



# Aplicación Citrix Workspace para Android

## **Contents**

<b>Acerca de esta versión</b>	<b>3</b>
<b>Requisitos previos para la instalación</b>	<b>16</b>
<b>Instalación, actualización</b>	<b>21</b>
<b>Introducción</b>	<b>23</b>
<b>Configuración</b>	<b>27</b>
<b>Autenticarse</b>	<b>46</b>
<b>SDK y API</b>	<b>47</b>

## Acerca de esta versión

January 15, 2021

### **Novedades en la versión 21.1.0**

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

### **Novedades en la versión 20.12.0**

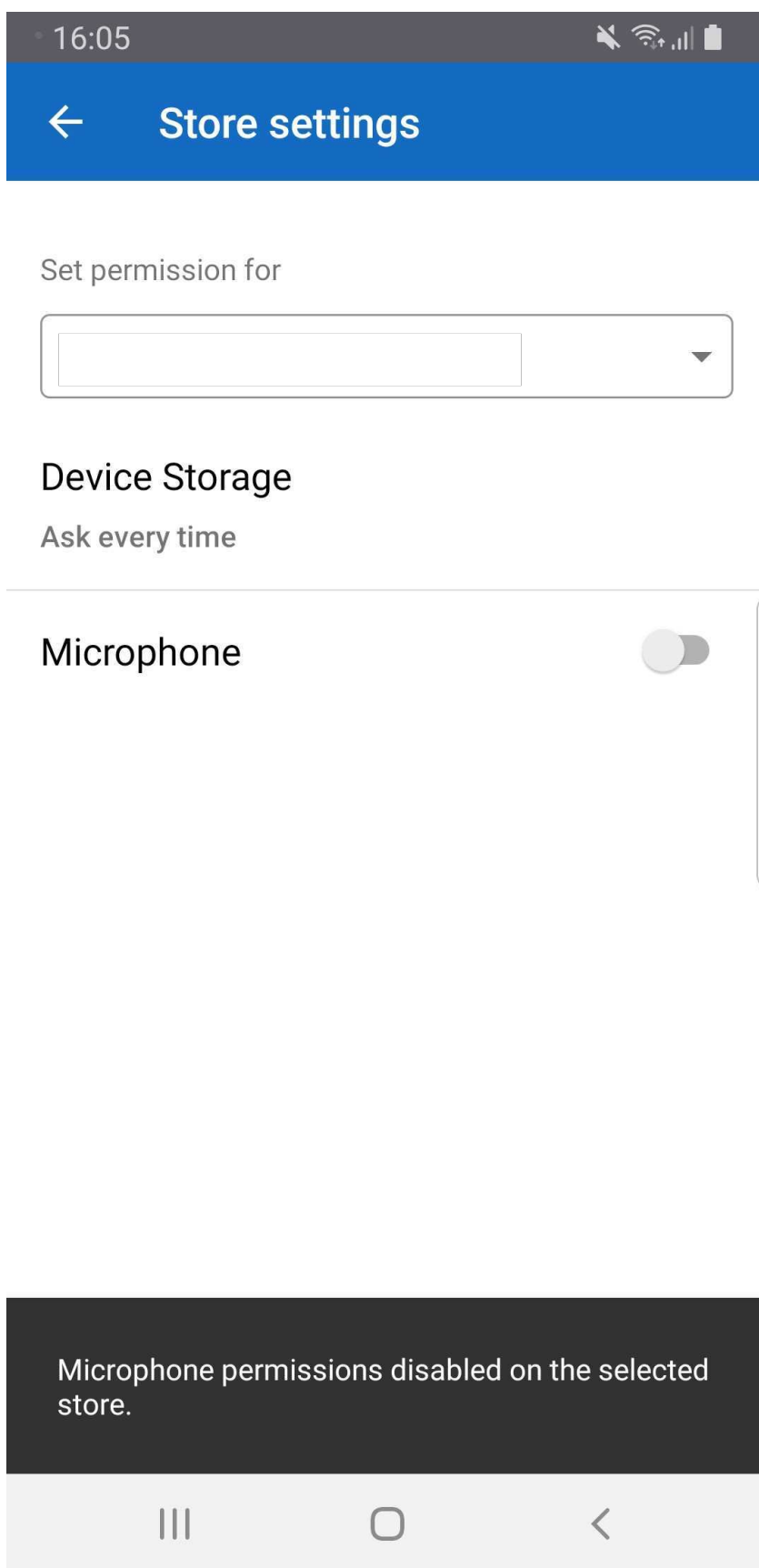
#### **Acceso a micrófonos por almacén**

La función de confianza en clientes selectivos permite a la aplicación Citrix Workspace confiar en el acceso desde una sesión de VDA. Puede conceder acceso a unidades cliente y dispositivos de hardware locales, como micrófonos y cámaras web.

Antes, la configuración del acceso al micrófono se aplicaba en todos los almacenes configurados.

A partir de esta versión, la aplicación Citrix Workspace requiere el permiso del usuario para acceder al micrófono. La configuración seleccionada para el acceso al micrófono se aplica por almacén.

Puede configurar los niveles de acceso desde **Parámetros > Parámetros de almacén**.



En la opción **Establecer permisos para**, seleccione el almacén en el menú desplegable. Habilite **Mi-crófono**.

### **Compatibilidad con Android Enterprise**

A partir de esta versión, la aplicación Citrix Workspace es compatible con Android Enterprise.

Para obtener más información, consulte [Android Enterprise](#) en la documentación de Citrix Endpoint Management.





### **Mecanismo mejorado para enviar comentarios**


Antes, podía proporcionar comentarios a Citrix mediante la aplicación Citrix Workspace solamente a través del correo electrónico.


Con esta versión, puede enviarnos comentarios sobre Workspace y notificarnos problemas desde la misma interfaz. Para enviar comentarios:

Haga clic en **Parámetros** > **Enviar comentarios a Citrix**.

Aparecerá el cuadro de diálogo **Notificar un problema**.

9:49   LTE   19%

 **Report an issue**

 Workspace

---

Request help from Support


---

Facing issues when adding a store



---



When did this issue occur? 3 hours ago

---


 2 screenshots

---

 Screenshot\_20201202-075311.png 

 Screenshot\_20201202-094455.png 

---

Log Options 

---

Send using Secure Mail

**Send**

---

Mediante el cuadro de diálogo Notificar un problema, puede:

- Solicitar ayuda a la Asistencia técnica
- Notificar un problema
- Enviar registros de problemas

### **Novedades en la versión 20.11.1**

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

### **Novedades en la versión 20.11.0**

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

### **Novedades en la versión 20.10.5**

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

### **Novedades en la versión 20.10.0**

La aplicación Citrix Workspace admite los requisitos actuales de la API de destino de Google Play para Android 10.

### **Novedades en la versión 20.9.5**

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

### **Novedades en la versión 20.9.0**

#### **Disponibilidad general de la redirección USB**

Ahora la función de redirección USB es totalmente funcional y está disponible para el público. De forma predeterminada, la función de redirección USB está inhabilitada.

La función de redirección de dispositivos USB genéricos permite la redirección de dispositivos USB arbitrarios desde máquinas cliente a Citrix Virtual Apps and Desktops. Esta función le permite interactuar con una amplia selección de dispositivos USB genéricos en una sesión como si estuvieran conectados físicamente a ella.

Como requisito previo para administrar esta función mediante Citrix Global App Configuration Service, debe **habilitar** la función de redirección USB en el Delivery Controller. Para obtener más información sobre cómo configurar la redirección USB en el Delivery Controller, consulte la sección [Dispositivos USB genéricos](#) en la documentación de Citrix Virtual Apps and Desktops.

Citrix Global App Configuration Service ofrece a los administradores de Citrix la capacidad de entregar URL de servicio de Citrix Workspace y la configuración de la aplicación Citrix Workspace a través de un servicio administrado de forma centralizada.

La función de redirección USB está integrada y se puede configurar a través de Citrix Global App Configuration Service. Puede administrar la función mediante Citrix Global App Configuration Service en el caso de redes no conectadas a dominios.

Para obtener información sobre cómo configurar la función con este método, consulte [Global App Configuration Service](#) en la documentación para desarrolladores.

### **Nota:**

Esta función está disponible para el público a partir de la versión 20.9.0. En la versión 20.8.0 y en las versiones anteriores, solo está disponible si se solicita.

### **Novedades en la versión 20.8.1**

En esta versión se han resuelto varios problemas para mejorar la estabilidad y el rendimiento generales.

### **Novedades en la versión 20.8.0**

#### **Mejora de la asignación de unidades de cliente (CDM)**

Antes se aplicaba una opción seleccionada de almacenamiento del dispositivo para todos los almacenes configurados.

Con esta versión, la aplicación Citrix Workspace le permite seleccionar una opción de almacenamiento del dispositivo dedicada para cada almacén configurado.

Durante el inicio de sesión, aparecerá un mensaje para seleccionar el tipo de almacenamiento del dispositivo, junto con los detalles del almacén. Puede realizar una de las siguientes acciones:

- Seleccione una de las opciones de almacenamiento del dispositivo y haga clic en **Aceptar**: La opción se aplicará solo a la sesión actual. En cada inicio, aparece un mensaje para que seleccione el tipo de almacenamiento del dispositivo.
- Seleccione una de las opciones de almacenamiento del dispositivo, seleccione **No volver a preguntar** y haga clic en **Aceptar**: La opción se aplicará a todos los inicios de sesión de ese almacén. No se le volverá a preguntar.



- Seleccione **Cancelar**: Se le pedirá que seleccione un tipo de almacenamiento del dispositivo en cada inicio y también dentro de una sesión. La sesión no tiene acceso al almacenamiento del dispositivo.

**Nota:**

Esta función solo se aplica en los inicios directos de ICA y en los almacenes configurados de Citrix Gateway. No es compatible con almacenes que no tienen una configuración SSL de extremo a extremo.

### **Novedades en la versión 20.7.5**

En la ficha **Recientes**, se muestran ahora las aplicaciones móviles nativas junto con las aplicaciones y escritorios publicados.

### **Novedades en la versión 20.7.0**

#### **Mejora de la interfaz de usuario**

A partir de esta versión, ya puede quitar los detalles de la cuenta de almacén a través de la opción **Modificar**. Haga clic en **Quitar cuenta** para quitar los detalles de la cuenta.

### **Novedades en la versión 20.6.5**

#### **Actualización de la criptografía**

Esta función es un cambio importante en el protocolo de comunicación segura. Los conjuntos de cifrado con el prefijo `TLS_RSA_` no ofrecen confidencialidad directa y no se consideran robustos.

En esta versión, los conjuntos de cifrado `TLS_RSA_` se han eliminado. Esta versión admite conjuntos de cifrado `TLS_ECDHE_RSA_` avanzados. Si su entorno no está configurado con los conjuntos de cifrado `TLS_ECDHE_RSA_`, no puede iniciar el cliente porque los cifrados no son robustos.

Se admiten los siguientes conjuntos de cifrado avanzado:

- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)`

TLS 1.0 admite los siguientes conjuntos de cifrado:

- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA`

TLS 1.2 admite los siguientes conjuntos de cifrado:

- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA`

### **Novedades en la versión 20.6.0**

En esta versión se han resuelto varios problemas para mejorar la estabilidad y el rendimiento generales.

### **Novedades en la versión 20.5.0**

#### **Opción para inhabilitar la visualización de mensajes de error**

Ahora puede inhabilitar la visualización del siguiente mensaje de error relacionado con la supervisión de red:

“Puede que la conexión se ralentice de forma temporal”.

Vaya a **Avanzado** y seleccione la opción **Inhabilitar mensajes de supervisión de red** para inhabilitar el mensaje de error relacionado con problemas de red en una sesión

### **Novedades en la versión 20.4.5**

En esta versión se han resuelto varios problemas para mejorar la estabilidad y el rendimiento generales.

### **Novedades en la versión 20.4.0**

En esta versión se han resuelto varios problemas para mejorar la estabilidad y el rendimiento generales.

### **Novedades en la versión 20.3.0**

A partir de la versión 20.3.0, la aplicación Citrix Workspace utiliza la versión 2.9 de Citrix HDX RealTime Media Engine (RTME).

#### **NOTA:**

No es necesario instalar HDX RTME para usar Skype Empresarial, solo se necesita la aplicación Citrix Workspace. Si HDX RTME ya está instalado en el dispositivo Chromebook, desinstálelo.

#### **Para habilitar HDX RTME desde la aplicación Citrix Workspace:**

De forma predeterminada, este parámetro está **desactivado**.

Para habilitar HDX RTME desde la aplicación Citrix Workspace, vaya a **Parámetros > Avanzado** y seleccione **Habilitar RealTime Media Engine**.

Para obtener más información, consulte la documentación de [HDX RealTime Optimization Pack 2.9](#).

### **Redirección automática de dispositivos USB**

Con esta versión, la aplicación Citrix Workspace le permite redirigir los dispositivos USB automáticamente al conectarlos. Al conectar un dispositivo USB, aparece un mensaje en el que se le pide permiso. Después de conceder el permiso, el dispositivo USB se redirige automáticamente.

#### **Nota:**

Esta función solo está disponible a la carta y funciona solamente si la función de redirección de dispositivos USB está habilitada.

### **Novedades en la versión 20.2.0**

En esta versión se ha mejorado las funciones de fiabilidad de la sesión y reconexión automática de clientes, así como el rendimiento y la estabilidad generales de la aplicación Citrix Workspace.

### **Novedades en 20.1.5**

En esta versión se han resuelto varios problemas para mejorar la estabilidad y el rendimiento generales.

### **Novedades en la versión 20.1.0**

En esta versión se han resuelto varios problemas para mejorar la estabilidad y el rendimiento generales.

### **Problemas resueltos**

#### **Problemas resueltos en la versión 21.1.0**

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

#### **Problemas resueltos en versiones anteriores**

#### **Problemas resueltos en la versión 20.12.0:**

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

#### **Problemas resueltos en la versión 20.11.1:**

- Una vez actualizada la versión de la aplicación Citrix Workspace para Android a la versión 20.11.0 mediante la tienda administrada Google Play, no se puede iniciar la aplicación Citrix Workspace y aparece el siguiente error:

“Your device is enrolled but store is not present. Remove your work profile to continue” (Su dispositivo está inscrito, pero la tienda no está presente. Quite su perfil de trabajo para continuar.)

Actualice la versión de la aplicación Citrix Workspace para Android a la versión 20.11.1 para resolver este problema.

[RFANDROID-7355]

**Problemas resueltos en la versión 20.11.0:**

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

**Problemas resueltos en la versión 20.10.5:**

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

**Problemas resueltos en la versión 20.10.0:**

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

**Problemas resueltos en la versión 20.9.5:**

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

**Problemas resueltos en la versión 20.9.0:**

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

**Problemas resueltos en la versión 20.8.1:**

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

**Problemas resueltos en la versión 20.8.0:**

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

**Problemas resueltos en la versión 20.7.5:**

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

**Problemas resueltos en la versión 20.7.0:**

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

**Problemas resueltos en la versión 20.6.5:**

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

**Problemas resueltos en la versión 20.6.0:**

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

**Problemas resueltos en la versión 20.5.0:**

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

**Problemas resueltos en la versión 20.4.5:**

- Es posible que HDX RealTime Optimization Pack no optimice Skype para Empresas durante el primer inicio. Como solución temporal, vuelva a iniciar la aplicación Citrix Workspace. (RFANDROID-5383)
- En un VDA habilitado para 3D Pro, es posible que aparezca una pantalla gris en algún momento al iniciar sesión. (RFANDROID-5471)

**Problemas resueltos en la versión 20.4.0:**

En esta versión se han resuelto varios problemas para mejorar la estabilidad y el rendimiento generales.

**Problemas resueltos en la versión 20.3.0:**

- Los intentos de iniciar aplicaciones SaaS pueden fallar en una sesión que se ejecuta en el modo quiosco cuando se trata de implementaciones en la nube. [RFANDROID-5137]

**Problemas resueltos en la versión 20.2.0:**

- En las implementaciones en la nube, el usuario se puede desplazar por la pantalla de bienvenida. [RFANDROID-5023]
- Pueden fallar los intentos de iniciar sesión en el modo quiosco. [RFANDROID-5133]

**Problemas resueltos en la versión 20.1.5:**

En esta versión se han resuelto varios problemas para mejorar la estabilidad y el rendimiento generales.

**Problemas resueltos en la versión 20.1.0:**

En esta versión se han resuelto varios problemas para mejorar la estabilidad y el rendimiento generales.

## **Problemas conocidos**

### **Problemas conocidos en la versión 21.1.0**

No se han observado nuevos problemas conocidos en esta versión.

### **Problemas conocidos en versiones anteriores**

#### **Problemas conocidos en la versión 20.12.0:**

No se han observado nuevos problemas conocidos en esta versión.

#### **Problemas conocidos en la versión 20.11.1:**

No se han observado nuevos problemas conocidos en esta versión.

#### **Problemas conocidos en la versión 20.11.0:**

No se han observado nuevos problemas conocidos en esta versión.

#### **Problemas conocidos en la versión 20.10.5:**

No se han observado nuevos problemas conocidos en esta versión.

#### **Problemas conocidos en la versión 20.10.0:**

No se han observado nuevos problemas conocidos en esta versión.

#### **Problemas conocidos en la versión 20.9.5:**

No se han observado nuevos problemas conocidos en esta versión.

#### **Problemas conocidos en la versión 20.9.0:**

No se han observado nuevos problemas conocidos en esta versión.

#### **Problemas conocidos en la versión 20.8.1:**

No se han observado nuevos problemas conocidos en esta versión.

#### **Problemas conocidos en la versión 20.8.0:**

No se han observado nuevos problemas conocidos en esta versión.

#### **Problemas conocidos en la versión 20.7.5:**

No se han observado nuevos problemas conocidos en esta versión.

#### **Problemas conocidos en la versión 20.7.0:**

No se han observado nuevos problemas conocidos en esta versión.

#### **Problemas conocidos en la versión 20.6.5:**

No se han observado nuevos problemas conocidos en esta versión.

**Problemas conocidos en la versión 20.6.0:**

No se han observado nuevos problemas conocidos en esta versión.

**Problemas conocidos en la versión 20.5.0:**

No se han observado nuevos problemas conocidos en esta versión.

**Problemas conocidos en la versión 20.4.5:**

No se han observado nuevos problemas conocidos en esta versión.

**Problemas conocidos en la versión 20.4.0:**

No se han observado nuevos problemas conocidos en esta versión.

**Problemas conocidos en la versión 20.3.0:**

- En un dispositivo Samsung DeX, es posible que no pueda cancelar la redirección de dispositivos USB si cierra la solicitud de permiso sin hacer clic en el botón **Cancelar**. [RFANDROID-5397]

**Problemas conocidos en la versión 20.2.0:**

- Los intentos de iniciar sesión fallan con un mensaje de error cuando se inhabilita la directiva **Fiabilidad de la sesión** en un VDA habilitado para SSL. [RFANDROID-5065]
- Los intentos de iniciar aplicaciones SaaS pueden fallar en una sesión que se ejecuta en el modo quiosco cuando se trata de implementaciones en la nube. [RFANDROID-5137]
- Los intentos de reconexión de clientes no funcionan y aparece el siguiente mensaje de error:  
“Problema general. Intente conectarse de nuevo”.

El problema se produce en los almacenes configurados de Citrix Gateway si la opción **Reconexión de la sesión** está inhabilitada y la opción **Reconexión automática de clientes** está habilitada en el Controller.

[RFANDROID-5138]

- Los intentos de reconexión fallan tras hacer clic en **Conectar** en el cuadro de diálogo **Reconexión automática de clientes**. El problema se produce en sesiones conectadas a Citrix XenApp y XenDesktop 7.6 CU 8. [RFANDROID-5151]

**Problemas conocidos en la versión 20.1.5:**

- En una configuración de varios almacenes en la nube, es posible que, al eliminar un almacén, no se eliminen los detalles de este. El almacén seguirá figurando hasta que el usuario quite la aplicación Workspace de la ficha **Recientes**. [RFANDROID-5043]

**Problemas conocidos en la versión 20.1.0:**

No se han observado nuevos problemas conocidos en esta versión.

## Avisos legales de terceros

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). Para 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](#).

La aplicación Citrix Workspace puede incluir software de terceros con licencias definidas en las condiciones del siguiente documento:

[Aplicación Citrix Workspace para Android: Avisos de terceros](#)

## Requisitos previos para la instalación

September 22, 2020

### Requisitos del sistema y compatibilidad

#### Requisitos de dispositivo

La aplicación Citrix Workspace para Android es compatible con Android 7.x (Nougat), 8.x (Oreo), 9.x (Pie), 10.x (Android Q) y 11 (Android R).

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

La aplicación Citrix Workspace permite iniciar sesiones desde Workspace para Web cuando el explorador web que se utilice funciona con Workspace para Web. Si no puede iniciar sesiones, configure su cuenta a través de la aplicación Citrix Workspace 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 almacenes de StoreFront. La aplicación Citrix Workspace para Android también admite versiones anteriores de StoreFront.



- StoreFront configurado con Workspace para sitios web

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

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

### **Conexiones, certificados y autenticación**

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

Para conexiones LAN:

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

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

- Citrix Gateway 11 y versiones posteriores (incluidas las versiones VPX, MPX y SDX)

### **Certificados TLS**

Cuando se protegen las conexiones remotas con 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 de Citrix mediante la aplicación Citrix Workspace para Android.

#### **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 Android admite certificados comodín.

### Certificados intermedios y Citrix Gateway

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

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

### 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:

- “Ejemplo de certificado de servidor”
- “Ejemplo de certificado intermedio”
- “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 con estos certificados válidos. Esta configuración, sin certificado raíz, es la que se suele recomendar:

- “Ejemplo de certificado de servidor”
- “Ejemplo de certificado intermedio”

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:

- “Ejemplo de certificado de servidor”
- “Ejemplo de certificado intermedio”
- “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):

- “Ejemplo de certificado de servidor”
- “Ejemplo de certificado intermedio 1”
- “Ejemplo de certificado intermedio 2”

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:

- “Ejemplo de certificado de servidor”
- “Ejemplo de certificado intermedio”

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

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

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

- “Ejemplo de certificado de servidor”

Cuando la aplicación Citrix Workspace para Android no puede localizar todos los certificados intermedios, la conexión falla.

### Autenticación

#### Nota:

La autenticación RSA SecurID no se admite en 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 Wi-Fi y sin Wi-Fi
- 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

Ahora la aplicación Citrix Workspace para Android admite los siguientes productos y configuraciones.

Lectores de tarjetas inteligentes compatibles:

- BaiMobile 3000MP USB Smart Card Reader

Tarjetas inteligentes compatibles:

- Tarjetas PIV
- Tarjetas CAC (Common Access Card)

Configuraciones admitidas:

- 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.

#### Nota:

Se pueden configurar otras soluciones de autenticación por token mediante RADIUS. Para obtener información sobre la autenticación de SafeWord con tokens, consulte [Configurar la autenticación de SafeWord](#).

## Instalación, actualización

July 21, 2020

## Actualizaciones

Para actualizar la aplicación Citrix Workspace a la versión más reciente, realice cualquiera de los siguientes pasos:

- Descargue la aplicación Citrix Workspace de la página [Descargas de Citrix](#) e instale la aplicación para actualizar Citrix Receiver a la aplicación Citrix Workspace.
- Actualice la versión de su aplicación Citrix Workspace mediante Google Play.

Para obtener información sobre las funciones disponibles en la aplicación Citrix Workspace para Android, consulte la [tabla de funciones de la aplicación Citrix Workspace](#).

Para acceder a la documentación de Citrix Receiver para Android, consulte [Citrix Receiver](#).

## HDX RealTime Media Engine

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

HDX RealTime Media Engine (RTME) es un plug-in de la aplicación Citrix Workspace 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 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.

### Nota:

- HDX RTME para la aplicación Citrix Workspace para Android solo se admite en Chromebooks con procesador Intel Core.
- Debe desinstalar la versión existente de HDX RTME para instalar la versión más reciente disponible con la aplicación Citrix Workspace.

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.

## Habilite HDX RTME desde la aplicación Citrix Workspace:

De forma predeterminada, este parámetro está **desactivado**.

Para habilitar HDX RTME desde la aplicación Citrix Workspace, vaya a **Configuración > Avanzado** y seleccione **Habilitar RealTime Media Engine**.

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

## 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. Esta funcionalidad se ofrece de forma predeterminada y no se requiere ninguna 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.

## Introducción

September 24, 2020

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

Complete 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 usar una configuración automática se puede introducir el nombre completo de dominio (FQDN) o un servidor de StoreFront o Citrix Gateway, o bien se puede usar una dirección de correo electrónico para crear una 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](#)

### Directiva de Google

A partir de la versión 1909 de la aplicación Citrix Workspace para Android, puede configurar la aplicación Citrix Workspace desde la consola de administración de Google mediante la directiva de Google. Esta función solo se ofrece en dispositivos Chromebook.

Con la directiva de Google, puede agregar la URL del almacén para agregar uno o más almacenes.

#### Problemas conocidos:

- Esta función no se ofrece en la versión 5.0 de Android ni en versiones anteriores.
- Cuando descarga el archivo ICA desde un explorador web e inicia la sesión, no se aplica el almacén agregado mediante la directiva de Google. En su lugar, la aplicación Citrix Workspace abre el archivo ICA descargado.

#### Archivo de ejemplo de la directiva de Google:

```
1 {
2
3   "v1": {
4
5     "stores": [
6       {
7
8         "url": <"https://xyz.example.com">
9         "is_web_interface_enabled":false
10      }
11   ,
12     {
13
14       "url": <https://xyz.example.com>
15       "is_web_interface_enabled":false
16     }
17   ]
18 }
19 }
```



```
17
18     ]
19   }
20
21 }
```

**Nota:**

Proporcione la URL completa del almacén y no solo el nombre del dominio.

### 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.

### Archivo de aprovisionamiento

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 configura Workspace para sitios 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 conectarse correctamente a sus aplicaciones y escritorios alojados en servidores:

- La dirección URL de StoreFront o del sitio de XenApp y XenDesktop que aloja los recursos; por ejemplo, nombredelservidor.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.

### **Conceder acceso a Citrix Virtual Apps and Desktops**

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

#### **StoreFront**

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

La autenticación entre la aplicación Citrix Workspace y un almacén de StoreFront se puede gestionar de varias formas:

- Los usuarios dentro del firewall pueden conectarse directamente a StoreFront.
- Los usuarios fuera del firewall pueden conectarse a StoreFront a través de Citrix Gateway.
- Los usuarios fuera del firewall pueden conectar a través de Citrix Gateway con StoreFront.

#### **Conexión con StoreFront**

La aplicación Citrix Workspace para Android permite iniciar 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, los almacenes que se crean consisten en servicios que proporcionan una infraestructura de recursos y autenticación para la aplicación Citrix Workspace. Cree almacenes que enumeren y agreguen escritorios y aplicaciones desde los sitios de XenDesktop y XenApp para, así, habilitar 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 los almacenes para StoreFront tal como lo haría con Citrix Virtual Apps and Desktops. No se requiere ninguna configuración especial para los dispositivos móviles.

### **Conectarse a través de Citrix Gateway**

Citrix Gateway 11 y versiones posteriores se admiten en la aplicación Citrix Workspace para Android para acceder a:

- Sitios de XenApp y XenDesktop
- Almacenes 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 en función del tipo de conexión (ICA, VPN sin clientes o VPN) y el tipo de implementación de Workspace (Workspace para Web o una aplicación Citrix Workspace instalada localmente) que se utilicen. Las directivas pueden crearse desde 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.

### **Citrix Endpoint Management**

La aplicación Workspace permite a los usuarios acceder a aplicaciones, archivos y otros recursos entregados por Citrix Endpoint Management. Para obtener más información, consulte [Integración en la experiencia de Citrix Workspace](#)

## **Configuración**

January 15, 2021

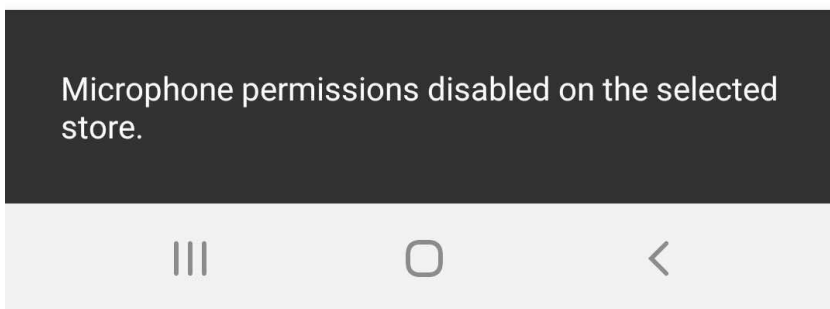
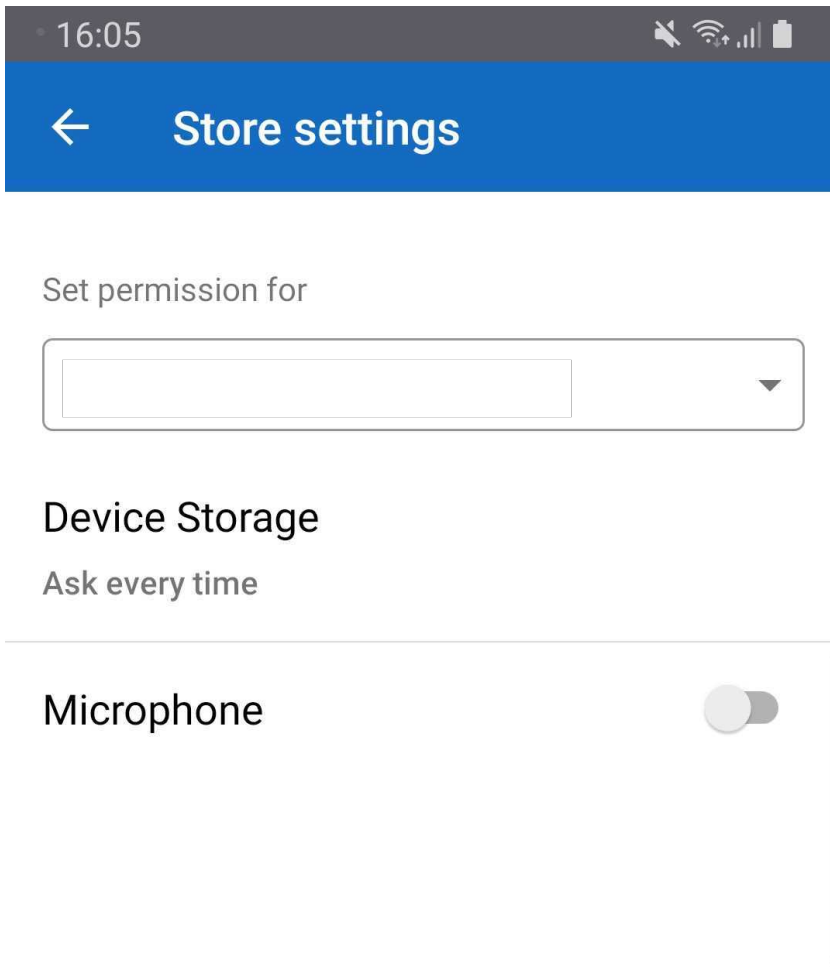
### **Acceso a micrófonos por almacén**

La función de confianza en clientes selectivos permite a la aplicación Citrix Workspace confiar en el acceso desde una sesión de VDA. Puede conceder acceso a unidades cliente y dispositivos de hardware locales, como micrófonos y cámaras web.

Antes, la configuración del acceso al micrófono se aplicaba en todos los almacenes configurados.

A partir de esta versión, la aplicación Citrix Workspace requiere el permiso del usuario para acceder al micrófono. La configuración seleccionada para el acceso al micrófono se aplica por almacén.

Puede configurar los niveles de acceso desde **Parámetros > Parámetros de almacén**.



En la opción **Establecer permisos para**, seleccione el almacén en el menú desplegable. Habilite **Micrófono**.

### Inicio automático del archivo ICA

Puede iniciar sus aplicaciones y escritorios publicados con un clic en el recurso. Esta función requiere la versión 1912 de StoreFront (local) o una posterior.

**Nota:**

- El inicio automático del archivo ICA solo está disponible en los dispositivos Chromebook y solo en las URL de almacén HTTPS.
- No seleccione la opción **Recordar mi elección** cuando inicie un recurso.

### Inicio mejorado de sesiones

Las aplicaciones y escritorios publicados se inician en ventanas separadas. Así, puede usar la ventana de enumeración de almacén e interactuar con ella sin tener que desconectar ni cerrar la sesión.

**Nota:**

- Esta función solo se ofrece en dispositivos Chromebook.
- Esta función no se ofrece en tabletas, teléfonos ni Samsung DeX.

### Limitaciones:

- Después de cambiar cualquier parámetro de usuario, debe volver a iniciar la sesión para que los cambios surtan efecto.
- Las aplicaciones y el escritorio se denominan “Espacio de trabajo” en la barra de tareas, no a partir de la sesión.
- No se puede utilizar más de una sesión a la vez.

### Workspace con funciones inteligentes

La aplicación Citrix Workspace para Android está optimizada para aprovechar las próximas funciones inteligentes cuando se publiquen. Para obtener más información, consulte [Funciones inteligentes de Workspace: Microaplicaciones](#).

### Indicador de estado de la batería

Ahora el estado de la batería del dispositivo se muestra en el área de notificaciones de las sesiones de Citrix Desktop.

**Nota:**

El indicador de estado de la batería no se muestra para el VDA del servidor.

### **Asignación de unidades de cliente**

La aplicación Citrix Workspace informa al servidor de las unidades de cliente disponibles. De forma predeterminada, a las unidades del cliente se les asignan letras de unidad del servidor, de manera que parezca que están directamente conectadas a la sesión. Estas asignaciones están disponibles solamente para el usuario durante la sesión actual.

**Nota:**

Esta función solo es compatible con versiones de Android con SDK que tengan la versión 24 o una posterior.

La asignación de unidades de cliente (CDM) permite dispositivos de almacenamiento plug-and-play en una sesión. Esto significa que puede utilizar dispositivos de almacenamiento masivo (como, por ejemplo, unidades extraíbles) para copiar y pegar documentos entre la unidad extraíble y el dispositivo del usuario.

#### **Limitaciones:**

- Se ha constatado que las API de Android son lentas, lo que retrasa ciertas operaciones.
- La asignación CDM para almacenamiento externo no es compatible con dispositivos Pixel.
- La asociación de tipos de archivo no se admite en dispositivos de almacenamiento externos.

#### **Problema conocido:**

- La pantalla de la aplicación Workspace puede cambiar entre primer plano y segundo plano al conectar un dispositivo de almacenamiento externo.

### **Citrix HDX RealTime Media Engine incrustado**

A partir de la versión 20.3.0, la aplicación Citrix Workspace utiliza la versión 2.9 de Citrix HDX RealTime Media Engine (RTME).

**NOTA:**

No es necesario instalar HDX RTME para usar Skype Empresarial, solo se necesita la aplicación Citrix Workspace. Si HDX RTME ya está instalado en el dispositivo Chromebook, desinstálelo.

#### **Para habilitar HDX RTME desde la aplicación Citrix Workspace:**

De forma predeterminada, este parámetro está **desactivado**.

Para habilitar HDX RTME desde la aplicación Citrix Workspace, vaya a **Parámetros > Avanzado** y seleccione **Habilitar RealTime Media Engine**.

Esta función se admite en:

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

**Nota:**

Solo se necesita la aplicación Citrix Workspace para usar Skype Empresarial. No es necesario instalar HDX RTME. Si HDX RTME ya está instalado en el dispositivo Chromebook, debe desinstalarlo.

Para obtener más información, consulte la documentación de [HDX RealTime Optimization Pack 2.9](#).

### Usuarios no autenticados

La aplicación Citrix Workspace admite usuarios no autenticados (anónimos). Los usuarios anónimos pueden iniciar correctamente sesiones de Citrix Virtual Apps and Desktops.

### Redirección de dispositivos USB

A partir de la versión 20.9.0, la función de redirección USB es totalmente funcional y está lista para la disponibilidad general. De forma predeterminada, la función de redirección USB está inhabilitada.

La función de redirección de dispositivos USB genéricos permite la redirección de dispositivos USB arbitrarios desde máquinas cliente a Citrix Virtual Apps and Desktops. Esta función le permite interactuar con una amplia selección de dispositivos USB genéricos en una sesión como si estuvieran conectados físicamente a ella.

Como requisito previo para administrar esta función mediante Citrix Global App Configuration Service, debe **habilitar** la función de redirección USB en el Delivery Controller. Para obtener más información sobre cómo configurar la redirección USB en el Delivery Controller, consulte la sección [Dispositivos USB genéricos](#) en la documentación de Citrix Virtual Apps and Desktops.

Citrix Global App Configuration Service ofrece a los administradores de Citrix la capacidad de entregar URL de servicio de Citrix Workspace y la configuración de la aplicación Citrix Workspace a través de un servicio administrado de forma centralizada.

La función de redirección USB está integrada y se puede configurar a través de Citrix Global App Configuration Service. Puede administrar la función mediante Citrix Global App Configuration Service en el caso de redes no conectadas a dominios.

Para obtener información sobre cómo configurar la función con este método, consulte [Global App Configuration Service](#) en la documentación para desarrolladores.



**Nota:**

Esta función está disponible para el público a partir de la versión 20.9.0. En la versión 20.8.1 y en las versiones anteriores, solo está disponible si se solicita.

La directiva Redirección de USB debe establecerse en **Permitida** en el Delivery Controller. Para obtener información sobre cómo configurar la redirección USB en Citrix Studio, consulte [Configurar la redirección de USB genérico](#) en la documentación de Citrix Virtual Apps and Desktops.

**Para impresoras y escáneres:**

Instale los controladores específicos del proveedor en el dispositivo. Una vez finalizada la instalación, es posible que el software del proveedor pida que vuelva a conectar el dispositivo USB. Vuelva a conectar el dispositivo USB para redirigirlo.

**Para Chromebooks:**

De forma predeterminada, el sistema operativo Chrome bloquea los dispositivos USB (por ejemplo, las unidades USB). En caso de Chromebooks administrados, debe incluir en la lista de dispositivos permitidos desde la consola de administración de Google.

Para obtener información sobre cómo incluir en la lista de dispositivos USB permitidos en un Chromebook, consulte el artículo [CTX200825](#) del Knowledge Center.

**Nota:**

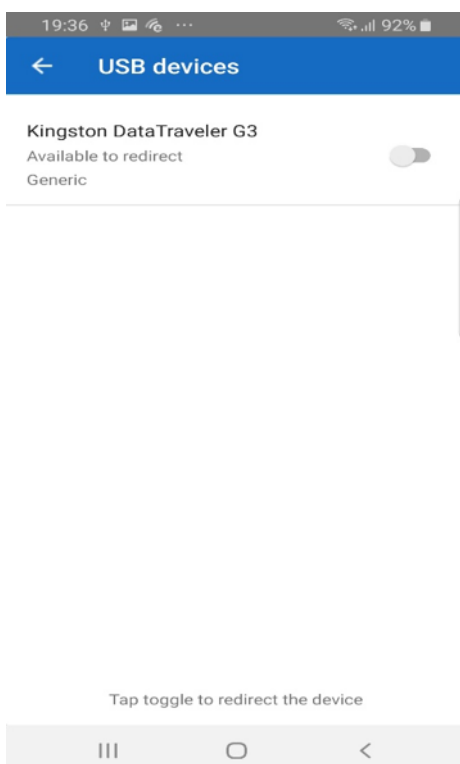
Según el dispositivo USB redirigido y la latencia de la red, puede que el dispositivo tarde un tiempo en aparecer en el Explorador de Windows.

**Configurar la redirección USB en teléfonos móviles, tabletas y Samsung DeX**

1. Agregue un almacén habilitado para directivas de redirección USB e inicie una sesión.
2. Haga clic en el icono de la barra de herramientas de la sesión como se muestra en el siguiente cuadro de diálogo:

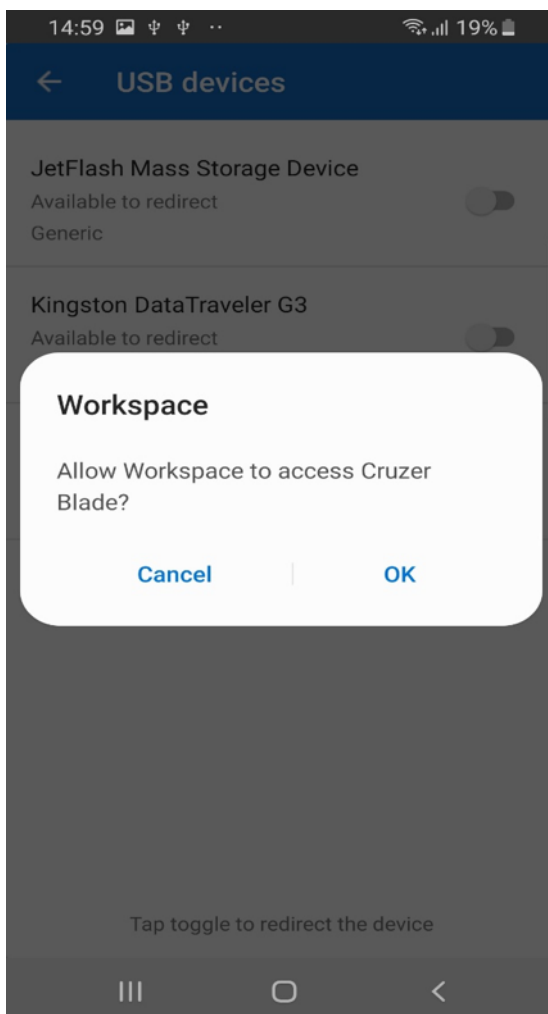


3. Haga clic en el **icono USB** de la barra de herramientas de la sesión.
4. Los dispositivos USB conectados aparecen en la ventana de dispositivos USB como se muestra a continuación:



5. Para redirigir un dispositivo USB concreto, haga clic en la opción Alternar situada junto al dispositivo en cuestión.

Aparecerá un cuadro de diálogo de permisos de Workspace.

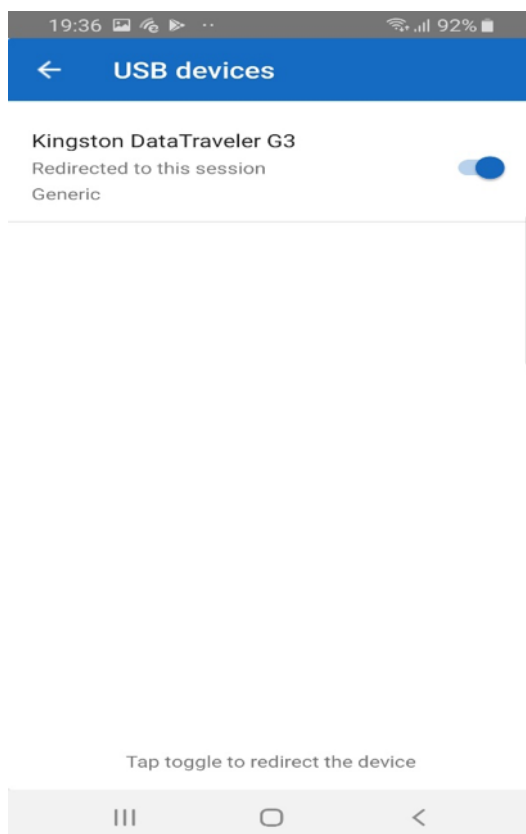


6. Haga clic en **Aceptar** para conceder permiso a que la aplicación Citrix Workspace redirija el dispositivo.

**Nota:**

Este paso es obligatorio para redirigir el dispositivo USB.

El dispositivo USB se redirige y el estado se muestra de la siguiente manera:



### Configurar la función de redirección USB en Chromebooks

1. Agregue un almacén habilitado para directivas de redirección USB e inicie una sesión.
2. Haga clic en **Aceptar** para conceder permiso a que la aplicación Citrix Workspace redirija el dispositivo.

**Nota:**

La concesión de permisos es un paso obligatorio y el mensaje solo aparece en una instalación nueva.

## Confirm USB Permission



Allow "Workspace" to access:  
Mass Storage Device from JetFlash (serial number  
17PWOCRFC077FA2S)

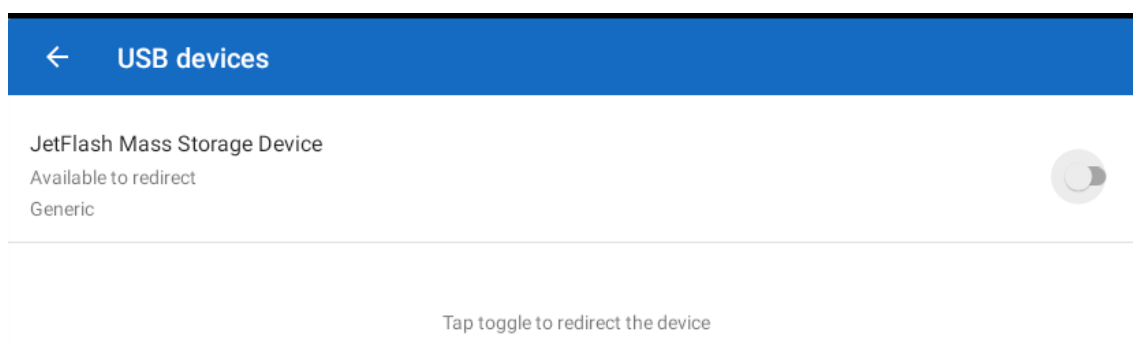
OK

Cancel

3. Conecte el dispositivo USB.
4. Haga clic en el icono de la barra de herramientas y, a continuación, en el icono USB de la barra de herramientas de la sesión.



Los dispositivos USB conectados se indican de la siguiente manera:



### Nota:

Si un dispositivo USB no aparece en la lista, compruebe que lo ha incluido en la lista blanca.

Para obtener información sobre cómo incluir en la lista de dispositivos USB permitidos en un Chromebook, consulte el artículo [CTX200825](#) del Knowledge Center.

5. Para redirigir el dispositivo USB, haga clic en la opción **Alternar** del dispositivo que quiere redirigir.
6. Haga clic en **Aceptar** para conceder permiso a que la aplicación Citrix Workspace redirija el dispositivo.

## Confirm USB Permission



Allow "Workspace" to access:  
Mass Storage Device from JetFlash (serial number  
17PWOCRFC077FA2S)

OK

Cancel

---

Se redirige el dispositivo USB y se actualiza el estado. Cierre el cuadro de diálogo para seguir utilizando el dispositivo USB redirigido.

**Nota:**

- Si se redirige una unidad USB, aparecerá como aparece en una sesión.
- Si se redirige una impresora o un escáner, se muestra en la sección **Dispositivos** del panel de control.

### Dispositivos USB probados

Dispositivo	Fabricante	Modelo
Impresora	HP	LaserJet P2014
Escáner	HP	Scanjet G3010
Escáner	Canon	CanoScan LiDE 700F
SpaceNavigator	3Dconnexion	
Impresora	Brother	QL-580N
Escáner	HP	Scanjet 200

### Problemas conocidos:

- No se admite más de un dispositivo USB a la vez.
- Por ahora, los dispositivos USB de audio y vídeo no son compatibles.

### 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.
- Para consultar la lista de Workspace Hubs disponibles, toque **Ver lista de hubs** desde el cuadro de diálogo de **Workspace Hub**.

### Configuración de Citrix Casting

Citrix Casting se habilita cuando se cumplen todos estos requisitos del sistema:

- 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 **Parámetros** y **Citrix Casting** en su dispositivo.

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

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

### Integración de Content Collaboration Service

Citrix Content Collaboration (anteriormente ShareFile) permite intercambiar documentos de forma fácil y segura, enviar documentos grandes por correo electrónico y manejar de forma segura transferencias de documentos a terceros. Existen muchas maneras de trabajar con Citrix Content Collaboration, incluida una interfaz web, clientes móviles, aplicaciones de escritorio e integración con Microsoft Outlook y Gmail.

Puede acceder a Citrix Content Collaboration desde la ficha **Archivos** de la aplicación Citrix Workspace. La ficha **Archivos** solo se ve si Content Collaboration está habilitado en la consola de Citrix Cloud. Para obtener información, consulte [Crear una cuenta de Content Collaboration \(ShareFile\) o vincularla a Citrix Cloud](#).

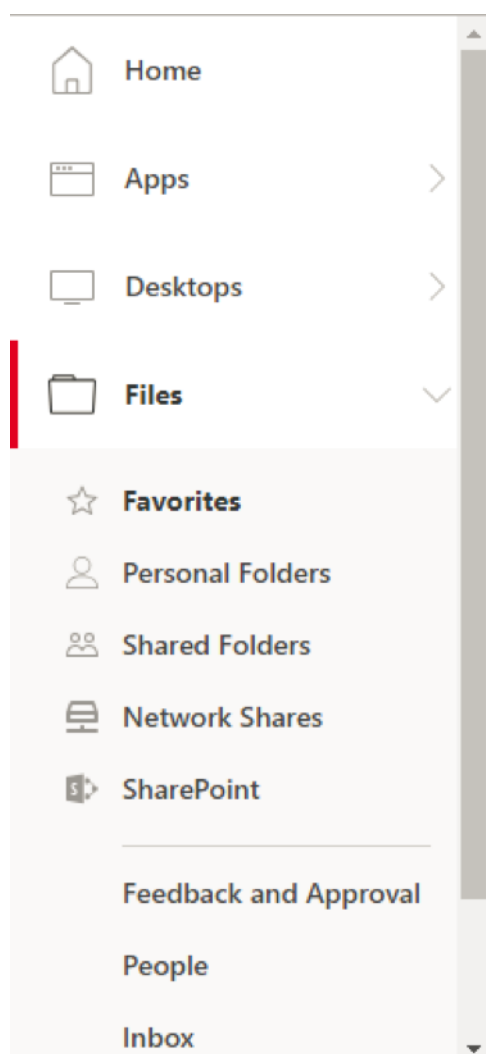
**Nota:**

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

La imagen siguiente muestra contenido de ejemplo de la ficha **Archivos** de la aplicación Citrix Workspace:



### Sincronización de la distribución de teclado

La aplicación Citrix Workspace 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**.

**Nota:**

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

**Limitaciones:**

- Esta función 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 es compatible, 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).

## **Tarjeta inteligente USB**

La aplicación Citrix Workspace admite el uso de lectores de tarjetas inteligentes USB con 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.
- Compatibilidad con 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 admite los siguientes tipos de tarjetas inteligentes USB:

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

La tarjeta inteligente USB se admite en el sistema operativo Android, de la versión 6.0 (Marshmallow) a la versión 7.12 (Nougat). Las versiones 8.0 (Oreo) y 9.0 (Pie) del sistema operativo Android no son compatibles. Esta es una limitación de terceros.

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

### Configurar 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 **Agregar cuenta**. Toque la opción **Usar tarjeta inteligente**.
  4. Para modificar una cuenta existente para usar la autenticación con tarjeta inteligente USB, toque **Cuentas > Modificar**, y toque la opción **Usar tarjeta inteligente**.

### Asociación de tipos de archivos

Como requisito previo para que funcione esta función, 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 o FTA) en una sesión, asegúrese de que los usuarios se conecten al servidor del almacén 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 mediante la aplicación Citrix Workspace para Android (al aplicar la asociación de tipos de archivo configurada por el administrador) o una aplicación diferente. En función de lo que haya seleccionado, puede haber o no una aplicación predeterminada. Puede cambiar la aplicación predeterminada mediante la opción para cambiar el valor predeterminado.

**Nota:**

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

### 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 mediante 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.

### Habilitar el acceso a archivos en Google Drive:

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 explorador 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 quiere abrir. Toque **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 se admite en las comunidades.
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. Esta 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.

### Programa para la mejora de la experiencia del usuario (CEIP)

Datos recopilados	Descripción	Para qué se utiliza
Datos de uso y configuración	El programa para la mejora de la experiencia del usuario de Citrix (Customer Experience Improvement Program o CEIP) recopila información de uso y configuración de la aplicación Citrix Workspace y envía esos datos automáticamente a Google Analytics para Firebase.	Esos datos ayudan a Citrix a mejorar la calidad, la fiabilidad y el rendimiento de la aplicación Citrix Workspace.

### Información adicional

Citrix gestionará sus datos de acuerdo con los términos de su contrato con Citrix y los protegerá como se especifica en el [anexo de seguridad de Citrix Services](#), disponible en el [Centro de confianza de Citrix](#).

Puede inhabilitar el envío de datos de CEIP a Citrix y a Google Analytics para Firebase (excepto los dos elementos de datos recopilados para Google Analytics para Firebase que se indican mediante un \* en la tabla que hay a continuación):

1. Inicie la aplicación Citrix Workspace y seleccione **Parámetros**.
2. Seleccione **Preferencias avanzadas**.  
Aparecerá la ventana **Preferencias avanzadas**.
3. Desmarque la opción **Enviar estadísticas de uso**.

Elementos concretos de datos CEIP recopilados por Google Analytics para Firebase:

Versión del sistema operativo*	Versión de la aplicación Workspace*	Configuración de la autenticación	Información de dispositivos
Método de inicio de sesiones	Tipo de almacén de Citrix	Configuración de la asignación de unidades del cliente	
Información de la sesión	Uso de <a href="#">Recieverconfig.txt</a>	Configuración de la redirección USB	Información de usuario de HDX RTME
Configuración de las conexiones HTTP y HTTPS	Información del protocolo de conexiones ICA	Acción de revisión de la aplicación Workspace	Inhabilitar la configuración de Firebase
Cantidad de almacenes agregados	Acción de captura de pantalla	Acciones de usuario de la función RSA	Cantidad de usuarios de StoreFront y de la aplicación Workspace
Acción de actualización de aplicaciones	Actualización del sistema operativo	Acción de visualización de pantalla	Eliminación de aplicaciones
Conexiones de vista web	Borrado de datos de aplicación	Ejecución de aplicaciones	Inicio de sesión de la aplicación

## Autenticarse

August 17, 2020

### RSA SecurID

#### Nota:

La aplicación Citrix Workspace ha pospuesto la funcionalidad del **modo de token siguiente** por una dependencia de terceros. Actualizaremos esta descripción en cuanto dispongamos de información al respecto.

Si esta función está habilitada, al introducir la contraseña incorrecta tres veces, Citrix Gateway plug-in solicita que se espere hasta que se active el próximo token antes de iniciar una sesión. Asimismo, el servidor RSA puede inhabilitar una cuenta de usuario si el usuario intenta iniciar una sesión demasiadas veces con la contraseña incorrecta.

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

#### 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 de nombre de archivo `.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 del sitio web y del 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 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 `.sd?id` con la aplicación Citrix Workspace, cambie la extensión de nombre de archivo por XML e impórtelo.

## SDK y API

July 21, 2020

### Citrix Virtual Channel SDK

El Citrix Virtual Channel Software Development Kit (SDK) admite 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 permite la escritura de canales virtuales nuevos en la aplicación Citrix Workspace para Android. Si quiere 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

© 2021 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).