Citrix Receiver para Android 3.13

Contents

Novedades

January 14, 2019

Novedades en la versión 3.13.9

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 3.13.8

Respaldo de asociación de tipos de archivo para StoreFront

Cuando se publican aplicaciones, se las asocia con ciertos tipos de archivos presentes en el servidor. Al hacerlo, se está redirigiendo el contenido desde el dispositivo del usuario al servidor. Los dispositivos que ejecutan Receiver para Android abren archivos de un tipo asociado con una aplicación publicada específica. Por ejemplo, cuando los usuarios hacen doble clic en un archivo adjunto de un correo electrónico, el archivo adjunto se abre en la aplicación asociada.

Para obtener más información, consulte Acceder a archivos usando la asociación de tipos de archivo.

Respaldo para fijar accesos directos en Chromebook

Los accesos directos a sus aplicaciones y escritorios favoritos están disponibles automáticamente desde el Apps Launcher de Chrome después de agregar su cuenta a Citrix Receiver para Android ejecutándose en un dispositivo Chromebook, no solo cuando se conecta a StoreFront, sino también a los sitios de servicios de XenApp (anteriormente conocidos como cuentas PNA).

> **Nota:**
>
> Esta función no está respaldada en la Interfaz Web.

Novedades en la versión 3.13.7

Modo de compatibilidad de NetScaler

La opción **Modo de compatibilidad de NetScaler** está disponible para solucionar un error de handshake de TLS, o error 41E, al conectar con versiones anteriores de NetScaler. Para obtener más información sobre el fallo de handshake, consulte el artículo CTX221453 de Knowledge Center. El valor predeterminado de Versiones de TLS es TLS 1.0, 1.1, 1.2.

Novedades en la versión 3.13.6

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento general.

Novedades en la versión 3.13.5

Agregar aplicaciones y escritorios favoritos a Chrome Launcher

En un Chromebook, después de agregar su cuenta a Citrix Receiver para Android, todas sus aplicaciones y escritorios favoritos se agregan automáticamente a Chrome Launcher (iniciador de Chrome) para un acceso rápido.

Respaldo HTTPS para Citrix Ready Workspace Hub

Ahora se admiten las conexiones HTTPS entre Citrix Receiver para Android y Citrix Ready Workspace Hub.

Novedades en la versión 3.13.4

Compatibilidad con Citrix Ready Workspace Hub

Basado en la plataforma Raspberry Pi 3, Citrix Ready Workspace Hub ofrece una conexión segura con aplicaciones y datos autorizados. Con esta versión, Citrix Receiver para Android respalda la autenticación de usuarios en hubs de espacio de trabajo Citrix Ready Workspace Hub como función experimental.

Con esta versión, Citrix Receiver para Android admite Citrix Casting. Citrix Casting hace posible que los usuarios muevan de forma segura y sin problemas sus sesiones de aplicaciones y escritorios virtuales desde un dispositivo móvil a un Citrix Ready Workspace Hub utilizando la itinerancia de sesiones y acoplamiento inalámbrico. La itinerancia de sesiones (“roaming”) permite que su teléfono se autentique en un Citrix Ready Workspace Hub y transfiera imperceptiblemente la sesión del usuario al hub de espacio de trabajo. El acoplamiento inalámbrico permite a los usuarios interactuar con su teléfono y enviar cualquier sesión de aplicación o de escritorio a cualquier Workspace Hub a su alrededor.

Permisos dinámicos

Anteriormente, Citrix Receiver para Android solicitaba todos los permisos durante la instalación. Con esta versión, cuando se ejecuta en dispositivos Android 6.x y versiones posteriores, Citrix Receiver

solicita dinámicamente permisos cuando los necesita para acceder a la tarjeta SD, la ubicación y el acceso al teléfono.

Modificar tipos de autenticación y puertas de enlace

Los usuarios ahora pueden modificar su puerta de enlace preferida y el tipo de autenticación después de agregar una cuenta.

> **Nota:**
>
> Citrix Receiver rellena todos los tipos de autenticación publicados por StoreFront. Los usuarios deben ponerse en contacto con su administrador para obtener los tipos de autenticación compatibles para la puerta de enlace seleccionada.

Novedades en la versión 3.13.3

Lanzamiento de sesiones con certificados que no son de confianza

En respuesta a una solicitud frecuente, los usuarios ahora pueden lanzar sesiones con un certificado que no sea de confianza.

> **Nota:**
>
> Aceptar un certificado que no es de confianza supone un riesgo. Los administradores deben enviar certificados de confianza por otros medios (correo electrónico, enlaces de descarga, el MDM existente, etc.) siempre que sea posible.

Inicio de sesión simplificado

Después de iniciar sesión por primera vez, Citrix Receiver para Android rellena automáticamente los campos de nombre de usuario y dominio en la pantalla de inicio de sesión para facilitar el inicio de sesión.

Códigos QR para Workspace Hub

Citrix Receiver para Android ahora detecta el Workspace Hub utilizando códigos QR.

Novedades en la versión 3.13.2

Sincronización de la distribución de teclado

A partir de esta versión, Citrix Receiver para Android ofrece una sincronización dinámica de la distribución del teclado desde el cliente al VDA en una sesión. Esto permite a los usuarios cambiar entre sus distribuciones de teclado preferidas en el dispositivo cliente, lo que proporciona una experiencia de usuario uniforme cuando, por ejemplo, cambian de una distribución de teclado en inglés a español. Cuando los usuarios cambien de distribución de teclado, verán brevemente un mensaje mientras tiene lugar la sincronización. A continuación, podrán seguir trabajando con la nueva distribución del teclado.

> **Nota:**
>
> Esta característica solo funciona en los teclados internos de los dispositivos, no en teclados externos. La casilla "Usar IME de cliente" en los Parámetros de Citrix Receiver para Android debe estar marcada para habilitar esta función.

Usar la interfaz web para iniciar sesión

Citrix Receiver para Android 3.13.2 permite a los usuarios utilizar un explorador Web para iniciar sesión, en lugar de utilizar la interfaz de usuario nativa para ciertas instalaciones más antiguas.

Novedades en la versión 3.13.1

Nueva interfaz de usuario para Citrix Receiver para Android

La interfaz de usuario (UI) de Citrix Receiver para Android se ha rediseñado en función de los comentarios proporcionados por la comunidad de usuarios y de acuerdo con las nuevas directrices de diseño material de Google para aplicaciones de Android.

Estas son algunas de las ventajas que ofrece la nueva experiencia de usuario:

- Un flujo de trabajo más simplificado para todas las tareas. Ahora es más fácil hacer las cosas que los usuarios necesitan para ser más productivos.
- Directrices de navegación para familiarizarse con la nueva interfaz.
- Ahora se proporciona respaldo para enviar comentarios dentro de la aplicación para que lleguen a Citrix con la recopilación de registros automática.
- Toasts y Snackbars de Android en varios lugares para ayudarle a identificar el estado de las operaciones, así como operaciones para Deshacer.

Compatibilidad con Citrix Ready Workspace Hub

Basado en la plataforma Raspberry Pi 3, Citrix Ready Workspace Hub ofrece una conexión segura con aplicaciones y datos autorizados. Con esta versión, Citrix Receiver para Android respalda la autenticación de usuarios en Citrix Ready Workspace Hub como función experimental. Esto permite a los usuarios autenticados transmitir sus sesiones a un Hub. Esta función está inhabilitada de forma predeterminada.

> **Nota:**
>
> Se requiere permiso de localización para la función experimental de Citrix Ready Workspace Hub. Puede denegar este permiso si hay ningún Workspace Hub.

Respaldo DTLS sobre transporte adaptable

Se ha habilitado el respaldo para DTLS para transporte adaptable usando NetScaler Gateway. Para usar el protocolo DTLS, asegúrese de que EDT está habilitado en el menú de Parámetros de Citrix Receiver para Android.

Escenarios de verificación recomendados para el respaldo de DTLS:

- Use la URL de la tienda para agregar la tienda y lanzar sesiones.
- Configure la directiva de transporte adaptable y utilice sesiones de XenApp y XenDesktop a través de EDT en lugar de TCP.

Para obtener más información sobre cómo configurar el transporte adaptable, consulte Transporte adaptable.

Configuración automática

Citrix Receiver para Android 3.13.1 ahora configura y detecta las tiendas para los usuarios automáticamente.

> **Nota:**
>
> La configuración manual de las tiendas se ha eliminado.

Problemas resueltos

August 31, 2018

Problemas resueltos en la versión 3.13.9

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos en la versión 3.13.8

- Después de agregar una cuenta, la configuración de Guardar contraseña de la Interfaz Web podría no reflejarse en una sesión. [RFANDROID-570]
- En un VDA ejecutado en la versión 7.5 Cumulative Update 5, es posible que no pueda abrir aplicaciones de edición de texto como el Bloc de notas en una sesión. [RFANDROID-2164]

Problemas resueltos en la versión 3.13.7

En esta versión también se ha resuelto una serie de problemas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos en la versión 3.13.6

- Es posible que Citrix Receiver para Android no lance una sesión al abrir un archivo ICA descargado desde el explorador Web. [#RFANDROID-2098]

Problemas resueltos en la versión 3.13.5

- Puede que Citrix Receiver para Android no inicie correctamente las aplicaciones software como servicio (SaaS). [#RFANDROID-1963]

Problemas resueltos en la versión 3.13.4

- Con esta corrección, puede cambiar el tamaño de Citrix Receiver dinámicamente al usar un Chromebook. [#RFANDROID-1991]

Problemas resueltos en la versión 3.13.3

- Los gráficos en los escritorios publicados pueden aparecer distorsionados al usar una cuenta de demostración en Android Nougat 7.1.1. [#RFANDROID-1990]
- Las tiendas configuradas con balizas internas que apuntan a una ubicación redirigida pueden no conectarse cuando están en una red interna. [#RFANDROID-1992]

Problemas resueltos en la versión 3.13.2

- Las sesiones desconectadas no se inician cuando se agrega la cuenta o se toca Actualizar en el menú. [#RFANDROID-1456]
- Citrix Receiver para Android no enumera las aplicaciones cuando se usa XenApp 6.5. [#RFANDROID-1887]
- Citrix Receiver para Android puede cerrarse inesperadamente al generar iconos antiguos. [#RFANDROID-1958]
- Citrix Receiver para Android puede cerrarse inesperadamente al registrar una cuenta de demostración con un usuario cuyo nombre o apellido contiene espacios en blanco. [#RFANDROID-1960]
- Es posible que Citrix Receiver para Android no pueda instalarse en Chromebooks compatibles con aplicaciones de Android. [#RFANDROID-1968]

Problemas resueltos en la versión 3.13.1

- Citrix Receiver no reconoce el nombre del cliente en el archivo default.ica cuando aparece en una entrada específica de aplicación. [#LC7539]
- La pantalla del VDI parpadea cuando se usa Citrix Receiver para Android 3.11.1. [#RFANDROID-1642, #LC7800]
- Cuando se usan solo certificados para autenticar una sesión, es posible que Citrix Receiver para Android no detecte la puerta de enlace. [#RFANDROID-1882]
- No se respetan las contraseñas que contienen un espacio en blanco al comienzo o al final. [#RFANDROID-1890]
- Citrix Receiver para Android puede cerrarse inesperadamente al conectarse a tiendas configuradas sin autenticación. [#RFANDROID-1929]
- Las tiendas de StoreFront configuradas sin autenticación en NetScaler Gateway pueden no detectarse. [#RFANDROID-1936]
- Es posible que los usuarios no puedan conectarse a los sitios de Interfaz Web configurados detrás de NetScaler Gateway. [#RFANDROID-1937]
- Las aplicaciones de 16 bits pueden aparecer distorsionadas en dispositivos que ejecutan Android Oreo. [#RFANDROID-1938]
- Se han resuelto problemas de conexión con tiendas de PNA y XenApp. Si encuentra el código de error 547, habilite la opción “Permitir acceso a tienda antigua” e intente conectarse de nuevo.

Problemas conocidos

August 31, 2018

Problemas conocidos en la versión 3.13.9

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 3.13.8

Si agrega la cuenta de tienda configurada para la asociación de tipos de archivo en Receiver para Android versión 3.13.7 o una versión anterior y actualiza Receiver a la versión más reciente, Citrix Receiver no se muestra como una opción en el cuadro de diálogo 'Abrir con' cuando selecciona un archivo para abrir.

Como solución alternativa, vaya a **Parámetros** y seleccione **Actualizar**.[RFANDROID-2241]

Problemas conocidos en la versión 3.13.7

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 3.13.6

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 3.13.5

Es posible que Citrix Receiver para Android no lance una sesión al abrir un archivo ICA descargado desde el explorador Web. Como solución temporal, descargue una aplicación de explorador de archivos desde Google Play Store, ubique el archivo en su dispositivo y ábralo directamente. [#RFANDROID-2098]

Problemas conocidos en la versión 3.13.4

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 3.13.3

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 3.13.2

- La opción Anclar al teléfono para agregar aplicaciones y escritorios a la pantalla del teléfono no funciona. [#RFANDROID-1896]
- Esta versión de Citrix Receiver para Android podría no funcionar correctamente con NetScaler Gateway integrado con el sitio Web y los servicios XenApp.

  Como solución temporal, haga lo siguiente:

  1. Toque en “Cerrar sesión (todo)” en Parámetros.
  2. Toque en “Cambiar de cuenta” para ir a la página “Cuentas”.
  3. Elimine la tienda desde la página “Cuentas”.
  4. Agregue la cuenta de nuevo. [#RFANDROID-1900]

Problemas conocidos en la versión 3.13.1

- Las sesiones desconectadas no se inician cuando se agrega la cuenta o se toca Actualizar en el menú. [#RFANDROID-1456]
- Las aplicaciones publicadas en XenApp 6.5 no se inician. [#RFANDROID-1887]
- La opción Anclar al teléfono para agregar aplicaciones y escritorios a la pantalla del teléfono no funciona. [#RFANDROID-1896]
- Esta versión de Citrix Receiver para Android podría no funcionar correctamente con NetScaler Gateway integrado con el sitio Web y los servicios XenApp.

  Como solución temporal, haga lo siguiente:

  1. Toque en “Cerrar sesión (todo)” en Parámetros.
  2. Toque en “Cambiar de cuenta” para ir a la página “Cuentas”.
  3. Elimine la tienda desde la página “Cuentas”.
  4. Vuelva a agregar la cuenta. [#RFANDROID-1900]

Avisos de terceros

August 31, 2018

Los productos de Citrix a menudo incluyen código de terceros que da licencia a Citrix para su uso y redistribución, bajo una licencia de código abierto (Open Source). En un esfuerzo por informar mejor a sus clientes, Citrix publica el código abierto incluido en los productos Citrix en una lista de código con licencia Open Source.

Puede revisar la lista Open Source aquí: https://www.citrix.com/buy/licensing/open-source.html

Para ver más información sobre código fuente, consulte: https://www.citrix.com/downloads/citrix-receiver/receiver-for-android-source/htmlparser.html

Requisitos del sistema

February 7, 2019

Requisitos de dispositivo

Esta versión de Citrix Receiver para Android y las posteriores respaldan Android 4.4 (KitKat), 5.x (Lollipop), 6.x (Marshmallow), 7.x (Nougat) y 8.x (Oreo).

Para obtener resultados óptimos, actualice los dispositivos Android con el software de Android más reciente.

Citrix Receiver para Android respalda el lanzamiento de sesiones desde Receiver para Web, siempre que el explorador Web que se utilice funcione con Receiver para Web. Si no puede iniciar sesiones, configure su cuenta a través de Citrix Receiver para Android directamente.

Consulte la sección Conectividad para obtener información sobre las conexiones seguras en su entorno Citrix.

> **Importante**
>
> Si tiene instalada una versión Tech Preview de Citrix Receiver para Android, desinstálela antes de instalar la nueva versión.

Requisitos del servidor

StoreFront:

- StoreFront 2.6 o versiones posteriores

  Ofrece acceso directo a tiendas de StoreFront. Receiver también respalda versiones anteriores de StoreFront.

- StoreFront configurado con un sitio de Receiver para Web

  Ofrece acceso a los almacenes o tiendas de StoreFront a través de un explorador Web. Para conocer las limitaciones de esta implementación, consulte la documentación de StoreFront.

Interfaz Web (no respaldada en entornos de XenDesktop 7 y posteriores):

- Interfaz Web 5.4 con sitios de Interfaz Web
- Interfaz Web 5.4 con sitios de Servicios XenApp

Interfaz Web en NetScaler:

Debe habilitar las directivas de reescritura suministradas por NetScaler.

XenApp y XenDesktop (cualquiera de los productos siguientes):

- XenApp 7.5 o versiones posteriores
- XenApp 6.5 para Windows Server 2008 R2
- XenDesktop 7.x o versiones posteriores

Conectividad

Citrix Receiver para Android admite conexiones HTTP, HTTPS e ICA sobre TLS con una comunidad de servidores XenApp mediante cualquiera de las configuraciones siguientes.

Para conexiones LAN:

- StoreFront 2.6 o versiones posteriores
- Interfaz Web 5.4
- Sitio de servicios XenApp (antes llamado Agente de Program Neighborhood).

Para conexiones remotas seguras (cualquiera de los productos siguientes):

- Citrix NetScaler Gateway 10 y 11 (incluidas las versiones VPX, MPX y SDX)
- XenMobile solo recibe respaldo con la versión 9 y 10.

Acerca de las conexiones seguras y los certificados TLS

Cuando se protegen las conexiones remotas usando TLS, el dispositivo móvil verifica la autenticidad del certificado TLS de la puerta de enlace remota con un almacén local de entidades de certificación raíz de confianza. Los dispositivos reconocen automáticamente los certificados emitidos comercialmente (como VeriSign y Thawte) siempre que exista el certificado raíz para la entidad de certificación en el almacén local.

Certificados privados (firmados automáticamente)

Si se ha instalado un certificado privado en la puerta de enlace remota, hay que instalar el certificado raíz de la entidad de certificación de la empresa en el dispositivo móvil, para poder acceder correctamente a los recursos Citrix mediante Receiver.

> **Nota:**
>
> Cuando el certificado de la puerta de enlace remota no se puede verificar en la conexión (debido a que no se incluyó el certificado raíz en el almacén de claves local), se muestra un mensaje de advertencia sobre la presencia de un certificado que no es de confianza. Si un usuario elige continuar, haciendo caso omiso del mensaje, se mostrará la lista de aplicaciones pero no se podrán ejecutar.

Certificados comodín

Se usan certificados comodín en lugar de los certificados de servidor individuales para cualquier servidor dentro del mismo dominio. Citrix Receiver para iPhone admite certificados comodín.

Certificados intermedios y NetScaler Gateway

Si la cadena de certificados incluye un certificado intermedio, deberá añadir este certificado al certificado del servidor Access Gateway. Consulte el artículo en Knowledge Center correspondiente a su edición de Access Gateway:

CTX114146: How to Install an Intermediate Certificate on NetScaler Gateway

Además de los temas de configuración en esta sección de la documentación de productos, vea también:

CTX124937: How to Configure NetScaler Gateway for Use with Citrix Receiver for Mobile Devices

Autenticación

> **Nota:**
>
> La autenticación RSA SecurID no está respaldada para las configuraciones de Secure Gateway. Para usar RSA SecurID utilice Access Gateway.

Citrix Receiver para Android admite la autenticación mediante NetScaler Gateway con los métodos siguientes, según la edición disponible:

- Sin autenticación (versiones Standard y Enterprise solamente)
- Autenticación de dominio

- RSA SecurID, incluidos los tokens de software para dispositivos con WiFi y sin WiFi
- Autenticación de dominio complementada con RSA SecurID
- Autenticación mediante envío de código de acceso por SMS (PIN de un solo uso)
- Autenticación con tarjeta inteligente

> **Nota:**
>
> La autenticación mediante tarjeta inteligente en sitios de Interfaz Web no está respaldada.

Citrix Receiver para Android ofrece ahora respaldo para los siguientes productos y configuraciones.

Lectores de tarjetas inteligentes compatibles:

- BaiMobile 3000MP Bluetooth Smart Card Reader

Tarjetas inteligentes respaldadas:

- Tarjetas PIV
- Tarjetas CAC (Common Access Card)

Configuraciones compatibles:

- Autenticación con tarjeta inteligente en NetScaler Gateway con StoreFront 2 o 3 y XenDesktop 7.x y versiones posteriores, o XenApp 6.5 y versiones posteriores
- Autenticación con tarjeta inteligente en NetScaler Gateway con Interfaz Web 5.4.2 y XenDesktop 7.x y versiones posteriores, o XenApp 6.5 y versiones posteriores

> **Nota:**
>
> Se pueden configurar otras soluciones de autenticación basadas en tokens usando RADIUS. Para obtener más información acerca de la autenticación con tokens de SafeWord, consulte Configuración de Autenticación de SafeWord.

Implementación

February 7, 2019

Cómo proporcionar información de acceso a los usuarios finales de dispositivos Android

Debe facilitar a los usuarios la información de cuenta de Citrix Receiver que necesitan para poder acceder a aplicaciones, escritorios y datos alojados en servidores. Puede proporcionarles esta información de las siguientes formas:

- Configurando la detección de cuentas basada en direcciones de correo electrónico

- Entregándoles un archivo de aprovisionamiento
- Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente

Configurar la detección de cuentas basada en direcciones de correo electrónico

Puede configurar Citrix Receiver para que use la detección de cuentas basada en correo electrónico. Cuando está configurada, los usuarios introducen su dirección de correo electrónico, en lugar de una dirección URL de servidor, durante la instalación y configuración inicial de Citrix Receiver. Citrix Receiver determina el servidor Access Gateway o StoreFront que está asociado con esa dirección de correo electrónico, basándose en los registros del servicio (SRV) de sistema de nombres de dominio (DNS) y pide a los usuarios que inicien la sesión para acceder a sus aplicaciones, escritorios y datos alojados en servidores.

> **Nota:**
>
> La detección de cuentas basada en correo electrónico no está respaldada si Citrix Receiver se conecta a una implementación de Interfaz Web.

Entrega de un archivo de aprovisionamiento a los usuarios

Es posible utilizar StoreFront para crear archivos de aprovisionamiento que contengan los detalles de conexión de las cuentas. Estos archivos se ponen a disposición de los usuarios para que puedan configurar Citrix Receiver de forma automática. Después de instalar Citrix Receiver, los usuarios solo tienen que abrir el archivo .cr en el dispositivo para configurar Citrix Receiver. Si se configuran sitios de Receiver para Web, los usuarios también pueden obtener los archivos de aprovisionamiento de Citrix Receiver desde esos sitios.

Para obtener más información, consulte la documentación de StoreFront.

Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente

Si va a entregar a los usuarios los datos de sus cuentas para que luego los introduzcan manualmente, asegúrese de distribuir la siguiente información para permitirles conectar con éxito con sus aplicaciones y escritorios alojados en servidores:

- La dirección URL de StoreFront o del sitio de servicios XenApp que aloja los recursos; por ejemplo, servidor.empresa.com.
- Para acceder mediante NetScaler Gateway, facilite la dirección de NetScaler Gateway y el método de autenticación requerido.

  Para obtener más información sobre cómo configurar NetScaler Gateway, consulte la documentación de NetScaler Gateway.

Cuando un usuario introduce la información de una cuenta nueva, Citrix Receiver intenta verificar la conexión. Si la conexión puede establecerse, Citrix Receiver solicita al usuario que inicie sesión en la cuenta.

Cómo proporcionar autenticación de RSA SecurID para dispositivos Android

Si se configura NetScaler Gateway para la autenticación RSA SecurID, Citrix Receiver respalda el modo de token siguiente (Next Token). Si esta característica está habilitada, cuando un usuario introduce la contraseña incorrecta tres veces (valor predeterminado), NetScaler Gateway plug-in solicita al usuario que espere hasta que se active el próximo token antes de iniciar una sesión. Asimismo, el servidor RSA se puede configurar para inhabilitar una cuenta de usuario si el usuario intenta iniciar una sesión demasiadas veces con la contraseña incorrecta.

Para ver instrucciones sobre cómo configurar la autenticación, consulte Autenticación y autorización.

> **Sugerencia**
>
> La autenticación RSA SecurID no está respaldada para las configuraciones de Secure Gateway. Para usar RSA SecurID, use NetScaler Gateway.

Instalación de tokens de software de RSA SecurID

Los archivos de autenticación RSA SecurID de software (RSA SecurID Software Authenticator) tienen la extensión .sdtid. Use el programa RSA SecurID Software Token Converter para convertir el archivo .sdtid a una cadena numérica con formato XML de 81 dígitos. En el sitio Web de RSA puede obtener el software y la información más reciente.

Siga estos pasos generales:

1. En un equipo (no en un dispositivo móvil), descargue la herramienta de conversión desde aquí. Siga las instrucciones en el sitio Web y en el archivo Léame que se incluye con la herramienta.
2. Pegue la cadena numérica convertida dentro de un mensaje de correo electrónico y envíelo a los dispositivos de usuario.
3. Asegúrese de que la fecha y la hora en el dispositivo móvil sean correctas, ya que esto es necesario para la autenticación.
4. En el dispositivo móvil, abra el correo y haga clic en la cadena para iniciar el proceso de importación del token de software.

Después de instalar el token de software en el dispositivo, se muestra una nueva opción en la ficha Configuración para administrar el token.

> **Nota:**
>
> Para los dispositivos móviles que no asocian el archivo .sdtid con Receiver, cambie la extensión del archivo por .xml y, a continuación, impórtelo.

Cómo guardar contraseñas

Mediante la consola de administración de la Interfaz Web de Citrix, puede configurar el método de autenticación para permitir que los usuarios guarden sus contraseñas. Cuando se configura la cuenta de usuario, la contraseña cifrada se guarda hasta que el usuario se conecta por primera vez.

- Si se habilita el almacenamiento de contraseñas, Citrix Receiver almacena la contraseña en el dispositivo para inicios de sesión futuros y ya no se solicitan las contraseñas cuando los usuarios se conectan con las aplicaciones.

> **Nota:**
>
> La contraseña se almacena solamente si los usuarios introducen una contraseña cuando se crea una cuenta. Si no se introduce una contraseña para la cuenta, no se guarda ninguna contraseña, independientemente de cómo se haya configurado este parámetro en el servidor.

- Si se inhabilita el almacenamiento de contraseñas (configuración predeterminada), Citrix Receiver solicita a los usuarios que introduzcan sus contraseñas cada vez que se conectan.

> **Nota:**
>
> Para conexiones directas con StoreFront, no es posible guardar la contraseña.

Para anular el parámetro de almacenamiento de contraseñas

Si se configura el servidor para que almacene las contraseñas, los usuarios que prefieran que les sean solicitadas las mismas cada vez que inician una sesión pueden anular dicho parámetro:

- Al crear la cuenta, deje el campo de contraseña en blanco.
- Al modificar la cuenta, elimine la contraseña y guarde la cuenta.

Configuración

January 14, 2019

Concesión de acceso a aplicaciones y escritorios virtuales

Citrix Receiver necesita la configuración de la Interfaz Web o de StoreFront para entregar aplicaciones y escritorios desde una implementación de XenApp o XenDesktop.

Interfaz Web

Existen dos tipos de sitios de Interfaz Web: sitios de servicios XenApp (anteriormente servicios de Program Neighborhood) y sitios Web XenApp. Los sitios de la Interfaz Web permiten que los dispositivos de usuario se conecten a la comunidad de servidores.

StoreFront

Puede configurar StoreFront para ofrecer servicios de autenticación y entrega de recursos para Citrix Receiver, lo que le permite crear unas tiendas o almacenes de empresa centralizadas para entregar escritorios y aplicaciones a través de XenApp y XenDesktop, así como aplicaciones móviles de Worx y aplicaciones móviles preparadas para la organización, a través de XenMobile.

La autenticación entre Citrix Receiver y un sitio de Interfaz Web o un almacén o tienda de StoreFront se puede gestionar de varias formas:

- Los usuarios dentro del firewall pueden conectar directamente con el sitio de Interfaz Web o StoreFront.
- Los usuarios situados fuera del firewall pueden conectarse a StoreFront o la Interfaz Web a través de NetScaler Gateway.
- Los usuarios fuera del firewall pueden conectar a través de NetScaler Gateway con StoreFront.

Conexiones a través de NetScaler Gateway

NetScaler Gateway 10 y 11 reciben respaldo en Citrix Receiver para Android para acceder a:

- Sitios de servicios XenApp y sitios Web XenApp de la Interfaz Web 5.4
- Tiendas de StoreFront 2.6, 3.0, 3.5, 3.6, 3.7, 3.8, 3.9 y 3.11

En los sitios de la Interfaz Web y StoreFront se respaldan tanto la autenticación de un solo origen como la autenticación de doble origen.

Se pueden crear varias directivas de sesión en un mismo servidor virtual dependiendo del tipo de conexión (ICA, CVPN o VPN) y el tipo de Receiver (Receiver para Web o Receiver instalado localmente) que se utilicen. Todas las directivas pueden obtenerse a partir de un único servidor virtual.

Para crear cuentas en Citrix Receiver, los usuarios deben introducir las credenciales de la cuenta, como la dirección de correo electrónico o el nombre de dominio completo correspondiente para el

servidor NetScaler Gateway. Por ejemplo, si no se puede establecer la conexión cuando se utiliza la ruta predeterminada, los usuarios deben introducir la ruta completa al servidor NetScaler Gateway.

Para conectar con XenMobile

Para permitir que los usuarios remotos se conecten mediante NetScaler Gateway a la implementación de XenMobile, puede configurar NetScaler Gateway para que funcione con AppController o StoreFront (ambos son componentes de XenMobile). El método que se debe utilizar para habilitar el acceso depende de la edición de XenMobile en la implementación:

Habilitación del acceso a XenMobile 9:

Autenticación con certificados de cliente

Habilitación del acceso a XenMobile 10:

XenMobile y NetScaler Gateway

Si desea implementar XenMobile en la red, integre XenMobile y AppController para permitir las conexiones de los usuarios remotos a AppController. Con esta implementación, los usuarios pueden conectarse a AppController para obtener aplicaciones Web, móviles y de software como servicio (SaaS), y acceder a documentos desde ShareFile. Los usuarios se pueden conectar mediante Citrix Receiver o el NetScaler Gateway Plug-in.

Si desea implementar XenMobile en la red, integre NetScaler y StoreFront para permitir las conexiones de los usuarios internos o remotos a StoreFront a través de NetScaler Gateway. Con esta implementación, los usuarios pueden conectarse a StoreFront para acceder a las aplicaciones publicadas desde XenApp y a los escritorios virtuales desde XenDesktop. Los usuarios se pueden conectar mediante Citrix Receiver.

Para implementar aplicaciones Windows y personalizadas para los usuarios, necesita empaquetar las aplicaciones usando el MDX Toolkit. Encontrará más información aquí:

MDX Toolkit

Conexión con StoreFront

Citrix Receiver para Android respalda el lanzamiento de sesiones desde Receiver para Web, siempre que el explorador Web que se utilice funcione con Receiver para Web. Si no puede iniciar sesiones, configure su cuenta a través de Citrix Receiver para Android directamente.

> **Sugerencia**
>
> Cuando se usa Citrix Receiver para Web desde un explorador Web, las sesiones no se inician automáticamente al descargar un archivo .ICA. El archivo .ICA debe abrirse manualmente después

> de descargarlo para que la sesión se inicie.

Con StoreFront, las tiendas que se crean consisten en servicios que proporcionan una infraestructura de recursos y autenticación para Citrix Receiver. Cree tiendas que enumeren y agrupen escritorios y aplicaciones de sitios de XenDesktop y comunidades XenApp, habilitando estos recursos para los usuarios.

Para los administradores que necesitan más control, Citrix proporciona una plantilla que se puede usar para crear un sitio de descargas de Receiver para Android.

Configure tiendas para StoreFront de la misma forma que con otras aplicaciones de XenApp y XenDesktop. No se requiere ninguna configuración especial para los dispositivos móviles. Para dispositivos móviles, use alguno de estos métodos:

Archivos de aprovisionamiento.Puede dar a los usuarios unos archivos de aprovisionamiento (.cr) que contienen los datos de conexión con sus tiendas. Después de la instalación, los usuarios abren el archivo en el dispositivo para configurar Citrix Receiver automáticamente. De forma predeterminada, los sitios de Receiver para Web ofrecen a los usuarios un archivo de aprovisionamiento para la única tienda para la que esté configurado el sitio en cuestión. De forma alternativa, es posible utilizar la consola de administración de Citrix StoreFront con el fin de generar archivos de aprovisionamiento para una o varias tiendas que se puedan distribuir manualmente a los usuarios.

Configuración manual.Puede informar directamente a los usuarios sobre las direcciones URL de las tiendas o de NetScaler Gateway que necesitan para acceder a sus escritorios y aplicaciones. Para las conexiones a través de NetScaler Gateway, los usuarios también deben conocer el método de autenticación requerido y la edición del producto. Después de la instalación, los usuarios deben introducir estos detalles en Citrix Receiver, que intenta verificar la conexión y, si la conexión es satisfactoria, solicita a los usuarios que inicien sesión.

Para configurar Citrix Receiver para acceder a aplicaciones:

Al crear una cuenta nueva, en el campo Dirección, introduzca la URL correspondiente a su tienda o almacén, por ejemplo, storefront.empresa.com.

Rellene el resto de los campos y seleccione el método de autenticación de NetScaler Gateway, como la habilitación del token de seguridad, la selección del tipo de autenticación y el almacenamiento de los parámetros.

Al agregar una cuenta usando una configuración automática se puede introducir el nombre completo de dominio (FQDN) o un servidor StoreFront o NetScaler, o se puede usar una dirección de correo electrónico para crear una nueva cuenta. A continuación se le pedirá que introduzca las credenciales de usuario antes de iniciar la sesión.

Más información:

Para obtener más información sobre cómo configurar el acceso a StoreFront a través de NetScaler Gateway, consulte:

Administración del acceso a StoreFront a través de NetScaler Gateway

Integración de StoreFront con NetScaler Gateway

Conexión con la Interfaz Web

Citrix Receiver puede iniciar aplicaciones mediante el sitio de la Interfaz Web. Configure el sitio de la Interfaz Web de la misma forma que lo haría para otras aplicaciones y escritorios de XenApp y XenDesktop. No se requiere ninguna configuración especial para los dispositivos móviles.

Citrix Receiver respalda solo la versión 5.4 de la Interfaz Web. Además, los usuarios pueden iniciar aplicaciones desde la Interfaz Web 5.4 mediante el explorador móvil Firefox.

Para iniciar aplicaciones en el dispositivo Android:

Desde el dispositivo, los usuarios inician una sesión en el sitio de la Interfaz Web con sus credenciales normales.

Para obtener información sobre cómo configurar sitios de Interfaz Web, consulte:

Configuración de la Interfaz Web

Sincronización de la distribución de teclado

Para habilitar la sincronización de la distribución del teclado, vaya a Parámetros en Citrix Receiver para Android y marque la casilla **IME del cliente**.

Notas:

- La versión del VDA debe 7.16 o posterior.
- Los administradores deben habilitar la función de Respaldo mejorado para idiomas asiáticos en el VDA. De manera predeterminada, esta funcionalidad está habilitada. Sin embargo, en los VDA de Windows Server 2016, es necesario agregar una clave nueva al Registro llamada DisableKeyboardSync, y darle el valor 0 en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA\IcaIme, para habilitar la función.
- Los administradores deben habilitar la función de asignación de distribución de teclado Unicode en el VDA. De forma predeterminada, esta función está inhabilitada. Para habilitarla, cree la clave CtxKlMap bajo HKEY_LOCAL_MACHINE\SOFTWARE\Citrix y establezca el valor DWORD EnableKlMap = 1 en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap.

Limitaciones:

- Esta característica solo funciona en los teclados internos de los dispositivos, no en teclados externos.
- Ciertos dispositivos móviles pueden no ser totalmente compatibles con la sincronización de la distribución del teclado, como el Nexus 5x.

- La distribución del teclado solo puede sincronizarse desde el cliente hacia el servidor. Cuando se cambia la distribución del teclado en el lado del servidor, la del cliente no puede cambiarse.
- Cuando se cambia la distribución de teclado del cliente a una distribución que no está respaldada, es posible que se sincronice la distribución en el VDA, pero no se puede confirmar la funcionalidad.
- Las aplicaciones remotas que se ejecutan con privilegios elevados (por ejemplo, aplicaciones ejecutadas como administrador) no se pueden sincronizar con la distribución de teclado del cliente. Para solucionar este problema, cambie manualmente la distribución del teclado en el VDA o inhabilite el control de cuentas de usuario (UAC).

Habilitación del respaldo para tarjetas inteligentes

Receiver para dispositivos móviles con Android proporciona respaldo para lectores de tarjeta inteligente Bluetooth con sitios de PNA, Interfaz Web y StoreFront. Si el respaldo para tarjetas inteligentes está habilitado, es posible utilizar tarjetas inteligentes para los siguientes propósitos:

- Autenticación de inicio de sesión con tarjetas inteligentes. Utilice tarjetas inteligentes para autenticar usuarios en Receiver.
- Respaldo para aplicaciones de tarjetas inteligentes. Habilite las aplicaciones publicadas compatibles con tarjetas inteligentes para que puedan acceder a dispositivos de tarjetas inteligentes locales.
- Firma de documentos y correo electrónico. Las aplicaciones como Microsoft Word y Outlook que se inician en las sesiones de ICA pueden acceder a las tarjetas inteligentes en el dispositivo móvil para firmar documentos y el correo electrónico.

Tarjetas inteligentes respaldadas:

- Tarjetas PIV
- Tarjetas CAC (Common Access Card)

Configuración del respaldo para tarjetas inteligentes en el dispositivo

1. Debe emparejar la tarjeta inteligente con el dispositivo móvil. Para obtener más información sobre el emparejamiento de los lectores de tarjeta inteligente con el dispositivo, consulte las especificaciones del lector de tarjeta inteligente.

   El respaldo para tarjetas inteligentes para los dispositivos Android presenta los siguientes requisitos previos y limitaciones.

   - Receiver admite esta función en todos los dispositivos Android incluidos en el middleware de Biometric Associates.

- Es posible que algunos usuarios tengan un número PIN global para tarjetas inteligentes. No obstante, cuando los usuarios inician sesión en una cuenta de tarjeta inteligente, deben introducir el PIN de PIV, no el PIN global de la tarjeta inteligente. Este es una limitación de terceros.
- Es posible que la autenticación con tarjeta inteligente sea más lenta que la autenticación mediante contraseña. Por ejemplo, después de desconectarse de una sesión, espere aproximadamente 30 segundos antes de volver a conectarse. Si se vuelve a conectarse a una sesión desconectada demasiado rápido, esto puede hacer que Receiver produzca un error.
- La autenticación mediante tarjeta inteligente no recibe respaldo para el acceso basado en exploradores Web o desde sitios XenApp.

2. Instale el servicio PC/SC-Lite de Android en el dispositivo Android antes de agregar una cuenta para tarjeta inteligente. Este servicio se encuentra disponible como un archivo .apk en el SDK de baiMobile.

   Para Android, el archivo PC/SC-Lite se puede descargar desde la tienda de aplicaciones Google Play.

3. En Receiver, seleccione el icono Parámetros y, a continuación, seleccione **Cuentas** y **Agregar cuenta**, o bien, edite una cuenta existente.
4. Configure la conexión y active la opción de tarjeta inteligente.

Instalación de Citrix Receiver en una tarjeta SD

Citrix Receiver para Android está optimizado para la instalación local en los dispositivos de los usuarios. No obstante, si los dispositivos no tienen suficiente espacio, los usuarios pueden instalar Receiver en una tarjeta SD externa y montarlo en el dispositivo para iniciar aplicaciones publicadas en sus dispositivos móviles. Este respaldo se suministra de forma predeterminada y no se requiere configuración adicional.

Para iniciar una aplicación con una tarjeta SD, seleccione la aplicación de la lista de aplicaciones de Receiver en el dispositivo de usuario, y después seleccione la opción Mover a tarjeta SD.

Si los usuarios deciden instalar Receiver en una tarjeta SD externa para iniciar aplicaciones, se generan los problemas siguientes:

- Al montar un dispositivo de almacenamiento USB mientras la tarjeta SD está montada en el dispositivo móvil hace que la tarjeta SD deje de estar disponible, y las aplicaciones que se estaban ejecutando se interrumpen cuando se monta el dispositivo USB.
- Algunos AppWidgets (como los widgets de pantalla principal) no están disponibles cuando se ejecuta una aplicación desde la tarjeta SD. Después de desmontar la tarjeta SD, los usuarios deben reiniciar los AppWidgets.

Si los usuarios instalan Receiver localmente en sus dispositivos de usuario, pueden mover Receiver a la tarjeta SD cuando lo necesiten.

Acceder a archivos usando la asociación de tipos de archivo

Como requisito previo para que funcione esta característica, vaya a los parámetros de Receiver para Android y configure la opción **Usar almacenamiento del dispositivo** en **Acceso total**.

Receiver para Android lee y aplica los parámetros configurados por los administradores en Citrix Studio.
Para aplicar la asociación de tipos de archivo (File Type Association - FTA) en una sesión, asegúrese de que los usuarios se conecten al servidor de la tienda donde está configurada la asociación de tipos de archivo.

En el dispositivo del usuario, seleccione el archivo que desea iniciar en el Explorador de archivos y haga clic en Abrir. El sistema operativo Android ofrece una opción para iniciar el archivo usando Receiver para Android (aplicando la asociación de tipos de archivo configurada por el administrador) o una aplicación diferente. Dependiendo de lo que haya seleccionado, puede haber o no una aplicación predeterminada. Puede cambiar la aplicación predeterminada utilizando la opción para cambiar el valor predeterminado.

> **Nota:**
>
> Esta función solo está disponible en StoreFront y requiere XenApp y XenDesktop versión 7 o una versión posterior.

Limitación

- Puede acceder solo a los formatos de archivo MIME admitidos por Microsoft Office, Adobe Acrobat Reader y Bloc de notas mediante la función de asociación de tipos de archivo.

Habilitar Citrix Ready Workspace Hub

September 19, 2018

Citrix Ready Workspace Hub está inhabilitado de manera predeterminada en Citrix Receiver para Android. Para usar el Hub con un dispositivo Android, siga los pasos indicados a continuación.

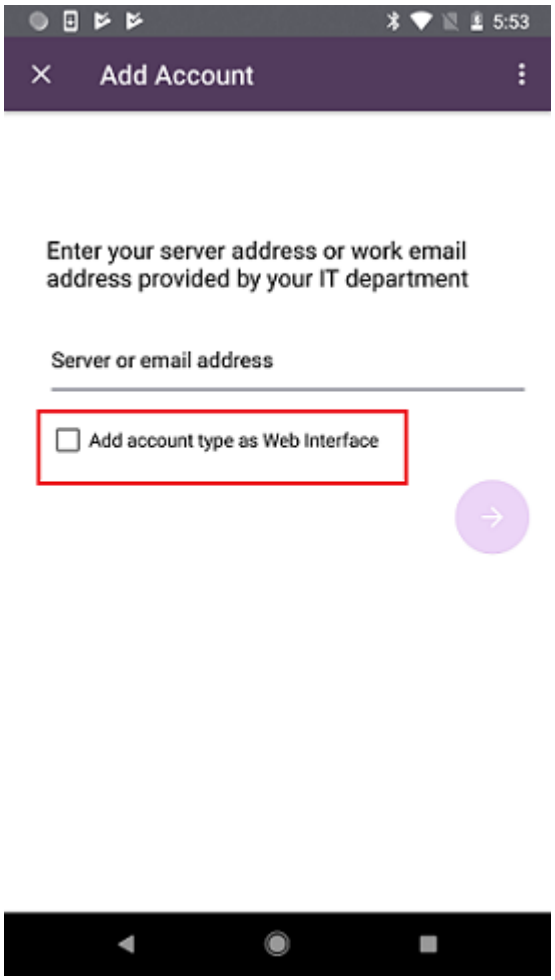
Requisitos previos del dispositivo:

- Tener instalado Citrix Receiver para Android 3.13.5, o una versión posterior

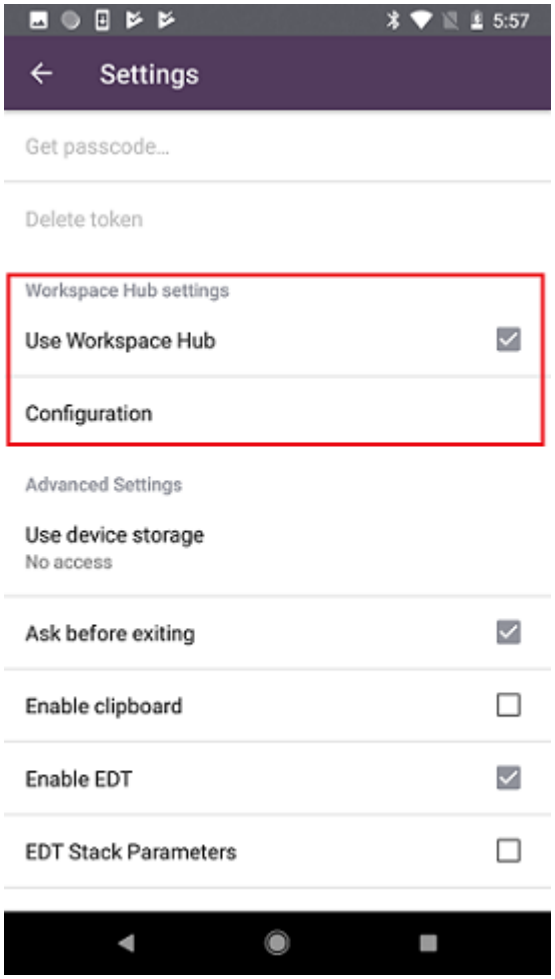
- Tener Bluetooth habilitado (para la autenticación de proximidad)
- El dispositivo móvil y Workspace Hub deben utilizar la misma red Wi-Fi

La autenticación de proximidad proporciona una forma de autenticar usuarios y lanzar una sesión automáticamente.

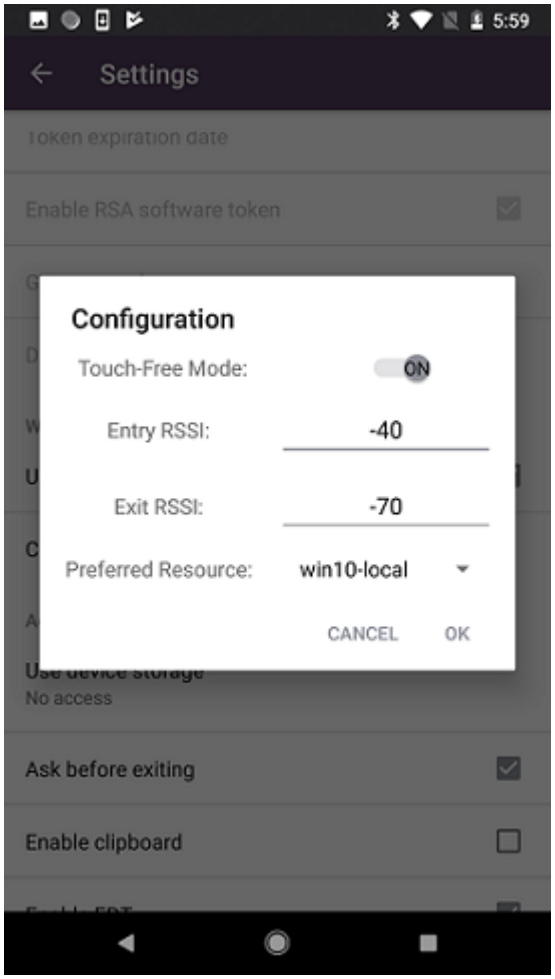
1. Para utilizar la autenticación de proximidad, habilite Bluetooth en el dispositivo móvil para asegurarse de que la casilla “Agregar tipo de cuenta como Interfaz Web” no esté seleccionada al configurar la cuenta de Citrix Receiver.



2. En Citrix Receiver, vaya a **Parámetros** y seleccione **Usar Workspace Hub**.



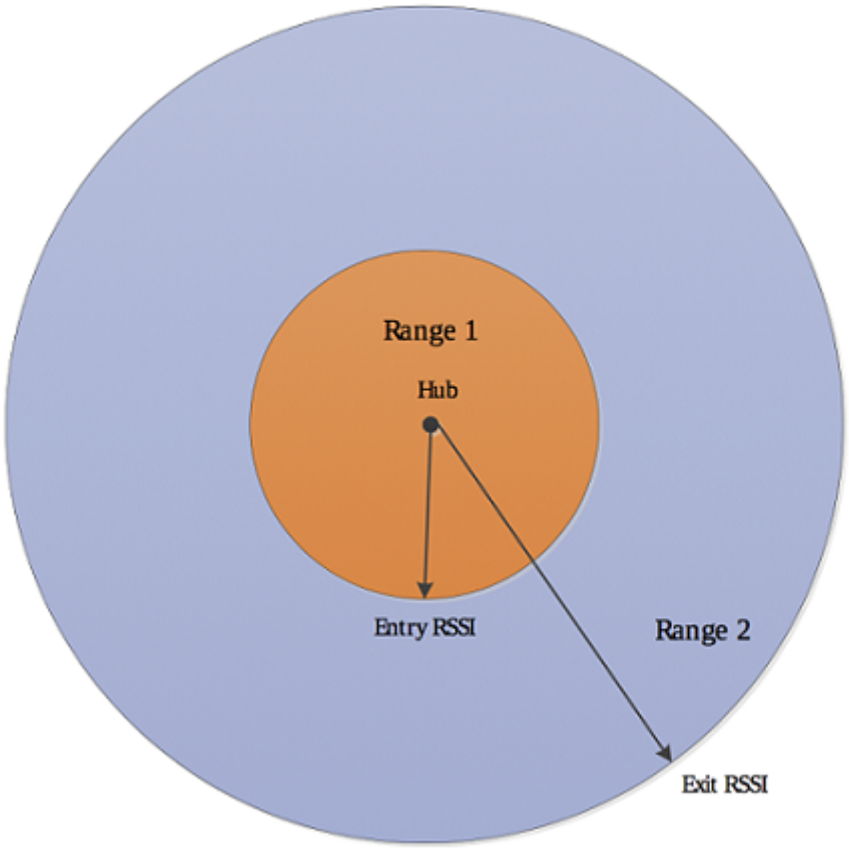
3. Haga clic en **Configuración** para abrir la página Configuración.



El **Modo sin contacto** es un conmutador que permite habilitar o inhabilitar la autenticación de proximidad. Cuando el modo sin contacto está desactivado, la autenticación de proximidad no está disponible, pero las demás funciones del Citrix Ready Workspace Hub sí lo están. Para usar el modo sin contacto, Bluetooth debe estar habilitado en el dispositivo.

RSSI representa la intensidad de la señal de Bluetooth en relación con la distancia entre el dispositivo móvil y el Hub. RSSI de entrada es el rango en el que se detectan las balizas del Workspace Hub. RSSI de salida es el comienzo del rango fuera del cual el dispositivo móvil ya no se comunica con el Workspace Hub. El RSSI de salida debe ser igual o menor que el RSSI de entrada y los valores deben ser negativos. Los valores predeterminados son -40 (RSSI de entrada) y -70 (RSSI de salida), respectivamente. Puede ajustar estos valores en función de su entorno y su rango desde el Workspace Hub.

Como se muestra a continuación, cuando se mueve el dispositivo móvil al Rango 1, se activa la autenticación de proximidad y su aplicación o escritorio predeterminado se inicia automáticamente en el Workspace Hub. Siempre que el dispositivo móvil permanezca dentro del rango 1 o 2, el escritorio o la aplicación seguirán ejecutándose en el Workspace Hub. Cuando el dispositivo se saca fuera del Rango 1 y 2, el escritorio o la aplicación se cierran automáticamente.



Recurso preferido es la aplicación o el escritorio predeterminado que se inicia cuando el dispositivo móvil entra en el rango de la autenticación de proximidad. Este parámetro es específico de la cuenta utilizada para iniciar sesión en Citrix Receiver. Si tiene más de una cuenta, debe definir un recurso preferido para cada una. Este parámetro es persistente, lo que significa que solo es necesario configurarlo una vez para cada cuenta. Una vez definido, el recurso preferido se iniciará cada vez que entre en el rango de autenticación de proximidad, hasta que decida cambiar el parámetro.

Solucionar problemas

November 8, 2018

Directiva de validación conjunta de certificados de servidor

Esta versión de Citrix Receiver para Android tiene una directiva nueva más estricta para validar los certificados de servidor.

> **Importante**
>
> Antes de instalar esta versión de Citrix Receiver para Android, confirme que los certificados presentes en el servidor o la puerta de enlace se han configurado correctamente como se describe aquí. Las conexiones pueden fallar si:
>
> - la configuración del servidor o la puerta de enlace incluye un certificado raíz incorrecto
> - la configuración del servidor o la puerta de enlace no incluye todos los certificados intermedios
> - la configuración del servidor o la puerta de enlace incluye un certificado intermedio caducado o no válido
> - la configuración del servidor o la puerta de enlace incluye un certificado intermedio con firmas cruzadas

Cuando valida un certificado de servidor, Citrix Receiver para Android usa ahora **todos** los certificados suministrados por el servidor (o la puerta de enlace). Al igual que en las versiones anteriores, esta versión de Citrix Receiver para Android también comprueba posteriormente que los certificados son de confianza.Si no todos los certificados son de confianza, la conexión falla.

Esta directiva es más estricta que la directiva de certificados presente en los exploradores Web.Muchos exploradores Web incluyen un gran conjunto de certificados raíz en los que confían.

El servidor (o la puerta de enlace) debe estar configurado con el conjunto correcto de certificados.Un conjunto incorrecto de certificados puede provocar que falle la conexión de Citrix Receiver para Android.

Supongamos que se configura una puerta de enlace con estos certificados válidos. Esta configuración se recomienda para los clientes que requieren una validación más estricta, que necesitan determinar exactamente cuál es el certificado raíz que usa Citrix Receiver para Android:

- “Certificado de servidor - ejemplo”
- “Certificado intermedio - ejemplo”
- “Certificado raíz - ejemplo”

A continuación, Citrix Receiver para Android comprobará que todos los certificados son válidos.Citrix Receiver para Android comprobará también que ya confía en “Certificado raíz - ejemplo”. Si Citrix Receiver para Android no confía en “Certificado raíz - ejemplo”, la conexión falla.

> **Importante**
>
> Algunas entidades de certificación tienen más de un certificado raíz. Si necesita usar esta validación más estricta, compruebe que la configuración usa el certificado raíz correspondiente. Por ejemplo, actualmente hay dos certificados (“DigiCert”/”GTE CyberTrust Global Root” y “DigiCert Baltimore Root”/”Baltimore CyberTrust Root”) que pueden validar los mismos certificados de servidor. En algunos dispositivos de usuario, están disponibles ambos certificados raíz. En

> otros dispositivos, solo uno está disponible (“DigiCert Baltimore Root” o “Baltimore CyberTrust Root”). Si configura “GTE CyberTrust Global Root” en la puerta de enlace, fallarán las conexiones de Citrix Receiver para Android en esos dispositivos de usuario.Consulte la documentación de la entidad de certificación para determinar qué certificado raíz debe usarse.Tenga en cuenta que los certificados raíz también caducan, como todos los demás certificados.
>
> **Nota**
>
> Algunos servidores y puertas de enlace nunca envían el certificado raíz, aunque se haya configurado. En esos casos, esta validación más estricta no es posible.

Supongamos ahora que se configura una puerta de enlace usando estos certificados válidos.Esta configuración, sin certificado raíz, es la que se suele recomendar:

- “Certificado de servidor - ejemplo”
- “Certificado intermedio - ejemplo”

Citrix Receiver para Android usará esos dos certificados. Luego, buscará un certificado raíz en el dispositivo del usuario.Si encuentra uno que se valida correctamente y también es de confianza (por ejemplo, “Certificado raíz - ejemplo”), la conexión se realiza correctamente. De lo contrario, la conexión falla. Esta configuración proporciona el certificado intermedio que necesita Citrix Receiver para Android, pero también permite que Citrix Receiver para Android elija cualquier certificado raíz válido y de confianza.

Supongamos ahora que se configura una puerta de enlace con estos certificados:

- “Certificado de servidor - ejemplo”
- “Certificado intermedio - ejemplo”
- “Certificado raíz incorrecto”

Un explorador Web podría ignorar el certificado raíz incorrecto. No obstante, Citrix Receiver para Android no ignorará el certificado raíz incorrecto y la conexión fallará.

Algunas entidades de certificación usan más de un certificado intermedio.En este caso, la puerta de enlace se configura normalmente con todos los certificados intermedios (pero sin el certificado raíz):

- “Certificado de servidor - ejemplo”
- “Certificado intermedio 1 - ejemplo”
- “Certificado intermedio 2 - ejemplo”

> **Importante**
>
> Algunas entidades de certificación usan un certificado intermedio con firmas cruzadas.Este tipo de certificado está pensado para situaciones en que hay más de un certificado raíz: un certificado raíz anterior se usa al mismo tiempo que un certificado raíz posterior.En este caso, habrá al menos dos certificados intermedios.Por ejemplo, el certificado raíz anterior “Class 3 Public Primary Certification Authority” tiene el certificado intermedio correspondiente de firmas cruzadas

> "VeriSign Class 3 Public Primary Certification Authority - G5".No obstante, un certificado raíz correspondiente posterior "VeriSign Class 3 Public Primary Certification Authority - G5" también está disponible y reemplaza a "Class 3 Public Primary Certification Authority". El certificado raíz posterior no usa ningún certificado intermedio con firmas cruzadas.
>
> **Nota**
>
> El certificado intermedio con firmas cruzadas y el certificado raíz tienen el mismo Nombre de sujeto (Emitido para), pero el certificado intermedio con firmas cruzadas tiene otro Nombre de emisor (Emitido por). Esto distingue el certificado intermedio con firmas cruzadas de un certificado intermedio normal (como "Certificado intermedio 2 - ejemplo").

Esta configuración, sin certificado raíz y sin certificado intermedio con firmas cruzadas, es la que se suele recomendar:

- "Certificado de servidor - ejemplo"
- "Certificado intermedio - ejemplo"

No configure la puerta de enlace para que use el certificado intermedio con firmas cruzadas, porque seleccionará el certificado raíz anterior:

- "Certificado de servidor - ejemplo"
- "Certificado intermedio - ejemplo"
- "Certificado intermedio con firmas cruzadas - ejemplo" [no recomendado]

No se recomienda configurar la puerta de enlace usando solamente el certificado del servidor:

- "Certificado de servidor - ejemplo"

En este caso, si Citrix Receiver para Android no puede localizar todos los certificados intermedios, la conexión fallará.

SDK y API

August 31, 2018

Citrix Virtual Channel SDK

El Citrix Virtual Channel Software Development Kit (SDK) ofrece respaldo para la escritura de aplicaciones del lado del servidor y controladores del lado del cliente para canales virtuales adicionales con el protocolo ICA. Las aplicaciones de canal virtual del lado del servidor se encuentran en servidores XenApp o XenDesktop. Esta versión del SDK ofrece respaldo para la escritura de canales virtuales

nuevos en Receiver para Android. Si desea escribir controladores virtuales para otras plataformas cliente, póngase en contacto con Citrix.

El Virtual Channel SDK ofrece:

- Interfaces de Citrix Android Virtual Driver AIDL: **IVCService.aidl** y **IVCCallback.aidl**, que se usan con las funciones de canal virtual en el SDK WFAPI (Citrix Server API SDK) para crear nuevos canales virtuales.
- Una clase auxiliar **Marshall.java** diseñada para facilitar la escritura de sus propios canales virtuales.
- Código fuente operacional de tres ejemplos de programas de canales virtuales, que demuestran varias técnicas de programación.

El Virtual Channel SDK requiere el SDK de WFAPI para escribir la parte del lado del servidor del canal virtual. Para obtener más información sobre el SDK, consulte Citrix Virtual Channel SDK para Citrix Receiver para Android.

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