Citrix Receiver para Android 3.7

Nov 20, 2015

Acerca de Citrix Receiver para Android 3.7.x

Nov 20, 2015

Citrix Receiver para Android 3.7.3 es la versión actual en Google Play. Los usuarios que ejecutan versiones anteriores deben actualizar el producto a la versión más reciente.

Citrix Receiver para Android 3.7.3 incluye respaldo para Android M (6.0).

Problemas resueltos en 3.7.3

Citrix Receiver para Android 3.7.3 soluciona problemas ocasionales en los que Citrix Receiver se bloquea al usarlo con Nexus 9 Bluetooth.

Esta reciente actualización incluye:

- **Ajuste a pantalla**. Cuando se publica una aplicación con una resolución específica, Receiver muestra ahora la aplicación en el área central y ajusta la pantalla dependiendo de la relación de aspecto; interpreta correctamente la relación entre el origen (la aplicación) y el destino (la pantalla).
- **Respaldo mejorado para el reflejo de la presentación de la sesión**. Receiver para Android mejora la experiencia del usuario haciendo coincidir las características de presentación entre la presentación en pantalla y el dispositivo Android.
- **Respaldo para Transport Layer Security (TLS)**. Receiver para Android ahora respalda los protocolos TLS 1.1 y TLS 1.2. Cuando está habilitado, TLS ofrece comunicaciones seguras entre el servidor y el cliente. Esta funcionalidad se puede configurar usando la interfaz o a través del archivo **receiverconfig**.
- Respaldo para ocultar la barra de menú en la sesión para dispositivos sin pantalla táctil.
- Gestión mejorada del teclado para el alfabeto Hangul coreano.

Estos son los problemas y limitaciones conocidas para esta versión de Receiver para Android:

- En la versión anterior, se ofrecía respaldo limitado para reflejar la pantalla de la sesión en una segunda pantalla; había una limitación por la cual, solo se respaldaban los dispositivos cuya resolución coincidía con la pantalla del dispositivo Android. En esta versión de Receiver para Android, esta limitación se ha quitado: se da respaldo a pantallas cuya resolución difiere del dispositivo Android, con las siguientes limitaciones: [#549471]
  - El tamaño de la sesión viene determinado por la resolución natural del dispositivo de pantalla conectado; todos los demás parámetros se ignoran porque la segunda pantalla no puede ajustarse a la imagen de la sesión. Además, las solicitudes para ajustar dinámicamente la resolución de la sesión para que coincida con la resolución de la pantalla conectada solo reciben respaldo parcial. En tales entornos, la conexión y desconexión de una segunda pantalla no le permitirá solicitar un cambio de tamaño de la sesión que cumpla con los parámetros de usuario normales.
  - El sistema puede volverse inestable al desconectar una segunda pantalla, haciendo que Receiver falle. Se recomienda que, al usar una segunda pantalla, se conecte ésta al dispositivo Android antes de iniciar la sesión.
  - La presentación en pantalla puede verse afectada negativamente en la pantalla conectada; en algunos casos, la pantalla conectada puede presentar fallos cosméticos, tales como una presentación incorrecta del puntero del mouse y fragmentación durante el movimiento de ventanas.

    - También existen algunas limitaciones que afectan a la interfaz de usuario mostrada en la pantalla principal del dispositivo Android. Por ejemplo, el mouse funciona para la dimensión de pantalla de un dispositivo y no para las pantallas secundarias. Además, no se muestra la barra de herramientas en la pantalla del dispositivo cuando el reflejo de pantalla está habilitado. [#549471]

- Al conectar una pantalla secundaria, la resolución de pantalla de la pantalla recién conectada es la misma que la del dispositivo. Este problema ocurre cuando el dispositivo conectado se acopla después de inicializar la sesión, y cuando el mouse no está conectado a la base de acoplamiento. Para resolver esta situación, conecte el mouse para la segunda sesión para volver a la resolución correcta. Este problema afecta específicamente al Multimedia Dock de Samsung Galaxy Note II. [#541028]
- Al quitar el mouse de una sesión acoplada la presentación en pantalla en el dispositivo gira 90 grados a la derecha. La orientación de la sesión vuelve a la normalidad después de unos momentos. Este problema afecta específicamente al Multimedia Dock de Samsung Galaxy Note II. [#541032]
- Al usar el reflejo de pantalla hacia un monitor externo usando una llave de hardware AllCast, no se oye sonido al reproducir archivos de medios. Este problema parece estar relacionado con la capacidad del dispositivo de pantalla: si se usa una televisión con altavoces, la salida del audio se realiza a través de la televisión. Si se usa un monitor sin altavoces, el audio debería sonar por los altavoces del dispositivo Android, pero no sucede así.[#544330]
- Al mover la lupa hacia el borde externo de la imagen de la sesión puede ser que la lupa muestre parte de la imagen de fondo que no está bajo ella. [#542299]
- En algunas ocasiones, al cerrar una sesión se puede producir una excepción de tiempo de ejecución. [#523824]
- El nivel máximo de "pellizco hacia afuera" no se mantiene después de girar la pantalla. Esto puede ocurrir después de iniciar una sesión y usar un "pellizco hacia adentro" para obtener la vista deseada y luego girar el dispositivo 90 grados; después de girar el dispositivo una segunda vez, el nivel de pellizco seleccionado previamente no se mantiene. [#538638]
- El teclado extendido se activa por error bajo ciertas condiciones; en algunos casos, esto ocurre cuando se detiene el reflejo de pantalla y se gira el dispositivo; en otros casos, sucede cuando se toca la pantalla del dispositivo mientras el reflejo de pantalla está habilitado. Estos problemas pueden ocurrir cuando el dispositivo Android no puede determinar si se está mostrando el teclado de pantalla; al entrar en modo reflejo cuando se conecta otro monitor, el dispositivo no interpreta el acto de mostrar el teclado extendido. [#545231]
- La creación de cuentas falla para dispositivos ASUS Nexus 7 que ejecutan Android versión 4.1.1. Para evitar este problema, actualice el dispositivo con el software de Android más reciente, tal como la versión 4.2.2.
- En algunos dispositivos Android, el clic con el botón secundario de puntero de Bluetooth Mouse sigue invocando la acción Atrás, lo que hace que el cuadro de diálogo Salir aparezca accidentalmente. Este problema ocurre solo en dispositivos cuyo firmware no respalda el clic con botón secundario de puntero. [#331168]
- En Receiver para Android 3.5, la función de túnel VPN completo no recibe respaldo cuando se usa autenticación con tarjeta inteligente. [#456657]
- Cuando se conecta con un NetScaler FIPS mientras la directiva "denysslreneg" tiene el valor No o Frontend Client y "Client Authentication" tiene el valor Optional, puede que vea este error al iniciar una sesión en Receiver.
    - Cuando inicia una sesión en Receiver introduciendo "Dominio\NombreDeUsuario" en el campo de nombre de usuario, puede que vea un mensaje donde se le indica que el nombre de usuario o la contraseña son incorrectos. Este mensaje muestra Dominio\Dominio\NombreDeUsuario en el campo de nombre de usuario. Para resolver el problema, quite uno de los nombres de dominio y vuelva a iniciar la sesión con el formato Dominio\NombreDeUsuario. [#466022]

Requisitos del sistema de Receiver para Android

Nov 20, 2015

- Citrix Receiver para Android 3.7.3 respalda las versiones de Android 4, 5 y 6 (Android M).
- Citrix Receiver para Android 3.7, 3.7.1 y 3.7.2 respaldan las versiones de Android 4 y 5.
- Para obtener resultados óptimos, actualice los dispositivos Android con el software de Android más reciente.
- Receiver para Android respalda el inicio de sesiones desde Receiver para Web, siempre que el explorador Web funcione con Receiver para Web. Si no puede iniciar sesiones, configure su cuenta a través de Receiver para Android directamente.
- Si se ha instalado una versión Technology Preview de Citrix Receiver, desinstálela antes de instalar la nueva versión.

Importante: Consulte la sección **Conectividad** (más abajo) para obtener información sobre conexiones seguras con su entorno Citrix.

Para conexiones con aplicaciones y escritorios virtuales, Citrix Receiver respalda el uso de Citrix StoreFront y la Interfaz Web:
StoreFront:

- StoreFront 3.0 (recomendado)
  Para acceder directamente a almacenes de StoreFront. Receiver también respalda versiones anteriores de StoreFront.

- StoreFront configurado con un sitio de Receiver para Web
  Para acceder a los almacenes 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):
- 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 Fundamentals 6.0 para Windows Server 2008 R2
  - XenApp 5 para Windows Server 2008
  - XenApp 5 para Windows Server 2003
  - Citrix Presentation Server 4.5
  - XenDesktop 7.x
  - XenDesktop 7
  - XenDesktop 5, 5.5 y 5.6

Citrix Receiver 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.x ó 2.6 (recomendado), Interfaz Web 5.4, o un sitio de Servicios XenApp (antes llamado Agente de Program Neighborhood).

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

- Citrix NetScaler Gateway 10 (incluidas versiones de VPX, MPX and SDX)
- Citrix Access Gateway Enterprise Edition 9.x y 10.x (incluidas las versiones VPX, MPX y SDX)
  - CloudGateway solo recibe respaldo con la versión 9.3 y versiones posteriores

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.

Importación de certificados raíz en dispositivos Android

Los dispositivos Android 4.x respaldan la importación de certificados raíz sin tener acceso a la raíz (root) del dispositivo. Los dispositivos Android anteriores a la versión 4.0 no respaldan la importación automática de certificados raíz.

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 Access 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 Base correspondiente a su edición de Access Gateway:

CTX114146: How to Install an Intermediate Certificate on Access Gateway Enterprise Edition (disponible solo en inglés)

Además de los temas de configuración en esta sección de eDocs, vea también:

CTX124937: How to Configure Citrix Access Gateway Enterprise Edition for Use with Citrix Receiver for Mobile Devices (disponible solo en inglés)

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

Citrix Receiver admite la autenticación mediante Access 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*

* Receiver para Android ofrece ahora respaldo para los siguientes productos y configuraciones.
Nota: La autenticación mediante tarjeta inteligente en sitios de Interfaz Web no está respaldada.
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.x 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 de tokens de SafeWord, consulte el artículo "Configuración de la autenticación de SafeWord" en eDocs para obtener las instrucciones referentes a la edición de Access Gateway disponible en su empresa.

Administración

Nov 20, 2015

Receiver requiere la configuración de la Interfaz Web para la implementación. 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. La autenticación entre Receiver y el sitio de la Interfaz Web se puede gestionar usando diversas soluciones, que se describen en esta sección.

Además, se puede configurar StoreFront para proporcionar servicios de autenticación y entrega de recursos para Receiver, lo que permite crear almacenes empresariales para la entrega de escritorios, aplicaciones y otros recursos para los usuarios.

Para obtener más información sobre cómo configurar las conexiones, incluidos vídeos, blogs y foros de asistencia, consulte http://community.citrix.com.

Instalación de Receiver en una tarjeta SD

Nov 20, 2015

Receiver para dispositivos móviles está optimizado para la instalación local en dispositivos de usuario. 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.

Para configurar Access Gateway Enterprise Edition para Citrix Receiver para Android

Nov 20, 2015

Importante:

- Access Gateway Enterprise Edition 9.x y 10.x reciben respaldo en Receiver para Android usando sitios de servicios XenApp.
- Access Gateway Enterprise Edition 9.x y 10.x reciben respaldo en Receiver para Android usando sitios Web XenApp.
- Receiver para Web no recibe respaldo en Receiver para Android.
- Access Gateway Enterprise Edition 9.x y 10.x reciben respaldo en Receiver para Android para acceder a almacenes de StoreFront.
- En los sitios de la Interfaz Web y StoreFront se respaldan tanto la autenticación de un solo origen como la autenticación de doble origen.
- Es necesario utilizar la Interfaz Web versión 5.4, que está respaldada en todos los exploradores Web integrados.
- 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 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 Access 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 Access Gateway.

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

- Si desea implementar CloudGateway Enterprise en la red, integre Access Gateway 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 Access Gateway Plug-in.
- Si desea implementar CloudGateway Express en la red, integre Access Gateway y StoreFront para permitir las conexiones de los usuarios internos o remotos a StoreFront mediante Access 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 obtener información sobre la configuración de estas conexiones, consulte "Integrating Access Gateway with CloudGateway" y los demás temas incluidos en la documentación de Access Gateway 10.

Para obtener más información sobre la configuración necesaria para Receiver en dispositivos móviles, vea también los temas de la documentación de Access Gateway 10:

- Creación del perfil de sesión destinado a Receiver para CloudGateway Enterprise
- Creación del perfil de sesión destinado a Receiver para CloudGateway Express
- Configuración de directivas personalizadas de acceso sin cliente para Receiver
- Cómo permitir el acceso desde dispositivos móviles

Y el tema siguiente en la documentación de XenMobile:

- Herramienta de preparación de aplicaciones móviles

Para permitir que los usuarios remotos se conecten mediante Access Gateway a la implementación de la Interfaz Web, configure Access Gateway para que funcione con la Interfaz Web, como se describe en "Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface" y en la documentación de Access Gateway 10.

Para configurar la Interfaz Web para Citrix Receiver para Android

Nov 20, 2015

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

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.

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

Para iniciar aplicaciones desde el sitio de la Interfaz Web con Receiver para Android, la tarjeta SD en el dispositivo debe estar disponible para que la sesión se pueda iniciar. Si la tarjeta SD no está disponible (por ejemplo, cuando está en uso o no está montada), el inicio de la sesión falla.

Habilitación del respaldo para tarjetas inteligentes

Nov 20, 2015

Receiver para dispositivos móviles con Android proporciona respaldo para lectores de tarjeta inteligente Bluetooth con sitios de PNA. 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)

Para configurar el 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: http://www.biometricassociates.com/downloads/user-guides/baiMobile-3000MP-User-Guide-for-Android-v2.0.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. Esta 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 de PNAgent 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

Nov 20, 2015

Si se configura Access Gateway para la autenticación RSA SecurID, 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), Access 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 obtener instrucciones sobre cómo configurar la autenticación con RSA SecurID, en eDocs, expanda el apartado correspondiente a la versión de Access Gateway que esté utilizando y busque el tema
— Configuración de la autenticación de RSA SecurID
.

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

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: http://www.rsa.com/node.aspx?id=2521. 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 Parámetros 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 sobre el acceso a los usuarios finales de Android

Nov 20, 2015

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

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 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 en la documentación de StoreFront.

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 Access Gateway.

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.

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 la forma de configurar Access Gateway o Secure Gateway, consulte la documentación de Access Gateway o XenApp (para Secure Gateway).

Cuando un usuario introduce la información de una cuenta nueva, Receiver intenta verificar la conexión. Si la conexión es

satisfactoria, Receiver solicita al usuario que se conecte a la cuenta.

Guardar contraseñas

Nov 20, 2015

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.
  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), 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.

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

Nov 20, 2015

Los siguientes parámetros se pueden personalizar desde la ficha Parámetros en Citrix Receiver para Android:

- **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**.
- **ShareFile**: Esta funcionalidad ya no recibe respaldo y se quitará en una próxima actualización. Use la aplicación de ShareFile.
- **Acerca de**: Acerca de Citrix Receiver, la versión y la información de copyright.

Prueba del sitio de demostración

Nov 20, 2015

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 que los usuarios prueben Citrix Receiver sin más demora.

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