próxima vez que deban autenticarse.

- Valores posibles: **Numeric** o **Alphanumeric**
- Valor predeterminado: **Numeric**

• **REFRESHINTERVAL**

- Nombre simplificado: REFRESHINTERVAL
- De forma predeterminada, Citrix Endpoint Management hace ping al servidor de detección automática (ADS) para buscar certificados anclados cada 3 días. Para cambiar el intervalo de actualización, vaya a **Parámetros > Propiedades de cliente**, agregue la clave personalizada **REFRESHINTERVAL** y establezca el **Valor** en la cantidad de horas.
- Valor predeterminado: **72** horas (3 días)

• **SEND_LDAP_ATTRIBUTES**

- Para implementaciones de solo MAM de dispositivos Android, iOS o macOS, puede configurar Citrix Endpoint Management para que los usuarios que se inscriban en Citrix Secure Hub con las credenciales de correo electrónico queden automáticamente inscritos en Citrix Secure Mail. Como resultado, los usuarios no ofrecen información adicional ni realizan pasos adicionales para inscribirse en Citrix Secure Mail.
- Para agregar o configurar esta directiva de cliente global, vaya a **Parámetros > Propiedades de cliente** y agregue la clave personalizada **SEND_LDAP_ATTRIBUTES** y defina el **Valor** de este modo.

- 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.
- Este es un ejemplo de respuesta de la cuenta de servicio para esta propiedad:

```
<property value="userPrincipalName=user@site.com,sAMAccountName=engl,displayName=user\,test1,email=user@site.com\,user@site.com"name="SEND_LDAP_ATTRIBUTES"/>
```
- En esta propiedad, Citrix Endpoint Management interpreta las comas como terminadores de cadenas. Por lo tanto, si un valor de atributo contiene una coma, debe ir precedida de una barra diagonal inversa. La barra diagonal inversa evita que el cliente interprete la coma como el final del valor del atributo. Los caracteres de barra diagonal invertida se representan así: `"\"`.

• **HIDE_THREE_FINGER_TAP_MENU**

- Cuando esta propiedad no está definida o está establecida en **false**, los usuarios pueden acceder al menú de funciones ocultas tras una pulsación con tres dedos en sus dispositivos. El menú de funciones ocultas permitía a los usuarios restablecer los datos de la aplicación. Establecer esta propiedad en **true** inhabilita el acceso de los usuarios al menú de funciones ocultas.
- Para configurar esta directiva de cliente global, vaya a **Parámetros > Propiedades de cliente**, agregue la clave personalizada **HIDE_THREE_FINGER_TAP_MENU** y defina el **valor**.

• **TUNNEL_EXCLUDE_DOMAINS**

- Nombre simplificado: Tunnel Exclude Domains
- De forma predeterminada, MDX excluye de los túneles de micro VPN a algunos puntos finales de servicio que usen los Mobile Apps SDK y las aplicaciones para varias funciones. Por ejemplo, esos dispositivos de punto final contienen servicios que no requieren el enrutamiento a través de redes de empresa (como Google Analytics, servicios de Citrix Cloud y servicios de Active Directory). Utilice esta propiedad de cliente para anular la lista predeterminada de dominios excluidos.
- Para agregar o configurar esta directiva de cliente global, vaya a **Parámetros > Propiedades de cliente** y agregue la clave personalizada **TUNNEL_EXCLUDE_DOMAINS** y defina el **Valor**.
- Valor: Para reemplazar la lista predeterminada por los dominios que quiere excluir del túnel, escriba una lista, separada por comas, de sufijos de dominio. Para incluir a todos los dominios en el túnel, escriba **none**. El valor predeterminado es:

`app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,
cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics
.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.
com, hockeyapp.net,mobile.launchdarkly.com,pushreg.xml.citrix.
com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.
com,ssl.google-analytics.com,stream.launchdarkly.com`

Las propiedades de cliente personalizadas para Citrix Endpoint Management son las siguientes:

ENABLE_MAM_NFACTOR_SSO:

- Esta propiedad le permite habilitar o inhabilitar el inicio de sesión único de MAM nFactor durante la inscripción en MAM o iniciar sesión en Secure Hub mientras usa la directiva de autenticación avanzada de NetScaler Gateway. Si el valor se establece en **true**, el inicio de sesión único de MAM nFactor se habilita durante la inscripción en MAM o el inicio de sesión en Secure Hub.
- Para configurar esta propiedad, vaya a **Parámetros > 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: Agregue la descripción correspondiente

Opciones de inscripción de usuarios

December 13, 2023

Los usuarios pueden inscribir sus dispositivos en Citrix Endpoint Management de varias formas. Antes de considerar los detalles, decida qué dispositivos quiere inscribir en MDM+MAM, MDM o MAM. Para obtener más información sobre estos modos de administración, consulte [Modos de administración](#).

En el nivel más alto, hay cuatro opciones de inscripción:

- **Invitación de inscripción:** Puede enviar una URL de invitación o una invitación de inscripción a los usuarios. Las URL y las invitaciones de inscripción no están disponibles para dispositivos Windows.
- **Self Help Portal:** Puede configurar un portal que visiten los usuarios para descargar Citrix Secure Hub, solicitar inscripciones y ver información de los dispositivos.
- **Inscripción manual:** Puede enviar un correo electrónico, un manual u otro comunicado para que los usuarios sepan que el sistema está activo y pueden inscribirse. Entonces, los usuarios se descargan Citrix Secure Hub e inscriben sus dispositivos manualmente.

- **Empresa:** Otra opción para la inscripción de dispositivos es mediante un Programa de implementación de Apple y Google Android Enterprise. A través de cada uno de estos programas, puede adquirir dispositivos preconfigurados y listos para que los usen los empleados. Para obtener más información, consulte los artículos del Programa de implementación de Apple en el [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 a usuarios de dispositivos iOS, macOS, Android Enterprise o Android heredado. Las invitaciones de inscripción no están disponibles para dispositivos Windows.

También puede enviar un enlace de instalación por SMTP a los usuarios con dispositivos iOS, macOS, Android Enterprise, Android o Windows. Para obtener más información, consulte [Inscribir dispositivos](#).

Si decide utilizar el método de invitación para la inscripción, puede:

- Seleccionar el modo de seguridad de inscripción **URL de invitación**, **URL de invitación + PIN** o **URL de invitación + contraseña**.
- Usar cualquier combinación de los distintos modos.
- Habilitar o inhabilitar los modos en la página **Parámetros** 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 fines. El uso más común de las invitaciones es notificar a los usuarios de que el sistema está disponible y pueden inscribirse. Las URL de invitación son únicas. Una vez que un usuario utiliza una URL de invitación, dicha URL deja de estar disponible. Puede usar esta propiedad para limitar la cantidad de usuarios o dispositivos que se inscriben en su sistema.

Al configurar un perfil de inscripción, puede controlar la cantidad de dispositivos que usuarios específicos pueden inscribir, en función de los grupos de Active Directory. Por ejemplo, puede autorizar solo un dispositivo por usuario a la división Finanzas.

Tenga en cuenta los costes adicionales y las dificultades de algunas opciones de inscripción. Para enviar invitaciones mediante SMTP se requiere una infraestructura adicional. Para obtener más información sobre esta opción, consulte [Notificaciones](#).

Asimismo, para enviar invitaciones por correo electrónico, debe comprobar que los usuarios tengan una manera de acceder al correo electrónico que no sea a través de Citrix Secure Hub. Para la inscripción MDM, puede utilizar modos de seguridad de inscripción con contraseña de un solo uso (OTP) como alternativa a las contraseñas de Active Directory.

Self Help Portal

A Self Help Portal se puede acceder en la misma URL que los administradores usan para acceder a la consola de Citrix Endpoint Management. Los usuarios finales ven Self Help Portal, en lugar de la consola de administración. Los usuarios pueden descargar Citrix Secure Hub, solicitar inscripciones y ver la información de los dispositivos en Self Help Portal.

Para configurar un portal, actualice estas propiedades del servidor en **Parámetros > Propiedades del servidor**:

- `shp.console.enable`: Se establece en **True** para proporcionar acceso al portal Self Help Portal.
- `enable.new.shp`: Se establece en **True** para permitir que los usuarios puedan habilitar sus dispositivos desde el portal Self Help Portal.

Inscripción manual

Con la inscripción manual, los usuarios se conectan a Citrix Endpoint Management a través de la detección automática, o bien introducen la información del servidor. Con la detección automática, los usuarios pueden iniciar sesión solamente con su dirección de correo electrónico o sus credenciales de Active Directory en el formato de nombre principal de usuario. Sin la detección automática, deben introducir la dirección del servidor y sus credenciales de Active Directory. Para obtener más información sobre cómo configurar la detección automática, consulte [Configurar el servicio de detección automática 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 a los grupos de usuarios durante determinados periodos de tiempo. Puede usar cualquier método similar donde los usuarios deban introducir sus credenciales o la información del servidor.

Incorporación de usuarios

Una vez que haya configurado su entorno, debe decidir cómo introducir a los usuarios en su entorno. En un apartado anterior de este artículo se analizan los detalles de los modos de seguridad para la inscripción de los usuarios. En esta sección se describe cómo establecer comunicación 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 la cantidad de usuarios al permitir que solo los usuarios con invitaciones se inscriban. También puede limitar la inscripción abierta por grupo de Active Directory.

Con el método de invitación, también puede limitar la cantidad de dispositivos que puede inscribir un usuario. En la mayoría de las situaciones, la inscripción abierta es una buena opción, pero hay aspectos a tener en cuenta:

- Para la inscripción en MAM, puede limitar fácilmente la inscripción abierta según la pertenencia a grupos de Active Directory.
- Para la inscripción en MDM, puede limitar la cantidad de dispositivos que pueden inscribirse en función de la pertenencia a grupos de Active Directory. Normalmente, no es ningún problema que solo permita dispositivos de empresa en su entorno. Sin embargo, conviene que tenga en cuenta este método en un área de trabajo BYOD donde quiera limitar la cantidad de dispositivos en el entorno.

La invitación selectiva generalmente se realiza con menos frecuencia porque requiere un poco más de trabajo que la inscripción abierta. Para que los usuarios puedan inscribir sus dispositivos en el 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 a cada usuario o grupo que quiera inscribir en su entorno. Ese proceso puede tardar mucho en función del tamaño de su organización. Es posible utilizar grupos de Active Directory para crear invitaciones por lotes, pero debe llevar a cabo este enfoque por fases.

Primer contacto con los usuarios

Después de decidir si utilizar la inscripción abierta o la invitación selectiva y configurar esos entornos, informe a los usuarios acerca de sus opciones de inscripción.

Si usa el método de invitación selectiva, los mensajes de correo electrónico intervienen en el proceso. También puede enviar correos electrónicos desde la consola de Citrix Endpoint Management para la inscripción abierta. Para obtener más información, consulte [Invitaciones de inscripción](#).

En ambos casos, tenga en cuenta que, para los correos electrónicos, necesitará un servidor SMTP. Esos servidores podrían implicar costes adicionales a considerar a la hora de tomar su decisión. Piense en cómo espera que los nuevos usuarios accedan a la información. Si quiere 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 otro medio que no sea Citrix Endpoint Management para un entorno de inscripción abierta. Para esa opción, asegúrese de incluir toda la información relevante.

Indique a los usuarios dónde pueden obtener la aplicación Citrix Secure Hub y qué método deben utilizar para inscribirse. Si la detección está desactivada, proporcione también a los usuarios la dirección del servidor de Citrix Endpoint Management. Para obtener más información sobre la detección, consulte [Configurar el servicio de detección automática de Citrix Endpoint Management](#).

Aprovisionar y desaprovisionar aplicaciones

March 1, 2024

El aprovisionamiento de aplicaciones gira en torno a la administración del ciclo de vida de las aplicaciones móviles: preparar, configurar, entregar y administrar aplicaciones móviles dentro de un entorno de Citrix Endpoint Management. En algunos casos, el desarrollo o la modificación del código de la aplicación también puede formar parte del proceso de aprovisionamiento. Citrix Endpoint Management está equipado con varias herramientas y procesos que puede usar para el aprovisionamiento de las aplicaciones.

Antes de leer este artículo sobre el aprovisionamiento de aplicaciones, se recomienda leer [Aplicaciones](#) y [Comunidades de usuarios](#). Cuando haya decidido el tipo de aplicaciones que su organización quiere entregar a los usuarios, puede precisar el proceso para administrar las aplicaciones a lo largo de sus ciclos de vida.

Tenga en cuenta los siguientes puntos a la hora de definir su proceso de aprovisionamiento de aplicaciones:

- **Creación de perfiles de aplicación:** Puede que su organización empiece con una cantidad limitada de aplicaciones. No obstante, la cantidad de aplicaciones a administrar podría aumentar rápidamente, a medida que la cantidad de usuarios aumente y su entorno crezca. Debe definir perfiles de aplicación específicos desde el principio para que el aprovisionamiento de aplicaciones sea fácil de administrar. Crear perfiles de aplicación ayuda a distribuir aplicaciones en grupos lógicos desde una perspectiva no técnica. Por ejemplo, puede crear perfiles de aplicación en función de los siguientes factores:
 - Versión: La versión de la aplicación para el seguimiento
 - Instancias: Varias instancias que se implementan para conjuntos diferentes de usuarios, por ejemplo, usuarios con diferentes niveles de acceso
 - Plataforma: iOS, Android o Windows
 - Público objetivo: Usuarios estándar, departamentos, ejecutivos de alto nivel
 - Propiedad: El departamento es propietario de la aplicación
 - Tipo: Enlaces web o aplicaciones públicas, MDX o web y SaaS
 - Ciclo de actualización: Con qué frecuencia se actualiza la aplicación
 - Licencias: Requisitos y propiedad de las licencias

- Directivas de MDX o SDK de MAM: Para aplicar funcionalidades de MDX a sus aplicaciones móviles
- Acceso de red: Tipo de acceso, como el túnel de tráfico HTTP y HTTPS con Single Sign-On (Túnel - SSO web).

Ejemplo:

Factor	Citrix Secure Mail	Mail	Interna	Epic Rover
Versión	10.1	10.1	X.x	X.x
Instancia	Dirección IP virtual	Médicos	Sanitarios	Sanitarios
Plataforma	iOS	iOS	iOS	iOS
Usuarios de destino	Usuarios de direcciones IP virtuales	Médicos	Personal sanitario	Personal sanitario
Propietario	TI	TI	TI	TI
Tipo	MDX	MDX	Nativa	Público
Ciclo de actualización	Trimestral	Trimestral	Anual	N/D
Licencias	N/D	N/D	N/D	Compras por volumen
Directivas MDX	Sí	Sí	Sí	No
Acceso de red	VPN	VPN	VPN	Público

- **Control de versiones de aplicación:** El mantenimiento y el seguimiento de las versiones de las aplicaciones son 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. En cuanto a usted, revisar y probar cada versión de la aplicación fuera del entorno de producción también es fundamental para evitar el impacto en 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 importante (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:** Cuando integra el SDK de MAM en las aplicaciones móviles que desarrolla, aplica funcionalidades de MDX a esas aplicaciones. Consulte [Introducción al SDK de MAM](#).

El SDK de MAM reemplaza a MDX Toolkit, cuya retirada está programada para julio de 2023. Para obtener información sobre el empaquetado de aplicaciones, consulte [MDX Toolkit](#). El proceso de aprovisionamiento de una aplicación empaquetada es distinto del proceso de aprovisionamiento de una aplicación estándar no empaquetada.

- **Seguridad de las aplicaciones:** Definir los requisitos de seguridad necesarios para las aplicaciones o los perfiles de aplicaciones forma parte del proceso de aprovisionamiento. Puede asignar los requisitos de seguridad a directivas específicas de MDM o MAM antes de implementar las aplicaciones. Esa planificación simplifica y agiliza la implementación de aplicaciones. Por ejemplo:
 - Puede que le interese implementar ciertas aplicaciones de forma diferente.
 - Es posible que quiera realizar cambios de arquitectura en el entorno de Citrix Endpoint Management. Los cambios dependen del tipo de cumplimiento de seguridad que requieren las aplicaciones. Por ejemplo, una aplicación concreta podría requerir cifrado SSL de extremo a extremo o geocerca.
- **Entrega de aplicaciones:** Citrix Endpoint Management permite entregar aplicaciones como aplicaciones MDM o como aplicaciones MAM. Las aplicaciones MDM aparecen en el almacén de aplicaciones. Este almacén permite entregar convenientemente aplicaciones públicas o nativas a los usuarios. Aparte de aplicar restricciones a nivel de dispositivo, no se necesitan otros controles de aplicación. Sin embargo, la entrega de aplicaciones mediante MAM ofrece un control total, tanto sobre la entrega de la aplicación como sobre la aplicación en sí. Entregar las aplicaciones a través de MAM suele ser más adecuado.
- **Mantenimiento de aplicaciones:**
 - Lleve a cabo una auditoría inicial. Realice un seguimiento de la versión de aplicación que está presente en el entorno de producción y del último ciclo de actualización. Tome nota de las funciones o las correcciones de errores específicas que requirieron la actualización.
 - Establezca puntos de referencia. Cree una lista de las versiones estables más recientes de cada aplicación. Esta versión de la aplicación debe estar disponible para poder volver a ella en caso de que se produzcan problemas inesperados después de la actualización. Desarrollar 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, a continuación, en toda la base de usuarios.
 - Suscríbase a las notificaciones de actualización de software de Citrix y las notificaciones de proveedores de software de terceros. Es importante para estar al día con las versiones más recientes de las aplicaciones. También puede estar disponible una compilación de acceso anticipado (EAR) para realizar pruebas con anticipación.
 - Diseñe una estrategia para notificar a los usuarios. Debe definir una estrategia para notificar a los usuarios cuando las actualizaciones de la aplicación estén disponibles. Forme

a los usuarios antes de la implementación. Considere enviar varias notificaciones antes de actualizar las aplicaciones. Dependiendo de la aplicación, el mejor método de notificación pueden ser notificaciones por correo electrónico o sitios web.

La administración del ciclo de vida de la aplicación implica el ciclo de vida completo de una aplicación, desde su implementación inicial hasta la retirada. El ciclo de vida de una aplicación consta de estas fases:

1. Requisitos para especificaciones. Empezar con los requisitos de usuario y el caso concreto del negocio.
2. Desarrollo: Validar que la aplicación cumple las necesidades del negocio.
3. Pruebas: Identificar usuarios de prueba, problemas y errores.
4. Implementación: Implementar la aplicación a los usuarios de producción.
5. Mantenimiento: Actualizar la versión de la aplicación. Implemente la aplicación en un entorno de prueba antes de actualizar la aplicación en un entorno de producción.

Operaciones del panel de mandos

March 1, 2024

Puede ver toda la información de un vistazo desde su panel de mandos en la consola de Citrix Endpoint Management. En esta información, puede utilizar widgets para ver rápidamente los problemas y las operaciones correctas que se hayan producido.

Por regla general, el panel de mandos es la pantalla que aparece justo tras iniciar sesión en la consola de Citrix Endpoint Management. Para acceder al panel de mandos desde cualquier otro sitio de la consola, haga clic en **Analizar**. Haga clic en **Personalizar** en el panel de mandos para modificar el diseño de la página y para modificar los widgets que aparecen.

- **Mis paneles de mandos:** Puede guardar hasta cuatro paneles de mandos diferentes. Puede seleccionar cada panel guardado para verlo y modificarlo por separado.
- **Estilo de diseño:** En esta fila, puede seleccionar la cantidad de widgets que aparecerán en el panel de mandos y cómo se etiquetarán.
- **Selección de widget:** Puede elegir qué información se mostrará en el panel de mandos.
 - **Notificaciones:** Marque la casilla situada encima de los números en la parte izquierda para agregar una barra de notificaciones encima de los widgets. Esta barra muestra la cantidad de dispositivos conformes, dispositivos inactivos, dispositivos borrados o dispositivos inscritos en las últimas 24 horas.
 - **Dispositivos por plataforma:** Muestra la cantidad de dispositivos administrados y no administrados por plataforma.

- **Dispositivos por operador:** Muestra la cantidad de dispositivos administrados y no administrados por operador. Haga clic en cada barra para ver un desglose por plataforma.
- **Dispositivos administrados por plataforma:** Muestra la cantidad de dispositivos administrados por plataforma.
- **Dispositivos no administrados por plataforma:** Muestra la cantidad de dispositivos no administrados por plataforma. Los dispositivos que aparecen en este gráfico pueden tener un agente instalado, pero se podrían haber borrado o revocado sus privilegios.
- **Dispositivos por estado de ActiveSync Gateway:** Muestra la cantidad de dispositivos agrupados por estado de ActiveSync Gateway. La información se muestra como estado Bloqueado, Permitido o Desconocido. Puede hacer clic en cada barra para desglosar los datos por plataforma.
- **Dispositivos por propietario:** Muestra la cantidad de dispositivos agrupados por propietario. La información se muestra como propiedad de la empresa, del empleado o propietario desconocido.
- **Implementaciones fallidas de grupos de entrega:** Muestra la cantidad total de implementaciones fallidas desglosadas por paquete. Solo se muestran los paquetes de implementaciones con errores.
- **Dispositivos por motivo de bloqueo:** Muestra la cantidad de dispositivos bloqueados por ActiveSync.
- **Aplicaciones instaladas:** Con este widget, puede escribir un nombre de aplicación y aparecerá un gráfico con información acerca de esa aplicación.
- **Uso de licencias de aplicaciones de compras por volumen:** Muestra estadísticas sobre el uso de licencias por parte de las aplicaciones de compras por volumen de Apple.

Casos de uso

A continuación, dispone de algunos ejemplos de las muchas maneras en que puede usar los widgets del panel de mandos para supervisar el entorno.

- Ha implementado las aplicaciones móviles de productividad Citrix y recibe tíquets de asistencia relacionados con ellas, donde se le informa que no se pueden instalar en los dispositivos. Utilice los widgets **Dispositivos no conformes** y **Aplicaciones instaladas** para ver los dispositivos que no tienen instaladas las aplicaciones móviles de productividad Citrix.
- Quiere supervisar los dispositivos inactivos para eliminarlos del entorno y reclamar las licencias. Use el widget **Dispositivos inactivos** para hacer un seguimiento de estos datos.
- Recibe tíquets de asistencia relacionados con datos que no se sincronizan correctamente. Puede 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 el entorno está configurado y los usuarios se han inscrito, puede ejecutar informes para conocer datos de su implementación. Citrix Endpoint Management incluye una serie de informes integrados para ver con mayor precisión los dispositivos que se ejecutan en su entorno. Para obtener más información, consulte [Informes](#).

Control de acceso basado en roles y asistencia de Citrix Endpoint Management

March 1, 2024

Citrix Endpoint Management utiliza el control de acceso basado en roles (RBAC) para restringir el acceso de grupos y usuarios a las funciones del sistema de Citrix Endpoint Management, como la consola de Citrix Endpoint Management, Self Help Portal y la API pública. En este artículo, se describen los roles integrados en Citrix Endpoint Management y se incluyen aspectos a tener en cuenta para elegir un modelo de asistencia para un Citrix Endpoint Management que utilice RBAC.

Roles integrados

Puede agregar roles y cambiar el acceso concedido a los siguientes roles integrados. Para conocer el conjunto completo de los permisos de funciones y acceso asociados a cada rol y su configuración predeterminada, descargue [Role-Based Access Control Defaults](#). Para una definición de cada función, consulte [Configurar roles con RBAC](#).

Rol de administrador

Acceso predeterminado concedido:

- Acceso completo al sistema, excepto a Self Help Portal.
- De forma predeterminada, los administradores pueden realizar algunas tareas de asistencia, (por ejemplo, comprobar la conectividad y crear paquetes de asistencia).

Consideraciones:

- ¿Algunos o todos los administradores necesitan acceso a Self Help Portal? Si es así, puede modificar el rol Admin o agregar roles de administrador.
- Para restringir más el acceso de algunos administradores o grupos de administradores, agregue roles basados en la plantilla de administrador y modifique los permisos.

Usuario

Acceso predeterminado concedido:

- Acceder a Self-Help Portal, 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 o desbloquear el dispositivo, bloquear o desbloquear el contenedor, ver la ubicación y establecer restricciones geográficas, hacer sonar el dispositivo, restablecer la contraseña del contenedor); agregar, eliminar y enviar invitaciones de inscripción.

Consideraciones:

- El rol Usuario permite habilitar 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 asistencia de Citrix Endpoint Management

Los modelos de asistencia que puede adoptar varían ampliamente y pueden implicar a terceros que gestionen la asistencia de nivel 1 y 2, mientras que los empleados gestionan la asistencia de nivel 3 y 4. Independientemente de cómo distribuya la carga de la asistencia, tenga en cuenta las consideraciones de esta sección que sean específicas a su implementación de Citrix Endpoint Management y su base de usuarios.

¿Los usuarios tienen dispositivos propiedad de la empresa o BYOD?

La pregunta principal que influye en la asistencia es a quién pertenece el dispositivo de usuario en su entorno de Citrix Endpoint Management. Si sus usuarios tienen dispositivos propiedad de la empresa, puede ofrecer un nivel de asistencia más bajo, como una forma de bloquear completamente los dispositivos. En ese caso, puede proporcionar un servicio de asistencia que ayude a los usuarios con los problemas de los dispositivos y les guíe para saber cómo usarlos. Según los tipos de dispositivo para los que vaya a ofrecer asistencia, plantéese cómo usar los roles de RBAC “Aprovisionamiento de dispositivos” y “Asistencia” para el servicio de asistencia.

Si los usuarios tienen dispositivos BYOD, puede que la organización espere que busquen sus propias fuentes de ayuda con el dispositivo. En ese caso, la asistencia que ofrezca la organización es más bien un rol administrativo centrado en los problemas específicos de Citrix Endpoint Management.

¿Cuál es su modelo de asistencia para los escritorios?

Plantéese si el modelo de asistencia para los escritorios se puede aplicar a otros dispositivos propiedad de la empresa. ¿Puede usar la misma organización de asistencia? ¿Qué formación adicional podrían necesitar?

¿Quiere dar a los usuarios acceso a Self Help Portal de Citrix Endpoint Management?

Aunque algunas empresas prefieren no conceder a los usuarios acceso a Citrix Endpoint Management, ofrecerles la capacidad de ayudarse a sí mismos puede aligerar la carga de la asistencia en su organización. Si el rol “Usuario” predeterminado de RBAC contiene permisos que no quiere conceder, considere la posibilidad de crear un rol que contenga solamente los permisos que quiera incluir. Puede crear tantos roles como sea necesario para cumplir los requisitos.

Proceso de asistencia de Citrix

March 1, 2024

Puede acudir a los servicios de asistencia técnica de Citrix para obtener ayuda con problemas relacionados con los productos Citrix. El personal de asistencia ofrece soluciones temporales y resoluciones, además de trabajar codo con codo con los equipos de desarrollo para ofrecer soluciones.

Citrix Consulting Services o Citrix Education Services ofrecen ayuda relacionada con la formación referente a los productos, y recomendaciones para el uso, la configuración, la instalación del producto o el diseño y la arquitectura del entorno.

Citrix Consulting ayuda con los proyectos relacionados con los productos Citrix, incluidos:

- Prueba de conceptos
- Evaluación del impacto económico
- Comprobaciones del estado de las infraestructuras
- Análisis de requisitos de diseño
- Verificación del diseño de arquitecturas
- Integración
- Desarrollo de procesos operativos

Citrix Education ofrece la mejor formación y certificación de TI de su clase en Citrix Virtualization, Citrix Cloud y las tecnologías de red.

Citrix recomienda que aproveche al máximo los recursos de ayuda de Citrix y sus recomendaciones antes de abrir un caso de asistencia. Por ejemplo, hay varios lugares desde donde puede acceder a artículos y publicaciones, escritos por expertos técnicos de Citrix. Asimismo, puede acudir a la documentación del producto para conocer las soluciones y las tecnologías Citrix, leer directamente las publicaciones de los ejecutivos, los equipos de producto y los expertos técnicos de Citrix. Consulte las páginas de [Knowledge Center](#), la [documentación de producto](#) y los [blogs](#), respectivamente.

Si lo que busca es una asistencia más interactiva, puede participar en los foros, donde puede hacer preguntas y obtener respuestas reales de otros clientes, compartir ideas, opiniones, información técnica y recomendaciones en grupos de usuarios y grupos de interés. En esos foros, también puede

comunicarse con los ingenieros de asistencia de Citrix que supervisan las redes sociales de Citrix Support. Consulte las páginas [Support Forums](#) y [Citrix Community](#) respectivamente.

También tiene acceso a cursos de formación y certificación para desarrollar sus habilidades. Consulte [Citrix Education](#).

Citrix Insight Services ofrece una sencilla plataforma de resolución de problemas en línea, que también puede comprobar el estado de su entorno Citrix. Disponible para Citrix Endpoint Management, Citrix Virtual Apps and Desktops, Citrix Hypervisor y NetScaler Gateway. Consulte [Analysis Tool](#).

Para buscar asistencia técnica, puede crear un caso de asistencia por teléfono o a través de la red. Puede usar el sitio web para problemas de intensidad baja y media; recomendamos la opción de teléfono para problemas de alta intensidad. Para contactar con asistencia por problemas con Citrix Endpoint Management, consulte [Soporte y servicios de Citrix](#).

Si busca un punto de contacto único altamente capacitado con amplia experiencia en la entrega de soluciones Citrix, Citrix Services ofrece un Technical Relationship Manager (un gestor técnico que mantiene contacto directo con el cliente). Para obtener más información sobre las ventajas y la oferta de los servicios de Citrix, consulte [Citrix Worldwide Services](#).

Enviar invitaciones de inscripción a grupos en Citrix Endpoint Management

March 1, 2024

Author:

John Bartel III

En Citrix Endpoint Management, puede enviar invitaciones de inscripción a grupos y grupos anidados. Las invitaciones de inscripción no están disponibles para dispositivos Windows.

Al configurar la invitación de grupo, puede especificar una o varias plataformas de dispositivo. También puede etiquetar los dispositivos para distinguir, por ejemplo, los dispositivos propiedad de la empresa y los dispositivos propiedad de los empleados. A continuación, puede establecer el tipo de autenticación para los dispositivos de usuario.

Nota:

Si va a utilizar plantillas de notificaciones personalizadas, debe definir esas plantillas antes de configurar los modos de seguridad para la inscripción. Para obtener más información acerca de las plantillas de notificaciones, consulte [Crear y actualizar plantillas de notificaciones](#).

Para obtener más información sobre la configuración básica de cuentas de usuario, roles, modos de seguridad de inscripción e invitaciones, consulte [Inscripción, roles y cuentas de usuario](#).

Pasos generales

1. En la consola de Citrix Endpoint Management, vaya a **Administrar > Invitaciones de inscripción**.
2. Haga clic en la opción **Agregar**, situada en la parte superior izquierda de la pantalla, y haga clic en **Agregar invitación**.
3. Haga clic en **Grupo**, en el menú **Destinatario**.

Este paso permite elegir una o varias plataformas. Si tiene varias plataformas distintas de sistemas operativos en la empresa, elija todas las plataformas. Deseleccione una plataforma solo si sabe pertinentemente que no hay usuarios que utilicen esa plataforma.

4. Puede etiquetar dispositivos durante el proceso de invitación. Elija **Empresa** o **Empleado**.
El etiquetado facilita la separación de dispositivos que sean propiedad de la empresa y dispositivos que sean propiedad de los empleados.
5. En la lista **Dominio**, elija el dominio donde existe el grupo.
6. En la lista **Grupo**, seleccione el grupo de Active Directory al que quiere enviar las invitaciones.
7. El **Modo de inscripción** permite establecer el tipo de seguridad de inscripción que prefiera para los usuarios.

- Nombre de usuario y contraseña
- High Security (Nivel alto de seguridad)
- URL de invitación
- URL de invitación y PIN
- URL de invitación y contraseña
- Dos factores
- Nombre de usuario + PIN

Nota:

Hemos retirado el modo de seguridad de inscripción **Alta seguridad**. Para enviar invitaciones de inscripción, puede utilizar solamente 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 manualmente sus credenciales.

8. Para las plantillas **Descarga de agente**, **URL de inscripción**, **PIN de inscripción** y **Confirmación de inscripción**, elija la plantilla de notificaciones personalizada que creó antes. O bien, elija el valor predeterminado que aparece en la lista.

Para estas plantillas de notificaciones, use la configuración del servidor SMTP definida en Citrix Endpoint Management. Configure la información SMTP antes de continuar.

Nota:

Las opciones **Caduca después de** y **Máximo de intentos** cambian en función de la opción de **Modo de inscripción** que elija. Esas opciones no se pueden cambiar.

9. Seleccione “Sí” en **Enviar invitación** y haga clic en **Guardar y enviar** para completar el proceso.

Admitir grupos anidados

Puede enviar invitaciones a grupos anidados. Por lo general, los grupos anidados se usan en entornos grandes, donde los grupos con permisos similares están vinculados entre sí.

Vaya a **Parámetros > LDAP** y, a continuación, habilite la opción **Admitir grupos anidados**.

Solución de problemas y limitaciones conocidas

Problema: Las invitaciones se envían a los usuarios, aunque estos se hayan eliminado de los grupos de Active Directory.

Solución: La propagación de los cambios depende del tamaño de su entorno de Active Directory. En un entorno grande, los cambios pueden tardar hasta seis horas en propagarse a todos los servidores. Si un usuario o grupo anidado se han eliminado recientemente, Citrix Endpoint Management aún puede considerar a esos usuarios como parte del grupo.

Por lo tanto, es mejor esperar un máximo de seis horas antes de enviar otra invitación grupal a los usuarios.

Configurar la autenticación por certificado en EWS para notificaciones push de Citrix Secure Mail

March 1, 2024

Para que las notificaciones push de Citrix Secure Mail funcionen, debe hacer lo siguiente:

- Configure Exchange Server para la autenticación basada en certificados. Este requisito es especialmente necesario cuando Citrix Secure Hub se inscribe en Citrix Endpoint Management con la autenticación basada en certificados.

- Debe configurar Active Sync y el directorio virtual de Servicios web de Exchange (EWS) en el servidor de correo de Exchange con la autenticación basada en certificados.

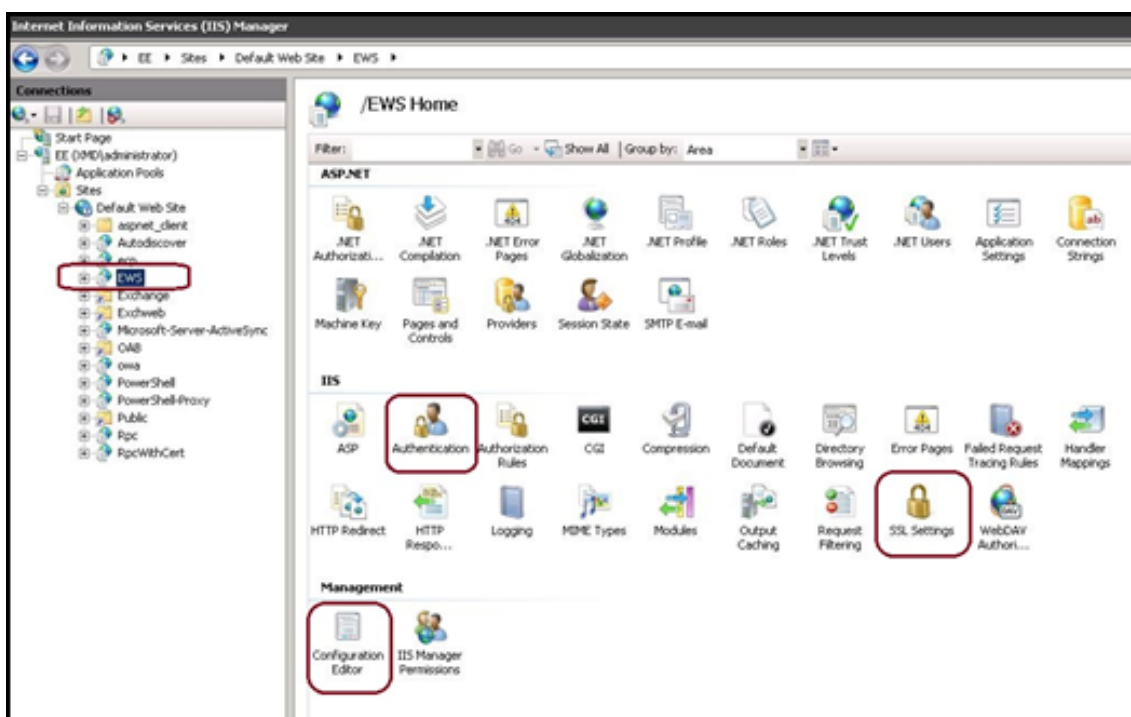
A menos que complete estas configuraciones, la suscripción a las notificaciones push de Citrix Secure Mail falla y las insignias de Citrix Secure Mail no se actualizan.

En este artículo se describen los pasos para configurar la autenticación basada en certificados. Las configuraciones son específicas para el directorio virtual EWS en Exchange Server.

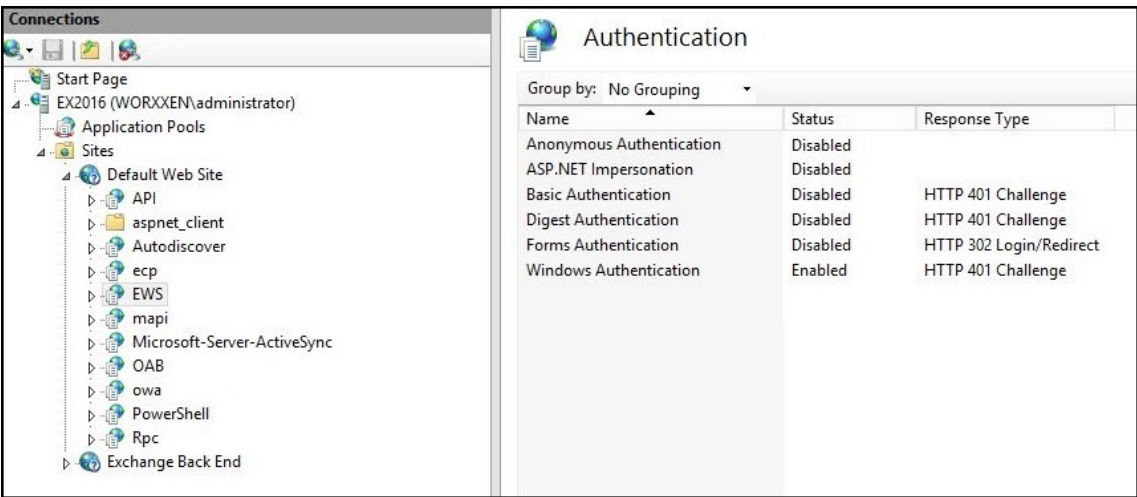
Para comenzar con la configuración, lleve a cabo lo siguiente:

1. Inicie sesión en el servidor o los servidores donde está instalado el directorio virtual de EWS.
2. Abra la consola del Administrador IIS.
3. En **Sitio web predeterminado**, haga clic en el directorio virtual de EWS.

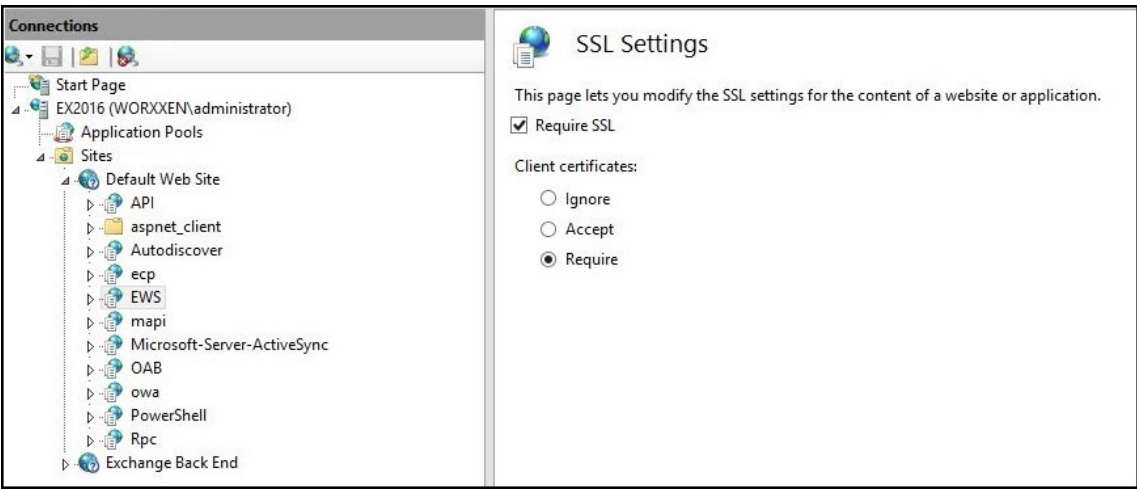
Los complementos de la autenticación, el editor de configuración y SSL están en el lado derecho de la consola del Administrador de IIS.



4. Compruebe que las configuraciones de **Autenticación de EWS** están configurados como se muestra en la siguiente imagen.



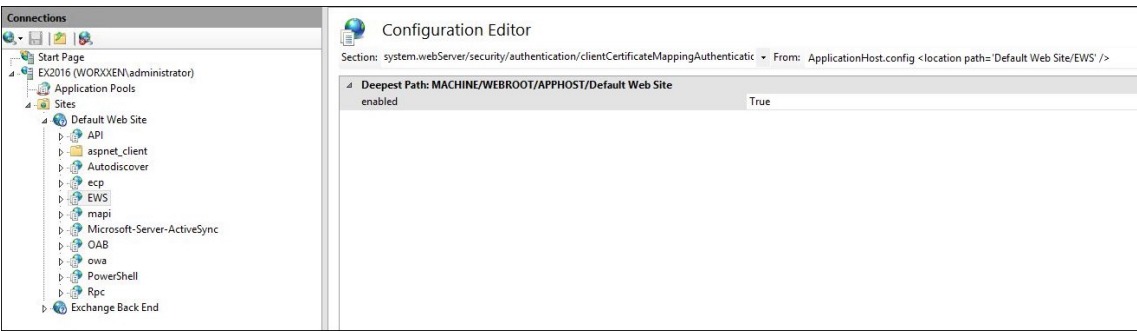
5. Defina la **Configuración de SSL** para el directorio virtual de EWS.
- Marque la casilla **Requerir SSL**.
 - En **Certificados de cliente**, haga clic en **Obligatorio**. O bien, si otros clientes de correo de EWS utilizan el nombre de usuario y la contraseña para autenticarse en Exchange Server, haga clic en **Aceptar**.



6. Haga clic en **Editor de configuración**. Vaya a la siguiente sección de la lista desplegable **Sección**:

- system.webServer/security/authentication/clientCertificateMappingAuthentication**

7. Defina **Habilitado** con el valor **True**.



8. Haga clic en **Editor de configuración**. Vaya a la siguiente sección de la lista desplegable **Sección**:

- **system.webServer/serverRuntime**

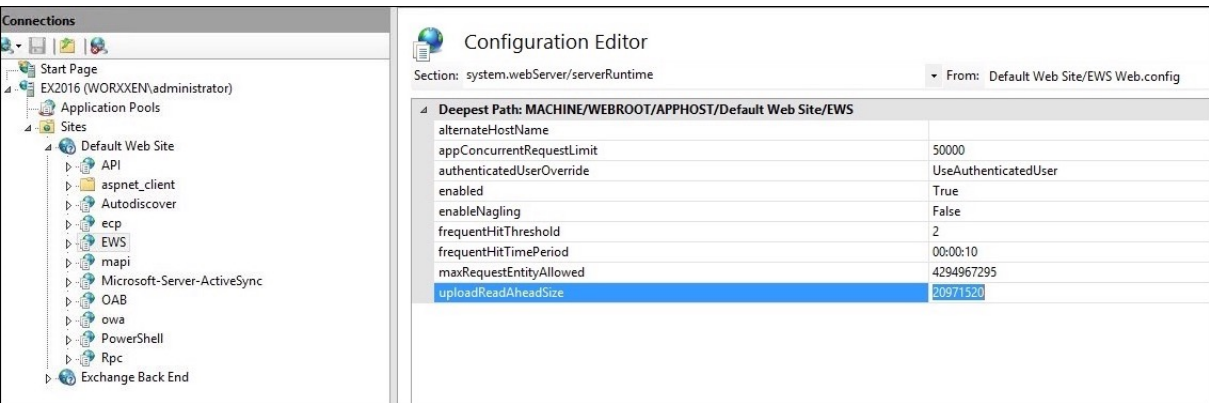
9. Establezca el valor de **uploadReadAheadSize** en **10485760** (10 MB) o **20971520** (20 MB) o en el valor correspondiente que requiera su organización.

Importante:

Si no establece este valor correctamente, la autenticación por certificado puede fallar con el código de error 413 durante la suscripción a las notificaciones push de EWS.

No establezca este valor en **0**.

Para obtener más información, consulte el artículo de Microsoft [Microsoft IIS server runtime](#).



Para obtener más información acerca de la solución de problemas de Citrix Secure Mail con las notificaciones push de iOS, consulte este [artículo de Citrix Support Knowledge Center](#).

Información relacionada

[Notificaciones push en Citrix Secure Mail para iOS](#)

Configurar un servidor Device Health Attestation local

March 1, 2024

Puede habilitar Device Health Attestation (DHA) para dispositivos móviles con Windows 10 o Windows 11 a través de un servidor Windows local. Para habilitar DHA local, 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 Device Health Attestation](#).

Requisitos previos para un servidor DHA

- Un servidor con Windows Server Technical Preview 5 o una versión posterior, instalado mediante la opción de instalación “Experiencia de escritorio”.
- Uno o varios dispositivos cliente con Windows 10 o Windows 11. Estos dispositivos deben tener TPM 1.2 o 2.0 con la versión más reciente de Windows.
- Los certificados:
 - **Certificado SSL de DHA:** Un certificado SSL x.509 encadenado a un certificado raíz empresarial de confianza con una clave privada exportable. Este certificado protege las comunicaciones de datos DHA en tránsito, incluidos:
 - ★ comunicaciones de servidor a servidor (servicio DHA y servidor MDM)
 - ★ comunicaciones de servidor a cliente (servicio DHA y un dispositivo con Windows 10 o Windows 11)
 - **Certificado de firma de DHA:** Un certificado x.509 encadenado a un certificado raíz empresarial de confianza con una clave privada exportable. El servicio DHA usa este certificado para la firma digital.
 - **Certificado de cifrado de DHA:** Un certificado x.509 encadenado a un certificado raíz empresarial de confianza 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

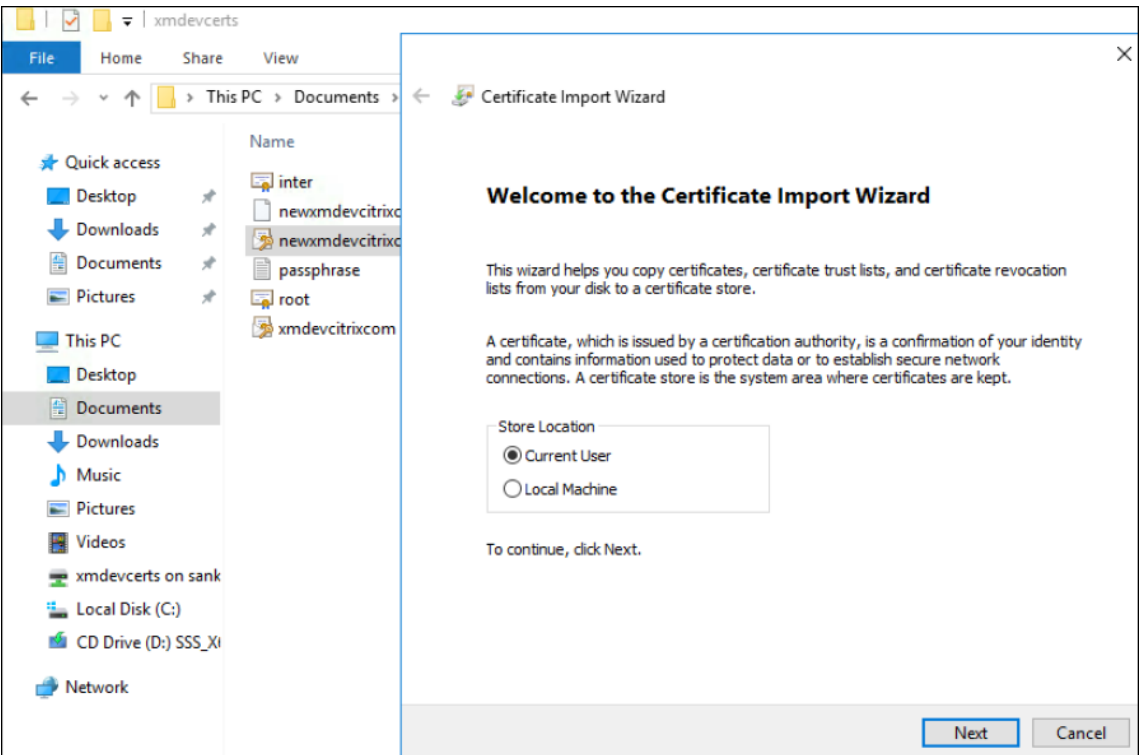
en modo de validación AIKCert deben tener acceso directo a Internet y pueden obtener un certificado AIK de Microsoft.

Agregar el rol del servidor DHA al servidor Windows

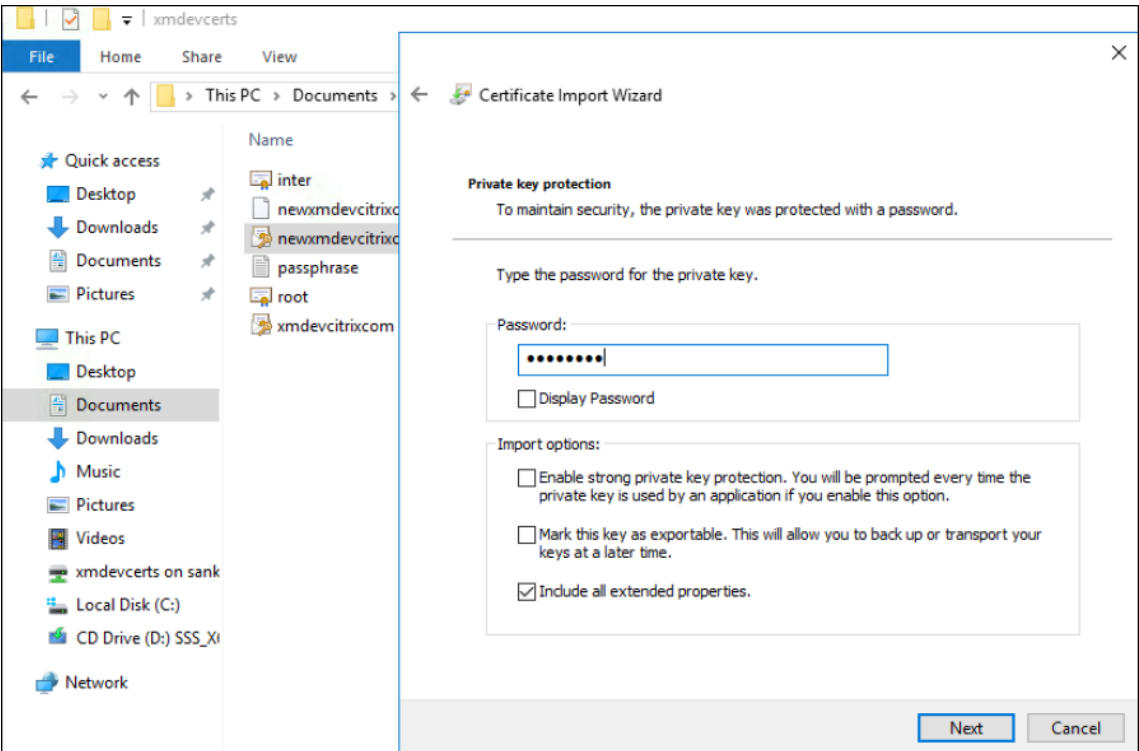
1. En el servidor Windows, si el Administrador de servidores aún no está abierto, haga clic en **Inicio** y luego en **Administrador de servidores**.
2. Haga clic en **Agregar roles y características**.
3. En la página **Antes de empezar**, haga clic en **Siguiente**.
4. En la página **Seleccionar tipo de instalación**, haga clic en **Instalación basada en características o en roles**, y luego haga clic en **Siguiente**.
5. En la página **Seleccionar servidor de destino**, marque **Seleccionar un servidor del grupo de servidores**, seleccione el servidor y luego haga clic en **Siguiente**.
6. En la página **Seleccionar roles de servidor**, marque la casilla **Atestación de estado de dispositivo**.
7. Opcional: Haga clic en **Agregar características** para instalar otros servicios y funciones que requiera el rol.
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 mantenimiento del dispositivo**, haga clic en **Siguiente**.
13. En la página **Confirmar selecciones de instalación**, haga clic en **Instalar**.
14. Cuando termine la instalación, haga clic en **Cerrar**.

Agregar el certificado SSL al almacén de certificados del servidor

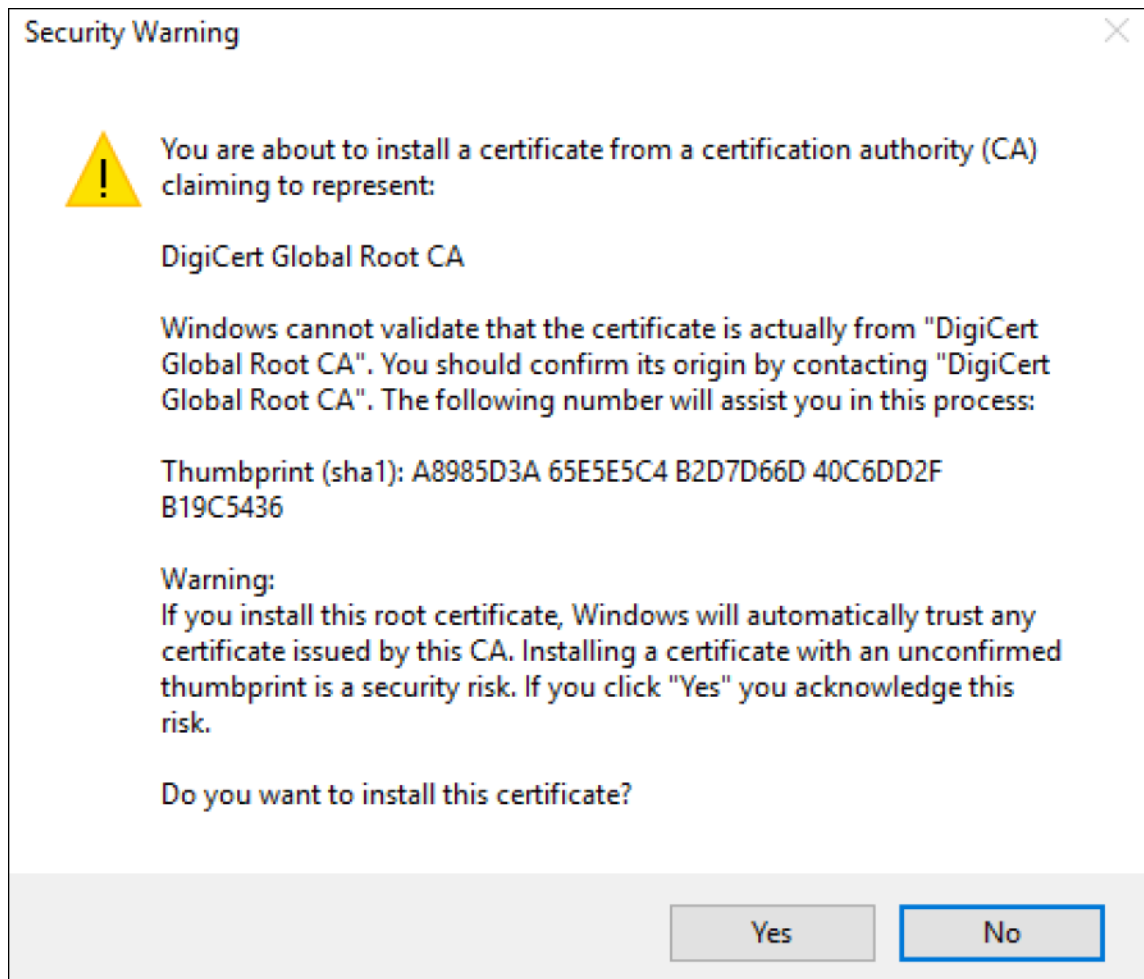
1. Vaya al archivo del certificado SSL y selecciónelo.
2. Seleccione **Usuario actual** como la ubicación del almacén y haga clic en **Siguiente**.



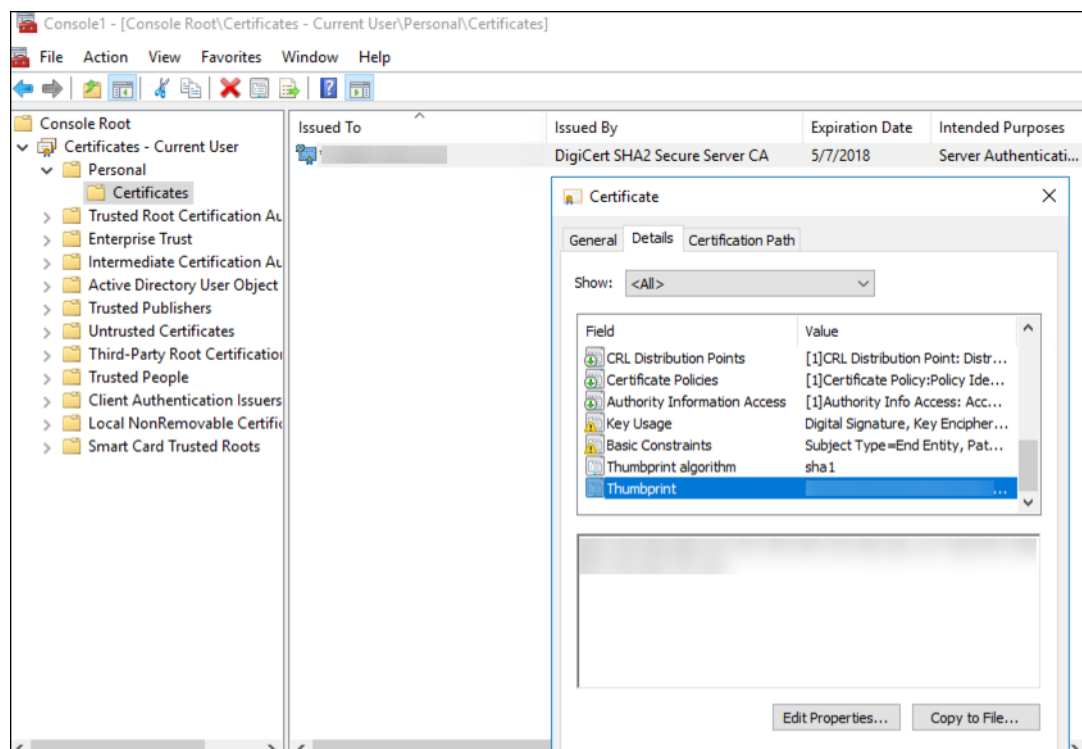
3. Escriba la contraseña de la clave privada.
4. Compruebe que la opción de importación **Incluir todas las propiedades extendidas** está seleccionada. Haga clic en **Siguiente**.



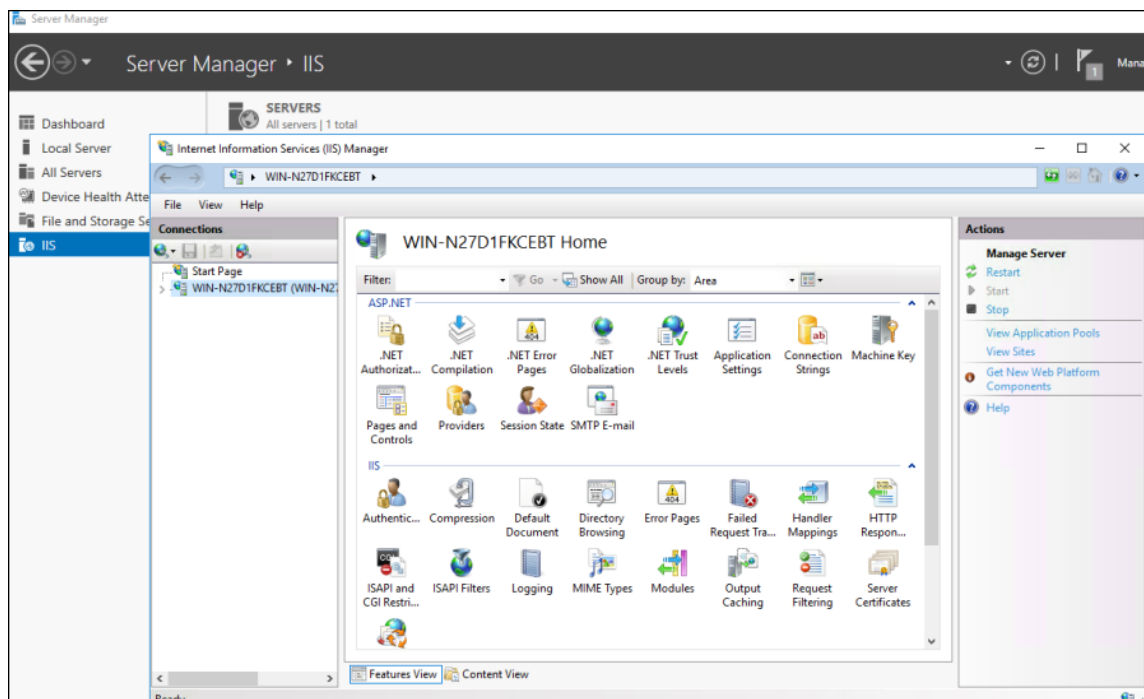
5. Cuando aparezca esta ventana, haga clic en **Sí**.



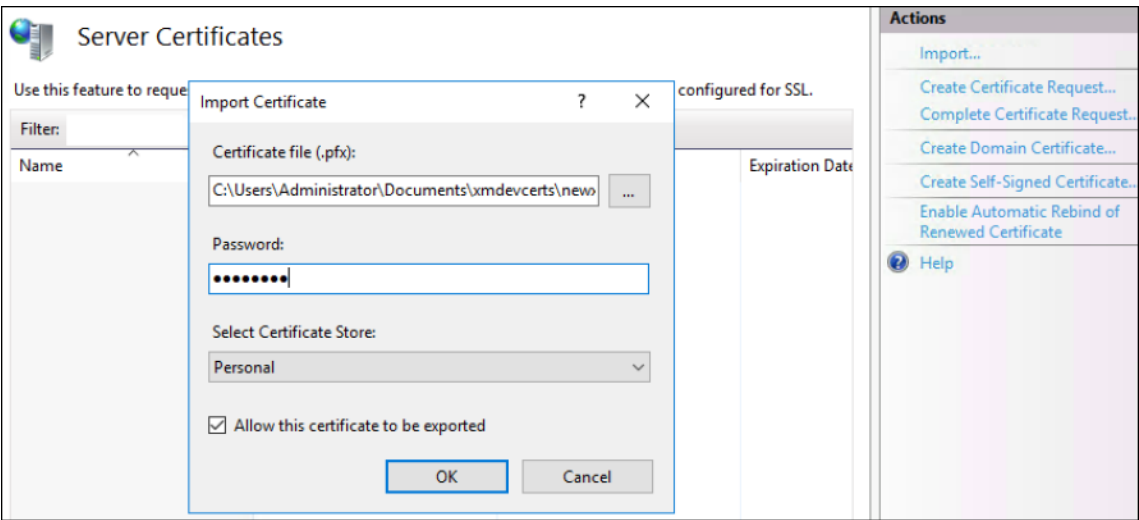
6. Confirme que el certificado está instalado:
- a) Abra la ventana del símbolo del sistema.
 - b) Escriba **mmc** y pulse la tecla **Intro**. Para ver los certificados ubicados en el almacén de la máquina local, debe tener el rol Administrador.
 - c) En el menú "Archivo", haga clic en **Agregar o quitar complemento**.
 - d) Haga clic en **Agregar**.
 - e) En el cuadro de diálogo "Agregar un 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 la cuenta de servicio, seleccione **Cuenta de servicio**.)
 - h) En el cuadro de diálogo "Seleccionar equipo", haga clic en **Finalizar**.



7. Vaya a **Administrador de servidores > IIS** y seleccione **Certificados de servidor** entre los iconos de la lista.

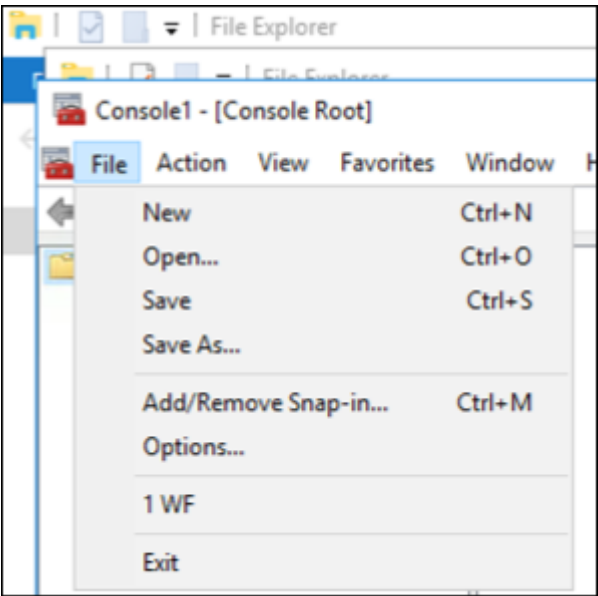


8. En el menú “Acción”, seleccione **Importar...** para importar el certificado SSL.

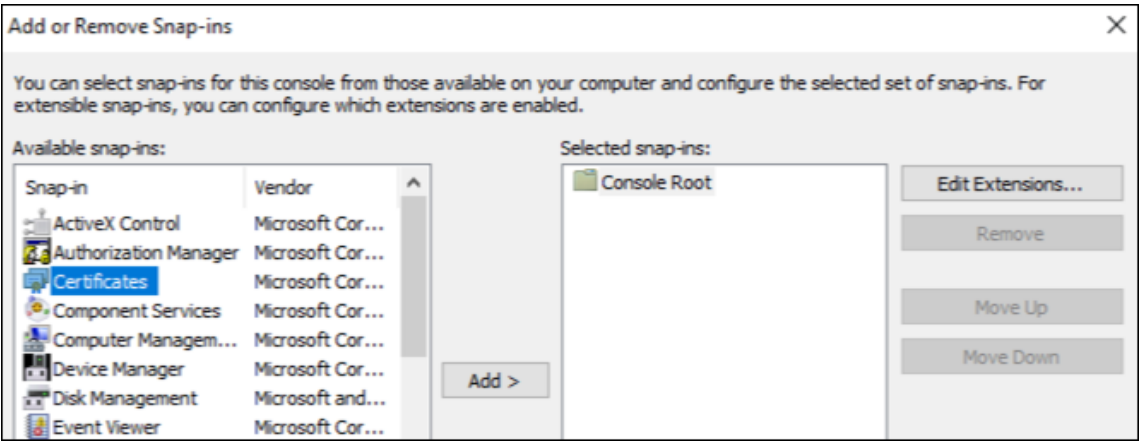


Recuperar y guardar la huella digital del certificado

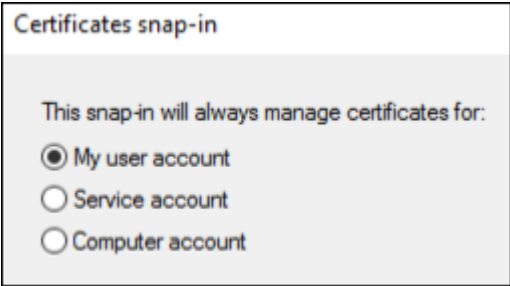
- 1. En la barra de búsqueda del Explorador de archivos, escriba `mmc`.
- 2. En la ventana “Raíz de consola”, haga clic en **Archivo > Agregar o quitar complemento**.



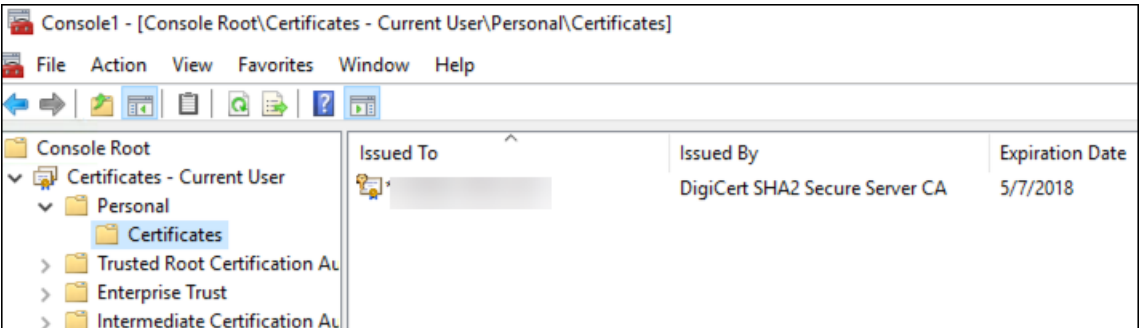
- 3. Seleccione el certificado del complemento disponible y agréguelo a los complementos seleccionados.



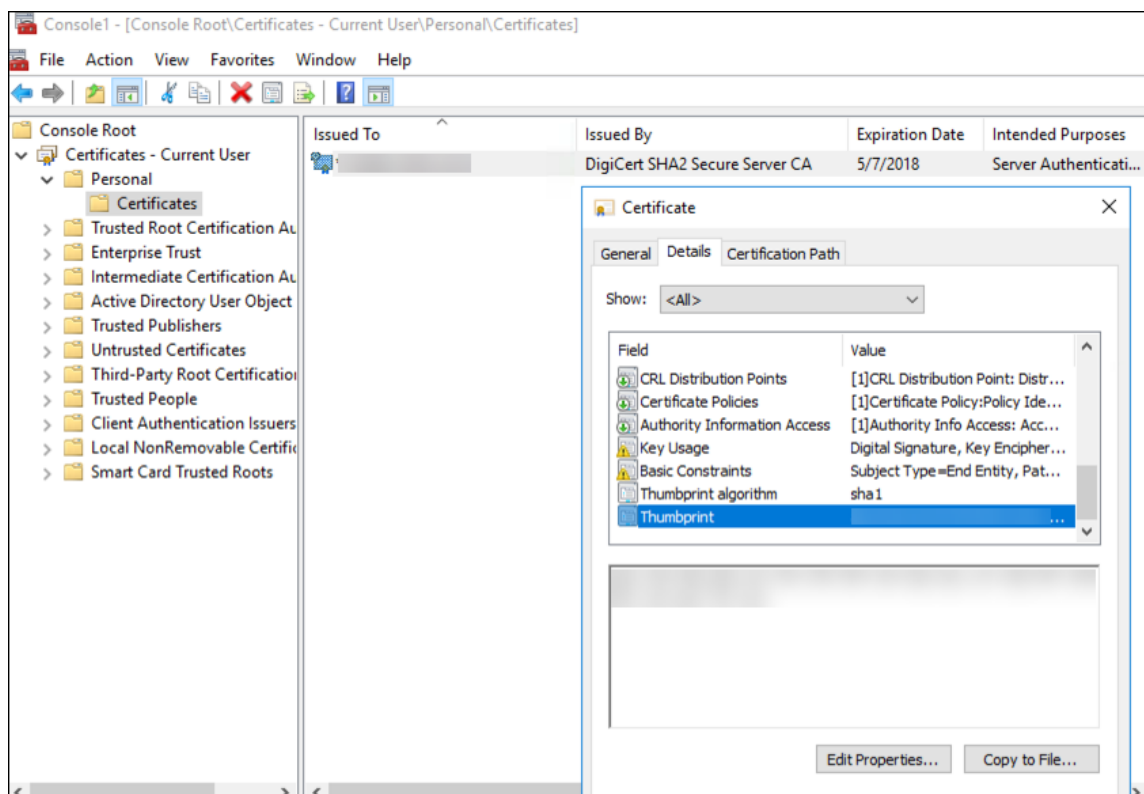
4. Seleccione **Mi cuenta de usuario**.



5. Seleccione el certificado y haga clic en **Aceptar**.



6. Haga doble clic en el certificado y en la ficha **Detalles**. Desplácese hacia abajo para ver la huella digital del certificado.



7. Copie la huella digital a un archivo. Elimine los espacios cuando use 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.

Reemplace el marcador de posición ReplaceWithThumbprint y escríbalo entre comillas dobles, como se muestra a continuación.

```
1 $key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
2   $_.Thumbprint -like "ReplaceWithThumbprint" }
3
4
5 $keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName
6
7 $keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys" +
8   $keyname icls $keypath /grant IIS_IUSRS` :R
9 <!--NeedCopy-->
```

Extraer el certificado raíz de TPM e instalar el paquete de certificado de confianza

Ejecute estos comandos en el servidor Windows:

```
1 mkdir .\TrustedTpm
2
3 expand -F:* .\TrustedTpm.cab .\TrustedTpm
4
5 cd .\TrustedTpm
6
7 .\setup.cmd
8 <!--NeedCopy-->
```

Configurar el servicio DHA

Ejecute este comando en el servidor Windows para configurar el servicio DHA.

Reemplace el marcador de posición ReplaceWithThumbprint.

```
1 Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
   ReplaceWithThumbprint
2
3 -SigningCertificateThumbprint ReplaceWithThumbprint
4
5 -SslCertificateStoreName My -SslCertificateThumbprint
   ReplaceWithThumbprint
6
7 -SupportedAuthenticationSchema "AikCertificate"
8 <!--NeedCopy-->
```

Ejecute estos comandos en el servidor Windows para configurar la directiva de cadena de certificados para el servicio DHA:

```
1 $policy = Get-DHASCertificateChainPolicy
2
3 $policy.RevocationMode = "NoCheck"
4
5 Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
6 <!--NeedCopy-->
```

Responda a estas indicaciones de la siguiente manera:

```
1 Confirm
2
3 Are you sure you want to perform this action?
4
5 Performing the operation "Install-DeviceHealthAttestation" on
   target "[Machine Name]".
6
7 [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?]
   Help (default is "Y"): A
```

```

8
9   Adding SSL binding to website 'Default Web Site'.
10
11  Add SSL binding?
12
13  [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
14
15  Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.
16
17  Add application pool?
18
19  [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
20
21  Adding web application 'DeviceHealthAttestation' to website '
    Default Web Site'.
22
23  Add web application?
24
25  [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
26
27  Adding firewall rule 'Device Health Attestation Service' to allow
    inbound connections on port(s) '443'.
28
29  Add firewall rule?
30
31  [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
32
33  Setting initial configuration for Device Health Attestation Service
    .
34
35  Set initial configuration?
36
37  [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
38
39  Registering User Access Logging.
40
41  Register User Access Logging?
42
43  [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y
44  <!--NeedCopy-->

```

Consultar la configuración

Para comprobar si DHASActiveSigningCertificate está activo, ejecute este comando en el servidor:

`Get-DHASActiveSigningCertificate`

Si el certificado está activo, aparece el tipo de certificado (de firma) y la huella digital.

Para comprobar si DHASActiveSigningCertificate está activo, ejecute estos comandos en el servidor.

Reemplace el marcador de posición ReplaceWithThumbprint y escríbalo entre comillas dobles, como

se muestra a continuación.

```
1 Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"  
   -Force  
2  
3 Get-DHASActiveEncryptionCertificate  
4 <!--NeedCopy-->
```

Si el certificado está activo, se muestra la huella digital.

Para realizar una comprobación final, vaya a la dirección URL:

<https://<dha.myserver.com>/DeviceHealthAttestation/ValidateHealthCertificate/v1>

Si el servicio DHA se está ejecutando, se muestra “Método no permitido”.





© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).