Citrix Receiver para Android 3.6

Nov 20, 2015

Acerca de Receiver 3.6 para Android

Nov 20, 2015

> **Important**
>
> Esta versión de Citrix Receiver no recibe respaldo en Android M (6.0). Si los usuarios han actualizado a Android M, pídales que actualicen Citrix Receiver a la versión más reciente. Los usuarios pueden obtener la versión más reciente en Google Play.

Novedades en la versión 3.6

Esta reciente actualización incluye:

- **Modo multitoque**. Se puede obtener una opción configurable para permitir que los gestos multitoque se envíen directamente a una aplicación o a un escritorio habilitados para uso táctil. El modo multitoque se puede habilitar usando el menú de la sesión. Los usuarios pueden cambiar entre modo multitoque, modo desplazamiento y modo panorámico. Nota: El modo multitoque requiere XenApp 7.0 o posterior y XenDesktop 7.0 o posterior y recibe respaldo en Windows 7, Windows 8, Windows 8.1 y Windows 2012 R2. Si el servidor no respalda el modo multitoque, se puede cambiar entre el modo desplazamiento y el modo panorámico.

Habilitar el modo desplazamiento	Habilitar el modo multitoque	Habilitar el modo panorámico
		

- **Rendimiento de los gráficos**. La velocidad de fotogramas y la velocidad de descodificación de Receiver para Android es ahora aproximadamente el doble al habilitar la descodificación de hardware y la generación por OpenGL en dispositivos compatibles y con resoluciones de sesión adecuadas.
- **Respaldo para puntero y teclado externos**. El comportamiento de Receiver para Android se adapta cuando se conecta un puntero y un teclado externo al dispositivo: por ejemplo, no se despliega el teclado de pantalla y se habilita el clic con botón secundario.
- **Uso de SSL v3 inhabilitado**. Para evitar nuevos ataques, como el de "POODLE" , contra el protocolo SSLv3, esta versión de Receiver para Android inhabilita su uso. Para obtener más información, consulte CTX 200238.
  Nota: Debe asegurarse de que TLS 1.0 esté habilitado.
- **Se ha quitado el respaldo para Android 2.3.3** (Gingerbread). Esta versión de Receiver para Android respalda Android 4.0 o posterior, incluido Android 5.0 (Lollipop).
- **Movilidad de sesión simple**. Cuando los usuarios inician una sesión en Receiver, como máximo una sesión activa en un dispositivo se moverá al dispositivo local. Las sesiones no se mueven cuando se utiliza Receiver para Web (a través de la Interfaz Web).

Problemas conocidos

- El botón central del puntero no se comporta de manera coherente. Esta versión respalda el uso de punteros de dos botones y punteros con rueda de desplazamiento. [#499353]
- Cuando el parámetro de uso de Texto predictivo de Receiver para Android está desactivado, y se usan gestos para introducir texto (desplazamiento por letras), las palabras no se muestran en la pantalla hasta que se inicia la palabra siguiente. El impacto que esto tiene en la usabilidad es que las palabras pueden aparecer juntas sin espacio entre ellas. Como solución temporal, habilite el parámetro para usar Texto predictivo en Receiver para Android. [#502503]

- Cuando se trabaja en modo Open GL, la sesión se perderá sin mostrar el diálogo de reconexión automática de clientes. Se captura un registro con el texto "ACR is disabled by ReceiverViewActivity (OpenGL mode)". [#506483]
- Se muestra un mensaje de error genérico ("Problema general. Intente conectar de nuevo.") cuando se intenta iniciar una aplicación en Receiver para Android que no tiene un certificado raíz de confianza en el dispositivo. [#506936]
- No se puede iniciar Receiver para Android en una configuración acoplada específica sin puntero. Esto se ha observado en un dispositivo Samsung S4 acoplado en una unidad multimedia de acoplamiento Samsung. Cuando se agrega un puntero a la configuración, Receiver para Android se inicia y funciona según lo previsto. Como solución temporal, agregue un puntero cuando lo tenga acoplado en esta configuración. [#512406]
- Receiver para Android deja de funcionar cuando se conecta con un servidor XenDesktop 7.0 en MediaCodec con OpenGL en modo de descodificación y generación. Un dispositivo que usa este modo de manera predeterminada es, por ejemplo, el Samsung Galaxy Note 10.1" 2014 Edition. Como solución temporal, configure el servidor XenDesktop 7.0 para que **no** use H.264 con texto sin pérdida. Para obtener más información consulte Optimización de la entrega de gráficos y multimedia en la documentación de XenDesktop 7.0. [#516465]
- El respaldo para acceso a ShareFile desde la ficha Parámetros de Receiver para Android se quitará en una actualización futura. Use la aplicación de ShareFile desde el dispositivo Android.
- 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 3.5 para Android, 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]
- La función de perfil móvil (Smooth Roaming) y el control del área de trabajo no reciben respaldo en Android. Puede que funcionen, pero no con fiabilidad. [#68728673]

Problemas resueltos

- Los gestos multitoque no están respaldados en Windows 7.
- Cuando se accede a una aplicación o escritorio desde una tableta con el teclado visible, al girar la tableta 90 grados y deseleccionar el teclado puede que no se vea la pantalla completa. Si la imagen no vuelve a pantalla completa después de deseleccionar el teclado, gire la tableta 90 grados para volver a la pantalla completa. [#457589]
- Receiver no respalda Bluetooth Mouse en el dispositivo Nexus 10. [#368795]
- Cuando se agrega una cuenta de StoreFront manualmente, se necesita la dirección completa del almacén para poder agregarla. [#455441]
- Si se configura ProxyType=None en las secciones WFClient y Application del archivo default.ica, esta configuración no funciona. [#495211]
- Cuando se gira rápidamente un dispositivo que ejecuta Receiver para Android 3.5, el área de trabajo de la sesión no responde a la rotación. [#495212]
- El campo Contraseña en Receiver para Android 3.5 no aparece en Samsung Galaxy Note 10.1. [#495336]
- Al agregar una nueva cuenta en Receiver para Android después de agregar un sitio de Access Gateway se produce un error. [#504846]

- Las entradas con el teclado aparecen como "-" en un Galaxy Note 10.1 cuando la función de introducción de texto inteligente (Smart typing) está habilitada. [#507650]
- Citrix Receiver for Android no funciona correctamente con imágenes de Android L Preview ni con el nuevo ART (Android RunTime). [#489152]
- En algunos dispositivos ocurre un error de excepción aritmética al agregar aplicaciones a los Favoritos. [#493904]

Requisitos del sistema de Receiver para Android

Nov 20, 2015

Requisitos de dispositivo

> **Important**
>
> Esta versión de Citrix Receiver no recibe respaldo en Android M (6.0). Si los usuarios han actualizado a Android M, pídales que actualicen Citrix Receiver a la versión más reciente. Los usuarios pueden obtener la versión más reciente en Google Play.

- Citrix Receiver para Android 3.6 recibe respaldo en las versiones de Android 4.0 y 5.0.
- Citrix Receiver para Android respalda el inicio de sesiones desde Citrix Receiver para Web, siempre que el explorador Web funcione con Citrix 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.

Servidor

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

StoreFront:

- StoreFront 2.6 (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

Conectividad

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, se debe disponer de un certificado raíz para la entidad de certificación de la empresa en el dispositivo móvil, para poder acceder correctamente a los recursos Citrix mediante Citrix 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)

Autenticación

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.

Configuración del entorno para Citrix Receiver para Android

Nov 20, 2015

Para que los usuarios puedan acceder a las aplicaciones publicadas en la implementación de XenApp o XenDesktop, antes hay que configurar los componentes siguientes en el entorno como se describe a continuación.

- Cuando publique aplicaciones en comunidades o sitios, tenga en cuenta las siguientes opciones para mejorar la experiencia de los usuarios que acceden a esas aplicaciones a través de almacenes de StoreFront:
  - Asegúrese de incluir descripciones significativas para las aplicaciones publicadas, dado que estas descripciones estarán visibles para los usuarios de Citrix Receiver.
  - Puede destacar ciertas aplicaciones publicadas a los usuarios de los dispositivos móviles listando las aplicaciones en la lista de aplicaciones destacadas de Citrix Receiver. Para rellenar la lista de aplicaciones Destacadas en Citrix Receiver, modifique las propiedades de las aplicaciones publicadas en los servidores para agregarles la cadena de texto KEYWORDS:Featured en el valor del campo Descripción de la aplicación.
  - Para habilitar el modo de ajuste de pantalla que ajusta la aplicación al tamaño de la pantalla de los dispositivos móviles, edite las propiedades de las aplicaciones publicadas en los servidores XenApp y agregue la cadena de texto KEYWORDS:mobile al valor del campo Descripción de la aplicación. Esta palabra clave también activa la función de desplazamiento automático para la aplicación.
  - Para suscribir automáticamente a todos los usuarios de un almacén a una aplicación, agregue la cadena KEYWORDS:Auto a la descripción que proporcione cuando publique la aplicación en XenApp. Cuando los usuarios inicien sesión en el almacén, la aplicación se suministrará automáticamente sin necesidad de que los usuarios tengan que suscribirse de forma manual a la aplicación.
  - Al publicar la aplicación de escritorio remoto (RDP) para Android, agregue el texto KEYWORDS:unikey al valor del campo Descripción de la aplicación para asegurarse de que la tecla Mayús funciona correctamente en los dispositivos de usuario. Esta palabra clave hace que Receiver envíe las pulsaciones del teclado mediante un mecanismo alternativo que hace que la tecla Bloq. Mayús funcione.

  Para obtener más información, consulte la documentación de StoreFront.

- Si la Interfaz Web de la implementación de XenApp o XenDesktop no dispone de un sitio Web o de un sitio de servicios XenApp, cree uno. Para obtener instrucciones sobre la creación de uno de estos sitios, consulte los temas de "Configuración de sitios" de la Interfaz Web 5.4.

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, los usuarios deben seleccionar la aplicación de la lista de aplicaciones de Receiver en el dispositivo de usuario, y después seleccionar 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 StoreFront para Citrix Receiver para Android

Nov 20, 2015

Para configurar StoreFront

Importante:

- Solo Citrix Access Gateway Enterprise Edition 9.3 y Access Gateway 10 reciben respaldo en Receiver 3.x para Android cuando se usa StoreFront.
- 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.

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

1. Instale y configure StoreFront. Para obtener más información, consulte StoreFront en la sección Tecnologías > StoreFront de eDocs. 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.
2. Configure almacenes 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 obtener detalles, consulte
   — Opciones de acceso de usuarios
   en la sección de StoreFront de eDocs. 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 almacenes. 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 el único almacén para el 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 uno o varios almacenes que se puedan distribuir manualmente a los usuarios.
   - Configuración manual. Es posible informar directamente a los usuarios sobre las direcciones URL de los almacenes o de Access Gateway que necesitan para acceder a sus escritorios y aplicaciones. Para las conexiones a través de Access Gateway, los usuarios también deben conocer el método de autenticación requerido y la edición de los productos. 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 Access Gateway

Si tiene usuarios que se conectan desde fuera de la red interna (por ejemplo, usuarios que se conectan desde Internet en ubicaciones remotas), configure la autenticación a través de Access Gateway.

- Solo Citrix Access Gateway Enterprise Edition 9.3 y Access Gateway 10 reciben respaldo en Receiver 3.x para Android cuando se usa StoreFront.
- Para obtener detalles, consulte su versión de Access Gateway en eDocs.

Para configurar Receiver para acceder a aplicaciones

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

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

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 ese nodo de eDocs.

En los siguientes temas, se ofrece información sobre los parámetros que se requieren en Receiver para dispositivos móviles:

- 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
- 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 los subtemas correspondientes en Citrix eDocs.

Para configurar la Interfaz Web para Citrix Receiver para Android

Nov 20, 2015

Para configurar el sitio de 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 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.

Para iniciar aplicaciones en el dispositivo Android

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 .apk de PC/SC-Lite se puede descargar desde:
   - Google Play Store
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.

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: 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

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 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.

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 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.

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

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.