citrix

Secure Hub

Contents

Citrix Secure Hub

July 18, 2022

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 al almacén de aplicaciones. Desde el almacén, 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.

Para obtener la información más reciente sobre las aplicaciones móviles de productividad, consulte Anuncios recientes.

En las siguientes secciones se indican las nuevas funciones de la versión actual y las versiones anteriores de Secure Hub.

> **Nota:**
>
> En junio de 2020, dejaron de admitirse las versiones de Android 6.x y iOS 11.x de Secure Hub, Secure Mail, Secure Web y la aplicación Citrix Workspace.

Novedades en la versión actual

Secure Hub 22.6.0

Secure Hub para Android

Esta versión incluye correcciones de errores.

Novedades en versiones anteriores

Secure Hub 22.5.0

Secure Hub para iOS

Esta versión incluye correcciones de errores.

Secure Hub 22.4.0

Secure Hub para Android

Esta versión incluye correcciones de errores.

Secure Hub 22.2.0

Secure Hub para iOS

Esta versión incluye correcciones de errores.

Secure Hub para Android

Esta versión incluye correcciones de errores.

Secure Hub 21.11.0

Secure Hub para Android

Compatibilidad con perfiles de trabajo para dispositivos propiedad de la empresa

Ahora, en dispositivos Android Enterprise, puede inscribir Secure Hub en el modo Perfil de trabajo para dispositivos propiedad de la empresa. Esta función está disponible en dispositivos con Android 11 o versiones posteriores. Los dispositivos previamente inscritos en el modo de propiedad de la empresa con acceso privado (COPE) migran automáticamente al modo Perfil de trabajo para dispositivos propiedad de la empresa cuando el dispositivo se actualiza de Android 10 a Android 11 o a una posterior.

Secure Hub 21.10.0

Secure Hub para iOS

Esta versión incluye correcciones de errores.

Secure Hub para Android

Compatibilidad con Android 12. A partir de esta versión, Secure Hub se admite en dispositivos con Android 12.

Secure Hub 21.8.0

Secure Hub para iOS

Esta versión incluye correcciones de errores.

Secure Hub 21.7.1

Secure Hub para Android

Compatibilidad con Android 12 en dispositivos ya inscritos. Si quiere actualizar el sistema operativo a Android 12, antes debe actualizar Secure Hub a la versión 21.7.1. Secure Hub 21.7.1 es la versión mínima necesaria para actualizar el sistema operativo a Android 12. Esta versión garantiza una actualización sin problemas de Android 11 a Android 12 para los usuarios ya inscritos.

> **Nota:**
>
> Si Secure Hub no se actualiza a la versión 21.7.1 antes de actualizar el sistema operativo a Android 12, es posible que el dispositivo requiera una reinscripción o un restablecimiento a los valores de fábrica para recuperar la funcionalidad anterior.
>
> Citrix se compromete a ofrecer mantenimiento desde el primer día para Android 12 y agregará más actualizaciones a las versiones posteriores de Secure Hub para garantizar la compatibilidad total de Android 12.

Secure Hub 21.7.0

Secure Hub para iOS

Esta versión incluye correcciones de errores.

Secure Hub para Android

Esta versión incluye correcciones de errores.

Secure Hub 21.6.0

Secure Hub para iOS

Esta versión incluye correcciones de errores.

Secure Hub para Android

Esta versión incluye correcciones de errores.

Secure Hub 21.5.1

Secure Hub para iOS

Esta versión incluye correcciones de errores.

Secure Hub para Android

Esta versión incluye correcciones de errores.

Secure Hub 21.5.0

Secure Hub para iOS

Con esta versión, las aplicaciones empaquetadas con la versión 19.8.0 de MDX Toolkit o una anterior ya no funcionarán. Debe empaquetar las aplicaciones con la versión más reciente de MDX Toolkit para volver a disfrutar de la funcionalidad adecuada.

Secure Hub 21.4.0

Nuevos colores para Secure Hub. Secure Hub se adhiere a los nuevos colores de la marca Citrix.

Secure Hub 21.3.2

Secure Hub para iOS

Esta versión incluye correcciones de errores.

Secure Hub 21.3.0

Esta versión incluye correcciones de errores.

Secure Hub 21.2.0

Secure Hub para Android

Esta versión incluye correcciones de errores.

Secure Hub 21.1.0

Secure Hub para iOS

Esta versión incluye correcciones de errores.

Secure Hub para Android

Esta versión incluye correcciones de errores.

Secure Hub 20.12.0

Secure Hub para iOS

Esta versión incluye correcciones de errores.

Secure Hub para Android

Secure Hub para Android admite el modo de arranque directo. Para obtener más información sobre el modo de arranque directo, consulte la documentación de Android en *Developer.android.com.*

Secure Hub 20.11.0

Secure Hub para Android

Secure Hub admite los requisitos actuales de la API de destino de Google Play para Android 10.

Secure Hub 20.10.5

Esta versión incluye correcciones de errores.

Secure Hub 20.9.0

Secure Hub para iOS

Secure Hub para iOS es compatible con iOS 14.

Secure Hub para Android

Esta versión incluye correcciones de errores.

Secure Hub 20.7.5

Secure Hub para Android

- Secure Hub para Android es compatible con Android 11.
- **Transición de Secure Hub de 32 bits a 64 bits para aplicaciones.** En la versión 20.7.5 de Secure Hub, la arquitectura de 32 bits para aplicaciones queda retirada, y Secure Hub se ha actualizado a 64 bits. Citrix recomienda a los clientes que actualicen a la versión 20.7.5 desde 20.6.5. Si los usuarios omiten la actualización de la versión de Secure Hub a 20.6.5 y, en su lugar, actualizan la versión 20.1.5 directamente a 20.7.5, deberán volver a autenticarse. La reautenticación implica introducir credenciales y restablecer el PIN de Secure Hub. La versión 20.6.5 de Secure Hub está disponible en Google Play Store.

- **Instale las actualizaciones desde el App Store.** En Secure Hub para Android, si hay actualizaciones disponibles para las aplicaciones, la aplicación se resalta y la función **Actualizaciones disponibles** aparece en la pantalla del App Store.

  Al tocar **Actualizaciones disponibles**, se le dirige a la tienda, donde se muestra una lista de las aplicaciones con actualizaciones pendientes. Toque **Detalles** en la aplicación para instalar las actualizaciones. Cuando se actualiza la aplicación, la flecha hacia abajo en **Detalles** cambia a una marca de verificación.

Secure Hub 20.6.5

Secure Hub para Android

Transición de 32 bits a 64 bits para aplicaciones. La versión 20.6.5 de Secure Hub es la última que admite una arquitectura de 32 bits para aplicaciones móviles Android. En versiones posteriores, Secure Hub admite la arquitectura de 64 bits. Citrix recomienda a los usuarios actualizar a Secure Hub versión 20.6.5 para que puedan actualizar a versiones posteriores sin necesidad de volver a autenticarse. Si los usuarios omiten la actualización a Secure Hub versión 20.6.5 y, en su lugar, actualizan a 20.7.5 directamente, deberán volver a autenticarse. La reautenticación implica introducir credenciales y restablecer el PIN de Secure Hub.

> **Nota:**
>
> La versión 20.6.5 no bloquea la inscripción de dispositivos que ejecutan Android 10 en modo administrador de dispositivos.

Secure Hub para iOS

Habilitación de un proxy configurado en dispositivos iOS. Secure Hub para iOS requiere habilitar una nueva propiedad de cliente, `ALLOW_CLIENTSIDE_PROXY`, si quiere permitir que los usuarios utilicen servidores proxy que configuran en **Parámetros > Wi-Fi**. Para obtener más información, consulte `ALLOW_CLIENTSIDE_PROXY` en Referencia de propiedades de cliente.

Secure Hub 20.3.0

> **Nota:**
>
> A partir de junio de 2020, no se admiten las versiones de Android 6.x y iOS 11.x de Secure Hub, Secure Mail, Secure Web y la aplicación Citrix Workspace.

Secure Hub para iOS

- **Extensión de red inhabilitada.** Debido a cambios recientes en las directrices de revisión de App Store, a partir de la versión 20.3.0, Secure Hub no admite la extensión de red (NE) en dispositivos con iOS. NE no tiene ningún impacto en las aplicaciones móviles de productividad desarrolladas por Citrix. Sin embargo, la eliminación de NE tiene un cierto impacto en las aplicaciones empaquetadas MDX de empresa implementadas. Los usuarios finales podrían observar cambios en Secure Hub mientras sincronizan componentes como tokens de autorización, temporizadores y reintentos de PIN. Para obtener más información, consulte https://support.citrix.com/article/CTX270296.

> **Nota:**
>
> No se pide a los nuevos usuarios que instalen VPN.

- **Compatibilidad con perfiles de inscripción mejorados.** Secure Hub admite las funciones de perfil de inscripción mejorado anunciadas para Citrix Endpoint Management en Compatibilidad con perfiles de inscripción.

Secure Hub 20.2.0

Secure Hub para iOS

Esta versión incluye correcciones de errores.

Secure Hub 20.1.5

Esta versión incluye:

- Actualización del formato y presentación de la directiva de privacidad del usuario. Esta actualización de funciones cambia el flujo de inscripción de Secure Hub.
- Problemas resueltos.

Secure Hub 19.12.5

Esta versión incluye correcciones de errores.

Secure Hub 19.11.5

Esta versión incluye correcciones de errores.

Secure Hub 19.10.5

Secure Hub para Android

Inscriba Secure Hub en modo COPE. En dispositivos Android Enterprise, inscriba Secure Hub en el modo COPE (propiedad de la empresa con acceso privado) cuando Citrix Endpoint Management esté configurado en el perfil de inscripción COPE.

Secure Hub 19.10.0

Esta versión incluye correcciones de errores.

Secure Hub 19.9.5

Secure Hub para iOS

Esta versión incluye correcciones de errores.

Secure Hub para Android

Compatibilidad con las funciones de Keyguard para los dispositivos de perfil de trabajo y completamente administrados de Android Enterprise. Android Keyguard administra las pantallas de bloqueo del dispositivo y de Work Challenge. Utilice la directiva de dispositivos de administración de Keyguard en Citrix Endpoint Management para controlar la administración de Keyguard en dispositivos de perfil de trabajo y en dispositivos totalmente administrados y dedicados. Con la administración de Keyguard, puede especificar las funciones disponibles para los usuarios, 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.

Para obtener más información acerca de los parámetros de las funciones y cómo configurar la directiva de dispositivos, consulte Directiva de dispositivos de administración de Keyguard.

Secure Hub 19.9.0

Secure Hub para iOS

Secure Hub para iOS es compatible con iOS 13.

Secure Hub para Android

Esta versión incluye correcciones de errores.

Secure Hub para Android 19.8.5

Esta versión incluye correcciones de errores.

Secure Hub 19.8.0

Secure Hub para iOS

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

Secure Hub para Android

Compatibilidad con Android Q. Esta versión incluye compatibilidad con Android Q. Antes de actualizarse a la plataforma Android Q: 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 Q. Consulte también la entrada del blog Citrix Endpoint Management and Android Enterprise - a Season of Change.

Secure Hub 19.7.5

Secure Hub para iOS

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

Secure Hub para Android

Compatibilidad con Samsung Knox SDK 3.x. Secure Hub para Android admite Samsung Knox SDK 3.x. Para obtener más información acerca de la migración a Samsung Knox 3.x, consulte la documentación para desarrolladores de Samsung Knox. Esta versión también admite los nuevos espacios de nombres de Samsung Knox. Para obtener más información acerca de los cambios en los espacios de nombres antiguos de Samsung Knox, consulte Cambios en los espacios de nombres antiguos de Samsung Knox.

> **Nota:**
>
> Secure Hub para Android no admite Samsung Knox 3.x en dispositivos con Android 5.

Secure Hub: De 19.3.5 a 19.6.6

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

Secure Hub 19.3.0

Compatibilidad con 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 sobre esta directiva, consulte Directiva de Wi-Fi.
- **Directiva de XML personalizado.** La directiva de XML personalizado ahora admite Android Enterprise. Para obtener más información sobre esta directiva, consulte Directiva de XML personalizado.
- **Directiva de archivos.** Puede agregar archivos de script en Citrix Endpoint Management para realizar funciones en dispositivos Android Enterprise. Para obtener más información sobre esta directiva, consulte Directiva de archivos.

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 la Directiva de restricciones.

De la versión 18.10.5 a la 18.11.0 de Secure Hub se incluyen 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 How Samsung DeX works.

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.

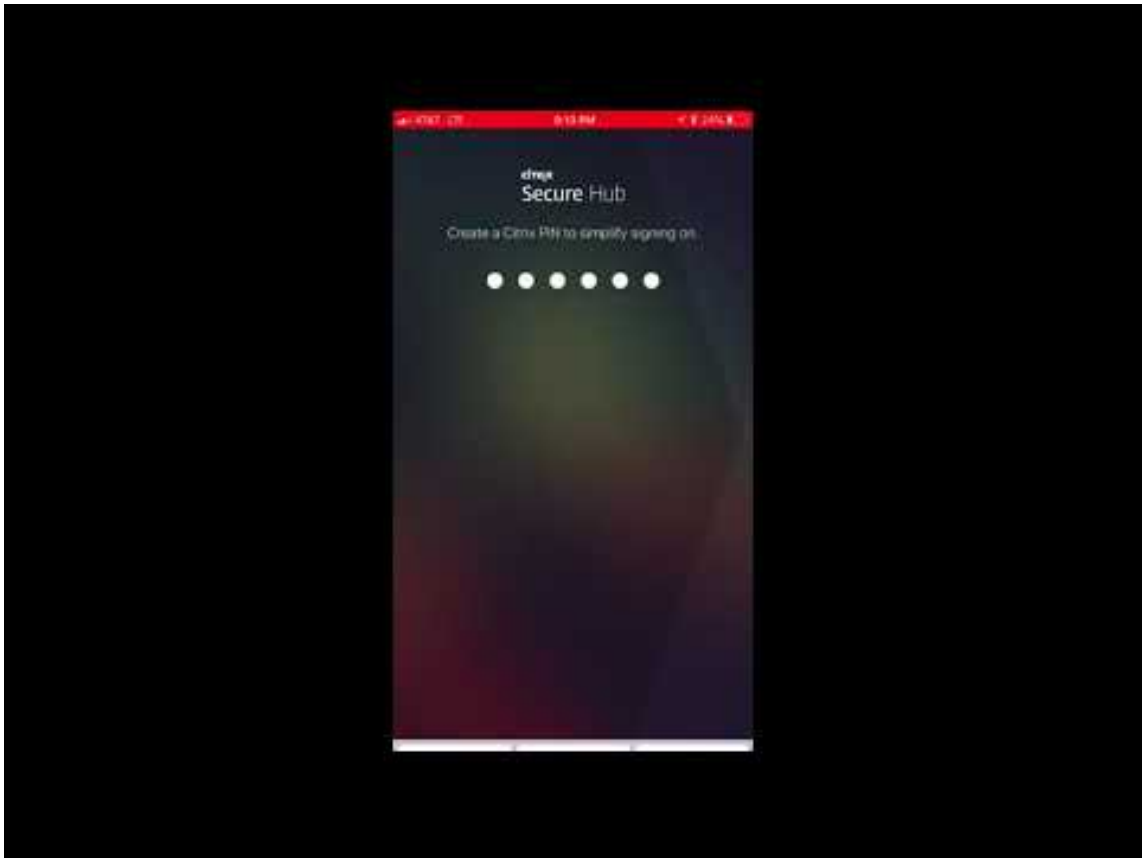
- **Disponibilidad de Android SafetyNet:** Puede configurar Endpoint Management para utilizar la funcionalidad **Android SafetyNet** para evaluar la compatibilidad y la seguridad de los dispositivos Android que tienen Secure Hub instalado. Los resultados se pueden utilizar para desencadenar acciones 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 la Directiva de restricciones.

De Secure Hub 10.8.60 a 18.9.0

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

Secure Hub 10.8.60

- Disponible en polaco.
- Compatibilidad con Android P.
- Se puede usar el almacén de aplicaciones de Workspace.
  Al abrir Secure Hub, los usuarios ya no ven el almacén de Secure Hub. El botón **Agregar aplicaciones** lleva a los usuarios al almacén 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 función, 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 Resumen de directivas MDX para aplicaciones de productividad móvil.
- 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 de dominio o dominio y token de seguridad.
- Habilite la integración de Workspace para Endpoint Management. Para obtener más información sobre la integración de espacios de trabajo, consulte Configurar espacios 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 detalles, consulte Inscripción en bloque de 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 información detallada, consulte la documentación para desarrolladores de Android.

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 información más detallada, consulte este artículo de Citrix Knowledge Center.

Secure Hub 10.8.5: Compatibilidad en Secure Hub para Android con el modo COSU de Android Enterprise (Android for Work). Para obtener más información, consulte la 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 el 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 función 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 por 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 más información, 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 por inactividad. Para obtener información sobre cómo habilitar la autenticación por huella dactilar, consulte Autenticación por huella dactilar o Touch ID.

Fijar certificados

Secure Hub para iOS y Android admite la fijación de certificados SSL. Esta función 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 más información, consulte Administración de dispositivos.
- No es posible establecer contacto con las entidades de certificación privadas o autofirmadas ni el servicio de detección automática (ADS) de Endpoint Management. 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 de Citrix Support y proporcione la información siguiente: No debe enviar la clave privada a 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, que deben ser certificados públicos y no la clave privada.
- Cómo administrar los certificados de servidor existentes: Si quiere quitar el certificado de servidor antiguo inmediatamente (porque no es seguro) o si quiere conservar la compatibilidad con el 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 mediante 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.

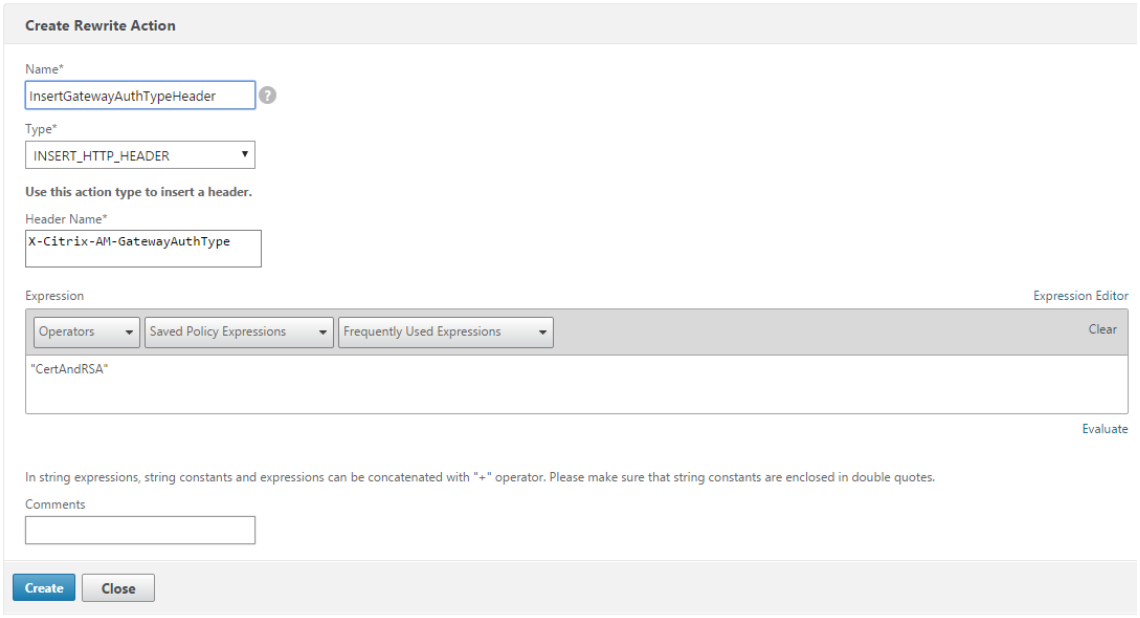
Para que Secure Hub use el tipo de autenticación "certificado + contraseña de un solo uso", agregue una acción de reescritura y una directiva de reescritura en Citrix ADC que inserte un encabezado de respuesta personalizado del formulario **X-Citrix-AM-GatewayAuthType: CertAndRSA** para indicar el tipo 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.

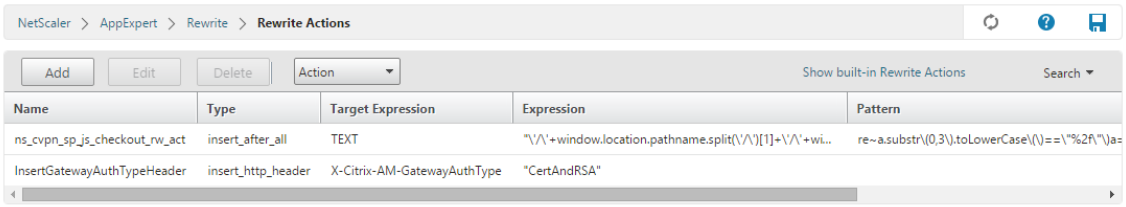
> **Nota:**
>
> Si se definen tipos de inicio de sesión diferentes para Endpoint Management y Citrix ADC, la configuración de Citrix ADC prevalece. Para obtener más información, consulte Citrix Gateway y Endpoint Management.

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

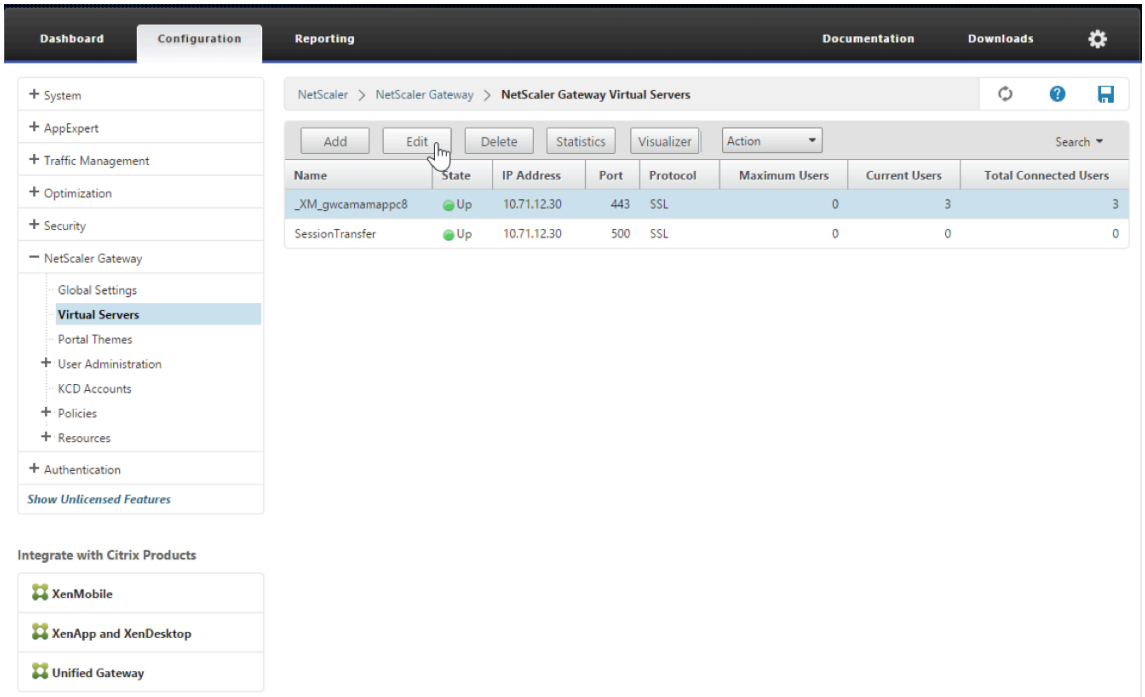
   Aparecerá la pantalla **Create Rewrite Action**.
3. Rellene los campos como se muestra en la siguiente imagen y, a continuación, haga clic en **Create**.



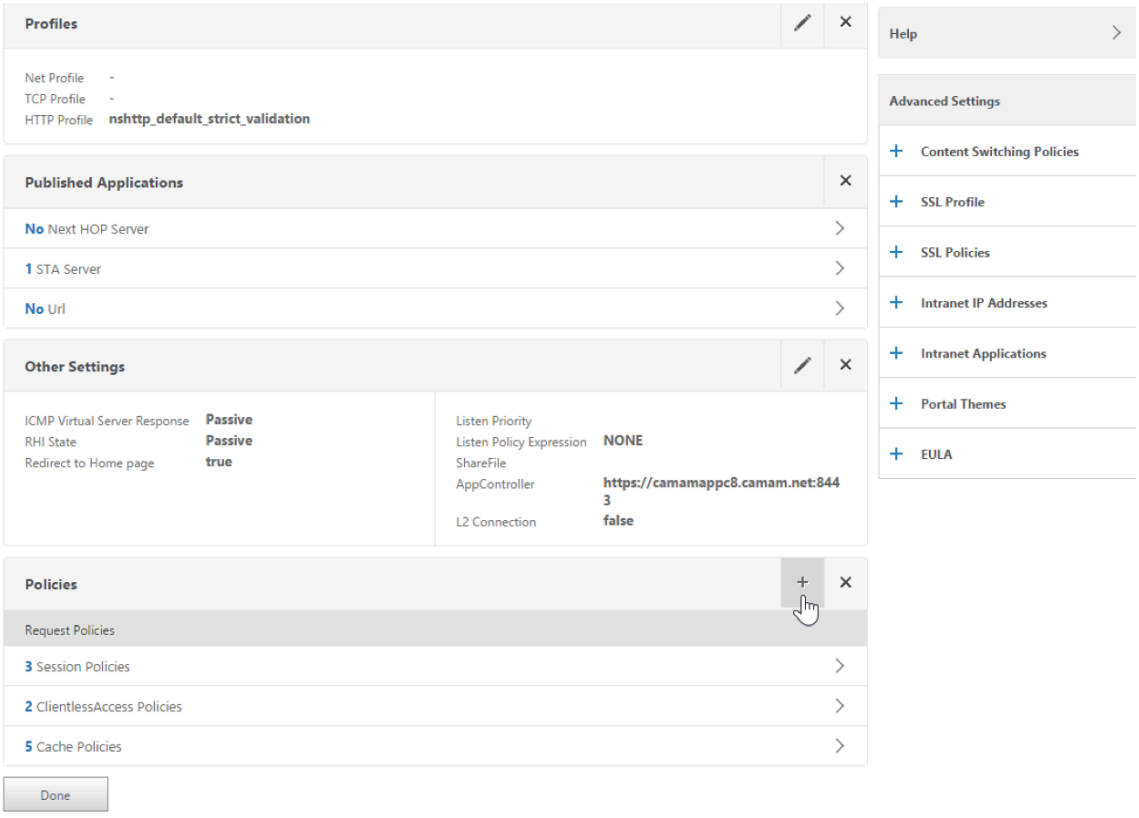
Aparece este resultado en la pantalla principal **Rewrite Actions**.



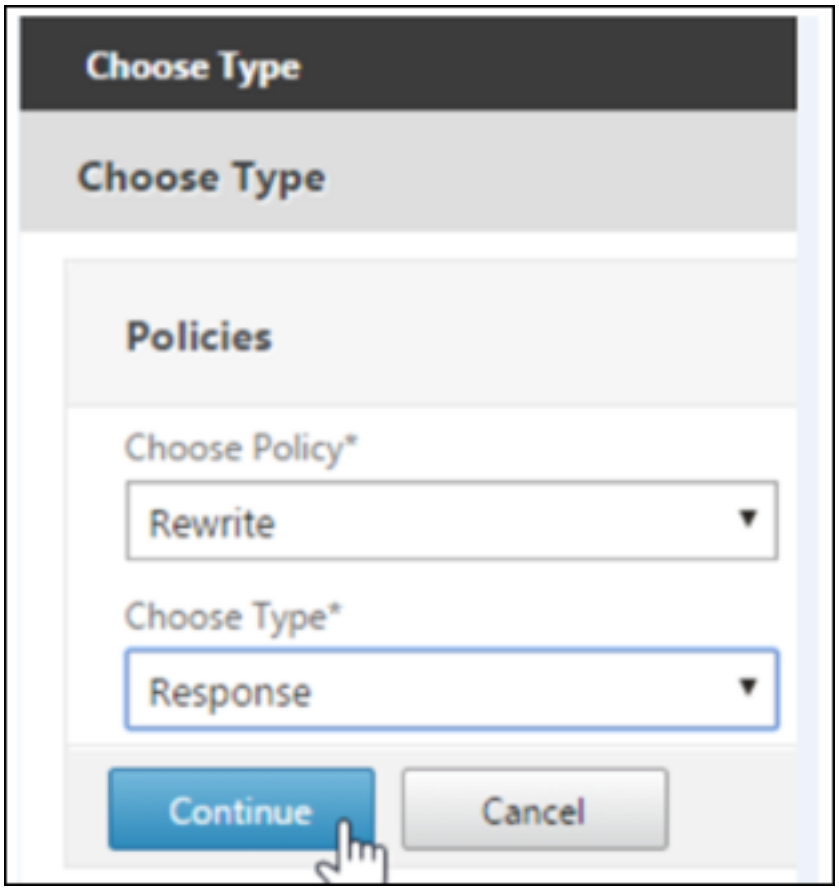
4. Vincule la acción de reescritura al servidor virtual como una directiva de reescritura. Vaya a **Configuration > NetScaler Gateway > Virtual Servers** y seleccione el servidor virtual.



5. Haga clic en **Edit**.
6. En la pantalla **Virtual Servers configuration**, vaya a **Policies**.
7. Haga clic en **+** para agregar una directiva.

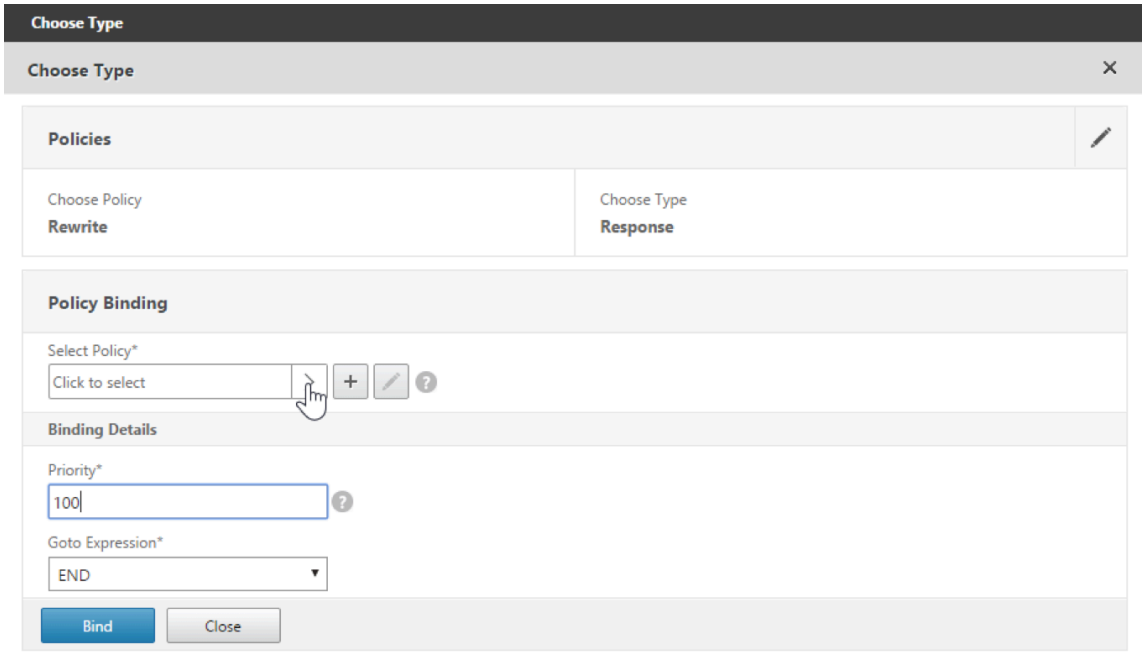


8. En el campo **Choose Policy**, elija **Rewrite**.
9. En el campo **Choose Type**, elija **Response**.



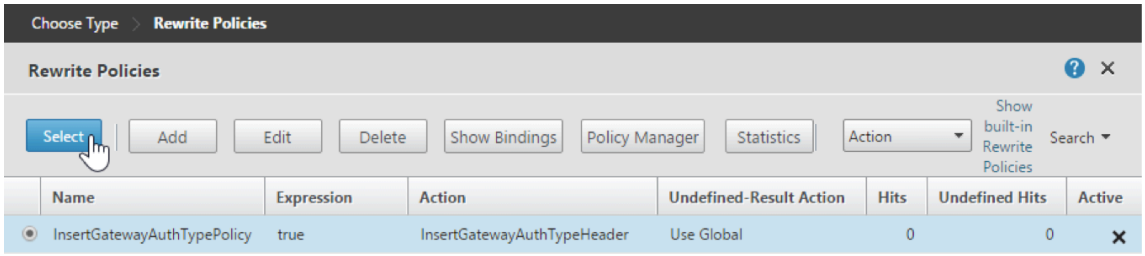
10. Haga clic en **Continue**.

    Se expande la sección **Policy Binding**.

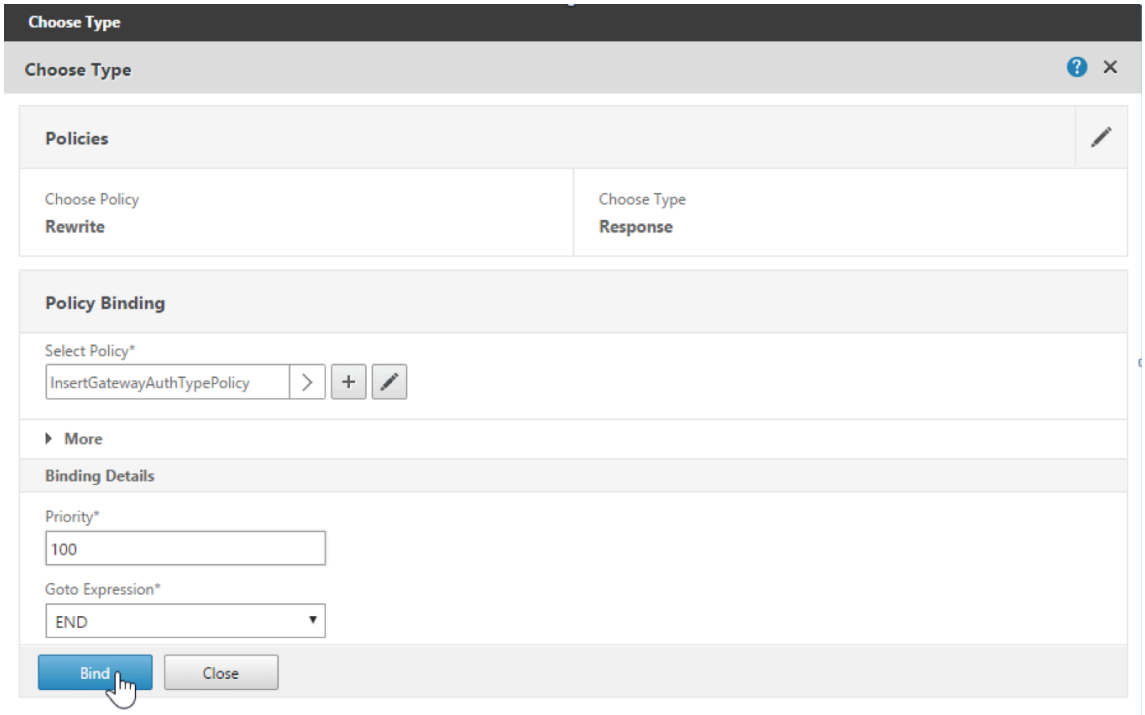


11. Haga clic en **Select Policy**.

    Aparecerá una pantalla con las directivas disponibles.

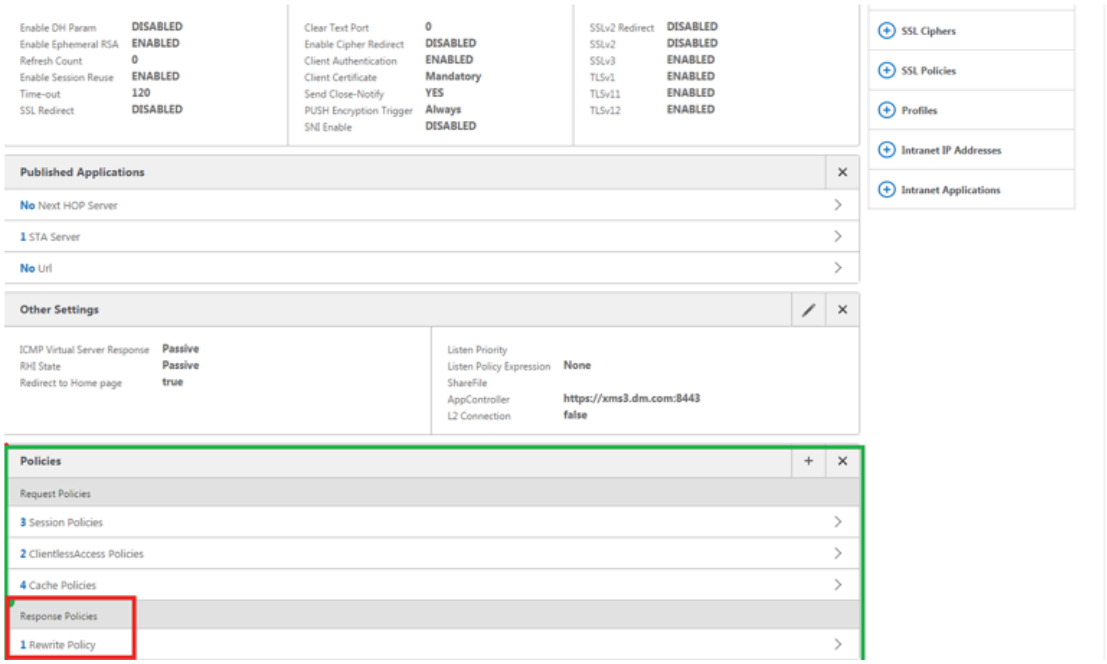


12. Haga clic en la fila de la directiva que acaba de crear y, a continuación, haga clic en **Select**. Aparece de nuevo la pantalla **Policy Binding**, con la directiva seleccionada.

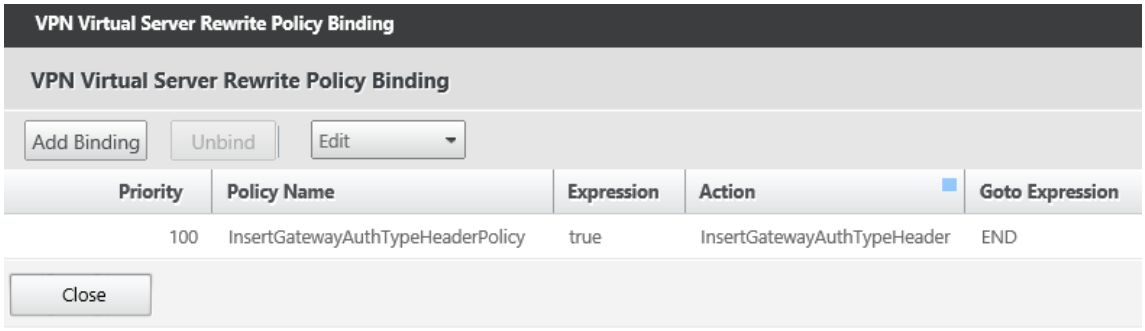


13. Haga clic en **Bind**.

    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 Citrix 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:

FQDN	Dirección IP	Port	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 admite 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.

Inhabilitar la opción Eliminar cuenta

Puede inhabilitar la opción **Eliminar cuenta** de Secure Hub en entornos donde está habilitado el servicio de detección automática Auto Discovery Service (ADS).

Siga estos pasos para inhabilitar la opción **Eliminar cuenta**:

1. Configure ADS para su dominio.
2. Abra **Información sobre el servicio de detección automática** en Citrix Endpoint Management y establezca el valor de `displayReenrollLink` en **False**.
   De manera predeterminada, este valor es **True**.
3. Si el dispositivo está inscrito en el modo MDM+MAM (ENT), cierre la sesión y vuelva a iniciarla para que los cambios entren en vigor.
   Si el dispositivo está inscrito en otros modos, debe reinscribir el dispositivo.

Uso de Secure Hub

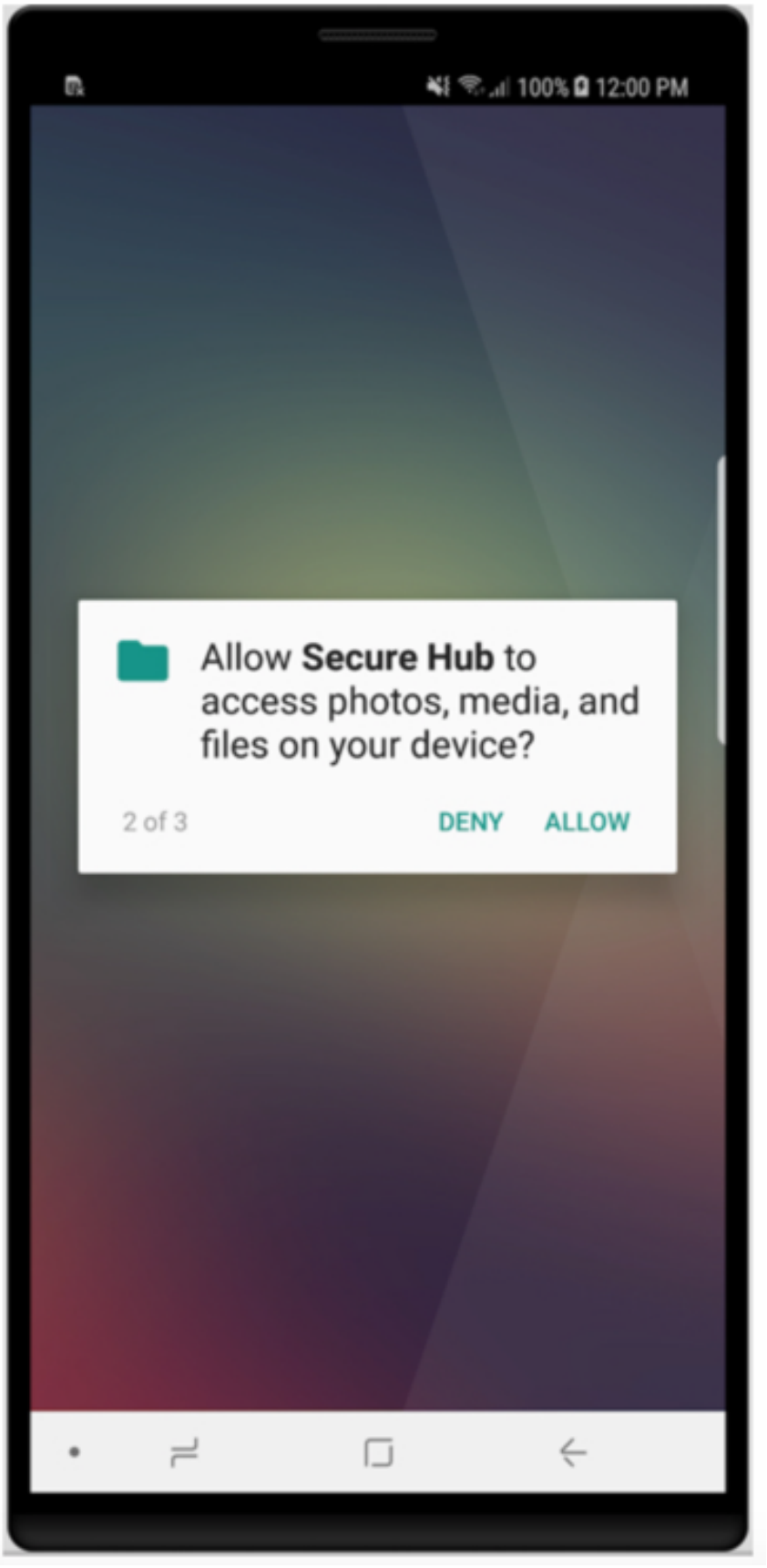
Los usuarios empiezan por descargar Secure Hub en sus dispositivos desde las tiendas de aplicaciones de Apple o Android.

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 detalles sobre la inscripción de dispositivos, consulte Inscripción, roles y cuentas de usuario.

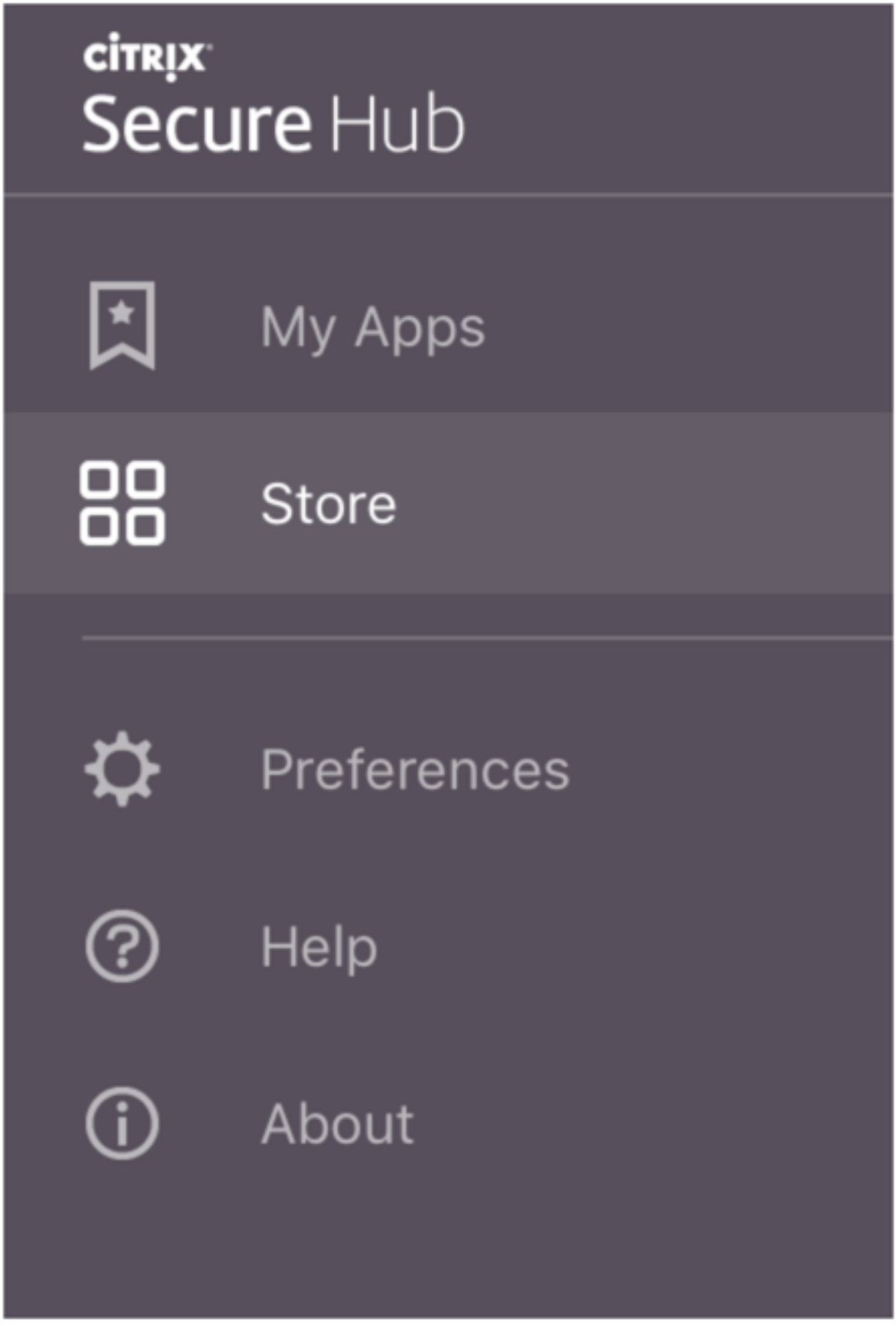
En Secure Hub para Android, durante la instalación inicial y la inscripción, aparece este mensaje: ¿Permitir que Secure Hub acceda a fotos, archivos multimedia y archivos en su dispositivo?

Este mensaje proviene del sistema operativo Android, no de Citrix. Cuando toca **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 iPhone iOS 9 o una versión posterior instalen aplicaciones móviles de productividad desde el almacén, 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.

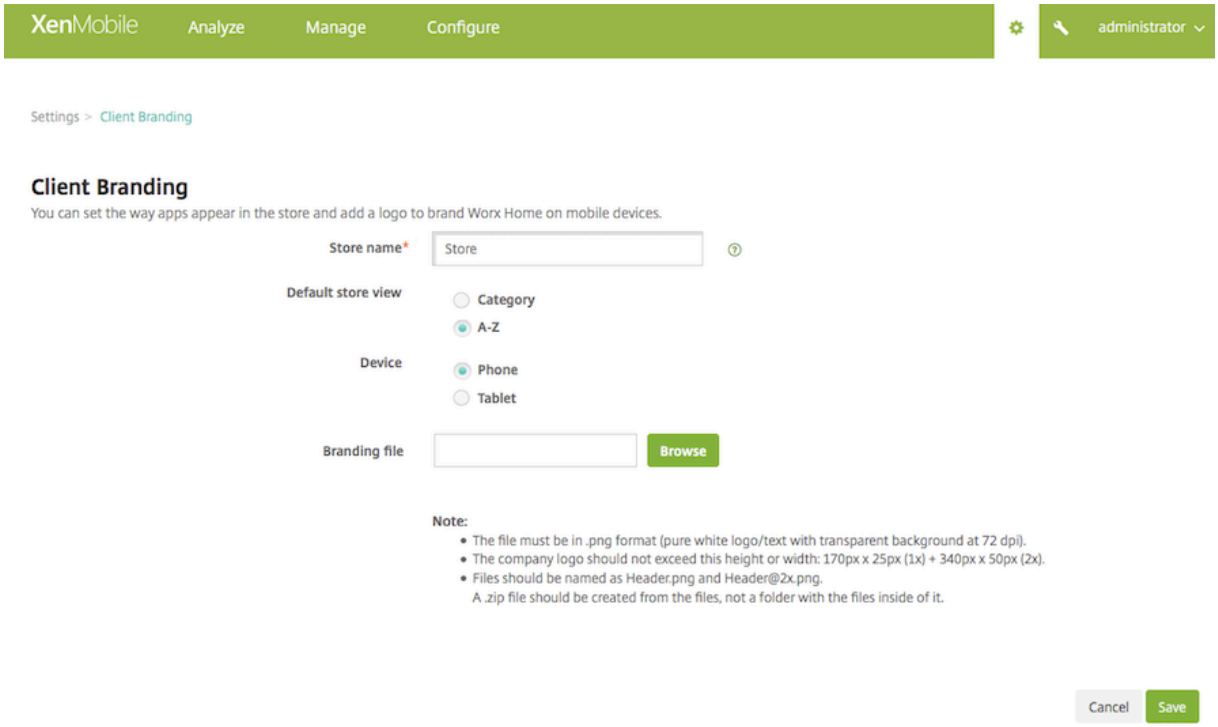
La primera vez que se usa Secure Mail, este obtiene el ID, el dominio y la dirección de correo electrónico del usuario desde Secure Hub. Secure Mail usa la dirección de correo electrónico para la detección automática. El servidor Exchange se identifica con el dominio y el ID del usuario, lo que permite 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 función, cree tres propiedades:

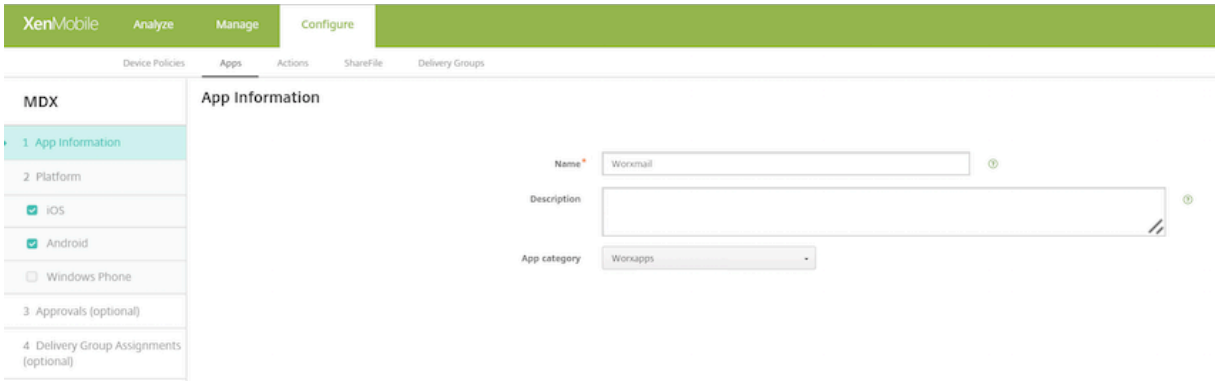
- La propiedad de servidor MAM_MACRO_SUPPORT. Para obtener instrucciones, consulte Propiedades de servidor.
- Las propiedades de cliente ENABLE_CREDENTIAL_STORE y SEND_LDAP_ATTRIBUTES. Para obtener instrucciones, consulte Propiedades de cliente.

Almacén personalizado

Si quiere personalizar el almacén, 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**.

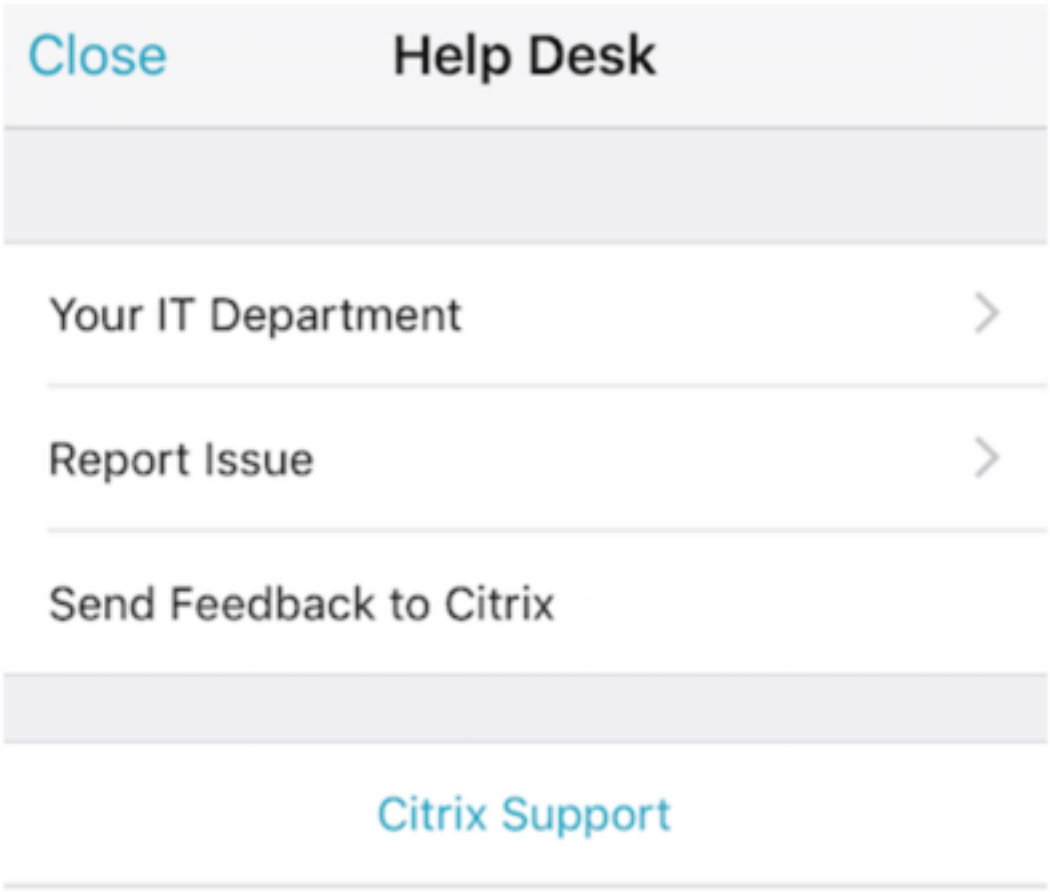


En el almacén de aplicaciones, los usuarios pueden explorar solo las aplicaciones y los escritorios que usted haya configurado y protegido en Endpoint Management. Para agregar la aplicación, los usuarios deben tocar en **Detalles** y, luego, en **Agregar**.

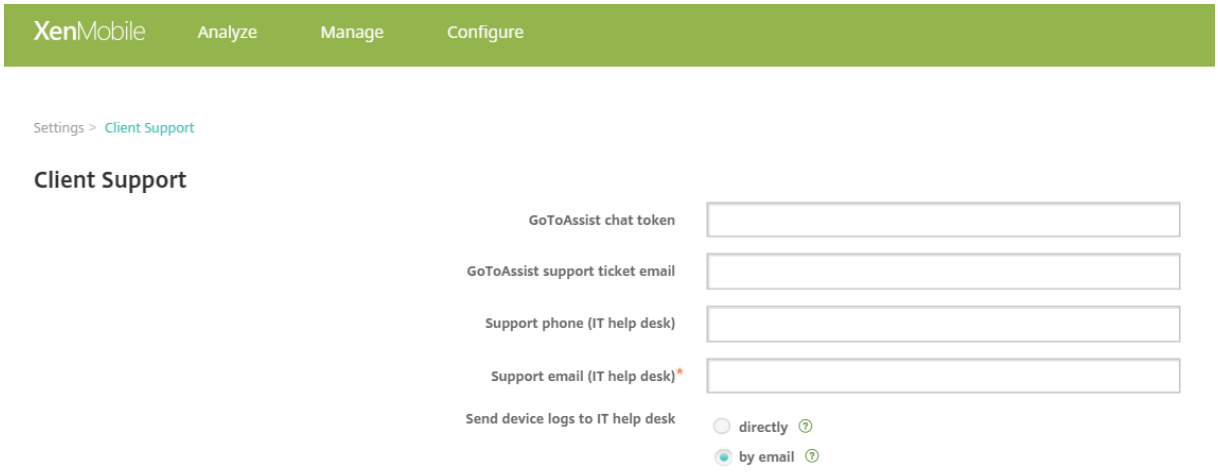
Opciones de Ayuda configuradas

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 más información, consulte Directiva de localización.

Recopilación y análisis de cierres inesperados

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

July 18, 2022

Citrix admite actualizaciones desde las dos últimas versiones de las aplicaciones móviles de productividad.

Secure Hub 22.6.0

No hay problemas conocidos ni resueltos en esta versión.

Secure Hub 22.5.0

No hay problemas conocidos ni resueltos en esta versión.

Secure Hub 22.4.0

No hay problemas conocidos ni resueltos en esta versión.

Problemas conocidos y problemas resueltos en versiones anteriores

Para ver los problemas resueltos y conocidos en versiones anteriores de Secure Hub, consulte Historial de problemas conocidos y resueltos en Secure Hub.

Situaciones de petición de credenciales

December 7, 2021

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 con o sin conexión (el dispositivo necesita una conexión de red a Endpoint Management).

Además, el tipo de credenciales que los usuarios escriben, como una contraseña de Active Directory, un PIN o código de acceso de Citrix, una contraseña de un solo uso o la autenticación con huella dactilar (denominada 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. Por ejemplo: Cuando 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 15 minutos. La directiva "Código de acceso de aplicación" **activada** 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.
- **Período 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 "Período 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 "Período máximo sin conexión" y la directiva MDX "Período 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 “Período 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 período de sondeo activo y del período 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 desconecta si no se produce ninguna actividad de sesión durante el período 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 verán un cuadro de 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 período de tiempo de espera forzado. La desconexión forzada obliga a reautenticarse después de un período determinado. La próxima vez los usuarios verán un cuadro de diálogo de autenticación para volver a conectarse a la red de la empresa. Está **desactivada** de forma predeterminada. 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 dejó la directiva MDX "Código de acceso de aplicación" habilitada de forma predeterminada y se usa 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 la sesión de Secure Hub y, a continuación, abren una aplicación administrada.

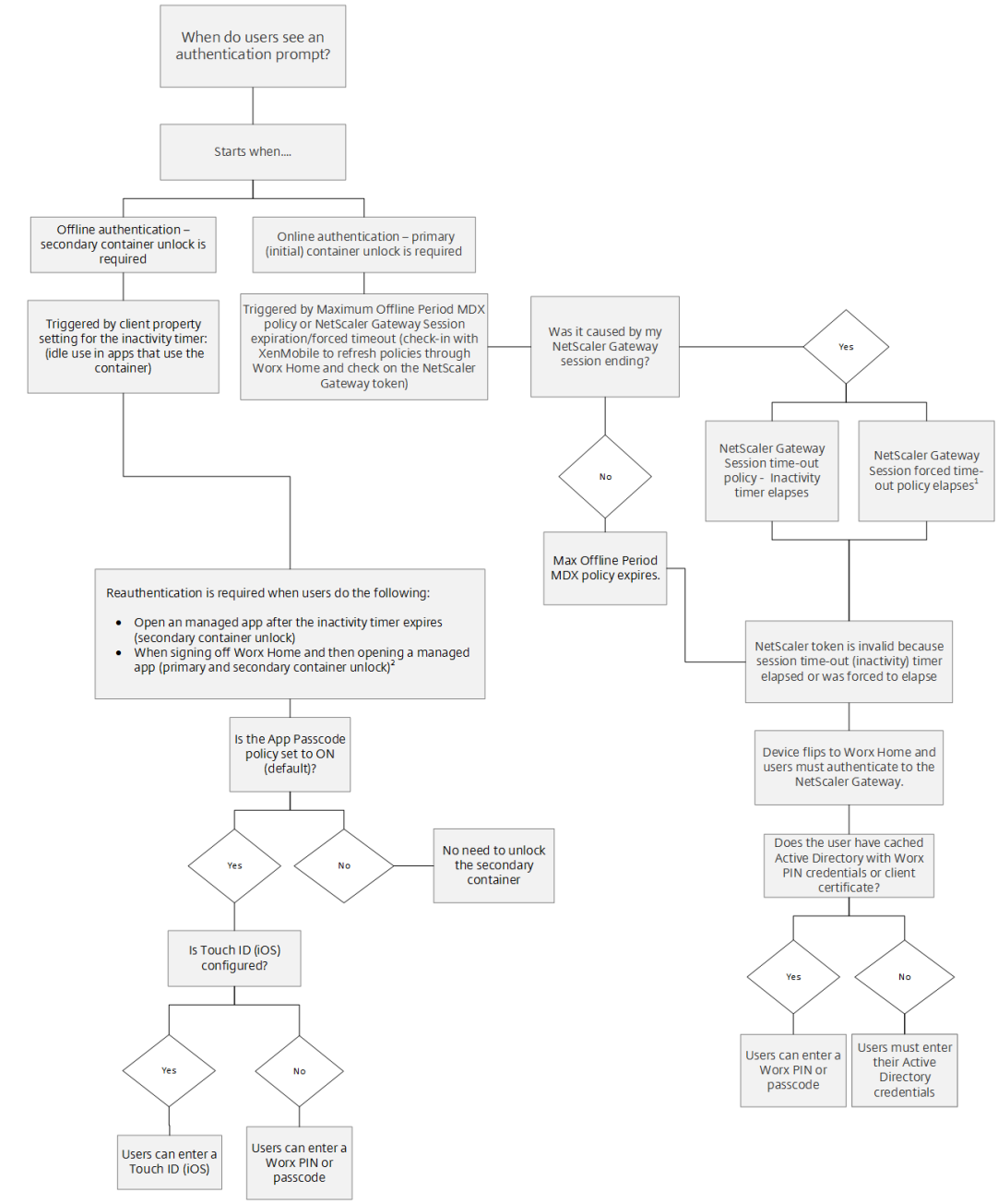
Se requieren credenciales de Active Directory para cualquiera de las circunstancias de desbloqueo de contenedor cuando se cumplen las siguientes condiciones:

- 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 dactilar, consulte Autenticación por huella dactilar 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.



1 If you set the session forced time-out policy to a lower value than for the inactivity time-out policy, the forced time-out policy overrides the inactivity time-out policy.
2 To see how these situations differ for iOS and Android devices, see the Credential Types section in Authentication Prompt Scenarios in the Citrix documentation.

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 "Período máximo sin conexión" y "Período de sondeo activo", y Endpoint Management detecta que hay directivas actualizadas que es necesario enviar al dispositivo a través de Secure Hub.

Inscribir dispositivos mediante credenciales derivadas

November 30, 2020

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).

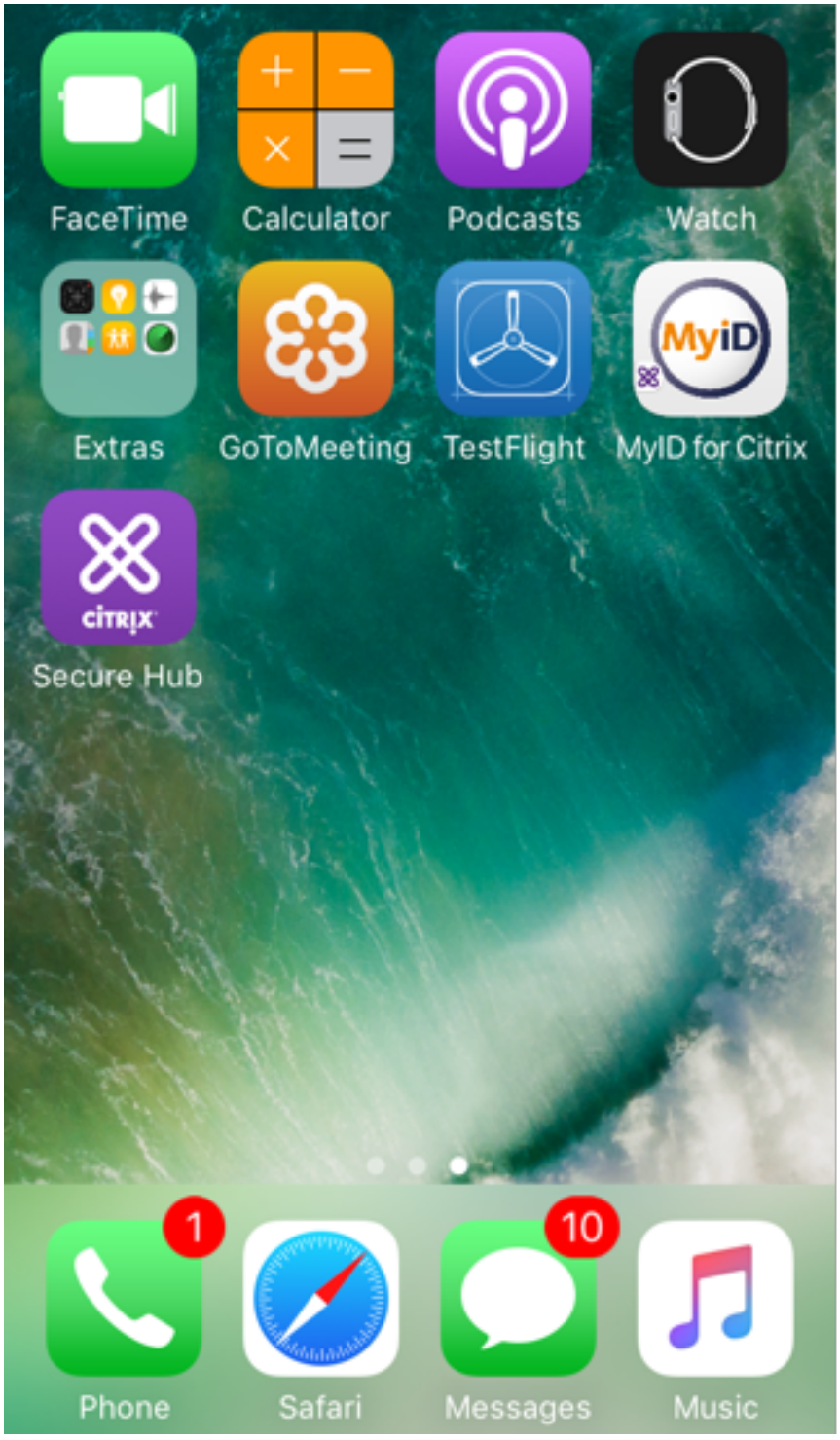
Las credenciales derivadas son un certificado de inscripción que contiene un identificador de usuario como, por ejemplo, su nombre principal o UPN. Endpoint Management almacena las credenciales obtenidas del proveedor de credenciales en un almacén seguro del dispositivo.

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.

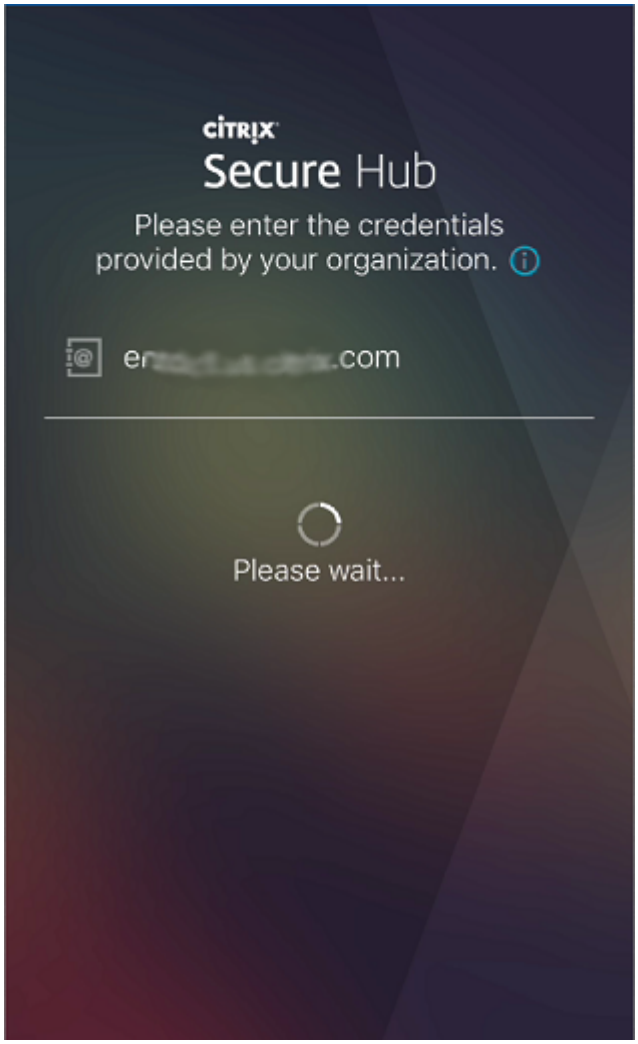
Pasos de inscripción de dispositivos cuando se utilizan credenciales derivadas

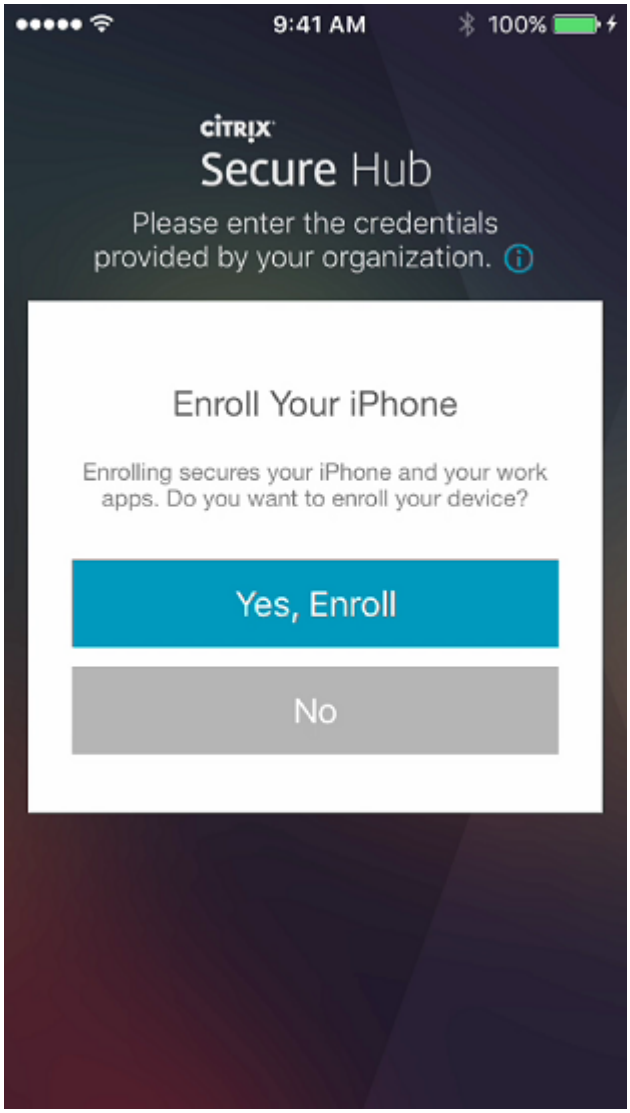
La inscripción requiere que los usuarios introduzcan su tarjeta inteligente en un lector conectado a su escritorio.

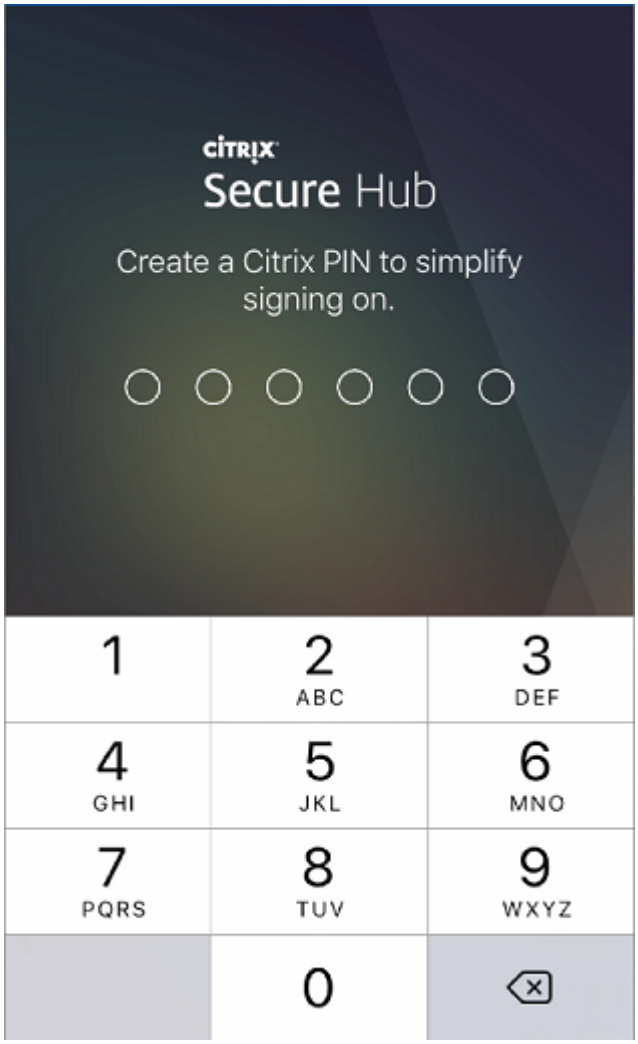
1. El usuario instala Secure Hub y la aplicación desde el proveedor de credenciales derivadas. En este ejemplo, la aplicación del proveedor de identidad es Intercede MyID Identity Agent.



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.

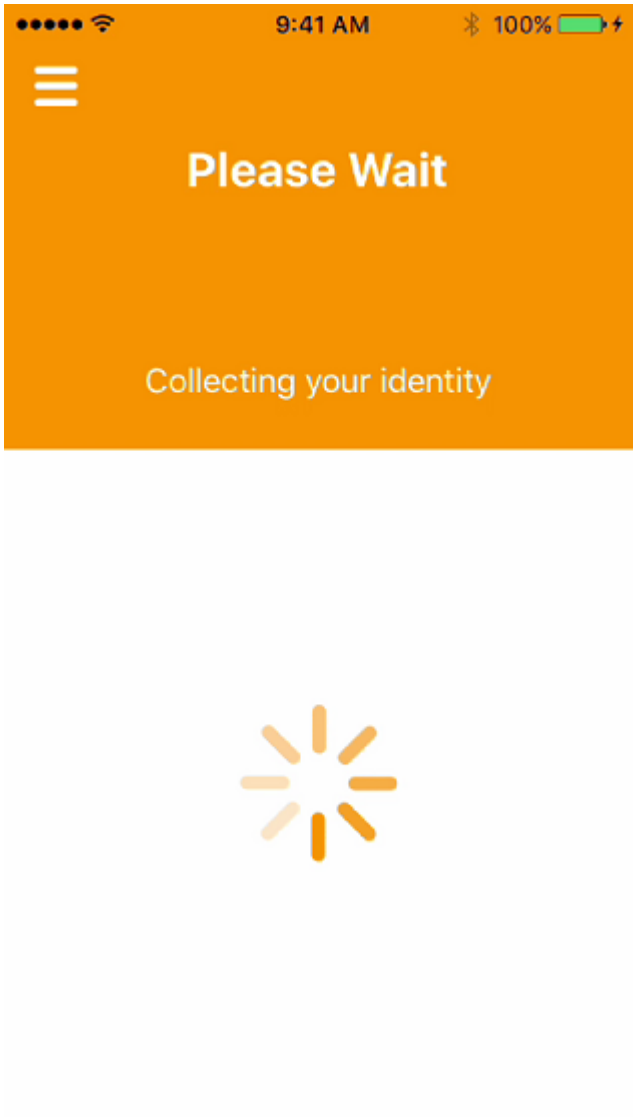




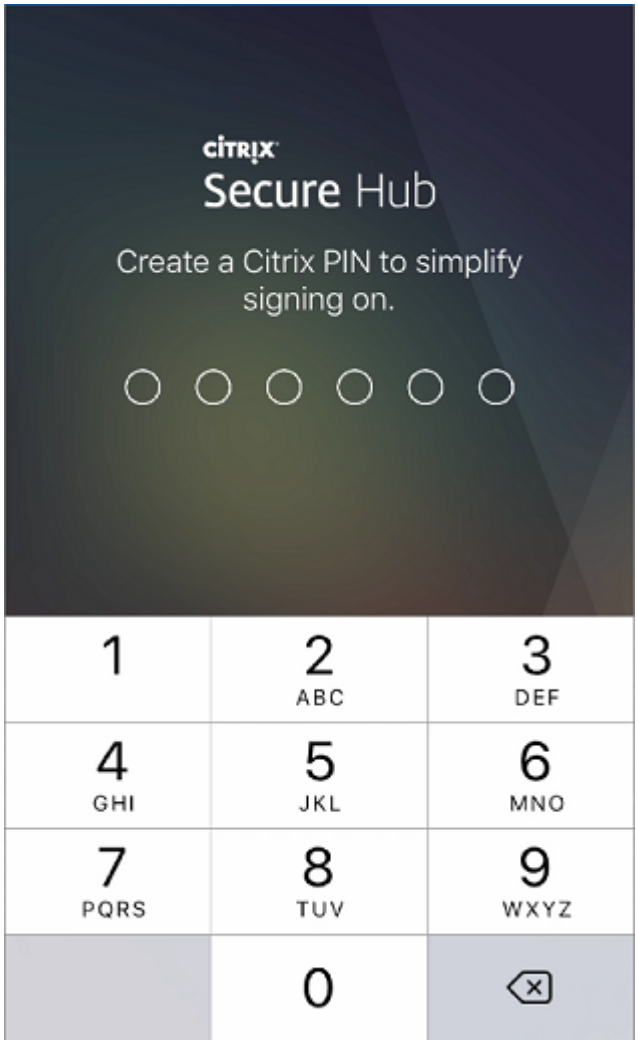


3. El usuario sigue las instrucciones para activar sus credenciales inteligentes. Aparecerá una pantalla de bienvenida, seguida de una solicitud para escanear un código QR.

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 mediante 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