Citrix Receiver para Android 3.11

Jun 04, 2017

Acerca de Citrix Receiver para Android 3.11

Jun 04, 2017

Citrix Receiver para Android permite el acceso inmediato a aplicaciones y escritorios virtuales desde tabletas y teléfonos móviles, incluidas las aplicaciones optimizadas para uso táctil para uso de baja intensidad en tabletas, como alternativa al uso de equipos de escritorio.

Citrix Receiver para Android 3.11 es la versión actual en Google Play. Los usuarios que ejecutan versiones anteriores deben actualizar el producto a la versión más reciente. El método preferido para instalar o actualizar Citrix Receiver para Android es obtenerlo desde Google Play en un dispositivo Android. Esto permite actualizar el producto automáticamente a medida que se publican nuevas versiones.

Citrix Receiver para Android se puede obtener en inglés, alemán, francés, español, japonés, chino simplificado, coreano, italiano, portugués, holandés, sueco y danés.

Novedades en Citrix Receiver para Android 3.11.1

En esta versión de Citrix Receiver para Android, se da respaldo para certificados SAN y se resuelven varios problemas con el fin de mejorar la experiencia de usuario.

Novedades en Citrix Receiver para Android 3.11

Esta versión de Citrix Receiver para Android ofrece un SDK de canal virtual (VC) para dar respaldo a la escritura de canales virtuales con Citrix Receiver para Android.

Problemas resueltos

Jun 04, 2017

Problemas resueltos en 3.11

Esta versión no corrige ningún problema notificado por clientes.

Problemas conocidos

Jun 04, 2017

Problemas conocidos en 3.11

Se han identificado los problemas siguientes en la versión 3.11:

- Al agregar un almacén que usa la experiencia unificada de StoreFront y el acceso se hace a través de NetScaler Gateway, los usuarios tienen que introducir sus credenciales de inicio de sesión varias veces para iniciar sesión con éxito (incluida la petición de credenciales de inicio de sesión de NetScaler). Este problema solo afecta en el primer uso del almacén; en usos posteriores, solo se inicia sesión a través de la petición de credenciales de NetScaler.

  [RFANDROID-772]

- En ciertos dispositivos, no se puede agregar almacenes usando una tarjeta inteligente.

  [RFANDROID-865]

- Cuando no hay ningún certificado instalado en un dispositivo de usuario, Citrix Receiver no puede lanzar sesiones a través de NetScaler Gateway y aparece el siguiente mensaje de error:

"Problema general Intente conectar de nuevo."

  [RFANDROID-916]

- Los intentos de conexión con StoreFront o con VDA pueden fallar al usar una tarjeta inteligente. Este problema está relacionado con la aplicación PCSC-Lite de baiMobile.

  [RFANDROID-1169]

- Si se establece el parámetro de pantalla en **Acercar 150 por ciento**, **Acercar 200 por ciento**, o **Acercar 250 por ciento** antes de actualizar desde la versión 3.10, el parámetro vuelve al valor predeterminado **Como el servidor** en lugar de **Ajustar a la pantalla** cuando se completa la actualización.

  [RFANDROID-1187]

HDX SDK para Android

- En algunos casos, al usar el botón Atrás del mouse se cierra el teclado de software. Al volver hacer clic con el botón Atrás para rehacer la acción original el problema se resuelve.

- En algunos casos, una sesión inactiva (que ha estado inactiva durante 10 minutos) puede mostrar un mensaje de error similar a: "Problema general. Intente conectar de nuevo". Para solucionar este problema, vuelva a iniciar la sesión.

  [RFANDROID-469]

- En algunas situaciones, una sesión activa puede mostrar un mensaje de error para avisar de un "problema general" al establecer una conexión MHL>HDMI. Para resolver este problema, intente conectar de nuevo el cable MHL>HDMI.

  [RFANDROID-529]

- En algunos casos, un escritorio puede pedir credenciales de inicio de sesión mientras una pantalla de apertura de sesión

aparece en frente de la pantalla de inicio de sesión; la pantalla de apertura de la sesión no se puede descartar, por lo que el usuario no puede iniciar la sesión.

[RFANDROID-554]

- Las contraseñas se muestran cuando el texto predictivo está habilitado.

  [RFANDROID-688]

- ACR no recibe respaldo cuando se usa la generación OpenGL. Para resolver este problema, configure Citrix Receiver para Android para inhabilitar OpenGL en el archivo receiverconfig.txt.

  [RFANDROID 703]

Requisitos del sistema

Jun 04, 2017

Requisitos de dispositivo

Citrix Receiver para Android 3.11 respalda Android 4.0 (Ice Cream Sandwich), 4.1/4.2/4.3 (Jelly Bean), 4.4 (KitKat), 5.0/5.1 (Lollipop), 6.0 (Marshmallow) y 7.0 (Nougat).

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.

> ### Important
>
> Si se ha instalado una versión Technology Preview de Citrix Receiver para Android, desinstálela antes de instalar la nueva versión.

Requisitos del servidor

StoreFront:

- StoreFront 3.8 (recomendado), 3.7, 3.6, 3.5, 3.0 y 2.6
  Para acceder directamente a almacenes o tiendas de StoreFront. Receiver también respalda versiones anteriores de StoreFront.
- StoreFront configurado con un sitio de Receiver para Web
  Para acceder a los almacenes o tiendas de StoreFront a través de un explorador Web. Para ver 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.x
- XenApp 6.5 para Windows Server 2008 R2
- XenApp 6 para Windows Server 2008 R2
- XenApp 5 para Windows Server 2008
- Citrix Presentation Server 4.5
- XenDesktop 7.x

- XenDesktop 7
- XenDesktop 5, 5.5 y 5.6

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, 3, 3.5, 3.6, 3.7 o 3.8 (recomendado)
- 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
>
> Si 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, aún 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 eDocs, 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 (OTP)
- 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 tarjeta inteligente compatibles:

- BaiMobile 3000MP Bluetooth Smart Card Reader

Tarjetas inteligentes compatibles:

- Tarjetas PIV
- Tarjetas CAC (Common Access Card)

Configuraciones compatibles:

- Autenticación con tarjeta inteligente en NetScaler Gateway con StoreFront 2 o 3 y XenDesktop 5.6 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 5.6 y versiones posteriores, o XenApp 6.5 y versiones posteriores

> **Nota**
>
> Se pueden configurar otras soluciones de autenticación basadas en tokens usando RADIUS. Para la autenticación con tokens de SafeWord, consulte el artículo "Configuración de la autenticación de SafeWord" en eDocs para obtener las instrucciones referentes

a la edición de NetScaler Gateway disponible en su empresa.

Concesión de acceso a aplicaciones y escritorios virtuales

Jun 04, 2017

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.

En este artículo:

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 y 3.8

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 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, los almacenes o 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:

Instalación de Citrix Receiver en una tarjeta SD

Jun 04, 2017

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.

Habilitación del respaldo para tarjetas inteligentes

Jun 04, 2017

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. Por ejemplo, para emparejar el lector de tarjeta inteligente Bluetooth baiMobile con el dispositivo Android, consulte: https://www.biometricassociates.com/downloads/user-guides/baiMobile-3000MP-User-Guide-for-Android-v3.2.pdf.
   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. Para obtener más información, consulte http://www.biometricassociates.com/products/smart-card-readers/android-supported-devices/.
   - 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.

Cómo proporcionar autenticación de RSA SecurID para dispositivos Android

Jun 04, 2017

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: ftp://ftp.emc.com/pub/agents/tokenconverter310.zip. 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 proporcionar información de acceso a los usuarios finales de Android

Jun 04, 2017

Debe proporcionar a los usuarios la información de cuenta de Receiver que necesitan para acceder a sus 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
- Entregándoles la información de cuenta para que la introduzcan manualmente

Configuración de la detección de cuentas basada en direcciones de correo electrónico

Puede configurar 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 Receiver. 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.

Para configurar su servidor DNS para respaldar la detección basada en correo electrónico, consulte Configuración de la detección de cuentas basada en direcciones de correo electrónico.

Para configurar Access Gateway para que acepte conexiones de usuario usando una dirección de correo electrónico para detectar la URL de StoreFront o Access Gateway, consulte Conexión a StoreFront mediante detección basada en correo electrónico en la documentación de NetScaler.

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 Receiver de forma automática. Después de instalar Receiver, los usuarios solo tienen que abrir el archivo .cr en el dispositivo para configurar Receiver. Si se configuran sitios de Receiver para Web, los usuarios también pueden obtener los archivos de aprovisionamiento de Receiver desde esos sitios.

Para obtener más información, consulte la documentación de StoreFront.

Entrega de la información de cuenta para introducirla 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 accesos mediante Access Gateway, proporcione la dirección de Access Gateway y el método de autenticación

requerido.
Para obtener más información sobre cómo configurar NetScaler Gateway, consulte la documentación de NetScaler Gateway o XenApp (para Secure Gateway).

Cuando un usuario introduce la información de una cuenta nueva, Citrix Receiver intenta verificar la conexión. Si la conexión es satisfactoria, Receiver solicita al usuario que se conecte a la cuenta.

Cómo guardar contraseñas

Jun 04, 2017

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, 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.

> ## Sugerencia
>
> 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), Receiver solicita a los usuarios que introduzcan sus contraseñas cada vez que se conectan.

> ## Nota
>
> Para conexiones de 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.

Cambio de los parámetros de Citrix Receiver en el dispositivo

Jun 04, 2017

Los parámetros siguientes se pueden personalizar desde la ficha Parámetros:

- **Mostrar**
  - Resolución de la sesión: Seleccione la resolución para la sesión. El valor predeterminado es **Ajustar a la pantalla**.
- **Teclado**
  - Texto predictivo: Habilite o inhabilite el texto predictivo. El valor predeterminado es **Desactivado**.
  - Teclado extendido: Habilite o inhabilite el teclado extendido. El valor predeterminado es **Desactivado**.
  - Teclas extendidas: Configure teclas especiales, por ejemplo CTRL o ALT, para mostrarlas en el teclado extendido.
  - IME del cliente: Cuando el editor IME en el cliente está habilitado, los usuarios pueden introducir texto en el punto de inserción en lugar de tener que hacerlo en una ventana aparte. El valor predeterminado es **Desactivado**.
- **Sonido**
  - Streaming de sonido: Configure los parámetros de sonido de la sesión: Sonido desactivado, Reproducir o Reproducir y grabar. El valor predeterminado es **Reproducir**.
- **Avanzado**
  - Usar almacenamiento del dispositivo: Permiso para acceder al almacenamiento del dispositivo. El valor predeterminado es **Sin acceso**.
  - Preguntar antes de salir: Configure si quiere pedir confirmación antes de salir. El valor predeterminado es **Activado**.
  - Portapapeles: Habilite o inhabilite el uso del portapapeles. El valor predeterminado es **Desactivado**.
  - Orientación de pantalla: Configure si desea fijar la orientación de la pantalla como Vertical, Horizontal o Automática (dinámica). El valor predeterminado es Automática.
  - Pantalla encendida: Configure si quiere dejar encendida la pantalla del dispositivo. El valor predeterminado es **Desactivado**.
- **Versión de TLS respaldada**: 1.0, 1.1 y 1.2. El nivel actual de TLS que se usa es el nivel más alto que admita el sitio.
- **Acerca de**: Acerca de Citrix Receiver, la versión y la información de copyright.

Prueba del sitio de demostración

Jun 04, 2017

Cuando los usuarios inician Citrix Receiver por primera vez, la página de bienvenida les ofrece la opción de abrir una cuenta de demostración en Citrix Cloud.

Los usuarios completan el registro de cuentas introduciendo sus nombres y direcciones de correo electrónico (las direcciones de correo electrónico se rellenan en algunos dispositivos). El sitio de demostración ya está configurado con aplicaciones publicadas y listo para que los usuarios prueben Citrix Receiver sin más demora.

Los usuarios pueden agregar, cambiar y quitar sus propias cuentas en Receiver.

SDK de Citrix Receiver para Android

Jun 04, 2017

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 de 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.