CITRIX

Secure Hub

Contents

Citrix Secure Hub 3

Problemas conocidos y problemas resueltos 15

Situaciones de petición de credenciales 24

Instalar VPN en iOS 27

Inscribir dispositivos mediante credenciales derivadas 30

Citrix Secure Hub

May 17, 2019

Citrix Secure Hub es la plataforma de uso de las aplicaciones móviles de productividad. Los usuarios inscriben sus dispositivos en Secure Hub para obtener acceso a la tienda de aplicaciones. Desde la tienda, pueden agregar aplicaciones móviles de productividad desarrolladas por Citrix y aplicaciones de terceros.

Puede descargar Secure Hub y otros componentes desde la página de descargas de Citrix Endpoint Management.

Para obtener más información sobre Secure Hub y otros requisitos del sistema para las aplicaciones móviles de productividad, consulte Requisitos del sistema.

Novedades en esta versión

Secure Hub 19.5.0

En esta versión se incluyen mejoras de rendimiento y correcciones de errores.

Novedades en versiones anteriores

Secure Hub 19.4.5 y 19.3.5

En estas versiones se incluyen mejoras de rendimiento y correcciones de errores.

Secure Hub 19.3.0

Soporte para Knox Platform for Enterprise de Samsung. Secure Hub para Android admite Knox Platform for Enterprise (KPE) en dispositivos Android Enterprise.

Secure Hub 19.2.0

En esta versión se incluyen mejoras de rendimiento y correcciones de errores.

Secure Hub 19.1.5

Secure Hub para Android Enterprise ahora admite las siguientes directivas:

- **Directiva de Wi-Fi**. La directiva de Wi-Fi ahora admite Android Enterprise. Para obtener más información acerca de esta directiva, consulte [Directiva de Wi-Fi.](/es-es/citrix-endpoint-management/policies/wifi-policy.html)
- **Directiva de XML personalizado**. La directiva de XML personalizado ahora admite Android Enterprise. Para obtener más información acerca de esta directiva, consulte [Directiva de XML personalizado.](/es-es/citrix-endpoint-management/policies/custom-xml-policy.html)
- **Directiva de archivos**. Puede agregar archivos de script en Citrix Endpoint Management para realizar funciones en dispositivos Android Enterprise. Para obtener más información acerca de esta directiva, consulte [Directiva de archivos.](/es-es/citrix-endpoint-management/policies/files-policy.html)

Secure Hub 19.1.0

Secure Hub cuenta con fuentes y colores renovados y otras mejoras de la interfaz de usuario. Este cambio de cara ofrece una experiencia de usuario enriquecida, al mismo tiempo que se ajusta a la estética de la marca Citrix en todo nuestro conjunto de aplicaciones móviles de productividad.

Secure Hub 18.12.0

En esta versión se incluyen mejoras de rendimiento y correcciones de errores.

Secure Hub 18.11.5

- **Configuraciones de la directiva Restricciones para Android Enterprise**. Las nuevas configuraciones de la directiva “Restricciones” permiten a los usuarios acceder a estas funciones en dispositivos Android Enterprise: mantener activa la pantalla, utilizar la barra de estado y Keyguard en la pantalla de bloqueo, administrar cuentas y compartir ubicaciones. Para obtener más información, consulte Directiva de restricciones.

Secure Hub de 18.10.5 a 18.11.0 incluye correcciones de errores y mejoras de rendimiento.

Secure Hub 18.10.0

- **Disponibilidad del modo Samsung DeX:** Samsung DeX permite a los usuarios conectar dispositivos habilitados para KNOX a una pantalla externa para usar aplicaciones, revisar documentos y ver vídeos en una interfaz similar a un PC. Para obtener información sobre los requisitos de dispositivos Samsung DeX y la configuración de Samsung DeX, consulte Cómo funciona Samsung DeX.

Para configurar las funcionalidades del modo Samsung DeX en Citrix Endpoint Management, actualice la directiva Restricciones para Samsung KNOX. Para obtener más información, consulte **Parámetros de Samsung KNOX** en Directiva de restricciones.

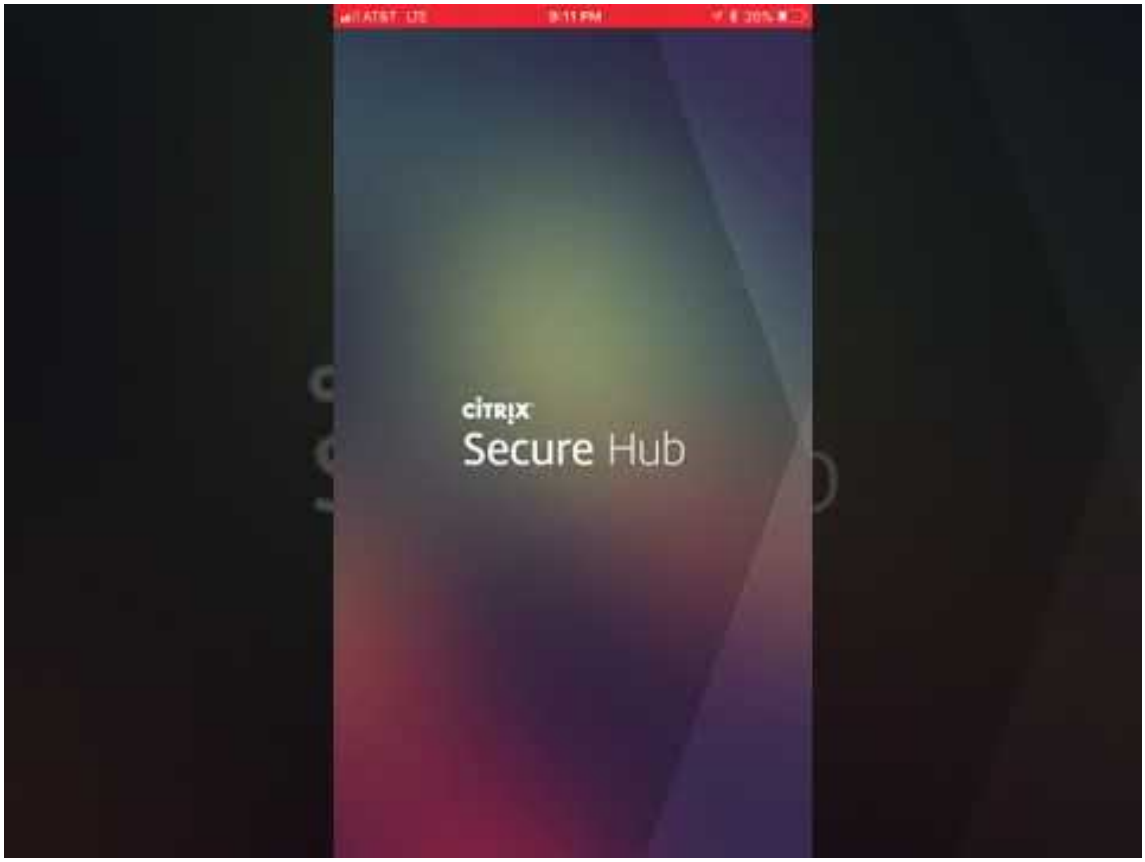
- **Disponibilidad de Android SafetyNet:** Puede configurar Endpoint Management para utilizar la funcionalidad **Android SafetyNet** para evaluar la compatibilidad y la seguridad de los dispositivos Android que tienen Secure Hub instalado. Los resultados se pueden utilizar para desencadenar acciones automatizadas en los dispositivos. Para obtener más información, consulte Android SafetyNet.
- **Impedir el uso de la cámara en dispositivos de Android Enterprise:** La nueva configuración **Permitir el uso de la cámara** de la directiva Restricciones permite impedir que los usuarios utilicen la cámara en sus dispositivos Android Enterprise. Para obtener más información, consulte Directiva de restricciones.

Secure Hub versión 10.8.60 a 18.9.0

Corrección de errores y mejoras de rendimiento.

Secure Hub 10.8.60

- Respaldo para el idioma polaco.
- Respaldo para Android P.
- Respaldo para usar la tienda de aplicaciones de Workspace.
  Al abrir Secure Hub, los usuarios ya no ven la tienda de Secure Hub. El botón **Agregar aplicaciones** lleva a los usuarios a la tienda de aplicaciones de Workspace. En el siguiente vídeo se muestra cómo un dispositivo iOS realiza una inscripción en Citrix Endpoint Management a través de la aplicación Citrix Workspace.



> Importante:
>
> Esta función solo está disponible para nuevos clientes. Actualmente no se admite la migración de clientes existentes.

Para usar esta característica, configure lo siguiente:

- Habilite las directivas de Caché de contraseñas y de Autenticación por contraseña. Para obtener más información sobre la configuración de directivas, consulte Vista general de las directivas MDX para aplicaciones móviles de productividad.
- Configure la autenticación de Active Directory como AD o AD + Cert. Se admiten esos dos modos. Para obtener más información acerca de la Configuración de la autenticación, consulte Autenticación con dominio o dominio y token de seguridad.
- Habilite la integración de Workspace para Endpoint Management. Para obtener más información acerca de la integración del espacio de trabajo, consulte Configurar el espacio de trabajo.

> Importante:
>
> Después de habilitar esta función, el inicio de sesión único (SSO) de Citrix Files se hace a través de Workspace, no a través de Endpoint Management (antes XenMobile). Se recomienda que inhabilite la integración de Citrix Files en la consola de Endpoint Manage-

> ment antes de habilitar la integración de Workspace.

Secure Hub 10.8.55

- La capacidad de pasar un nombre de usuario y una contraseña al portal Google Zero Touch y KNOX Mobile Environment (KME) mediante la configuración JSON. Para obtener información detallada, consulte Inscribir en bloque dispositivos Samsung KNOX.
- Cuando se habilita la fijación de certificados, los usuarios no pueden inscribirse en Endpoint Management con un certificado autofirmado. Si los usuarios intentan inscribirse en Endpoint Management con un certificado autofirmado, se les advierte de que el certificado no es de confianza.

Secure Hub 10.8.25: Secure Hub para Android es compatible con dispositivos Android P.

> Nota:
>
> Antes de actualizar a la plataforma Android P, 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. Ya no se confía en los certificados que no contienen un SAN que coincida con el nombre de host. Para obtener más información, consulte el artículo Android P behavior changes en Cambios en el comportamiento de Android P.

Actualización de Secure Hub para iOS del 19 de marzo de 2018: Secure Hub 10.8.6 para iOS soluciona un problema con la directiva de aplicación VPP. Para obtener más información, consulte este artículo de Citrix Knowledge Center.

Secure Hub 10.8.5: Respaldo en Secure Hub para Android para el modo COSU de Android Enterprise (Android for Work). Para obtener más detalles, consulte Documentación de Citrix Endpoint Management.

Administrar Secure Hub

La mayoría de las tareas de administración relacionadas con Secure Hub se llevan a cabo durante la configuración de Endpoint Management. Para que Secure Hub esté disponible para los usuarios en iOS o Android, cargue Secure Hub en la App Store de iOS y la tienda Google Play respectivamente.

Secure Hub actualiza la mayoría de las directivas MDX almacenadas en Endpoint Management para las aplicaciones instaladas cuando la sesión de un usuario en Citrix Gateway se renueva después de autenticarse mediante Citrix Gateway.

> Importante:
>
> Los cambios en estas directivas requieren que el usuario elimine y vuelva a instalar la aplicación para aplicar la directiva actualizada: Grupo de seguridad, Habilitar cifrado y Secure Mail Exchange Server.

PIN de Citrix

Puede configurar Secure Hub para que use el PIN de Citrix, una característica de seguridad habilitada en la consola de Endpoint Management en **Parámetros** > **Propiedades de cliente**. Para este parámetro, los usuarios de los dispositivos móviles inscritos deben iniciar sesión en Secure Hub y activar al menos una aplicación MDX empaquetada mediante un número de identificación personal (PIN).

La función PIN de Citrix simplifica la experiencia de autenticación del usuario al iniciar sesión en las aplicaciones seguras empaquetadas. No es necesario que los usuarios escriban repetidamente otras credenciales (como los nombres de usuario y las contraseñas de Active Directory).

Sin embargo, los usuarios que inicien sesión en Secure Hub por primera vez sí deberán introducir el nombre de usuario y la contraseña de Active Directory. Durante el inicio de sesión, Secure Hub guardará las credenciales de Active Directory o un certificado de cliente en el dispositivo de usuario y, a continuación, pedirá al usuario que escriba un PIN. Cuando el usuario vuelva a iniciar sesión, introducirá el PIN para acceder a sus aplicaciones Citrix y al Store de manera segura hasta que se agote el tiempo de espera de inactividad que tenga la sesión activa del usuario. Hay otras propiedades de cliente relacionadas que permiten cifrar secretos con el PIN, especificar el tipo de código de acceso para el PIN y especificar otros requisitos de longitud y complejidad para el mismo. Para obtener información detallada, consulte Propiedades de cliente.

Cuando la autenticación con huella digital (touch ID) está habilitada, los usuarios pueden iniciar sesión con una huella digital cuando se requiere la autenticación sin conexión debido a la inactividad de una aplicación. Los usuarios aún tendrán que introducir el PIN cuando inicien sesión en Secure Hub por primera vez, cuando reinicien el dispositivo o cuando se agote el tiempo de espera de inactividad. Para obtener información sobre cómo habilitar la autenticación por huella digital, consulte Autenticación por huella digital o Touch ID.

Fijar certificados

Secure Hub para iOS y Android respalda la fijación de certificados SSL. Esta característica comprueba que sea el certificado firmado por su empresa el que se utilice cuando los clientes Citrix se comuniquen con Endpoint Management, lo que impedirá conexiones desde clientes a Endpoint Management si la instalación de un certificado raíz en el dispositivo pone en riesgo la sesión SSL. Si Secure Hub detecta cambios en la clave pública del servidor, rechazará la conexión.

A partir de Android N, el sistema operativo ya no permite las entidades de certificación (CA) que agregue el usuario. Citrix recomienda utilizar una entidad de certificación raíz pública en lugar de una entidad de certificación agregada por el usuario.

Es posible que los usuarios que se actualicen a Android N tengan problemas si utilizan entidades de certificación privadas o autofirmadas. Las conexiones en dispositivos Android N se interrumpen en las siguientes situaciones:

- Las entidades de certificación privadas o autofirmadas y la opción "Required Trusted CA for Endpoint Management" están **activadas**. Para obtener información detallada, consulte Servicio de detección automática de Endpoint Management.
- Las entidades de certificación privadas o autofirmadas y el servicio de detección automática (ADS) de Endpoint Management no es accesible. Por razones de seguridad, cuando no se puede establecer conexión con el servicio ADS, la opción "Required Trusted CA" se **activa** aunque se haya establecido como **desactivada** al principio.

Antes de inscribir dispositivos o actualizar Secure Hub, puede habilitar la fijación de certificados. La opción está **desactivada** de manera predeterminada y está administrada por el servicio de detección automática (ADS). Cuando se habilita la fijación de certificados, los usuarios no pueden inscribirse en Endpoint Management con un certificado autofirmado. Si los usuarios intentan inscribirse con un certificado autofirmado, se les advierte de que el certificado no es de confianza. La inscripción falla si los usuarios no aceptan el certificado.

Para usar la fijación de certificados, solicite que Citrix cargue los certificados en el servidor Citrix ADS. Inicie un caso de asistencia técnica desde el portal de asistencia técnica de Citrix.. Luego, debe proporcionar la siguiente información:

- El dominio que contiene las cuentas con las que se van a inscribir los usuarios.
- El nombre de dominio completo (FQDN) de Endpoint Management.
- El nombre de la instancia de Endpoint Management. De forma predeterminada, el nombre de la instancia es zdm y en el campo se distinguen mayúsculas y minúsculas.
- El tipo de ID de usuario, que puede ser UPN o correo electrónico. De forma predeterminada, el tipo es UPN.
- El puerto utilizado para la inscripción de iOS si se ha cambiado el número del puerto predeterminado (8443) a otro número de puerto.
- El puerto a través del cual Endpoint Management acepta las conexiones, si se ha cambiado el número del puerto predeterminado (443) a otro número de puerto.
- La dirección URL completa de su Citrix Gateway.
- Si quiere, puede agregar una dirección de correo electrónico para el administrador.
- Los certificados con formato PEM que quiere que se agreguen al dominio.
- Cómo administrar los certificados de servidor existentes: Si quiere quitar el certificado de servidor antiguo inmediatamente (porque no es seguro) o si quiere seguir dando respaldo al certificado de servidor antiguo hasta que caduque.

Su caso de asistencia técnica se actualizará cuando sus datos y su certificado se hayan agregado a los servidores Citrix.

Certificado + autenticación de contraseña de un solo uso

Puede configurar Citrix ADC para que Secure Hub se autentique usando un certificado y un token de seguridad que sirva como una contraseña de un solo uso. Esta configuración ofrece una opción segura que no deja huella de Active Directory en los dispositivos.

Para que Secure Hub use este tipo de autenticación, haga lo siguiente: Agregue una acción de reescritura y una directiva de reescritura en Citrix ADC que inserte un encabezado de respuesta personalizado del formulario **X-Citrix-AM-GatewayAuthType: CertAndRSA** para indicar el tipo de inicio de sesión de Citrix Gateway.

Por lo general, Secure Hub utiliza el tipo de inicio de sesión de Citrix Gateway configurado en la consola de Endpoint Management. No obstante, Secure Hub no obtiene esta información hasta que completa el inicio de sesión por primera vez. Por lo tanto, el encabezado personalizado es obligatorio.

> Nota:
>
> Si se definen tipos de inicio de sesión diferentes para Endpoint Management y Citrix ADC, la configuración de Citrix ADC prevalece. Para obtener información detallada, consulte Citrix Gateway y Endpoint Management.

1. En Citrix ADC, vaya a **Configuration > AppExpert > Rewrite > Actions**.
2. Haga clic en **Agregar**.

   Aparecerá la pantalla **Create Rewrite Action**.
3. Rellene los campos como se muestra en la siguiente imagen y, a continuación, haga clic en **Create**.

   Aparece este resultado en la pantalla principal **Rewrite Actions**.
4. Vincule la acción de reescritura al servidor virtual como una directiva de reescritura. Vaya a **Configuration > NetScaler Gateway > Virtual Servers** y seleccione el servidor virtual.
5. Haga clic en **Modificar**.
6. En la pantalla **Virtual Servers configuration**, vaya a **Policies**.
7. Haga clic en **+** para agregar una directiva.
8. En el campo **Choose Policy**, elija **Rewrite**.
9. En el campo **Choose Type**, elija **Response**.
10. Haga clic en **Continuar**.

    Se expande la sección **Policy Binding**.

11. Haga clic en **Select Policy**.

    Aparecerá una pantalla con las directivas disponibles.

12. Haga clic en la fila de la directiva que acaba de crear y, a continuación, haga clic en **Select**. Aparece de nuevo la pantalla **Policy Binding**, con la directiva seleccionada.

13. Haga clic en **Bind**.

    Si la vinculación se realiza correctamente, la pantalla principal aparece mostrando la configuración de la directiva de reescritura.

14. Para ver los datos de la directiva, haga clic en **Rewrite Policy**.

Requisitos de puerto para la conectividad con ADS para dispositivos Android

La configuración de puertos garantiza que los dispositivos Android que se conectan desde Secure Hub puedan acceder a Citrix ADS desde dentro de la red corporativa. La capacidad para acceder a ADS es importante para descargar las actualizaciones de seguridad disponibles a través del ADS. Es posible que las conexiones ADS no sean compatibles con el servidor proxy. En este caso, permita que la conexión ADS circunvale el servidor proxy.

> Importante:
>
> Secure Hub para iOS y Android requiere autorización para que los dispositivos Android accedan a ADS. Para obtener más información, consulte Requisitos de puertos en la documentación de Endpoint Management. Esta comunicación tiene lugar en el puerto de salida 443. Es muy probable que el entorno existente esté diseñado para permitir este acceso. Los clientes que no puedan garantizar esta comunicación no deberían actualizar a Secure Hub 10.2. Si tiene dudas o preguntas, contacte con la asistencia de Citrix.

Requisitos previos:

- Deben obtener certificados de Endpoint Management y Citrix ADC. Los certificados deben estar en formato PEM y deben ser un certificado público y no la clave privada.
- Ponerse en contacto con la asistencia técnica de Citrix y solicitar la habilitación de la fijación de certificados. Durante este proceso, se le pedirán los certificados.

Las nuevas mejoras para la fijación de certificados requieren que los dispositivos se conecten al servicio ADS antes de que el dispositivo se inscriba. Este requisito previo garantiza que Secure Hub tenga disponible la información de seguridad más actualizada para el entorno en que se va a inscribir el dispositivo. Si los dispositivos no pueden contactar con el servicio ADS, Secure Hub no permitirá inscribirlos. Por lo tanto, la apertura del acceso al servicio ADS dentro de la red interna es vital para permitir la inscripción de dispositivos.

Para que Secure Hub para Android acceda al servicio ADS, abra el puerto 443 para el nombre de dominio completo (FQDN) y las direcciones IP siguientes:

Nombre de dominio completo (FQDN)	Dirección IP	Puerto	Uso de IP y puerto
discovery.mdm.zenprise.com	52.5.138.94	443	Secure Hub - Comunicación ADS
discovery.mdm.zenprise.com	52.1.30.122	443	Secure Hub - Comunicación ADS
ads.xm.cloud.com: Tenga en cuenta que Secure Hub 10.6.15 y versiones posteriores utiliza ads.xm.cloud.com.	34.194.83.188	443	Secure Hub - Comunicación ADS
ads.xm.cloud.com: Tenga en cuenta que Secure Hub 10.6.15 y versiones posteriores utiliza ads.xm.cloud.com.	34.193.202.23	443	Secure Hub - Comunicación ADS

Si se habilita la fijación de certificados:

- Secure Hub fija el certificado de su empresa durante la inscripción del dispositivo.
- Durante una actualización, Secure Hub descarta cualquier certificado que esté fijado en ese momento y fija el certificado del servidor durante la primera conexión de los usuarios ya inscritos.

  > Nota:
  >
  > Si habilita la fijación de certificados después de realizar una actualización, los usuarios deben reinscribirse.

- La renovación de certificados no requiere la reinscripción, siempre que la clave pública del certificado no se haya modificado.

La fijación de certificados respalda los certificados de hoja, no certificados de emisor ni certificados intermedios. La fijación de certificados se aplica a servidores Citrix, tales como Endpoint Management y Citrix Gateway, no a servidores de terceros.

Uso de Secure Hub

Los usuarios empiezan por descargar Secure Hub en sus dispositivos desde las tiendas de aplicaciones de Apple o Android.

Cuando Secure Hub se abre, los usuarios deben introducir las credenciales proporcionadas por su empresa para inscribir sus dispositivos en Secure Hub. Para obtener más información acerca de la inscripción de dispositivos, consulte Inscripción, roles y cuentas de usuario.

En Secure Hub para Android, durante la instalación inicial y la inscripción, aparece este mensaje: ¿Permitir que Secure Hub acceda a fotos, archivos multimedia y archivos en su dispositivo?

Este mensaje proviene del sistema operativo Android, no de Citrix. Cuando toca en **Permitir**, ni Citrix ni los administradores de Secure Hub ven sus datos personales en ningún momento. Sin embargo, si lleva a cabo una sesión de asistencia remota con su administrador, este puede ver sus archivos personales en la sesión.

Una vez inscritos, los usuarios verán las aplicaciones y los escritorios que usted haya insertado en su ficha **Mis aplicaciones**. Los usuarios pueden agregar más aplicaciones desde Store. En los teléfonos, el enlace a Store se encuentra dentro de **Parámetros**, cuyo icono está situado en la esquina superior izquierda.

En las tabletas, Store es una ficha aparte.

Cuando los usuarios con iPhones iOS 9 o posterior instalen aplicaciones móviles de productividad desde la tienda, verán un mensaje. El mensaje indica que el desarrollador empresarial, Citrix, no es de confianza en ese iPhone. Asimismo, el mensaje indica que la aplicación no estará disponible hasta que el desarrollador sea de confianza. Si aparece ese mensaje, Secure Hub pedirá a los usuarios que consulten una guía que les ofrecerá instrucciones para establecer relaciones de confianza entre el iPhone y las aplicaciones de empresa de Citrix.

Inscripción automática en Secure Mail

Para implementaciones de solo MAM, puede configurar Endpoint Management para que los usuarios con dispositivos iOS o Android que se inscriban en Secure Hub con las credenciales de correo electrónico se inscriban automáticamente en Secure Mail. Los usuarios no tienen que introducir información adicional ni realizar pasos adicionales para inscribirse en Secure Mail.

La primera vez que se usa Secure Mail, este obtiene el ID, el dominio y la dirección de correo electrónico del usuario desde Secure Hub. Secure Mail usa la dirección de correo electrónico para la detección automática. El servidor Exchange se identifica con el dominio y el ID del usuario, lo que permite a Secure Mail autenticar automáticamente al usuario. Se solicita al usuario que introduzca una contraseña si la directiva está configurada para no admitirla automáticamente. Sin embargo, no es necesario que el usuario introduzca ninguna información adicional.

Para habilitar esta funcionalidad, cree tres propiedades:

- La propiedad de servidor MAM_MACRO_SUPPORT. Para obtener instrucciones, consulte Propiedades de servidor.

- Las propiedades de cliente ENABLE_CREDENTIAL_STORE y SEND_LDAP_ATTRIBUTES. Para obtener instrucciones, consulte Propiedades de cliente.

Tienda personalizada

Si quiere personalizar la tienda, vaya a **Parámetros > Personalización de marca de cliente** para cambiar el nombre, agregar un logotipo y especificar la forma en que aparecerán las aplicaciones.

Puede modificar las descripciones de las aplicaciones desde la consola de Endpoint Management. Haga clic en **Configurar**, y luego en **Aplicaciones**. Seleccione la aplicación en la tabla y haga clic en **Modificar**. Seleccione las plataformas de la aplicación cuya descripción esté modificando e introduzca el texto en el cuadro **Descripción**.

En la tienda de aplicaciones, los usuarios pueden explorar solo las aplicaciones y los escritorios que usted haya configurado y protegido en Endpoint Management. Para agregar la aplicación, los usuarios deben tocar en **Detalles** y, luego, en **Agregar**.

Opciones de Ayuda configuradas

Secure Hub también ofrece a los usuarios varios métodos de obtención de ayuda. En tabletas, pueden tocar en el signo de interrogación en la esquina superior derecha para ver las opciones de ayuda. En los teléfonos, los usuarios pueden tocar en el icono del menú de tres líneas situado en la esquina superior izquierda y, a continuación, en **Ayuda**.

Su departamento de TI muestra el número de teléfono y la dirección de correo electrónico del servicio de asistencia o Help Desk de su empresa, al que los usuarios pueden acceder directamente desde la aplicación. Debe introducir estos números de teléfono y direcciones de correo electrónico en la consola de Endpoint Management. Haga clic en el icono de engranaje en la esquina superior derecha. Aparecerá la página **Parámetros**. Haga clic en **Más** y, a continuación, en **Asistencia del cliente**. Aparece la pantalla para escribir la información.

Notificar problema muestra una lista de las aplicaciones del usuario. Los usuarios seleccionan la aplicación que presenta el problema. Secure Hub genera automáticamente los registros y, a continuación, abre un mensaje en Secure Mail con los registros adjuntos comprimidos en archivo ZIP. Los usuarios pueden agregar el asunto y la descripción del problema. También pueden adjuntar una captura de pantalla.

Enviar comentarios a Citrix abre un mensaje en Secure Mail con una dirección de asistencia de Citrix ya rellenada. En el cuerpo del mensaje, el usuario puede escribir sugerencias para mejorar Secure Mail. Si Secure Mail no está instalado en el dispositivo, se abre el programa de correo nativo.

Los usuarios también pueden tocar en **Asistencia técnica de Citrix**, con lo que irán a Citrix Knowledge Center. Desde aquí, pueden buscar artículos de asistencia técnica para todos los productos Citrix.

En **Preferencias**, los usuarios verán información sobre sus cuentas y dispositivos.

Directivas de localización geográfica

Secure Hub también ofrece directivas de geoseguimiento y geolocalización para, por ejemplo, garantizar que un dispositivo propiedad de la empresa no abandone un perímetro geográfico determinado. Para obtener información detallada, consulte directiva de localización geográfica.

Recopilar y analizar fallos

Secure Hub recopila y analiza automáticamente la información de un fallo, de modo que usted pueda ver qué fue lo que provocó ese fallo. El software Crashlytics admite esta función.

Para obtener más funciones disponibles para iOS y Android, consulte la Tabla de funciones por plataforma de Citrix Secure Hub.

Problemas conocidos y problemas resueltos

May 17, 2019

Problemas conocidos en la versión 19.5.0

Secure Hub para iOS

No hay ningún problema conocido en esta versión.

Secure Hub para Android

- Después de la inscripción, los dispositivos OnePlus Android versión 7.1.1 y OnePlus 5T Android versión 9.0.3 requieren el reinicio manual de Secure Hub para solicitar el PIN de Citrix. [CXM-64120]
- En Secure Hub para Android, las aplicaciones necesarias no se implementan en dispositivos Android a menos que actualice la directiva o actualice la tienda. [CXM-65635]

Problemas resueltos en la versión 19.5.0

Secure Hub para iOS

No hay problemas resueltos en esta versión.

Secure Hub para Android

- En Secure Hub para Android, los dispositivos Android 6.0 no se inscriben si hay varios nombres alternativos de sujeto en el certificado del servidor. [CXM-65030]
- En Secure Hub para Android, las aplicaciones administradas no se desinstalan al desinscribir los dispositivos. [CXM-65369]

Problemas resueltos y conocidos en versiones anteriores

Problemas conocidos en la versión 19.4.5

No hay ningún problema conocido en esta versión.

Problemas resueltos en la versión 19.4.5

Secure Hub para iOS

En dispositivos iOS, al hacer clic en el enlace de inscripción de dispositivos, el nombre de dominio completo de instancia de Endpoint Management no se rellena automáticamente en Secure Hub. Se produce un error en la solicitud de inscripción del dispositivo. [CXM-65423]

Secure Hub para Android

No hay problemas resueltos en esta versión.

Problemas conocidos en la versión 19.3.5

Secure Hub para iOS

Cuando se envían notificaciones desde Secure Hub para iOS, el recuento de insignias de notificación no se actualiza para Secure Hub. [CXM-53500]

Secure Hub para Android

No hay ningún problema conocido en esta versión.

Problemas resueltos en la versión 19.3.5

Secure Hub para iOS

No hay problemas resueltos en esta versión.

Secure Hub para Android

- En Secure Hub para Android, cuando inscribe dispositivos compartidos, implementa la directiva **clip Web** y agrega aplicaciones web y SaaS, la implementación se realiza correctamente. Sin embargo, esta implementación aparece como un error en la pantalla **Inventario de aplicaciones** de la consola de Citrix Endpoint Management. [CXM-57500]
- En Secure Hub para Android, cuando los usuarios inician sesión con PIN Secure, se establece un túnel VPN, pero Secure Web no carga ningún sitio web. Sin embargo, el sitio web se cargará como se esperaba cuando Secure Web se cierra y se vuelve a abrir. [CXM-60751]
- Si se ha configurado Secure Mail para Android con directivas de Microsoft Intune, después de la autenticación se muestra una pantalla vacía. [CXM-61457]
- En Secure Hub para Android, las aplicaciones que tienen el cifrado inhabilitado intentan obtener claves de cifrado de Secure Hub. [CXM-61459]
- Secure Mail para Android se bloquea al iniciarse cuando se instala la versión 5.0.4324.0 del Portal de empresa de Intune. Para obtener más detalles, consulte este artículo de Citrix Support Knowledge Center. [CXM-62516]
- En Secure Hub para Android, no se pueden usar las aplicaciones del sistema en dispositivos Android Enterprise de uso único y propiedad de la empresa (COSU) que se ejecutan en Android 7.1.1. [CXM-63653]
- En Secure Hub para Android, al configurar varias aplicaciones de Google Play como “aplicaciones obligatorias” e intentar inscribirse, se le pedirá que instale la primera aplicación. El mensaje inicial va seguido inmediatamente de otro mensaje que pide instalar la segunda aplicación, y así sucesivamente. [CXM-63654]

Problemas conocidos en la versión 19.3.0

Secure Hub para iOS

No hay ningún problema conocido en esta versión.

Secure Hub para Android

- En Secure Hub para Android, cuando inscribe dispositivos compartidos, implementa la directiva clip Web y agrega aplicaciones web y SaaS, la implementación se realiza correctamente. Sin embargo, esta implementación aparece como un error en la pantalla Inventario de aplicaciones de la consola de Citrix Endpoint Management. [CXM-57500]

- En dispositivos Android Enterprise, cuando se establece una acción de bloqueo para infracciones de geocerca en la directiva Ubicación, el dispositivo le solicita que establezca una nueva contraseña en lugar de utilizar el código de acceso generado por el sistema. [CXM-60425]

Problemas resueltos en la versión 19.3.0

Secure Hub para iOS

No hay problemas resueltos en esta versión.

Secure Hub para Android

Bloquear dispositivos Android Enterprise completamente administrados de forma remota mediante la acción de seguridad para bloquear con código de acceso podría fallan sin notificarle del fallo. Para comprobar que un dispositivo está bloqueado, configure la acción de bloquear con código de acceso dos veces. El dispositivo se bloquea con el segundo código de acceso configurado. [CXM-61095]

Problemas conocidos en la versión 19.3.0

Secure Hub para iOS

No hay ningún problema conocido en esta versión.

Secure Hub para Android

- En Secure Hub para Android, cuando inscribe dispositivos compartidos, implementa la directiva clip Web y agrega aplicaciones web y SaaS, la implementación se realiza correctamente. Sin embargo, esta implementación aparece como un error en la pantalla Inventario de aplicaciones de la consola de Citrix Endpoint Management. [CXM-57500]
- En dispositivos Android Enterprise, cuando se establece una acción de bloqueo para infracciones de geocerca en la directiva Ubicación, el dispositivo le solicita que establezca una nueva contraseña en lugar de utilizar el código de acceso generado por el sistema. [CXM-60425]

Problemas resueltos en la versión 19.3.0

Secure Hub para iOS

No hay problemas resueltos en esta versión.

Secure Hub para Android

Bloquear dispositivos Android Enterprise completamente administrados de forma remota mediante la acción de seguridad para bloquear con código de acceso podría fallan sin notificarle del fallo. Para comprobar que un dispositivo está bloqueado, configure la acción de bloquear con código de acceso dos veces. El dispositivo se bloquea con el segundo código de acceso configurado. [CXM-61095]

Problemas conocidos en la versión 19.2.0

No hay problemas conocidos en la versión 19.2.0.

Problemas resueltos en la versión 19.2.0

Secure Hub para iOS

En Secure Hub para iOS, el siguiente mensaje de error de protocolo de enlace SSL aparece repetidamente cuando los usuarios inician sesión en la tienda de Secure Hub: Se ha agotado el tiempo de espera de la solicitud de red para obtener aplicaciones desde el servidor. [CXM-61339]

Secure Hub para Android

- La directiva “Archivos” para Android Enterprise no se implementa en dispositivos Android que estén en el modo de perfil de trabajo. [CXM-61196]
- En Secure Hub para Android, la autorización de inicio de sesión de un nuevo usuario tarda mucho en dispositivos compartidos. Cuando cierre la sesión como usuario inscrito e intente iniciar sesión como nuevo usuario, Secure Hub se mantendrá hasta que reinicie el dispositivo. [CXM-61338]
- En Secure Hub para Android, los clientes de la nube no pueden inscribir dispositivos Android Enterprise con un proveedor de identidades externo. [CXM-61738]
- En Secure Hub para Android, cuando se encuentra en el modo de uso único y propiedad de la empresa (COSU), los iconos de la aplicación se solapan en Secure Hub. [CXM-61740]
- En Secure Hub para Android, cuando la fijación de certificados está habilitada para la configuración existente, la autenticación falla y vuelve a la pantalla de usuario por primera vez cuando el certificado tiene varios nombres alternativos de sujeto. [CXM-61933]

Problemas conocidos en la versión 19.1.5

- En Secure Hub para Android, cuando actualiza la contraseña debido a un cambio en la directiva de contraseña, las aplicaciones con insignia no aparecen en los dispositivos Samsung Galaxy S8. [CXM-61177]

- En Secure Hub para Android, la directiva “Archivos” para Android Enterprise no se implementa en dispositivos que estén en el modo de perfil de trabajo. [CXM-61196]

Problemas resueltos en la versión 19.1.5

- En Secure Hub para Android, cuando los usuarios inician sesión con PIN Secure, se establece un túnel VPN, pero Secure Web no carga ningún sitio web. Sin embargo, el sitio web se carga como se esperaba cuando Secure Web se cierra y se vuelve a abrir. [CXM-58576]
- En Secure Hub para Android, cuando inicia sesión con PIN Secure, se establece un túnel VPN, pero Secure Web no carga ningún sitio web. Sin embargo, el sitio web se carga como se esperaba cuando Secure Web se cierra y se vuelve a abrir. [CXM-60751]
- En Secure Hub para Android, cuando intenta capturar registros de la aplicación interna llamada TechXpert, Secure Hub se reinicia y pide que se vuelva a autenticar. [CXM-61310]

Problemas conocidos en la versión 19.1.0

Secure Hub para iOS

En Secure Hub para iOS, cuando implementa aplicaciones MDX, web o SaaS, aparecen en la pantalla **Mis aplicaciones**. Cuando toca en **Más**, aparece una ventana emergente con las opciones **Eliminar** y **Cancelar** en el formato de interfaz de usuario anterior. [CXM-60683]

Problemas resueltos en la versión 18.12.0

- En los dispositivos Samsung KNOX inscritos en Android For Work, cuando la directiva de contraseñas está configurada para caducar en uno o dos días, aparece repetidamente el mensaje “Contraseña caducada”. [CXM-59250]
- No se puede inscribir dispositivos OnePlus 5T para Android Enterprise utilizando el método de inscripción por código QR. [CXM-59288]

Problemas resueltos en la versión 18.11.0

Secure Hub para iOS

- No se puede realizar el inicio de sesión único (SSO) en dispositivos Android inscritos en el modo Dispositivo compartido. Aparece el siguiente error: Sus credenciales de empresa no se pueden obtener en este momento. El inicio de sesión manual en ShareFile está bloqueado por directiva administrativa. [CXM-58238]
- No pueden modificar los niveles de volumen de Android en dispositivos de uso único (COSU) de propiedad de la empresa. [CXM-58323]

Problemas resueltos en la versión 18.10.5

- Si tiene el modo FIPS habilitado en XenMobile Server, después de que los usuarios actualicen Secure Hub para iOS a la versión 18.10.5, aparecerá un mensaje de error relacionado con el cifrado cuando los usuarios abran las aplicaciones. Para actualizaciones de estado en la resolución, consulte este artículo de Citrix Knowledge Center. [CXM-56454]

Problemas resueltos de la versión 10.8.25 a 18.10.6

- Las versiones de Secure Hub de 10.8.25 a 18.10.6 (Android) no contienen problemas conocidos. Se han resuelto los siguientes problemas en Secure Hub. La lista incluye problemas con MDX que afectan a Secure Hub.

Problemas resueltos en la versión 18.10.0

- Si la directiva mVPN está desactivada en la consola de EMS, Secure Hub muestra una pantalla vacía al intentar abrir las aplicaciones administradas de Intune. [CXM-56033, CXM-56086, CXM-54393, CXM-54823]

Problemas resueltos en la versión 10.8.60

- En los dispositivos Samsung Galaxy Tab Active 2 SM-T395, la acción de seguridad "Borrado completo" falla en Secure Hub para Android cuando los administradores establecen la restricción de desactivar el restablecimiento a los valores de fábrica en XenMobile. [CXM-54452]
- Secure Hub para Android se bloquea durante la inscripción de dispositivos cuando la directiva de VPN está configurada y la aplicación Citrix SSO no está instalada en el dispositivo. La aplicación se desbloquea si hace clic en el botón **Atrás** o la reinicia. [CXM-54627]
- En un entorno de Android Enterprise, Secure Hub para Android se bloquea durante la inscripción en el modo de propietario de dispositivo. [CXM-55008]
- Después de que los usuarios escriban un PIN válido de Secure Hub para iOS, Secure Hub solicita repetidamente el PIN a los usuarios. [CXM-55047]
- En un entorno de Android Enterprise, Secure Hub para Android se bloquea durante la inscripción en el modo de propietario de perfil. [CXM-55076]
- Usar Android Enterprise en Secure Hub para Android implica que se instala Google Chrome de forma predeterminada. [CXM-55232]
- Si Secure Hub para iOS se actualiza a la versión 10.8.55, no se permiten inscripciones de dispositivos iOS nuevos o existentes. [CXM-55267]

Problemas resueltos en la versión 10.8.55

- Los usuarios no pueden iniciar sesión en Secure Hub para inscribirse en las cuentas de Android for Work cuando las credenciales de G Suite difieren de las credenciales de Endpoint Management. [CXM-53956]

Problemas relacionados con MDX resueltos en la versión 10.8.55

- Las aplicaciones de empresa pueden experimentar problemas de conectividad a los recursos internos cuando el modo de VPN preferido está configurado en Secure Browse (Exploración segura). [CXM-52309]
- Las aplicaciones que tienen como clase android.support.multidex.MultiDexApplication o android.app.Application no pueden conectarse a redes internas en el modo Exploración segura. [CXM-53126]
- En los dispositivos Android, se generan varios certificados y los certificados se revocan antes de su fecha de caducidad. [CXM-53428]

Problemas conocidos en la versión 10.8.55

- Después de quitar la cuenta de Secure Hub del dispositivo, se produce un error en la reinscripción de la administración de dispositivos móviles MDM. [CXM-54142]

Problema conocido en la versión 10.8.50

- En Secure Hub para Android, los usuarios no pueden agregar un acceso directo de enlace Web. [XMHELP-952]

Problemas resueltos en la versión 10.8.35

- En Android O, los accesos directos creados por las directivas no aparecen en la pantalla de inicio del dispositivo. Este comportamiento se da por razones de diseño en Android O. [CXM-35460]
- Después de un período de inactividad, Secure Hub no se abre en las tabletas Samsung con Android. [CXM-50797]
- En Secure Hub para Android, no se puede implementar la directiva de envío push en dispositivos Samsung KNOX. [CXM-50869]
- En Secure Hub para iOS, ocurre a veces el siguiente problema: después de que los usuarios cambien su contraseña de Active Directory, deben seguir escribiendo su PIN en bucle. [CXM-50224]

Problemas resueltos en la versión 10.8.25

- Para las aplicaciones iOS Cordova de terceros que se empaquetaron con la versión 10.7.20 del MDX Toolkit, después de habilitar la directiva **Oscurecer contenido de pantalla**, aparece una pantalla en negro en los dispositivos iOS, en lugar de una pantalla para el PIN. [CXM-48471]
- En los dispositivos Zebra T51 con Android 7, los usuarios no pueden instalar la aplicación Citrix Launcher. [CXM-50621]

Problemas resueltos en la versión 10.8.20

- Después de que los usuarios actualicen sus dispositivos Android a la versión 8 (Oreo), no pueden instalar aplicaciones empresariales o .apk desde la tienda de aplicaciones que implemente desde Endpoint Management. El problema persiste incluso aunque los usuarios permitan la instalación de aplicaciones de terceros. El problema no está limitado a los dispositivos Samsung. [CXM-50401]

Problemas resueltos en la versión 10.8.15

- Secure Hub para Android se bloquea mientras intenta obtener datos de la ubicación en dispositivos con Android O. [CXM-47893]

Problemas resueltos en la versión 10.8.10

- En dispositivos Android, cuando varias aplicaciones no se instalan automáticamente o los usuarios no hacen clic en **Instalar**, las aplicaciones se siguen descargando. Como resultado, el uso de datos aumenta. [CXM-46404]
- En dispositivos con Android 7 o posterior: cuando envía la acción de seguridad de bloqueo con una contraseña al dispositivo desde XenMobile Server, el dispositivo se bloquea. Sin embargo, la contraseña del dispositivo no cambia si los usuarios tienen una contraseña para la pantalla de bloqueo. Los usuarios pueden usar el código de acceso original para desbloquear el dispositivo. [CXM-47908]

Actualización de Secure Hub para iOS del 19 de marzo de 2018: Secure Hub 10.8.6 para iOS soluciona un problema con la directiva de aplicación VPP. Para obtener más información, consulte este artículo de Citrix Knowledge Center.

Situaciones de petición de credenciales

April 29, 2019

Hay varios casos en los que se solicita a los usuarios que se autentiquen en Secure Hub escribiendo sus credenciales en los dispositivos.

Las situaciones cambian según los siguientes factores:

- La configuración de propiedades de cliente y directivas de aplicaciones MDX en la consola de Endpoint Management.
- Si la autenticación se realiza sin conexión, o si es necesario autenticarse con conexión (el dispositivo necesita una conexión de red a Endpoint Management).

Además, el tipo de credenciales que los usuarios escriben (contraseña de Active Directory, PIN o código de acceso de Citrix, contraseña de un solo uso, autenticación con huella dactilar o Touch ID en iOS) también cambia según el tipo de autenticación y la frecuencia de autenticación que se necesiten.

Veamos las situaciones que provocan una petición de credenciales.

- **Reinicio de dispositivo:** Cuando los usuarios reinician sus dispositivos, deben volver a autenticarse en Secure Hub.
- **Inactividad sin conexión (tiempo de espera):** Con la directiva MDX "Código de acceso de aplicación" habilitada (lo está de forma predeterminada), la propiedad de cliente de Endpoint Management denominada "Inactivity Timer" (Temporizador de inactividad) entra en vigor. El temporizador de inactividad de la propiedad Inactivity Timer limita cuánto tiempo puede pasar sin actividad del usuario en cualquiera de las aplicaciones que usan el contenedor seguro.

Cuando el temporizador de inactividad expira, los usuarios tienen que volver a autenticarse en el contenedor seguro en el dispositivo. Si, por ejemplo, los usuarios dejan su dispositivo en algún lugar y se alejan, si el temporizador de inactividad ha expirado, otra persona no podrá tomar el dispositivo y acceder a los datos confidenciales del contenedor. La propiedad de cliente Inactivity Timer se define en la consola de Endpoint Management. El valor predeterminado es de 15 minutos. La directiva "Código de acceso de aplicación" con el valor **Sí** y la propiedad de cliente "Inactivity Timer" son las responsables de los casos más comunes de petición de credenciales.

- **Cierre de sesión en Secure Hub**. Cuando los usuarios cierran sesión en Secure Hub, tienen que autenticarse de nuevo la próxima vez que accedan a Secure Hub o cualquiera de las aplicaciones MDX, cuando la aplicación requiere un código de acceso según lo determinen la directiva MDX "Código de acceso de aplicación" y el estado del temporizador de inactividad.
- **Periodo máximo sin conexión:** Esta situación es específica de ciertas aplicaciones individuales porque está condicionada por una directiva MDX específica de cada aplicación. La directiva MDX

"Periodo máximo sin conexión" tiene un valor predeterminado de 3 días. Si se agota el período de tiempo definido en Secure Hub para ejecutar una aplicación sin autenticarse en línea, debe conectarse a Endpoint Management para confirmar que tiene derecho a usar la aplicación y para actualizar las directivas. Cuando esta conexión tiene lugar, la aplicación provoca la autenticación en línea en Secure Hub. Los usuarios deben volver a autenticarse para poder acceder a la aplicación MDX.

Tenga en cuenta esta relación entre la directiva "Periodo máximo sin conexión" y la directiva MDX "Periodo de sondeo activo":

- El período de sondeo activo es el intervalo durante el cual las aplicaciones se conectan a Endpoint Management para realizar acciones de seguridad, tales como el bloqueo y el borrado de aplicaciones. Además, la aplicación también comprueba si hay directivas de aplicación actualizadas.
- Después de la comprobación correcta de directivas mediante la directiva "Periodo de sondeo activo", el temporizador del período máximo sin conexión se restablece y comienza de nuevo la cuenta atrás.

Ambas conexiones con Endpoint Management, para la caducidad del periodo de sondeo activo y del periodo máximo sin conexión, requieren un token válido de Citrix Gateway en el dispositivo. Si el dispositivo tiene un token válido de Citrix Gateway, la aplicación obtiene las nuevas directivas desde Endpoint Management sin interrupciones a los usuarios. Si la aplicación necesita un token de Citrix Gateway, se produce un cambio a Secure Hub, y los usuarios ven una solicitud de autenticación en Secure Hub.

En los dispositivos Android, las pantallas de actividad de Secure Hub se abren directamente en la parte superior de la pantalla actual de la aplicación. En dispositivos iOS, no obstante, Secure Hub debe ponerse primero en el primer plano, lo que desplaza temporalmente la aplicación actual.

Después de que los usuarios introduzcan sus credenciales, Secure Hub vuelve a la aplicación original. En este caso, si permite guardar en caché las credenciales de Active Directory o si tiene configurado un certificado de cliente, los usuarios pueden introducir un PIN, una contraseña o proporcionar su huella digital. Si no ha permitido la caché de credenciales, los usuarios deben introducir sus credenciales de Active Directory completas.

El token de Citrix ADC puede dejar de ser válido debido a la inactividad en la sesión de Citrix Gateway o a alguna directiva de tiempo de espera de sesión, según se explica en la siguiente lista de directivas de Citrix Gateway. Cuando los usuarios vuelvan a iniciar sesión en Secure Hub, podrán continuar ejecutando la aplicación.

- **Directivas de sesión de Citrix Gateway:** Hay dos directivas de Citrix Gateway que también afectan cuándo se les pide a los usuarios que se autentiquen. En estos casos, se autentican para crear una sesión en línea con Citrix ADC para conectarse a Endpoint Management.
  - **Tiempo de espera de sesión:** La sesión de Citrix ADC para Endpoint Management se de-

sconecta si no se produce ninguna actividad de sesión durante el periodo definido. El valor predeterminado es de 30 minutos Sin embargo, si utiliza el asistente de Citrix Gateway para configurar la directiva, el valor predeterminado es de 1440 minutos. Los usuarios, a continuación, ven un diálogo de autenticación para volver a conectarse a la red de la empresa.

- **Tiempo de espera forzado:** Si esta directiva está **activada**, la sesión de Citrix ADC para Endpoint Management se desconecta una vez transcurrido el periodo de tiempo de espera forzado. La desconexión forzada hace obligatoria la reautenticación después de un periodo de tiempo determinado. Los usuarios ven un diálogo de autenticación para volver a conectarse a la red de la empresa la próxima vez. El valor predeterminado es **No**. Sin embargo, si utiliza el asistente de Citrix Gateway para configurar la directiva, el valor predeterminado es de 1440 minutos.

Tipos de credenciales

En la sección anterior, se ha descrito cuándo se solicita a los usuarios que se autentiquen. En esta sección, se describen los tipos de credenciales que deben introducir. La autenticación es necesaria mediante varios métodos, para poder obtener acceso a datos cifrados en el dispositivo. Para desbloquear inicialmente el dispositivo, desbloquee el *contenedor principal*. Después de ello y cuando el contenedor esté de nuevo protegido, para obtener acceso nuevamente, desbloquee un *contenedor secundario*.

> Nota:
>
> El término *aplicación administrada* del artículo hace referencia a una aplicación empaquetada con el MDX Toolkit, donde se ha dejado la directiva MDX "Código de acceso de aplicación" habilitada de forma predeterminada y se está usando la propiedad de cliente Inactivity Timer (Temporizador de inactividad).

Las circunstancias que determinan los tipos de credenciales son las siguientes:

- **Desbloqueo de contenedor principal:** Para desbloquear el contenedor principal, se necesita contraseña de Active Directory, PIN o código de acceso de Citrix, contraseña de uso único, Touch ID o ID de huella digital.
  - En iOS, cuando los usuarios abren Secure Hub o una aplicación administrada por primera vez después de instalarla en el dispositivo.
  - En iOS, cuando los usuarios reinician un dispositivo y, a continuación, abren Secure Hub.
  - En Android, cuando los usuarios abren una aplicación administrada si Secure Hub no se está ejecutando.
  - En Android, cuando los usuarios reinician Secure Hub por cualquier motivo, incluido un reinicio del dispositivo.

- **Desbloqueo de contenedor secundario:** Para desbloquear el contenedor secundario, se necesita la autenticación por huella digital (si se ha configurado) un código de acceso o PIN de Citrix o las credenciales de Active Directory.
  - Cuando los usuarios abren una aplicación administrada después de expirar el temporizador de inactividad.
  - Cuando los usuarios cierran sesión en Secure Hub y después abren una aplicación administrada.

Se requieren credenciales de Active Directory para cualquiera de las circunstancias de desbloqueo de contenedor cuando se cumplen las siguientes condiciones:

- Cuando los usuarios cambian la contraseña asociada a su cuenta de empresa.
- Si no ha configurado las propiedades de cliente en la consola de Endpoint Management para habilitar el PIN de Citrix: ENABLE_PASSCODE_AUTH y ENABLE_PASSWORD_CACHING.
- Cuando finaliza la sesión de NetScaler Gateway, lo que ocurre cuando se agota el tiempo de espera de la sesión o caduca el temporizador del tiempo de espera de desconexión forzosa, si el dispositivo no guarda en caché las credenciales o no tiene un certificado de cliente.

Cuando la autenticación con huella digital está habilitada, los usuarios pueden iniciar sesión con una huella digital cuando se requiere la autenticación sin conexión debido a la inactividad de una aplicación. Los usuarios aún tendrán que introducir el PIN cuando inicien sesión en Secure Hub por primera vez o cuando reinicien el dispositivo. Para obtener información sobre cómo habilitar la autenticación por huella digital, consulte Autenticación por huella digital o Touch ID.

El siguiente gráfico resume el flujo de decisiones que determina qué credenciales debe introducir un usuario cuando se le pide una autenticación.

Si cambia de la pantalla de Secure Hub

Otra situación a tener en cuenta es cuando se necesita cambiar de una aplicación a Secure Hub y luego de vuelta a la aplicación. El cambio muestra una notificación que los usuarios deben confirmar. Cuando esto ocurre, no se necesita autenticación. La situación se produce cuando se establece una conexión con Endpoint Management, según se especifica en las directivas MDX “Periodo máximo sin conexión” y “Periodo de sondeo activo”, y Endpoint Management detecta que hay directivas actualizadas que es necesario enviar al dispositivo a través de Secure Hub.

Instalar VPN en iOS

March 8, 2019

En dispositivos iOS 10 y versiones posteriores, se utiliza la red privada virtual (VPN) de Secure Hub para proteger los datos locales que se comparten entre Secure Hub y las aplicaciones MDX. La VPN de Secure Hub se ejecuta en dispositivos iOS 10 y versiones posteriores. Secure Hub VPN ofrece una experiencia de usuario mejor porque Secure Hub y las aplicaciones MDX se pueden comunicar de forma fluida a través de la VPN.

La red privada virtual de Secure Hub funciona para aplicaciones firmadas por certificados de cuenta de desarrollador de Apple Enterprise ("ID de equipo"), certificados de Citrix, certificados de empresa o certificados de proveedores de software independientes (ISV) externos.

La red privada virtual de Secure Hub se utiliza de forma predeterminada en los dispositivos iOS 10. Si la red privada virtual de Secure Hub no se está ejecutando en el dispositivo iOS 10, MDX usa el llavero compartido de iOS para proteger el uso compartido de datos. El mecanismo de llavero compartido de iOS requiere que todas las aplicaciones participantes estén firmadas por el mismo certificado para poder acceder al llavero compartido específico de ese certificado de "ID de equipo" de iOS. Si una aplicación no está firmada con el mismo certificado que la aplicación de Secure Hub firmada por Citrix, es posible que la aplicación acuda a Secure Hub para obtener la información necesaria.

La VPN de Secure Hub solo está disponible para las implementaciones MAM y Enterprise de Endpoint Management. La VPN de Secure Hub no se aplica a entornos solo MDM de Endpoint Management, por lo que no se instala durante inscripciones en modo solo MDM.

La VPN de Secure Hub se utiliza para la comunicación entre Secure Hub y las aplicaciones móviles de productividad. No filtra ni supervisa el tráfico de red en el dispositivo y es independiente del mecanismo de micro VPN de MDX.

> Nota:
>
> Citrix recomienda dejar la VPN de Secure Hub habilitada en entornos donde está habilitada de forma predeterminada.
>
> iOS no permite ejecutar más de un cliente VPN al mismo tiempo en el dispositivo iOS. Por lo tanto, tenga en cuenta la situación siguiente. La VPN de Secure Hub no se puede usar si es necesario ejecutar otra aplicación de VPN (como Cisco AnyConnect o Citrix VPN) en dispositivos iOS para poder establecer una VPN de nivel de dispositivo. Puede configurar una VPN por aplicación de iOS incluso aunque la VPN de Secure Hub no esté inhabilitada. La aplicación que utiliza la VPN por aplicación de iOS establece una conexión de VPN por aplicación cuando está en primer plano.
>
> Para inhabilitar la VPN de Secure Hub, consulte la sección siguiente en este artículo. Si la VPN de Secure Hub está inhabilitada, es posible que los usuarios experimenten más "cambios" de una aplicación administrada a Secure Hub.

Inhabilitar o rehabilitar la VPN de Secure Hub en Endpoint Management

De forma predeterminada, la red privada virtual de Secure Hub se habilita cuando los usuarios empiezan a utilizar Secure Hub 10.3.10 o una versión posterior en iOS 10.

Para inhabilitar la red privada virtual de Secure Hub y establecer que los dispositivos iOS de la implementación utilicen el mecanismo de llavero compartido, lleve a cabo lo siguiente:

1. En la consola de Endpoint Management, vaya a **Parámetros > Cliente > Propiedades de cliente**.
2. En la página **Propiedades de cliente**, cree una propiedad de cliente personalizada llamada **ENABLE_NETWORK_EXTENSION** y déle el valor 0.

   Para volver a habilitar la red privada virtual (VPN) de Secure Hub, vaya a la VPN de Secure Hub y establezca el valor de la propiedad **ENABLE_NETWORK_EXTENSION** en 1.

Instalar la VPN de Secure Hub en el dispositivo cliente

La red privada virtual de Secure Hub se instala en dos casos: después de instalar Secure Hub 10.3.10 o posterior en un dispositivo iOS 10, o bien cuando un usuario actualiza a iOS 10 un dispositivo que ya ejecuta Secure Hub 10.3.10 o posterior.

Los usuarios verán este mensaje informativo.

A continuación, los usuarios verán un mensaje de iOS donde se pide permiso para agregar configuraciones de VPN. Este mensaje aparece solo una vez, cuando la red privada virtual (VPN) se instala por primera vez. No aparece cuando los usuarios vuelven a abrir Secure Hub.

El mensaje de esta pantalla no se puede personalizar. Es un diálogo estándar de iOS utilizado para todas las instalaciones de VPN.

Si el usuario selecciona **No Permitir** en la pantalla que pide permiso para agregar la configuración de VPN, verá otro mensaje donde se indica que debe instalar la VPN para poder acceder a Secure Hub.

Ejecutar la VPN de Secure Hub en el dispositivo cliente

Cuando la VPN de Secure Hub se está ejecutando correctamente, aparece el texto **Conectando…** en la pantalla **General > VPN** en Ajustes de iOS.

Este es el comportamiento esperado y no significa que los mecanismos de uso compartido y comunicación de MDX no funcionen. No se requiere ninguna acción por parte de los usuarios si ven este mensaje.

Inscribir dispositivos mediante credenciales derivadas

March 8, 2019

Las credenciales derivadas ofrecen una autenticación sólida para dispositivos móviles. Las credenciales, obtenidas de una tarjeta inteligente, residen en el dispositivo móvil, en lugar de la tarjeta. La tarjeta inteligente es una tarjeta Personal Identity Verification (PIV) o Common Access Card (CAC).

Las credenciales derivadas son un certificado de inscripción que contiene un identificador de usuario como, por ejemplo, su nombre principal o UPN. Endpoint Management almacena las credenciales obtenidas del proveedor de credenciales en un almacén seguro del dispositivo.

Endpoint Management puede utilizar credenciales derivadas para inscribir dispositivos iOS. Si se configura para las credenciales derivadas, Endpoint Management no admitirá invitaciones de inscripción u otros modos de inscripción para dispositivos iOS. No obstante, puede usar el mismo servidor Endpoint Management para inscribir dispositivos Android mediante invitaciones de inscripción u otros modos de inscripción.

Pasos de inscripción de dispositivos cuando se utilizan credenciales derivadas

La inscripción requiere que los usuarios introduzcan su tarjeta inteligente en un lector conectado a su escritorio.

1. El usuario instala Secure Hub y la aplicación desde el proveedor de credenciales derivadas. En este ejemplo, la aplicación del proveedor de identidad es Intercede MyID Identity Agent.
2. El usuario inicia Secure Hub. Cuando se le solicite, el usuario escribe el nombre de dominio completo (FQDN) de Endpoint Management y, a continuación, hace clic en **Siguiente**. Comienza la inscripción en Secure Hub. Si Endpoint Management admite credenciales derivadas, Secure Hub pide al usuario que cree un PIN de Citrix.
3. El usuario sigue las instrucciones para activar sus credenciales inteligentes. Aparecerá una pantalla de bienvenida, seguida de una solicitud para escanear un código QR.
4. El usuario introduce su tarjeta en el lector de tarjetas inteligentes que está conectado a su escritorio. La aplicación de escritorio muestra un código QR y pide al usuario que escanee el código usando su dispositivo móvil.

   El usuario introduce su PIN de Secure Hub cuando se le solicite.

Después de autenticar el PIN, Secure Hub descarga los certificados. El usuario sigue las indicaciones para completar la inscripción.

Para ver información de dispositivos en la consola de Endpoint Management, lleve a cabo una de estas acciones:

- Vaya a **Administrar > Dispositivos** y, a continuación, seleccione un dispositivo para ver un cuadro de comandos. Haga clic en **Mostrar más**.
- Vaya a **Analizar > Panel de mandos**.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States