



Aplicación Citrix Workspace para Android

Contents

Novedades en la aplicación Citrix Workspace para Android	3
Problemas resueltos	4
Problemas conocidos	6
Avisos de terceros	7
Requisitos del sistema	7
Implementación	11
Configuración	15
Solucionar problemas	25
SDK y API	28

Novedades en la aplicación Citrix Workspace para Android

May 23, 2019

Novedades en la versión 1904.1

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

Novedades en la versión 1904

Citrix HDX RealTime Media Engine incrustado

En versiones anteriores, Citrix HDX RealTime Media Engine (RTME) se instaló por separado utilizando un APK de Google Play.

Con esta versión, RTME de Citrix HDX está integrado con el instalador de la aplicación Citrix Workspace.

Esta función se admite en:

- Chromebooks con procesadores x86.
- Dispositivos con Android 6.0 o versiones posteriores.

Para obtener más información, consulte la documentación de [HDX RealTime Media Engine](#).

Novedades en la versión 1903.1

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento general. Para obtener más información, consulte [Problemas resueltos](#).

Novedades en la versión 1903

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento general. Para obtener más información, consulte [Problemas resueltos](#).

Novedades en la versión 1902.1

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento general. Para obtener más información, consulte [Problemas resueltos](#).

Novedades en la versión 1902

Disponibilidad para usuarios no autenticados

En esta versión, la aplicación Citrix Workspace admite usuarios no autenticados (anónimos). Los usuarios anónimos ahora pueden iniciar sesión con éxito en Citrix Virtual Apps and Desktops.

Novedades en la versión 1901

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento general. Para obtener más información, consulte [Problemas resueltos](#).

Problemas resueltos

May 23, 2019

Problemas corregidos en 1904

- Iniciar una sesión después de activar un dispositivo acoplado en Samsung DeX puede provocar que la aplicación Citrix Workspace para Android deje de responder y aparezca el siguiente mensaje de error:
“No se puede conectar con el servidor”.
[RFANDROID-2607]
- Al cambiar entre aplicaciones, es posible que la aplicación Citrix Workspace para Android deje de responder al volver a la aplicación. [RFANDROID-2906]
- El icono de menú no funciona cuando se cambia el tamaño de la aplicación a una resolución inferior. [RFANDROID-3110]
- No se puede copiar un archivo grande de la unidad de cliente asignada a la sesión. [RFANDROID-3785]

Problemas resueltos en la versión 1903.1

- No aparece ninguna notificación toast al cerrar la sesión. [RFANDROID-3082]
- En una configuración de Citrix Cloud, el cuadro de diálogo **Intentar de nuevo** aparece continuamente y no funciona incluso cuando el usuario confirma la acción. [RFANDROID-3108]

- En un dispositivo móvil, cuando accede a aplicaciones que no sean la aplicación Citrix Workspace, aparece el siguiente mensaje de forma aleatoria.

“No se puede conectar al servidor; inténtelo de nuevo.”

[RFANDROID-3172]

Problemas resueltos en la versión 1903

- Cuando ejecuta una sesión HDX en un dispositivo Samsung DeX, aparece una pantalla azul. [RFANDROID-2913]
- Las sesiones HDX que se ejecuten en dispositivos Android 9 pueden aparecer dañados si establece la profundidad de color en **8 bits** o **16 bits** en Citrix Studio. [RFANDROID-2914]
- Cuando trata de cambiar la contraseña, aparece el nombre de usuario que inició sesión previamente en lugar del nombre de usuario que ha iniciado sesión actualmente. [RFANDROID-3042]
- Cuando mueve una sesión extendida al segundo plano, la sesión se sigue mostrando en el monitor externo. [RFANDROID-3122]

Problemas resueltos en la versión 1902.1

- Cuando inicia una sesión con EDT habilitado, aparece una pantalla negra. [LD0739]
- Al cambiar las opciones de los parámetros del Teclado extendido, es posible que la selección no se refleje en la sesión. [RFANDROID-2387]
- Cuando desacopla un dispositivo Android de Samsung DeX en una sesión activa, las teclas Bloq Num no se sincronizan. [RFANDROID-2875]

Problemas resueltos en la versión 1902

- En un dispositivo Android 7 con un teclado físico conectado, el teclado de software no aparece al tocar la opción **Teclado** en la barra de herramientas de la sesión. [RFANDROID-1442]
- En una configuración multitienda de StoreFront, el cuadro de diálogo **Agregar cuenta** muestra las tiendas que se añadieron anteriormente. [RFANDROID-1903]
- Cuando intenta agregar una cuenta de Citrix Cloud, el cuadro de diálogo **Autenticación** no ofrece el tiempo suficiente para introducir la información. [RFANDROID-2884]
- Cuando intenta cambiar de un aplicación a otra en una sesión, aparece el siguiente mensaje de error:

No se puede conectar con el servidor. Inténtelo de nuevo”.

Al pulsar **Intentar de nuevo**, se restablecerá la conexión. [RFANDROID-2910]

Problemas resueltos en la versión 1901

- Cuando toca en la opción **Detalles** de una aplicación que tiene un nombre largo (por ejemplo, 64 caracteres), el nombre de la aplicación aparece desbordado y el botón los puntos suspensivos no aparece. [RFANDROID-1894]
- El nombre de usuario no se rellena automáticamente cuando se accede a la aplicación Citrix Secure Hub mediante la aplicación Citrix Workspace. [RFANDROID-2885]
- Cuando toca en **Actualizar**, el estado de instalación de la aplicación no se actualiza y se muestra incorrectamente. [RFANDROID-2886]

Problemas conocidos

May 23, 2019

Problemas conocidos en la versión 1904.1

- Aparece el siguiente mensaje de error al intentar importar el token de software de RSA.
“Error desconocido”
[LD1085]

Problemas conocidos en la versión 1904

- La aplicación Citrix Workspace no admite la configuración de la tienda Citrix Cloud en dispositivos con Android 5 o versiones anteriores. Actualice a la versión 5.1 o a una versión posterior. [RFANDROID-3804]

Problemas conocidos en la versión 1903.1

- La aplicación Citrix Workspace para Android no admite el parámetro de pila personalizado Enlightened Data Transport Manager Self Service. [LD1096]

Problemas conocidos en la versión 1903

No se han observado nuevos problemas en esta versión.

Problemas conocidos en la versión 1902.1

- En una sesión que se ejecuta en Samsung DeX, las aplicaciones no se extienden a pantalla completa cuando se maximizan. [RFANDROID-3105]

Problemas conocidos en la versión 1902

No se han observado nuevos problemas en esta versión.

Problemas conocidos en versiones anteriores

Problemas conocidos en la versión 1808:

- Cuando ejecuta la aplicación Citrix Workspace para Android en un sistema operativo Chrome, la resolución de pantalla en el VDA es diferente de la establecida en el cliente. También se ve una barra gris. [RFANDROID-2478]
- Los usuarios que actualicen a la aplicación Citrix Workspace y se conecten a una tienda de área de trabajo marcada no verán ningún recurso. Como solución temporal, cierre sesión y vuelva a la aplicación Citrix Workspace. [RFANDROID-2505]

Avisos de terceros

April 30, 2019

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

Para obtener más información acerca del código de licencia Open Source consulte [Open Source Licensed Code](#).

Requisitos del sistema

February 7, 2019

Sistema operativo

Chrome OS Systems admite Android API versión 19 y posterior.

Requisitos de dispositivo

Esta versión de la aplicación Citrix Workspace para Android y las posteriores respaldan Android 4.4 (KitKat), 5.x (Lollipop), 6.x (Marshmallow), 7.x (Nougat), 8.x (Oreo) y 9.x (Pie).

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

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

Importante:

Si tiene instalada una versión Tech Preview de la aplicación Citrix Workspace para Android, desinstálela antes de instalar la nueva versión.

Requisitos del servidor

StoreFront:

- StoreFront 2.6 o versiones posteriores
Ofrece acceso directo a tiendas de StoreFront. La aplicación Citrix Workspace para Android también admite versiones anteriores de StoreFront.
- StoreFront configurado con un sitio de la aplicación Citrix Workspace para Web
Ofrece acceso a los almacenes o tiendas de StoreFront a través de un explorador Web. Para conocer las limitaciones de esta implementación, consulte la documentación de StoreFront.

Interfaz Web (no respaldada en entornos de Citrix Virtual Apps and Desktops 7 y posteriores):

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

Interfaz web en Citrix Gateway:

Debe habilitar las directivas de reescritura suministradas por Citrix Gateway.

Citrix Virtual Apps and Desktops (cualquiera de los siguientes productos):

- Citrix Virtual Apps 7.5 o posterior

- XenApp 6.5 para Windows Server 2008 R2
- Citrix Virtual Apps and Desktops 7.x o posterior

Conectividad

La aplicación Citrix Workspace para Android admite conexiones HTTP, HTTPS e ICA sobre TLS con un servidor Citrix Virtual Apps and Desktops mediante cualquiera de las configuraciones siguientes.

Para conexiones LAN:

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

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

- Citrix Gateway 11 y posteriores (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 la aplicación Citrix Workspace.

Nota:

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

Certificados comodín

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

Certificados intermedios y Citrix Gateway

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

[CTX114146](#) y [CTX124937](#)

Autenticación

Nota:

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

La aplicación Citrix Workspace para Android admite la autenticación mediante Citrix Gateway con los métodos siguientes, según la edición disponible:

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

Nota:

La autenticación mediante tarjeta inteligente en sitios de Interfaz Web no está respaldada.

La aplicación Citrix Workspace para Android ofrece ahora respaldo para los siguientes productos y configuraciones.

Lectores de tarjetas inteligentes compatibles:

- BaiMobile 3000MP USB Smart Card Reader

Tarjetas inteligentes respaldadas:

- Tarjetas PIV
- Tarjetas CAC (Common Access Card)

Configuraciones compatibles:

- Autenticación con tarjeta inteligente en Citrix Gateway con StoreFront 2 o 3 y Citrix Virtual Apps and Desktops 7.x y versiones posteriores, o XenApp 6.5 y versiones posteriores
- Autenticación con tarjeta inteligente en Citrix Gateway con Interfaz Web 5.4.2 y Citrix Virtual Apps and Desktops 7.x y versiones posteriores, o XenApp 6.5 y versiones posteriores

Nota:

Se pueden configurar otras soluciones de autenticación basadas en tokens usando RADIUS. Para la autenticación con tokens de SafeWord, consulte [Configuración de Autenticación de SafeWord](#).

Implementación

April 30, 2019

HDX RealTime Media Engine

HDX RealTime Media Engine (RTME) es un plug-in de la aplicación Citrix Workspace para Android que admite llamadas de audio y vídeo claras y nítidas de alta definición. Podrá participar en llamadas de audio-vídeo o audio con usuarios de HDX RealTime Media Engine.

HDX RealTime Media Engine se integra con la aplicación Citrix Workspace en el dispositivo de punto final y realiza todo el procesamiento de medios directamente en el dispositivo del usuario, reduciendo así la carga del servidor, permitiendo una gran escalabilidad, reduciendo el consumo de ancho de banda de red y garantizando una calidad óptima de sonido y vídeo.

El plug-in RTME de Citrix HDX está integrado con el instalador de la aplicación Citrix Workspace.

Nota:

HDX RTME para la aplicación Citrix Workspace para Android solo se respalda con Chromebooks con procesador Intel Core.

En la aplicación Citrix Workspace para Android, las siguientes funciones de HDX RealTime Media Engine no están disponibles:

- Codificación de cámara USB UVC 1.1
- Enumeración por dispositivo y cambio desde los parámetros de Skype Empresarial. Solo se usan dispositivos predeterminados.
- Códecs G722.1C, RTAudio y RTVideo.
- Dispositivos HID, control automático de ganancias y control de admisión de llamadas.

- En el modo de **reserva**, la cámara Web y los dispositivos de audio no están disponibles debido a las limitaciones de la aplicación Citrix Workspace para Android.

Para obtener más información acerca de HDX RealTime Media Engine, consulte la documentación de [HDX RealTime Optimization Pack](#).

Cómo proporcionar la información de acceso

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

- Configurando la detección de cuentas basada en direcciones de correo electrónico
- Entregándoles un archivo de aprovisionamiento
- Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente

Configurar la detección de cuentas basada en direcciones de correo electrónico

Puede configurar la aplicación Citrix Workspace 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 la aplicación Citrix Workspace para Android. La aplicación Citrix Workspace para Android determina el servidor Citrix 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:

No está disponible la detección de cuentas basada en correo electrónico si la aplicación Citrix Workspace se conecta a una implementación de Interfaz Web.

Entrega de un archivo de aprovisionamiento a los usuarios

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

Para obtener más información, consulte la documentación de [StoreFront](#).

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

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

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

Para obtener más información, consulte la documentación de [Citrix Gateway](#).

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

Cómo proporcionar autenticación de RSA SecurID para dispositivos Android

Si se configura Citrix Gateway para la autenticación RSA SecurID, la aplicación Citrix Workspace para Android respalda el modo de token siguiente (Next Token). Si esta función está habilitada, cuando un usuario introduce la contraseña incorrecta tres veces (valor predeterminado), Citrix Gateway plugin 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 disponible en las configuraciones de Citrix Secure Web Gateway. Para usar RSA SecurID utilice Citrix 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 [aquí](#). Siga las instrucciones en el sitio Web y en el archivo Léame que se incluye con la herramienta.
2. Pegue la cadena numérica convertida dentro de un mensaje de correo electrónico y envíelo a los dispositivos de usuario.
3. Asegúrese de que la fecha y la hora en el dispositivo móvil sean correctas, ya que esto es necesario para la autenticación.
4. En el dispositivo móvil, abra el correo y haga clic en la cadena para iniciar el proceso de importación del token de software.

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

Nota:

En los dispositivos móviles que no asocian el archivo .sdtid con la aplicación Citrix Workspace para Android, cambie la extensión del archivo por .xml e impórtelo.

Guardar contraseñas

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

- Si se habilita el almacenamiento de contraseñas, la aplicación Citrix Workspace 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), la aplicación Citrix Workspace solicita a los usuarios que introduzcan sus contraseñas cada vez que se conectan.

Nota:

No puede almacenar la contraseña en las conexiones directas de StoreFront.

Para anular el parámetro de contraseñas almacenadas

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

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

Configuración

April 30, 2019

Citrix Casting

Citrix Casting combina entornos digitales y físicos para entregar aplicaciones y datos dentro de un espacio inteligente y seguro. El sistema completo conecta dispositivos (o cosas), como aplicaciones móviles y sensores, para crear un entorno inteligente que responda adecuadamente.

Citrix Ready Workspace Hub se ha construido sobre la plataforma Raspberry Pi 3. El dispositivo que ejecuta la aplicación Citrix Workspace se conecta a Citrix Ready Workspace Hub y transmite las aplicaciones o los escritorios hacia una pantalla más grande.

Con Citrix Casting, puede:

- Moverse por su sesión sin iniciar una sesión VDA en los dispositivos móviles.
- Ver la lista de centros de trabajo (hubs) disponibles tocando en **Ver lista de hubs** desde el cuadro de diálogo de **Workspace Hub**.

Configuración de Citrix Casting

Citrix Casting se habilita en la aplicación Citrix Workspace cuando se cumplen todos los requisitos de sistema siguientes:

- Aplicación Citrix Workspace 1809 para Android o una versión posterior
- Bluetooth habilitado
- Ubicación habilitada
- El dispositivo móvil y Workspace Hub deben utilizar la misma red Wi-Fi

Para activar la función Citrix Casting, toque en **Parámetros** y **Citrix Casting** en su dispositivo.

Limitaciones conocidas

- La Interfaz Web no admite el roaming de la sesión. Por lo tanto, no marque la casilla **Agregar tipo de cuenta como Interfaz Web**.

Para obtener más información sobre Citrix Ready Workspace Hub en la aplicación Citrix Workspace para Android, consulte [Configurar Citrix Ready Workspace Hub](#).

Para obtener información sobre Citrix Ready Workspace Hub, consulte la documentación de [Citrix Ready Workspace Hub](#).

Concesión de acceso a aplicaciones y escritorios virtuales

La aplicación Citrix Workspace necesita la configuración de la Interfaz Web o de StoreFront para entregar aplicaciones, archivos y escritorios desde una implementación de Citrix Virtual Apps and Desktops.

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 al servidor.

StoreFront

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

La autenticación entre la aplicación Citrix Workspace 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 Citrix Gateway.
- Los usuarios fuera del firewall pueden conectar a través de Citrix Gateway con StoreFront.

Conexión a través de Citrix Gateway

Citrix Gateway 11 y versiones posteriores reciben respaldo en la aplicación Citrix Workspace para Android para acceder a:

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

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 implementación de Workspace (Workspace para Web o una aplicación Citrix Workspace instalada localmente) que se utilicen. Todas las directivas pueden obtenerse a partir de un único servidor virtual.

Para crear cuentas en la aplicación Citrix Workspace, 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 Citrix 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 Citrix Gateway.

Para conectarse a Citrix Endpoint Management

Para permitir que los usuarios remotos se conecten mediante Citrix Gateway a la implementación de XenMobile, puede configurar Citrix 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:

[Citrix Gateway y Citrix Endpoint Management](#)

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 la aplicación Citrix Workspace o el Citrix Gateway Plug-in.

Si implementa XenMobile en la red, integre Citrix Gateway con StoreFront para permitir las conexiones de usuarios internos y usuarios remotos a StoreFront a través de Citrix Gateway. Con esta implementación, los usuarios pueden conectarse a StoreFront para acceder a las aplicaciones publicadas y escritorios virtuales desde Citrix Virtual Apps and Desktops. Los usuarios se pueden conectar mediante la aplicación Citrix Workspace.

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

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

Sugerencia

Cuando se usa Workspace para Web desde un explorador Web, las sesiones no se inician automáticamente al descargar un archivo .ICA. El archivo .ICA debe abrirse manualmente después de descargarlo para que la sesión se inicie.

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

Para los administradores que necesitan más control, Citrix ofrece una plantilla que se puede usar para crear un sitio de descargas para la aplicación Citrix Workspace para Android.

Configure las tiendas para StoreFront tal como lo haría con Citrix Virtual Apps and Desktops. 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 almacenes. Después de la instalación, los usuarios abren el archivo en el dispositivo para configurar la aplicación Citrix Workspace automáticamente. De forma predeterminada, los sitios de Workspace para Web ofrecen a los usuarios un archivo de aprovisionamiento para el único almacén para el que esté configurado el sitio en cuestión. También 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 Citrix Gateway que necesitan para acceder a sus escritorios y aplicaciones. Para las conexiones a través de Citrix 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 la aplicación Citrix Workspace, que intenta verificar la conexión y, si la conexión es satisfactoria, solicita a los usuarios que inicien sesión.

Configuración de la aplicación Citrix Workspace

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 Citrix 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 Citrix Gateway, 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.

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

[Configurar y administrar almacenes](#)

[Integración de StoreFront con Citrix Gateway](#)

Integrar Content Collaboration Service en la aplicación Citrix Workspace

Esta versión presenta la integración de Citrix Content Collaboration Service en la aplicación Citrix Workspace. Citrix Content Collaboration permite intercambiar documentos de manera fácil y segura, enviar documentos grandes por correo electrónico, gestionar de forma segura las transferencias de documentos a terceros y acceder a un espacio de colaboración. Citrix Content Collaboration ofrece muchas maneras de trabajar, incluida una interfaz web, clientes móviles, aplicaciones de escritorio e integración con Microsoft Outlook y Gmail.

Puede acceder a la funcionalidad Citrix Content Collaboration desde la aplicación Citrix Workspace. Para ello, vaya a la ficha Archivos que se muestra en la aplicación Citrix Workspace. La ficha Archivos solo se ve si Content Collaboration está habilitado en la configuración de Workspace, en la consola de Citrix Cloud.

Nota:

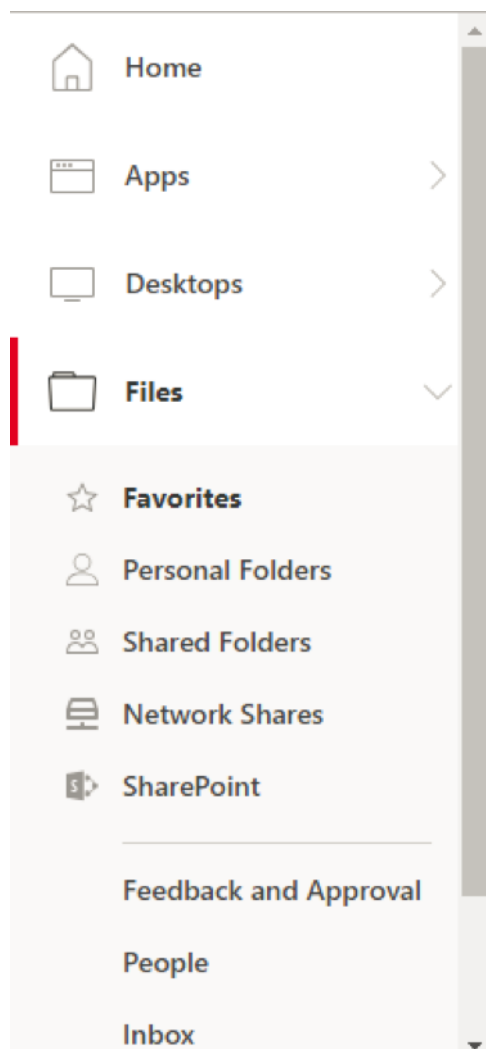
La integración de Citrix Content Collaboration en la aplicación Citrix Workspace no se admite en Windows Server 2012 y Windows Server 2016 debido a una opción de seguridad establecida en el sistema operativo.

Limitaciones:

- Restablecer la aplicación Citrix Workspace no hace que Citrix Content Collaboration cierre sesión.

- Cambiar de almacén en la aplicación Citrix Workspace no hace que Citrix Content Collaboration cierre la sesión.

En la siguiente imagen se muestra contenido de ejemplo en la ficha **Archivos** de la nueva aplicación Citrix Workspace:



Conexión con la Interfaz Web

La aplicación Citrix Workspace 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 Citrix Virtual Apps and Desktops. No se requiere ninguna configuración especial para los dispositivos móviles.

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

Para iniciar aplicaciones en el dispositivo Android:

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

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

[Configuración de la Interfaz Web.](#)

Sincronización de la distribución de teclado

La aplicación Citrix Workspace para Android ofrece opciones separadas para habilitar el IME del cliente y la sincronización de la distribución del teclado, en la sección **Parámetros**.

La opción **Habilitar IME del cliente** le permite escribir caracteres de doble byte (como los caracteres chinos, japoneses y coreanos) directamente en el punto de inserción de una sesión.

La opción **Sincronizar teclado** permite sincronizar automáticamente la distribución del teclado con el agente VDA y el dispositivo del cliente.

En una instalación nueva y de forma predeterminada, la opción **Habilitar IME del cliente** está **Activada** para los idiomas japonés, chino y coreano y la opción **Sincronizar teclado** está **Desactivada**.

Para habilitar la sincronización de la distribución del teclado dinámico, **active** las opciones **Habilitar IME del cliente** y **Sincronizar teclado**.

Notas:

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

Limitaciones:

- Esta característica solo funciona en los teclados internos de los dispositivos, no en teclados externos.
- Ciertos dispositivos móviles pueden no ser totalmente compatibles con la sincronización de la distribución del teclado, como el Nexus 5x.
- La distribución del teclado solo puede sincronizarse desde el cliente hacia el servidor. Cuando se cambia la distribución del teclado en el lado del servidor, la del cliente no puede cambiarse.

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

Configurar tarjetas inteligentes USB

La aplicación Citrix Workspace proporciona respaldo para lectores de tarjeta inteligente USB con sitios de PNA, Interfaz Web y StoreFront. Si están habilitadas, puede usar tarjetas inteligentes USB con estos fines:

- Inicio de sesión con tarjeta inteligente - Autentica usuarios a la aplicación Citrix Workspace.
- Respaldo para aplicaciones de tarjetas inteligente - Permite que las aplicaciones publicadas compatibles con tarjetas inteligentes puedan acceder a dispositivos de tarjetas inteligentes locales.

La aplicación Citrix Workspace admite esta función en todos los dispositivos Android incluidos en [Biometric Associates](#).

La aplicación Citrix Workspace respalda los siguientes tipos de tarjetas inteligentes USB:

- Tarjetas Personal Identity Verification (PIV)
- Tarjetas CAC (Common Access Card)

La tarjeta inteligente USB se respalda en el sistema operativo Android, de la versión 6.0 (Marshmallow) a la versión 7.12 (Nougat). El sistema operativo Android Versión 8.0 (Oreo) y 9.0 (Pie) no están respaldados. Este es una limitación de terceros.

También puede habilitar la autenticación con tarjeta inteligente USB desde **Parámetros > Administrar cuentas**.

Respaldo de tarjetas inteligentes USB

Requisito previo:

- Descargue e instale el servicio Android PC/SC-Lite desde Google Play Store.
1. Conecte el lector de tarjetas inteligentes USB al dispositivo móvil. Para obtener información sobre cómo conectar lectores de tarjetas inteligentes, consulte las especificaciones del lector de tarjetas inteligentes proporcionadas por el fabricante.
 2. Agregar una cuenta de StoreFront que tenga una tarjeta inteligente habilitada

3. En la página de inicio de sesión de la aplicación Citrix Workspace, toque en **Agregar cuenta**. Toque en la opción **Usar tarjeta inteligente**.
4. Para modificar una cuenta existente para usar la autenticación con tarjeta inteligente USB, toque en **Cuentas > Editar**, y toque la opción **Usar tarjeta inteligente**.

Instalación de la aplicación Citrix Workspace en una tarjeta SD

La aplicación Citrix Workspace para Android está optimizada para la instalación local en los dispositivos de los usuarios. No obstante, si los dispositivos no tienen suficiente espacio, los usuarios pueden instalar la aplicación Citrix Workspace para Android 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 la aplicación Citrix Workspace en el dispositivo de usuario, y después seleccione la opción Mover a tarjeta SD.

Si los usuarios deciden instalar la aplicación Citrix Workspace para Android 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 la aplicación Citrix Workspace para Android localmente en sus dispositivos de usuario, pueden mover la aplicación Citrix Workspace para Android a la tarjeta SD cuando sea necesario.

Acceder a archivos usando la asociación de tipos de archivo

Como requisito previo para que funcione esta característica, vaya a los parámetros de la aplicación Citrix Workspace para Android y configure la opción **Usar almacenamiento del dispositivo** en **Acceso total**. También está disponible, como opción adicional, **“Preguntar siempre”** para que se le solicite permiso antes de acceder al almacenamiento de su dispositivo en una sesión.

Nota:

La opción **Preguntar siempre** es un parámetro por sesión. No se traslada a la siguiente sesión.

Al seleccionar **Preguntar siempre**, cualquier acceso a su dispositivo generado por el sistema podría provocar la aparición de la ventana **Usar almacenamiento del dispositivo** (por ejemplo, en el cierre de sesión). Este es el comportamiento esperado.

La aplicación Citrix Workspace para Android lee y aplica los parámetros configurados por los administradores en Citrix Studio.

Para aplicar la asociación de tipos de archivo (File Type Association - FTA) en una sesión, asegúrese de que los usuarios se conecten al servidor de la tienda donde está configurada la asociación de tipos de archivo.

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

Nota:

Esta función solo está disponible en StoreFront y requiere Citrix Virtual Apps and Desktops versión 7 o una versión posterior.

Respaldo para usar la asociación de tipos de archivo (FTA) con Google Drive

Al usar un Chromebook, puede acceder a los archivos que residen en Google Drive desde la aplicación Citrix Workspace mediante la función de asociación de tipos de archivo (FTA). Puede utilizar sin problemas las aplicaciones de Android disponibles en los Chromebooks para acceder a estos archivos. Por ejemplo, si guarda un archivo .doc en Google Drive, puede abrir el archivo utilizando una aplicación de Android (en este caso, Microsoft Word) en el Chromebook desde la aplicación Citrix Workspace.

Nota

Solo los dispositivos Chromebook admiten asociación de tipos de archivo con Google Drive.

Para habilitar el acceso a los archivos en Google Drive, haga lo siguiente:

1. Descargue el componente de Citrix File Access (FileAccess.exe) de la [Página de descargas de la aplicación Citrix Workspace para Chrome](#) e instálelo en el VDA.
2. Con Citrix Studio, configure las asociaciones de tipo de archivo (FTA) adecuadas para las aplicaciones publicadas. Las asociaciones de tipos de archivo se pueden configurar a partir de las respectivas propiedades o parámetros de la aplicación. Para obtener más información sobre cómo configurar las asociaciones de tipos de archivo, consulte el artículo de Knowledge Center [CTX218743](#).

3. En una sesión de Citrix Virtual Apps and Desktops, abra el navegador predeterminado, agregue la siguiente URL a los sitios de confianza: <https://accounts.google.com> y <https://ssl.gstatic.com>.
4. En el dispositivo Chromebook, seleccione el archivo que desea abrir. Toque en **Abrir** y seleccione la aplicación Citrix Workspace de la lista.

Problemas conocidos y limitaciones

1. 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 la aplicación Citrix Workspace se bloquee.
2. La autenticación mediante tarjeta inteligente no está respaldada en los sitios de servicios de XenApp.
3. 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.
4. Citrix recomienda que salga y reinicie la sesión de la aplicación Citrix Workspace después de cerrar la sesión de la cuenta de la tarjeta inteligente.
5. No se admite el uso de varias tarjetas inteligentes USB.
6. Puede acceder solo a los formatos de archivo MIME admitidos por Microsoft Office, Adobe Acrobat Reader y Bloc de notas mediante la función de asociación de tipos de archivo.

Solucionar problemas

April 30, 2019

Directiva de validación conjunta de certificados de servidor

Esta versión de la aplicación Citrix Workspace para Android tiene una directiva más estricta para validar los certificados de servidor.

Importante:

Antes de instalar esta versión de la aplicación Citrix Workspace para Android, confirme que los certificados presentes en el servidor o en Citrix Gateway se han configurado correctamente como se describe aquí. Las conexiones pueden fallar si:

- la configuración del servidor o de Citrix Gateway incluye un certificado raíz incorrecto.

- la configuración del servidor o de Citrix Gateway no incluye todos los certificados intermedios.
- la configuración del servidor o de Citrix Gateway incluye un certificado intermedio caducado o no válido.
- la configuración del servidor o de Citrix Gateway incluye un certificado intermedio con firmas cruzadas.

Cuando valida un certificado de servidor, la aplicación Citrix Workspace para Android usa ahora **todos** los certificados suministrados por el servidor (o por Citrix Gateway) para validarlo. Luego también verifica que los certificados sean de confianza. Si no todos los certificados son de confianza, la conexión falla.

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

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

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

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

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

Importante

Algunas entidades de certificación tienen más de un certificado raíz. Si necesita usar esta validación más estricta, compruebe que la configuración usa el certificado raíz correspondiente. Por ejemplo, actualmente hay dos certificados (“DigiCert”/”GTE CyberTrust Global Root” y “DigiCert Baltimore Root”/”Baltimore CyberTrust Root”) que pueden validar los mismos certificados de servidor. En algunos dispositivos de usuario, están disponibles ambos certificados raíz. En otros dispositivos, solo uno está disponible (“DigiCert Baltimore Root” o “Baltimore CyberTrust Root”). Si configura “GTE CyberTrust Global Root” en la puerta de enlace, fallarán las conexiones de la aplicación Citrix Workspace para Android en esos dispositivos de usuario. Consulte la documentación de la entidad de certificación para determinar qué certificado raíz debe usarse. Tenga en cuenta que los certificados raíz también caducan, como todos los demás certificados.

Nota:

Algunos servidores y Citrix Gateway nunca envían el certificado raíz, aunque se haya configurado. En esos casos, esta validación más estricta no es posible.

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

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

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

Supongamos ahora que se configura una Citrix Gateway con estos certificados:

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

La aplicación Citrix Workspace para Android lee el certificado raíz incorrecto y la conexión falla.

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

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

Algunas entidades de certificación usan un certificado intermedio con firmas cruzadas. Este tipo de certificado está pensado para situaciones en que hay más de un certificado raíz: un certificado raíz anterior se usa al mismo tiempo que un certificado raíz posterior. En este caso, habrá al menos dos certificados intermedios. Por ejemplo, el certificado raíz anterior “Class 3 Public Primary Certification Authority” tiene el certificado intermedio con firma cruzada correspondiente “VeriSign Class 3 Public Primary Certification Authority - G5.” Sin embargo, un certificado raíz posterior correspondiente “VeriSign Class 3 Public Primary Certification Authority - G5” también está disponible, que reemplaza a la “Class 3 Public Primary Certification Authority.” El certificado raíz posterior no usa ningún certificado intermedio con firmas cruzadas.

El certificado intermedio con firmas cruzadas y el certificado raíz tienen el mismo Nombre de sujeto (Emitido para), pero el certificado intermedio con firmas cruzadas tiene otro Nombre de emisor (Emitido por). Esto distingue el certificado intermedio con firmas cruzadas de un certificado intermedio normal (como “Certificado intermedio 2 - ejemplo”).

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

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

No configure Citrix Gateway para que use el certificado intermedio con firmas cruzadas, porque seleccionará el certificado raíz anterior:

- “Certificado de servidor - ejemplo”
- “Certificado intermedio - ejemplo”
- “Certificado intermedio con firmas cruzadas de ejemplo” [no se recomienda]

No se recomienda configurar Citrix Gateway usando solamente el certificado del servidor:

- “Certificado de servidor - ejemplo”

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

SDK y API

November 8, 2018

Citrix Virtual Channel SDK

El Citrix Virtual Channel Software Development Kit (SDK) ofrece respaldo para la escritura de aplicaciones del lado del servidor y controladores del lado del cliente para canales virtuales adicionales con el protocolo ICA. Las aplicaciones de canal virtual del lado del servidor se encuentran en servidores Citrix Virtual Apps and Desktops. Esta versión del SDK ofrece respaldo para la escritura de canales virtuales nuevos en la aplicación Citrix Workspace para Android. Si desea escribir controladores virtuales para otras plataformas cliente, póngase en contacto con el equipo de Asistencia técnica de Citrix.

El Virtual Channel SDK ofrece:

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

El Virtual Channel SDK requiere el SDK de WFAPI para escribir la parte del lado del servidor del canal virtual. Para obtener más información sobre el SDK, consulte [Citrix Virtual Channel SDK para la aplicación Citrix Workspace para Android](#).

**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2019 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).