Aplicaciones móviles de productividad

Contents

Calendario de publicación de versiones para aplicaciones móviles de productividad

June 6, 2024

Las versiones de las aplicaciones móviles de productividad de Citrix se publican cada dos semanas. Aunque las fechas exactas pueden cambiar, conocer este ritmo puede ayudarle a planificar con antelación. También queremos facilitarle la administración de las implementaciones y las actualizaciones de las aplicaciones.

Acerca del proceso de publicación por fases de Secure Mail y Secure Web

Cuando haya nuevas versiones de Secure Mail y Secure Web disponibles, las versiones se publicarán de forma escalonada de la siguiente manera:

- Para los usuarios de iOS y Android, las actualizaciones de Secure Mail y Secure Web están disponibles en el App Store y Google Play para un porcentaje cada vez mayor de usuarios en el transcurso de una semana (siete días).
- Las nuevas descargas de Secure Mail y Secure Web para iOS obtienen la nueva versión durante esta semana. Las nuevas descargas de Secure Mail y Secure Web para Android ejecutarán la versión anterior durante la semana, hasta que la implantación de la nueva versión llegue al 100 % de los usuarios.
- Para los usuarios, algunas funciones se publican gradualmente por fases.

Requisitos previos para la administración de marcas de funcionalidad

Si se produce un problema con Secure Hub o Secure Mail en producción, se puede inhabilitar la funcionalidad afectada desde el código de la aplicación. Para ello, se utilizan marcas de función y un servicio externo denominado LaunchDarkly. No es necesario que realice ninguna configuración para permitir el tráfico a LaunchDarkly, salvo si tiene un firewall o proxy bloqueando el tráfico saliente. En ese caso, puede habilitar el tráfico a LaunchDarkly a través de direcciones URL o direcciones IP específicas, según sus requisitos de directiva. Para obtener más información sobre la compatibilidad con MDX para excluir dominios del túnel a partir de aplicaciones móviles de productividad 10.6.15, consulte la documentación de MDX Toolkit. Para ver las preguntas frecuentes sobre las marcas de funcionalidad y LaunchDarkly, consulte este artículo de asistencia de Knowledge Center.

> **Nota:**

> Para obtener información avanzada sobre las funciones de Citrix Endpoint Management que se están retirando gradualmente, consulte Elementos retirados.

Aplicaciones móviles de productividad admitidas

February 27, 2024

Los usuarios que tienen las actualizaciones automáticas habilitadas reciben la versión más reciente desde el almacén de aplicaciones. La versión más reciente de las aplicaciones móviles de productividad es esta:

- 23.10.0 (Secure Web para Android)
- 23.9.0 (Secure Mail y Secure Web para iOS)
- 23.8.2 (Secure Mail para Android)

Citrix admite actualizaciones desde las dos últimas versiones de las aplicaciones móviles de productividad. Las dos versiones más recientes de las aplicaciones móviles de productividad son estas:

- 23.8.1 (Secure Mail para Android)
- 23.8.0 (Secure Web para Android)
- 23.7.0 (Secure Mail para Android y Secure Mail para iOS)
- 23.5.0 (Secure Mail para iOS y Secure Web para Android)
- 23.2.0 (Secure Web para iOS)
- 22.9.1 (Secure Web para iOS)

> **Importante:**
>
> El cifrado MDX alcanzó el fin de su vida (EOL) el 1 de septiembre de 2020. Para los dispositivos inscritos en la administración de dispositivos (AD) antigua:
>
> - Si no utiliza el cifrado MDX, no hace falta hacer nada.
> - Si utiliza el cifrado MDX, migre sus dispositivos Android a Android Enterprise. Los dispositivos Android 10 deben inscribirse o reinscribirse con Android Enterprise. Esto incluye los dispositivos Android en modo de solo MAM. Consulte Migrar la administración de dispositivos a Android Enterprise para obtener información detallada.

Sistemas operativos compatibles

Compatibilidad de las aplicaciones móviles de productividad con los siguientes sistemas operativos:

Nombre del producto	Sistema operativo	Versión mínima de implementación	Última versión disponible
Secure Hub	Android	7.x	14.x
	iOS	12.x	17.x
Secure Mail	Android	8.x	14.x
	iOS	13.x	17.x
Secure Web	Android	8.x	14.x
	iOS	13.x	17.x

Compatibilidad de las versiones más recientes de las aplicaciones móviles de productividad con la última versión y las dos versiones anteriores de Citrix Endpoint Management. Para obtener más información sobre los sistemas operativos compatibles con Citrix Endpoint Management, consulte Sistemas operativos de dispositivos compatibles.

La versión más reciente de las aplicaciones móviles de productividad requiere la versión más reciente de Secure Hub. Debe mantener Secure Hub actualizado.

> **Nota:**
>
> En cualquier momento, Citrix solo garantiza compatibilidad con las versiones más recientes y las dos anteriores (N, N-1 y N-2) de los sistemas operativos Android e iOS.

Otras consideraciones y limitaciones

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

Secure Mail

- Actualmente, Endpoint Management no admite NetScaler 12.0.41.16 debido a un problema con Secure Ticket Authority (STA) y Secure Mail. El problema está resuelto en NetScaler 12.0 compilación 41.22.
- Secure Mail para Exchange 2007 y Lotus Notes 8.5.3 alcanzó el final de su vida útil (EOL) el 30 de septiembre de 2017.
- Para obtener el mejor rendimiento al enviar datos adjuntos en Citrix Files, se recomienda usar las versiones más recientes de Citrix Files. Citrix Files no está disponible para Windows.

- En entornos de IBM Notes, debe configurar el servidor de IBM Domino Traveler 9.0. Para ver información detallada, consulte Integrar Exchange Server o IBM Notes Traveler Server.

> **Nota:**
>
> - Citrix Files para XenMobile alcanzó el fin de su vida útil el 1 de julio de 2023. Para obtener más información, consulte Fin de vida y aplicaciones retiradas.

Secure Web

Instale la versión más reciente de Android WebView en los dispositivos. Los usuarios pueden descargar Android WebView desde Google Play.

QuickEdit

QuickEdit sigue estando disponible como una aplicación móvil de productividad. No se aplicará el final de su vida útil (EOL) el 1 de septiembre de 2018 como se comunicó anteriormente.

Citrix Content Collaboration para Endpoint Management

Los usuarios acceden a Citrix Content Collaboration para Endpoint Management desde los almacenes públicos de aplicaciones después de la versión 6.5.

ShareConnect

ShareConnect alcanzó el final de su vida útil (EOL) el 30 de junio de 2020. Para obtener información más detallada, consulte Fin de vida y aplicaciones obsoletas.

Citrix Secure Notes y Citrix Secure Tasks

Citrix Secure Notes y Citrix Secure Tasks alcanzaron el final de su vida útil (EOL) el 31 de diciembre de 2018. Para obtener información más detallada, consulte Fin de vida y aplicaciones obsoletas.

Tareas y aspectos relevantes para administradores

June 6, 2024

En este artículo se describen las tareas y los aspectos que son relevantes para los administradores de las aplicaciones móviles de productividad.

Administrar marcas de función

Si se produce un problema una aplicación móvil de productividad durante la producción, se puede inhabilitar la función afectada con el código de la aplicación. Podemos desactivar la función de Secure Hub, Secure Mail y Secure Web para iOS y Android. Para ello, se utilizan marcas de función y un servicio externo denominado LaunchDarkly. No es necesario que realice ninguna configuración para permitir el tráfico a LaunchDarkly, salvo si tiene un firewall o proxy bloqueando el tráfico saliente. En ese caso, puede habilitar el tráfico a LaunchDarkly a través de direcciones URL o direcciones IP específicas, según sus requisitos de directiva. Para obtener más información sobre la funcionalidad de MDX para excluir dominios del túnel, consulte la documentación de MDX Toolkit.

Puede habilitar el tráfico y la comunicación en LaunchDarkly de las siguientes formas:

Permitir el tráfico a las siguientes URL

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `firehose.launchdarkly.com`

Crear una lista de permitidos por dominio

Antes ofrecíamos una lista de direcciones IP que utilizar cuando las directivas internas requieran únicamente direcciones IP. Ahora, debido a que Citrix ha realizado mejoras en la infraestructura, estamos eliminando las direcciones IP públicas a partir del 16 de julio de 2018. Le recomendamos que cree una lista de permitidos por dominio, si es posible.

Incluir direcciones IP en una lista de permitidos

Si necesita incluir las direcciones IP en una lista de permitidos, para obtener una lista de todos los intervalos de direcciones IP actuales, consulte esta lista de direcciones IP públicas de LaunchDarkly. Puede usar esta lista para asegurarse de que las configuraciones de su firewall se actualicen automáticamente de acuerdo con las actualizaciones de la infraestructura. Para obtener detalles sobre el estado actual de los cambios en la infraestructura, consulte la Página de estado de LaunchDarkly.

> Nota:
>
> Las aplicaciones de almacén público requieren una instalación limpia la primera vez que se implementan. No es posible actualizar la aplicación desde la versión empaquetada de la empresa a la versión del almacén de aplicaciones.

> Con la distribución desde un almacén público de aplicaciones, no es necesario firmar y empaquetar aplicaciones desarrolladas por Citrix con MDX Toolkit. Puede usar el MDX Toolkit para empaquetar aplicaciones de empresa o de terceros.

Requisitos del sistema para LaunchDarkly

- Endpoint Management 10.7 o una versión posterior.
- Compruebe que las aplicaciones pueden comunicarse con los siguientes servicios si el parámetro de túnel dividido está **desactivado** en Citrix ADC:
  - Servicio de LaunchDarkly
  - Servicio de escucha de APNs

Almacenes de aplicaciones admitidos

Las aplicaciones móviles de productividad están disponibles en el App Store de Apple y en Google Play.

En China, donde Google Play no está disponible, Secure Hub para Android está disponible en las siguientes tiendas de aplicaciones:

- https://shouji.baidu.com
- https://apk.hiapk.com
- https://apk.91.com

Habilitar la distribución desde almacenes públicos de aplicaciones

1. Descargue los archivos .mdx para la tienda pública de iOS y Android desde la página de descargas de Endpoint Management.
2. Cargue los archivos MDX en la consola de Endpoint Management. Las versiones de almacén público de las aplicaciones móviles de productividad se siguen cargando como aplicaciones MDX. No las cargue como aplicaciones de almacén público en el servidor. Para ver los pasos a seguir, consulte Agregar aplicaciones.
3. Cambie los valores predeterminados de las directivas por los valores adecuados para sus directivas de seguridad (optativo).
4. Envíe las aplicaciones como aplicaciones obligatorias (opcional). Este paso requiere que su entorno tenga habilitada la administración de dispositivos móviles.
5. Instale las aplicaciones en el dispositivo desde el App Store, Google Play o el almacén de aplicaciones de Endpoint Management.

- En Android, al usuario se le dirige a Google Play para instalarse la aplicación. En iOS, en implementaciones MDM, la aplicación se instala sin redirigir al usuario a la tienda de aplicaciones.
- Cuando la aplicación se instala desde el App Store o Google Play, se produce la siguiente acción. La aplicación se convierte en una aplicación administrada siempre que el archivo MDX correspondiente se haya cargado en el servidor. Cuando pasa a ser una aplicación administrada, la aplicación pide un PIN de Citrix. Cuando los usuarios escriben el PIN de Citrix, Secure Mail muestra la pantalla de configuración de la cuenta.

6. Las aplicaciones están accesibles solo si el usuario está inscrito en Secure Hub y el archivo MDX correspondiente se encuentra en el servidor. Si no se cumple alguna de esas condiciones, los usuarios pueden instalarse la aplicación, pero estará bloqueada.

Si actualmente utiliza aplicaciones de Citrix Ready Marketplace que están en almacenes públicos de aplicaciones, ya conocerá el proceso de implementación. Las aplicaciones móviles de productividad adoptan el mismo enfoque que varios proveedores de software independientes. Incruste el SDK de MDX en la aplicación para prepararla de cara al almacén público.

> Nota:
>
> Las versiones de almacén público de la aplicación Citrix Files para iOS y para Android ahora son universales. La aplicación Citrix Files es la misma para teléfonos y tabletas.

Notificaciones push de Apple

Para obtener más información sobre la configuración de las notificaciones push, consulte Configurar Secure Mail para notificaciones push.

Preguntas frecuentes sobre los almacenes públicos de aplicaciones

- ¿Puedo implementar varias copias de la aplicación de almacén público para grupos diferentes de usuarios? Por ejemplo, si le interesa implementar directivas distintas a grupos diferentes de usuarios.

  Cargue un archivo MDX diferente para cada grupo de usuarios. Sin embargo, en este caso, un solo usuario no puede pertenecer a varios grupos. Si un mismo usuario pertenece a varios grupos, se asignarán varias copias de la misma aplicación a ese usuario. No se pueden implementar varias copias de una aplicación de almacén público en un mismo dispositivo, porque el ID de aplicación no se puede cambiar.

- ¿Puedo distribuir aplicaciones de almacén público como aplicaciones obligatorias?

  Sí. La distribución push de aplicaciones en los dispositivos requiere MDM; no se admite en implementaciones de solo MAM.

- ¿Debo actualizar las reglas de las directivas de tráfico o Exchange Server que se basan en el agente de usuario?

  A continuación, se presentan las reglas y las directivas de agente del usuario desglosadas por plataforma.

  > Importante:
  >
  > Secure Notes y Secure Tasks han alcanzado el estado Fin de vida (EOL) el 31 de diciembre de 2018. Para obtener información más detallada, consulte Fin de vida y aplicaciones obsoletas.

Android

Aplicación	Servidor	Cadena de usuario-agente
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		WorxMail
Citrix Secure Tasks	Exchange	WorxMail
Citrix Secure Notes	Exchange	WorxMail
	Citrix Files	Secure Notes

iOS

Aplicación	Servidor	Cadena de usuario-agente
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		com.citrix.browser
Citrix Secure Tasks	Exchange	WorxTasks
Citrix Secure Notes	Exchange	WorxNotes
	Citrix Files	Secure Notes

- ¿Puedo impedir actualizaciones de la aplicación?

No. Cuando se publica una actualización en el almacén público de aplicaciones, los usuarios que tengan habilitada la actualización automática de las aplicaciones, recibirán la actualización.

- ¿Puedo aplicar actualizaciones de la aplicación?

  Sí, las actualizaciones se aplican a través de la directiva de período de gracia para la actualización. Esta directiva se define cuando el nuevo archivo MDX correspondiente a la versión actualizada de la aplicación se carga en Endpoint Management.

- ¿Cómo puedo probar las aplicaciones antes de que la actualización llegue a los usuarios si no puedo controlar el momento de la actualización?

  Al igual que con Secure Hub, las aplicaciones se pueden probar en TestFlight for iOS durante el periodo EAR. Para Android, las aplicaciones están disponibles en el programa Beta de Google Play durante el periodo EAR. Puede probar las actualizaciones de la aplicación durante este tiempo.

- ¿Qué ocurre si no actualizo el nuevo archivo MDX antes de que la actualización automática llegue a los dispositivos de los usuarios?

  La aplicación actualizada sigue siendo compatible con el archivo MDX antiguo. Si hay alguna función que dependa de una directiva nueva, la función no se habilitará.

- ¿La aplicación se convertirá en aplicación administrada si Secure Hub está instalado o la aplicación se tiene que inscribir para ello?

  El usuario debe estar inscrito en Secure Hub para que la aplicación de almacén público se active como aplicación administrada (protegida por MDX) y sea utilizable. Si Secure Hub está instalado, pero no se ha inscrito, el usuario no podrá usar la aplicación de almacén público.

- ¿Necesito una cuenta de desarrollador de Apple Enterprise para las aplicaciones de almacén público?

  No. Puesto que Citrix se ocupa ahora de mantener los certificados y los perfiles de aprovisionamiento para las aplicaciones móviles de productividad, ya no es necesario tener una cuenta de desarrollador de Apple Enterprise para implementar estas aplicaciones para los usuarios.

- ¿El final de la distribución empresarial afecta a alguna aplicación empaquetada que ya se haya implementado?

  No, solo se aplica a las aplicaciones móviles de productividad: Secure Mail, Secure Web y Citrix Content Collaboration para Endpoint Management, QuickEdit y ShareConnect. Cualquier aplicación empaquetada de empresa que tenga implementada y que haya sido desarrollada internamente o por terceros puede seguir mediante el empaquetado empresarial. MDX Toolkit seguirá ofreciendo el empaquetado empresarial para los desarrolladores de aplicaciones.

- Cuando instalo una aplicación desde Google Play, obtengo un error de Android con el código "505".

  > Nota:
  >
  > Android 5.x dejó de admitirse el 31 de diciembre de 2018.

  Este es un problema conocido con Google Play y Android (versiones 5.x). Si ocurre este error, siga estos pasos para borrar los datos obsoletos del dispositivo que impiden la instalación de la aplicación:

1. Reinicie el dispositivo.
2. Borre la memoria caché y los datos de Google Play mediante los ajustes del dispositivo.
3. Como último recurso, quite y vuelva a agregar la cuenta de Google en el dispositivo.

Para obtener más información, busque en este sitio las palabras clave "Fix Google Play Store Error 505 in Android: Unknown Error Code".

- ¿Si la aplicación en Google Play se ha sacado ya a producción y no hay ninguna nueva versión beta disponible, por qué sigo viendo "Beta"junto al nombre de la aplicación en Google Play?

  Si participa en nuestro programa EAR (Early Release Program), siempre verá "Beta"junto al título de la aplicación. Este nombre solo notifica a los usuarios de su nivel de acceso a una aplicación determinada. El nombre "Beta"indica que los usuarios reciben la versión disponible más reciente de la aplicación. La versión más reciente puede ser la más reciente publicada en producción o en pruebas.

- Después de instalar y abrir la aplicación, los usuarios ven el mensaje "Aplicación no autorizada" , aunque el archivo MDX se encuentre en la consola de Endpoint Management.

  Esto puede ocurrir si el usuario instala la aplicación directamente desde el App Store o Google Play y si la presentación de Secure Hub no se ha actualizado. Secure Hub debe actualizarse si el temporizador de inactividad caduca. Las directivas se actualizan cuando el usuario abre Secure Hub y vuelve a autenticarse. La aplicación estará autorizada la próxima vez que el usuario la abra.

- ¿Necesito un código de acceso para usar la aplicación? Al instalar la aplicación desde el App Store o Google Play, aparece una pantalla que me pide introducir un código de acceso.

  Si ve una pantalla donde se le pide un código de acceso, es porque no se ha inscrito en Endpoint Management a través de Secure Hub. Inscríbase con Secure Hub y compruebe que el archivo MDX de la aplicación se ha implementado en el servidor. Compruebe también que la aplicación se pueda usar. El código de acceso está limitado al uso interno de Citrix. Las aplicaciones requieren que se active una implementación de Endpoint Management.

- ¿Puedo implementar aplicaciones iOS de almacén público mediante VPP o DEP?

  Endpoint Management está optimizado para la distribución por VPP de las aplicaciones de almacén público que no están habilitadas para MDX. Aunque puede distribuir las aplicaciones de almacén público de Endpoint Management mediante VPP, la implementación no es óptima hasta que realicemos mejoras adicionales a Endpoint Management y la almacén de Secure Hub para resolver las limitaciones. Para ver una lista de los problemas conocidos a la hora de implementar las aplicaciones de Endpoint Management desde la tienda pública vía VPP, además de posibles soluciones temporales a esos problemas, consulte este artículo en Knowledge Center de Citrix.

Directivas MDX para aplicaciones móviles de productividad

Las directivas MDX permiten configurar los parámetros que Endpoint Management aplica. Las directivas cubren parámetros de autenticación, seguridad de los dispositivos, requisitos de red y de acceso, cifrado, interacción con las aplicaciones y restricciones de las aplicaciones, entre otros aspectos. Varias directivas MDX se aplican a todas las aplicaciones móviles de productividad Algunas directivas son específicas de cada aplicación.

Los archivos de directivas se suministran en formato MDX para las versiones de almacén público de las aplicaciones móviles de productividad. Asimismo, puede configurar directamente las directivas desde la consola de Endpoint Management cuando agregue una aplicación.

Para obtener descripciones completas de las directivas MDX, consulte los siguientes artículos de esta sección:

- Vista general de las directivas MDX para aplicaciones móviles de productividad
- Directivas MDX para aplicaciones móviles de productividad para Android
- Directivas MDX para aplicaciones móviles de productividad para iOS

Las secciones siguientes describen las directivas MDX relacionadas con las conexiones de usuario.

Modo dual en Secure Mail para Android

Dispone de un SDK de administración de aplicaciones móviles (MAM) para reemplazar áreas de funcionalidad MDX que no cubren las plataformas iOS y Android. La tecnología de empaquetado MDX está programada para alcanzar el final de su vida útil (EOL) en septiembre de 2021. Para seguir administrando sus aplicaciones empresariales, debe incorporar el SDK de MAM.

A partir de la versión 20.8.0, las aplicaciones de Android se publican con MDX y el SDK de MAM en preparación para la estrategia del final de vida útil de MDX mencionada anteriormente. El modo dual MDX está diseñado para ofrecer una forma de transición desde el MDX Toolkit actual a nuevos SDK de MAM. El uso del modo dual le permite:

- Continuar administrando aplicaciones con MDX Toolkit (conocido ahora como MDX antiguo en la consola de Endpoint Management)
- Gestionar aplicaciones que incorporan el nuevo SDK de MAM.

  > **Nota:**
  >
  > Cuando utiliza el SDK de MAM, no es necesario empaquetar las aplicaciones.

No se requiere ningún paso adicional después de cambiar al SDK de MAM.

Para obtener más información sobre el SDK de MAM, consulte los siguientes artículos:

- Introducción al SDK de MAM
- Sección de Citrix Developer sobre Administración de dispositivos
- entrada del blog de Citrix
- Descargar el SDK al iniciar sesión en Descargas de Citrix

Requisitos previos

Para implementar correctamente la funcionalidad del modo dual, compruebe lo siguiente:

- Actualice Citrix Endpoint Management a las versiones 10.12 RP2 o posterior, o 10.11 RP5 o posterior.
- Actualice sus aplicaciones móviles a la versión 20.8.0 o posterior.
- Actualice el archivo de directivas a la versión 20.8.0 o posterior.
- Si su organización utiliza aplicaciones de terceros, asegúrese de incorporar el SDK de MAM en dichas aplicaciones antes de cambiar a la opción SDK de MAM para las aplicaciones móviles de productividad de Citrix. Todas las aplicaciones administradas deben transferirse al SDK de MAM al mismo tiempo.

> **Nota:**
>
> El SDK de MAM es compatible con todos los clientes basados en la nube.

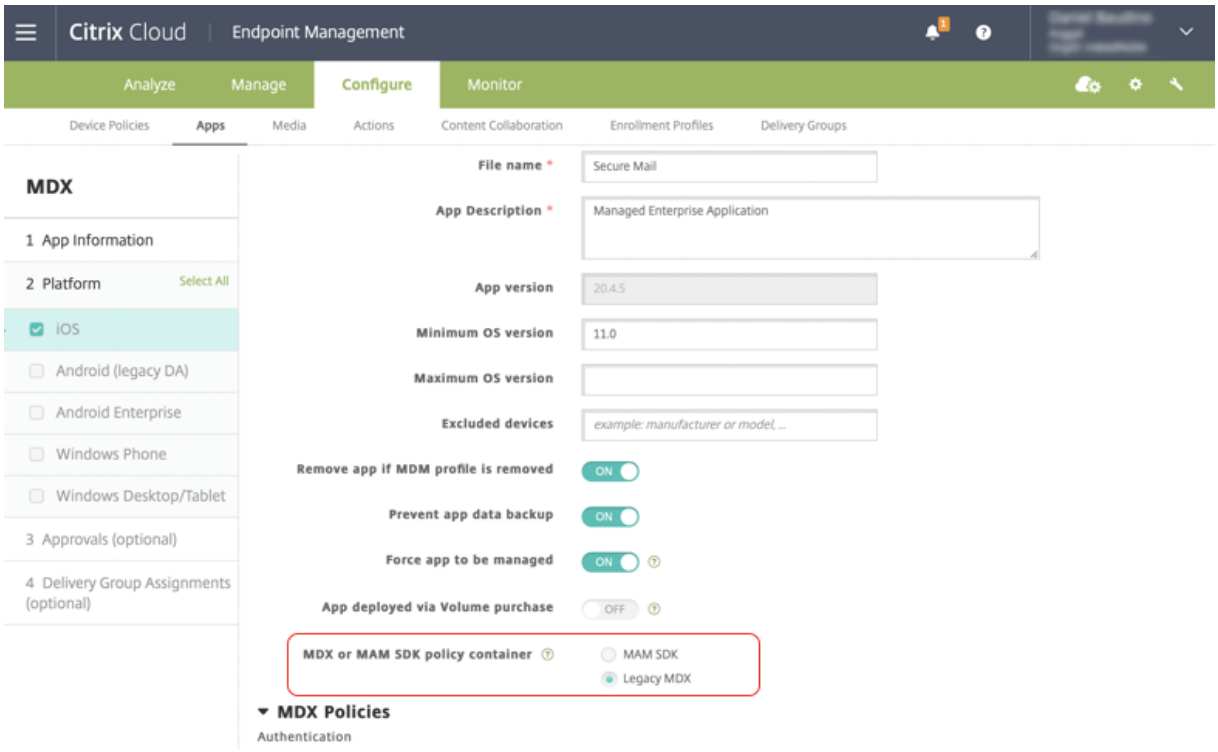
Limitaciones

- El SDK de MAM solamente admite aplicaciones publicadas bajo la plataforma Android Enterprise en la implementación de Citrix Endpoint Management. Para las aplicaciones recién publicadas, el cifrado predeterminado es el basado en plataforma.
- El SDK de MAM solamente admite el cifrado basado en plataforma, y no el cifrado MDX.
- Si no actualiza Citrix Endpoint Management y los archivos de directiva se ejecutan en la versión 20.8.0 o posterior para las aplicaciones móviles, se crearán entradas duplicadas de la directiva de conexión en red para Secure Mail.

Al configurar Secure Mail en Citrix Endpoint Management, la función de modo dual le permite continuar administrando aplicaciones con MDX Toolkit (ahora MDX antiguo) o cambiar al nuevo SDK de MAM. Citrix recomienda cambiar al SDK de MAM, ya que los SDK de MAM son más modulares y están pensados para permitirle usar solamente el subconjunto de la funcionalidad MDX que su organización utiliza.

En el **contenedor de directivas MDX o del SDK de MAM**, obtiene las siguientes opciones para la configuración de directivas:

- **SDK de MAM**
- **MDX antiguo**



En la directiva **Contenedor de directivas MDX o de SDK de MAM**, solo puede cambiar de la opción **MDX antiguo** a la del **SDK de MAM**. La posibilidad de cambiar de **SDK de MAM** a **MDX antiguo** no está permitida, y debe volver a publicar la aplicación. El valor predeterminado es **MDX antiguo**. Asegúrese de establecer el mismo modo de directiva para las aplicaciones Secure Mail y Secure Web que se ejecutan en el mismo dispositivo. No puede tener dos modos diferentes ejecutándose en un mismo dispositivo.

Conexiones de usuario a la red interna

Las conexiones por túnel con la red interna pueden utilizar un túnel VPN completo o una variante de VPN sin cliente, conocida como SSO web en túnel. La directiva "Modo preferido de VPN"controla

este comportamiento. De forma predeterminada, las conexiones usan SSO web en túnel, que se recomienda para conexiones que requieren SSO. Se recomienda el parámetro "Túnel VPN completo" para conexiones que usan certificados de cliente o SSL de extremo a extremo con un recurso de la red interna. El parámetro gestiona cualquier protocolo por TCP y se puede usar con equipos Windows y Mac, así como con dispositivos iOS y Android.

La directiva Permitir cambio de modo VPN permite cambiar automáticamente entre el modo "Túnel VPN completo"y el modo "SSO web en túnel", según sea necesario. De manera predeterminada, esta directiva está desactivada. Si la directiva está activada, las solicitudes de red que no llegan a realizarse debido a una solicitud de autenticación que no se puede resolver en el modo preferido de VPN se vuelven a intentar en el modo alternativo. Por ejemplo, el modo "Túnel VPN completo", pero no el modo "SSO web en túnel", admite desafíos de servidor ante certificados de cliente. Del mismo modo, los desafíos de autenticación HTTP son más propensos a resolverse con SSO cuando se utiliza el modo SSO web en túnel.

Restricciones al acceso de red

La directiva "Acceso de red"especifica si hay restricciones para el acceso de red. De forma predeterminada, el acceso a Secure Mail no está restringido, lo que significa que no hay ninguna restricción para el acceso de red. Las aplicaciones tienen acceso sin restricciones a las redes a las que está conectado el dispositivo. De manera predeterminada, el acceso a Secure Web se canaliza por un túnel a la red interna, lo que significa que se usa un túnel VPN para cada aplicación hacia la red interna para todo el acceso de red y se usan los parámetros de túnel dividido de Citrix ADC. También puede especificarse la opción de bloquear acceso, de modo que la aplicación funcione como si el dispositivo no estuviera conectado a la red.

No bloquee la directiva "Acceso de red"si quiere permitir funciones como AirPrint, iCloud y las API de Facebook y Twitter.

La directiva "Acceso de red"también interactúa con la directiva "Servicios de red en segundo plano". Para ver información detallada, consulte Integrar Exchange Server o IBM Notes Traveler Server.

Propiedades de cliente de Endpoint Management

En las propiedades de cliente, se ofrece información que se proporciona directamente a Secure Hub en los dispositivos de los usuarios. Las propiedades de cliente se encuentran en la consola de Endpoint Management, en **Parámetros > Cliente > Propiedades de cliente**.

Las propiedades de cliente se usan para configurar parámetros como los siguientes:

Caché de contraseñas del usuario

El caché de contraseñas del usuario permite guardar localmente la contraseña de Active Directory del usuario en el dispositivo móvil. Si se habilita el almacenamiento en caché de las contraseñas de usuario, se pide a los usuarios que definan un código de acceso o un PIN de Citrix.

Temporizador de inactividad

El temporizador de inactividad define el tiempo en minutos que los usuarios pueden dejar sus dispositivos inactivos y acceder a una aplicación sin que se solicite un PIN o un código de acceso de Citrix. Si quiere activar este parámetro para una aplicación MDX, debe **activar** la directiva "Código de acceso de aplicación". Si la directiva "Código de acceso de aplicación"está **desactivada**, se redirige a los usuarios a Secure Hub para una autenticación completa. Al cambiar este parámetro, el valor se aplicará la próxima vez que los usuarios deban autenticarse.

Autenticación por PIN de Citrix

El PIN de Citrix simplifica la experiencia de autenticación del usuario. El PIN se usa para proteger un certificado de cliente o para guardar las credenciales de Active Directory localmente en el dispositivo. Si configura los parámetros de PIN, la experiencia de inicio de sesión de los usuarios es la siguiente:

1. La primera vez que los usuarios inician Secure Hub, se les solicita introducir un PIN, con lo que se almacenan en caché las credenciales de Active Directory.
2. La próxima vez que los usuarios inicien una aplicación móvil de productividad (como Secure Mail), tendrán que introducir el PIN para iniciar sesión.

Las propiedades de cliente permiten habilitar la autenticación con PIN, especificar el tipo de PIN, así como su complejidad y longitud, y los requisitos para cambiarlo.

Autenticación por huella digital o Touch ID

La autenticación por huella digital, también conocida como autenticación de Touch ID, es una alternativa al PIN de Citrix en dispositivos iOS. La función es útil para casos en que las aplicaciones empaquetadas (salvo Secure Hub) necesitan una autenticación sin conexión; por ejemplo, cuando se agota el tiempo del temporizador de inactividad. Puede habilitar esta funcionalidad en los siguientes casos de autenticación:

- PIN de Citrix + Configuración de certificado de cliente
- PIN de Citrix + Configuración de contraseña de AD guardada en caché

- PIN de Citrix + Configuración de certificado de cliente y configuración de contraseña de AD guardada en caché
- El PIN de Citrix está desactivado

Si falla la autenticación por huella digital o si un usuario cancela la solicitud de autenticación por huella digital, las aplicaciones empaquetadas recurren a la autenticación con el PIN de Citrix o con la contraseña de AD.

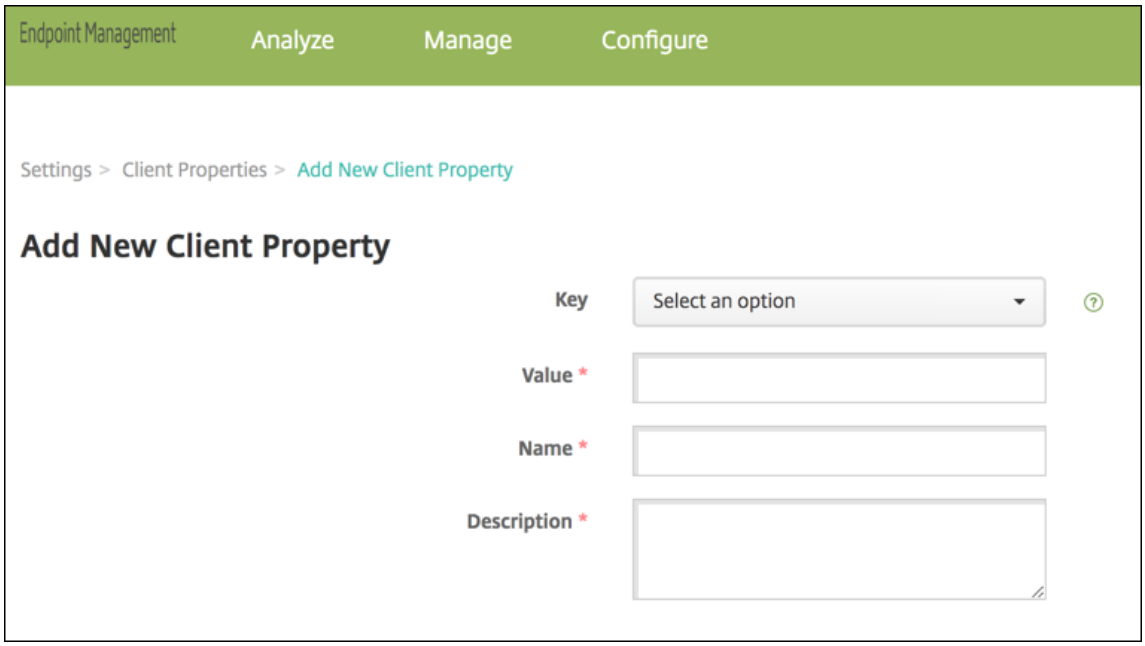
Requisitos para la autenticación por huella digital

- Dispositivos iOS (versión mínima 8.1) que admiten la autenticación por huella digital y tienen al menos una huella digital configurada.
- La entropía de usuario debe estar desactivada.

Para configurar la autenticación por huella digital

> Importante:
>
> Si la entropía de usuario está activada, se ignora la propiedad "Enable Touch ID Authentication" . La entropía de usuario se habilita mediante "Encrypt secrets using the Passcode key".

1. En la consola de Endpoint Management, vaya a **Parámetros > Cliente > Propiedades de cliente**.
2. Haga clic en **Agregar**.



3. Agregue la clave **ENABLE_TOUCH_ID_AUTH**, establezca el **Valor** en **True**, y establezca el nombre de la directiva en **Habilitar autenticación con huella digital**.

Después de configurar la autenticación por huella digital, los usuarios no necesitan volver a inscribirse en sus dispositivos.

Para obtener más información sobre la clave Encrypt secrets using Passcode (Cifrar secretos mediante un código de acceso) y las propiedades del cliente en general, consulte el artículo de Endpoint Management sobre Propiedades del cliente.

Google Analytics

Citrix Secure Mail utiliza Google Analytics para recopilar estadísticas y datos de análisis de información de uso sobre aplicaciones para mejorar la calidad de los productos. Citrix no recopila ni almacena ninguna otra información personal de los usuarios.

Inhabilitar Google Analytics

Los administradores pueden inhabilitar Google Analytics al configurar la propiedad de cliente personalizada **DISABLE_GA**. Para inhabilitar Google analytics, haga lo siguiente:

1. Inicie sesión en la consola de Citrix Endpoint Management y vaya a **Parámetros** > **Propiedades de cliente** > **Agregar nueva propiedad de cliente**.
2. Agregue el valor **DISABLE_GA** al campo **Clave**.
3. Establezca el valor de la propiedad del cliente en **true**.

> **Nota:**
>
> Si no configura el valor **DISABLE_GA** en la consola de Citrix Endpoint Management, los datos de Google Analytics están activos.

Funciones desglosadas por plataforma

June 6, 2024

En las siguientes tablas se resumen las funciones de las aplicaciones móviles de productividad de Citrix. **X** indica que la función está disponible para la plataforma. Para las funciones de QuickEdit, consulte Citrix QuickEdit.

Citrix Secure Hub

Función	iOS	Android
Iniciar sesión para autenticarse	X	X
Supervisar la observancia de directivas	X	X
Acceder a aplicaciones y escritorios	X	X
Aplicaciones y escritorios HDX	X	X
Crear y enviar registros de problemas	X	X
Adjuntar capturas de pantalla a los registros	X	X
Contactar con el servicio de asistencia desde dentro de la aplicación	X	X
Contactar con el servicio de asistencia técnica de Citrix desde dentro de la aplicación	X	X
Recopilación y análisis de cierres inesperados	X	X
Autenticación sin conexión	X	X
Envío de registros con Citrix Secure Mail	X	X
Google Analytics	X	X
Modo horizontal y vertical	X	X
Guía en las aplicaciones para establecer relaciones de confianza	X	X
Cuando se inscribe con correo electrónico, inscripción automática en Secure Mail (solo MAM)	X	X
Autenticación Touch ID sin conexión	X	X
Inscribirse con credenciales derivadas	X	

Función	iOS	Android
Autenticación biométrica		X
Usar el almacén de aplicaciones de Workspace	X	X

Citrix Secure Mail

Función	iOS	Android
Productividad de correo electrónico		
Minimizar borradores	X	X
Deshacer correos enviados		X
Administración de cifrado	X	X
Widget para la agenda del Calendario		X
Imagen de contacto en Secure Mail	X	X
Compatibilidad con mensajes de correo electrónico adaptativos	X	X
Sincronización automática de la carpeta Borradores	X	X
Sincronización de archivos adjuntos en la carpeta		X
Borradores		
Enviar, recibir, responder, responder a todos, reenviar correo electrónico	X	X
Crear, modificar, eliminar borradores	X	X
Marcar correo con indicador	X	X
Marcar como no leído	X	X
Ver todas las carpetas y subcarpetas	X	X

Función	iOS	Android
Guardado automático de borradores cuando la aplicación se pone en segundo plano	X	X
Del correo a la nota con Citrix Secure Notes. **Importante:** Secure Notes alcanzó el final de su vida útil (EOL) el 31 de diciembre de 2018. Para obtener información más detallada, consulte Fin de vida y aplicaciones obsoletas.	X	X
Buscar correo (local y en el servidor)	X	X
Seleccionar período de sincronización de correo (hasta 1 mes o Todos los correos)	X	X
Ver correo no leído	X	X
Visualización y reproducción segura de datos adjuntos de imágenes, vídeo y audio	X	X
Varios archivos de datos adjuntos	X	X
Responder y reenviar datos adjuntos	X	X
Adjuntar archivos desde Citrix Files	X	X
Adjuntar archivos desde conectores y zonas restringidas de Citrix Files	X	X
Repositorio de datos adjuntos	X	X
Modificar texto enriquecido	X	X
Notificación de correo electrónico con vista previa del asunto en la pantalla de bloqueo	X	X

Función	iOS	Android
Responder y eliminar correo electrónico e invitaciones desde la pantalla de notificación	X	
Adjuntar o tomar fotos	X	X
Seleccionar varios mensajes	X	X
Descargar adjuntos	X	X
Cargar imágenes en línea	X	X
Ordenación rápida	X	X
Enviar, recibir, abrir y guardar archivos ZIP adjuntos	X	X
Modos horizontal y vertical	X: Vistas de contactos, calendario, redacción, lectura y lista de mensajes	X: Solo vistas de redacción y lectura de correo
El texto pegado conserva el formato	X	X
SMS de contactos	X	X
FaceTime de contactos	X	
Los mensajes no enviados debido a problemas de conectividad o de buzón lleno se guardan en Outlook	X	X
Mostrar carpetas recientes		X
Tirar hacia abajo para actualizar el correo	X	X
Marca de hora de la última actualización	X	X
Gesto de deslizamiento hacia la izquierda para ver acciones de mensaje	X	X
Compatibilidad con Microsoft Exchange e IBM Notes Traveler	X	X
Tocar para actualizar correo, calendario y contactos	X	X

Función	iOS	Android
Respeta los parámetros de accesibilidad/tipo de fuente del dispositivo en las vistas de correo	X	X
Cifrado y firma S/MIME	X	X
Importar certificados S/MIME por correo electrónico	X	X
Integrar S/MIME, Intercede	X	
Integrar S/MIME, Entrust	X	
Protección Microsoft IRM para el cuerpo del mensaje	X	X
Notificaciones push	X	X
Las notificaciones push en la Bandeja de entrada actualizan automáticamente todas las carpetas, incluido el calendario	X	
Abrir documentos de Office 365	X	X
Acciones de 3D Touch	X	
Iconos contextuales en pantalla de bloqueo	X	X
Buscar en carpetas	X	X
Carpeta de correo de contactos VIP	X	X
Tamaño de letra dinámico	X	X
Mantener carpetas expandidas	X	X
Marcas de clasificación de mensajes	X	X
Revisión ortográfica	X	
Adjuntar la última foto tomada	X	X
Vista previa de las direcciones URL	X	X
Abrir enlaces de Citrix Files en Citrix Files	X	X

Función	iOS	Android
Compatibilidad con archivos `.pass`	X	
Seleccionar varios mensajes de correo electrónico en el modo de búsqueda	X	X
Insertar imágenes alineadas	X	X
Actualizar a Exchange ActiveSync (EAS) 16	X	X
Impedir que los usuarios utilicen dominios desconocidos o personales	X	
Compatibilidad con pantallas superanchas		X
Configurar varias cuentas de Exchange	X	X
Deslizarse a izquierda o derecha para más acciones	X	X
Cifrar respuestas o reenvíos de correos cifrados	X	
Imprimir correos electrónicos e imágenes en línea	X	
Usar la función Líneas de previsualización en los Parámetros para configurar cuántas líneas del cuerpo de un mensaje de correo electrónico quiere que aparezcan en la vista previa del buzón.	X	
Compatibilidad con mensajes de correo electrónico adaptativos	X	X
Vista previa de datos adjuntos en la aplicación (MS Office o imágenes)	X	X
Grupo de contactos personales	X	X

Función	iOS	Android
Migrar nombres de usuario a direcciones de correo electrónico (UPN)	X	X
Notificar mensajes de phishing	X	X
Autenticación moderna (OAuth)	X	X
Imprimir archivos adjuntos	X	
Android Enterprise (Android for Work)	X	
Firmas de texto enriquecido	X	
Notificaciones push enriquecidas	X	
Feeds	X	X
Mejoras para adjuntar fotos	X	X
Notificaciones de grupo	X	
Integración con Slack (Tech Preview)	X	X
Administrar feeds	X	
Dominios internos	X	X
Administrar sus feeds	X	X
Integración de MS Teams	X	X
Opción de autodiagnóstico (**Solucionar problemas**)		X
Modo dual (SDK de MAM)	X	X
Herramienta de autodiagnóstico		X
Calendario		
Previsualización e importación de archivos ICS como eventos de calendario		X
Arrastrar y colocar eventos del Calendario	X	X
Vistas de día, semana, mes y agenda	X	X

Función	iOS	Android
Avisos detallados en la pantalla de bloqueo	X	X
Sincronización de seis meses	X	X
Establecer eventos como privados	X	X
Desplazarse a la hora anterior al primer evento	X	
Opciones de actualización manual	X	X
Definir recordatorios	X	X
Tocar en una dirección para verla en un mapa	X	X
Números de semana	X	X
Tamaño de letra dinámico	X	X
Marcas de clasificación de seguridad	X	X
Toques largos en las direcciones	X	
Establecer el primer día de la semana laboral	X	X
Centrar la vista en la semana de la fecha seleccionada	X	
Fecha actual siempre resaltada	X	X
Datos adjuntos del calendario provenientes del repositorio de datos adjuntos	X	X
Compatibilidad con calendarios personales	X	X
Mostrar conflictos con eventos de calendario personal		X
Imprimir eventos del calendario	X	
Tocar en los números de teléfono y las direcciones web que aparecen en la línea de Asunto del calendario	X	

Función	iOS	Android
Buscar en el calendario	X	
Reuniones		
Responder, responder a todos y reenviar reuniones	X	X
Vista de organizador de respuestas de invitación	X	X
Vista de organizador de la disponibilidad de invitados con sugerencias de disponibilidad	X	X
Tocar para unirse a reuniones en línea. **Nota:** Para WebEx y Lync, debe configurar directivas en Citrix Endpoint Management para habilitar estas aplicaciones.	X	X
Tocar para unirse a conferencias de audio	X	X
Programar audio, conferencia y reunión en línea en una nueva invitación	X	X
Agregar enlaces de ShareFile a las nuevas invitaciones	X	X
Reenviar invitaciones con datos adjuntos	X	X
Tocar para enviar un mensaje de “voy a llegar tarde”	X	X
Tocar para responder al organizador de la reunión	X	X
Tocar para responder a todos los invitados de la reunión	X	X
Tocar para responder a todos los invitados de la reunión	X	X
Tocar para responder con datos adjuntos a todos los invitados de la reunión	X	X
Marcar para entrar en GoToMeeting	X	X

Función	iOS	Android
Responder a invitaciones desde la pantalla de notificación o la pantalla de bloqueo	X	X
Marcar para entrar en reuniones de WebEx o Lync	X	X
Ocultar eventos rechazados	X	X
Mostrar más de 3 eventos simultáneos	X	X
Vista rápida del estado de los invitados	X	X
Eliminar, responder, responder a todos, agregar comentarios en eventos cancelados	X	X
Mostrar el nombre del organizador en invitaciones reenviadas	X	X
Dispositivos compartidos	X	X
Unirse a reuniones de Skype Empresarial	X	X
Responder a notificaciones de reunión (Aceptar, Rechazar y Provisional)	X	X
Responder a notificaciones de mensajes (Responder y Eliminar)	X	
Contactos		
Crear carpetas en **Contactos**		X
Sincronización bidireccional de contactos	X	X
Búsquedas de información de contacto detallada en la lista global de direcciones	X	X
Exportar contactos de Secure Mail a los contactos locales y sincronizarlos	X	X

Función	iOS	Android
Contactos: Favoritos y Categorías		X
Controlar qué campos de contacto se exportan	X	X
Datos de contactos que no son de Secure Mail	X	X
Tamaño de letra dinámico	X	X
Marcar contactos como VIP	X	X
Compartir contactos con `.vcards`	X	X
Ver contactos con presión larga		X
Exportar contactos, incluso aunque exista la cuenta nativa de correo electrónico	X	X
Ver carpetas y subcarpetas	X	
Parámetros configurados en el dispositivo		
Compatibilidad con iMessage	X	
Opciones avanzadas para controlar notificaciones	X	X
Control de notificación de pantalla bloqueada	X	X
Sonidos de notificaciones para correo y calendario	X	X
Actualizar automáticamente las carpetas	X	X
Establecer notificaciones de Fuera de la oficina, internas y externas	X	X
Preguntar antes de eliminar	X	X
Correos agrupados por conversación o vista cronológica	X	X
Cargar datos adjuntos en Wi-Fi	X	X

Función	iOS	Android
Definir la carga de adjuntos por Wi-Fi como parámetro predeterminado	X	X
Establecer el período sincronización de correo	X	X
Sincronización ilimitada / Sincronización de todo el correo		X
Establecer firma de correo electrónico	X	X
Mostrar contactos por nombre o por apellido	X	X
Avance automático	X	X
Usar hora local		X
Plantillas de respuesta rápida		X
Frecuencia de configuración de correo push		X
Exportar o importar la configuración	X	X
Tocar en el botón Atrás del dispositivo para descartar las opciones del botón de acción flotante		X
Microsoft Teams	X	X

Citrix Secure Web

Función	iOS	Android
Usar dos aplicaciones simultáneamente con Multitarea	X	
Descargar archivos	X	X
Agregar favoritos	X	X

Función	iOS	Android
Borrar contraseñas y nombres de usuario guardados	X	X
Eliminar caché/historial/cookies	X	X
Bloquear ventanas emergentes	X	X
Guardar páginas sin conexión	X	X
Buscar en la barra de direcciones	X	X
Abrir elementos descargados desde las notificaciones	X	X
Guardado automático de contraseñas	X	X
Compatibilidad con proxies		
Proxies de empresa	X	X
Listas de bloqueados y listas de permitidos de direcciones URL	X	X
Historial	X	X
Página de inicio predeterminada	X	X
Fichas	X	X
Inserción push de marcadores	X	X
Bloqueo de captura de pantalla		X
Buscar en la página actual	X	X
Acciones de 3D Touch	X	
Dispositivos compartidos	X	X
Protección frente a intentos de manipulación de archivos con dispositivos compartidos	X	
Exportar o importar la configuración	X	X
Modo horizontal y vertical	X	X
Android Enterprise (Android for Work)		X

Función	iOS	Android
Tirar para actualizar el contenido en pantalla	X	X
Secure Web como explorador predeterminado		X

Citrix Secure Hub

June 6, 2024

Citrix Secure Hub es el launchpad 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:**
>
> La compatibilidad con las versiones de Android 6.x e iOS 11.x de Secure Hub finalizó en octubre de 2023.

Novedades en la versión actual

Secure Hub para iOS 24.5.0

Compatible con Return to Service de iOS 17

Secure Hub admite la función Return to Service de iOS 17, que proporciona una experiencia de administración de dispositivos móviles (MDM) más eficiente y segura. Antes había que configurar manualmente para un nuevo usuario después de borrar el dispositivo. Ahora, la función Return to Service

automatiza este proceso, ya sea para reutilizar un dispositivo de la empresa o para integrar un dispositivo personal (BYOD) con las directivas de seguridad correctas.

Con la función Return to Service, el servidor de MDM puede enviar un comando de borrar que incluye detalles de Wi-Fi y un perfil de inscripción de MDM predeterminado al dispositivo del usuario. A continuación, el dispositivo borra automáticamente todos los datos del usuario, se conecta a la red Wi-Fi especificada y se vuelve a inscribir en el servidor de MDM usando el perfil de inscripción proporcionado.

Novedades en versiones anteriores

Secure Hub para Android 24.3.0

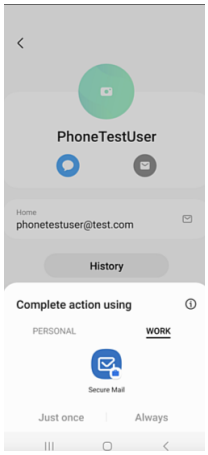
Compatible con Samsung Knox Enhanced Attestation v3 Secure Hub ahora es compatible con Samsung Enhanced Attestation v3 y aprovecha la atestación de Knox para reforzar las medidas de seguridad de los dispositivos Samsung administrados a través de Citrix Endpoint Management. Este protocolo de certificación avanzado verifica la integridad y el estado de seguridad de los dispositivos, asegurándose de que no están rooteados y de que ejecutan firmware autorizado. Esta función proporciona una capa esencial de protección contra las amenazas de seguridad y garantiza el cumplimiento de las directivas de seguridad empresariales.

Secure Hub para Android 23.12.0

Seguridad mejorada con Samsung Knox La incorporación de la directiva de dispositivos clave de Knox Platform for Enterprise en Citrix Endpoint Management mejora significativamente las funciones de seguridad de Secure Hub en los dispositivos Samsung. Esta directiva le permite proporcionar la información de licencia requerida de la plataforma Samsung Knox Platform for Enterprise (KPE) y utilizar las licencias de KPE para mejorar la seguridad de su dispositivo Samsung. Samsung Knox garantiza que los datos empresariales permanezcan protegidos y, al mismo tiempo, mantiene la facilidad de administración y una experiencia de usuario fluida.

Para obtener información, consulte Directiva de Knox Platform for Enterprise.

Acceda a Secure Mail desde el perfil personal del usuario Los usuarios ahora pueden acceder a Secure Mail y utilizarlo en su perfil de trabajo desde su perfil personal. Cuando los usuarios hacen clic en una dirección de correo electrónico de su libreta de direcciones de su perfil personal, tienen la opción de usar Secure Mail en su perfil de trabajo. Esta función ofrece más comodidad, ya que permite a los usuarios enviar un correo electrónico desde su perfil personal. Esta función es aplicable a dispositivos BYOD o WPCOD.



Secure Hub para iOS 24.1.0

En esta versión se han resuelto algunos problemas para mejorar la estabilidad y el rendimiento generales.

Secure Hub para Android 23.12.0

Agregue una sugerencia sobre el PIN de autenticación en la página de inicio de sesión A partir de la versión 23.12.0, puede agregar una sugerencia sobre el PIN de autenticación en la página de inicio de sesión. Esta función es opcional y se aplica a los dispositivos inscritos para la autenticación de dos factores. La sugerencia le permite saber cómo acceder al PIN.

Puede configurar una sugerencia como texto o enlace. El texto de la sugerencia ofrece información concisa sobre el PIN, mientras que el enlace proporciona información detallada sobre cómo acceder al PIN. Para obtener más información sobre cómo configurar una sugerencia, consulte Configurar la sugerencia a través de la consola de Citrix Endpoint Management.

Compatibilidad de la autenticación nFactor con la función de inicio de sesión único A partir de la versión 23.12.0 de Secure Hub para Android, la inscripción o el inicio de sesión de nFactor para la administración de aplicaciones móviles (MAM) admiten la función de inicio de sesión único (SSO). Esta función permite que las credenciales de inicio de sesión introducidas anteriormente pasen por el proceso de inscripción o inicio de sesión de MAM, lo que elimina la necesidad de que los usuarios las introduzcan manualmente de nuevo. Para obtener más información sobre la propiedad nFactor SSO, consulte la referencia a la propiedad del cliente en la documentación de Citrix Endpoint Management.

Compatibilidad con borrado completo en modo de arranque directo Anteriormente, era necesario desbloquear el dispositivo para ejecutar un comando de borrado completo en un dispositivo

reiniciado. Ahora se puede ejecutar un comando de borrado completo en modo de arranque directo, incluso si el dispositivo está bloqueado. Esta función es útil desde el punto de vista de la seguridad, especialmente cuando el dispositivo está en poder de una persona no autorizada. Para obtener más información sobre el comando de borrado completo, consulte Acciones de seguridad en la documentación de Citrix Endpoint Management.

Se ha optimizado la velocidad de carga de la App Store de Secure Hub La App Store de Secure Hub ahora se carga más rápido que antes, lo que permite a los usuarios acceder a ella con mayor rapidez.

Secure Hub para iOS 23.11.0

Agregue una sugerencia sobre el PIN de autenticación en la página de inicio de sesión A partir de la versión 23.11.0, puede agregar una sugerencia sobre el PIN de autenticación en la página de inicio de sesión. Esta función es opcional y se aplica a los dispositivos inscritos para la autenticación de dos factores. La sugerencia le permite saber cómo acceder al PIN.

Puede configurar una sugerencia como texto o enlace. El texto de la sugerencia ofrece información concisa sobre el PIN, mientras que el enlace proporciona información detallada sobre cómo acceder al PIN. Para obtener más información sobre cómo configurar una sugerencia, consulte el artículo Configurar la sugerencia a través de la consola de Citrix Endpoint Management .

Compatibilidad de la autenticación nFactor con la función de inicio de sesión único A partir de la versión 23.11.0 de Secure Hub para iOS, se garantiza compatibilidad de la inscripción o el inicio de sesión de nFactor para la administración de aplicaciones móviles (MAM) con la función de inicio de sesión único (SSO). Esta función permite que las credenciales de inicio de sesión introducidas anteriormente pasen por el proceso de inscripción o inicio de sesión de MAM, lo que elimina la necesidad de que los usuarios las introduzcan manualmente de nuevo.

Para obtener más información sobre la propiedad nFactor SSO, consulte la referencia a la propiedad del cliente en la documentación de Citrix Endpoint Management.

Secure Hub 23.10.0

Secure Hub para Android

Secure Hub para Android 23.10.0 es compatible con Android 14. La actualización de la versión 23.10.0 de Secure Hub garantiza la asistencia ininterrumpida para los dispositivos que se actualicen a Android 14.

Secure Hub 23.9.0

Secure Hub para Android

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Secure Hub 23.8.1

Secure Hub para iOS En esta versión se han resuelto algunos problemas para mejorar la estabilidad y el rendimiento generales.

Secure Hub 23.8.0

Secure Hub para iOS En esta versión se han resuelto algunos problemas para mejorar la estabilidad y el rendimiento generales.

Secure Hub 23.7.0

Secure Hub para Android

API Play Integrity Google pronto dejará de usar la API de SafetyNet Attestation y migrará a la API de Play Integrity sugerida.

Para obtener más información, consulte Play Integrity API en la documentación de Citrix Endpoint Management.

Para obtener información sobre la retirada de productos, consulte Elementos eliminados y obsoletos en la documentación de Citrix Endpoint Management.

Para obtener más información sobre la función SafetyNet de Android, consulte SafetyNet

Secure Hub 23.4.0

Secure Hub para iOS

Experiencia de usuario mejorada A partir de la versión 23.4.0, Secure Hub para iOS mejora estos aspectos de la experiencia de usuario:

- Experiencia en los almacenes:

  Antes, la página Mis aplicaciones aparecía primero. Con la versión 23.4.0, la página Almacén aparece primero.

  Antes, el almacén de Secure Hub realizaba la acción de recarga cada vez que el usuario hacía clic en la opción Almacén.

  Con la versión 23.4.0, se mejora la experiencia de usuario. Ahora, la aplicación se carga de nuevo cuando el usuario la inicia por primera vez, la reinicia o desliza el dedo hacia abajo por la pantalla.

- Interfaz de usuario: Antes, la opción Cerrar sesión se encontraba en la parte inferior izquierda de la pantalla. En la versión 23.4.0, la opción Cerrar sesión forma parte del menú principal y está por encima de la opción Acerca de.
- Hipervínculos: Antes, los hipervínculos de la página de detalles de la aplicación aparecían como texto sin formato. Con la versión 23.4.0, se puede hacer clic en los hipervínculos, y estos tienen un formato de subrayado para indicar que son enlaces.

Experiencia en la transición de MDX al SDK de MAM A partir de la versión 23.4.0, la experiencia en la transición del MDX antiguo al SDK de MAM se ha mejorado para las aplicaciones de modo dual de iOS. Esta función mejora la experiencia de usuario al usar aplicaciones móviles de productividad, ya que reduce los mensajes de alerta y cambia a Secure Hub.

Usar el PIN de Citrix para desbloquear aplicaciones Antes, el usuario final introducía el código de acceso del dispositivo para desbloquear aplicaciones basadas en la administración de aplicaciones móviles (MAM).

A partir de la versión 23.4.0, el usuario final puede introducir el PIN de Citrix como código de acceso para desbloquear aplicaciones basadas en MAM. Los administradores pueden configurar la complejidad del código de acceso mediante las propiedades de cliente en el servidor de CEM.

Cuando la aplicación esté inactiva durante más tiempo del permitido, los usuarios finales pueden introducir el PIN de Citrix para desbloquear la aplicación en función de la configuración establecida por los administradores.

Para Secure Hub para Android, hay una propiedad de cliente independiente para configurar cómo gestionar el temporizador de inactividad en las aplicaciones de MAM. Para obtener más información, consulte Temporizador de inactividad independiente para Android.

Secure Hub 23.4.1

Secure Hub para Android En esta versión se han resuelto algunos problemas para mejorar la estabilidad y el rendimiento generales.

Secure Hub 23.4.0

Secure Hub para Android En esta versión se han resuelto algunos problemas para mejorar la estabilidad y el rendimiento generales.

Secure Hub 23.2.0

Secure Hub para Android

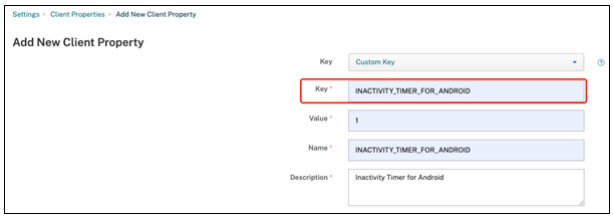
> **Nota:**
>
> - No se recopilan datos analíticos de los usuarios de la Unión Europea (UE) ni del Espacio Económico Europeo (EEE) ni de Suiza ni del Reino Unido.

VPN en modo túnel completo de MDX La micro VPN de MDX (modo túnel completo) se ha retirado.

Para obtener más información, consulte Elementos retirados en la documentación de Citrix Endpoint Management.

Temporizador de inactividad independiente para Android Antes, la propiedad de cliente **Temporizador de inactividad** era común en Secure Hub para Android e iOS.

A partir de la versión 23.2.0, un administrador de TI puede usar la nueva propiedad de cliente **Inactivity_Timer_For_Android** para separar el temporizador de inactividad de iOS. Un administrador de TI puede establecer el **valor** de **Inactivity_Timer_For_Android** en 0 para inhabilitar el temporizador de inactividad de Android de forma independiente. De esta forma, todas las aplicaciones del perfil de trabajo, incluida Secure Hub, desafían únicamente el PIN de trabajo.



Para obtener más información sobre cómo agregar y modificar una propiedad de cliente, consulte Propiedades de cliente en la documentación de XenMobile.

Secure Hub 22.11.0

Secure Hub para Android Esta versión incluye correcciones de errores.

Secure Hub 22.9.0

Secure Hub para Android Esta versión incluye:

- Complejidad del código de acceso del dispositivo (a partir de Android 12)
- Compatibilidad con SDK 31
- Problemas resueltos

Complejidad del código de acceso del dispositivo (a partir de Android 12) Se prefiere la complejidad del código de acceso a un requisito de contraseña personalizado. El nivel de complejidad del código de acceso es uno de los niveles predefinidos. Por lo tanto, el usuario final no puede establecer una contraseña con un nivel de complejidad inferior.

La complejidad del código de acceso para dispositivos con Android 12 o una versión posterior es la siguiente:

- **Aplicar complejidad de código de acceso:** Requiere una contraseña con un nivel de complejidad definido por la plataforma en lugar de un requisito de contraseña personalizado. Solo para dispositivos con Android 12 o una versión posterior y Secure Hub 22.9 o una versión posterior.
- **Nivel de complejidad:** Niveles predefinidos de complejidad de contraseñas.
  - **Nada:** No se requiere contraseña.
  - **Baja:** Las contraseñas pueden ser:
    - Un patrón
    - Un PIN con un mínimo de cuatro números
  - **Media:** Las contraseñas pueden ser:
    - Un PIN sin secuencias repetidas (4444) ni secuencias ordenadas (1234) y con un mínimo de cuatro números
    - Letras con un mínimo de cuatro caracteres
    - Letras y números con un mínimo de cuatro caracteres
  - **Alta:** Las contraseñas pueden ser:
    - Un PIN sin secuencias repetidas (4444) ni secuencias ordenadas (1234) y con un mínimo de ocho números
    - Letras con un mínimo de seis caracteres
    - Letras y números con un mínimo de seis caracteres

> **Notas:**
>
> - Para los dispositivos BYOD, los parámetros del código de acceso, como la longitud mínima, los caracteres obligatorios, el reconocimiento biométrico y las reglas avanzadas, no se aplican a partir de Android 12. En su lugar, utilice la complejidad de códigos de acceso.
> - Si la complejidad del código de acceso para el perfil de trabajo está habilitada, también debe estar habilitada la complejidad del código de acceso para el dispositivo.

Para obtener más información, consulte Parámetros de Android Enterprise en la documentación de Citrix Endpoint Management.

Secure Hub 22.7.0

Secure Hub para Android Esta versión incluye correcciones de errores.

Secure Hub 22.6.0

Secure Hub para Android Esta versión incluye correcciones de errores.

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 de aplicaciones, 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.

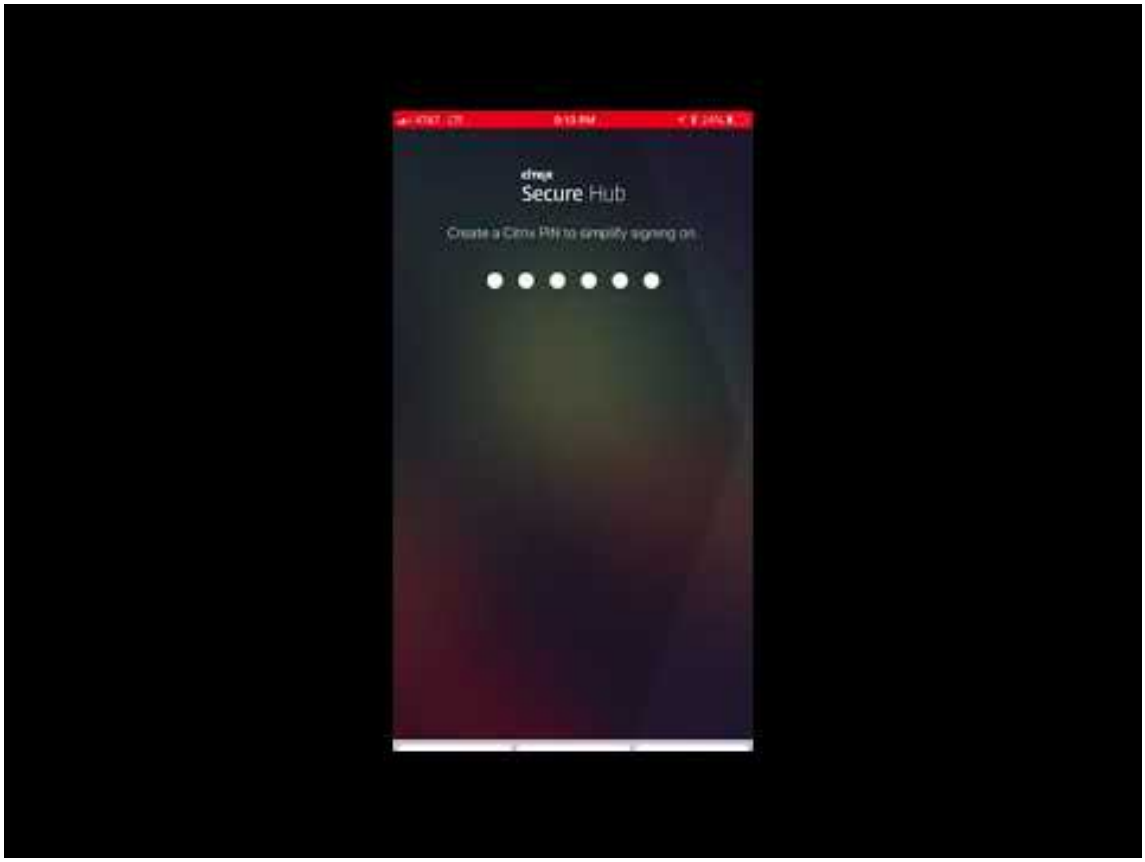
- **Disponibilidad de Android SafetyNet:** Puede configurar Endpoint Management para utilizar la funcionalidad **Android SafetyNet** para evaluar la compatibilidad y la seguridad de los dispositivos Android que tienen Secure Hub instalado. Los resultados se pueden utilizar para desencadenar acciones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

> comienda que inhabilite la integración de Citrix Files en la consola de Endpoint Management 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.

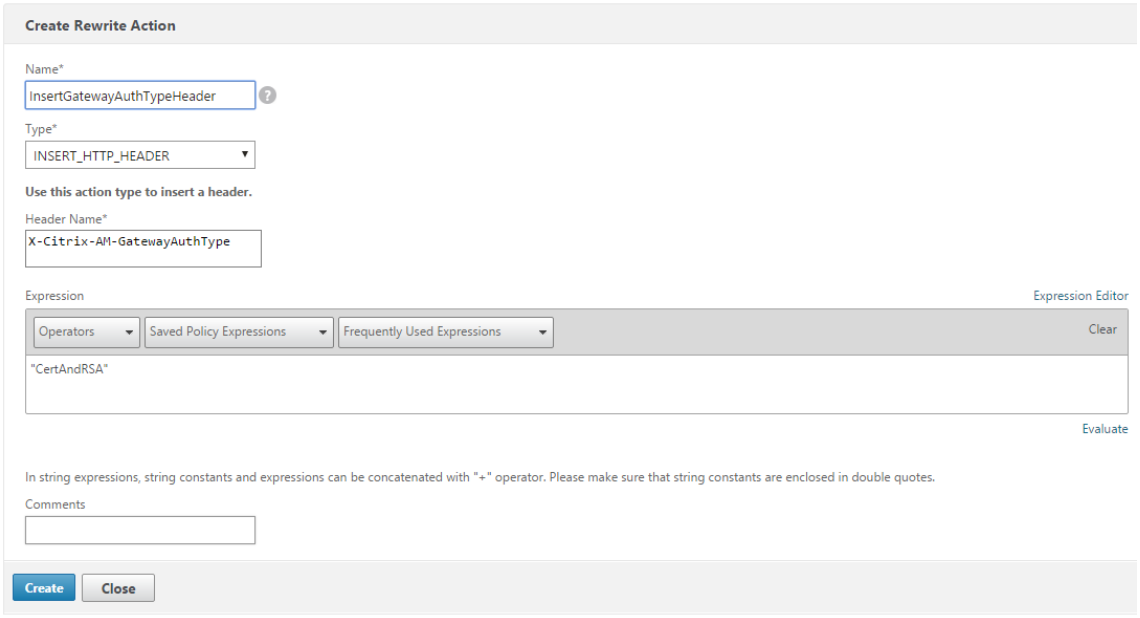
Para que Secure Hub use el tipo de autenticación "certificado + contraseña de un solo uso", agregue una acción de reescritura y una directiva de reescritura en Citrix ADC que inserte un encabezado de respuesta personalizado del formulario **X-Citrix-AM-GatewayAuthType: CertAndRSA** para indicar el tipo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

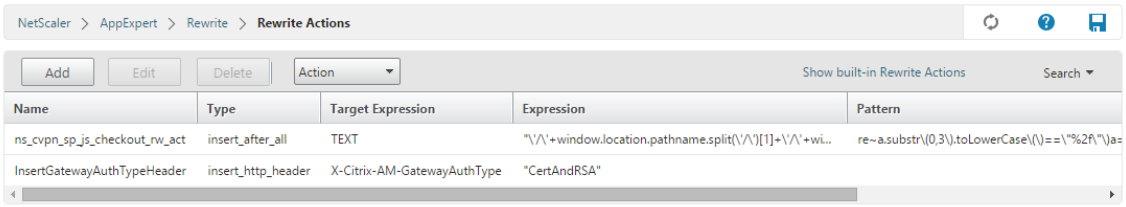
> **Nota:**
>
> Si se definen tipos de inicio de sesión diferentes para Endpoint Management y Citrix ADC, la configuración de Citrix ADC prevalece. Para obtener más información, consulte Citrix Gateway y Endpoint Management.

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

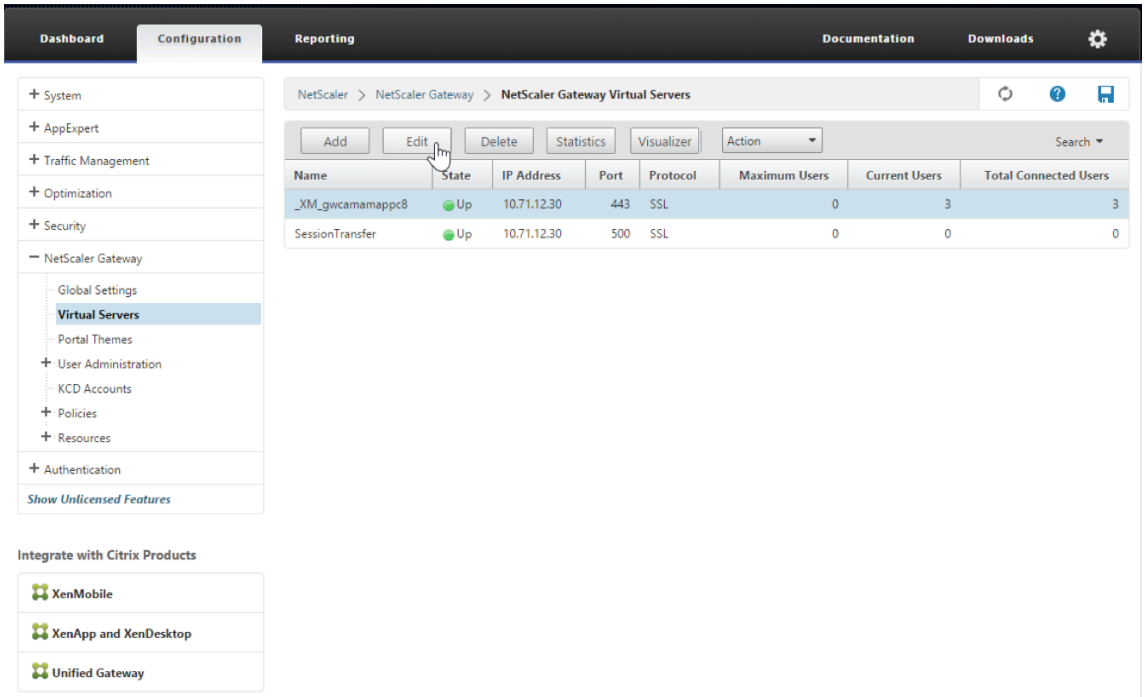
   Aparecerá la pantalla **Create Rewrite Action**.
3. Rellene los campos como se muestra en la siguiente imagen y, a continuación, haga clic en **Create**.



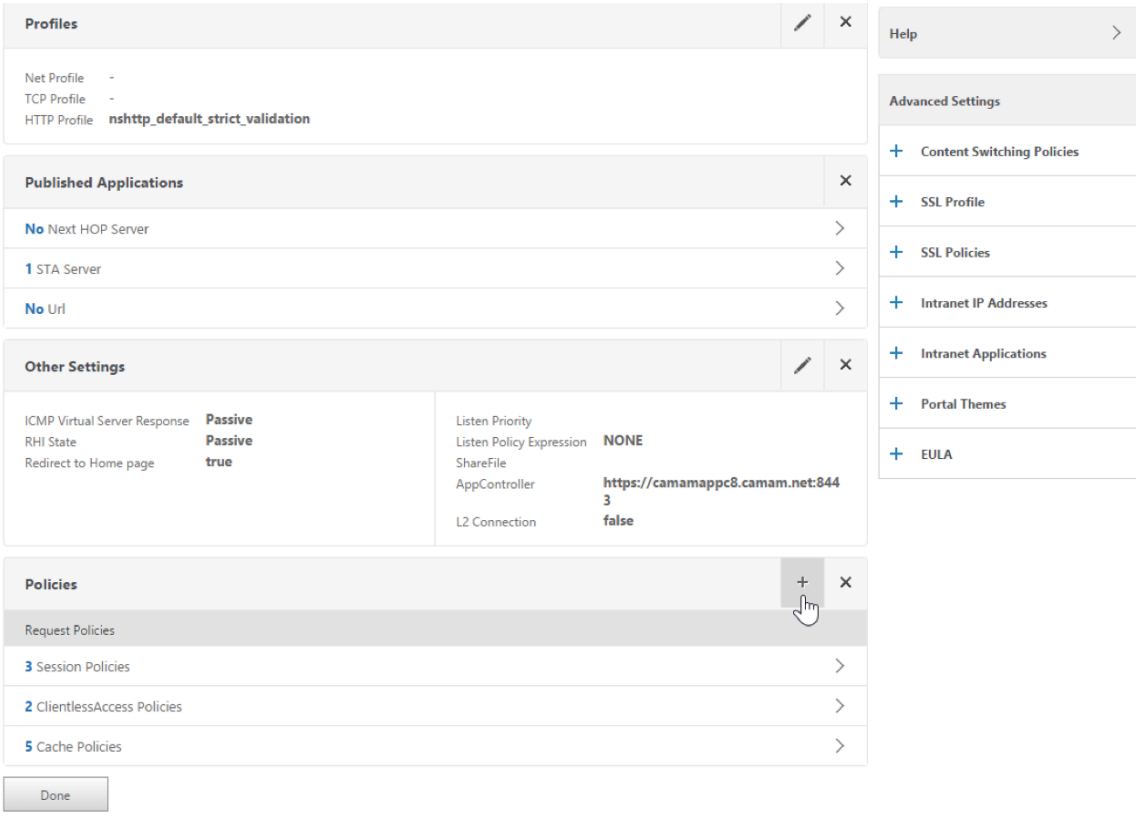
Aparece este resultado en la pantalla principal **Rewrite Actions**.



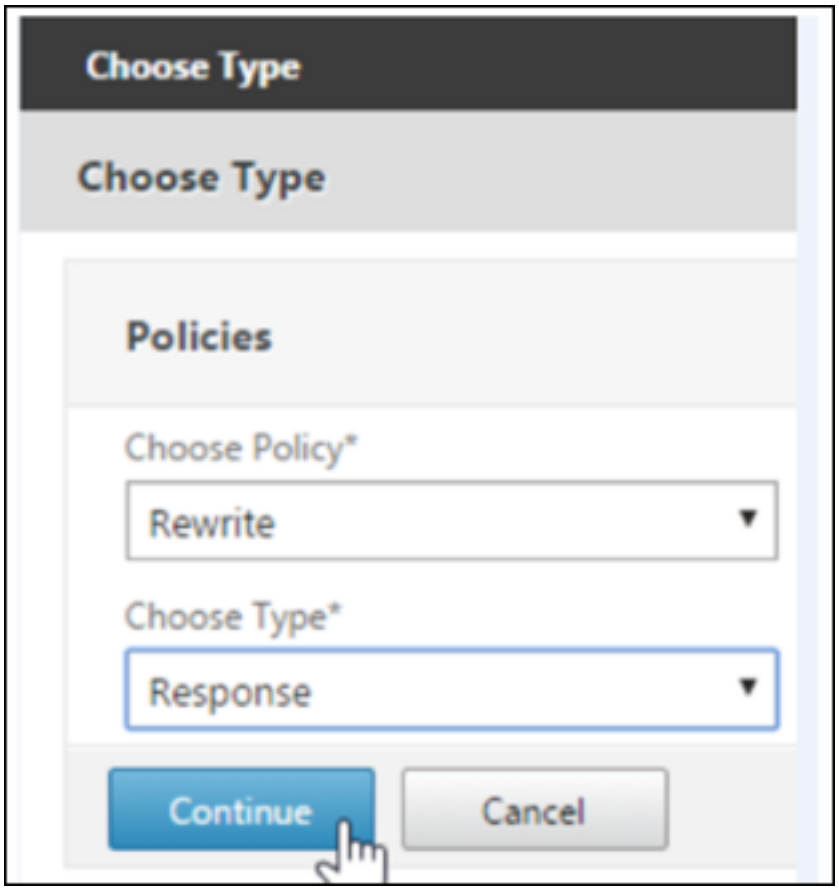
4. Vincule la acción de reescritura al servidor virtual como una directiva de reescritura. Vaya a **Configuration > NetScaler Gateway > Virtual Servers** y seleccione el servidor virtual.



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

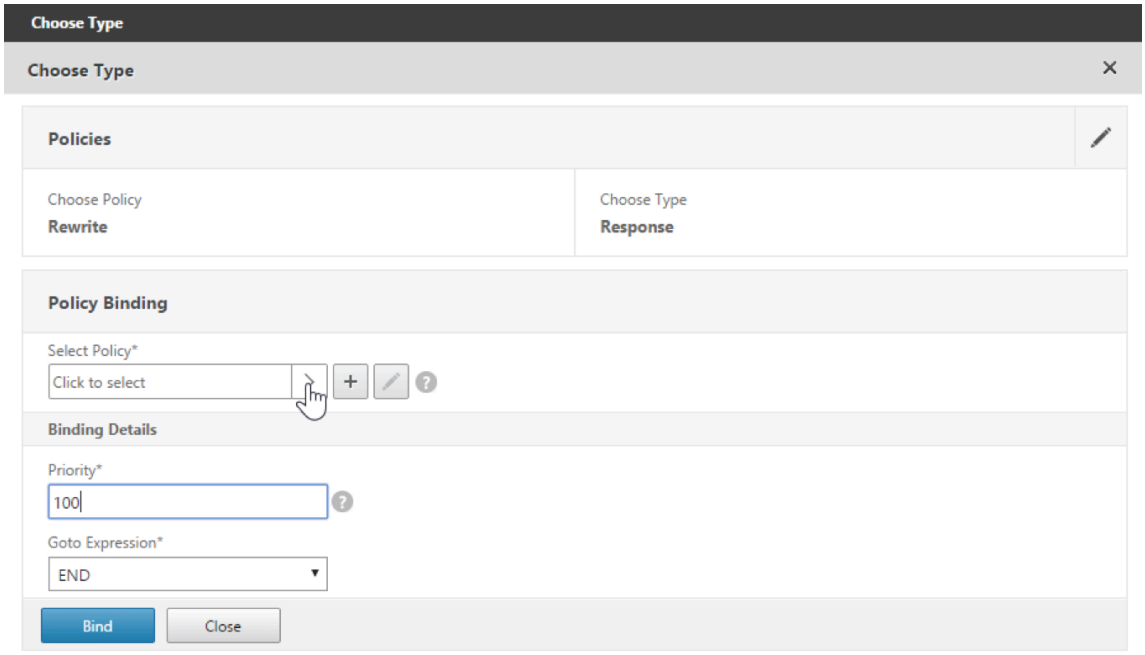


8. En el campo **Choose Policy**, elija **Rewrite**.
9. En el campo **Choose Type**, elija **Response**.



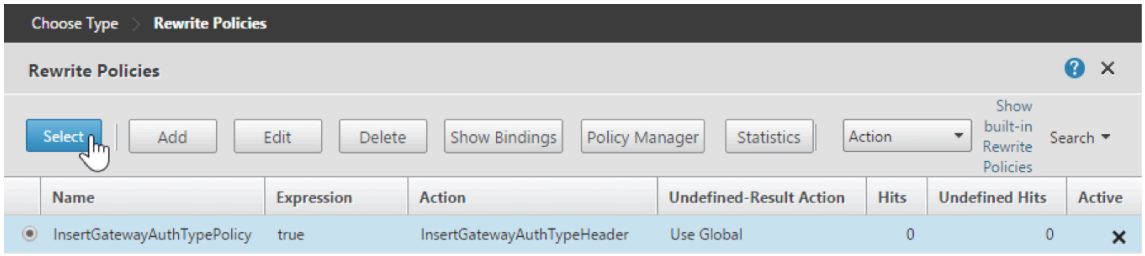
10. Haga clic en **Continuar**.

    Se expande la sección **Policy Binding**.

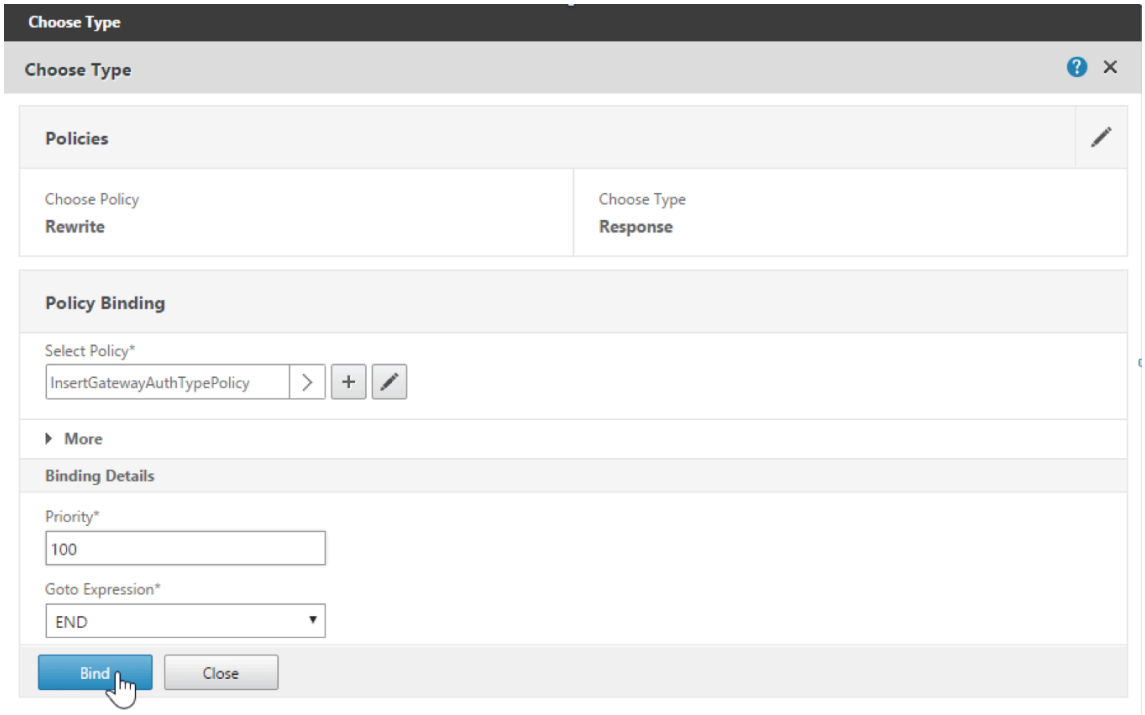


11. Haga clic en **Select Policy**.

    Aparecerá una pantalla con las directivas disponibles.

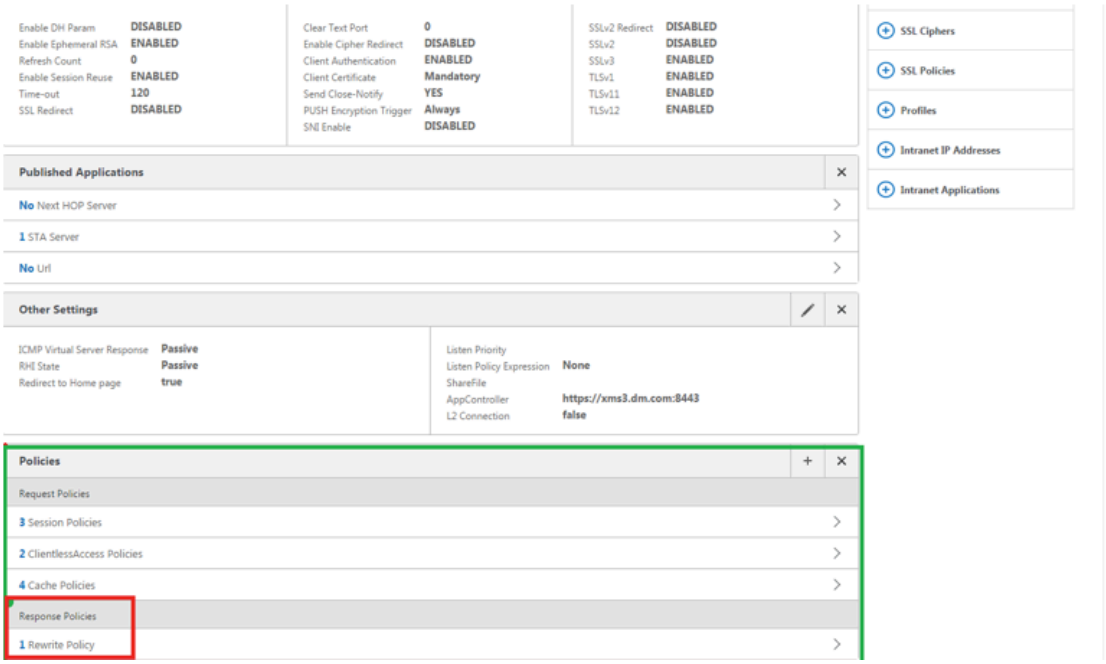


12. Haga clic en la fila de la directiva que acaba de crear y, a continuación, haga clic en **Select**. Aparece de nuevo la pantalla **Policy Binding**, con la directiva seleccionada.

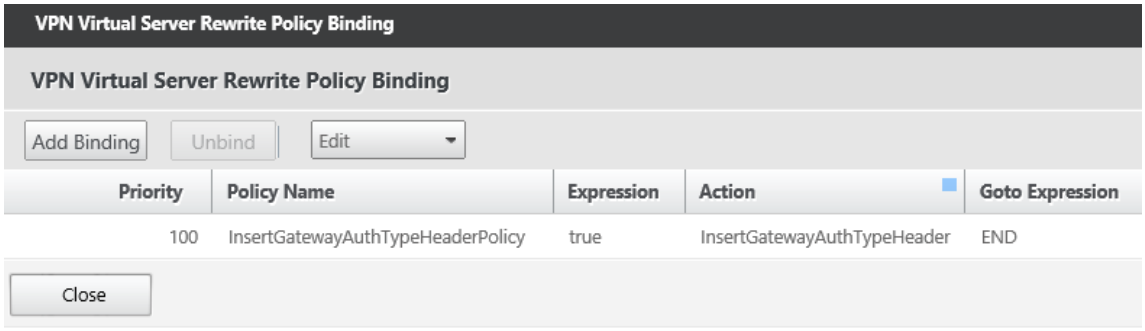


13. Haga clic en **Bind**.

    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 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	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 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

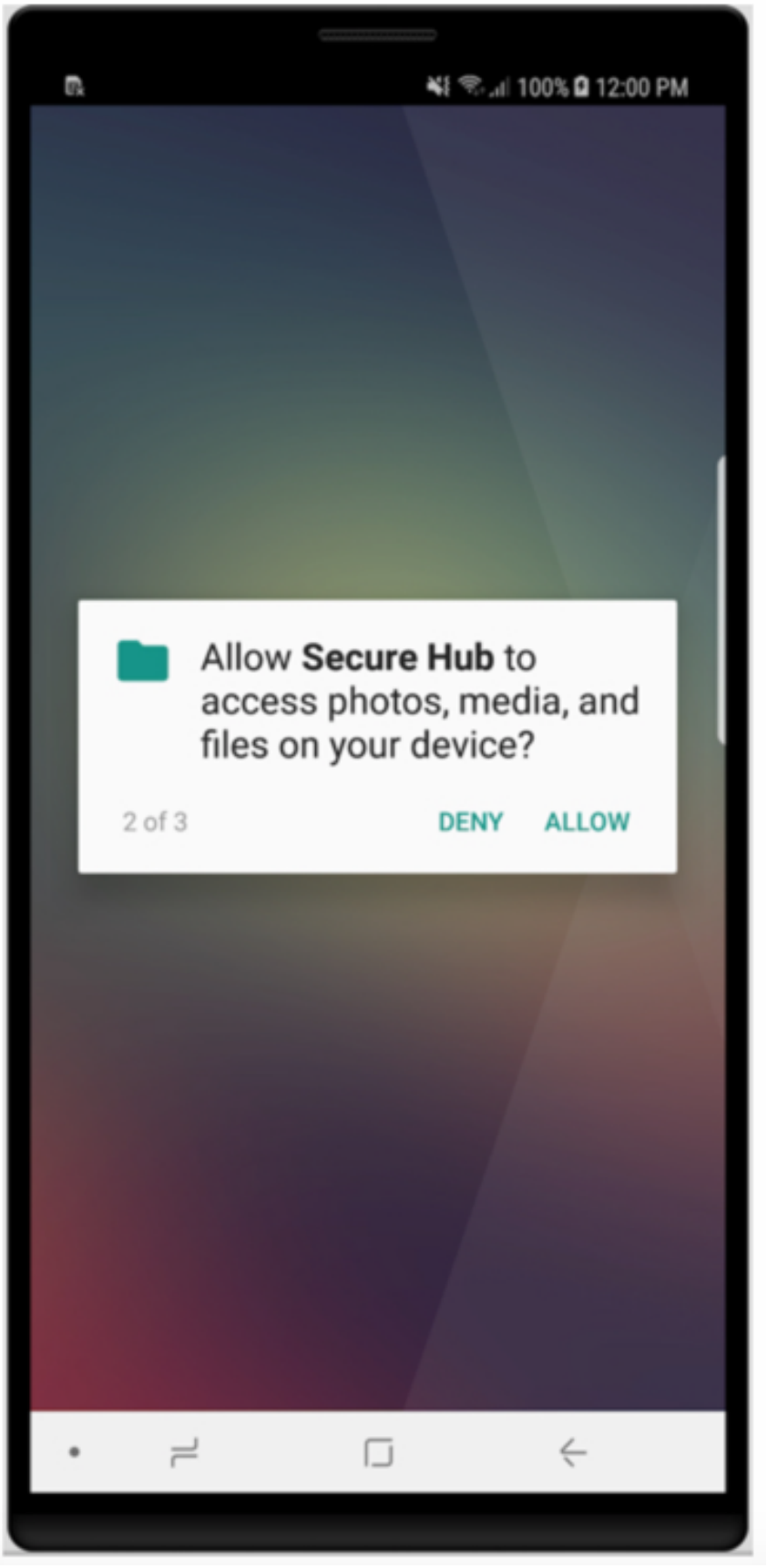
Los usuarios empiezan por descargar Secure Hub en sus dispositivos desde las tiendas de aplicaciones de Apple o Android.

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.

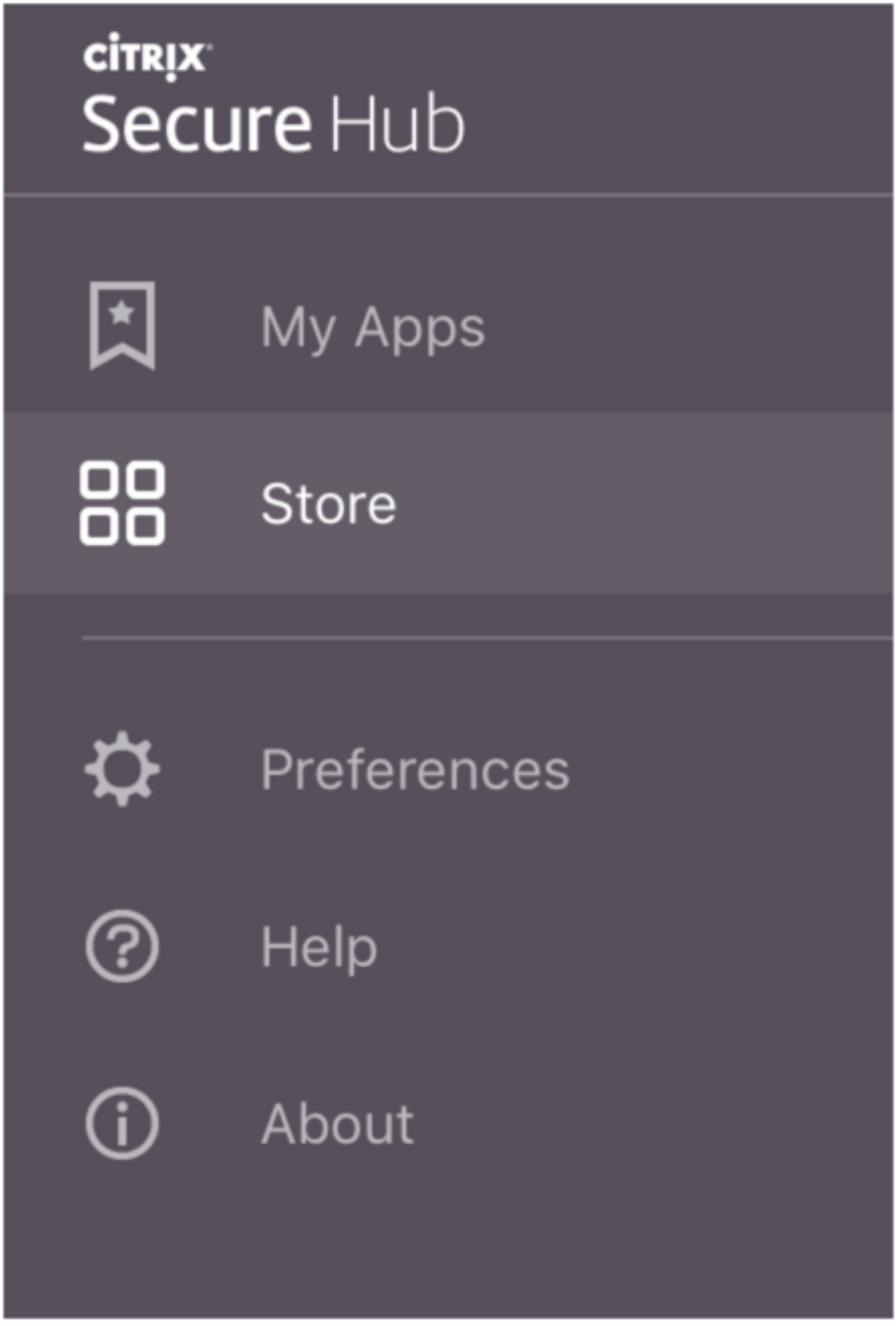
En Secure Hub para Android, durante la instalación inicial y la inscripción, aparece este mensaje: ¿Permitir que Secure Hub acceda a fotos, archivos multimedia y archivos en su dispositivo?

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.

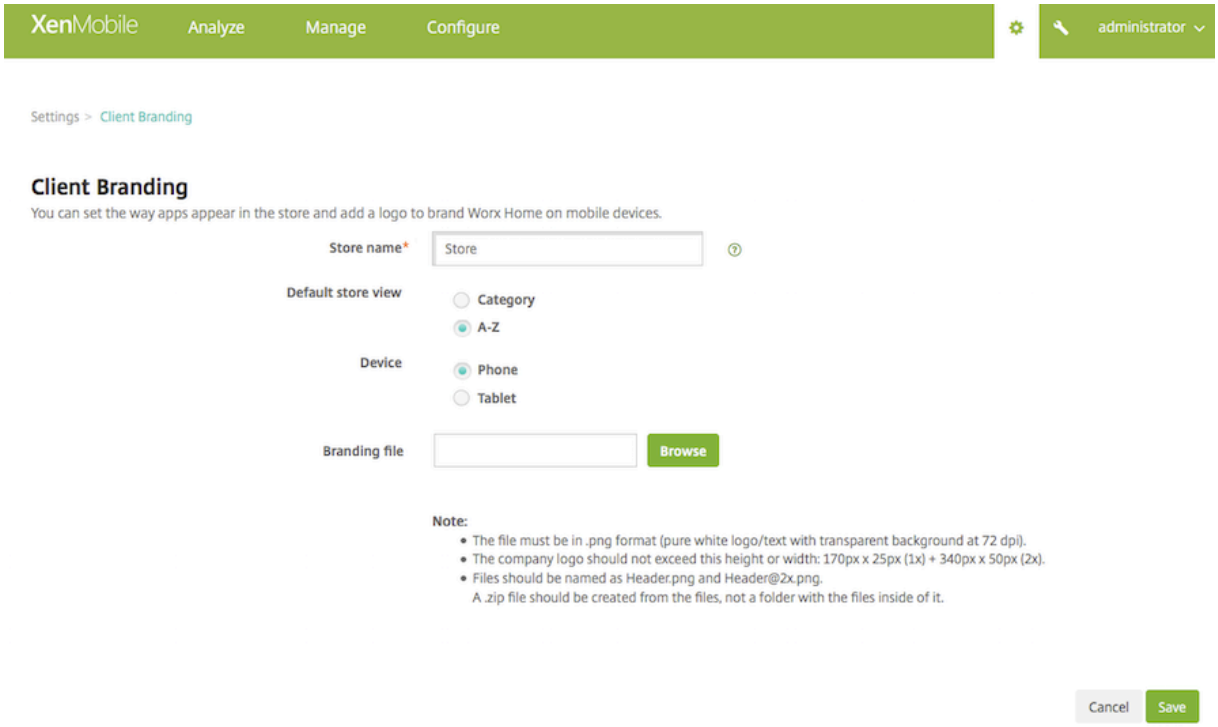
La primera vez que se usa Secure Mail, este obtiene el ID, el dominio y la dirección de correo electrónico del usuario desde Secure Hub. Secure Mail usa la dirección de correo electrónico para la detección automática. El servidor Exchange se identifica con el dominio y el ID del usuario, lo que permite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

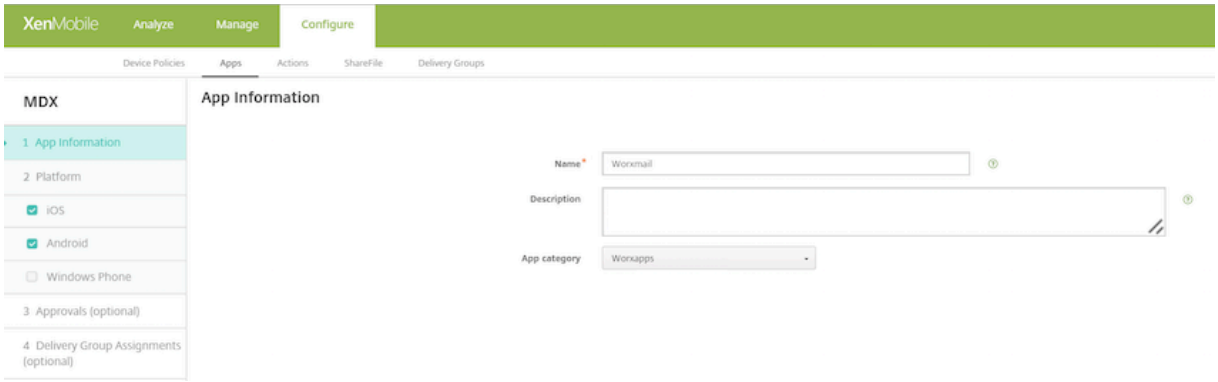
- La propiedad de servidor MAM_MACRO_SUPPORT. Para obtener instrucciones, consulte Propiedades de servidor.
- Las propiedades de cliente ENABLE_CREDENTIAL_STORE y SEND_LDAP_ATTRIBUTES. Para obtener instrucciones, consulte Propiedades de cliente.

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**.

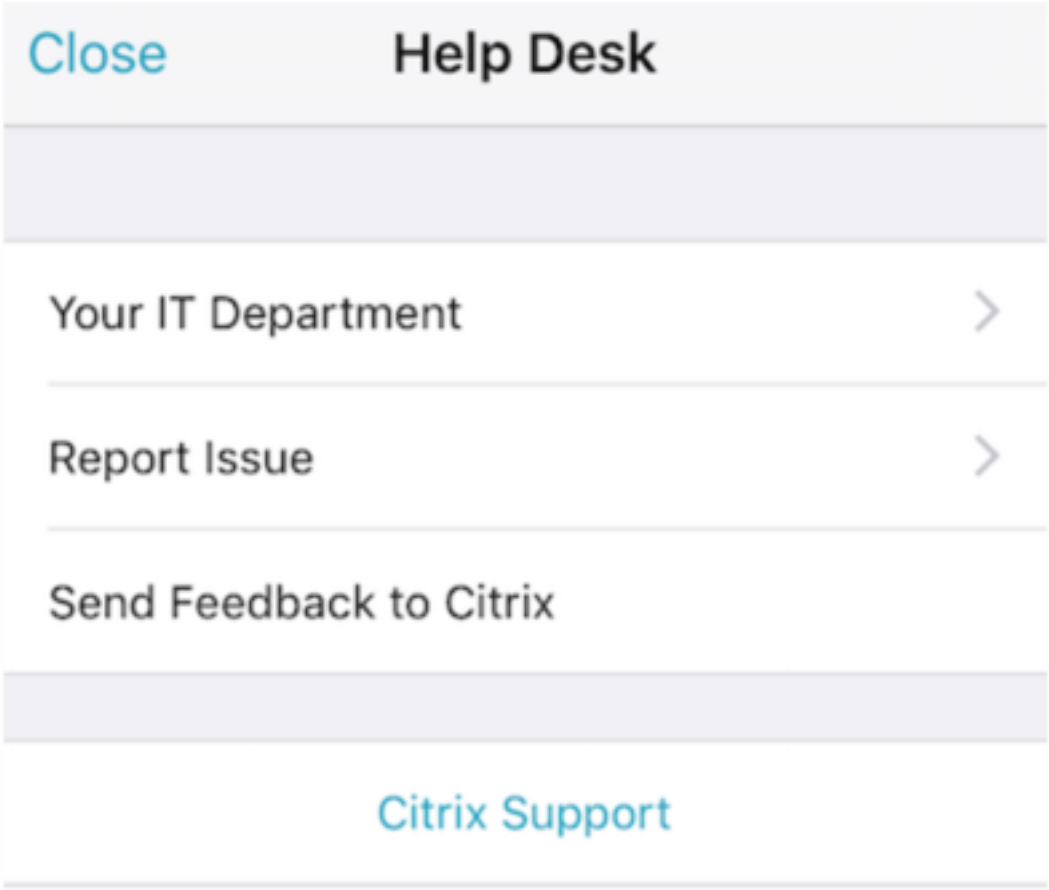


En el almacén de aplicaciones, los usuarios pueden explorar solo las aplicaciones y los escritorios que usted haya configurado y protegido en Endpoint Management. Para agregar la aplicación, los usuarios deben tocar en **Detalles** y, luego, en **Agregar**.

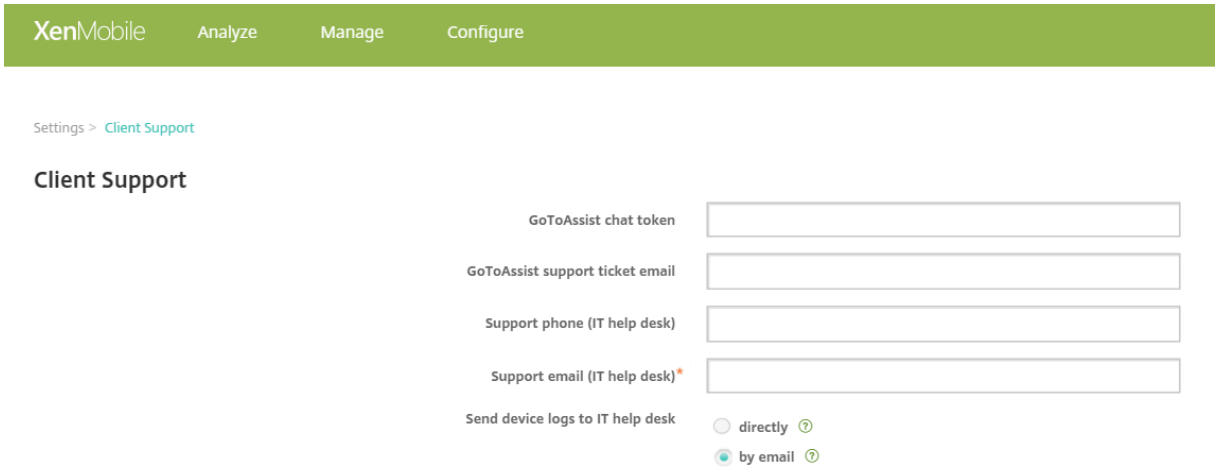
Opciones de Ayuda configuradas

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.

Generar registros del lado del dispositivo para Secure Hub

En esta sección se explica cómo generar los registros del lado del dispositivo de Secure Hub y cómo configurar el nivel de depuración correcto en ellos.

Para obtener registros de Secure Mail, haga lo siguiente:

1. Vaya a **Secure Hub > Ayuda > Notificar problema**. Seleccione Secure Mail de la lista de aplicaciones.
   Se abrirá un mensaje de correo electrónico dirigido al servicio de asistencia.
2. Cambie la configuración de registros solo si el equipo de asistencia se lo indica. Confirme siempre que los parámetros están bien configurados.
3. Vuelva a Secure Mail y reproduzca el problema. Anote la hora a la que comenzó a reproducirse el problema y la hora en que se produjo o se mostró el mensaje de error.
4. Vuelva a **Secure Hub > Ayuda > Notificar problema**. Seleccione Secure Mail de la lista de aplicaciones.
   Se abrirá un mensaje de correo electrónico dirigido al servicio de asistencia.
5. Introduzca el asunto y describa brevemente el problema en el cuerpo del mensaje. Incluya las marcas de hora recopiladas en el paso 3 y haga clic en **Enviar**.
   Se abrirá el mensaje escrito con registros comprimidos como archivos adjuntos.
6. Vuelva a hacer clic en **Enviar**.

   Los archivos ZIP enviados incluyen los siguientes registros:

   - CtxLog_AppInfo.txt (iOS), Device_And_AppInfo.txt (Android), logx.txt y WH_logx.txt (Windows Phone)

   Los registros de información de la aplicación incluyen información acerca del dispositivo y la aplicación.

Introducción a Secure Mail

June 6, 2024

Citrix Secure Mail permite a los usuarios administrar su correo electrónico, su calendario y sus contactos en sus teléfonos móviles y tabletas. Para mantener la continuidad con las cuentas de Microsoft Outlook o IBM Notes, Secure Mail se sincroniza con Microsoft Exchange Server e IBM Notes Traveler Server.

Como parte de la familia de aplicaciones de Citrix, Secure Mail es compatible con Single Sign-On en Citrix Secure Hub. Una vez que los usuarios inician sesión en Secure Hub, pueden pasar directamente a Secure Mail sin tener que volver a introducir su nombre de usuario y contraseña. Puede configurar Secure Mail para que se instale automáticamente en los dispositivos de los usuarios cuando se inscriban en Secure Hub, o bien, puede dejar que sean los usuarios quienes agreguen la aplicación desde el Store.

> **Nota:**
>
> Exchange Server 2010 dejó de admitirse el 13 de octubre de 2020.

Secure Mail es compatible con:

- Exchange Server 2019 Cumulative Update 14
- Exchange Server 2019 Cumulative Update 13
- Exchange Server 2019 Cumulative Update 12
- Exchange Server 2019 Cumulative Update 11
- Exchange Server 2019 Cumulative Update 10
- Exchange Server 2019 Cumulative Update 9
- Exchange Server 2019 Cumulative Update 8
- Exchange Server 2019 Cumulative Update 7
- Exchange Server 2019 Cumulative Update 6
- Exchange Server 2016 Cumulative Update 23
- Exchange Server 2016 Cumulative Update 22
- Exchange Server 2016 Cumulative Update 21
- Exchange Server 2016 Cumulative Update 20
- Exchange Server 2016 Cumulative Update 19
- Exchange Server 2016 Cumulative Update 18
- Exchange Server 2016 Cumulative Update 17
- Exchange Server 2013 Cumulative Update 23
- Exchange Server 2013 Cumulative Update 22
- Exchange Server 2013 Cumulative Update 21
- HCL Domino versión 12.0.2 FP2
- HCL Traveler versión 12.0.2.1 Compilación 202302010413_30
- HCL Domino 11 (antes denominado Lotus Notes)
- HCL Domino 10.0.1 (antes denominado Lotus Notes)
- HCL Domino 9.0.1 FP10 HF197 (antes denominado Lotus Notes)
- HCL Domino 10.0.1.0, compilación 201811191126_20 (antes denominado Lotus Notes)
- HCL Domino 9.0.1.21 (antes denominado Lotus Notes)
- Microsoft Office 365 (Exchange Online)

Para comenzar, descargue Secure Mail y otros componentes de Endpoint Management desde la

página de descargas de Citrix Endpoint Management.

Para conocer los requisitos del sistema de Secure Mail y otras aplicaciones móviles de productividad, consulte Requisitos del sistema.

Para obtener más información acerca de las notificaciones en Secure Mail para iOS y Android cuando la aplicación está cerrada o se ejecuta en segundo plano, consulte Notificaciones push para Secure Mail.

Para conocer las funciones de iOS admitidas en Secure Mail, consulte Funciones de iOS para Secure Mail.

Para conocer las funciones de Android admitidas en Secure Mail, consulte Funciones de Android para Secure Mail.

Para conocer las funciones de iOS y Android admitidas en Secure Mail, consulte Funciones de iOS y Android para Secure Mail.

Para ver documentación de ayuda para usuarios, consulte la página Citrix Secure Mail del Centro de ayuda para usuarios de Citrix.

Citrix Secure Web

July 15, 2023

Citrix Secure Web es un explorador web para dispositivos móviles compatible con HTML5 que ofrece acceso seguro a sitios web internos y externos. Puede configurar Secure Web para que se instale automáticamente en los dispositivos de los usuarios cuando se inscriban en Secure Hub. Alternativamente, puede agregar la aplicación desde el almacén de aplicaciones de Endpoint Management.

Para conocer los requisitos del sistema para Secure Web y otras aplicaciones móviles de productividad, consulte Requisitos del sistema.

Integrar y entregar Secure Web

> **Nota:**
>
> MDX Toolkit 10.7.10 es la última versión que admite el empaquetado de aplicaciones móviles de productividad. Los usuarios pueden acceder a las versiones de las aplicaciones móviles de productividad 10.7.5 y posteriores desde los almacenes públicos de aplicaciones.

Para integrar y entregar Secure Web, siga estos pasos generales:

1. Para habilitar Single Sign-On (SSO) en la red interna, configure Citrix Gateway.

   Para el tráfico HTTP, Citrix ADC puede proporcionar SSO para todos los tipos de autenticación de proxy admitidos en Citrix ADC. Para el tráfico HTTPS, la directiva de caché de contraseñas web permite a Secure Web autenticar y proporcionar SSO al servidor proxy a través de MDX. MDX solo admite autenticación de proxy básica, implícita y NTLM. La contraseña se almacena en caché mediante MDX y se guarda en la caja fuerte compartida de Endpoint Management, que es una zona de almacenamiento segura para datos confidenciales de aplicación. Para obtener más información acerca de la configuración de Citrix Gateway, consulte Citrix Gateway.

2. Descargue Secure Web.
3. Determine cómo desea configurar las conexiones de usuario a la red interna.
4. Agregue Secure Web a Endpoint Management siguiendo los mismos pasos que se siguen para agregar otras aplicaciones MDX y después configure las directivas MDX. Para obtener más información acerca de las directivas específicas de Secure Web, consulte "Acerca de las directivas de Secure Web"más adelante en este artículo.

Configurar conexiones de usuario

Secure Web admite las siguientes configuraciones para las conexiones de usuario:

- **Túnel - SSO web:** Las conexiones por túnel con la red interna pueden utilizar una variante de VPN sin cliente, conocida como SSO web en túnel. Esta es la configuración predeterminada para la directiva **Modo preferido de VPN**. SSO web en túnel es la configuración recomendada para conexiones que requieren Single Sign-On (SSO).
- **Túnel VPN completo:** Las conexiones por túnel a la red interna pueden usar un túnel VPN completo, configurado en la directiva **Modo preferido de VPN**. Se recomienda la opción "Túnel VPN completo"para conexiones que usan certificados de cliente o SSL de extremo a extremo con un recurso de la red interna. Sin embargo, Secure Web no es una aplicación que pueda leer certificados de cliente almacenados en un dispositivo móvil. Es posible que se instalen algunas aplicaciones empresariales empaquetadas de terceros que puedan ofrecer esta función. El túnel VPN completo gestiona cualquier protocolo por TCP y se puede usar con equipos con Windows y Mac, así como con dispositivos iOS y Android.
- La directiva **Permitir cambio de modo VPN** permite cambiar automáticamente entre el modo "Túnel VPN completo"y el modo "SSO web en túnel", según sea necesario. De manera predeterminada, esta directiva está desactivada. Si la directiva está activada, las solicitudes de red que no llegan a realizarse debido a una solicitud de autenticación que no se puede resolver en el modo preferido de VPN se vuelven a intentar en el modo alternativo. Por ejemplo, los desafíos de servidor ante certificados de cliente pueden aceptarse en el modo "Túnel VPN completo" , pero no si se utiliza el modo "SSO web en túnel". Del mismo modo, los desafíos de autenti-

cación HTTP son más propensos a resolverse con SSO cuando se utiliza el modo SSO web en túnel.

En la tabla siguiente, se indica si Secure Web pide credenciales al usuario en función de la configuración y del tipo de sitio:

Modo de conexión	Tipo de sitio	Caché de contraseñas	Single Sign-On configurado para Citrix Gateway	Secure Web pide credenciales en el primer acceso a un sitio web	Secure Web pide credenciales en un acceso posterior al sitio web	Secure Web pide credenciales después de un cambio de contraseña
SSO web en túnel	HTTP	No	Sí	No	No	No
SSO web en túnel	HTTPS	No	Sí	No	No	No
VPN completo	HTTP	No	Sí	No	No	No
VPN completo	HTTPS	Sí. Si la directiva MDX "Habilitar caché de contraseñas web"de Secure Web está activada.	No	Sí. Necesario para almacenar la credencial en caché de Secure Web.	No	Sí

Directivas de Secure Web

Al agregar Secure Web, tenga en cuenta las directivas MDX que son específicas de Secure Web. Para todos los dispositivos móviles admitidos:

Sitios web permitidos o bloqueados

Secure Web normalmente no filtra enlaces web. Puede usar esta directiva para configurar una lista de sitios permitidos o bloqueados específicos. Puede configurar patrones de dirección URL para re-

stringir los sitios web que el explorador puede abrir, mediante un formato de lista separada por comas. Cada patrón de la lista va precedido del signo Más (+) o del signo Menos (-). El explorador web coteja las direcciones URL con estos patrones en el orden indicado hasta que se produce una coincidencia. Cuando se encuentra una coincidencia, el prefijo determina la acción a tomar de la siguiente forma:

- Un signo Menos (-) como prefijo indica al explorador web que bloquee la URL. En este caso, la URL se trata como si la dirección del servidor web no pudiera resolverse.
- Un signo Más (+) como prefijo permite que la URL se procese normalmente.
- Si no figura ningún signo delante del patrón, se considera que va precedido del signo Más (+).
- Si una dirección URL no coincide con ningún patrón de la lista, la dirección URL se considera permitida

Para bloquear todas las demás URL, termine la lista con un signo menos seguido de un asterisco (-*). Por ejemplo:

- El valor de directiva `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` permite direcciones URL con HTTP dentro del dominio `mycorp.com`, pero las bloquea en cualquier otro sitio; permite direcciones URL con HTTPS y FTP en cualquier lugar, pero bloquea todas las demás URL.
- El valor de directiva `+http://*.training.lab/*,+https://*.training.lab/*,-*` permite a los usuarios abrir cualquier sitio en el dominio Training.lab (intranet) a través de HTTP o HTTPS. Sin embargo, no puede abrir direcciones URL públicas, como Facebook, Google y Hotmail, independientemente del protocolo.

Está vacío de forma predeterminada (se permiten todas las URL).

Bloquear ventanas emergentes

Las ventanas emergentes son fichas nuevas que algunos sitios web abren sin su permiso. Esta directiva determina si Secure Web permite las ventanas emergentes. Cuando se activa, Secure Web impide que los sitios web abran ventanas emergentes. El valor predeterminado es Desactivado.

Marcadores precargados

Define un conjunto de marcadores precargados para el explorador Secure Web. La directiva es una lista de tuplas separadas por comas que incluyen el nombre de la carpeta, el nombre descriptivo y la dirección web. Cada triplo debe seguir el formato carpeta, nombre, URL. El nombre y la carpeta pueden ir entre comillas dobles (“).

Por ejemplo, los valores de directiva `,"Mycorp, Inc. home page",https://www.mycorp.com, "MyCorp Links",Account logon,https://www.mycorp.com/Accounts "MyCorp Links/Investor Relations","Contact us",https://www.mycorp.com/`

`IR/Contactus.aspx` definen tres marcadores. El primero es un enlace primario (sin nombre de carpeta), titulado "Mycorp, Inc. home page". El segundo enlace se colocará en una carpeta llamada "MyCorp Links"y se etiquetará "Account logon". El tercero se colocará en una subcarpeta llamada "Investor Relations"dentro de la carpeta "MyCorp Links"y se mostrará como "Contact us".

Está vacío de forma predeterminada.

URL de página de inicio

Define el sitio web que Secure Web carga al iniciarse. Está vacío de forma predeterminada (página de inicio predeterminada).

Solo para dispositivos Android e iOS admitidos:

Interfaz de usuario del explorador web

Establece el comportamiento y la visibilidad de los controles de la interfaz de usuario del explorador para Secure Web. Normalmente están disponibles todos los controles del explorador. Estos incluyen los controles para avanzar, retroceder, barra de dirección y actualizar/detener la carga de la página. Esta directiva se puede configurar para restringir el uso y la visibilidad de algunos de estos controles. El valor predeterminado es Todos los controles visibles.

Opciones

- Todos los controles visibles. Todos los controles están visibles y no se restringe su uso para los usuarios.
- Barra de direcciones de solo lectura. Todos los controles están visibles, pero los usuarios no pueden modificar el campo de dirección del explorador web.
- Ocultar barra de direcciones. Oculta la barra de direcciones, pero no los demás controles.
- Ocultar todos los controles. Oculta toda la barra de herramientas para proporcionar una experiencia de exploración sin marcos.

Habilitar caché de contraseñas web

Cuando los usuarios de Secure Web introducen sus credenciales al abrir o solicitar un recurso Web, esta directiva determina si Secure Web guarda la contraseña en caché silenciosamente en el dispositivo. Esta directiva se aplica a las contraseñas introducidas en diálogos de autenticación y no a las contraseñas introducidas en formularios Web.

Si está **activada**, Secure Web guarda todas las contraseñas que los usuarios introducen cuando solicitan un recurso Web. Si está **desactivada**, Secure Web no guarda en caché las contraseñas y elimina las contraseñas que se hayan guardado previamente. El valor predeterminado es **Desactivado**.

Esta directiva solo se habilita cuando la directiva "Modo preferido de VPN"se establece en "Túnel VPN completo"para esta aplicación.

Servidores proxy

También puede configurar los servidores proxy de Secure Web cuando se usa el modo SSO web en túnel. Para obtener detalles, consulte esta entrada de blog.

Sufijos DNS

En Android, si los sufijos DNS no están configurados, es posible que la VPN falle. Para obtener información sobre cómo configurar sufijos DNS, consulte Compatibilidad con consultas DNS mediante sufijos DNS para dispositivos Android.

Preparar sitios de intranet para Secure Web

Esta sección está dirigida a desarrolladores de sitios web que necesitan preparar un sitio de intranet para usarlo con Secure Web para Android y para iOS. Los sitios de intranet diseñados para exploradores de escritorio requieren ciertos cambios para que funcionen correctamente en dispositivos Android e iOS.

Secure Web se basa en Android WebView e iOS WkWebView para ofrecer tecnologías web. Algunas de las tecnologías web que admite Secure Web son:

- AngularJS
- ASP .NET
- JavaScript
- jQuery
- WebGL

Algunas de las tecnologías web que no admite Secure Web son:

- Flash
- Java

En la siguiente tabla, se muestran las funcionalidades y las tecnologías de generación de HTML que admite Secure Web. X indica que la función está disponible para una combinación de plataforma, explorador web y componente.

Tecnología	Secure Web en iOS	Secure Web en Android 6.x/7.x
Motor de JavaScript	JavaScriptCore	V8
Almacenamiento local	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
srcet	X	X
WebGL		X
API de requestAnimationFrame		X
API de Navigation Timing		X
API de Resource Timing		X

Las tecnologías funcionan del mismo modo en todos los dispositivos. No obstante, Secure Web devuelve distintas cadenas de agente de usuario en los distintos dispositivos. Para determinar la versión del explorador usada para Secure Web, puede ver la cadena del agente de usuario. Desde Secure Web, vaya a https://whatsmyuseragent.com/.

Solucionar problemas en sitios de intranet

Para solucionar problemas de representación cuando el sitio de intranet se ve en Secure Web, compare cómo se genera el sitio web en Secure Web y en un explorador web de terceros compatible.

Para iOS, los exploradores de terceros compatibles para realizar pruebas son Chrome y Dolphin.

Para Android, el explorador de terceros compatible para realizar pruebas es Dolphin.

> **Nota:**
>
> Chrome es un explorador nativo en Android. No lo utilice para la comparación.

En iOS, asegúrese de que los marcadores admiten VPN en el nivel de dispositivo. Para configurar la VPN en el dispositivo, vaya a **Configuración > VPN > Agregar configuración VPN**.

También puede usar aplicaciones cliente VPN disponibles en App Store, tales como Citrix VPN, Cisco AnyConnect o Pulse Secure.

- Si una página web aparece igual en los dos exploradores, el problema reside en el sitio web. Actualice el sitio y asegúrese de que funciona bien para el sistema operativo.

- Si el problema en la página web solo aparece cuando se abre en Secure Web, póngase en contacto con el equipo de asistencia de Citrix para abrir un tíquet de asistencia. Proporcione los pasos detallados del problema, incluida la información de qué tipo de explorador web y de sistema operativo ha utilizado. Si tiene problemas al generar páginas en Secure Web para iOS, incluya un archivo web de la página según se describe en los pasos siguientes. Esto ayudará a Citrix a resolver el problema más rápidamente.

Para crear un archivo web

Con Safari en macOS 10.9 o posterior, puede guardar una página web como archivo web (denominado Lista de lectura). El archivo web incluye todos los archivos vinculados, como imágenes, CSS y JavaScript.

1. En Safari, vacíe la carpeta Lista de lectura; en el **Finder**, haga clic en el menú **Ir** de la barra **Menú**, elija **Ir a la carpeta**, introduzca la ruta ~/Library/Safari/ReadingListArchives/, y luego elimine todas las carpetas de esa ubicación.
2. En la barra **Menú**, vaya a **Safari > Preferencias > Avanzado** y habilite la opción **Mostrar el menú Desarrollo** en la barra de menú.
3. En la barra **Menú**, vaya a **Desarrollo > Agente de usuario** e introduzca el agente de usuario de Secure Web: (Mozilla/5.0 (iPad; CPU OS 8_3 como macOS) AppleWebKit/600.1.4 (KHTML, como Gecko) Mobile/12F69 Secure Web/ 10.1.0 (compilación 1.4.0) Safari/8536.25).
4. En Safari, abra el sitio web que quiere guardar como una lista de lectura (archivo web).
5. En la barra **Menú**, vaya a **Marcadores > Agregar a la lista de lectura**. El archivado se produce en segundo plano y puede tardar unos minutos.
6. Busque la lista de lectura archivada: en la barra **Menú**, vaya a **Visualización > Mostrar barra lateral de lista de lectura**.
7. Verifique el archivado:
   - Desactive la conectividad de red en el Mac.
   - Abra el sitio web desde la lista de lectura.

     El sitio web se genera al completo.
8. Comprima el archivo. Para ello, en el **Finder**, haga clic en el menú **Ir** en la barra **Menú**, elija **Ir a la carpeta** e indique la ruta ~/Library/Safari/ReadingListArchives/. A continuación, comprima la carpeta que tiene como nombre una cadena hexadecimal aleatoria. Puede enviar ese archivo a la asistencia técnica de Citrix cuando abra un tíquet de asistencia.

Funciones de Secure Web

Secure Web utiliza las tecnologías de intercambio de datos móviles para crear un túnel VPN dedicado para el acceso de los usuarios a sitios web internos y externos, y a todos los demás sitios web. Esto incluye sitios con información confidencial en un entorno protegido por las directivas de su organización.

La integración de Secure Web con Secure Mail y Citrix Files ofrece una experiencia de usuario fluida, contenida en el entorno seguro de Endpoint Management. Éstos son algunos ejemplos de las funciones de integración:

- Cuando los usuarios tocan enlaces **mailto**, se abre un nuevo mensaje de correo electrónico en Citrix Secure Mail sin necesidad de volver a autenticarse.
- En iOS, los usuarios pueden abrir un enlace en Secure Web desde una aplicación de correo electrónico nativa si insertan **ctxmobilebrowser://** delante de la URL. Por ejemplo, para abrir `example.com` desde una aplicación de correo electrónico nativa, use la dirección URL ctxmobilebrowser://example.com.
- Cuando los usuarios hacen clic en un enlace de intranet dentro de un mensaje de correo electrónico, Secure Web va a ese sitio de la intranet sin necesidad de volver a autenticarse.
- Los usuarios pueden cargar archivos en Citrix Files, que pueden descargar de la Web mediante Secure Web.

Asimismo, los usuarios de Secure Web pueden realizar las siguientes acciones:

- Bloquear ventanas emergentes.

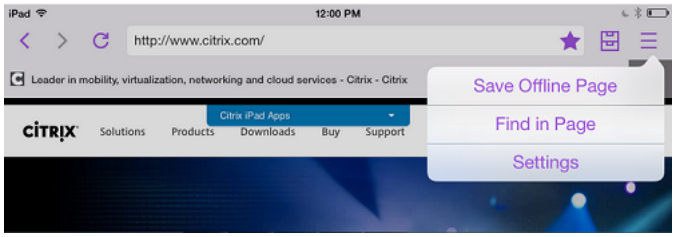
  > **Nota:**
  >
  > Mucha de la carga de memoria de Secure Web se dedica a la generación de ventanas emergentes, de modo que el rendimiento suele mejorar si se selecciona la opción de bloqueo de las ventanas emergentes en los Parámetros.

- Agregar sus sitios favoritos como Marcadores.
- Descargar archivos.
- Guardar páginas sin conexión.
- Guardado automático de contraseñas.
- Borrar caché, historial y cookies.
- Inhabilitar cookies y almacenamiento local de HTML5.
- Compartir dispositivos de forma segura con otros usuarios.
- Hacer búsquedas desde la barra de direcciones.

- Permitir que las aplicaciones web que los usuarios ejecutan dentro de Secure Web accedan a su ubicación.
- Exportar e importar parámetros.
- Abrir archivos directamente en Citrix Files, sin necesidad de descargarlos. Para habilitar esta función, agregue **ctx-sf**: a la directiva "Direcciones URL permitidas"en Endpoint Management.
- En iOS, puede usar acciones de 3D Touch para abrir una nueva ficha y acceder a páginas sin conexión, sitios favoritos y descargas directamente desde la pantalla inicial.
- En iOS, puede descargar archivos de cualquier tamaño y abrirlos en Citrix Files y otras aplicaciones.

  > **Nota:**
  >
  > Si Secure Web se pone en segundo plano, la descarga se detiene.

- Buscar un término en la vista de la página actual con la opción **Buscar en la página**.



Secure Web también admite texto dinámico. La aplicación muestra la fuente de texto que los usuarios definen en sus dispositivos.

> **Nota:**
>
> - Citrix Files para XenMobile alcanzó el fin de su vida útil el 1 de julio de 2023. Para obtener más información, consulte Fin de vida y aplicaciones retiradas.

Citrix Content Collaboration para Endpoint Management

July 15, 2023

Los clientes de Citrix Content Collaboration para Endpoint Management son versiones con prestaciones MDX de los clientes móviles de Citrix Files. Estos clientes ofrecen un acceso seguro e integrado a los datos de aplicaciones empaquetadas con MDX. Los clientes de Citrix Content Collaboration para Endpoint Management también aprovechan las funciones MDX, tales como las micro VPN, Single Sign-On (SSO) en Secure Hub y la autenticación de dos factores.

Citrix Files es un servicio para compartir y sincronizar archivos de empresa, por tanto permite que los usuarios se intercambien documentos de una manera sencilla y segura. Citrix Files ofrece a los usuarios una variedad de opciones de acceso, incluidos los clientes móviles de Citrix Files (como Citrix Files para teléfonos Android y Citrix Files para iPad).

Puede integrar Citrix Files con Endpoint Management para ofrecer el conjunto completo de funciones de Citrix Files o para ofrecer acceso solo a conectores de zonas de almacenamiento. De forma predeterminada, la consola de Citrix Endpoint Management solo permite la configuración de Citrix Files. Sin embargo, si quiere configurar Endpoint Management para usarlo con conectores de zonas de almacenamiento, consulte Usar Citrix Content Collaboration con Endpoint Management en la documentación de Citrix Endpoint Management.

Utilice Endpoint Management, Citrix Files, controladores de zonas de almacenamiento y Citrix ADC de la siguiente manera para implementar y administrar clientes de Citrix Content Collaboration para Endpoint Management:

- Cuando Endpoint Management se configura con Citrix Files, actúa como un proveedor de identidades (IdP) SAML e implementa clientes de Citrix Content Collaboration para Endpoint Management. Citrix Files administra los datos de Citrix Files. Ningún dato de Citrix Files pasa a través de Endpoint Management.
- Cuando Endpoint Management está configurado con Citrix Files o con conectores de zonas de almacenamiento, el Controller de zonas de almacenamiento proporciona conectividad a los datos situados en recursos compartidos de red y SharePoint. Los usuarios acceden a los datos almacenados a través de las aplicaciones móviles de productividad de Citrix Files. Los usuarios pueden modificar documentos de Microsoft Office, abrir una vista previa y anotar archivos PDF de Adobe desde dispositivos móviles.
- Citrix ADC administra las solicitudes de los usuarios externos, protegiendo las conexiones, equilibrando la carga de solicitudes y gestionando la conmutación de contenido para conectores de zonas de almacenamiento.

Para descargar clientes de Citrix Content Collaboration para Endpoint Management, consulte las descargas de Citrix.com.

Para conocer los requisitos del sistema de Citrix Content Collaboration para Endpoint Management y otras aplicaciones móviles de productividad, consulte Aplicaciones móviles de productividad admitidas.

En qué se diferencian los clientes de Citrix Content Collaboration para Endpoint Management de los clientes móviles de Citrix Files

A continuación se describen las diferencias entre los clientes de Citrix Content Collaboration para Endpoint Management y los clientes móviles de Citrix Files.

Acceso de usuarios

Clientes de Citrix Content Collaboration para Endpoint Management:

Los usuarios obtienen y abren los clientes de Citrix Content Collaboration para Endpoint Management desde Secure Hub.

Clientes móviles de Citrix Files:

Los usuarios obtienen los clientes móviles de Citrix Files desde almacenes de aplicaciones.

SSO

Clientes de Citrix Content Collaboration para Endpoint Management:

Para integrar Endpoint Management con Citrix Files, puede configurar Endpoint Management como un IdP de SAML para Citrix Files. En esta configuración, Secure Hub obtiene un token de SAML para el cliente de Citrix Content Collaboration para Endpoint Management, mediante Endpoint Management como el IdP de SAML. Un usuario que inicie el cliente de Citrix Content Collaboration para Endpoint Management, pero no haya iniciado sesión en Secure Hub recibe una petición para iniciar sesión en Secure Hub. No es necesario que el usuario conozca el dominio ni la información de la cuenta de Citrix Files.

Clientes móviles de Citrix Files:

Puede configurar Endpoint Management y Citrix Gateway como un IdP de SAML para Citrix Files. En esta configuración, un usuario que haya iniciado sesión en Citrix Files a través de un explorador web u otro cliente de Citrix Files es redirigido al entorno de Endpoint Management para la autenticación. Después de la autenticación en Endpoint Management, el usuario recibe un token de SAML válido para iniciar sesión en su cuenta de Citrix Files.

Micro VPN

Clientes de Citrix Content Collaboration para Endpoint Management:

Los usuarios remotos pueden conectarse mediante una conexión VPN o micro VPN a través de Citrix Gateway para acceder a aplicaciones y escritorios de la red interna. Esta función es transparente para los usuarios y está disponible mediante la integración de Citrix ADC con Endpoint Management.

Clientes móviles de Citrix Files:

No aplicable.

Autenticación de dos factores

Clientes de Citrix Content Collaboration para Endpoint Management:

La integración de Citrix ADC con Endpoint Management también permite la autenticación mediante una combinación de la autenticación de certificados de cliente y otro tipo de autenticación; por ejemplo, LDAP o RADIUS.

Clientes móviles de Citrix Files:

No aplicable.

Permisos de carpeta

Clientes de Citrix Content Collaboration para Endpoint Management y clientes móviles de Citrix Files:

Citrix Files determina este aspecto cuando se trata de una integración de Endpoint Management con Citrix Files.

Protección del acceso a documentos

Clientes de Citrix Content Collaboration para Endpoint Management:

Los usuarios pueden abrir datos adjuntos recibidos en Secure Mail o descargados por cualquiera de las aplicaciones empaquetadas con MDX. Cuando el usuario realiza una acción "Abrir en"solo aparecen aplicaciones empaquetadas con MDX. Los datos de una aplicación no empaquetada no están disponibles en un cliente de Citrix Content Collaboration para Endpoint Management. Los usuarios de Secure Mail pueden adjuntar archivos desde el repositorio de Citrix Files sin necesidad de descargarlos en el dispositivo. Si un usuario tiene un Citrix Files empaquetado y un Citrix Files no empaquetado en el mismo dispositivo, el cliente Citrix Files empaquetado no puede acceder a los archivos en la cuenta de Citrix Files personal del usuario. El cliente de Citrix Files empaquetado solo puede acceder al subdominio de Citrix Files configurado en Endpoint Management.

Clientes móviles de Citrix Files:

Los usuarios pueden abrir los datos adjuntos desde cualquier aplicación.

Acceso a la cuenta de Citrix Files

Clientes de Citrix Content Collaboration para Endpoint Management:

En la integración de Endpoint Management con Citrix Files, para acceder a una cuenta personal de Citrix Files o una cuenta de terceros de Citrix Files, los usuarios deben usar una versión no MDX de Citrix Files en el dispositivo.

Clientes móviles de Citrix Files:

En la integración de Endpoint Management con Citrix Files, está disponible desde los clientes de Citrix Files.

Directivas de dispositivo

Clientes de Citrix Content Collaboration para Endpoint Management y clientes móviles de Citrix Files:

Las directivas de ambos, Endpoint Management y Citrix Files, se aplican a los clientes de Citrix Content Collaboration para Endpoint Management. Por ejemplo, desde la consola de Endpoint Management, puede realizar un borrado de dispositivo. Desde la consola de Citrix Files, puede borrar remotamente la aplicación Citrix Files.

Directivas MDX

Clientes de Citrix Content Collaboration para Endpoint Management:

En Citrix Endpoint Management, las directivas MDX permiten configurar parámetros que el almacén de aplicaciones de Endpoint Management aplica. Las directivas disponibles solamente a través de MDX incluyen la capacidad para bloquear la cámara, el micrófono, la redacción de correo electrónico, la captura de pantalla y las operaciones de portapapeles: cortar, copiar y pegar.

Clientes móviles de Citrix Files:

No aplicable.

Cifrado de datos

Clientes de Citrix Content Collaboration para Endpoint Management y clientes móviles de Citrix Files:

Cifra todos los datos almacenados mediante AES-256 y protege los datos en tránsito con SSL 3.0 y un mínimo de cifrado de 128 bits.

Disponibilidad

Clientes de Citrix Content Collaboration para Endpoint Management:

Los clientes de Citrix Content Collaboration para Endpoint Management se incluyen en las ediciones Endpoint Management Advanced y Enterprise.

Clientes móviles de Citrix Files:

Todas las ediciones de Endpoint Management incluyen todas las funciones de Citrix Files. Puede integrar Endpoint Management con el conjunto completo de funciones de Citrix Files o solo con los conectores de zonas de almacenamiento.

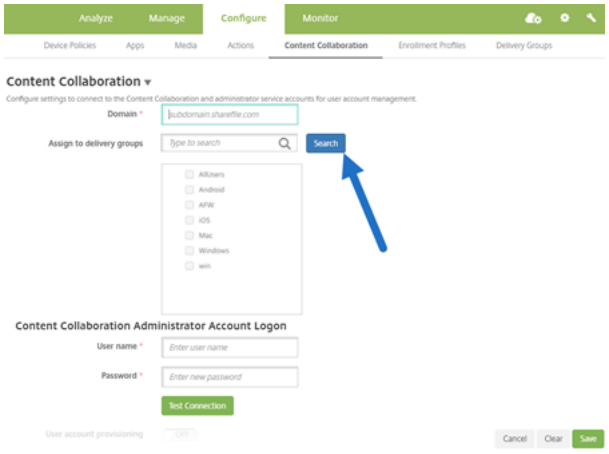
Integrar y entregar clientes de Citrix Content Collaboration para Endpoint Management

Para integrar y entregar clientes de Citrix Content Collaboration para Endpoint Management, siga estos pasos generales:

1. Habilite Endpoint Management como un IdP de SAML para Citrix Files, para poder ofrecer el inicio SSO en Citrix Files desde los clientes de Citrix Files. Para ello, configure la información de la cuenta de Citrix Files en Endpoint Management. Para obtener más información, consulte la sección "Para configurar la información de la cuenta de Citrix Files en Endpoint Management para SSO".

   > **Importante:**
   >
   > Si quiere usar Endpoint Management como IdP de SAML para clientes de Citrix Files que no son MDX (como la aplicación web de Citrix Files y los clientes de Citrix Files Sync), se requiere una configuración adicional. Para obtener más información, consulte este artículo en el sitio Web de asistencia técnica de Citrix Files:
   >
   > Citrix Files (ShareFile) Single Sign-On SSO. El artículo contiene un enlace para descargar la guía de configuración de Endpoint Management.

2. Descargue los clientes de Citrix Files.
3. Agregue los clientes de Citrix Files a Endpoint Management. Para obtener más información, consulte "Para agregar Citrix Files a Endpoint Management"más adelante en este artículo.
4. Valide la configuración. Para obtener más información, consulte "Para validar clientes de Citrix Files", indicado más adelante en este artículo.



Acerca de los parámetros:

- Dominio es el subdominio de Citrix Files que se utilizará para los clientes.
- Solo los usuarios de los grupos de entrega seleccionados tendrán acceso SSO a Citrix Files desde los clientes.

  Si un usuario en un grupo de entrega no tiene cuenta de Citrix Files, Endpoint Management aprovisiona Citrix Files para él cuando se agrega el cliente de Citrix Files a Endpoint Management.
- Endpoint Management utiliza la información de inicio de sesión de la cuenta del administrador de Citrix Files para guardar la configuración de SAML en el plano de control de Citrix Files.

> **Importante:**
>
> La configuración que permite el acceso SSO en Citrix Files desde los clientes de Citrix Files no autentica a los usuarios en recursos compartidos de red ni en bibliotecas de documentos de SharePoint. El acceso a esos orígenes de datos de Connector requiere la autenticación en el dominio de Active Directory donde residan dichos recursos compartidos de red y servidores SharePoint.

Para configurar la información de la cuenta de Citrix Files en Endpoint Management para SSO

Para habilitar el inicio de sesión único (SSO) en las aplicaciones móviles de productividad desde Secure Hub, indique información sobre la cuenta de Citrix Files y la cuenta de servicio de administrador de Citrix Files en la consola de Endpoint Management. Con esa configuración, Endpoint Management actúa como un IdP de SAML para: Citrix Files, clientes de las aplicaciones móviles de productividad, clientes de Citrix Files y clientes de Citrix Files que no son MDX. Cuando un usuario inicia un cliente de aplicaciones móviles de productividad, Secure Hub obtiene un token de SAML para el usuario desde Endpoint Management y lo envía al cliente de Citrix Files.

En la consola de Endpoint Management, haga clic en **Configurar** > **Content Collaboration**, que es el nombre antiguo de Citrix Files.

Para agregar clientes de Citrix Content Collaboration para Endpoint Management a Endpoint Management

Cuando agrega clientes de Citrix Content Collaboration para Endpoint Management a Endpoint Management, puede habilitar el acceso SSO a los orígenes de datos del conector desde clientes de Citrix Content Collaboration para Endpoint Management. Para hacerlo, configure las directivas "Acceso de red"y "Modo preferido de VPN"como se describe en esta sección.

Requisitos previos

- Endpoint Management debe poder conectarse al subdominio de Citrix Files. Para probar la conexión, haga ping a su subdominio de Citrix Files desde el servidor Endpoint Management.
- La zona horaria configurada para la cuenta de Citrix Files y para el hipervisor que ejecuta Endpoint Management debe ser la misma. Si no tienen la misma zona horaria, las solicitudes de SSO pueden fallar porque el token de SAML puede no llegar a Citrix Files en el plazo de tiempo esperado. Para configurar el servidor NTP para Endpoint Management, use la interfaz de línea de comandos de Endpoint Management.

  > **Nota:**
  >
  > Tenga en cuenta que el host de Hyper-V establece la hora en una VM de Linux a la zona horaria local y no UTC.

- Inicie sesión en la cuenta de ShareFile como administrador y verifique la configuración de Single Sign-On de SAML en **Parámetros** > **Parámetros de administración** > **Seguridad** > **Directiva de seguridad e inicio de sesión** > **Configuración de SAML 2.0 / Single Sign-on**.
- Descargue clientes de Citrix Content Collaboration para Endpoint Management.

Pasos:

1. En la consola de Endpoint Management, haga clic en **Configurar > Aplicaciones** > **Agregar**.
2. Haga clic en **MDX**.
3. Escriba un **Nombre**, y de manera opcional, una **Descripción** y una **Categoría de la aplicación**.
4. Haga clic en **Siguiente** y cargue el archivo MDX del cliente de Citrix Content Collaboration para Endpoint Management.
5. Haga clic en **Siguiente** para configurar la información de la aplicación y las directivas.

   La configuración que permite el acceso SSO en Citrix Files desde los clientes de Citrix Content Collaboration para Endpoint Management no autentica a los usuarios en recursos compartidos de red ni en bibliotecas de documentos de SharePoint.
6. Para habilitar el acceso SSO entre la micro VPN de Secure Hub y el Controller de zonas de almacenamiento, configure estas directivas:

   - Establezca la directiva "Acceso de red"en **Túnel a la red interna**.

     En este modo, el framework MDX intercepta todo el tráfico de red desde el cliente de Citrix Content Collaboration para Endpoint Management. A continuación, el tráfico de red se redirige a través de Citrix Gateway mediante una micro VPN específica de la aplicación.
   - Establezca la directiva Modo preferido de VPN en **Túnel - SSO web**.

     En este modo de canalización por túnel, el framework MDX termina el tráfico SSL/HTTP desde una aplicación MDX, que a continuación inicia nuevas conexiones con conexiones

internas en nombre del usuario. Esta configuración de directiva permite que el marco de MDX detecte y responda a los desafíos de autenticación emitidos por servidores web.

7. Complete las aprobaciones y asignaciones de grupo de entrega según sea necesario.

Solo los usuarios de los grupos de entrega seleccionados tendrán acceso SSO a Citrix Files desde los clientes de Citrix Content Collaboration para Endpoint Management. Si un usuario en un grupo de entrega no tiene cuenta de Citrix Files, Endpoint Management aprovisiona Citrix Files para él cuando se agrega el cliente de Citrix Content Collaboration para Endpoint Management a Endpoint Management.

Para validar clientes de Citrix Content Collaboration para Endpoint Management

1. Después de completar la configuración descrita en este artículo, inicie el cliente de Citrix Content Collaboration para Endpoint Management. Citrix Files no le pedirá que inicie sesión.
2. En Secure Mail, redacte un mensaje de correo electrónico y agregue datos adjuntos desde Citrix Files. Se abre la página de inicio de Citrix Files, sin pedirle que inicie sesión.

> **Nota:**
>
> - Citrix Files para XenMobile alcanzó el fin de su vida útil el 1 de julio de 2023. Para obtener más información, consulte Fin de vida y aplicaciones retiradas.

Fin de vida y aplicaciones retiradas

June 6, 2024

Estas aplicaciones ya han llegado al ciclo Fin de vida (End Of Life o EOL) o están a punto de alcanzar ese estado. Cuando una versión del producto alcanza la fecha de fin de vida, aún se puede utilizar el producto en las condiciones de su contrato de licencia del producto, pero las opciones de asistencia disponibles son limitadas. La información histórica aparece en Knowledge Center o en otros recursos electrónicos. La documentación dejará de actualizarse y se suministrará tal y como está en este momento. Para obtener más información sobre los hitos de ciclo de vida útil de los productos, consulte la Tabla de productos.

> **Nota:**
>
> Para obtener información avanzada sobre las funciones de Citrix Endpoint Management que se están retirando gradualmente, consulte Elementos retirados.

Citrix Files para XenMobile (MDX): Citrix Files para XenMobile alcanzó el fin de su vida útil el 1 de julio de 2023.

Recomendamos a los clientes usar Citrix Files, disponible en el App Store de Apple y en Google Play. Está preparado para el SDK de MAM.

SDK de Secure Mail para Intune (iOS y Android): Secure Mail alcanzó el fin de su vida útil el 30 de abril de 2023.

Citrix Files para Intune: Se retiró el 31 de diciembre de 2020.

Le recomendamos que explore las prestaciones de las plataformas para colocar en un contenedor la aplicación Citrix Files habitual (disponible en las tiendas de aplicaciones) a través de Android Enterprise (con un perfil de trabajo) y la inscripción de usuarios de iOS.

ShareConnect: ShareConnect llegó al fin de vida (EOL) el 30 de junio de 2020.

Secure Notes: La fecha del ciclo de Fin de vida fue el 31 de diciembre de 2018.

Si necesita las funciones de Secure Notes y Secure Tasks, recomendamos Notate para Citrix, una aplicación de terceros que se puede proteger con directivas MDX.

Si los usuarios de Secure Notes y Secure Tasks almacenaron datos en Outlook, pueden acceder a esos datos en Notate. Si los usuarios almacenaron datos en ShareFile, ahora Citrix Files, esos datos no se migran.

Los usuarios pueden seguir ejecutando Secure Notes más allá de la fecha de ciclo de vida de EOL, hasta que el sistema operativo de su plataforma deje de admitir la interfaz de usuario. No obstante, no recomendamos que utilice un producto no admitido.

Secure Tasks: La fecha del ciclo de Fin de vida fue el 31 de diciembre de 2018.

Secure Forms: La fecha del ciclo de Fin de vida fue el 31 de marzo de 2018. Se recomienda a los clientes pasar a la aplicación Citrix ShareFile Workflows, incluida con las cuentas Citrix Files Platinum y Premium de ShareFile. Para obtener más detalles, consulte Citrix ShareFile Workflows.

ScanDirect: ScanDirect llegó al EOL el 1 de septiembre de 2018.

Permitir la interacción segura con aplicaciones Office 365

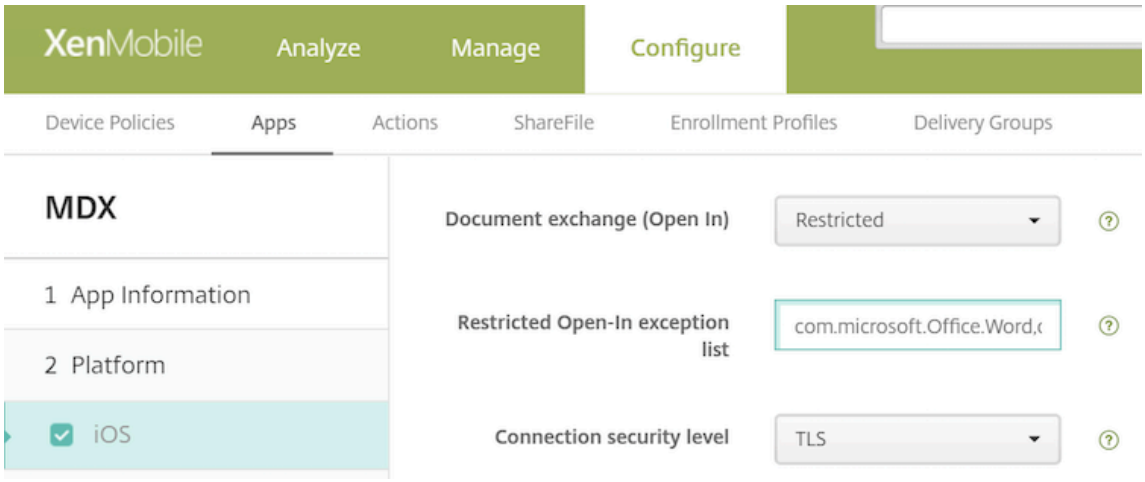
December 7, 2021

Citrix Secure Mail, Citrix Secure Web y Citrix Files ofrecen la opción de abrir el contenedor MDX para permitir que los usuarios transfieran documentos y datos a aplicaciones de Microsoft Office 365. En plataformas iOS y Android, esta capacidad se gestiona mediante las directivas de apertura en la consola de Endpoint Management.

Una vez abiertos en una aplicación de Microsoft, los datos dejan de estar cifrados y protegidos en el contenedor MDX. Antes de habilitar esta función, tenga en cuenta lo que ello implica en cuanto a la seguridad. Concretamente, los clientes a los que concierna la prevención de pérdida de datos o quienes estén sujetos a HIPAA u otros requisitos de estricto cumplimiento deben sopesar si les compensa abrir el contenedor.

Habilitar Office 365 en iOS

1. Descargue la versión más reciente de las aplicaciones Secure Mail, Secure Web o Citrix Files desde la página de descargas de Endpoint Management.
2. Cargue los archivos en la consola de Endpoint Management.
3. Busque la directiva **Intercambio de documentos (Abrir en)** y establézcala en **Restringida**. En la **Lista de excepciones de la apertura restringida**, Microsoft Word, Excel, PowerPoint, OneNote y Outlook aparecen automáticamente. Por ejemplo: com.microsoft.Office.Word, com.microsoft.Office.Excel, com.microsoft.Office.Powerpoint, com.microsoft.onenote, com.microsoft.onenoteiPad, com.microsoft.Office.Outlook



En inscripciones MDM, hay otros controles disponibles para los dispositivos iOS.

Puede cargar aplicaciones de iTunes en la consola de Endpoint Management y enviarlas a los dispositivos. Si elije esta opción, **active** estas directivas:

- Quitar aplicación si se quita el perfil MDM
- Impedir copia de seguridad de datos de la aplicación
- Forzar administración de la aplicación (tenga en cuenta que un borrado selectivo elimina la aplicación y los datos)

Para evitar el flujo de datos y documentos desde las aplicaciones de Microsoft a aplicaciones no administradas que haya presentes en el dispositivo, vaya a **Configurar > Dispositivos > Restricciones**

> iOS en la consola de Endpoint Management y **desactive** las directivas **Documentos de aplicaciones administradas en aplicaciones no administradas** y **Documentos de aplicaciones no administradas en aplicaciones administradas**.

Habilitar Office 365 en Android

1. Descargue la versión más reciente de las aplicaciones Secure Mail, Secure Web o Citrix Files desde la página de descargas de Endpoint Management.
2. Cargue los archivos en la consola de Endpoint Management.
3. Busque la directiva **Intercambio de documentos (Abrir en)** y establézcala en **Restringida**.
4. En la **Lista de excepciones de la apertura restringida**, agregue los siguientes ID de paquete:

   ```
   { package=com.microsoft.office.word } { package=com.microsoft.office.powerpoint } { package=com.microsoft.office.excel }
   ```

5. Configure otras directivas de aplicación de la manera habitual y guarde las aplicaciones.

Los usuarios deben guardar los archivos desde Secure Mail, Secure Web o Citrix Files en sus dispositivos y abrirlos con una aplicación de Office 365.

Tanto para iOS como para Android, los usuarios pueden abrir y modificar los siguientes tipos de archivos en sus dispositivos:

Formatos de archivo admitidos

Para conocer los formatos de archivo compatibles, consulte la documentación de Microsoft Office.