



# Aplicación Citrix Workspace para Linux

## **Contents**

<b>Acerca de esta versión</b>	<b>3</b>
<b>Requisitos previos para instalar la aplicación Citrix Workspace</b>	<b>24</b>
<b>Instalación, desinstalación y actualización</b>	<b>33</b>
<b>Introducción</b>	<b>41</b>
<b>Configuración</b>	<b>49</b>
<b>Autenticarse</b>	<b>112</b>
<b>Protección</b>	<b>114</b>
<b>Storebrowse</b>	<b>121</b>
<b>Solución de problemas</b>	<b>131</b>
<b>SDK y API</b>	<b>150</b>

## Acerca de esta versión

July 30, 2021

### Novedades en la versión 2106

#### Chromium Embedded Framework (CEF) para la redirección de contenido del explorador web

La redirección de contenido del explorador web basada en CEF ya es totalmente funcional. Esta función está activada de forma predeterminada.

**Nota:**

Esta función no está disponible en la plataforma armhf.

Para obtener más información, consulte [Habilitar la redirección de contenido del explorador web basada en CEF](#).

#### 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 aparece en los agentes VDA de servidor.

Para obtener más información, consulte [Indicador de estado de la batería](#).

#### Continuidad del servicio (versión Technical Preview pública)

**Nota:**

Esta función se halla actualmente en versión Technical Preview pública para la aplicación Citrix Workspace.

La continuidad del servicio elimina o minimiza la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Los usuarios pueden iniciar sus aplicaciones y escritorios virtuales, independientemente del estado de los servicios en la nube.

Para obtener información sobre los requisitos que permiten la continuidad del servicio en la aplicación Citrix Workspace, consulte [Requisitos del sistema](#).

Para obtener información sobre la instalación de la continuidad del servicio con la aplicación Citrix Workspace, consulte [Instalar Continuidad del servicio](#).

Para obtener más información, consulte la sección [Continuidad del servicio](#) de la documentación de Citrix Workspace.

### Mejora en la protección de aplicaciones **Función experimental**

Antes, el administrador de autenticación y los cuadros de diálogo de Self-Service Plug-in no estaban protegidos incluso tras instalar y habilitar la protección de aplicaciones.

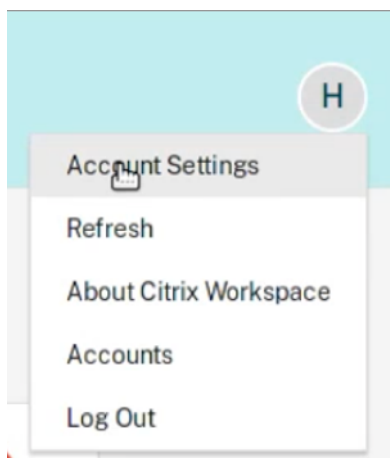
A partir de esta versión, la aplicación Citrix Workspace presenta una opción que le permite configurar las funciones de protección contra el registro de tecleo y protección contra capturas de pantalla por separado para las interfaces del administrador de autenticación y del Self-Service Plug-in.

Para obtener más información, consulte [Protección de aplicaciones](#).

### Mejora de la interfaz de usuario

Antes, el menú de parámetros estaba disponible en la opción **Preferencias** de Desktop Viewer.

A partir de esta versión, el menú de parámetros aparece al lado de Self-Service Plug-in. Las opciones de menú se han mejorado para alinearse con la apariencia de la versión nativa de Citrix Workspace. Esto ofrece una experiencia de usuario más fluida.



#### Nota:

Esta mejora está disponible de forma predeterminada en la versión 2106 de la aplicación Citrix Workspace en implementaciones en la nube.

Para volver a la apariencia nativa y antigua, haga lo siguiente:

Vaya a `$(ICAROOT)/config/AuthManConfig.xml` y establezca el valor de `WebUISettings` en **false**

## Mejora para Microsoft Teams

Ahora puede configurar la interfaz de red preferida para el tráfico multimedia.

Vaya a `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` y cree una clave con el nombre `NetworkPreference` (REG\_DWORD).

Seleccione uno de estos valores según corresponda:

- 1: Ethernet
- 2: Wi-Fi
- 3: Móvil
- 4: VPN
- 5: Bucle invertido
- 6: Cualquiera

De forma predeterminada, el motor de medios WebRTC elige la mejor ruta disponible.

## Novedades en la versión 2104

### Protección de aplicaciones en Red Hat Package Manager (RPM) **Función experimental**

Ahora, la función Protección de aplicaciones está disponible en la versión RPM de la aplicación Citrix Workspace.

Para obtener más información, consulte [Protección de aplicaciones](#).

### Mejora del protocolo HDX Enlightened Data Transport (EDT)

En versiones anteriores, al establecer `HDXoverUDP` en `Preferred`, el transporte de datos por EDT se utiliza como transporte principal, y TCP queda como opción de emergencia.

Con la fiabilidad de la sesión habilitada, EDT y TCP se intentan en paralelo durante la conexión inicial, la reconexión de fiabilidad de la sesión y la reconexión automática de clientes. Esta mejora reduce el tiempo de conexión cuando se prefiere EDT, pero el transporte UDP subyacente necesario no está disponible y hay que recurrir a TCP.

De forma predeterminada, después de recurrir a TCP, el transporte adaptable vuelve a intentar utilizar EDT cada cinco minutos.

### Optimización de Microsoft Teams

Con esta versión, la función de eliminación de eco está inhabilitada de forma predeterminada. Le recomendamos no usar los altavoces y el micrófono integrados para las llamadas. Utilice unos auriculares en su lugar.

Esta corrección tiene como objetivo resolver problemas de audio entrecortado detectados en clientes ligeros.

### Continuidad del servicio (Technical Preview)

**Nota:**

Esta función se halla actualmente en Technical Preview. Citrix recomienda utilizar esta función solo en entornos que no sean de producción. Para registrarse, utilice este formulario Podio: [Sign up: Service Continuity Tech Preview for Citrix Workspace](#).

La continuidad del servicio elimina o minimiza la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Los usuarios pueden iniciar sus aplicaciones y escritorios virtuales, independientemente del estado de los servicios en la nube.

Para obtener más información, consulte la sección [Continuidad del servicio](#) de la documentación de Citrix Workspace.

### Novedades en la versión 2103

#### Anclar el diseño de pantalla con varios monitores

Con esta versión, puede guardar la selección del diseño de pantalla con varios monitores. El diseño es la manera en que se muestra una sesión de escritorio. Anclarlo ayuda a reiniciar una sesión con el diseño seleccionado, lo que ofrece una mejor experiencia de usuario.

Como requisito previo, debe habilitar esta función en el archivo `AuthManConfig.xml`. Vaya a `$/ICAROOT/config/AuthManConfig.xml` y agregue estas entradas para habilitar la función de anclaje de diseño de pantalla:

```
1 <key>ScreenPinEnabled</key>
2 <value> true </value>
```

Solo después de agregar la clave anterior, podrá ver la opción **Diseño de pantalla** en el **indicador de aplicaciones**.

**Nota:**

Esta función no está disponible en el inicio web de la aplicación Citrix Workspace.

Para obtener más información, consulte [Anclar el diseño de pantalla con varios monitores](#).

#### Aumento de la cantidad de canales virtuales admitidos

En versiones anteriores del cliente, las sesiones admitían hasta 32 canales virtuales.

Con esta versión, puede utilizar hasta 64 canales virtuales en una sesión.

### Mejoras de Microsoft Teams

Ahora el códec de vídeo VP9 está inhabilitado de forma predeterminada.

### Novedades en la versión 2101

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

Con esta versión, el acceso a las unidades asignadas viene con una función de seguridad adicional.

Ahora, puede seleccionar el nivel de acceso a la unidad asignada desde cada almacén de la sesión.

Para evitar que aparezca el cuadro de diálogo de nivel de acceso cada vez, seleccione la opción **No volver a preguntarme**. La configuración se aplica a ese almacén concreto.

Si decide no seleccionar la opción, puede establecer los niveles de acceso cada vez que se inicie una sesión.

#### Protección de aplicaciones en paquetes Debian **Función experimental**

Ahora, la función Protección de aplicaciones está disponible en la versión Debian de la aplicación Citrix Workspace.

Para una instalación silenciosa del componente de protección de aplicaciones, ejecute el siguiente comando desde el terminal antes de instalar la aplicación Citrix Workspace:

```
1 export DEBIAN_FRONTEND="noninteractive"
2 sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select no"
3 sudo debconf-show icaclient
4 * app_protection/install_app_protection: no
5 sudo apt install -f ./icaclient_<version>._amd64.deb
```

### Mejoras de Microsoft Teams

- Ahora el instalador de la aplicación Citrix Workspace incluye tonos de llamada de Microsoft Teams.
- La salida de audio cambia automáticamente a los dispositivos de audio recién conectados y se establece un volumen de audio adecuado.
- El proxy HTTP está disponible para la autenticación anónima.

## Novedades en la versión 2012

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

Anteriormente, la configuración del acceso a archivos a través de CDM se aplicaba a todos los almacenes configurados.

A partir de esta versión, la aplicación Citrix Workspace le permite configurar el acceso a archivos CDM por almacén.

#### Nota:

La configuración de acceso a archivos no es persistente en todas las sesiones cuando se utiliza Workspace para Web. De forma predeterminada, se utiliza la opción **Preguntarme cada vez**.

Para obtener más información, consulte [Asignación de unidades de cliente](#).

### Protección de aplicaciones **Función experimental**

#### Nota:

- Esta función solo está disponible cuando la aplicación Citrix Workspace se instala mediante el paquete tarball. Además, x64 y armhf son los únicos dos paquetes que se admiten.
- Esta función solo está disponible en implementaciones locales de Citrix Virtual Apps and Desktops.

La protección de aplicaciones es una función adicional que proporciona una mayor seguridad al usar Citrix Virtual Apps and Desktops. La función restringe la posibilidad de que los clientes puedan verse amenazados por malware de registro de pulsaciones de teclas y malware de capturas de pantalla. La protección de aplicaciones evita la exfiltración de información confidencial, como credenciales de usuario e información confidencial mostrada en la pantalla. La función evita que los usuarios y los atacantes hagan capturas de pantalla y usen registradores de pulsaciones de teclas para obtener y explotar información confidencial.

Para obtener información sobre cómo configurar la protección de aplicaciones en Citrix Virtual Apps and Desktops, consulte la sección [Protección de aplicaciones](#) de la documentación de Citrix Virtual Apps and Desktops.

Para obtener más información sobre la protección de aplicaciones en la aplicación Citrix Workspace, consulte [Protección de aplicaciones](#).

### Mejora en la autenticación **Función experimental**

Ahora presentamos el cuadro de diálogo de autenticación dentro de la aplicación Citrix Workspace y mostramos los detalles del almacén en la pantalla de inicio de sesión para ofrecer una mejor experi-



encia de usuario. Ciframos y almacenamos tokens de autenticación para que no tenga que volver a introducir credenciales cuando se reinicie el sistema o la sesión.

**Nota:**

- Esta mejora de la autenticación solo se aplica en implementaciones en la nube.
- Esta mejora de la autenticación no está disponible en la plataforma armhf.

**Requisito previo:**

Debe instalar la biblioteca libsecret.

Esta función está inhabilitada de forma predeterminada.

Para obtener más información, consulte [Autenticarse](#).

**Mejora de la configuración de audio**

A partir de esta versión, el valor predeterminado del atributo `VdcamVersion4Support` en el archivo `module.ini` es `True`.

Para obtener más información, consulte [Sonido](#).

**Novedades en la versión 2010**

**Redirección de sonido mejorada**

Antes solo se asignaba el dispositivo de audio predeterminado en una sesión aunque hubiera muchos dispositivos disponibles en la máquina. Por regla general, el dispositivo asignado aparecía como **Citrix HDX Audio**.

Con esta versión, la aplicación Citrix Workspace para Linux muestra todos los dispositivos de audio locales que hay disponibles en una sesión. En lugar de **Citrix HDX Audio**, ahora aparecen con sus respectivos nombres de dispositivo. Puede cambiar a cualquiera de los dispositivos disponibles de forma dinámica en una sesión. A diferencia de las versiones anteriores, ahora no es necesario seleccionar el dispositivo de audio predeterminado antes de iniciar la sesión. Las sesiones se actualizan dinámicamente al conectar o quitar dispositivos de audio.

Para obtener más información, consulte [Sonido](#).

Además, esta versión soluciona problemas para mejorar la función ICA multisequencia.

**Novedades en la versión 2009**

**Mejora del registro**

Anteriormente, los archivos `debug.ini` y `module.ini` se utilizaban para configurar la captura de registros.

A partir de la versión 2009, puede configurar los registros mediante uno de los métodos siguientes:

- Interfaz de la línea de comandos
- Interfaz gráfica de usuario (GUI)

También a partir de la versión 2009, se elimina el archivo de configuración `debug.ini` del instalador de la aplicación Citrix Workspace.

Los registros capturan los detalles de la implementación, los cambios de configuración y las actividades administrativas de la aplicación Citrix Workspace en una base de datos de registros. Un desarrollador externo puede usar el SDK de la captura de registros, que se incluye como parte del SDK de optimización de plataformas de la aplicación Citrix Workspace.

Puede utilizar la información de registro para:

- Diagnosticar y solucionar problemas técnicos que se produzcan después de cualquier cambio. El registro proporciona un rastro de los pasos seguidos.
- Ayudar en la administración de cambios y en el seguimiento de las configuraciones.
- Realizar informes sobre las actividades administrativas.

**Nota:**

Este mecanismo de registros solo se aplica en la versión comercial.

Para obtener más información acerca de los registros, consulte [Captura de registros](#).

### **Novedades en la versión 2006**

#### **Optimización para Microsoft Teams**

Optimización para Microsoft Teams de escritorio mediante Citrix Virtual Apps and Desktops y la aplicación Citrix Workspace. La optimización para Microsoft Teams es similar a HDX RealTime Optimization para Microsoft Skype Empresarial. La diferencia es que agrupamos todos los componentes necesarios para la optimización de Microsoft Teams en el VDA y en la aplicación Citrix Workspace.

La aplicación Citrix Workspace para Linux ofrece funciones de audio, vídeo y uso compartido de la pantalla con la optimización de Microsoft Teams.

**Nota:**

La optimización de Microsoft Teams solo se ofrece en distribuciones x64 de Linux.

Para obtener información sobre cómo habilitar los registros, siga los pasos indicados en [Registros en Microsoft Teams](#).

Para obtener información sobre los requisitos del sistema, consulte [Optimización de Microsoft Teams](#).

Para obtener más información, consulte [Optimización para Microsoft Teams](#) y [Redirección de Microsoft Teams](#).

### **Canal virtual NetScaler App Experience (NSAP) disponible**

Anteriormente disponible como una función experimental, ahora la función de canal virtual NetScaler App Experience (NSAP) es una funcionalidad completa. El canal virtual NSAP ayuda a obtener datos HDX Insight, lo que mejora la escalabilidad y el rendimiento. De forma predeterminada, el canal virtual NSAP está habilitado. Para inhabilitarlo, cambie el indicador NSAP `NSAP=Off` en el archivo `module.ini`.

Para obtener más información, consulte [HDX Insight](#) en la documentación de Linux Virtual Delivery Agent y [HDX Insight](#) en la documentación del servicio Citrix Application Delivery Management.

### **Actualización en Citrix Analytics Service**

La aplicación Citrix Workspace está diseñada para transmitir datos a Citrix Analytics Service desde sesiones ICA que se inician desde un explorador web.

Para obtener más información sobre cómo utiliza esta información Citrix Analytics, consulte [Autoservicio para el rendimiento](#) y [Búsqueda de autoservicio para Virtual Apps and Desktops](#).

### **Actualización de la versión de TLS**

Antes, la versión mínima de TLS admitida era 1.0, y la versión máxima de TLS admitida era 1.2.

A partir de esta versión, la versión mínima y la versión máxima de TLS que se admiten son 1.2. Para configurar un valor diferente de `MinimumTLS`, consulte [TLS](#).

### **Actualización de CryptoKit**

La versión 14.2 de CryptoKit está integrada en la versión 1.1.1d de OpenSSL.

### **Novedades en la versión 2004**

#### **Idiomas disponibles**

Ahora la aplicación Citrix Workspace para Linux está disponible en italiano.

#### **Rendimiento mejorado de enumeración e inicio de sesión**

Con esta versión, los usuarios de la nube notarán tiempos de inicio de sesión más cortos y tiempos de enumeración de aplicaciones más cortos.

### **Optimización de audio para Microsoft Teams: [Función experimental](#)**

Como función experimental, la aplicación Citrix Workspace ofrece la optimización de audio para Microsoft Teams que se ejecuta dentro de una sesión de Citrix Virtual Desktops.

**Nota:**

La optimización del audio de Microsoft Teams solo se ofrece en las distribuciones x64 de Linux.

Para obtener más información, consulte las secciones [Optimización para Microsoft Teams](#) y [Redirección de Microsoft Teams](#) de la documentación de Citrix Virtual Apps and Desktops.

### **Canal virtual NetScaler App Experience (NSAP) disponible [Función experimental](#)**

Como función experimental, los datos de HDX Insight se obtienen del canal virtual NSAP y se envían sin comprimir, lo que mejora la escalabilidad y el rendimiento. De forma predeterminada, el canal virtual NSAP está habilitado. Para inhabilitarlo, cambie el indicador NSAP `NSAP=Off` en el archivo `module.ini`.

Para obtener más información, consulte [HDX Insight](#) en la documentación de Linux Virtual Delivery Agent y [HDX Insight](#) en la documentación del servicio Citrix Application Delivery Management.

## **Novedades en la versión 1912**

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

En la versión 1910 se introdujo la función de interfaz de usuario transparente (transparent user interface o TUI), incluido el indicador **VDTUI**. Esta función ayuda al sistema cliente a recibir los paquetes TUI enviados por el servidor, y el cliente puede acceder a los componentes relacionados con la IU. Sin embargo, con el indicador **desactivado**, el cuadro de diálogo "Iniciando" se muestra en la parte superior de otras ventanas de la aplicación, con lo que oculta la solicitud de inicio de sesión.

Ahora, el indicador **VDTUI**, ubicado en el archivo `module.ini`, está **activado** de forma predeterminada. Por eso, el cuadro de diálogo "Iniciando" ya no aparece al iniciar una aplicación. En su lugar, aparece el cuadro de diálogo "Conectando" con una barra de progreso. El cuadro de diálogo también muestra el progreso del inicio de la aplicación.

### **GStreamer 1.x: [Función experimental](#)**

En versiones anteriores, GStreamer 0.10 era la versión predeterminada disponible para la redirección multimedia. A partir de esta versión, puede configurar GStreamer 1.x como la versión predeterminada.

#### **Limitaciones:**

- Al reproducir un vídeo, es posible que las opciones de rebobinar hacia delante y hacia atrás no funcionen según lo previsto.

- Al iniciar la aplicación Citrix Workspace en dispositivos armhf, es posible que GStreamer 1.x no funcione según lo previsto.

Para obtener más información, consulte [Habilitar GStreamer 1.x](#).

### **Chromium Embedded Framework (CEF) para la redirección de contenido del explorador web (Browser Content Redirection o BCR): Función experimental**

La función BCR redirige el contenido de un explorador web a un dispositivo cliente. La función crea un explorador correspondiente que se inserta en la aplicación Citrix Workspace.

Anteriormente, la función BCR usaba una superposición de [WebKitGTK+](#) para representar el contenido. A partir de esta versión, la función BCR utiliza una superposición basada en CEF para una mejor experiencia de usuario. Reduce la carga de red, el procesamiento de páginas y la generación de gráficos para el dispositivo de punto final.

Para obtener más información, consulte [Habilitar la redirección de contenido de explorador web basada en CEF](#).

Para obtener información sobre la redirección de contenido de explorador web, consulte [Redirección de contenido de explorador web](#) en la documentación de Citrix Virtual Apps and Desktops.

#### **Notas:**

- El binario **pacexec** se ha eliminado de la versión x86 de la aplicación Citrix Workspace.
- Es posible que Citrix Files no sea compatible con la función “Workspace with Intelligence”.

## **Novedades en la versión 1910**

### **Idiomas disponibles**

Ahora la aplicación Citrix Workspace para Linux está disponible en portugués de Brasil.

### **Icono del indicador de aplicaciones**

El indicador de aplicaciones se inicia cuando se abre la aplicación Citrix Workspace. Es un icono que está presente en el área de notificaciones. Con la introducción del indicador de aplicaciones, mejora el rendimiento del inicio de sesión de la aplicación Citrix Workspace para Linux.

Puede constatar la mejora del rendimiento en estos casos:

- Primer inicio de la aplicación Citrix Workspace
- Cerrar la aplicación y volver a iniciarla
- Salir de la aplicación y volver a iniciarla

### Nota:

El paquete `libappindicator` es necesario para que el indicador de aplicaciones aparezca. Instale desde la web el paquete `libappindicator` adecuado para su distribución de Linux.

### Interfaz de usuario transparente

El protocolo ICA de Citrix utiliza el protocolo de canal virtual [TUI VC] para interfaces de usuario transparentes con el objetivo de transmitir datos entre servidores de Citrix Virtual Apps and Desktops y servidores host. El protocolo TUI transmite mensajes de componentes de interfaz de usuario [IU] para conexiones remotas.

Anteriormente, la aplicación Citrix Workspace para Linux no era compatible con la función TUI VC. Como resultado, el sistema cliente no podía gestionar de manera eficiente los datos de componentes de IU procedentes del servidor. Por lo tanto, cuando se intentaba iniciar una aplicación, el cuadro de diálogo “Iniciando ” se mostraba encima de otras aplicaciones.

Ahora, la aplicación Citrix Workspace para Linux admite la función TUI VC. Esta función ayuda al cliente a recibir los paquetes TUI enviados por el servidor, y el cliente puede acceder a los componentes relacionados con la IU. Esta funcionalidad le ayuda a controlar la visualización de la pantalla superpuesta predeterminada. Puede activar y desactivar el indicador `VDTUI` en el archivo `module.ini`: `VDTUI - On/Off`

Para obtener más información sobre los canales virtuales, consulte [Canales virtuales ICA de Citrix](#) en la documentación de Citrix Virtual Apps and Desktops.

### Problemas resueltos

#### Problemas resueltos en la versión 2106

- Al utilizar la aplicación Citrix Workspace 1912 para Linux, es posible que la redirección del portapapeles falle, con lo que la sesión deja de responder. El problema se produce al copiar y pegar una gran cantidad de datos. [CVADHELP-16210]
- Es posible que las videollamadas de Microsoft Teams no optimizadas no tengan audio. El audio no se puede recuperar hasta que haya desconectado y haya vuelto a conectar la sesión. [CVADHELP-16846]
- Es posible que no se puedan descargar archivos alojados en un recurso de red local. [CVADHELP-17337]
- Es posible que las sesiones iniciadas en dispositivos de punto final Linux fallen. El problema se produce cuando la directiva Multisequencia está habilitada. [RFLNX-6960]
- Al utilizar la versión 1.15.1 de GStreamer, es posible que la redirección de cámaras web falle y que la sesión se desconecte. [HDX-30550]

## Problemas resueltos en versiones anteriores

### Problemas resueltos en la versión 2104

- Al utilizar la redirección de contenido del explorador web, el enfoque del teclado no regresa a la ventana principal incluso después de buscar contenido en la barra de búsqueda de YouTube. [RFLNX-5349]
- Al compartir una pantalla en Microsoft Teams durante una llamada entre dos usuarios, es posible que el audio se oiga distorsionado. El problema se produce con los clientes ligeros Dell Wyse 5070 y 5470. [RFLNX-6537]
- Al utilizar Microsoft Teams en la aplicación Citrix Workspace para Linux, es posible que algunas llamadas se desconecten de manera inesperada. [RFLNX-6719]
- En esta versión se resolvieron una serie de problemas para mejorar la estabilidad y el rendimiento generales. [RFLNX-7006]
- Al utilizar Chromium Embedded Framework, es posible que la redirección de contenido del explorador web provoque una alta utilización de la CPU. [RFLNX-7217]
- Al cambiar entre aplicaciones publicadas y locales, es posible que la ventana de la aplicación publicada no escale correctamente en el modo de pantalla completa. [CVADHELP-14812]
- Al abrir Microsoft Excel a través de la aplicación Citrix Workspace para Linux e ir a **Datos > Nueva consulta**, es posible que el menú emergente **Configuración de origen de datos** no se abra como se esperaba. [CVADHELP-16509]
- Es posible que las versiones 2101 y 2102 de la aplicación Citrix Workspace para Linux muestren una dirección IP de cliente no válida en Citrix Director. [CVADHELP-16923]
- Es posible que el nombre del dispositivo de audio no se pueda leer. El problema se produce en los sistemas operativos en chino. [CVADHELP-17290]

### Problemas resueltos en la versión 2103

- Es posible que, al intentar realizar una videollamada no optimizada, se pierda audio. El audio no se puede recuperar hasta que haya desconectado y haya vuelto a conectar la sesión. [CVADHELP-16846]
- Esta corrección establece el valor predeterminado de AudioLatencyControlEnabled en True, lo que reduce la latencia de audio. [RFLNX-6620]
- Es posible que la función de uso compartido de la pantalla en Microsoft Teams falle en el modo integrado. [RFLNX-6659]

### Problemas resueltos en la versión 2101

- Cuando se utiliza un proxy personalizado, puede aparecer un mensaje de autenticación adicional. El problema se debe a Chromium Embedded Framework (CEF) que utiliza el explorador

web para redirigir el contenido. Como solución temporal, configure el agente para omitir el mensaje adicional. [CVADHELP-14804]

- Al intentar volver a conectarse a una sesión, es posible que la sesión deje de responder. El problema se produce con las sesiones habilitadas para tarjetas inteligentes. Como solución temporal, vuelva a insertar la tarjeta inteligente. [CVADHELP-15028]
- Con Microsoft Teams en modo **Optimizado**, es posible que la reproducción de vídeo deje de responder durante las llamadas de conferencias. El problema se produce cuando un participante cambia de una cámara integrada a una cámara USB. [CVADHELP-16400]
- Con Microsoft Teams en modo **Optimizado**, es posible que el proceso `HdxRtcEngine.exe` se cierre de forma inesperada. [CVADHELP-16504]

### Problemas resueltos en la versión 2012

- Al intentar abrir una página web redirigida mediante la redirección de contenido del explorador web, es posible que la página web deje de responder. El problema se produce al hacer clic en un enlace que se abre en una ventana o ficha nuevas. [RFLNX-5306]
- Al utilizar la redirección de contenido de explorador web basado en CEF, los micrófonos y las cámaras no se redirigen. Para habilitar la redirección, establezca el atributo `CefEnableMediaDevices` en `True` en el archivo `All_Regions.ini`. [RFLNX-5337]
- Al presionar las teclas **Alt+Ctrl**, es posible que se atasquen. El problema se produce cuando la opción Distribución del teclado está establecida en Server Default. [RFLNX-5444]
- Es posible que no se puedan seleccionar las opciones de USB, el protocolo de transferencia de imágenes (PTP) ni el protocolo de transferencia de medios (MTP) en teléfonos Android. Para solucionar este problema con los VDA de Windows y Linux, agregue la siguiente regla de permiso en el archivo `usb.conf`:

```
ALLOW: VID = (vid del dispositivo) disableselectconfig=1
```

[CVADHELP-15304]

- Es posible que Citrix Director indique incorrectamente el número de versión de la aplicación Citrix Workspace como 2009 en lugar de 2010. [RFLNX-5743]
- Puede iniciar correctamente la aplicación Citrix Workspace para Linux en su primer intento, pero es posible que después no pueda. [RFLNX-5971]
- Al intentar agregar un almacén no autenticado (anónimo), es posible que aparezcan dos mensajes de error. El problema se produce con la aplicación Citrix Workspace 2010 para Linux. [RFLNX-5980]

### Problemas resueltos en la versión 2010



- Cuando ejecuta una videollamada o comparte la pantalla en Microsoft Teams, es posible que la pantalla parpadee. [RFLNX-4778]
- No se pueden personalizar los archivos webrpc.log y webrtc.log. [RFLNX-5221]
- Se enumeran los recursos de un almacén incluso después de haberlo eliminado mediante la utilidad Storebrowse. [RFLNX-5499]
- Cuando una configuración regional en alemán o francés está instalada en la máquina, es posible que la optimización de Microsoft Teams no funcione. [RFLNX-5599]
- Cuando se inicia una sesión desde la aplicación Citrix Workspace para Linux, puede que esa sesión parpadee. El problema se produce porque la sesión se desconecta y se vuelve a conectar. El problema se produce principalmente con las aplicaciones de Microsoft. [CVADHELP-14194]
- Al realizar operaciones de Portapapeles (como copiar y pegar contenido entre varias sesiones), puede que las operaciones fallen de forma intermitente. [CVADHELP-15228]
- Cuando se inicia una presentación de diapositivas con Microsoft PowerPoint iniciado a través de la aplicación Citrix Workspace para Linux 1906 o una versión posterior, puede que la presentación no se abra en el modo de pantalla completa. [CVADHELP-15648]
- Es posible que la aplicación Citrix Workspace para Linux no muestre un cuadro de diálogo de autenticación para los almacenes que usan almacenamiento local HTML5. El problema se produce cuando se utiliza la interfaz de usuario de autoservicio. [CVADHELP-15720]

### **Problemas resueltos en la versión 2009**

- A veces, la vista Reunión no se restaura mientras cambia de tareas en Microsoft Teams. El problema se produce cuando una ventana local se superpone a la ventana remota. Como resultado, la ventana remota no recibe los eventos del mouse. Como solución temporal, en la pantalla minimizada, coloque el cursor sobre el reloj digital y haga doble clic en el nombre de la persona que llama. [RFLNX-4937]
- En una sesión que se ejecuta en conexiones UDP, el rendimiento puede ser lento. [RFLNX-5135]
- Cuando arrastra por la pantalla la ventana de una aplicación publicada de terceros integrada, es posible que la ventana se minimice automáticamente. [CVADHELP-13677]
- Un único dispositivo USB redirigido a una sesión que se ejecuta en un dispositivo puede ser redirigido inesperadamente a una sesión entrante que se ejecuta en el mismo dispositivo. [CVADHELP-13684]
- En un entorno de varios monitores, cuando intenta volver a iniciar una sesión de pantalla completa en un monitor, la barra de conexión permanece en otro monitor. El problema se produce incluso cuando el cursor del mouse permanece en el mismo monitor. [CVADHELP-14642]
- Cuando intenta volver a conectarse a una sesión, es posible que la sesión se desconecte inmediatamente después de que aparezca el escritorio. El problema se produce con las sesiones que requieren autenticación con tarjeta inteligente. [CVADHELP-15036]

### **Problemas resueltos en la versión 2006**

- Al utilizar Microsoft Teams, la opción “Llamada de prueba” no aparece. [RFLNX-4234]
- Es posible que no se puedan iniciar sesiones en las distribuciones Red Hat 8.2, CentOS 8.x y Fedora 29, 30 y 31. [RFLNX-3114] [RFLNX-4438] [RFLNX-4296]
- Con los binarios de `wfica_for_plugins` agregados de nuevo al SDK de optimización de plataformas, se eliminó una dependencia innecesaria que se introdujo en LIBS\_GTK. [RFLNX-4604]
- La redirección BCR basada en CEF con obtención del servidor y generación en el cliente falla. Como resultado, la redirección del contenido de explorador web falla. [RFLNX-4459]
- Después de hacer clic en una aplicación publicada en Citrix StoreFront, aparece un cuadro de diálogo de conexión que permanece allí. El problema se produce en el modo no integrado. [CVADHELP-13896]
- Después de seleccionar la opción **Activar** para activar la aplicación Citrix Workspace en el escritorio, se descarga el archivo **receiverconfig.cr**. Es posible que se produzca un error al abrir ese archivo para intentar agregar el almacén a la aplicación Citrix Workspace. [CVADHELP-14389]
- Es posible que no se pueda asignar la aplicación Citrix Workspace para Linux a un puerto serie COM, lo que indica que no se puede contactar con el puerto. El problema se produce cuando las entradas COM anteriores no se rellenan [CVADHELP-14391]
- Es posible que la aplicación Citrix Workspace para Linux no identifique determinadas tarjetas inteligentes. Como resultado, no se pueden iniciar sesiones con dichas tarjetas. [CVADHELP-14878]

### Problemas resueltos en la versión 2004

- Si quita la sección **Preferencias** del archivo **All\_Regions.ini**, se producirá un error en el proceso `wfica`. Como resultado, las sesiones no se podrán conectar. [RFLNX-3965]
- El submenú **Preferencias > Cuentas** no aparece en la ventana de autoservicio después de agregar por primera vez un almacén de nube. [RFLNX-3605]
- Linux Platform Optimization SDK no funciona para las versiones 1908, 1910 y 1912 de la aplicación Citrix Workspace. El problema se produce cuando se quitan los archivos binarios `wfica_for_plugins` del paquete del instalador de la aplicación Citrix Workspace. [RFLNX-4298]
- Cuando agrega un almacén mediante el comando **storebrowse**, el almacén no aparece en la ficha **Preferencias > Cuentas**. El problema se produce cuando la interfaz de usuario de autoservicio se ejecuta en el back-end. [RFLNX-3683]
- En una sesión, `wfica` puede cerrarse inesperadamente en un sitio web con la redirección de contenido del explorador web (BCR) habilitada. El problema se produce si establece el valor de **AllowMultiStream** en **True**. [CVADHELP-13168]
- En una configuración de monitor doble, los intentos de cambiar la visualización del escritorio publicado al modo de pantalla completa pueden fallar cuando los monitores tienen diferentes

resoluciones. [CVADHELP-13990]

- Es posible que haya problemas de visualización en sesiones integradas. El problema se produce cuando se cambia el tamaño de una ventana integrada o se cambia entre ventanas integradas. [CVADHELP-13458]
- Después de iniciar una sesión de escritorio desde un almacén de PNA, es posible que la ventana de la barra de progreso se siga viendo, a menos que la cierre manualmente. [CVADHELP-14405]

### Problemas resueltos en la versión 1912

- En Ubuntu16.04x64, el icono de la aplicación Citrix Workspace podría aparecer incorrectamente en la barra de tareas. [RFLNX-3582]
- Después de cambiar el enlace simbólico [enlace simbólico] de gst-play por gst-play1.0, es posible que los archivos de vídeo MP4 aparezcan sin audio y con una pantalla en negro al fondo. [RFLNX-2429]
- Cuando cambia del modo de salvapantallas al modo de sesión ICA de pantalla completa, puede que el teclado deja de estar en el foco. El problema ocurre en dispositivos ArmHardFloat (armhf) que se ejecutan en el sistema operativo Raspberry Pi. [RFLNX-3553]
- Al utilizar la interfaz de usuario de autoservicio, es posible que las opciones de la ventana **Preferencias** no funcionen como se espera. El problema ocurre cuando el paquete libwebkit1 no está disponible, como es el caso de los clientes de Debian 10 buster. [RFLNX-3596]
- Cuando cualquier otro usuario del sistema (no el primer usuario) intenta iniciar la aplicación Citrix Workspace, es posible que no se abra la interfaz de usuario de autoservicio y aparezca el siguiente mensaje de error:  
“Bind Error - address already in use”.  
[RFLNX-3601]
- En Ubuntu 18.04 y versiones posteriores, cuando usa la interfaz de usuario de autoservicio para iniciar aplicaciones, la aplicación iniciada se denomina “wfica\_seamless” y no después de la aplicación. El problema se produce porque el entorno de escritorio predeterminado es GNOME. [RFLNX-3650]
- Al cerrar sesión y volver a entrar con otra cuenta de usuario, la página Inicio > Favoritos muestra una lista incorrecta de Aplicaciones favoritas. [RFLNX-3458]
- Después de cerrar la interfaz de usuario de autoservicio, aparece el siguiente mensaje de error:  
“free(): double free detected in tcache 2 Aborted”.  
El problema se produce con dispositivos ArmHardFloat (armhf) que se ejecutan en el sistema operativo Raspbian Buster. [RFLNX-3578]

- Cuando la directiva Experiencia unificada está inhabilitada, es posible que las aplicaciones inhabilitadas se enumeren en la aplicación Citrix Workspace para Linux. [CVADHELP-13742]
- No se puede asignar una unidad USB extraíble a un VDA en el cliente CentOS 7.7. [CVADHELP-13422]

### Problemas resueltos en la versión 1910

- La aplicación Citrix Workspace para Linux dependía de libcurl3 para la instalación. Con esta corrección, esta dependencia se ha eliminado para facilitar la instalación. [RFLNX-3487]
- Es posible que la representación de datos H.264 cifrados con el paquete de optimización de la API de presentación para Unix y Video Decode (VDPAU) no funcione como se espera. [RFLNX-2892]
- Al utilizar las versiones 1906 o 1908 de la aplicación Citrix Workspace para Linux, es posible que la página de inicio de sesión no aparezca cuando los usuarios compartidos cierran la sesión de Workspace. En su lugar, aparece la siguiente solicitud de inicio de sesión: Inicie sesión para acceder a su Workspace. [RFLNX-3519]
- Cuando una sesión de escritorio ocupa varios monitores, es posible que la barra de herramientas desaparezca. [RFLNX-3248]

### Problemas conocidos

#### Problemas conocidos en la versión 2106

- En una sesión de escritorio, después de redirigir una página mediante la redirección de contenido del explorador web basado en CEF, es posible que el enfoque del teclado permanezca en la superposición de la redirección (por ejemplo, en la búsqueda de YouTube). El enfoque del teclado no cambia a otras aplicaciones abiertas. El problema se produce solo tras iniciar sesiones con Self-Service Plug-in o StoreBrowse. Como solución temporal, para cambiar el enfoque a otras aplicaciones, haga clic en la barra de herramientas de la sesión y seleccione el botón **Inicio**. [RFLNX-7704]
- En una sesión de escritorio, después de redirigir una página mediante la redirección de contenido del explorador web basado en CEF, el enfoque del teclado cambia a la ubicación actual del mouse. El problema se debe a una limitación externa en el marco CEF de código abierto. [RFLNX-7724]
- Al intentar hacer clic en la superposición de la redirección de contenido del explorador web (por ejemplo, en la búsqueda de YouTube) con otra aplicación en primer plano, la página del explorador no aparece en primer plano. [RFLNX-7730]
- Después de redirigir una página mediante la redirección de contenido del explorador web basado en CEF, al cerrar la página web redirigida, se captura un fallo de segmentación en los registros de errores. [RFLNX-7667]

- Durante las llamadas de audio entre dos usuarios de Microsoft Teams, es posible que el audio no funcione durante los primeros 15 segundos de la llamada. Como solución temporal, en el archivo `module.ini`, establezca el atributo `VdcamVersion4Support` en `False`. [HDX-29526]

## Problemas conocidos en versiones anteriores

### Problemas conocidos en la versión 2104

- En la versión 1912 LTSR CU2 de VDA, es posible que se desconecten sesiones. El problema se produce al habilitar la directiva **Multisequencia** en el Delivery Controller. Como solución temporal, actualice la versión del VDA a la versión 2012 o a una posterior. [RFLNX-6960]

### Problemas conocidos en la versión 2103

- Durante una videollamada o al compartir la pantalla, es posible que Microsoft Teams deje de responder y que la llamada se corte. [CVADHELP-16918]

### Problemas conocidos en la versión 2101

- Al reproducir vídeos largos, el audio se detiene, pero el vídeo continúa reproduciéndose normalmente. El problema se produce cuando se establece `VdcamVersion4Support` en `True`. Como solución temporal, establezca la opción de audio múltiple `VdcamVersion4Support` en `False` para inhabilitarla. [RFLNX-6472]
- Durante las reuniones de Microsoft Teams, es posible que el audio suene entrecortado cuando tiene el micrófono silenciado. El problema se produce en clientes ligeros. [RFLNX-6537]
- A veces, es posible que la aplicación Citrix Workspace no pueda generar vídeos entrantes en Microsoft Teams. [RFLNX-6662]
- Al utilizar el indicador `cefenabledmediadevices` con Microsoft Teams, el micrófono no funciona como es debido. El problema se produce cuando se utiliza la redirección de contenido del explorador web basada en CEF con Microsoft Teams. [RFLNX-6689]

### Problemas conocidos en la versión 2012

- Cuando una sesión se cierra o se desconecta de manera abrupta, es posible que el proceso `HdxRtcEngine.exe` se cierre de manera inesperada. [RFLNX-5885]
- Al intentar introducir texto, el cursor se vuelve de color blanco. El problema se produce en un caso de doble salto al conectarse desde una máquina Linux de punto final. Como solución temporal, consulte los artículos [CTX272423](#) y [CTX131504](#) de Knowledge Center. [CVADHELP-16170]
- Al establecer HDX Optimization para una videollamada de Microsoft Teams, es posible que el vídeo deje de responder y que el audio deje de funcionar. El problema se produce cuando desconecta o vuelve a conectar unos auriculares durante la llamada. [CVADHELP-16186]

### Problemas conocidos en la versión 2010

- No se pueden ver los archivos en la ficha **Archivos**. El problema se produce en implementaciones en la nube. [RFLNX-5596]
- En Microsoft Teams, debe seleccionar manualmente el dispositivo de audio. El dispositivo de audio no se configura automáticamente como predeterminado. [RFLNX-5652]
- Puede que los menús desplegables fallen en una sesión en modo de pantalla completa. El problema se produce cuando la redirección de contenido del explorador está habilitada. [CVADHELP-13884]
- Puede que la opción de recurrir a TCP no funcione aunque **HDXoverUDP** esté establecido en **Preferred**. El problema ocurre cuando se conecta mediante Citrix Gateway. [CVADHELP-15526]

### Problemas conocidos en la versión 2009

- Es posible que la función ICA de multisección no funcione correctamente. [RFLNX-4286]
- Cuando ejecuta una videollamada o comparte la pantalla en Microsoft Teams, es posible que la pantalla parpadee. [RFLNX-4778]
- Es posible que no pueda cambiar entre sesiones de escritorio. [CVADHELP-15229]

### Problemas conocidos en la versión 2006

- A veces, la vista **Reunión** no se restaura mientras cambia de tareas en Microsoft Teams. El problema se produce cuando una ventana local se superpone a la ventana remota. Como resultado, la ventana remota no recibe los eventos del mouse. Como solución temporal, en la pantalla minimizada, coloque el cursor sobre el reloj digital y haga doble clic en el nombre de la persona que llama. [RFLNX-4937]
- A veces, la reconexión de sesiones falla. El problema se produce al configurar el protocolo Multi-Stream ICA (MSI) con un solo puerto a través de TCP con SD-WAN. [RFLNX-4782]

### Problemas conocidos en la versión 2004

- Es posible que la aplicación Citrix Workspace para Linux no identifique determinadas tarjetas inteligentes. Como resultado, no se pueden iniciar sesiones con dichas tarjetas.
- Cuando se inicia una sesión después de habilitar el protocolo Multi-Stream ICA (MSI) en la aplicación Workspace y en SD-WAN, la sesión se cierra inesperadamente. Aparece el siguiente mensaje de error:

“Se ha perdido la conexión con VDA...”

El problema se produce porque no se admite MSI de un solo puerto. [RFLNX-4219]

- Es posible que no se puedan iniciar sesiones en las distribuciones CentOS 8.x, Fedora 29, 30 y 31. Como solución temporal, consulte el artículo [CTX270926](#) de Knowledge Center. [RFLNX-3114]

### Problemas conocidos en la versión 1912

- Al usar la redirección de contenido del explorador web basada en CEF, el enfoque del teclado no vuelve a apuntar a la ventana principal si se redirige una URL. Como solución temporal, abra una nueva ficha en el explorador web y alterne entre las fichas para acceder a la ficha principal. [RFLNX-3871]
- Al usar la redirección de contenido del explorador web basada en CEF, es posible que aparezca una notificación que indica que el proceso webcontainer se ha detenido. El problema se produce al cerrar la instancia del explorador web. [RFLNX-3872]
- Cuando se utiliza la interfaz de usuario de autoservicio, es posible que las opciones de la ventana **Preferencias** no funcionen como se espera y que la aplicación Workspace deje de responder temporalmente. El problema ocurre en la distribución Ubuntu 19.10. [RFLNX-3720]
- Los feeds de Workspace Intelligence no se admiten en la aplicación Citrix Workspace 1912.
- La redirección de la cámara web no funciona con Microsoft Teams. Esto es una limitación porque Citrix no admite la optimización para Microsoft Teams [MTOPT] en la aplicación Citrix Workspace para Linux. [RFLNX-3674]

### Problemas conocidos en la versión 1910

- Al utilizar la interfaz de usuario de autoservicio, es posible que las opciones de la ventana **Preferencias** no funcionen como se espera. El problema ocurre cuando el paquete libwebkit1 no está disponible, como es el caso de los clientes de Debian 10 buster. Como solución temporal, quite la biblioteca **UIDialogLibWebKit.so** del directorio `install/path/lib`. [RFLNX-3596]
- Debido a cambios de arquitectura, ya no se puede establecer la conexión con el almacén en la nube [configuración en la nube]. Citrix recomienda utilizar la versión más reciente de la aplicación Citrix Workspace.

### Avisos legales de terceros

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

### [Avisos legales de terceros en la aplicación Citrix Workspace para Linux](#)

### Funciones experimentales

En ocasiones, Citrix publica funciones experimentales como mecanismo para buscar [comentarios](#) de los clientes sobre la conveniencia potencial de nuevas tecnologías o funciones. Citrix no acepta ca-

sos de asistencia para funciones experimentales, pero agradece comentarios para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. Citrix no se compromete a producir funciones experimentales y puede retirarlas por cualquier motivo en cualquier momento.

## Requisitos previos para instalar la aplicación Citrix Workspace

July 30, 2021

### Requisitos del sistema y compatibilidad

En esta tabla se indican los requisitos del sistema del kernel Linux, el espacio en disco y la visualización de vídeo en color:

Hardware	Requirements
Linux kernel	- Version 2.6.29 or later
Disk Space	- A minimum of 55 MB - Additional 110 MB if you expand/extract the installation package on the disk - A minimum of 1 GB RAM for system-on-a-chip (SoC) devices that use HDX MediaStream Flash Redirection
Color video display	- 256 color video display or higher

En esta tabla se indican los requisitos del sistema de las bibliotecas, la interfaz de usuario de autoservicio y las bibliotecas de códecs:

En esta tabla se indican los requisitos del protocolo de red:

Network	Requirements
Network protocol	- TCP/IP

En esta tabla se indican los requisitos del sistema de H.264, la redirección de HDX MediaStream para Flash y la integración de Customer Experience Improvement Program (CEIP):



Components	Requirements
H.264	For x86 devices: <ul style="list-style-type: none"> <li>- A minimum processor speed of 1.6 GHz</li> <li>- Single-monitor sessions</li> <li>- Display resolutions for example, 1280 x 1024 pixels</li> </ul>
	For the HDX 3D Pro feature: <ul style="list-style-type: none"> <li>- A minimum processor speed of 2 GHz</li> <li>- A native hardware with accelerated graphics driver</li> </ul>
	For ARM devices: <ul style="list-style-type: none"> <li>- A hardware H.264 decoder is required for both general H.264 support and HDX 3D Pro</li> </ul> <p><b>Note:</b> Performance improves after using faster processor clock speeds.</p>
HDX MediaStream Flash Redirection	For all HDX MediaStream Flash Redirection requirements, see Knowledge Center article <a href="http://support.citrix.com/article/CTX134786">http://support.citrix.com/article/CTX134786</a> .  Citrix recommends testing with the latest plug-in before deploying a new version to take advantage of the latest functionality and security-related fixes.
Customer Experience Improvement Program (CEIP) integration	<ul style="list-style-type: none"> <li>- zlib 1.2.3.3</li> <li>- libtar 1.2 and later</li> <li>- libjson 7.6.1 or later</li> </ul>

En esta tabla se indican los requisitos del sistema de la compresión de vídeo de cámaras web de HDX RealTime y la redirección de HDX MediaStream para Windows Media:

Components	Requirements
HDX RealTime Webcam Video Compression	<ul style="list-style-type: none"> <li>- A Video4Linux compatible Webcam</li> <li>- GStreamer 0.10.25 (or a later 0.10.x version), including the distribution's "plugins-good" package</li> </ul> <p style="text-align: center;">Or</p> <p>GStreamer 1.0 (or a later 1.x version), including the distribution's "plugins-base," "plugins-good," "plugins-bad," "plugins-ugly," and "gstreamer-libav" packages</p>
HDX MediaStream Windows Media Redirection	<ul style="list-style-type: none"> <li>- GStreamer 0.10.25 (or a later 0.10.x version), including the distribution's "plugins-good" package. In general, version 0.10.15 or later is sufficient for HDX MediaStream Windows Media Redirection</li> </ul> <p style="text-align: center;">Or</p> <p>GStreamer 1.0 (or a later 1.x version), including the distribution's "plugins-base," "plugins-good," "plugins-bad," "plugins-ugly," and "gstreamer-libav" packages</p> <p><b>Note:</b> If GStreamer is not included in your Linux distribution, you can download it from <a href="https://gstreamer.freedesktop.org/download/">https://gstreamer.freedesktop.org/download/</a>.</p> <p>Use of certain codes (for example, those in "plugins-ugly") might require a license from the manufacturer of that technology. Contact your system administrator for help.</p>

En esta tabla se indican los requisitos del sistema de la redirección de contenido del explorador web, Philips SpeechMike, la optimización de Microsoft Teams y la mejora de autenticación:

En esta tabla se indican los requisitos del sistema de Continuidad del servicio:

\*A partir de la versión 1910, es posible que la aplicación Citrix Workspace para Linux no funcione según lo esperado a menos que el sistema operativo cumpla estos requisitos de versión de GCC:

- Versión de GCC para la arquitectura x64: 4.8 o posterior
- Versión de GCC para la arquitectura armhf: 4.9 o posterior

### Nota

A partir de la versión 2101, es posible que la aplicación Citrix Workspace para Linux no funcione según lo esperado a menos que el sistema operativo cumpla los siguientes requisitos:

- Versión 4.9 de GCC o una posterior
- glibcxx 3.4.20 o una versión posterior

### Tabla de compatibilidad

La aplicación Citrix Workspace para Linux es compatible con todas las versiones actualmente compatibles de los productos Citrix. Para obtener más información acerca de la vida útil de los productos Citrix y para determinar cuándo deja Citrix de ofrecer versiones específicas de los productos, consulte la [tabla de ciclos de vida de productos Citrix](#).

### Requisitos del servidor

#### StoreFront

- Puede utilizar todas las versiones admitidas de la aplicación Citrix Workspace para acceder a los almacenes de StoreFront mediante conexiones desde la red interna y a través de Citrix Gateway:
  - StoreFront 1811 y versiones posteriores.
  - StoreFront 3.12.
- Puede usar el almacén de StoreFront que está configurado con Workspace para Web. Workspace para Web ofrece acceso a los almacenes de StoreFront desde un explorador web. Para conocer las limitaciones de esta implementación, consulte [Consideraciones importantes](#) en la documentación de StoreFront.

### Conexiones y certificados

#### Conexiones

La aplicación Citrix Workspace para Linux admite conexiones HTTPS y conexiones ICA sobre TLS a través de las siguientes configuraciones.

- Para conexiones LAN:
  - StoreFront con servicios de StoreFront o Workspace para Web
- Para conexiones locales o remotas seguras:
  - Citrix Gateway 12.0
  - NetScaler Gateway 10.1 y versiones posteriores
  - NetScaler Access Gateway Enterprise Edition 10
  - NetScaler Access Gateway Enterprise Edition 9.x

- NetScaler Access Gateway VPX

Para obtener información sobre las versiones de Citrix Gateway admitidas en StoreFront, consulte [Requisitos del sistema](#) para StoreFront.

## Certificados

Para garantizar transacciones seguras entre el servidor y el cliente, use los siguientes certificados:

### Certificados privados (autofirmados)

Si se ha instalado un certificado privado en la puerta de enlace remota, se debe disponer de un certificado raíz para la entidad de certificación de la empresa en el dispositivo con el fin de poder acceder a los recursos Citrix mediante la aplicación Citrix Workspace.

#### Nota:

Si el certificado de la puerta de enlace remota no se puede verificar en la conexión (debido a que no se incluyó el certificado raíz en el almacén de claves local), se muestra un mensaje de advertencia sobre la presencia de un certificado que no es de confianza. Si un usuario elige ignorar la advertencia y continuar con la conexión, se mostrarán aplicaciones, pero no se podrán iniciar. El certificado raíz debe instalarse en el almacén de certificados del cliente.

### Certificados raíz

Para equipos unidos a dominios, puede utilizar la plantilla administrativa de objeto de directiva de grupo para distribuir y configurar la confianza en los certificados de la CA.

Para equipos que no están unidos a un dominio, la organización puede crear un paquete de instalación personalizado para distribuir e instalar el certificado de la CA. Póngase en contacto con el administrador del sistema para recibir ayuda.

### Instalación de certificados raíz en los dispositivos de usuario

Para utilizar TLS necesita un certificado raíz en el dispositivo del usuario que pueda verificar la firma de la entidad de certificación en el certificado del servidor. De manera predeterminada, la aplicación Citrix Workspace admite los siguientes certificados.

---

Certificado	Entidad emisora
Class4PCA_G2_v2.pem	Verisign Trust Network
Class3PCA_G2_v2.pem	Verisign Trust Network
BTCTRoot.pem	Baltimore Cyber Trust Root

Certificado	Entidad emisora
GTECTGlobalRoot.pem	GTE Cyber Trust Global Root
Pcs3ss_v4.pem	Class 3 Public Primary Certification Authority
GeoTrust_Global_CA.pem	GeoTrust
DigiCertGlobalRootCA.pem	DigiCert Global Root CA

### 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 Linux admite el uso de certificados comodín, aunque deben usarse solo de acuerdo con la directiva de seguridad de la organización. En la práctica, se puede considerar la posibilidad de usar alternativas a certificados comodines, como, por ejemplo, un certificado que contenga la lista de nombres de servidor dentro de la extensión de nombre de sujeto alternativo (Subject Alternative Name o SAN). Estos certificados pueden ser emitidos por entidades de certificación tanto privadas como públicas.

### Certificados intermedios y Citrix Gateway

Si la cadena de certificados incluye un certificado intermedio, deberá agregar este certificado al certificado del servidor Citrix Gateway. Para obtener más información, consulte [Configurar certificados intermedios](#) en la documentación de Citrix Gateway.

Si el servidor de StoreFront no puede proporcionar los certificados intermedios que coincidan con el certificado que está utilizando, o si instala certificados intermedios para admitir usuarios de tarjetas inteligentes, siga estas instrucciones antes de agregar un almacén de StoreFront:

1. Obtenga uno o varios certificados intermedios por separado en formato PEM.

**Sugerencia:**

Si no puede encontrar un certificado en formato PEM, use la utilidad `openssl` para convertir un certificado en formato CRT a un archivo PEM.

2. Como el usuario que instala el paquete (normalmente root):
  - a) Copie uno o varios archivos a `$(ICAROOT)/keystore/intcerts`.
  - b) Ejecute el siguiente comando como usuario que instaló el paquete:

```
$(ICAROOT)/util/ctx_rehash
```

### Directiva de validación conjunta de certificados de servidor

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

#### Importante:

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

- La configuración del servidor o la puerta de enlace incluye un certificado raíz incorrecto
- La configuración del servidor o la puerta de enlace no incluye todos los certificados intermedios
- La configuración del servidor o la puerta de enlace incluye un certificado intermedio caducado o no válido
- La configuración del servidor o la puerta de enlace incluye un certificado intermedio con firmas cruzadas

Cuando valida un certificado de servidor, la aplicación Citrix Workspace para Linux usa ahora **todos** los certificados suministrados por el servidor (o la puerta de enlace) para validarlo. Al igual que en las versiones anteriores, esta versión de la aplicación Citrix Workspace para Linux también comprueba posteriormente que los certificados son 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 la puerta de enlace) 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 Linux.

Supongamos que se configura una puerta de enlace 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 Linux:

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

A continuación, la aplicación Citrix Workspace para Linux comprueba que todos los certificados son válidos. La aplicación Citrix Workspace para Linux comprueba también que ya confía en “Ejemplo de certificado raíz”. Si la aplicación Citrix Workspace para Linux no confía en “Ejemplo de certificado raíz”, 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, fallan las conexiones de la aplicación Citrix Workspace para Linux 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.
- Algunos servidores y puertas de enlace 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”

A continuación, la aplicación Citrix Workspace para Linux usa estos dos certificados. Luego, busca un certificado raíz en el dispositivo del usuario. Si encuentra uno que se valida correctamente y también es de confianza (por ejemplo, “Ejemplo de certificado raíz”), la conexión se realiza correctamente. De lo contrario, la conexión falla. Esta configuración proporciona el certificado intermedio que necesita la aplicación Citrix Workspace para Linux, pero también permite que la aplicación Citrix Workspace para Linux elija cualquier certificado raíz válido y de confianza.

Supongamos ahora que se configura una puerta de enlace con estos certificados:

- “Ejemplo de certificado de servidor”
- “Ejemplo de certificado intermedio”
- “Certificado raíz incorrecto”

Un explorador web podría ignorar el certificado raíz incorrecto. No obstante, la aplicación Citrix Workspace para Linux no ignora el certificado raíz incorrecto y la conexión falla.

Algunas entidades de certificación usan más de un certificado intermedio. En este caso, la puerta de enlace 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”

### Importante:

- 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, hay al menos dos certificados intermedios. Por ejemplo, el certificado raíz anterior “Class 3 Public Primary Certification Authority” tiene el certificado intermedio correspondiente de firmas cruzadas “Verisign Class 3 Public Primary Certification Authority - G5”. No obstante, un certificado raíz posterior correspondiente “Verisign Class 3 Public Primary Certification Authority - G5” también está disponible y reemplaza a “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 la puerta de enlace para que use el certificado intermedio con firmas cruzadas, porque selecciona el certificado raíz anterior:

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

No se recomienda configurar la puerta de enlace solamente con el certificado del servidor:

- “Ejemplo de certificado de servidor”

En este caso, si la aplicación Citrix Workspace para Linux no puede ubicar todos los certificados intermedios, la conexión falla.

### Hdxcheck

Citrix ofrece un script, `workspacecheck.sh`, como parte del paquete de instalación de la aplicación Citrix Workspace. El script comprueba si su dispositivo cumple todos los requisitos del sistema para poder utilizar todas las funcionalidades de la aplicación Citrix Workspace para Linux. Este script se halla en el directorio `Utilities` del paquete de instalación.



### Para ejecutar el script workspacecheck.sh

1. Abra el terminal de su máquina Linux.
2. Escriba `cd $ICAROOT/util` y presione **Entrar** para ir al directorio `Utilities` del paquete de instalación.
3. Escriba `./workspacecheck.sh` para ejecutar el script.

## Instalación, desinstalación y actualización

July 30, 2021

Puede instalar la aplicación Citrix Workspace mediante uno de los siguientes métodos:

- Descargue la aplicación Citrix Workspace desde [Descargas de Citrix](#).
- Implementar la aplicación Citrix Workspace con Citrix Workspace para Web (configurada con StoreFront).

### Instalación manual

Descargue los siguientes paquetes de la página [Descargas de Citrix](#).

### Paquetes Debian

Instale uno de los paquetes `Icaclient` o uno de los paquetes `IcaclientWeb`, según la arquitectura de su sistema operativo.

Para utilizar la redirección USB genérica, instale uno de los paquetes `ctxusb`, según la arquitectura de su sistema operativo.

Nombre del paquete	Contenido
<b>Paquetes Debian (Ubuntu, Debian, Linux Mint, etc.)</b>	
<code>icaclient_20.06.0.15_amd64.deb</code>	Compatibilidad con el autoservicio, x86_64 de 64 bits
<code>icaclient_20.06.0.15_i386.deb</code>	Compatibilidad con el autoservicio, x86 de 32 bits
<code>icaclient_20.06.0.15_armhf.deb</code>	Compatibilidad con el autoservicio, armhf
<code>icaclientWeb_20.06.0.15_amd64.deb</code>	Solo Receiver para Web, x86_64 de 64 bits
<code>icaclientWeb_20.06.0.15_i386.deb</code>	Solo Receiver para Web, x86 de 32 bits

Nombre del paquete	Contenido
icaclientWeb_20.06.0.15_armhf.deb	Solo Receiver para Web, armhf
ctxusb_20.06.0.15_amd64.deb	Paquete USB, x86_64 de 64 bits
ctxusb_20.06.0.15_i386.deb	Paquete USB, x86 de 32 bits
ctxusb_20.06.0.15_armhf.deb	Paquete USB, armhf

### Instalación con un paquete Debian

Al instalar la aplicación Citrix Workspace desde el paquete Debian en Ubuntu, abra los paquetes en el Centro de software de Ubuntu.

En las siguientes instrucciones, reemplace

**nombre\_del\_paquete** por el nombre del paquete que intenta instalar.

Este procedimiento usa una línea de comandos y el administrador de paquetes nativo de Ubuntu/Debian/Mint. En su lugar, para instalar el paquete, haga doble clic en el paquete DEB descargado, dentro del explorador de archivos. Normalmente, se inicia un administrador de paquetes que descarga el software necesario que falte. Si no hay ningún administrador de paquetes disponible, Citrix recomienda utilizar **gdebi**, una herramienta de línea de comandos.

#### Requisitos previos:

Debe instalar el paquete `icaclient` o el paquete `icaclientWeb`.

Para instalar el paquete mediante la línea de comandos:

1. Inicie sesión como usuario con privilegios (root).
2. Abra una ventana de terminal.
3. Ejecute la instalación de los 3 paquetes siguientes. Para ello, escriba `gdebi packagename.deb`. Por ejemplo:
  - `gdebi icaclient\\_19.0.6.6\\_amd64.deb`
  - `gdebi icaclientWeb\\_19.0.6.6\\_i386.deb`
  - `gdebi ctxusb\\_2.7.6\\_amd64.deb`

Para usar `dpkg` en los ejemplos anteriores, reemplace `gdebi` por `dpkg -i`.

Si usa `dpkg`, instale las dependencias que falten; para ello, escriba `sudo apt-get -f install..`

### Nota:

- El paquete `ctxusb` es opcional para ofrecer la funcionalidad de redirección de USB genérico.
- A partir de la versión 2101, aparece un mensaje interactivo pidiéndole que instale la protección de aplicaciones.

4. Acepte el Contrato de licencia del usuario final (EULA).

### Instalar el componente de protección de aplicaciones en paquetes Debian

A partir de la versión 2102, la protección de aplicaciones se ofrece en la versión Debian de la aplicación Citrix Workspace.

Para una instalación silenciosa del componente de protección de aplicaciones, ejecute el siguiente comando desde el terminal antes de instalar la aplicación Citrix Workspace:

```
1 `export DEBIAN_FRONTEND="noninteractive"`  
2  
3 `sudo debconf-set-selections <<< "icaclient app_protection/  
   install_app_protection select no"`  
4  
5 `sudo debconf-show icaclient`  
6  
7 `sudo apt install -f ./icaclient_<version>._amd64.deb`
```

### Instalar Continuidad del servicio en paquetes Debian

A partir de la versión 2106, puede instalar Continuidad del servicio en la versión Debian de la aplicación Citrix Workspace.

Ejecute estos comandos desde el terminal antes de instalar la aplicación Citrix Workspace:

```
sudo apt-get update  
sudo apt-get install libwebkit2gtk-4.0-37 gnome-keyring libsecret-1-0
```

### Paquetes Red Hat

Instale uno de los paquetes `ICAClient` o uno de los paquetes `ICAClientWeb`, según la arquitectura de su sistema operativo.

Para utilizar la redirección USB genérica, instale uno de los paquetes `ctxusb`, según la arquitectura de su sistema operativo.

Nombre del paquete	Contenido
<b>Paquetes Red Hat (Red Hat, SUSE, Fedora, etc.)</b>	
ICAClient-rhel-20.06.0.15-0.x86_64.rpm	Compatibilidad con el autoservicio, basado en Red Hat (incluido Linux VDA), x86_64 de 64 bits
ICAClient-rhel-20.06.0.15-0.i386.rpm	Compatibilidad con el autoservicio, basado en Red Hat, x86 de 32 bits
ICAClientWeb-rhel-20.06.0.15-0.x86_64.rpm	Solo Receiver para Web, basado en Red Hat, x86_64 de 64 bits
ICAClientWeb-rhel-20.06.0.15-0.i386.rpm	Solo Receiver para Web, basado en Red Hat, x86 de 32 bits
ICAClient-suse-20.06.0.15-0.x86_64.rpm	Compatibilidad con el autoservicio, basado en SUSE, x86_64 de 64 bits
ICAClient-suse-20.06.0.15-0.i386.rpm	Compatibilidad con el autoservicio, basado en SUSE, x86 de 32 bits
ICAClientWeb-suse-20.06.0.15-0.x86_64.rpm	Solo Receiver para Web, basado en SUSE, x86_64 de 64 bits
ICAClientWeb-suse-20.06.0.15-0.i386.rpm	Solo Receiver para Web, basado en SUSE, x86 de 32 bits
ctxusb-20.06.0.15-1.x86_64.rpm	Paquete USB, x86_64 de 64 bits
ctxusb-20.06.0.15-1.i386.rpm	Paquete USB, x86 de 32 bits

**Nota:**

Se retira el paquete RPM *SuSE 11 SP3 Full Package (compatibilidad con el autoservicio)*.

**Instalación con un paquete RPM**

Si está instalando la aplicación Citrix Workspace desde el paquete RPM en SUSE, use las utilidades YaST o Zypper. La utilidad RPM instala el paquete RPM. Se produce un error si faltan las dependencias necesarias.

**Para configurar el repositorio EPEL en Red Hat**

Descargue el paquete fuente RPM apropiado desde:

[https://fedoraproject.org/wiki/EPEL#Extra\\_Packages\\_for\\_Enterprise\\_Linux\\_.28EPEL.29](https://fedoraproject.org/wiki/EPEL#Extra_Packages_for_Enterprise_Linux_.28EPEL.29).

Para obtener información sobre cómo usarlo, consulte [https://fedoraproject.org/wiki/EPEL#How\\_can\\_I\\_use\\_these\\_extra\\_packages.3F](https://fedoraproject.org/wiki/EPEL#How_can_I_use_these_extra_packages.3F)

Por ejemplo, en Red Hat Enterprise 7.x, puede instalar el repositorio EPEL mediante este comando:

```
1 yum localinstall epel-release-latest-7.noarch.rpm
```

#### Sugerencia:

El Administrador de paquetes RPM no instala el software necesario que falte. Para descargarlo e instalarlo, se recomienda usar **zypper install <nombre de archivo>** en una línea de comandos en OpenSUSE, o bien **yum localinstall <nombre de archivo>** en Fedora/Red Hat.

### Para la instalación a partir del paquete RPM

#### Requisitos previos:

Debe instalar el paquete `icaclient` o el paquete `icaclientWeb`.

1. Configure el repositorio EPEL.
2. Inicie sesión como usuario con privilegios (root).
3. Escriba `zypper` en \ para ejecutar la instalación de los tres paquetes siguientes.

#### Nota:

- `ctxusb` es un paquete opcional. Instale el paquete para ofrecer la redirección de USB genérico.
- `ctxappprotection` es un paquete opcional. Instale el paquete solo si quiere instalar el componente de protección de aplicaciones.

4. Abra una ventana de terminal.

#### Para las instalaciones de SUSE:

- `zypper in ICAClient-suse-19.12.0.19-0.x86_64.rpm`
- `zypper in ICAClient-suse-19.12.0.19-0.i386.rpm`
- `zypper in ctxusb-2.7.19-1.x86_64.rpm`
- `zypper in ctxappprotection-21.4.0.2-0.x86_64.rpm`

#### Para las instalaciones de Red Hat:

- `yum localinstall ICAClient-rhel-19.12.0.19-0.i386.rpm`
- `yum localinstall ICAClientWeb-rhel-19.12.0.19-0.i386.rpm`

- `yum localinstall ctxusb-2.7.19-1.i386.rpm`
- `yum localinstall ctxappprotection-21.4.0.2-0.x86_64.rpm`

5. Acepte el Contrato de licencia del usuario final (EULA).

### Para instalar un paquete que falta

En una distribución basada en Red Hat (RHEL, CentOS, Fedora, etc.), si aparece el siguiente mensaje de error:

```
1 "… requires libwebkitgtk-1.0.so.0"
```

Agregue un repositorio EPEL (los detalles se pueden consultar en <https://fedoraproject.org/wiki/EPEL>).

### Paquetes tarball

Instale uno de los paquetes siguientes, según la arquitectura de su sistema operativo.

Nombre del paquete	Contenido
<b>Tarballs (instalación por script para cualquier distribución)</b>	
linuxx64-20.06.0.15.tar.gz	Intel de 64 bits
linuxx86-20.06.0.15.tar.gz	Intel de 32 bits
linuxarmhf-20.06.0.15.tar.gz	armhf

La diferencia entre paquetes compatibles con la aplicación Workspace para Web y los que ofrecen el autoservicio es que estos últimos requieren otros elementos dependientes para el autoservicio, además de los necesarios para la aplicación Workspace para Web. Los elementos dependientes para el autoservicio son un conjunto más grande que los que se requieren para la aplicación Workspace para Web, pero los archivos instalados son idénticos.

- Si solo necesita la aplicación Workspace para Web o si su distribución no cuenta con los paquetes necesarios para dar disponer del autoservicio, instale solo el paquete de la aplicación Workspace para Web.
- De lo contrario, instale la aplicación Citrix Workspace desde el paquete Debian o el paquete RPM. Estos archivos son más fáciles de usar, ya que instalan automáticamente los paquetes que sean necesarios.

- Si quiere personalizar la ubicación de instalación, instale la aplicación Citrix Workspace desde el paquete tarball.

**Nota:**

- No utilice dos métodos de instalación diferentes en la misma máquina. Si lo hace, es probable que vea mensajes de error y un comportamiento no deseado.

### Instalación con un paquete tarball

**Nota:**

El paquete tarball no realiza comprobaciones de dependencias ni instala dependencias. Es necesario resolver por separado todas las dependencias del sistema.

1. Abra una ventana de terminal.
2. Extraiga el contenido del archivo `.tar.gz` en un directorio vacío. Por ejemplo, escriba: `tar xvfz packagename.tar.gz`.
3. Escriba `./setupwfc` y presione Entrar para ejecutar el programa de instalación.
4. Acepte el valor predeterminado de 1 (para instalar la aplicación Citrix Workspace) y presione **Entrar**.
5. Escriba la ruta y el nombre del directorio de instalación requerido y, a continuación, presione Entrar; también puede presionar directamente Entrar para instalar la aplicación Citrix Workspace en la ubicación predeterminada.

El directorio predeterminado para las instalaciones de usuarios con privilegios (root) es `/opt/Citrix/ICAClient`.

El directorio predeterminado para las instalaciones de usuarios sin privilegios es `$HOME/ICAClient/platform`. “Platform” es un identificador generado por el sistema para el sistema operativo instalado; por ejemplo, `$HOME/ICAClient/linuxx86` para la plataforma Linux/x86.

**Nota:**

Si especifica una ubicación no predeterminada, establezca la ubicación de `$ICAROOT` en `$HOME/.profile` o en `$HOME/.bash\_profile`.

6. Cuando se le solicite continuar, escriba `y`, luego, presione Entrar.
7. Puede elegir si quiere integrar la aplicación Citrix Workspace en el entorno de escritorio. La instalación crea una opción de menú desde la cual los usuarios pueden iniciar la aplicación Citrix Workspace. Escriba `y` en el símbolo del sistema para habilitar la integración.

8. Si ha instalado GStreamer previamente, puede elegir si quiere integrarlo con la aplicación Citrix Workspace y, de ese modo, ofrecer la aceleración multimedia HDX MediaStream. Para integrar la aplicación Citrix Workspace con GStreamer, escriba `y` en el símbolo del sistema.

**Nota:**

En algunas plataformas, instalar el cliente a partir de un paquete tarball puede provocar que el sistema deje de responder tras solicitarle una integración en KDE y GNOME. Este problema ocurre con la primera inicialización de gstreamer-0.10. Si se produce este problema, finalice el proceso de instalación (con la combinación de teclas Ctrl+C) y ejecute el comando `gst-inspect-0.10 --gst-disable-registry-fork --version`. Después de ejecutar el comando, puede volver a ejecutar el paquete tarball sin sufrir el problema.

9. Si ha iniciado sesión como usuario con privilegios (root), podrá elegir si quiere instalar la compatibilidad con USB para las aplicaciones VDI publicadas de Citrix Virtual Apps and Desktops. Escriba `y` en el símbolo del sistema para instalar la compatibilidad con USB.

**Nota:**

Si no ha iniciado sesión como usuario con privilegios (root), aparecerá esta advertencia:

“USB support cannot be installed by non-root users. Run the installer as root to access this install option”.

10. Una vez completada la instalación, aparecerá nuevamente el menú principal de instalación. Para salir de la instalación, escriba `3` y presione Entrar.

## Desinstalación

Este procedimiento se ha probado con el paquete tarball. Quite los paquetes RPM y Debian con las herramientas estándar del sistema operativo.

La variable de entorno ICAROOT se debe establecer en el directorio de instalación del cliente. El directorio predeterminado para las instalaciones de usuarios sin privilegios es `$HOME/ICAClient/platform`. La variable “platform” es un identificador generado por el sistema para el sistema operativo instalado; por ejemplo, `$HOME/ICAClient/linuxx86` para la plataforma Linux/x86. El valor predeterminado de las instalaciones con usuarios con privilegios es `/opt/Citrix/ICAClient`.

**Nota:**

Para desinstalar la aplicación Citrix Workspace, tiene que haber iniciado sesión con la misma cuenta de usuario que utilizó para instalarla.



### Para desinstalar la aplicación Citrix Workspace en el paquete tarball

1. Para ejecutar la instalación, escriba `$ICAROOT/setupwfc` y presione Entrar.
2. Para quitar el cliente, escriba 2 y presione **Entrar**.

### Para desinstalar la aplicación Citrix Workspace en sistemas operativos Debian/Ubuntu

Ejecute este comando desde la carpeta de instalación de la aplicación Citrix Workspace:

```
apt remove icaclient  
apt autoremove
```

O BIEN

```
apt remove icaclient  
apt purge icaclient
```

### Para desinstalar la aplicación Citrix Workspace en los sistemas operativos Fedora/RHEL/CentOS

Ejecute este comando desde la carpeta de instalación de la aplicación Citrix Workspace:

```
yum remove icaclient
```

## Actualizaciones

Para actualizar de Citrix Receiver a la aplicación Citrix Workspace, descargue e instale la versión más reciente de la aplicación Citrix Workspace desde [Descargas de Citrix](#).

La superposición de pantalla de **Citrix Workspace** aparece en el primer inicio de la aplicación, al actualizar la versión de la aplicación, y al desinstalarla y reinstalarla. Haga clic en **Aceptar** para seguir usando la aplicación Citrix Workspace o haga clic en **Más información** para obtener más detalles.

## Introducción

July 30, 2021

## Configuración

Puede descargar el paquete de instalación, personalizar la configuración y, a continuación, instalar la aplicación Citrix Workspace. Asimismo, puede modificar el contenido del paquete de la aplicación Citrix Workspace y, a continuación, volver a empaquetar los archivos.

### Personalizar la instalación

1. Expanda el archivo del paquete de la aplicación Citrix Workspace en un directorio vacío. El archivo del paquete se llama `platform.major.minor.release.build.tar.gz` (por ejemplo, `linuxx86.13.2.0.nnnnnn.tar.gz` para la plataforma Linux/x86).
2. Realice los cambios requeridos en el paquete de la aplicación Citrix Workspace. Por ejemplo, puede agregar un certificado raíz TLS para utilizar un certificado de una entidad de certificación que no forma parte de la instalación estándar de la aplicación Citrix Workspace.
3. Abra el `PkgID` archivo.
4. Agregue la siguiente línea para indicar que se ha modificado el paquete:  

```
MODIFIED=traceinfo
```

donde `traceinfo` es la información que indica quién realizó el cambio y cuándo lo hizo.
5. Guarde el archivo y ciérrelo.
6. Abra la lista de archivos del paquete, `plataforma/plataforma.psf` (por ejemplo, `linuxx86/linuxx86.psf` para la plataforma Linux/x86).
7. Actualice la lista de archivos del paquete para reflejar los cambios que ha realizado al paquete. Si no se actualiza, puede producirse un error al instalar el nuevo paquete. Los cambios pueden consistir en una actualización en el tamaño de todos los archivos modificados, o la inclusión de nuevas líneas en cualquiera de los archivos agregados al paquete. Las columnas en la lista de archivos del paquete son:
  - Tipo de archivo
  - Ruta relativa
  - Subpaquete (siempre establecido en `cor`)
  - Permisos
  - Propietario
  - Grupo
  - Tamaño
8. Guarde el archivo y ciérrelo.
9. Use el comando `tar` para reconstruir el archivo de paquete de la aplicación Citrix Workspace. Por ejemplo, `tar czf ./newpackage.tar.gz *`, donde `newpackagez` es el nombre del nuevo archivo de paquete de la aplicación Citrix Workspace.

### El webkit más reciente está disponible

La aplicación Citrix Workspace para Linux necesita `libwebkit2gtk` (2.16.6 o una versión posterior).

`libwebkit2gtk` tiene las siguientes ventajas:

- Experiencia de interfaz de usuario mejorada. webkit2gtk es compatible con la función de redirección de contenido del explorador web. Utilice la versión 2.24 de webkit2gtk o una posterior para obtener una mejor experiencia de visionado en YouTube.
- La versión 2.16.6 de webkit2gtk y posteriores mejoran la experiencia de inicio de sesión y el tiempo que se tarda en iniciar sesión.
- La aplicación funciona mejor con distribuciones de Linux más recientes y ofrece las últimas correcciones de seguridad del WebKit.

### Nota:

webkit2gtk no está disponible en algunas distribuciones de Linux. Como solución temporal, tenga en cuenta las siguientes opciones:

- Compile webkit2gtk a partir de la fuente antes de instalar la versión 1906 de la aplicación Citrix Workspace.
- Descargue el paquete web desde la [página Descargas](#). Este paquete solo admite inicios web.
- Mueva a una distribución de Linux posterior que admita webkit2gtk 2.16.6 o una versión más reciente.

## Inicio

Puede iniciar la aplicación Citrix Workspace en el símbolo del sistema de un terminal o desde alguno de los entornos de escritorio admitidos.

Compruebe que la variable de entorno `ICAROOT` está establecida de modo que apunte al directorio de instalación real.

### Sugerencia:

Las instrucciones siguientes no se aplican a instalaciones realizadas a partir de paquetes web ni a aquellas en que se usa tarball, sino a aquellas en las que los requisitos de autoservicio no se han cumplido.

## Símbolo del sistema de un terminal

Para iniciar la aplicación Citrix Workspace en el símbolo del sistema de un terminal, escriba:

```
/opt/Citrix/ICAClient/selfservice
```

A continuación, presione Entrar (donde `/opt/Citrix/ICAClient` es el directorio en el que se instaló la aplicación Citrix Workspace).

## Escritorio Linux

Para iniciar la aplicación Citrix Workspace desde un entorno de escritorio, búsquela con un administrador de archivos.

En algunos escritorios, también puede iniciar la aplicación Citrix Workspace desde un menú. La aplicación Citrix Workspace puede estar ubicada en distintos menús, según la distribución de Linux que se esté mediante.

## Preferencias

Para definir sus preferencias, haga clic en **Preferencias** en el menú de la aplicación Citrix Workspace. Puede controlar cómo se muestran los escritorios, conectar con diferentes aplicaciones y escritorios, y administrar el acceso de dispositivos y archivos.

## Administración de una cuenta

Para acceder a escritorios y aplicaciones, se necesita una cuenta de XenDesktop o Citrix Virtual Apps. Es posible que su servicio de asistencia de TI le pida que agregue una cuenta a Citrix Workspace para este fin. También pueden pedirle que use un servidor Citrix Gateway o Access Gateway diferente para una cuenta existente. También puede quitar cuentas de Citrix Workspace.

1. En la página **Cuentas** del cuadro de diálogo **Preferencias**, lleve a cabo una de las siguientes acciones:
  - Para agregar una cuenta, haga clic en **Agregar**. Para obtener más información, contacte con el administrador del sistema.
  - Para cambiar los datos de un almacén utilizado por la cuenta (por ejemplo, la puerta de enlace predeterminada), haga clic en **Modificar**.
  - Para quitar una cuenta, haga clic en **Quitar**.
2. Siga las instrucciones en pantalla. Debe autenticarse en el servidor cuando se le solicite.

## Pantalla de escritorio

### Nota:

Esta función no está disponible en sesiones de Citrix Virtual Apps para UNIX.

Puede mostrar los escritorios en toda la pantalla del dispositivo de usuario (el modo de Pantalla completa), que es el valor predeterminado, o puede mostrarlos en una ventana aparte (modo de Ventana).

- En la página **General** del cuadro de diálogo **Preferencias**, seleccione uno de esos modos mediante la opción **Mostrar escritorio en**.

Utilice la funcionalidad de la barra de herramientas **You can enable Desktop Viewer** para modificar dinámicamente la configuración de la ventana de la sesión remota.

## Desktop Viewer

Los requisitos para el acceso por parte de los usuarios a los escritorios virtuales pueden variar de usuario a usuario y a medida que evolucionan las necesidades de la empresa.

Use Desktop Viewer cuando los usuarios necesiten interactuar con el escritorio virtual. El escritorio virtual del usuario pueden ser un escritorio virtual publicado, o un escritorio compartido o escritorio dedicado. En este caso de acceso, la funcionalidad de la barra de herramientas de Desktop Viewer permite al usuario alternar entre una sesión en modo de ventana y una sesión a pantalla completa; además, admite varios monitores para los monitores intersecados. Los usuarios pueden alternar entre sesiones de escritorio y trabajar mediante varias conexiones de Citrix Virtual Apps and Desktops en el mismo dispositivo de usuario. Para gestionar mejor las sesiones de los usuarios, se ofrecen botones para minimizar todas las sesiones de escritorio, enviar la secuencia Ctrl+Alt+Supr, desconectar la sesión y cerrarla.

Al presionar **Ctrl+Alt+Inter**, se muestran los botones de la barra de herramientas de Desktop Viewer en una ventana emergente.

## Reconexión de sesión automática

La aplicación Citrix Workspace puede volver a conectarse a escritorios y aplicaciones que se hayan desconectado. Por ejemplo, tras un problema de infraestructura de red.

- En la página **General** del cuadro de diálogo **Preferencias**, seleccione una opción en **Reconectar aplicaciones y escritorios**.

## Acceso a los archivos locales

Es posible que un escritorio virtual o una aplicación necesiten acceder a archivos ubicados en el dispositivo. El usuario puede controlar este acceso.

1. En la página **Acceso a archivos** del cuadro de diálogo **Preferencias**, seleccione una unidad asignada y, a continuación, una de las siguientes opciones:
  - **Lectura y escritura:** Para permitir que el escritorio o la aplicación lean y escriban en los archivos locales.
  - **Solo lectura:** Para permitir que el escritorio o la aplicación lean, pero no escriban, en los archivos locales.
  - **Sin acceso:** Para impedir que el escritorio o la aplicación accedan a los archivos locales.
  - **Preguntar siempre:** Para pedir permiso al usuario cada vez que el escritorio o la aplicación necesiten acceder a archivos locales.
2. Haga clic en **Agregar**, especifique la ubicación y seleccione una unidad para asignársela.

## Micrófono y cámara web

Para configurar un micrófono o una cámara web, puede cambiar la forma en que un escritorio virtual o una aplicación acceden a su micrófono o cámara web locales:

En la página **Micrófono y cámara web** del cuadro de diálogo **Preferencias**, seleccione una de las siguientes opciones:

- **Usar mi micrófono y mi cámara web:** Para permitir que el escritorio o la aplicación usen el micrófono y la cámara web.
- **No usar mi micrófono ni mi cámara web:** Para prohibir que el escritorio o la aplicación usen el micrófono y la cámara web.

## Flash Player

Puede elegir cómo se muestra el contenido de Flash. Este contenido se muestra normalmente con el reproductor **Flash Player** e incluye animaciones, vídeo y aplicaciones.

En la página **Flash** del cuadro de diálogo **Preferencias**, seleccione una de las siguientes opciones:

- **Optimizar el contenido:** Para mejorar la calidad de la reproducción, con el riesgo de disminuir la seguridad.
- **No optimizar el contenido:** Proporciona calidad de reproducción básica, sin disminuir la seguridad.
- **Preguntar siempre:** Para pedir permiso cada vez que se muestra contenido de Flash.

## Conectar

La aplicación Citrix Workspace ofrece a los usuarios acceso de autoservicio seguro a aplicaciones y escritorios virtuales, y acceso a demanda a aplicaciones de Windows, web y de Software como servicio (SaaS). Las páginas web de Citrix StoreFront, o las páginas web antiguas creadas con la Interfaz Web, administran el acceso de los usuarios.

## Para conectarse a los recursos mediante la interfaz de usuario de Citrix Workspace

La página de inicio de la aplicación Citrix Workspace muestra las aplicaciones y los escritorios virtuales que están disponibles para los usuarios, basándose en los parámetros de cuenta del usuario (es decir, el servidor al que se conecta) y en los parámetros configurados por los administradores de Citrix Virtual Apps and Desktops. Desde la página **Preferencias > Cuentas**, puede configurar la dirección URL de un servidor de StoreFront o, si está configurada la detección de cuentas basada en correo electrónico, escribir la dirección de correo electrónico.

### **Sugerencia:**

Si utiliza el mismo nombre para varios almacenes en el servidor de StoreFront, agregue números a esos nombres para evitar duplicados. Los nombres de dichos almacenes dependen del orden en que se agregaron. Para la aplicación Citrix Workspace, se muestra la URL del almacén y esta identifica de forma única el almacén.

Después de conectarse a un almacén, el autoservicio muestra las fichas **Favoritos**, **Escritorios** y **Aplicaciones**. Para iniciar una sesión, haga clic en el icono correspondiente. Para agregar un icono a **Favoritos**, haga clic en el enlace **Detalles** situado junto al icono y seleccione **Agregar a Favoritos**.

### **Configuración de los parámetros de conexión**

Puede configurar distintos parámetros predeterminados para las conexiones entre la aplicación Citrix Workspace y los servidores de Citrix Virtual Apps and Desktops. También puede cambiar esos parámetros para conexiones individuales, si es necesario.

Aunque las tareas y responsabilidades de los administradores y los usuarios pueden superponerse, el término “usuario” se emplea para distinguir las tareas generales de los usuarios de las realizadas típicamente por los administradores.

### **Conexión con recursos desde una línea de comandos o explorador**

Cuando se hace clic en el icono de una aplicación o de un escritorio en la página de inicio de la aplicación Citrix Workspace, se crea una conexión con un servidor. Además, se pueden abrir conexiones desde una línea de comandos o desde un explorador web.

### **Para crear una conexión a un servidor de StoreFront o Program Neighborhood mediante una línea de comandos**

#### **Requisito previo:**

Asegúrese de que la aplicación Citrix Workspace conoce el almacén. Si es necesario, agréguelo mediante el comando siguiente:

```
./util/storebrowse --addstore \
```

1. Obtenga el ID único del escritorio o de la aplicación con que quiere conectarse. Esta es la primera cadena entre comillas en una línea adquirida en uno de los siguientes comandos:

- Lista de todos los escritorios y las aplicaciones en el servidor:

```
./util/storebrowse -E <store URL>
```

- Lista de los escritorios y las aplicaciones a los que se ha suscrito:

```
./util/storebrowse -S <store URL>
```

2. Ejecute el siguiente comando para iniciar el escritorio o la aplicación:

```
./util/storebrowse -L <desktop or application ID> <store URL>
```

Si no puede conectarse a un servidor, es posible que el administrador tenga que cambiar la ubicación del servidor o los detalles del proxy SOCKS. Para obtener más información, consulte [servidor proxy](#).

### Para crear una conexión desde un explorador web

Por regla general, la configuración para iniciar sesiones desde un explorador web se realiza automáticamente durante la instalación. Debido a la gran variedad de exploradores y sistemas operativos, puede ser necesaria alguna configuración manual.

Si configura de forma manual los archivos MAILCAP y MIME para Firefox, Mozilla o Chrome, utilice estas modificaciones para que los archivos ICA inicien el archivo ejecutable de la aplicación Citrix Workspace, wfica. Para utilizar otros exploradores, modifique la configuración del explorador, según corresponda.

1. Ejecute los siguientes comandos para una instalación de la aplicación Citrix Workspace sin privilegios de administrador. La configuración de ICAROOT se puede cambiar si se instala en una ubicación no predeterminada. Puede probar el resultado con el comando

```
xdg-mime query default application/x-ica, el cual debe devolver “wfica desktop”.
```

```
setenv ICAROOT=/opt/Citrix/ICAClient
```

```
xdg-icon-resource install --size 64
```

```
$ICAROOT/icons/000\\_Receiver_64.png Citrix Workspace app
```

```
xdg-mime default wfica.desktop application/x-ica
```

```
xdg-mime default new\\_store.desktop application/vnd.citrix.receiver.  
configure
```

2. Cree o extienda el archivo /etc/xdg/mimeapps.list (para la instalación de administrador) o \$HOME/.local/share/applications/mimeapps.list (mimeapps.list). El archivo debe comenzar por [Default Applications] y seguir con:

```
application/x-ica=wfica.desktop;
```

```
application/vnd.citrix.receiver.configure=new\\_store.desktop;
```

Quizá deba configurar la página Preferencias o Aplicaciones de Firefox.

Para “Citrix ICA settings file content”, seleccione:

- “Citrix Workspace app Engine (predeterminado)” en el menú desplegable

O bien:



- “Utilizar otros...” y, a continuación, seleccione el archivo `/usr/share/applications/wfica.desktop` (para una instalación de administrador de la aplicación Citrix Workspace)
- O bien:
- `$HOME/.local/share/applications/wfica.desktop` (para una instalación que sea de no administrador).

### Central de conexiones

Los usuarios pueden administrar sus conexiones activas con la Central de conexiones. La Central de conexiones es una herramienta de productividad que permite a usuarios y administradores solucionar inconvenientes en conexiones lentas o problemáticas. Con la Central de conexiones, los usuarios pueden administrar las conexiones de este modo:

- Cerrar aplicaciones.
- Cerrar la sesión. Este paso finaliza la sesión y cierra todas las aplicaciones que hubiera abiertas.
- Desconectarse de una sesión. Este paso interrumpe la conexión seleccionada con el servidor sin cerrar ninguna aplicación que haya abierta (a menos que el servidor esté configurado para cerrar aplicaciones en caso de desconexión).
- Ver estadísticas de transporte de la conexión.

### Administración de una conexión

Para administrar una conexión desde la **Central de conexiones**:

1. En el menú de la aplicación Citrix Workspace, haga clic en **Central de conexiones**.  
Aparecerán los servidores que se utilizan y todas las sesiones que están activas.
2. Lleve a cabo una de las siguientes acciones:
  - Seleccione un servidor, desconecte o cierre la sesión, o consulte sus propiedades.
  - Seleccione una aplicación, cierre la ventana.

## Configuración

July 30, 2021

Cuando se utiliza la aplicación Citrix Workspace para Linux, los siguientes pasos de configuración permiten a los usuarios acceder a sus aplicaciones y escritorios alojados.

## Parámetros

### Archivos de configuración

Para cambiar parámetros más avanzados o menos comunes, puede modificar los archivos de configuración de la aplicación Citrix Workspace. Estos archivos de configuración se leen cada vez que `wfica` se inicia. Puede actualizar varios archivos, según el efecto que quiera lograr con los cambios.

Si se pueden compartir sesiones, puede que se use una sesión existente en lugar de una recién configurada. Este parámetro puede hacer que la sesión ignore los cambios hechos en el archivo de configuración.

### Parámetros predeterminados

Si quiere que los cambios se apliquen a todos los usuarios de la aplicación Citrix Workspace, modifique el archivo de configuración `module.ini` del directorio `$ICAROOT/config`.

#### Nota:

Si una entrada en `All\\_Regions.ini` se establece en un valor específico, el valor de esa entrada en `module.ini` no se utiliza. Los valores indicados en `All\\_Regions.ini` tienen prioridad sobre el valor en `module.ini`.

### Archivo de plantilla

Si el archivo `$HOME/.ICAClient/wfclient.ini` no existe, `wfica` copia `$ICAROOT/config/wfclient.template` para crearlo. Cuando se realizan cambios en este archivo de plantilla, estos se aplican a todos los usuarios de la aplicación Citrix Workspace.

### Configuración de usuario

Para aplicar cambios de configuración a un usuario, modifique el archivo `wfclient.ini` en el directorio `$HOME/.ICAClient` del usuario. La configuración de este archivo se aplica a las conexiones futuras de ese usuario.

### Validación de las entradas del archivo de configuración

Para limitar los valores permitidos de las entradas en `wfclient.ini`, especifique las opciones o los intervalos de opciones que se permiten en `All\\_Regions.ini`.

Si solo especifica un valor posible, ese es el que se usa. Tenga en cuenta que `$HOME/.ICAClient/All\\_Regions.ini` solo puede coincidir con los valores posibles establecidos en `$ICAROOT/config/All\\_Regions.ini` o limitarlos, pero no puede quitarles las restricciones.

**Nota:**

El valor establecido en `wfclient.ini` tiene prioridad sobre el valor de `module.ini`.

## Parámetros

Los parámetros enumerados en cada archivo se agrupan en secciones. Cada sección comienza con un nombre entre corchetes que indica parámetros relacionados; por ejemplo, `\[ClientDrive\]` para los parámetros relacionados con la asignación de unidades del cliente (CDM).

Se proporcionan valores predeterminados automáticamente para los parámetros que falten excepto donde se indique. Si el parámetro está presente, pero no tiene ningún valor asignado, el valor predeterminado se aplica automáticamente. Por ejemplo, si `InitialProgram` va seguido de un signo igual (=), pero no hay ningún valor, se aplica el valor predeterminado para este parámetro (no ejecutar ningún programa después de iniciar sesión).

## Precedencia

`All\_Regions.ini` especifica parámetros que pueden definir otros archivos. Puede restringir los valores de los parámetros o establecerlos de forma precisa.

Para una conexión cualquiera, los archivos se comprueban por este orden:

1. `All\_Regions.ini`: Los valores de este archivo anulan los de:
  - El archivo ICA de conexiones
  - `wfclient.ini`
2. `module.ini`: Los valores de este archivo se utilizan si no se han definido en `All\_Regions.ini`, el archivo ICA de conexiones o `wfclient.ini`, pero no están limitados por entradas de `All\_Regions.ini`.

Si no se encuentra ningún valor en ninguno de estos archivos, se usa el valor predeterminado en el código de la aplicación Citrix Workspace.

**Nota:**

Hay excepciones en este orden de prioridad. Por ejemplo, el código lee algunos valores específicamente de `wfclient.ini` por razones de seguridad.

## Continuidad del servicio (versión Technical Preview pública)

**Nota:**

Esta función se halla actualmente en versión Technical Preview pública para la aplicación Citrix Workspace.

La continuidad del servicio elimina o minimiza la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Los usuarios pueden iniciar sus aplicaciones y escritorios virtuales, independientemente del estado de los servicios en la nube.

Para obtener información sobre los requisitos que permiten la continuidad del servicio en la aplicación Citrix Workspace, consulte [Requisitos del sistema](#).

Para obtener información sobre la instalación de la continuidad del servicio con la aplicación Citrix Workspace, consulte [Instalar Continuidad del servicio](#).

Para obtener más información, consulte la sección [Continuidad del servicio](#) de la documentación de Citrix Workspace.

### Anclar el diseño de pantalla con varios monitores

A partir de la versión 2103, puede guardar la selección del diseño de pantalla con varios monitores. El diseño es la manera en que se muestra una sesión de escritorio. Anclarlo ayuda a reiniciar una sesión con el diseño seleccionado, lo que ofrece una mejor experiencia de usuario.

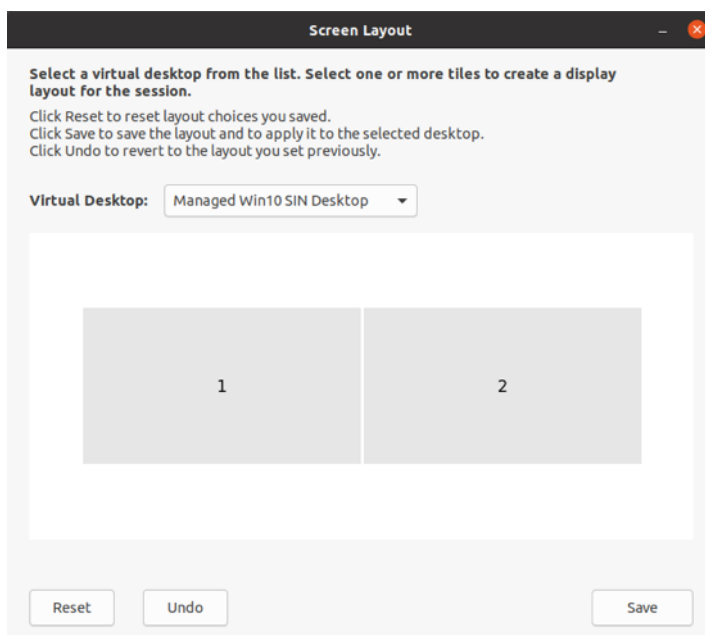
Como requisito previo, debe habilitar esta función en el archivo `AuthManConfig.xml`. Vaya a `§ICAROOT/config/AuthManConfig.xml` y agregue estas entradas:

```
1 <key>ScreenPinEnabled</key>
2 <value> true </value>
```

Solo después de agregar la clave anterior, podrá ver la opción **Diseño de pantalla** en el icono del indicador de aplicaciones. Para obtener más información sobre el icono del indicador de aplicaciones, consulte [Icono del indicador de aplicaciones](#).

Para seleccionar el diseño de la pantalla, haga clic en el icono del indicador de aplicaciones en la barra de tareas y seleccione **Diseño de pantalla**. Aparece el cuadro de diálogo **Diseño de pantalla**.

Si no, para abrir el cuadro de diálogo **Diseño de pantalla**, también puede presionar **Ctrl + M** cuando se encuentre en la ventana de autoservicio.



Seleccione un escritorio virtual en el menú desplegable. La selección del diseño se aplica solamente al escritorio que seleccione.

Seleccione uno o varios mosaicos para formar una selección rectangular del diseño. A continuación, la sesión se muestra según la selección del diseño.

### **Limitaciones:**

- Al habilitar el anclaje de pantalla, se inhabilita la función para guardar el diseño durante las sesiones.
- Esta función solo se aplica a escritorios marcados como favoritos.

### **Protección de aplicaciones [Función experimental](#)**

#### **Nota:**

- Esta función está disponible cuando la aplicación Citrix Workspace se instala mediante los paquetes tarball, Debian y Red Hat Package Manager (RPM). Además, x64 y armhf son las únicas arquitecturas compatibles.
- Esta función está disponible en implementaciones locales de Citrix Virtual Apps and Desktops y Citrix Virtual Apps and Desktops Service con StoreFront.

La protección de aplicaciones es una función adicional que proporciona una mayor seguridad al usar Citrix Virtual Apps and Desktops. La función restringe la posibilidad de que los clientes puedan verse amenazados por malware de registro de pulsaciones de teclas y malware de capturas de pantalla. La protección de aplicaciones evita la exfiltración de información confidencial, como credenciales de usuario e información confidencial mostrada en la pantalla. La función evita que los usuarios y los atacantes hagan capturas de pantalla y usen registradores de pulsaciones de teclas para obtener y

explotar información confidencial.

**Requisito previo:**

Ubuntu 18.04 o una versión posterior.

**Instalación del componente de protección de aplicaciones:**

Al instalar la aplicación Citrix Workspace con el paquete tarball, aparece el mensaje siguiente.

“¿Quiere instalar el componente de protección de aplicaciones? Advertencia: No puede inhabilitar esta función. Para inhabilitarla, debe desinstalar la aplicación Citrix Workspace. Para obtener más información, póngase en contacto con el administrador de sistemas. [\$INSTALLER\_N predeterminado]:”

Introduzca **Y** para instalar el componente de protección de aplicaciones.

De forma predeterminada, el componente de protección de aplicaciones no está instalado.

Reinicie la máquina para que los cambios surtan efecto. Es posible que la protección de aplicaciones no funcione como es debido a menos que reinicie la máquina.

**Instalación del componente de protección de aplicaciones en paquetes RPM:**

A partir de la versión 2104, la protección de aplicaciones se ofrece en la versión RPM de la aplicación Citrix Workspace.

Para instalar la protección de aplicaciones, haga esto:

1. Al instalar la aplicación Citrix Workspace.
2. Instale el paquete `ctxappprotection<version>.rpm` de protección de aplicaciones desde el instalador de la aplicación Citrix Workspace.
3. Reinicie el sistema para que los cambios surtan efecto.

**Instalación del componente de protección de aplicaciones en paquetes Debian:**

A partir de la versión 2101, la protección de aplicaciones se ofrece en la versión Debian de la aplicación Citrix Workspace.

Para una instalación silenciosa del componente de protección de aplicaciones, ejecute el siguiente comando desde el terminal antes de instalar la aplicación Citrix Workspace:

```
1 export DEBIAN_FRONTEND="noninteractive"
2 sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select no"
3
4 sudo debconf-show icaclient
5 * app_protection/install_app_protection: no
6
```

```
7 sudo apt install -f ./icaclient_<version>._amd64.deb
```

A partir de la versión 2106, la aplicación Citrix Workspace presenta una opción que le permite configurar las funciones de protección contra el registro de teclado y protección contra capturas de pantalla por separado para las interfaces del administrador de autenticación y del Self-Service Plug-in.

### Configuración de la protección de aplicaciones para el administrador de autenticación:

Vaya a `$(ICAROOT)/config/AuthManConfig.xml` y modifique el archivo de esta manera:

```
1 /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
  authmananti -A 1
2 <key>AuthManAntiScreenCaptureEnabled</key>
3 <value>true</value>
4 <key>AuthManAntiKeyLoggingEnabled</key>
5 <value>true </value>
```

### Configuración de la protección de aplicaciones para la interfaz del Self-Service Plug-in:

Vaya a `$(ICAROOT)/config/AuthManConfig.xml` y modifique el archivo de esta manera:

```
1 /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
  protection -A 4
2 <!-- Selfservice app protection configuration -->
3 <Selfservice>
4 <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
5 <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
6 </Selfservice>
```

### Problemas conocidos:

- Al minimizar una pantalla protegida, la protección de aplicaciones continúa ejecutándose en segundo plano.

### 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 aparece en los agentes VDA de servidor.

El indicador de estado de la batería está habilitado de forma predeterminada.

Para inhabilitar el indicador de estado de la batería:

1. Vaya a la carpeta <ICAROOT>/config/module.ini.
2. Vaya a la sección `ICA 3.0`.
3. Configure esta opción: `MobileReceiver= Off`.

## 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 para Linux y envía esos datos automáticamente a Google Analytics.	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](#).

Citrix también utiliza Google Analytics para recopilar determinados datos de la aplicación Citrix Workspace como parte del programa CEIP. Consulte cómo gestiona Google [los datos recopilados para Google Analytics](#).

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

1. Vaya a la carpeta `\<ICAROOT\>/config/module.ini` y vaya a la sección `CEIP`.
2. Seleccione la entrada `EnableCeip` y establézcala en `Disable`.

#### Nota:

Una vez establecida la clave `EnableCeip` en `Disable`, si quiere inhabilitar el envío de los dos últimos elementos de datos de CEIP que recopila Google Analytics (es decir, la versión del sis-



tema operativo y la versión de la aplicación Workspace), vaya a la siguiente sección y configure el valor como se sugiere:

**Ubicación:** <ICAROOT>/config/module.ini

**Sección:** GoogleAnalytics

**Entrada:** DisableHeartBeat

**Valor:** True

Elementos concretos de datos CEIP recopilados por Google Analytics:

---

Versión del sistema operativo*	Versión de la aplicación Workspace*	Nombre de la aplicación	ID de cliente
Método de inicio de sesiones	Versión del compilador	Plataforma de hardware	

---

### Icono del indicador de aplicaciones

El indicador de aplicaciones se inicia cuando se abre la aplicación Citrix Workspace. Es un icono que está presente en el área de notificaciones. Con la introducción del indicador de aplicaciones, mejora el rendimiento del inicio de sesión de la aplicación Citrix Workspace para Linux.

Puede constatar la mejora del rendimiento en estos casos:

- Primer inicio de la aplicación Citrix Workspace
- Cerrar la aplicación y volver a iniciarla
- Salir de la aplicación y volver a iniciarla

#### Nota:

El paquete `libappindicator` es necesario para que el indicador de aplicaciones aparezca. Instale desde la web el paquete `libappindicator` adecuado para su distribución de Linux.

### Proxy de ICA a X

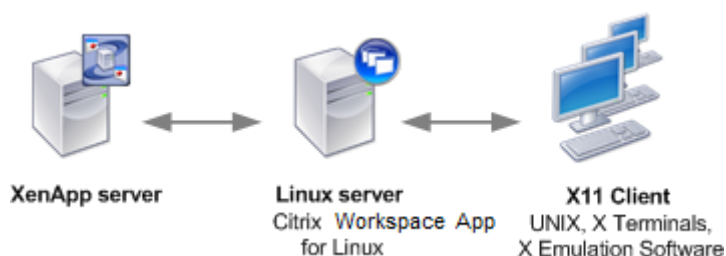
Puede utilizar una estación de trabajo que ejecuta la aplicación Citrix Workspace como servidor y redirigir la salida a otro dispositivo compatible con X11. Se recomienda realizar esto para entregar aplicaciones de Microsoft Windows a terminales X o estaciones de trabajo UNIX en las que la aplicación Citrix Workspace no está disponible.

### Nota:

El software de la aplicación Citrix Workspace está disponible para muchos dispositivos X y en esos casos la mejor solución es instalar el software en los dispositivos. Esta forma de ejecutar la aplicación Citrix Workspace, como proxy de ICA a X, se conoce también como ICA en el lado del servidor.

Cuando se ejecuta la aplicación Citrix Workspace, se la puede considerar como un convertor de ICA a X11 que dirige la salida de X11 al escritorio de Linux local. Sin embargo, también es posible redirigir la salida a otra pantalla de X11. Puede ejecutar simultáneamente varias copias de la aplicación Citrix Workspace en un sistema, para que cada una de ellas envíe su salida a un dispositivo diferente.

En este gráfico se muestra un sistema con la aplicación Citrix Workspace para Linux configurado como proxy de ICA a X:



Para configurar este tipo de sistema, necesita un servidor Linux que actúe como el proxy de ICA a X11:

- Si ya tiene terminales X, puede ejecutar la aplicación Citrix Workspace en el servidor Linux que normalmente proporciona las aplicaciones X para los terminales X.
- Si quiere implementar estaciones de trabajo UNIX en las que la aplicación Citrix Workspace no está disponible, necesita tener un servidor adicional que actúe como proxy. Esta función puede cumplirla un PC que ejecute Linux.

El dispositivo final recibe las aplicaciones a través de X11 gracias al protocolo ICA. De forma predeterminada, puede utilizar la asignación de unidades solamente para acceder a las unidades en el proxy. Esto no supone ningún problema si utiliza terminales X que, por lo general, no tienen unidades locales. Si distribuye aplicaciones a otras estaciones de trabajo UNIX, puede:

- Montar la estación de trabajo UNIX local mediante NFS como proxy en la estación de trabajo y, a continuación, apuntar una asignación de unidad del cliente al punto de montaje NFS en el proxy.
- Utilizar un proxy de NFS a SMB, como SAMBA, o bien un cliente NFS en el servidor, como Microsoft Services para UNIX.

Algunas funciones no se transfieren al dispositivo final:

- Redirección de USB
- Redirección de tarjetas inteligentes
- Redirección de puertos COM

- No se transfiere sonido al dispositivo X11, aunque el servidor que actúa como proxy admita sonido.
- Las impresoras de los clientes no se transfieren al dispositivo X11. Acceda manualmente a la impresora de UNIX desde el servidor a través de la impresión LPD, o bien utilice una impresora de red.
- No se espera que la redirección de entrada multimedia funcione porque requiere una cámara web en la máquina que ejecuta la aplicación Citrix Workspace, que es el servidor que actúa como un proxy. Sin embargo, la redirección de salida multimedia funciona con GStreamer instalado en el servidor que actúa como proxy (no comprobado).

Para iniciar la aplicación Citrix Workspace con ICA en el lado del servidor desde un terminal X o una estación de trabajo UNIX:

1. Utilice ssh o telnet para conectarse al dispositivo que actúa como proxy.
2. En un intérprete de comandos del dispositivo proxy, configure la variable de entorno **DISPLAY** para el dispositivo local. Por ejemplo, en un intérprete de comandos de C, escriba:

```
setenv DISPLAY <local:0>
```

**Nota:**

Si utiliza el comando `ssh -X` para conectarse al dispositivo que hace de proxy, no es necesario establecer la variable de entorno **DISPLAY**.

3. En un símbolo del sistema del dispositivo local, escriba `xhost <nombre del servidor proxy>`
4. Si la aplicación Citrix Workspace no se instaló en el directorio de instalación predeterminado, asegúrese de que la variable de entorno `ICAROOT` esté configurada para apuntar al directorio de instalación real.
5. Ubique el directorio donde está instalada la aplicación Citrix Workspace. En la línea de comandos, escriba `selfservice &`.

### Redirección de contenido servidor-cliente

La redirección de contenido servidor-cliente permite que los administradores especifiquen que las URL en aplicaciones publicadas se abran con aplicaciones locales. Por ejemplo, cuando se abre un enlace correspondiente a una página Web mientras se utiliza Microsoft Outlook en una sesión, el archivo se abre en el explorador web del dispositivo del usuario. La redirección de contenido servidor-cliente permite que los administradores asignen recursos de Citrix de forma más eficiente, para brindar un mejor rendimiento a los usuarios.

Los siguientes tipos de URL pueden redirigirse:

- HTTP
- HTTPS

- RTSP (Real Player)
- RTSPU (Real Player)
- PNM (versiones anteriores de Real Player)

Si la aplicación Citrix Workspace para Linux no tiene una aplicación apropiada o no puede acceder directamente al contenido, la URL se abre con la aplicación del servidor.

La redirección de contenido servidor-cliente se configura en el servidor y se habilita de forma predefinida en la aplicación Citrix Workspace siempre que la ruta incluya RealPlayer y al menos una de las siguientes opciones: Firefox, Mozilla o Netscape.

Para habilitar la redirección de contenido servidor-cliente si en la ruta no se encuentran RealPlayer ni un explorador

1. Abra el archivo de configuración `wfclient.ini`.
2. En la sección [Browser], modifique los siguientes parámetros:

Path=path

Command=command

donde “ruta” es el directorio donde está ubicado el archivo ejecutable del explorador y “comando” es el nombre del archivo ejecutable utilizado para controlar las URL de exploradores redirigidas, junto a la URL enviada por el servidor. Por ejemplo:

`$(ICAROOT)/nslaunch Netscape, Firefox, Mozilla`

- 1 Este parámetro especifica lo siguiente:
- 2
- 3 - Se ejecuta la utilidad “nslaunch” para insertar la URL en una ventana existente del explorador web.
- 4 - Se prueba cada explorador web de la lista, uno por uno, hasta que pueda mostrarse el contenido de forma correcta.

1. En la sección [Player], modifique los siguientes parámetros:

Path=path

Command=command

donde ruta es el directorio donde está ubicado el archivo ejecutable de RealPlayer y comando es el nombre del archivo ejecutable utilizado para controlar las URL multimedia redirigidas, junto a la URL enviada por el servidor.

2. Guarde el archivo y ciérrelo.

**Nota:**

En el caso de los dos parámetros Path, solo es necesario especificar el directorio donde están ubicados los archivos ejecutables del explorador y de RealPlayer. No es necesario especificar la ruta completa a los archivos ejecutables. Por ejemplo, en la sección [Browser], la ruta puede configurarse como /usr/X11R6/bin en lugar de /usr/X11R6/bin/netscape. Además, puede especificar varios nombres de directorios en una lista de elementos separados con dos puntos. Si no se especifican estos parámetros, se utilizará la ruta \$PATH actual del usuario.

Para inhabilitar la redirección de contenido servidor-cliente desde Citrix Workspace:

1. Abra el archivo de configuración module.ini.
2. Cambie el parámetro CREnabled a Off.
3. Guarde el archivo y ciérrelo.

## Conexión

### Configuración de conexiones

En dispositivos con una capacidad de procesamiento limitada o un ancho de banda limitado, se intercambia rendimiento por funcionalidad y viceversa. Los usuarios y los administradores pueden elegir una combinación aceptable de funcionalidad y rendimiento interactivo. Llevando a cabo al menos uno de estos cambios, a menudo en el servidor y no en el dispositivo del usuario, se puede reducir el ancho de banda requerido para la conexión y se puede mejorar el rendimiento:

- **Habilite la reducción de retardo SpeedScreen:** la reducción de retardo SpeedScreen mejora el rendimiento en conexiones con altos niveles de latencia al proporcionar comentarios instantáneos al usuario en respuesta a los datos introducidos o a las acciones con el puntero. Use el Administrador de reducción de retardo SpeedScreen para habilitar esta función en el servidor. En la aplicación Citrix Workspace, de forma predeterminada, esta opción está inhabilitada para el teclado y solo está habilitada para el puntero en conexiones con una latencia elevada. Consulte la guía de referencia de OEM de la aplicación Citrix Workspace para Linux (en inglés).
- **Habilite la compresión de datos:** la compresión de datos reduce la cantidad de datos transferidos a través de la conexión. Esto requiere recursos adicionales del procesador para comprimir y descomprimir datos, pero puede aumentar el rendimiento en conexiones de poco ancho de banda. Use las configuraciones de directiva de Citrix **Calidad de sonido y Compresión de imágenes** para habilitar esta función.
- **Reduzca el tamaño de la ventana:** cambie la dimensión de la ventana al tamaño utilizable más pequeño posible. En la comunidad, defina las opciones de sesión.
- **Reduzca la cantidad de colores:** reduzca la cantidad de colores a 256. En el sitio de Citrix Virtual Apps and Desktops, configure las opciones de la sesión.
- **Reduzca la calidad de sonido:** si la asignación de sonido está habilitada, reduzca la calidad

de sonido al parámetro más bajo mediante la configuración de directiva de Citrix Calidad de sonido.

## Fuente

### Suavizado de fuentes ClearType

El suavizado de fuentes ClearType (también conocido como presentación de fuentes de subpíxel) mejora la calidad de las fuentes en pantalla más allá de las posibilidades que permite el suavizado de fuentes estándar o “anti-aliasing”. Puede activar o desactivar esta función. También puede especificar el tipo de suavizado si modifica este parámetro en la sección [WFClient] del archivo de configuración apropiado:

FontSmoothingType = número

Donde “número” puede ser uno de los siguientes valores:

Valor	Comportamiento
0	Se usa la preferencia local existente en el dispositivo. Este valor está definido por el parámetro FontSmoothingTypePref.
1	Sin suavizado
2	Suavizado estándar
3	Suavizado ClearType (subpíxel horizontal)

Tanto el suavizado estándar como el suavizado ClearType pueden aumentar los requisitos de ancho de banda de la aplicación Citrix Workspace.

#### Importante:

El servidor puede configurar FontSmoothingType mediante el archivo ICA. Esto tiene prioridad sobre el valor que esté definido en [WFClient].

Si el servidor establece el valor en 0, la preferencia local está determinada por otro parámetro en [WFClient]:

FontSmoothingTypePref = número

Donde el número puede ser uno de estos valores:

Valor	Comportamiento
0	Sin suavizado

Valor	Comportamiento
1	Sin suavizado
2	Suavizado estándar
3	Suavizado ClearType (subpíxel horizontal) (valor predeterminado)

## Carpeta

### Configuración de la redirección de carpetas especiales

En este contexto, existen solo dos carpetas especiales por usuario:

- La carpeta Escritorio del usuario
- La carpeta Documentos del usuario (Mis Documentos en Windows XP)

La redirección de carpetas especiales le permite especificar las ubicaciones de las carpetas especiales de un usuario para que permanezcan fijas en diferentes tipos de servidores y configuraciones de comunidades de servidores. Esto es particularmente importante si, por ejemplo, un usuario móvil inicia sesión en servidores de distintas comunidades de servidores. En el caso de estaciones de trabajo estáticas y basadas en escritorios, donde el usuario puede iniciar sesión en servidores que residen en una sola comunidad de servidores, la redirección de carpetas especiales rara vez es necesaria.

Para configurar la redirección de carpetas especiales:

A continuación, dispone de un procedimiento en dos partes. En primer lugar, debe habilitar la redirección de carpetas especiales a través de una entrada en `module.ini`; a continuación, debe especificar las ubicaciones de las carpetas en la sección `[WFClient]`, según se describe aquí:

1. Agregue el siguiente texto en `module.ini` (por ejemplo, `$ICAROOT/config/module.ini`):

```
[ClientDrive]
```

```
SFRAllowed = True
```

2. Agregue el texto siguiente en la sección `[WFClient]` (por ejemplo, `$HOME/.ICAClient/wfclient.ini`):

```
DocumentsFolder = documentos
```

```
DesktopFolder = escritorio
```

Donde “documentos” y “escritorio” son los nombres de archivo de UNIX, incluida la ruta completa, de los directorios que quiere utilizar como las carpetas Escritorio y Documentos respectivamente de los usuarios. Por ejemplo:

```
DesktopFolder = $HOME/.ICAClient/desktop
```

- Puede especificar cualquier componente en la ruta con una variable de entorno, por ejemplo, \$HOME.
- Debe especificar valores para ambos parámetros.
- Los directorios que especifique deben estar disponibles a través de la asignación de dispositivos del cliente. Es decir, el directorio debe estar en el subárbol de un dispositivo cliente asignado.
- Como letras de unidad, debe utilizar C o letras posteriores.

### Asignación de unidades de cliente

La asignación de unidades del cliente permite redirigir letras de unidades del servidor de Citrix Virtual Apps o al de Citrix Virtual Desktops a directorios existentes en el dispositivo del usuario local. Por ejemplo, la unidad H: de una sesión de usuario de Citrix se puede asignar a un directorio en el dispositivo del usuario local que ejecuta la aplicación Workspace.

La asignación de unidades del cliente puede hacer que cualquier directorio montado en el dispositivo del usuario local, incluidos CD-ROM, DVD o dispositivos USB portátiles, esté disponible para el usuario durante una sesión, siempre que el usuario local tenga permiso para acceder a él. Cuando un servidor está configurado para permitir la asignación de unidades del cliente, los usuarios pueden acceder a los archivos guardados localmente, trabajar con ellos durante su sesión y, luego, guardarlos nuevamente en una unidad local o en una unidad del servidor.

La aplicación Citrix Workspace admite la asignación de dispositivos del cliente para conexiones a servidores Citrix Virtual Apps and Desktops. La asignación de dispositivos del cliente permite que una aplicación remota que se ejecuta en el servidor acceda a dispositivos conectados al dispositivo del usuario local. El usuario puede usar las aplicaciones y los recursos del sistema como si se ejecutaran localmente. Antes de utilizar estas funciones, asegúrese de que el servidor admita la asignación de dispositivos del cliente.

#### Nota:

El modelo de seguridad SELinux, Security-Enhanced Linux, puede afectar al funcionamiento de la asignación de unidades del cliente y la redirección de USB (tanto en Citrix Virtual Apps como en Virtual Desktops). Si se requieren estas funciones, inhabilite SELinux antes de configurarlas en el servidor.

Existen dos tipos de asignación de unidades disponibles:

- Asignación estática de unidades del cliente: Permite que los administradores asignen cualquier parte del sistema de archivos del dispositivo del usuario a una letra de unidad especificada en el servidor cuando se inicia la sesión. Por ejemplo, puede utilizarse para asignar total o parcialmente el directorio de inicio (home) o /tmp de un usuario, y también los puntos de montaje de dispositivos de hardware como CD-ROM, DVD o dispositivos de memoria USB.



- **Asignación dinámica de unidades del cliente:** Supervisa los directorios en los que, por lo general, los dispositivos de hardware como CD-ROM, DVD y dispositivos USB portátiles se montan en el dispositivo del usuario. Y todos los dispositivos nuevos que aparezcan durante una sesión se asignan automáticamente a la siguiente letra de unidad disponible en el servidor.

Cuando la aplicación Citrix Workspace se conecta a Citrix Virtual Apps o a Citrix Virtual Desktops, se restablecen las asignaciones de unidades del cliente a menos que la asignación de dispositivos del cliente esté inhabilitada. También pueden utilizarse directivas para tener mayor control sobre la forma en que se aplica la asignación de dispositivos del cliente. Para obtener más información, consulte la documentación del [Citrix Virtual Apps and Desktops](#).

Los usuarios pueden asignar unidades mediante el cuadro de diálogo Preferencias.

**Nota:**

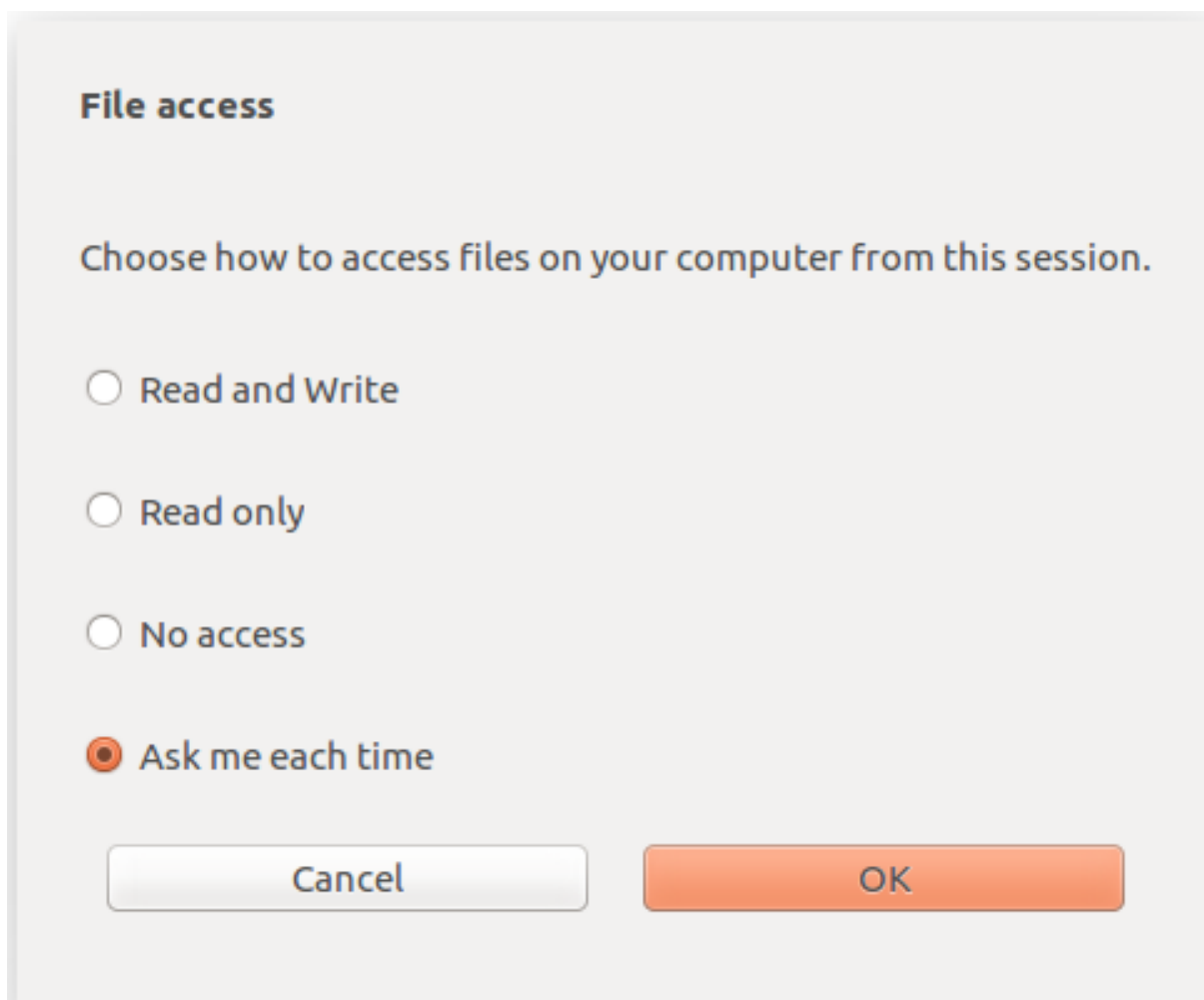
De manera predeterminada, al habilitar la asignación estática de unidades del cliente también se habilita la asignación dinámica de unidades del cliente. Para inhabilitar esta última pero habilitar la primera, establezca `Dynami cCDM` en `False` en `wfclient.ini`.

Anteriormente, la configuración del acceso a archivos a través de CDM se aplicaba a todos los almacenes configurados.

A partir de la versión 2012, la aplicación Citrix Workspace le permite configurar el acceso a archivos CDM por almacén.

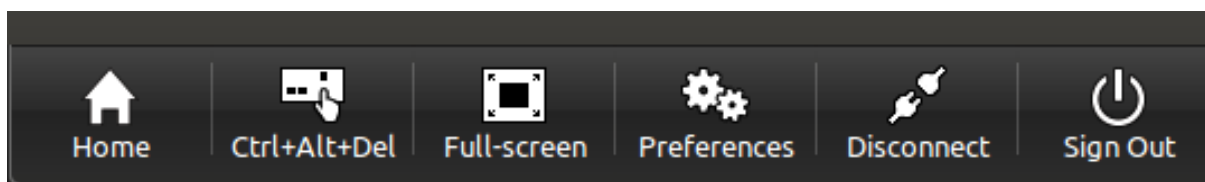
**Nota:**

La configuración de acceso a archivos no es persistente en todas las sesiones cuando se utiliza Workspace para Web. De forma predeterminada, se utiliza la opción **Preguntarme cada vez**.

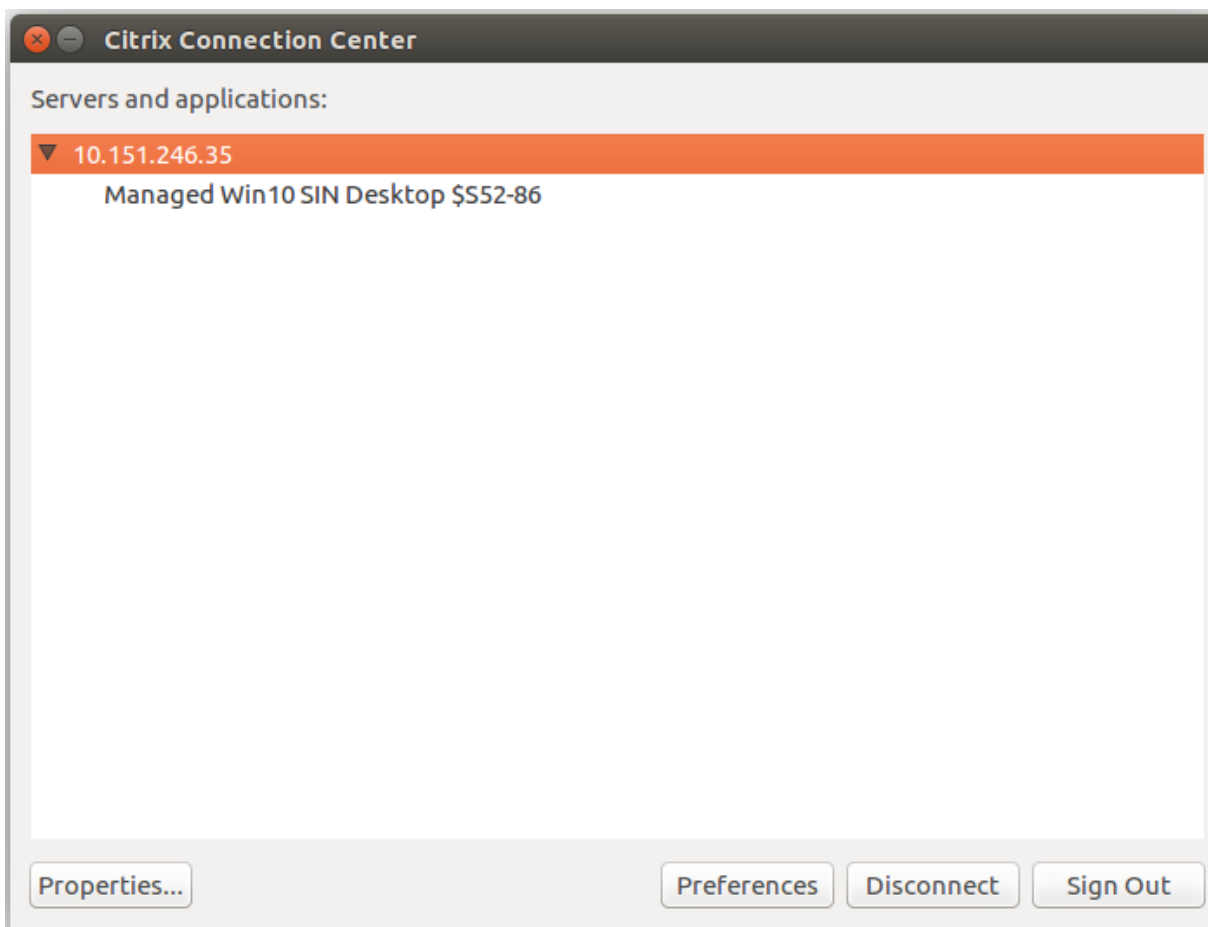


Puede utilizar el archivo `wfclient.ini` para configurar los atributos de la ruta asignada y el nombre de archivo. Utilice la GUI para establecer un nivel de acceso a archivos como se muestra en la captura de pantalla anterior.

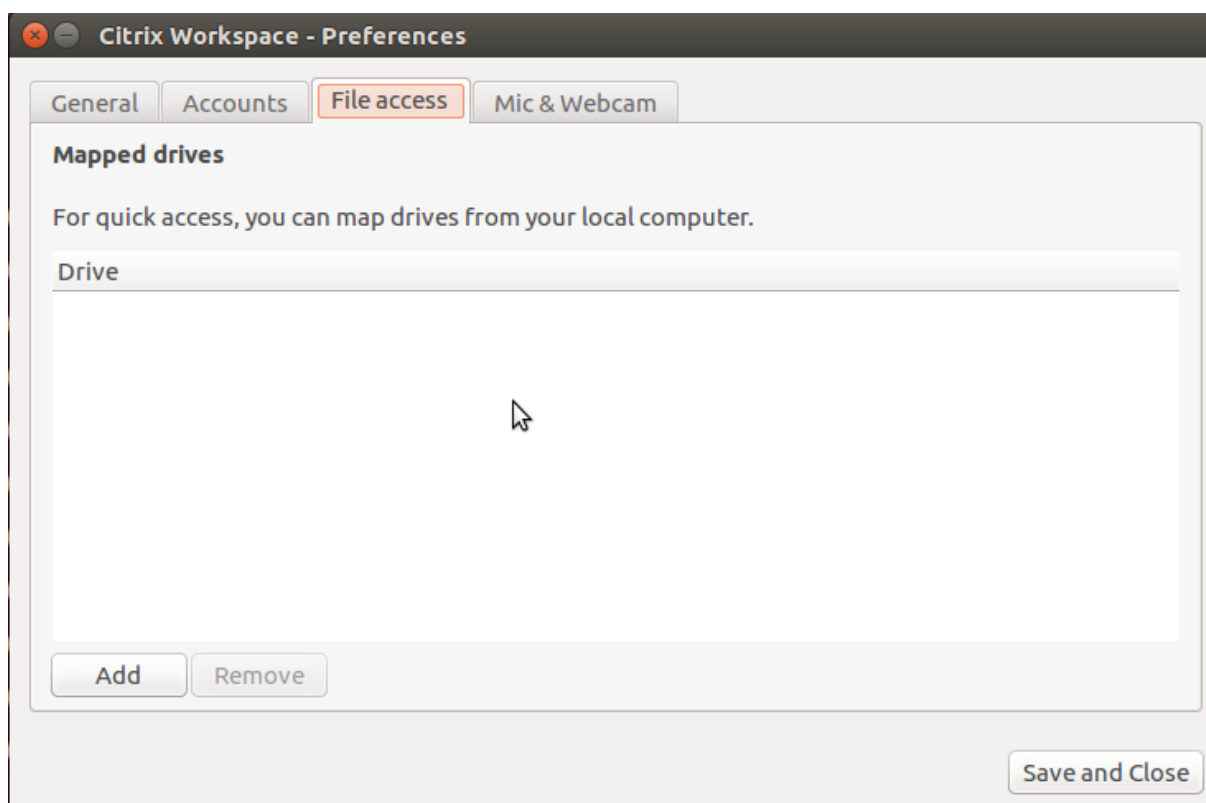
En una sesión de escritorio, para establecer un nivel de acceso a archivos, vaya a **Preferencias** > cuadro de diálogo **Acceso a archivos** desde Desktop Viewer.



En una sesión de aplicación, para establecer un nivel de acceso a archivos, abra el cuadro de diálogo **Acceso a archivos** desde la **Central de conexiones de Citrix**.



El cuadro de diálogo **Acceso a archivos** incluye el nombre de la carpeta asignada y su ruta.



El indicador del nivel de acceso ya no se admite en el archivo `wfclient.ini`.

### Asignar impresoras del cliente

La aplicación Citrix Workspace admite la impresión en impresoras de red e impresoras conectadas localmente a los dispositivos de usuario. De forma predeterminada, a menos que se creen directivas para modificarlo, Citrix Virtual Apps permite a los usuarios:

- Imprimir en todos los dispositivos de impresión accesibles desde el dispositivo de usuario.
- Agregar impresoras

Sin embargo, es posible que estos parámetros no sean los adecuados para todos los entornos. Por ejemplo, la configuración predeterminada que permite a los usuarios imprimir en todas las impresoras accesibles desde el dispositivo de usuario es la más fácil de administrar inicialmente. Sin embargo, esa configuración predeterminada puede crear inicios de sesión lentos en algunos entornos. En esa situación, quizá le interese limitar la lista de impresoras configuradas en el dispositivo del usuario.

También es posible que las directivas de seguridad de la empresa no permitan que los usuarios asignen puertos locales de impresión. Para ello, en el servidor, configure la directiva de ICA Conectar automáticamente puertos COM del cliente como Inhabilitada.

Para limitar la lista de impresoras configuradas en el dispositivo del usuario:

1. Abra el archivo de configuración, `wfclient.ini`, en uno de los siguientes directorios:

- \$HOME/.ICAClient, para limitar las impresoras de un solo usuario
  - \$ICAROOT/config, para limitar las impresoras de todos los usuarios de la aplicación Workspace. En este caso, “todos los usuarios” se refiere a los primeros que usan el programa self-service después del cambio.
2. En la sección [WFClient] del archivo, escriba:  

```
ClientPrinterList=impresora1:impresora2:impresora3
```

Donde impresora1, impresora2 y sucesivos son los nombres de las impresoras elegidas. Separe los nombres de las impresoras con dos puntos (:).
  3. Guarde el archivo y ciérrelo.

### Asignación de impresoras del cliente en UNIX

En un entorno UNIX, se ignoran los controladores de impresora definidos por la aplicación Citrix Workspace. El sistema de impresión en el dispositivo del usuario debe tener la capacidad de manejar el formato de impresión generado por la aplicación.

Antes de que los usuarios puedan utilizar una impresora del cliente desde Citrix Virtual Apps para UNIX, el administrador debe habilitar la impresión. Para obtener más información, consulte la sección Citrix Virtual Apps para UNIX de la documentación de [Citrix Virtual Apps and Desktops](#).

### Asignación de una impresora local

La aplicación Citrix Workspace para Linux admite el controlador de impresora universal PS de Citrix. De modo que, en la mayoría de los casos, no se requiere ninguna configuración local para que los usuarios utilicen impresoras de red o impresoras conectadas localmente a los dispositivos de usuario. Sin embargo, puede asignar manualmente impresoras del cliente en Citrix Virtual Apps para Windows si, por ejemplo, el software de impresión del dispositivo del usuario no admite el controlador de impresora universal.

Para asignar una impresora local en un servidor:

1. En la aplicación Citrix Workspace, establezca una conexión de servidor e inicie sesión en un equipo que ejecute Citrix Virtual Apps.
2. En el menú Inicio, seleccione **Configuración > Impresoras**.
3. En el menú Archivo, seleccione **Agregar impresora**.  
Aparecerá el asistente Agregar impresora.
4. Utilice el asistente para agregar una impresora de red desde la red del cliente, dominio del cliente. Por lo general, este es un nombre de impresora estándar, similar a las creadas por Servicios de Escritorio remoto nativos, como “HP LaserJet 4 de nombre\_cliente en sesión 3”.

Para obtener más información sobre cómo agregar impresoras, consulte la documentación de su sistema operativo Windows.

## Sonido

Antes solo se asignaba el dispositivo de audio predeterminado en una sesión aunque hubiera muchos dispositivos disponibles en la máquina. Por regla general, el dispositivo asignado aparecía como **Citrix HDX Audio**.

A partir de la versión 2010, la aplicación Citrix Workspace para Linux muestra todos los dispositivos de audio locales disponibles en una sesión. En lugar de **Citrix HDX Audio**, ahora aparecen con sus respectivos nombres de dispositivo. Puede cambiar a cualquiera de los dispositivos disponibles de forma dinámica en una sesión. A diferencia de las versiones anteriores, ahora no es necesario seleccionar la entrada o salida de audio predeterminada antes de iniciar la sesión. Las sesiones se actualizan dinámicamente al conectar o quitar dispositivos de audio.

A partir de la versión 2012, la función de redirección de audio mejorada está habilitada de forma predeterminada.

Para inhabilitar esta función, haga lo siguiente:

1. Vaya a la carpeta `<ICAROOT>/config/` y abra el archivo `module.ini`.
2. Vaya a la sección `clientaudio` y agregue la siguiente entrada:

```
VdcamVersion4Support=False
```

### Nota:

- Cuando la función de redirección de audio mejorada está inhabilitada, solo aparece en la sesión el dispositivo de audio predeterminado con el nombre **Citrix HDX Audio**.
- La opción **Micrófono y cámara web** del cuadro de diálogo **Preferencias** permanece desactivada de forma predeterminada. Para obtener información sobre cómo habilitar el micrófono y la cámara web, consulte [Preferencias](#).

### Limitaciones conocidas:

- En un VDA con Windows Server 2016, no se puede cambiar la selección del dispositivo de audio en una sesión. La selección se establece solo en la entrada y salida de audio predeterminada.
- La redirección de dispositivos de audio no es compatible con HDMI ni dispositivos de audio Bluetooth.
- Puede cambiar el dispositivo de audio predeterminado solo en el sistema operativo Windows 10, Windows 7 y Windows 8. En los sistemas operativos de servidor Windows (como Windows Server 2012, 2016, 2019), no se puede cambiar el dispositivo de audio predeterminado debido a una limitación en las sesiones de Escritorio remoto de Microsoft.

Por lo general, el dispositivo de sonido predeterminado es el dispositivo ALSA predeterminado configurado para el sistema. Utilice el siguiente procedimiento para especificar un dispositivo diferente:

1. Elija y abra un archivo de configuración teniendo en cuenta los usuarios que quiera afectar con sus cambios. Para obtener más información sobre la forma en que las actualizaciones a archivos de configuración específicos afectan a los diferentes usuarios, consulte los [parámetros predeterminados](#).
2. Agregue la siguiente opción y cree la sección si es necesario:

```
1 [ClientAudio]
2
3 AudioDevice = <device>
```

Donde la información de dispositivo está ubicada en el archivo de configuración de ALSA del sistema operativo.

**Nota:**

La ubicación de esta información no es estándar en todos los sistemas operativos Linux. Citrix le recomienda consultar la documentación del sistema operativo para obtener más detalles sobre cómo ubicar esta información.

### Asignación de sonido del cliente

La asignación de sonido del cliente permite que las aplicaciones que se ejecutan en el servidor de Citrix Virtual Apps o Citrix Virtual Desktops reproduzcan sonido a través de dispositivos de sonido instalados en el dispositivo de usuario. Puede definir la calidad del sonido para cada conexión en el servidor, pero los usuarios también pueden definirla en el dispositivo del usuario. Si los parámetros de calidad de sonido del dispositivo de usuario y del servidor son diferentes, se utilizará el parámetro de calidad más bajo.

La asignación de sonido del cliente puede suponer una carga excesiva para los servidores y para la red. Cuanto mayor es la calidad de sonido, mayor ancho de banda se requiere para transferir los datos de sonido. El sonido de calidad más alta también consume más recursos de la CPU para su procesamiento.

Configure la asignación de sonido del cliente a través de directivas. Para obtener más información, consulte la documentación del [Citrix Virtual Apps and Desktops](#).

**Nota:**

La asignación de sonido del cliente no se ofrece en conexiones a Citrix Virtual Apps para UNIX.

## Habilitación del sonido UDP

El sonido UDP puede mejorar la calidad de las llamadas telefónicas que se realizan a través de Internet. Se utiliza el protocolo UDP (User Datagram Protocol) en lugar del protocolo TCP (Transmission Control Protocol).

### Limitaciones:

- El sonido UDP no está disponible en las sesiones cifradas (es decir, las sesiones donde se utiliza el cifrado TLS o ICA). En esas sesiones, la transmisión de sonido se realiza mediante TCP.
  - La prioridad del canal ICA puede afectar el sonido UDP.
1. Configure las siguientes opciones en la sección ClientAudio de module.ini:
    - Establezca EnableUDPAudio con el valor True. De forma predeterminada, este valor está establecido en False, lo que inhabilita el sonido UDP.
    - Especifique los números de puerto mínimo y máximo para el tráfico de sonido UDP mediante UDPAudioPortLow y UDPAudioPortHigh respectivamente. De forma predeterminada, se utilizan los puertos de 16500 a 16509.
  2. Establezca los parámetros de sonido de cliente y de servidor de la manera que se detalla a continuación a fin de que el sonido resultante sea de calidad mediana (es decir, ni alta ni baja).

		Calidad de sonido en el cliente	Calidad de sonido en el cliente	Calidad de sonido en el cliente
		Alto	Medio	Bajo
Calidad de sonido en el servidor	Alto	Alto	Medio	Bajo
Calidad de sonido en el servidor	Medio	Medio	Medio	Bajo
Calidad de sonido en el servidor	Bajo	Bajo	Bajo	Bajo

### UDP en el cliente

En el archivo `$ICAROOT/config/module.ini`, agregue lo siguiente:

En la sección [ClientAudio]:

EnableUDPAudio=True



UDPAudioPortLow=int

UDPAudioPortHigh=int

En el archivo \$HOME/.ICAClient/wfclient.ini, agregue lo siguiente:

En la sección [WFClient]:

AllowAudioInput=True

EnableAudioInput=true

AudioBandWidthLimit=1

**Nota:**

- Si no se puede encontrar la carpeta .ICAClient (solo ocurre en la primera instalación e inicio), abra la aplicación Citrix Workspace y ciérrela. Esta acción crea la carpeta .ICAClient.
- Cuando AudioBandWidthLimit se establece en 1, la calidad de audio del cliente es media.

Agregue lo siguiente en wfclient.ini.\* Establezca la directiva en DDC:

Establezca “Redirección de Windows Media” en “Prohibido”

Establezca “Sonido sobre UDP” en “Permitido”

Establezca “Transporte de sonido en tiempo real sobre UDP” en “Habilitado”

Establezca “Calidad de sonido” en “Media”

### **Cómo cambiar la manera en la que se usa la aplicación Citrix Workspace**

La tecnología ICA está altamente optimizada y, en general, no necesita requisitos elevados de ancho de banda ni de CPU. Sin embargo, si utiliza una conexión con muy poco ancho de banda, tenga en cuenta lo siguiente para preservar el rendimiento:

- **Evite el acceso a archivos grandes mediante la asignación de unidades del cliente.** Cuando se accede a un archivo grande con la asignación de unidades del cliente, el archivo se transfiere a través de la conexión del servidor. En conexiones lentas, puede tardar mucho tiempo.
- **Evite imprimir documentos grandes en impresoras locales.** Al imprimir un documento en una impresora local, el archivo que debe imprimirse se transfiere a través de la conexión del servidor. En conexiones lentas, puede tardar mucho tiempo.
- **Evite reproducir contenido multimedia.** La reproducción de contenido multimedia utiliza una gran cantidad de ancho de banda y puede reducir el rendimiento.

### **USB**

La compatibilidad con USB permite a los usuarios interactuar con una amplia variedad de dispositivos USB cuando se conectan con un escritorio virtual. Los usuarios pueden conectar dispositivos USB a sus equipos, para utilizarlos de forma remota en sus escritorios virtuales. Los dispositivos

USB disponibles para la comunicación remota son, entre otros, las unidades flash, los teléfonos inteligentes, las impresoras, los escáneres, los reproductores MP3, los dispositivos de seguridad y las PC tabletas.

La redirección de USB requiere la versión Citrix Virtual Apps 7.6 (o posterior) o Citrix Virtual Desktops. Citrix Virtual Apps no ofrece la redirección de dispositivos USB de almacenamiento masivo y requiere una configuración especial para admitir dispositivos de sonido. Para obtener más detalles, consulte [Documentación de Citrix Virtual Apps 7.6](#).

Las funciones isócronas de los dispositivos USB (como cámaras web, micrófonos, altavoces y auriculares) se admiten en entornos LAN típicos de baja latencia y alta velocidad. Pero, por lo general, la redirección estándar de sonido o cámara web es más adecuada.

Los siguientes tipos de dispositivo se admiten directamente en una sesión Citrix Virtual Apps and Desktops, y por lo tanto no admiten USB:

- Teclados
- Mouse
- Tarjetas inteligentes
- Auriculares con micro
- Cámaras web

**Nota:**

Los dispositivos USB especializados (por ejemplo, los teclados Bloomberg y mouse 3D) pueden configurarse para admitir USB. Para obtener información sobre cómo configurar reglas de directivas para otros dispositivos USB especializados, consulte [CTX119722](#).

De manera predeterminada, existen ciertos tipos de dispositivos USB que no se admiten para la comunicación remota a través de Citrix Virtual Apps and Desktops. Por ejemplo, un usuario puede tener una tarjeta de interfaz de red conectada a la placa del sistema mediante un dispositivo USB interno. Colocar este dispositivo en comunicación remota no sería apropiado. Los siguientes tipos de dispositivos USB no se admiten de forma predeterminada en sesiones de Citrix Virtual Apps and Desktops:

- Dispositivos Bluetooth
- Tarjetas de interfaz de red integradas
- Hubs USB

Para actualizar la lista predeterminada de los dispositivos USB disponibles para la comunicación remota, modifique el archivo `usb.conf`, ubicado en `$ICAROOT/`. Para obtener más información, consulte la sección “Actualización de la lista de dispositivos USB que se encuentran disponibles para la comunicación remota”.

Para permitir la comunicación remota de los dispositivos USB con escritorios virtuales, habilite la regla de directivas USB. Para obtener más información, consulte la documentación del [Citrix Virtual](#)

## Apps and Desktops.

### Funcionamiento de los USB

Cuando un usuario conecta un dispositivo USB, éste se coteja con la directiva USB y, si está permitido, se lo redirige al escritorio virtual. Si la directiva predeterminada rechaza el dispositivo, solo estará disponible para el escritorio local.

En el caso de los escritorios a los que se accede mediante el modo Desktop Appliance, cuando un usuario conecta un dispositivo USB, ese dispositivo se redirige automáticamente al escritorio virtual. El escritorio virtual es el que controla el dispositivo USB y lo muestra en la interfaz de usuario.

Para que la redirección tenga lugar, la ventana de la sesión debe tener el foco cuando el usuario conecta el dispositivo USB, a menos que se esté mediante el modo Desktop Appliance.

### Dispositivos de almacenamiento masivo

Si un usuario se desconecta de un escritorio virtual cuando un dispositivo USB de almacenamiento masivo se encuentra aún conectado con el escritorio local, ese dispositivo no se redirigirá al escritorio virtual de nuevo cuando el usuario se reconecte. Para garantizar que el dispositivo de almacenamiento masivo se redirija al escritorio virtual, el usuario debe retirar y volver a introducir el dispositivo después de reconectar.

#### Nota:

Si coloca un dispositivo de almacenamiento masivo en una estación de trabajo Linux que se ha configurado para rechazar el uso remoto de dispositivos de almacenamiento masivo USB, el software de la aplicación Workspace no aceptará el dispositivo. Es posible que se abra un explorador de archivos de Linux aparte. Por lo tanto, Citrix recomienda que configure previamente los dispositivos de usuarios sin seleccionar el parámetro **Browse removable media when inserted** de forma predeterminada. En dispositivos basados en Debian, puede hacerlo desde la barra de menú de Debian, en **Desktop > Preferences > Removable Drives and Media**. En la ficha **Storage**, en **Removable Storage**, desmarque la casilla de verificación **Browse removable media when inserted**.

A la hora de redirigir el dispositivo USB del cliente, tenga en cuenta la siguiente nota.

#### Nota:

- Si la directiva de servidor Redirección de dispositivos USB del cliente está activada, los dispositivos de almacenamiento masivo se redirigen siempre como dispositivos USB, incluso aunque la asignación de unidades del cliente esté activada.
- La aplicación no admite la redirección de dispositivos compuestos para dispositivos USB.

## Clases USB

Las reglas de directivas USB predeterminadas admiten las siguientes clases de dispositivos USB:

- Sonido (clase 01)

Incluye micrófonos, altavoces, auriculares y controladores MIDI.

- Interfaz física (clase 05)

Estos dispositivos son similares a los dispositivos HID, pero, en general, proporcionan respuesta o información en tiempo real. Incluyen joystick de Force Feedback, plataformas de movimiento y exoesqueletos de Force Feedback.

- Digitalización de imágenes fijas (clase 06)

Abarca los escáneres y las cámaras digitales. Las cámaras digitales suelen admitir la clase de digitalización de imagen fija que utiliza el protocolo de transferencia de imágenes (PTP) o el protocolo de transferencia multimedia (MTP) para transferir imágenes a un equipo u otro dispositivo periférico. Las cámaras también pueden aparecer como dispositivos de almacenamiento masivo. Puede ser posible configurar una cámara para que utilice cualquiera de las clases desde los menús de configuración que proporciona la cámara propiamente dicha.

Si una cámara aparece como un dispositivo de almacenamiento masivo, se utiliza la asignación de unidades del cliente y no se necesita el uso de USB.

- Impresoras (clase 07)

En general, la mayoría de las impresoras se incluyen en esta clase, aunque algunas utilizan protocolos específicos del fabricante (clase ff). Las impresoras multifunción pueden tener un concentrador interno o ser dispositivos compuestos. En ambos casos, el elemento de impresión generalmente utiliza la clase de la impresora y el elemento de fax o de escaneado utiliza otra clase, por ejemplo, la digitalización de imágenes fijas.

Las impresoras normalmente funcionan de forma adecuada sin la funcionalidad USB.

- Almacenamiento masivo (clase 08)

Los dispositivos de almacenamiento masivo más comunes son las unidades flash USB. Otros incluyen las unidades de disco duro con conexión USB, las unidades de CD/DVD y los lectores de tarjetas SD/MMC. Existe una amplia variedad de dispositivos con almacenamiento interno que también presentan una interfaz de almacenamiento masivo, por ejemplo, reproductores multimedia, cámaras digitales y teléfonos móviles. Las subclases conocidas, entre otras, son:

- 01 Dispositivos flash limitados
- 02 Dispositivos CD/DVD típicos (ATAPI/MMC-2)
- 03 Dispositivos de cinta típicos (QIC-157)
- 04 Unidades de disquete típicas (UFI)

- 05 Unidades de disquete típicas (SFF-8070i)

- 06 La mayoría de los dispositivos de almacenamiento masivo utiliza esta variante de SCSI

A menudo se puede acceder a los dispositivos de almacenamiento masivo a través de la asignación de unidades del cliente y por lo tanto no se requiere la funcionalidad USB.

Importante: Se sabe que algunos virus se propagan en forma activa a través de todos los tipos de almacenamiento masivo. Piense bien si existe una necesidad comercial de permitir el uso de los dispositivos de almacenamiento masivo, ya sea a través de la asignación de unidades del cliente o mediante el uso de USB. Para minimizar el riesgo, el servidor puede configurarse para evitar que los archivos se ejecuten mediante la asignación de unidades del cliente.

- Seguridad del contenido (clase 0d)

Los dispositivos para seguridad del contenido aplican la protección del contenido, generalmente para la administración de derechos digitales o para la gestión de licencias. Esta clase incluye las llaves.

- Atención médica personal (clase 0f)

Estos dispositivos incluyen los dispositivos de atención médica personal como los sensores de presión arterial, los monitores de frecuencia cardíaca, podómetros, monitores de píldoras y espirómetros.

- Específico del proveedor y de la aplicación (clases fe y ff)

Muchos dispositivos utilizan protocolos específicos del proveedor o protocolos no estandarizados por el consorcio USB, que generalmente se muestran como específicos del proveedor (clase ff).

### **Clases de dispositivos USB**

Las reglas de directivas USB predeterminadas rechazan las siguientes clases de dispositivos USB:

- Comunicaciones y control CDC (clases 02 y 0a)

Incluye módems, adaptadores ISDN, adaptadores de red y algunos teléfonos y equipos de fax.

La directiva USB predeterminada no permite estos dispositivos porque es posible que uno de ellos proporcione la conexión al escritorio virtual propiamente dicho.

- Dispositivos de interfaz humana (HID) (clase 03)

Incluye una amplia variedad de dispositivos de entrada y de salida. Los dispositivos de interfaz humana (HID, por su sigla en inglés) típicos son los teclados, los mouse, los dispositivos señaladores, las tabletas gráficas, los controladores de juegos, los botones y las funciones de control.

La subclase 01 se conoce como la clase de interfaz de arranque, y se utiliza para los teclados y punteros.

La directiva USB predeterminada no permite teclados USB (clase 03, subclase 01, protocolo 1) ni mouse USB (clase 03, subclase 01, protocolo 2). Esto se debe a que la mayoría de los teclados y mouse se manejan adecuadamente sin el uso de USB. Además, suele ser necesario utilizar estos dispositivos de forma local y remota cuando se conecta a un escritorio virtual.

- Concentradores USB (clase 09)

Los concentradores USB permiten conectar dispositivos adicionales al equipo local. No es necesario acceder a estos dispositivos de forma remota.

- Tarjeta inteligente (clase 0b)

Los lectores de tarjetas inteligentes incluyen lectores de tarjetas inteligentes con y sin contacto, y tokens USB con un chip de tarjeta inteligente equivalente incorporado.

Se accede a los lectores de tarjeta inteligente mediante la comunicación remota de la tarjeta inteligente y no se necesita la funcionalidad USB.

- Vídeo (clase 0e)

La clase vídeo abarca los dispositivos que se utilizan para controlar vídeos o material relacionado con vídeos, como las cámaras web, videograbadoras digitales, conversores de vídeo analógico, algunos sintonizadores de televisión y algunas cámaras digitales que admiten la transmisión por secuencias de vídeo.

De forma predeterminada, el rendimiento óptimo de la cámara web se logra a través de la compresión de vídeo de cámara web HDX RealTime.

- Controladores inalámbricos (clase e0)

Abarca una amplia variedad de controladores inalámbricos como los controladores de banda ultraancha y Bluetooth.

Es posible que algunos de estos dispositivos proporcionen acceso de red importante o conecten periféricos importantes, como mouse o teclados Bluetooth.

La directiva USB predeterminada no permite estos dispositivos. No obstante, es posible que en el caso de dispositivos particulares sea apropiado proporcionar acceso al uso de USB.

## **Lista de dispositivos USB**

Puede actualizar el rango de dispositivos USB disponibles para la comunicación remota con escritorios. Para ello, modifique la lista de reglas predeterminadas que contiene el archivo `usb.conf`, ubicado en el dispositivo del usuario en `$(CAROOT)/`.

Para actualizar la lista, agregue reglas de directivas nuevas para permitir o denegar dispositivos USB no incluidos en el rango predeterminado. Las reglas creadas de este modo por el administrador controlan qué dispositivos se ofrecen al servidor. Las reglas en el servidor controlan cuáles de ellos se aceptarán.

La configuración de directivas predeterminada para los dispositivos inhabilitados es la siguiente:

DENY: class=09 # Dispositivos del hub

DENY: class=03 subclass=01 # Dispositivo de arranque HID (teclados y mouse)

DENY: class=0b # Tarjeta inteligente

DENY: class=e0 # Controladores inalámbricos

DENY: class=02 # Control CDC y comunicaciones

DENY: class=03 # UVC (cámara web)

DENY: class=0a # Datos de CDC

ALLOW: # Recurso de reserva definitivo: permitir todo lo demás

### Reglas de directivas USB

Sugerencia: Cuando cree reglas de directivas, consulte los códigos de clase USB que se encuentran disponibles en el sitio web de USB

<http://www.usb.org/>. Las reglas de directivas de usb.conf en el dispositivo del usuario adoptan el formato {ALLOW|DENY;} seguido de un conjunto de expresiones basadas en valores para las siguientes etiquetas:

---

Etiqueta	Descripción
VID	Identificador del proveedor tomado del descriptor del dispositivo
REL	Identificador de la versión tomado del descriptor del dispositivo
PID	Identificador del producto tomado del descriptor del dispositivo
Class	Clase, tomada del descriptor del dispositivo o de un descriptor de la interfaz
SubClass	Subclase del descriptor del dispositivo o de un descriptor de la interfaz
Prot	Protocolo tomado del descriptor del dispositivo o de un descriptor de la interfaz

---

Al crear reglas de directivas, tenga en cuenta lo siguiente:

- Las reglas no distinguen entre mayúsculas y minúsculas.

- Las reglas pueden tener un comentario optativo al final que se introduce con el signo #. No es obligatorio utilizar un delimitador y el comentario se ignora para la comparación.
- Se ignoran las líneas en blanco y las que son exclusivamente de comentario.
- El espacio en blanco que se utiliza como separador se ignora, pero no puede aparecer en el medio de un número o de un identificador. Por ejemplo, Deny: Class=08 SubClass=05 es una regla válida, pero Deny: Class=0 8 Sub Class=05 no lo es.
- Las etiquetas deben utilizar el operador de coincidencia =. Por ejemplo: VID=1230.

#### Ejemplo

El siguiente ejemplo muestra una sección del archivo usb.conf en el dispositivo del usuario. Para que se implementen estas reglas, el mismo conjunto de reglas debe existir en el servidor.

ALLOW: VID=1230 PID=0007 # Otra Industria, Otra unidad de Flash

DENY: Class=08 SubClass=05 # Almacenamiento masivo

DENY: Class=0D # Todos los dispositivos de seguridad

#### Modos de inicio

Con el modo Desktop Appliance es posible cambiar cómo un escritorio virtual gestiona los dispositivos USB conectados con anterioridad. En la sección WfClient del archivo \$ICAROOT/config/module.ini de cada dispositivo del usuario, configure DesktopApplianceMode = booleano del siguiente modo.

---

TRUE	Todos los dispositivos USB que ya están conectados al inicio, siempre que los dispositivos no estén inhabilitados con una regla de denegación (DENY) en las directivas de USB en el servidor (entrada del Registro) o en el dispositivo del usuario (archivo de configuración de reglas de directivas).
FALSE	No se inicia ningún dispositivo USB.

---

#### Cámaras web

De forma predeterminada, el rendimiento óptimo de la cámara web se logra a través de la compresión de vídeo de cámara web HDX RealTime. Sin embargo, en algunos casos, es posible que se requiera que los usuarios conecten cámaras web a través de USB. Para realizar esta acción, debe inhabilitar la



compresión de vídeo de cámara web HDX RealTime.

### redirección de cámaras web

A continuación, se presentan algunos puntos sobre la redirección de la cámara web:

- La redirección de la cámara web funciona con y sin RTME.
- La redirección de la cámara web funciona para aplicaciones de 32 bits. Por ejemplo, Skype, o GoToMeeting. Utilice un explorador de 32 bits para verificar la redirección de la cámara web online. Por ejemplo, [www.webcamtests.com](http://www.webcamtests.com)
- El uso de la cámara web es exclusivo de las aplicaciones. Por ejemplo, cuando Skype se ejecuta con una cámara web y usted inicia GoToMeeting, debe salir de Skype para usar la cámara web con GoToMeeting.

### Xcapture

El paquete de la aplicación Citrix Workspace incluye una aplicación auxiliar, xcapture, para el intercambio de datos gráficos entre el portapapeles del servidor y las aplicaciones Windows de X no conformes con ICCCM en el escritorio X. Los usuarios pueden utilizar xcapture para:

- Capturar cuadros de diálogo o áreas de la pantalla y copiarlos entre el escritorio del dispositivo del usuario (incluidas aplicaciones no conformes con ICCCM) y una aplicación que se ejecuta en una ventana de conexión
- Copiar gráficos entre una ventana de conexión y las utilidades xmag o xv que sirven para la manipulación de gráficos X

Para iniciar xcapture desde la línea de comandos:

En el símbolo del sistema, escriba `/opt/Citrix/ICAclient/util/xcapture` y presione Entrar (donde `/opt/Citrix/ICAclient` es el directorio en el que se instaló la aplicación Citrix Workspace).

Para copiar desde el escritorio del dispositivo del usuario:

1. En el cuadro de diálogo xcapture, haga clic en **From Screen**. El cursor adoptará la forma de una cruz.
2. Elija entre las siguientes tareas:
  - Select a window (Seleccionar una ventana). Mueva el cursor por la ventana que quiere copiar y haga clic con el botón central del puntero.
  - Seleccione una región. Mantenga presionado el botón principal del puntero y arrastre el cursor para seleccionar el área que quiere copiar.
  - Cancel the selection (Cancelar la selección). Haga clic con el botón secundario del puntero. Puede cancelar la selección mientras arrastra el cursor. Para eso, debe hacer clic con el botón secundario del puntero sin soltar el botón principal o central.

3. En el cuadro de diálogo xcapture, haga clic en **To ICA**. El botón xcapture cambia de color para indicar que está procesando la información.
4. Cuando se complete la transferencia, utilice el comando de pegar adecuado en la aplicación ejecutada desde la ventana de conexión.

Para copiar desde xv a una aplicación en una ventana de conexión:

1. Desde xv, copie la información.
2. En el cuadro de diálogo xcapture, haga clic en From XV y luego en To ICA. El botón xcapture cambia de color para indicar que está procesando la información.
3. Cuando se complete la transferencia, utilice el comando de pegar adecuado en la aplicación ejecutada desde la ventana de conexión.

Para copiar desde una aplicación en una ventana de conexión a xv:

1. Desde la aplicación en una ventana de conexión, copie la información.
2. En el cuadro de diálogo xcapture, haga clic en From ICA y luego en To XV. El botón xcapture cambia de color para indicar que está procesando la información.
3. Cuando se complete la transferencia, pegue la información en xv.

## Puntero

### Mouse relativo

La función de puntero relativo ofrece una opción para interpretar la posición del puntero de un modo relativo en lugar de hacerlo de un modo absoluto. Esta funcionalidad se necesita para aplicaciones que exigen la entrada de datos de un mouse relativo y no de un mouse absoluto.

#### Nota:

Esta función solo está disponible en sesiones que se ejecutan en Citrix Virtual Apps o Citrix Virtual Desktops 7.8 (o versiones posteriores). De forma predeterminada, está inhabilitada.

### Para habilitar la funcionalidad:

En el archivo `$HOME/.ICAClient/wfclient.ini`, en la sección [WFClient], agregue la entrada `RelativeMouse=1`.

Este paso habilita la función, pero la mantiene inactiva hasta que usted la active.

#### Sugerencia:

Consulte la sección Valores alternativos de puntero relativo para obtener información adicional acerca de la habilitación de las funcionalidades del mouse relativo.

### Para activar la función:

Introduzca `Ctrl/F12`.

Una vez que la función está habilitada, escriba Ctrl/F12 nuevamente para sincronizar la posición del puntero del servidor con el cliente. Las posiciones del puntero del servidor y del cliente no están sincronizadas cuando se utiliza el mouse relativo.

#### **Para desactivar la función:**

Introduzca Ctrl-Mayús/F12.

La función también se desactiva cuando la ventana de una sesión deja de estar activa y en primer plano.

#### **Valores alternativos de puntero relativo**

También puede considerar los siguientes valores de RelativeMouse:

- RelativeMouse=2: Habilita la función y la activa siempre que se enfoque la ventana de una sesión.
- RelativeMouse=3: Habilita y activa la función, y la mantiene activa en todo momento.
- RelativeMouse=4: Habilita o inhabilita la funcionalidad cuando se oculta o se muestra el puntero del mouse del lado del cliente. Este modo es adecuado para habilitar o inhabilitar automáticamente el mouse relativo para interfaces de aplicaciones de estilo de juego en primera persona.

Para cambiar los comandos del teclado, agregue parámetros como:

- RelativemouseOnChar=F11
- RelativeMouseOnShift=Mayús
- RelativemouseOffChar = F11
- RelativeMouseOffShift = Mayús

Los valores admitidos de **RelativemouseOnChar** y **RelativemouseOffChar** se recogen en [Hotkey Keys], en el archivo config/module.ini del árbol de instalación de la aplicación Citrix Workspace. Los valores de **RelativeMouseOnShift** y **RelativeMouseOffShift** establecen las teclas modificadoras para usarse, y se recogen en el título [Hotkey Shift States].

## **Teclado**

### **Comportamiento del teclado**

Para generar una combinación de teclas Ctrl+Alt+Supr remota:

1. Decida la combinación de teclas que creará la combinación Ctrl+Alt+Supr en el escritorio virtual remoto.
2. En la sección WFClient del archivo de configuración apropiado, configure UseCtrlAltEnd según sea necesario:
  - True significa que Ctrl+Alt+Fin pasa la combinación Ctrl+Alt+Supr al escritorio remoto.

- False (valor predeterminado) significa que Ctrl+Alt+Entrar pasa la combinación Ctrl+Alt+Supr al escritorio remoto.

## Redirección genérica

Configuración del teclado Bloomberg v4 a través de una redirección de USB genérico del lado del cliente:

Como requisito previo, la directiva debe habilitarse en Domain Delivery Controller (DDC).

1. Busque el vid y el pid del teclado Bloomberg. Por ejemplo, en Debian y Ubuntu ejecute el siguiente comando:

```
lsusb
```

2. Vaya a \$ICAROOT y modifique el archivo usb.conf.
3. Agregue la siguiente entrada en el archivo usb.conf para que pueda realizarse la redirección del teclado Bloomberg a través de un USB y, a continuación, guarde el archivo.

```
ALLOW: vid=1188 pid=9545
```

4. Reiniciar el demonio ctxusbd en el cliente. Por ejemplo, en Debian y Ubuntu ejecute el siguiente comando:

```
systemctl restart ctxusbd
```

5. Abra una sesión de cliente. Asegúrese de que el foco se encuentra en esa sesión mientras conecta el teclado Bloomberg v4 para su redirección.

## Redirección selectiva

Esta función permite utilizar la interfaz del teclado Bloomberg v4 en varias sesiones. Esta funcionalidad proporciona flexibilidad para utilizar el teclado en todas las sesiones remotas salvo las interfaces de las funciones de huella dactilar y audio. Las interfaces de las funciones de huella dactilar y audio se redirigen a sesiones únicas como sucedía anteriormente.

Puede llevar a cabo la redirección del teclado Bloomberg de la siguiente manera:

- a través de una redirección de USB genérico
- a través de una redirección de USB genérico y con función de redirección selectiva

### Nota:

De forma predeterminada, esta funcionalidad se habilita en las plataformas x86 y x64, y se inhabilita en las plataformas armhf.

Para habilitar la funcionalidad:

1. Modifique la sección BloombergRedirection de la siguiente manera en el archivo config/All\_Regions.ini.

```
BloombergRedirection=true
```

2. Siga todos los pasos descritos en Redirección genérica.

Para inhabilitar esta función:

1. Modifique la sección BloombergRedirection en el archivo config/All\_Regions.ini.
2. Establezca el valor BloombergRedirection en "False".

```
BloombergRedirection=false
```

3. Siga todos los pasos descritos en Redirección genérica.

**Nota:**

Al establecer el valor en "False" se revierte la funcionalidad al comportamiento de las versiones anteriores del cliente, en las que todas las interfaces se redirigen a una única sesión.

## Redirección de contenido de explorador web

### Chromium Embedded Framework (CEF) para la redirección de contenido del explorador web

En versiones anteriores a la versión 1912, BCR utilizaba una superposición basada en WebkitGTK+ para generar el contenido. Sin embargo, en los clientes ligeros había problemas de rendimiento. A partir de la versión 1912, BCR utiliza una superposición basada en CEF. Esta funcionalidad enriquece la experiencia del usuario para la redirección de contenido de explorador web. Reduce la carga de red, el procesamiento de páginas y la generación de gráficos para el dispositivo de punto final.

A partir de la versión 2106, la redirección de contenido del explorador web basada en CEF es totalmente funcional. Esta función está activada de forma predeterminada.

Si es necesario, puede reemplazar el archivo `libffmpeg.so` proporcionado en el paquete de la aplicación Workspace por un archivo `libffmpeg.so` adecuado que tenga los códecs necesarios, en la ruta `$(ICAROOT)/cef/libffmpeg.so`.

**Nota:**

Esta función no está disponible en la plataforma armhf.

### Habilitar la redirección de contenido del explorador web basada en CEF

Para habilitar la redirección de contenido del explorador web basada en CEF:

1. Modifique el archivo que se encuentra en:

```
$(ICAROOT)/config/All_Regions.ini
```

donde \$ICAROOT es el directorio de instalación predeterminado de la aplicación Citrix Workspace.

2. Agregue esta entrada en la sección [`Client Engine\WebPageRedirection`] y configure uno de estos valores:

- True: Indica que la redirección de contenido del explorador web basada en CEF está habilitada.
- False: Indica que la redirección de contenido del explorador web basada en CEF está inhabilitada.

#### **Problema conocido:**

- Al establecer la opción `UseCefBrowser` en **true** en el archivo `~/ .ICAClient/All_Regions .ini`, es posible que el IME japonés, chino y coreano no funcione en campos donde se pueda introducir texto. La aplicación Citrix Workspace para Linux no admite el IME japonés, chino ni coreano cuando se utiliza Secure SaaS con el explorador integrado de Citrix.

Para obtener información sobre la redirección de contenido de explorador web, consulte [Redirección de contenido de explorador web](#) en la documentación de Citrix Virtual Apps and Desktops.

#### **Reconexión automática**

Este apartado describe la función de reconexión automática de clientes de HDX Broadcast. Citrix recomienda utilizar esta función en combinación con la función Fiabilidad de la sesión de HDX Broadcast.

Las sesiones se pueden desconectar debido a redes poco fiables, una latencia en la red muy variable o limitaciones en el alcance de los dispositivos inalámbricos. Con la función de reconexión automática de clientes de HDX Broadcast, la aplicación Citrix Workspace para Linux puede detectar desconexiones accidentales de las sesiones y volver a conectar automáticamente las sesiones afectadas.

Cuando esta función está habilitada en el servidor, los usuarios no tienen que volver a conectarse de forma manual para continuar trabajando. Citrix Workspace lleva a cabo un número determinado de intentos de reconectar la sesión hasta que lo logra, o hasta que el usuario cancela los intentos de reconexión. Si es necesaria la autenticación del usuario, aparece un cuadro de diálogo para ingresar las credenciales durante la reconexión automática. La reconexión automática no se produce si los usuarios salen de las aplicaciones sin realizar el cierre de la sesión. Los usuarios solo pueden volver a conectarse a sesiones desconectadas.

De forma predeterminada, la aplicación Citrix Workspace para Linux espera 30 segundos antes de intentar volver a conectarse a una sesión desconectada y realiza tres intentos de volver a conectarse a esa sesión.

Al conectarse mediante Access Gateway, ACR no se encuentra disponible. Para protegerse ante interrupciones de red, compruebe que la función de fiabilidad de la sesión está habilitada tanto en el

servidor como en el cliente, y que, además, está configurada en Access Gateway.

Para obtener instrucciones acerca de la configuración de la reconexión automática de clientes de HDX Broadcast, consulte la documentación de Citrix Virtual Apps and Desktops.

## Fiabilidad de la sesión

Este apartado describe la función de fiabilidad de sesiones de HDX Broadcast, que se encuentra habilitada de forma predeterminada.

Con la función de fiabilidad de sesiones de HDX Broadcast, los usuarios seguirán viendo una ventana con la aplicación publicada si la conexión a la aplicación se interrumpe. Por ejemplo, los usuarios inalámbricos que pasen por un túnel pueden perder la conexión al entrar, pero volverán a conectarse al salir del túnel. Durante el período de inactividad, todos los datos, entradas de teclado y otras interacciones del usuario se almacenan, mientras que la aplicación parece bloqueada y no responde. Cuando la conexión se restablece, dichas interacciones se reproducen en la aplicación.

Cuando se configuran la reconexión automática de clientes y la fiabilidad de la sesión, esta última tiene prioridad si se produce algún problema de conexión. La función Fiabilidad de la sesión intenta volver a establecer una conexión con la sesión existente. Puede llevar hasta 25 segundos detectar un problema de conexión. Y luego transcurre un período configurable (el valor predeterminado es 180 segundos) para intentar la reconexión. Si la función de fiabilidad de sesiones no consigue completar la reconexión, es la reconexión automática de clientes la que intenta completarla.

Si la función de fiabilidad de sesiones de HDX Broadcast está habilitada, el puerto predeterminado que se utiliza para la comunicación de la sesión cambia de 1494 a 2598.

Los usuarios de Citrix Workspace no pueden anular la configuración del servidor.

### Importante:

La función de fiabilidad de sesiones de HDX Broadcast necesita que otra función, el protocolo CGP, esté habilitada (mediante la configuración de directivas) en el servidor. Si se inhabilita el protocolo CGP, también se inhabilita la función de fiabilidad de sesiones de HDX Broadcast.

## Rendimiento multimedia

La aplicación Citrix Workspace abarca un amplio conjunto de tecnologías que ofrece una experiencia de alta definición para los usuarios en entornos con abundantes recursos multimedia de hoy en día. Estas tecnologías mejoran la experiencia de los usuarios cuando estos se conectan a aplicaciones y escritorios alojados, como se muestra a continuación:

- [Redirección de HDX MediaStream para Windows Media](#)
- [Redirección de HDX MediaStream para Flash](#)
- [Compresión de vídeo de cámara web HDX RealTime](#)

- [H.264](#)

### Nota:

Citrix admite la coexistencia de RTOP con la aplicación Citrix Workspace para Linux versión 1901 y versiones posteriores con GStreamer 0.1.

### Redirección de HDX MediaStream para Windows Media

La redirección de HDX MediaStream para Windows Media supera la necesidad de contar con anchos de banda elevados para la captura y reproducción multimedia en escritorios virtuales Windows a los que se accede desde dispositivos de usuario Linux. La redirección de Windows Media ofrece un mecanismo para reproducir los archivos en tiempo de ejecución multimedia en el dispositivo del usuario y no en el servidor, reduciendo así los requisitos de ancho de banda para reproducir archivos multimedia.

La redirección de Windows Media mejora el rendimiento del Reproductor de Windows Media y de los reproductores compatibles que se ejecutan en escritorios virtuales Windows. Existe un amplio rango de formatos de archivo compatibles, entre ellos:

- Advanced Systems Format (ASF)
- Motion Picture Experts Group (MPEG)
- Audio-Video Interleaved (AVI)
- MPEG Audio Layer-3 (MP3)
- Archivos de sonido WAV

La aplicación Citrix Workspace incluye una tabla basada en texto, `MediaStreamingConfig.tbl`, para traducir los GUID de formatos multimedia específicos de Windows a tipos MIME que GStreamer puede usar. Esta tabla de traducciones puede actualizarse para realizar las siguientes acciones:

- Agregar a la tabla filtros o formatos de archivos multimedia previamente desconocidos o no admitidos
- Bloquear los GUID problemáticos para recurrir a la generación en el lado del servidor
- Agregar parámetros adicionales a las cadenas MIME existentes para permitir la solución de problemas en formatos que no funcionen correctamente mediante la modificación de los parámetros de GStreamer en las secuencias
- Administrar y distribuir configuraciones personalizadas según los tipos de archivo multimedia admitidos por GStreamer en un dispositivo del usuario

Con la obtención de contenido en el lado del cliente, también es posible permitir que el dispositivo del usuario transmita por secuencias multimedia directamente desde las direcciones URL con el formato `http://`, `<mms://>` o `<rtsp://>` en lugar de transmitir por secuencias multimedia a través de un servidor Citrix. El servidor se encarga de dirigir el dispositivo del usuario al contenido multimedia y de enviar los comandos de control (incluidos Reproducir, Pausar, Detener, Volumen y Buscar). Pero el



servidor no manipula los datos multimedia. Esta función requiere bibliotecas avanzadas multimedia de GStreamer en el dispositivo.

Para implementar la redirección de HDX MediaStream para Windows Media:

1. Instale GStreamer 0.10, un marco de trabajo multimedia de código abierto, en cada dispositivo del usuario que lo requiera. Por regla general, GStreamer se instala antes de instalar la aplicación Citrix Workspace para que, durante el proceso de instalación de la aplicación Citrix Workspace, este se configure para utilizar GStreamer.

La mayoría de las distribuciones de Linux incluyen GStreamer. De forma alternativa, puede descargar GStreamer desde <http://gstreamer.freedesktop.org>.

2. Para habilitar la obtención de contenido en el lado del cliente, instale los *plug-ins* de origen de protocolo de GStreamer para los tipos de archivo que los usuarios reproducirán en el dispositivo. La utilidad `gst-launch` permite verificar que el *plug-in* se encuentre instalado y funcione correctamente. Si `gst-launch` puede reproducir la dirección URL, el *plug-in* requerido funciona correctamente. Por ejemplo, ejecute `gst-launch-0.10 playbin2 uri=<http://example-source/file.wmv>` y compruebe que el vídeo se reproduce correctamente.
3. Cuando instale la aplicación Citrix Workspace en el dispositivo, seleccione la opción de GStreamer si está utilizando el script `tarball` (esto se hace automáticamente para los paquetes DEB y RPM).

Tenga en cuenta lo siguiente con respecto a la funcionalidad de obtención de contenido en el lado del cliente:

- De manera predeterminada, esta función está habilitada. Es posible inhabilitarla mediante la opción `SpeedScreenMMACSFEnabled` en la sección Multimedia de `All-Regions.ini`. Si esta opción se establece en `False`, se utiliza la redirección de Windows Media para el procesamiento de medios.
- De forma predeterminada, todas las funcionalidades de MediaStream utilizan el protocolo `playbin2` de GStreamer. Es posible revertir al protocolo `playbin` anterior en todas las funcionalidades de MediaStream, excepto la obtención de contenido en el lado del cliente que continuará mediante `playbin2`, mediante la opción `SpeedScreenMMAEnablePlaybin2` en la sección Multimedia de `All-Regions.ini`.
- La aplicación Citrix Workspace no reconoce archivos de lista de reproducción ni archivos de información de configuración de secuencia como `.asx` o `.nsc`. Cuando sea posible, los usuarios deben especificar una URL estándar que no haga referencia a estos tipos de archivo. Utilice `gst-launch` para verificar que una dirección URL determinada sea válida.

Nota sobre GStreamer 1.0:

- De forma predeterminada, se utiliza GStreamer 0.10 para la redirección de HDX MediaStream para Windows Media. GStreamer 1.0 solo se utiliza cuando GStreamer 0.10 no está disponible.

- Si quiere utilizar GStreamer 1.0, siga estas instrucciones:
  1. Busque el directorio de instalación de los plugins de GStreamer. La ubicación de instalación de los plugins varía en función de la distribución, la arquitectura del sistema operativo y la instalación en sí de GStreamer. La ruta de instalación típica es `/usr/lib/x86_64-linux-gnu/gstreamer-1.0` o `$HOME/.local/share/gstreamer-1.0`.
  2. Busque el directorio de instalación de la aplicación Citrix Workspace para Linux. El directorio predeterminado para las instalaciones de usuarios con privilegios (root) es `/opt/Citrix/ICA-Client`. El directorio predeterminado para las instalaciones de usuarios sin privilegios es `$HOME/ICAclient/platform` (donde “platform” puede ser `linuxx64`, por ejemplo). Para obtener más información, consulte [Instalación y configuración](#).
  3. Instale `libgstflatstm1.0.so` mediante un vínculo simbólico en el directorio de plugins de GStreamer: `ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so`. Este paso puede requerir permisos elevados (como `sudo`, por ejemplo).
  4. Use `gst_play1.0` como reproductor en: `ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play`. Este paso puede requerir permisos elevados (como `sudo`, por ejemplo).
- Si quiere usar GStreamer 1.0 para la compresión de vídeo de cámara web HDX RealTime, use `gst_read1.0` como el lector: `ln -sf $ICACLIENT_DIR/util/gst_read1.0 $ICACLIENT_DIR/util/gst_read`.

### Habilitar GStreamer 1.x

En versiones anteriores a 1912, GStreamer 0.10 era la versión predeterminada admitida para la redirección multimedia. A partir de la versión 1912, puede configurar GStreamer 1.x como la versión predeterminada.

#### Limitaciones:

- Al reproducir un vídeo, es posible que rebobinar hacia delante y hacia atrás no funcione según lo previsto.
- Al iniciar la aplicación Citrix Workspace en dispositivos armhf, es posible que GStreamer 1.x no funcione según lo previsto.

### Para instalar GStreamer 1.x

Instale el framework GStreamer 1.x y los siguientes plug-ins desde <https://gstreamer.freedesktop.org/documentation/installing/on-linux.html>:

- `Gstreamer-plugins-base`
- `Gstreamer-plugins-bad`
- `Gstreamer-plugins-good`
- `Gstreamer-plugins-ugly`
- `Gstreamer-libav`

### Para crear binarios localmente

En algunas distribuciones de SO de Linux (por ejemplo, SUSE y openSUSE), es posible que el sistema no encuentre los paquetes de GStreamer en la lista de fuentes predeterminada. En este caso, descargue el código fuente y cree todos los binarios localmente:

1. Descargue el código fuente desde <https://gstreamer.freedesktop.org/src/>.
2. Extraiga el contenido.
3. Vaya al directorio donde está disponible el paquete descomprimido.
4. Ejecute los comandos siguientes:

```
1 $sudo ./configure
2 $sudo make
3 $sudo make install
```

De forma predeterminada, los binarios generados están disponibles en `/usr/local/lib/gstreamer-1.0/`.

Para obtener información sobre la solución de problemas, consulte el artículo [CTX224988](#) de Knowledge Center.

### Para configurar GStreamer 1.x

Para configurar GStreamer 1.x y usarlo con la aplicación Citrix Workspace, aplique la siguiente configuración desde el símbolo del shell:

- `$ln -sf $ICACLIENT_DIR/util/libgstflatstm1.0.so $GST_PLUGINS_PATH/libgstflatstm1.0.so.`
- `$ln -sf $ICACLIENT_DIR/util/gst_play1.0 $ICACLIENT_DIR/util/gst_play`

Donde:

- `ICACLIENT_DIR`: Es la ruta de instalación de la aplicación Citrix Workspace para Linux.
- `GST_PLUGINS_PATH`: Es la ruta del plug-in de GStreamer. Por ejemplo, en una máquina Debian de 64 bits es `/usr/lib/x86_64-linux-gnu/gstreamer-1.0/`.

### Limitaciones:

- Al utilizar la versión 1.15.1 de GStreamer o una posterior, es posible que la redirección de cámaras web falle y que la sesión se desconecte.

### Redirección de HDX MediaStream para Flash

La Redirección de Flash de HDX MediaStream habilita el contenido de Adobe Flash para que se reproduzca de forma local en los dispositivos de los usuarios, y les brinda una reproducción de sonido y vídeo de alta definición sin aumentar los requisitos de ancho de banda.

1. Compruebe que el dispositivo del usuario cumpla los requisitos de esta función. Para obtener más información, consulte [Requisitos del sistema](#).
2. Agregue los siguientes parámetros a la sección [WFClient] de wfclient.ini (para todas las conexiones hechas por un usuario específico) o a la sección [Client Engine\Application Launching] de All\_Regions.ini (para todos los usuarios del entorno):

- **HDXFlashUseFlashRemoting=Ask: Never; Always**

Habilita HDX MediaStream para Flash en el dispositivo del usuario. De forma predeterminada, este parámetro está establecido en **Never** y se presenta un cuadro de diálogo a los usuarios para preguntarles si quieren optimizar el contenido de Flash al conectarse a páginas Web que contienen Flash.

- **HDXFlashEnableServerSideContentFetching=Disabled; Enabled**

Habilita o inhabilita la obtención de contenido en el servidor para la aplicación Citrix Workspace. De forma predeterminada, este parámetro está configurado como inhabilitado: **Disabled**.

- **HDXFlashUseServerHttpCookie=Disabled; Enabled**

Habilita o inhabilita la redirección de cookies HTTP. De forma predeterminada, este parámetro está configurado como inhabilitado: **Disabled**.

- **HDXFlashEnableClientSideCaching=Disabled; Enabled**

Habilita o inhabilita el almacenamiento en caché del cliente del contenido Web obtenido por la aplicación Citrix Workspace. De forma predeterminada, este parámetro está configurado como habilitado: **Enabled**.

- **HDXFlashClientCacheSize= [25-250]**

Define el tamaño, en megabytes (MB), de la caché en el cliente. Puede introducirse cualquier tamaño entre 25 MB y 250 MB. Cuando se alcance el tamaño máximo, se eliminará el contenido existente en el caché para permitir el almacenamiento de contenido nuevo. De forma predeterminada, este parámetro está configurado como **100**.

- **HDXFlashServerSideContentCacheType=Persistent: Temporary; NoCaching**

Define el tipo de almacenamiento en caché que utiliza la aplicación Citrix Workspace para el contenido que se obtiene en el servidor. De forma predeterminada, este parámetro está configurado como persistente:

**Persistent.**

**Nota:** Este parámetro solo es necesario si:

**HDXFlashEnableServerSideContentFetching** está configurado como habilitado:  
**Enabled.**

3. La redirección de Flash está inhabilitada de forma predeterminada. En /config/module.ini, cambie FlashV2=Off por FlashV2=On para habilitar la función.

### Compresión de vídeo de cámara web HDX RealTime

HDX RealTime ofrece una opción de compresión de vídeo de cámara web para mejorar la eficiencia del ancho de banda durante las conferencias de vídeo, y de ese modo garantizar que los usuarios experimenten un rendimiento óptimo al utilizar aplicaciones como GoToMeeting con HD Faces o Skype Empresarial.

1. Compruebe que el dispositivo del usuario cumpla los requisitos de esta función.
2. Compruebe que el canal virtual **Multimedia** esté habilitado. Para hacerlo, abra el archivo de configuración module.ini, ubicado en el directorio \$ICAROOT/config, y verifique que **MultiMedia** en la sección [ICA3.0] esté establecido en "On".
3. Para habilitar la entrada de sonido, haga clic en Usar mi micrófono y mi cámara web en la página Micrófono y cámara web del cuadro de diálogo Preferencias.

### Inhabilitar la compresión de vídeo de cámara web HDX RealTime

De forma predeterminada, el rendimiento óptimo de la cámara web se logra a través de la compresión de vídeo de cámara web HDX RealTime. Sin embargo, en algunos casos, es posible que se requiera que los usuarios conecten cámaras web a través de USB. Para ello, debe hacer lo siguiente:

- Inhabilitar la compresión de vídeo de cámara web HDX RealTime
  - Habilitar la compatibilidad de USB para cámaras web
1. Agregar el parámetro siguiente en la sección [WFClient] del archivo INI apropiado:  
HDXWebCamEnabled=Off  
  
Para obtener más información, consulte [parámetros predeterminados](#).
  2. Abra el archivo usb.conf que, por lo general, se encuentra en \$ICAROOT/usb.conf.
  3. Elimine o convierta en comentario la siguiente línea:

```
DENY: class 0e # UVC (opción predeterminada a través de la compresión de vídeo de cámara web HDX RealTime)
```

4. Guarde el archivo y ciérrelo.

### SaaS seguro con el explorador Citrix incrustado: **Función experimental**

El acceso seguro a las aplicaciones SaaS ofrece una experiencia de usuario unificada en la entrega de aplicaciones SaaS publicadas a los usuarios. Las aplicaciones SaaS están disponibles con el inicio Single Sign-On. Ahora los administradores pueden filtrar el acceso a sitios web específicos y categorías

de sitios web concretas para proteger la red de la organización y los dispositivos de los usuarios finales frente al malware y las filtraciones de datos.

La aplicación Citrix Workspace para Linux admite el uso de aplicaciones SaaS mediante Access Control Service. Este servicio permite a los administradores proporcionar una experiencia coherente, con Single Sign-On e inspección de contenido.

### **Requisito previo:**

Compruebe que el paquete `libgtkglext1` esté disponible.

La entrega de aplicaciones SaaS desde la nube presenta los siguientes beneficios:

- Configuración simple: Fácil de operar, actualizar y consumir.
- Single Sign-On: Inicio de sesión sin complicaciones gracias a Single Sign-On.
- Plantilla estándar para aplicaciones diferentes: Configuración basada en plantillas para las aplicaciones de uso extendido.

#### **Nota:**

SaaS con Citrix Browser Engine solo se admite en plataformas x64 y x86 y no en hardware ArmHardFloatPort (armhf).

Para obtener información sobre cómo configurar aplicaciones SaaS mediante Access Control Services, consulte la documentación de [Control de acceso](#).

Para obtener más información acerca de las aplicaciones SaaS con la aplicación Citrix Workspace, consulte [Configuración de Workspace](#) en la documentación más reciente de la aplicación Citrix Workspace para Windows.

## **H.264**

La aplicación Citrix Workspace admite la presentación de gráficos H.264, incluidos gráficos HDX 3D Pro, proporcionados por Citrix Virtual Apps and Desktops 7. Se utiliza la función de códec de compresión profunda, que se encuentra habilitada de forma predeterminada. Esta función ofrece un mejor rendimiento de las aplicaciones de gráficos de nivel profesional en redes WAN, comparado con el códec de JPEG existente.

Siga las instrucciones en este tema para inhabilitar esta función (y procesar gráficos mediante el códec de JPEG en su lugar). También puede inhabilitar el seguimiento de texto, pero, a su vez, mantener habilitado el códec de compresión profunda. Esto ayuda a reducir los costes de CPU durante el procesamiento de gráficos que incluyen imágenes complejas, con cantidades de texto relativamente pequeñas o de poca importancia.

#### **Importante:**

Para configurar esta funcionalidad, no use ninguna opción con pérdida en la directiva Calidad

visual de Citrix Virtual Apps and Desktops. Si lo hace, la codificación H.264 se inhabilita en el servidor y no funciona en la aplicación Citrix Workspace.

Para inhabilitar el códec de compresión profunda:

En `wfclient.ini`, establezca **H264Enabled** con el valor `False`. Esto también inhabilita el seguimiento de texto.

Para inhabilitar solo el seguimiento de texto

Con el códec de compresión profunda habilitado, en el archivo `wfclient.ini` configure **TextTrackingEnabled** con el valor `False`.

### Mosaicos de pantalla

Es posible mejorar la manera en que se procesan los cuadros de pantalla codificados con JPEG mediante las funcionalidades Decodificación de mapas de bits directamente en la pantalla, Decodificación de cuadros por lotes y XSync diferida.

1. Asegúrese de que su biblioteca JPEG admite estas funciones.
2. En la sección `Thinwire3.0` de `wfclient.ini`, establezca `DirectDecode` y `BatchDecode` en `True`.

Nota: La habilitación de la decodificación de cuadros por lotes también habilita la XSync diferida.

### Captura de registros

En versiones anteriores, los archivos `debug.ini` y `module.ini` se utilizaban para configurar los registros.

A partir de la versión 2009, puede configurar los registros mediante uno de los métodos siguientes:

- Interfaz de la línea de comandos
- Interfaz gráfica de usuario (GUI)

También a partir de la versión 2009, se elimina el archivo de configuración `debug.ini` del paquete de instalación de la aplicación Citrix Workspace.

Los registros capturan los detalles de implementación de la aplicación Citrix Workspace, los cambios de configuración y las actividades administrativas en una base de datos de registros. Un desarrollador externo puede aprovechar este mecanismo de registro mediante el SDK de registro, que se incluye como parte del SDK de optimización de plataformas de la aplicación Citrix Workspace.

Puede utilizar la información de registro para:

- Diagnosticar y solucionar problemas técnicos que se produzcan después de cualquier cambio. El registro proporciona un rastro de los pasos seguidos.

- Ayudar en la administración de cambios y en el seguimiento de las configuraciones.
- Realizar informes sobre las actividades administrativas.

Si la aplicación Citrix Workspace está instalada con privilegios de usuario root, los registros se almacenan en `/var/log/citrix/ICAClient.log`. De lo contrario, los registros se almacenan en ``${HOME} /.ICAClient/logs/ICAClient.log`.

### Interfaz de la línea de comandos

1. En el símbolo del sistema, vaya a la ruta `/opt/Citrix/ICAClient/util`.
2. Ejecute el siguiente comando para definir las preferencias de registro.

```
./setlog help
```

Se muestran todos los comandos disponibles.

En la tabla siguiente se enumeran varios módulos y sus valores de clase de seguimiento correspondientes. Utilice la tabla siguiente para un conjunto de valores de registro de línea de comandos específico:

Módulo	Clase del registro
Afirmaciones	LOG_ASSERT
Monitor de audio	TC_CM
BCR con CEF	TC_CEFBCR
Asignación de sonido del cliente	TC_CAM
Central de conexiones	TC_CONNCENTER
Puerto de comunicación del cliente	TC_CCM
Asignación de unidades del cliente	TC_CDM
Clip	TC_CLIP
Asignación de impresoras del cliente	TC_CPM
Asignación de impresoras del cliente	TC_CPM
Fuente	TC_FONT
Fotograma	TC_FRAME
Abstracción de gráficos	TC_GA
Editor de métodos de entrada	TC_IME
IPC	TC_IPC
Asignación de teclado	TC_KEY



Módulo	Clase del registro
Controlador de licencias	TC_VDLIC
Contenido multimedia	TC_MMVD
Asignación de mouse	TC_MOU
MS Teams	TC_MTOP
Otras bibliotecas	TC_LIB
Controlador de protocolo	TC_PD
Almacén PNA	TC_PN
Registros de eventos estándar	LOG_CLASS
SRCC	TC_SRCC
Inicio de sesión SSPI	TC_CSM
Tarjeta inteligente	TC_SCARDVD
Autoservicio	TC_SS
Extensión de autoservicio	TC_SSEXT
StoreFrontLib	TC_STF
Controlador de transporte	TC_TD
Thinwire	TC_TW
Interfaz de ventana transparente	TC_TUI
Canal virtual	TC_VD
PAL	TC_VP
IU	TC_UI
UIDialogLibWebKit3	TC_UIDW3
UIDialogLibWebKit3_ext	TC_UIDW3E
Demonio USB	TC_CTXUSB
Controlador de fotogramas de vídeo	TC_VFM
WebKit	TC_WEBKIT
Controlador WinStation	TC_WD
WfICA	TC_NCS
Motor Wfica	TC_WENG
Wfica Shell	TC_WFSHELL

Módulo	Clase del registro
Ayudante web	TC_WH
Latencia cero	TC_ZLC

### Interfaz gráfica (GUI)

Vaya a **Menú > Preferencias**. Aparecerá el cuadro de diálogo **Citrix Workspace - Preferencias**.

A niveles cada vez mayores de detalle de trazado, están disponibles los siguientes valores:

- Inhabilitada
- Solo errores
- Normal
- El modo Verbose

De forma predeterminada, la opción **Registro** se establece en **Normal**.

Debido a la gran cantidad de datos que se pueden generar, es posible que el rastreo afecte de manera significativa al rendimiento de la aplicación Citrix Workspace. No se recomienda el nivel **Verbose** a menos que sea necesario para solucionar problemas.

Haga clic en **Guardar y cerrar** después de seleccionar el nivel de registro deseado. Los cambios se aplican dinámicamente en la sesión.

Haga clic en el icono de configuración situado junto al menú desplegable de opciones de **Registro**. Aparecerá el cuadro de diálogo **Preferencias de registro de Citrix**.

#### Nota:

Si elimina el archivo `ICAClient.log`, debe reiniciar el servicio de registros `ctxlogd`.

Por ejemplo, si utiliza una instalación compatible con el sistema, ejecute el siguiente comando:

```
systemctl restart ctxlogd.
```

#### Habilitar el registro en la versión 2006 y versiones anteriores:

Si tiene la versión 2006 o una anterior, habilite los registros mediante el procedimiento siguiente:

1. Descargue e instale la aplicación Citrix Workspace en su máquina Linux.
2. Defina la variable de entorno `ICAROOT` en la ubicación de instalación.

Por ejemplo, `/opt/Citrix/ICAClient`.

De forma predeterminada, la clase de rastreo `TC_ALL` está habilitada para proporcionar todos los rastreos.

3. Para recopilar registros de un módulo en concreto, abra el archivo `debug.ini` en `$ICAROOT` y agregue los parámetros de rastreo requeridos a la sección `[wfica]`.

Agregue las clases de seguimiento con un símbolo "+". Por ejemplo, `+TC_LIB`.

Puede agregar varias clases separadas por barras verticales ("|").

Por ejemplo, `+TC_LIB|+TC_MMVD`.

En la tabla siguiente se enumeran varios módulos y sus valores de clase de seguimiento correspondientes:

### Solución de problemas:

Si `ctxlogd` deja de responder, los registros se rastrean en `syslog`.

Para obtener información acerca de cómo obtener registros nuevos y actualizados en inicios posteriores, consulte [Configuración de Syslog](#).

### Configuración de Syslog

De forma predeterminada, todos los registros de `syslog` se guardan en `/var/log/syslog`. Puede configurar la ruta y el nombre del archivo de registros. Para ello, modifique la siguiente línea en la sección `[REGLAS]`, en el archivo `/etc/rsyslog.conf`. Por ejemplo:

```
1 user.* -/var/log/logfile_name.log
```

Guarde los cambios y reinicie el servicio `syslog` mediante el comando:

```
sudo service rsyslog restart
```

### Puntos que tener en cuenta:

- Para comprobar que hay disponible un nuevo `syslog`, elimine `syslog` y ejecute el comando: `sudo service rsyslog restart`.
- Para evitar mensajes duplicados, agregue **\$RepeatedMsgReduction on** al principio del archivo `rsyslog.conf`.
- Para recibir registros, compruebe que la línea **\$ModLoad imuxsock.so** no esté comentada al principio del archivo `rsyslog.conf`.

### Registro remoto

Para habilitar el registro remoto:

- **Configuración del lado del servidor:** Quite las marcas de comentario en las siguientes líneas del archivo `rsyslog.conf`, presente en el servidor `syslog`:

```
$ModLoad imtcp  
$InputTCPServerRun 10514
```

- **Configuración del lado del cliente:** Agregue la siguiente línea en el archivo `rsyslog.conf` para reemplazar el host local por la IP del servidor remoto:

```
*.* @localhost:10514
```

## Optimización para Microsoft Teams

Optimización para Microsoft Teams de escritorio mediante Citrix Virtual Apps and Desktops y la aplicación Citrix Workspace. La optimización para Microsoft Teams es similar a HDX RealTime Optimization para Microsoft Skype Empresarial. La diferencia es que agrupamos todos los componentes necesarios para la optimización de Microsoft Teams en el VDA y en la aplicación Workspace para Linux.

La aplicación Citrix Workspace para Linux ofrece funciones de audio, vídeo y uso compartido de la pantalla con la optimización de Microsoft Teams.

### Nota:

- La optimización de Microsoft Teams solo se ofrece en distribuciones x64 de Linux.

Para obtener información sobre cómo habilitar los registros, siga los pasos indicados en [Registros en Microsoft Teams](#).

Para obtener información sobre los requisitos del sistema, consulte [Optimización de Microsoft Teams](#).

Para obtener más información, consulte [Optimización para Microsoft Teams](#) y [Redirección de Microsoft Teams](#).

## Registros en Microsoft Teams

Para habilitar los registros en Microsoft Teams:

1. Vaya al archivo `/opt/Citrix/ICAClient/debug.ini`.
2. Modifique la sección `[HDXTeams]` de la siguiente manera:

```
1 [HDXTeams]  
2 ; Retail logging for HDXTeams 0/1 = disabled/enabled  
3 HDXTeamsLogSwitch = 1  
4 ; Debug logging; , It is in decreasing order
```

```
5 ; LS_NONE = 4, LS_ERROR = 3, LS_WARNING = 2, LS_INFO = 1,  
   LS_VERBOSE = 0  
6 WebrtcLogLevel = 0  
7 ; None = 5, Info = 4, Warning = 3, Error = 2, Debug = 1, Trace = 0  
8 WebrpcLogLevel = 0
```

## Canal virtual NetScaler App Experience (NSAP) disponible

Anteriormente disponible como una función experimental, ahora la función de canal virtual NetScaler App Experience (NSAP) está disponible en su totalidad. Todos los datos de HDX Insight se obtienen exclusivamente del canal virtual NSAP y se envían sin comprimir. Esta manera mejora la escalabilidad y el rendimiento de las sesiones. De forma predeterminada, el canal virtual NSAP está habilitado. Para inhabilitarlo, cambie el indicador VDNSAP `VDNSAP=Off` en el archivo `module.ini`.

Para obtener más información, consulte [HDX Insight](#) en la documentación de Linux Virtual Delivery Agent y [HDX Insight](#) en la documentación del servicio Citrix Application Delivery Management.

## Persistencia del diseño en varios monitores

Esta función conserva la información sobre el diseño en el monitor de la sesión en los dispositivos de punto final. La sesión aparece en los mismos monitores configurados.

### Requisito previo:

Esta función requiere lo siguiente:

- StoreFront 3.15 o una versión posterior.
- Si `.ICAClient` ya está presente en la carpeta de inicio del usuario actual:

Elimine el archivo `All_Regions.ini`

O bien:

Para conservar el archivo `AllRegions.ini`, agregue las siguientes líneas al final de la sección `[Client Engine\Application Launching]`:

`SubscriptionUrl=`

`PreferredWindowsBounds=`

`PreferredMonitors=`

`PreferredWindowState=`

`SaveMultiMonitorPref=`

Si la carpeta `.ICAClient` no está presente, entonces es que indica una nueva instalación de la aplicación Citrix Workspace. En ese caso, se conserva la configuración predeterminada para la función.

## Casos de uso

- Inicie una sesión en cualquier monitor en modo ventana y guarde la configuración. Cuando reinicie la sesión, aparecerá en el mismo modo, en el mismo monitor y en la misma posición.
- Inicie una sesión en cualquier monitor en modo de pantalla completa y guarde la configuración. Cuando reinicie la sesión, aparecerá en modo de pantalla completa en el mismo monitor.
- Estire y amplíe una sesión en modo ventana a varios monitores y luego cambie al modo de pantalla completa. La sesión continúa en pantalla completa en todos los monitores. Cuando reinicie la sesión, aparecerá en modo de pantalla completa, ampliada a todos los monitores.

### Nota:

El diseño de los elementos se sobrescribe con cada operación de guardado. Además, el diseño se guarda solo en el StoreFront activo.

Si inicia varias sesiones de escritorio desde el mismo StoreFront en diferentes monitores, guardar el diseño en una sesión guarda la información de diseño de todas las sesiones.

## Guardar diseño

Para habilitar la función de guardar diseño:

1. Instale StoreFront 3.15 o una versión posterior (igual o posterior a 3.15.0.12) en un Delivery Controller (DDC) compatible.
2. Descargue la versión comercializada de la aplicación Citrix Workspace para Linux 1808 o versiones posteriores desde la página [Descargas](#) y luego instálela en su máquina Linux.
3. Establezca la variable de entorno ICAROOT en la ubicación de instalación.
4. Compruebe si el archivo **All\_Regions.ini** está presente en la carpeta **.ICAClient**. Si es así, elimínelo.
5. En el archivo **\$ICAROOT/config/All\_Regions.ini**, busque el campo – **SaveMultiMonitorPref**. De forma predeterminada, el valor de este campo es “true” (lo que significa que esta función está activada). Para desactivar esta función, establezca este campo en “false”.  
Si realiza algún cambio en el valor **SaveMultiMonitorPref**, debe eliminar el archivo **All\_Regions.ini** presente en la carpeta **.ICAClient** para evitar discrepancias de valores y un posible bloqueo de perfil. Establezca o desactive la marca **SaveMultiMonitorPref** antes de iniciar sesiones
6. Lance una nueva sesión de escritorio.
7. Haga clic en **Guardar diseño** en la barra de herramientas de Desktop Viewer para guardar el diseño de la sesión actual. Aparece una notificación en la parte inferior derecha de la pantalla, que indica que la operación se ha realizado correctamente.  
Cuando hace clic en Guardar diseño, el icono pasa a ser gris. Esto indica que la operación de guardado está en curso. Tras guardarse el diseño, el icono aparece como siempre.

Sin embargo, si el icono aparece en gris durante mucho tiempo, consulte el artículo [CTX235895](#) de Knowledge Center para obtener información sobre la solución al problema.

8. Desconecte la sesión o ciérrela.

Vuelva a iniciar la sesión. La sesión aparece en el mismo modo, en el mismo monitor y en la misma posición.

### Limitaciones y casos no admitidos:

- No se admite el guardado de un diseño de sesión en modo ventana que abarca varios monitores, debido a limitaciones con el administrador de pantalla de Linux.
- En esta versión, no se admite el guardado de información de sesión en monitores con resolución variada, y guardarla podría dar lugar a un comportamiento impredecible.
- Implementaciones de clientes con varios almacenes de StoreFront

### Uso de Citrix Virtual Desktops en monitores dobles

1. Seleccione Desktop Viewer y haga clic en la flecha hacia abajo.
2. Seleccione la opción **Ventana**.
3. Arrastre la pantalla Citrix Virtual Desktops entre los dos monitores. Asegúrese de que aproximadamente la mitad de la pantalla esté presente en cada monitor.
4. En la barra de herramientas de Citrix Virtual Desktops, seleccione **Pantalla completa**.

La pantalla se extiende ahora a ambos monitores.

### Workspace Launcher

Citrix presenta Workspace Launcher (WebHelper) para iniciar aplicaciones y escritorios publicados.

Anteriormente, el plug-in del explorador provisto junto con la aplicación Citrix Workspace para Linux que permitía a los usuarios iniciar aplicaciones y escritorios publicados se basaba en NPAPI.

Como solución, Citrix presenta Workspace Launcher (WebHelper). Para habilitar esta función, configure StoreFront para enviar solicitudes a Workspace Launcher para detectar la instalación de la aplicación Citrix Workspace.

A partir de la versión 1901, Citrix Workspace Launcher funciona con conexiones directas a StoreFront y Citrix Gateway. Esta función ayuda a iniciar el archivo ICA automáticamente y a detectar la instalación de la aplicación Citrix Workspace.

Como solución, Citrix presenta Workspace Launcher (WebHelper). Para habilitar esta función, configure StoreFront para enviar solicitudes a Workspace Launcher para detectar la instalación de la aplicación Citrix Workspace.

Para obtener más información sobre cómo configurar StoreFront, consulte **Solución - 2 > a) Configuración de administrador** en el artículo del Knowledge Center [CTX237727](#).

### Nota:

Citrix Workspace Launcher actualmente funciona solo con conexiones directas a StoreFront. No se admite en otros casos, como en las conexiones a través de Citrix Gateway.

### Inhabilitar el nuevo modo de interfaz de usuario web del espacio de trabajo

Cuando inicia la aplicación Citrix Workspace para Linux mediante un archivo ejecutable de autoservicio proveniente de proveedores de terceros de clientes ligeros, la aplicación puede dejar de responder debido al 100% de utilización de CPU.

Como solución temporal, para volver al antiguo modo de interfaz de usuario, puede hacer lo siguiente:

1. Elimine los archivos en caché con el comando:  

```
rm -r ~/.ICAClient
```
2. Vaya al archivo `$ICAROOT/config/AuthManconfig.xml`.
3. Cambie el valor de la clave `CWACapableEnabled` a “false”.
4. Inicie la aplicación Citrix Workspace para Linux. Podrá comprobar que el archivo ejecutable de autoservicio carga la IU anterior.

### Sincronización de la distribución de teclado

La sincronización de la distribución del teclado entre el cliente y VDA le permite cambiar entre distintas distribuciones de teclado preferidas en el dispositivo cliente cuando utilice un VDA de Linux o de Windows. Esta función está inhabilitada de forma predeterminada.

#### Requisito previo:

- Habilite la función de asignación de distribución de teclado Unicode en el Windows VDA. Para obtener más información, consulte el artículo [CTX226335](#) de Knowledge Center.
- Habilite la función Sincronización de la distribución de teclado dinámico en Linux VDA. Para obtener más información, consulte [Sincronización de la distribución de teclado dinámico](#)
- La sincronización de la distribución del teclado depende de la librería XKB, que permite sincronizar automáticamente la distribución del teclado con el agente VDA y el dispositivo del cliente.
- Al utilizar Windows Server 2016 o Windows Server 2019, vaya a la ruta `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme` del Editor del Registro y agregue un nuevo valor DWORD con nombre de clave `DisableKeyboardSync` y establezca su valor en 0.

Para habilitar esta función, agregue las líneas siguientes al archivo `module.ini`:



```
[ICA 3.0]
KeyboardSync=activado

[KeyboardSync]
DriverName = VDIME.DLL
```

Si activa **KeyboardSync** en el archivo module.ini y establece **KeyboardLayout=(Perfil de usuario)** en el archivo **wfclient.ini** el controlador virtual vdime detecta la distribución activa del teclado en el cliente y envía la información al VDA. Cuando la distribución del teclado cambia en una sesión de cliente, vdime percibe el cambio y envía inmediatamente la nueva distribución al VDA.

Para inhabilitar esta función, establezca **KeyboardSync = Off** en el archivo module.ini para volver al comportamiento anterior. En el comportamiento anterior, la distribución del teclado se lee desde el archivo **\$HOME/.ICAClient/wfclient.ini** y se envía al VDA junto con otra información del cliente cuando se inicia la sesión.

## Uso

Con esta función habilitada, cuando la distribución del teclado cambia en el dispositivo cliente durante una sesión, también cambia la distribución del teclado de la sesión.

## Distribución del teclado con Windows VDA y Linux VDA

### Nota:

La configuración regional del teclado Linux para todas las referencias de la siguiente tabla es un guion.

Distribución del teclado Linux	Distribución del teclado Linux/Linux VDA	Configuración regional de Windows	ID de teclado de Windows	Distribución Linux VDA
ara	-	ar-SA	00000401	ara
ara	azerty	ar-DZ	00020401	ara
at	-	de-AT	00000407	at
be	iso-alternate	fr-BE	0000080c	be
be	-	nl-BE	00000813	be
bg	-	bg-BG	00030402	bg
bg	fonética	bg-BG	00040402	bg

<b>Distribución del teclado Linux</b>	<b>Distribución del teclado Linux/Linux VDA</b>	<b>Configuración regional de Windows</b>	<b>ID de teclado de Windows</b>	<b>Distribución Linux VDA</b>
bg	bas_phonetic	bg-BG	00020402	bg
br	-	pt-BR	00000416	br
by	-	be-BY	00000423	by
ca	eng	en-CA	00000409	ca
ca	multix	fr-CA	00011009	ca
ca	fr-antiguo	fr-CA	00000c0c	ca
ca	-	fr-CA	00001009	ca
ch	fr	fr-CH	0000100c	ch
ch	-	de-CH	00000807	ch
cn	-	en-US	00000409	us
cz	-	cs-CZ	00000405	cz
cz	Qwerty	cs-CZ	00010405	cz
de	-	de-DE	00000407	de
de	mac	de-DE	00000407	de
dk	-	da-DK	00000406	dk
ee	-	et-EE	00000425	ee
es	-	es-ES	0000040a	es
es	mac	es-ES	0000040a	es
fi	-	fi-FI	0000040b	fi
fr	-	fr-FR	0000040c	fr
fr	mac	fr-FR	0000040c	fr
gb	-	en-GB	00000809	gb
gb	mac	en-GB	00000809	gb
gb	extd	en-GB	00000452	gb
gr	-	el-GR	00000408	gr
hr	-	hr-HR	0000041a	hr
hu	-	hu-HU	0000040e	hu

<b>Distribución del teclado Linux</b>	<b>Distribución del teclado Linux/Linux VDA</b>	<b>Configuración regional de Windows</b>	<b>ID de teclado de Windows</b>	<b>Distribución Linux VDA</b>
ie	-	en-IE	00001809	ie
il	-	he-IL	0002040d	il
in	eng	en-IN	00004009	in
iq	-	ar-IQ	00000401	iq
is	-	is-IS	0000040f	is
it	-	it-IT	00000410	it
jp	-	en-US	00000409	us
jp	mac	en-US	00000409	us
kr	-	en-US	00000409	us
latam	-	es-MX	0000080a	latam
lt	-	lt-LT	00010427	lt
lt	ibm	lt-LT	00000427	lt
lt	std	lt-LT	00020427	lt
lv	-	lv-LV	00020426	lv
no	-	nb-NO	00000414	no
pl	-	pl-PL	00000415	pl
pl	qwertz	pl-PL	00010415	pl
pt	-	pt-PT	00000816	pt
pt	mac	pt-PT	00000816	pt
ro	std	ro-RO	00010418	ro
rs	-	sr-Cyrl-RS	00000c1a	rs
rs	latin	sr-Latn-RS	0000081a	rs
ru	-	ru-RU	00000419	ru
ru	typewriter	ru-RU	00010419	ru
ru	mac	ru-RU	00000419	ru
se	-	sv-SE	0000041d	se
se	mac	sv-SE	0000041d	se

Distribución del teclado Linux	Distribución del teclado Linux/Linux VDA	Configuración regional de Windows	ID de teclado de Windows	Distribución Linux VDA
si	-	sl-SI	00000424	si
sk	-	sk-SK	0000041b	sk
sk	Qwerty	sk-SK	0001041b	sk
th	-	th-TH	0000041e	th
th	Pat	th-TH	0001041e	th
tj	-	tg-Cyrl-TJ	00000428	tj
tr	-	tr-TR	0000041f	tr
tr	f	tr-TR	0001041f	tr
tw	-	en-US	00000409	us
ua	-	uk-UA	00000422	ua
us	-	en-US	00000409	us
us	mac	en-US	00000409	us
us	dvorak	en-US	00010409	us
us	dvorak-l	en-US	00030409	us
us	dvorak-r	en-US	00040409	us
us	intl	nl-NL	00020409	us
vn	-	vi-VN	0000042a	vn

### Distribución del teclado VDA

La función de distribución del teclado VDA ayuda en el uso de esta distribución, independientemente de los parámetros de la distribución del teclado del cliente. Es compatible con los siguientes tipos de teclado: PC/XT 101, 102, 104, 105, 106.

Para utilizar la distribución del teclado en el lado del servidor:

1. Inicie el archivo `wfclient.ini`.
2. Cambie el valor del atributo `KeyboardLayout` de la siguiente manera:

```
KeyboardLayout=(Server Default)
```

El valor predeterminado del atributo `KeyboardLayout` es (User Profile).

3. Vuelva a iniciar la sesión para que los cambios surtan efecto.

### Asociación de tipos de archivos

Una instancia de Citrix Virtual Apps Services también puede publicar un archivo, en lugar de una aplicación o un escritorio. Este proceso se denomina publicación de contenido y permite que pnbrowse abra el archivo publicado.

Existe una limitación en los tipos de archivo que reconoce la aplicación Citrix Workspace para Linux. Para que el sistema reconozca el tipo de archivo del contenido publicado y que los usuarios lo vean a través de la aplicación Citrix Workspace, debe asociarse una aplicación publicada con el tipo de archivo publicado. Por ejemplo, para ver un archivo Adobe PDF publicado a través de la aplicación Citrix Workspace, debe publicarse una aplicación como Adobe PDF Viewer. A menos que se publique una aplicación adecuada, los usuarios no podrán ver el contenido publicado.

Para habilitar la asociación de tipos de archivo del lado del cliente:

1. Asegúrese de que la aplicación que quiere asociar sea una aplicación favorita o suscrita.
2. Para obtener la lista de aplicaciones publicadas y la URL del servidor, ejecute los comandos:

```
1 ./util/storebrowse -l
2
3 ./util/storebrowse -S <StoreFront URL>
```

3. Ejecute el comando `./util/ctx_app_bind` con la siguiente sintaxis:

```
./util/ctx_app_bind [-p] example_file|MIME-type published-application [
server|server-URI]
```

Por ejemplo:

```
./util/ctx_app_bind a.txt BVT_DB.Notepad_AWTSVDA-0001 https://awddc1.
bvt.local/citrix/store/discovery
```

4. Asegúrese de que el archivo que está intentando abrir esté habilitado para la asignación de unidades de cliente (CDM).
5. Haga doble clic en el archivo para abrirlo mediante la aplicación asociada.

### Asociar una aplicación publicada a tipos de archivo

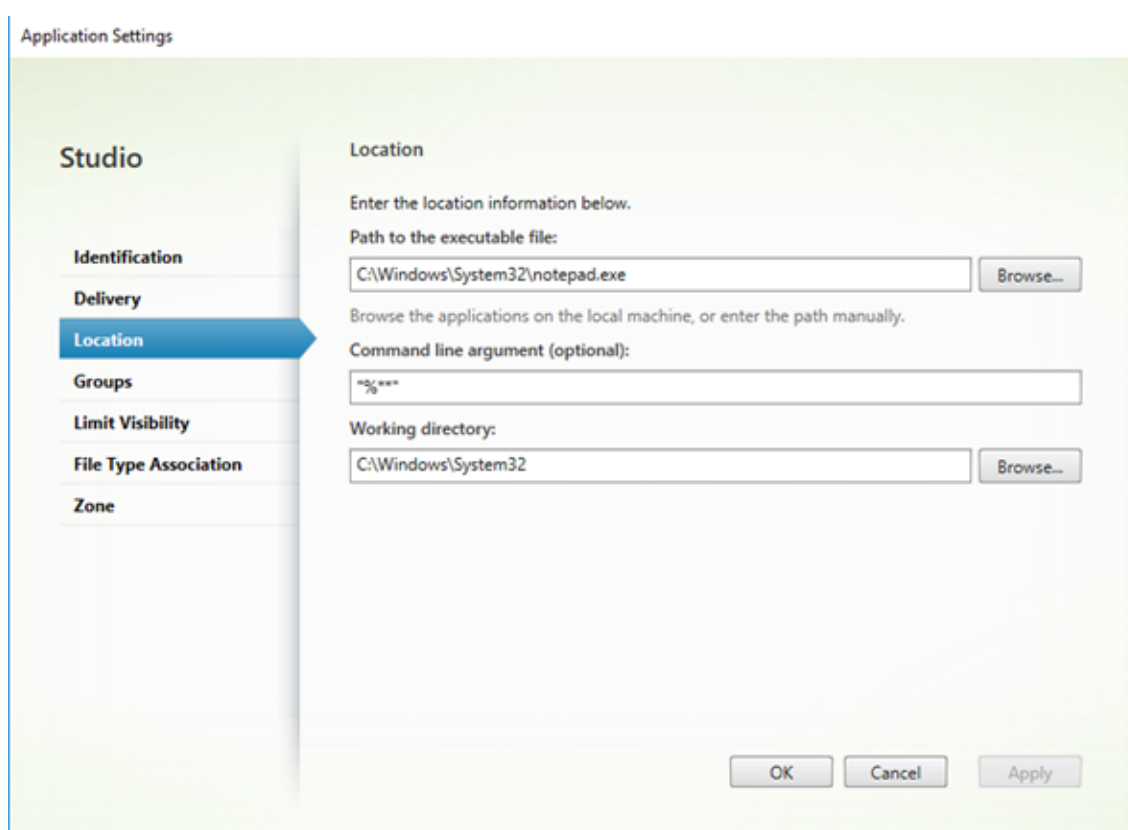
La aplicación Citrix Workspace para Android lee y aplica los parámetros configurados por los administradores en Citrix Studio.

#### Requisito previo:

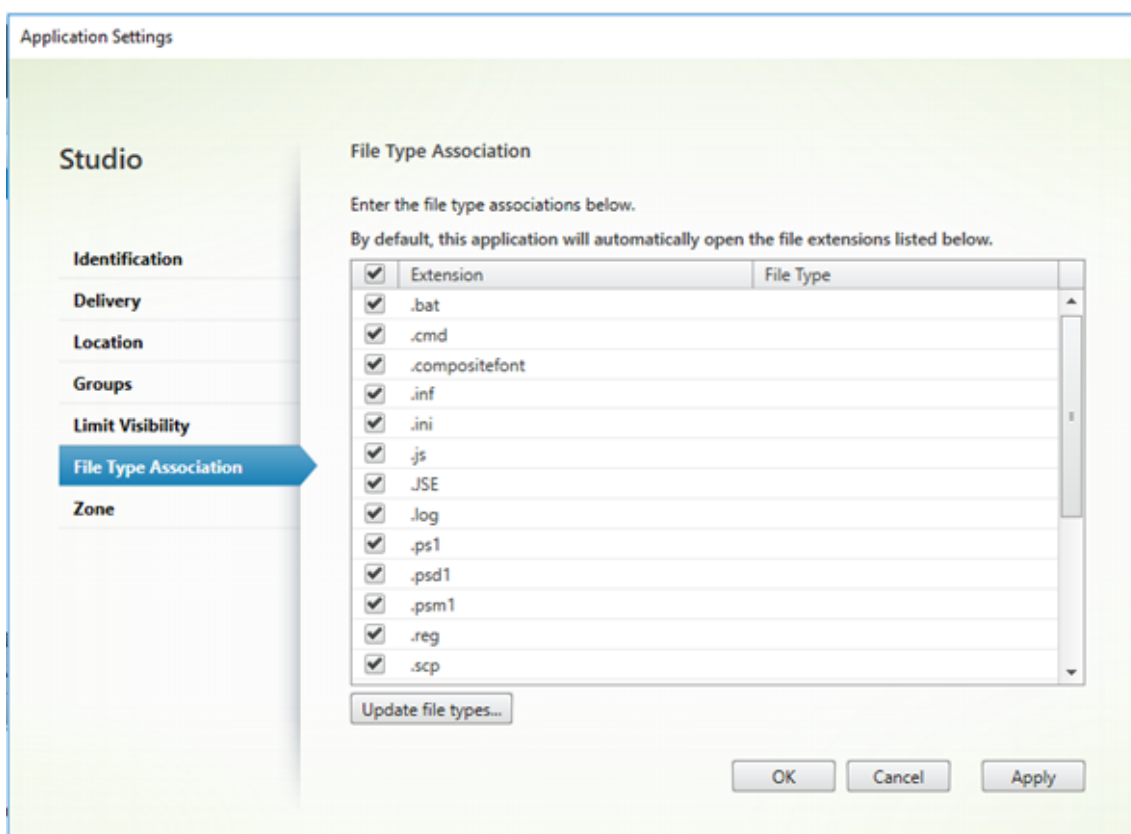
Debe conectarse al servidor del almacén donde está configurada la asociación de tipos de archivo (FTA).

Para vincular una extensión de nombre de archivo a una aplicación Citrix Workspace para Linux:

1. Publique la aplicación.
2. Inicie sesión en Citrix Studio.
3. Haga clic con el botón secundario en la aplicación y seleccione **Propiedades**.
4. Seleccione **Ubicación**.
5. Agregue “%\*\*” al campo de argumento de la línea de comandos (opcional) para omitir la validación de líneas de comandos y, a continuación, haga clic en Aceptar.



6. Haga clic con el botón secundario en la aplicación y seleccione **Propiedades**.
7. Seleccione **Asociación de tipos de archivo**.
8. Seleccione las extensiones que quiere que Citrix Workspace asocie con la aplicación.



9. Haga clic en **Aplicar** y en **Actualizar tipos de archivo**.
10. Siga los pasos mencionados en [Asociación de tipos de archivos](#) para habilitar la asociación de tipos de archivo del lado del cliente.

**Nota:**

Asegúrese de que la asociación de tipos de archivo de StoreFront esté activada. De forma predeterminada, la asociación de tipos de archivo está habilitada.

## Soporte para Citrix Analytics

La aplicación Citrix Workspace para Linux está instrumentada para transmitir registros de forma segura a Citrix Analytics cuando la aplicación desencadene determinados eventos. Los registros se analizan y almacenan en servidores Citrix Analytics cuando están habilitados. Para obtener más información sobre Citrix Analytics, consulte la documentación de [Citrix Analytics](#).

## Interfaz de usuario transparente

El protocolo ICA de Citrix utiliza el protocolo de canal virtual [TUI VC] para interfaces de usuario transparentes con el objetivo de transmitir datos entre servidores de Citrix Virtual Apps and Desktops y

servidores host. El protocolo TUI transmite mensajes de componentes de interfaz de usuario [IU] para conexiones remotas.

La aplicación Citrix Workspace para Linux admite la función TUI VC. Esta función ayuda al cliente a recibir los paquetes TUI enviados por el servidor, y el cliente puede acceder a los componentes relacionados con la IU. Esta funcionalidad le ayuda a controlar la visualización de la pantalla superpuesta predeterminada. Puede activar y desactivar el indicador `VDTUI` en el archivo `module.ini`: `VDTUI - On/Off`

Para obtener más información sobre los canales virtuales, consulte [Canales virtuales ICA de Citrix](#) en la documentación de Citrix Virtual Apps and Desktops.

## Autenticarse

July 30, 2021

Para ofrecer una mejor experiencia, a partir de la aplicación Citrix Workspace 2012, presentamos el cuadro de diálogo de autenticación dentro de la aplicación Citrix Workspace y mostramos los detalles del almacén en la pantalla de inicio de sesión. Ciframos y almacenamos tokens de autenticación para que no tenga que volver a introducir credenciales cuando se reinicie el sistema o la sesión.

### Nota:

Esta mejora de la autenticación solo se aplica a implementaciones en la nube.

### Requisito previo:

Debe instalar la biblioteca `libsecret`.

Esta función está inhabilitada de forma predeterminada.

### Para habilitar esta mejora:

1. Busque el archivo de configuración: `$ICAROOT/config/AuthManConfig.xml`.
2. Establezca el valor de `AuthManLiteEnabled` en **true**.

## Tarjeta inteligente

Para configurar la compatibilidad con tarjetas inteligentes en la aplicación Citrix Workspace para Linux, debe configurar el servidor de StoreFront a través de la consola de StoreFront.

La aplicación Citrix Workspace admite lectores de tarjetas inteligentes compatibles con los controladores PCSC-Lite y PKCS #11. Ahora, la aplicación Citrix Workspace busca `opensc-pkcs11.so` en una de las ubicaciones estándares de forma predeterminada.



La aplicación Citrix Workspace puede encontrar `opensc-pkcs11.so` en una ubicación no estándar u otro controlador de `PKCS\##11`. Puede almacenar la ubicación respectiva mediante el siguiente procedimiento:

1. Busque el archivo de configuración: `$ICAROOT/config/AuthManConfig.xml`.
2. Busque la línea `<key>PKCS11module</key>` y agregue la ubicación del controlador al elemento `<value>` que hay justo después de la línea.

**Nota:**

Si indica un nombre de archivo para la ubicación del controlador, la aplicación Citrix Workspace va a ese archivo en el directorio `$ICAROOT/PKCS\ ##11`. Si no, también puede utilizar una ruta de acceso absoluta que empiece por `“/”`.

Después de extraer una tarjeta inteligente, debe configurar el comportamiento de la aplicación Citrix Workspace. Para ello, actualice `SmartCardRemovalAction` en el archivo de configuración siguiendo estos pasos:

1. Busque el archivo de configuración: `$ICAROOT/config/AuthManConfig.xml`.
2. Busque la línea `<key>SmartCardRemovalAction</key>` y agregue `noaction` o `forcelogout` al elemento `<value>` que hay justo después de la línea.

El comportamiento predeterminado es `noaction`. No se realiza ninguna acción para borrar las credenciales almacenadas y los tokens generados al extraer la tarjeta inteligente.

La acción `forcelogout` borra todas las credenciales y todos los tokens que hubiera en StoreFront al extraer la tarjeta inteligente.

### Habilitar la compatibilidad con tarjetas inteligentes

La aplicación Citrix Workspace admite varios lectores de tarjetas inteligentes si la tarjeta inteligente está habilitada tanto en el servidor como en la aplicación Citrix Workspace.

Puede usar tarjetas inteligentes con estos fines:

- Autenticación de inicio de sesión con tarjeta inteligente: Permite la autenticación en los servidores de Citrix Virtual Apps.
- Compatibilidad con aplicaciones de tarjetas inteligentes: Permite que las aplicaciones publicadas compatibles con tarjetas inteligentes puedan acceder a dispositivos de tarjetas inteligentes locales.

Los datos de la tarjeta inteligente contienen información confidencial de seguridad, y deben transmitirse a través de un canal autenticado y seguro, como TLS.

La compatibilidad con tarjetas inteligentes tiene los siguientes requisitos previos:

- Sus lectores de tarjetas inteligentes y aplicaciones publicadas deben ser compatibles con el estándar de la industria PC/SC.
- Instale el controlador apropiado para su tarjeta inteligente.
- Instale el paquete PC/SC Lite.
- Debe instalar y ejecutar el demonio `pcscd`, lo que proporciona al middleware acceso mediante PC/SC a las tarjetas inteligentes.
- En un sistema de 64 bits, las versiones de 32 y 64 bits del paquete “libpcsclite1” deben estar presentes.

Para obtener más información sobre cómo configurar la compatibilidad con tarjetas inteligentes en los servidores, consulte [Tarjetas inteligentes](#) en la documentación de Citrix Virtual Apps and Desktops.

### Compatibilidad con autenticación de varios factores (nFactor)

La autenticación de varios factores mejora la seguridad de las aplicaciones porque requiere que los usuarios proporcionen varias pruebas de identidad para obtener acceso. La autenticación de varios factores hace que el administrador pueda configurar los pasos de autenticación y los formularios de recopilación de credenciales asociados.

La aplicación Citrix Workspace nativa admite este protocolo a partir de la funcionalidad de formularios de inicio de sesión ya implementada para StoreFront. Las páginas de inicio de sesión web de los servidores virtuales de Citrix Gateway y Traffic Manager también utilizan este protocolo.

Para obtener más información, consulte [Autenticación SAML](#) y [Autenticación de varios factores \(nFactor\)](#) en la documentación de Citrix ADC.

## Protección

April 16, 2021

Para proteger la comunicación entre el sitio y la aplicación Citrix Workspace, se pueden integrar las conexiones de la aplicación Citrix Workspace a través de tecnologías de seguridad como Citrix Gateway.

#### Nota:

Citrix recomienda utilizar Citrix Gateway entre los servidores de StoreFront y los dispositivos de los usuarios.

- Un firewall: Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino. Si utiliza la aplicación Citrix Workspace a través de un firewall que asigna la dirección IP de red interna del servidor a una dirección de Internet externa (es decir, traducción de direcciones de red, NAT), configure la dirección externa.

- Servidor de confianza.
- Solo para implementaciones de Citrix Virtual Apps (no se aplica a XenDesktop 7): Un servidor proxy SOCKS o un servidor proxy seguro (también conocido como servidor proxy de seguridad, servidor proxy HTTPS o servidor proxy de túnel TLS). Se pueden utilizar servidores proxy para limitar el acceso hacia y desde la red, y para gestionar las conexiones entre la aplicación Citrix Workspace y los servidores. La aplicación Citrix Workspace admite protocolos de proxy seguro y SOCKS.
- Solo para implementaciones de Citrix Virtual Apps: Soluciones Citrix Secure Web Gateway o Traspaso SSL con protocolos TLS (Transport Layer Security). Se admite de la versión 1.0 a la versión 1.2 de TLS.

### Citrix Gateway

Citrix Gateway (antes llamado Access Gateway) protege las conexiones a los almacenes de StoreFront, y permite a los administradores un control detallado del acceso de los usuarios a los escritorios y las aplicaciones.

Para conectarse a escritorios y aplicaciones a través de Citrix Gateway:

1. Especifique la dirección URL de Citrix Gateway que le suministre el administrador. Puede hacerlo mediante alguno de estos procedimientos:
  - La primera vez que use la interfaz de usuario de autoservicio, se le solicitará que introduzca la dirección URL en el cuadro de diálogo Agregar cuenta
  - Cuando utilice más tarde la interfaz de usuario de autoservicio, puede introducir la URL en Preferencias > Cuentas > Agregar
  - Si quiere establecer una conexión mediante el comando storebrowse, escriba la dirección URL en la línea de comandos

La dirección URL especifica la puerta de enlace y, si quiere, un almacén concreto:

- Para conectar con el primer almacén que encuentre la aplicación Citrix Workspace, use una URL con, por ejemplo, el formato: <https://gateway.company.com>.
  - Para conectar con un almacén específico, use una URL con, por ejemplo, el formato: <https://gateway.company.com?<storename>>. Esta dirección URL dinámica no tiene el formato estándar; no incluya = (el signo igual) en la URL. Si quiere establecer una conexión a un almacén concreto mediante storebrowse, puede que se necesiten comillas alrededor de la dirección URL en el comando storebrowse.
2. Cuando se le solicite, conéctese al almacén (a través de la puerta de enlace) con su nombre de usuario, contraseña y token de seguridad. Para obtener más información sobre este paso, consulte la documentación de Citrix Gateway.

Una vez completado el proceso de autenticación, se muestran los escritorios y las aplicaciones.

## Servidor proxy

Los servidores proxy se utilizan para limitar el acceso entrante y saliente de la red, y para gestionar conexiones entre la aplicación Citrix Workspace y los entornos de Citrix Virtual Apps and Desktops. La aplicación Citrix Workspace admite el protocolo SOCKS, junto con Citrix Secure Web Gateway y Traspaso SSL Citrix, el protocolo de proxy seguro y la autenticación de desafío y respuesta de Windows NT (NTLM).

La lista de tipos de proxy admitidos está restringida por el contenido de Trusted\_Regions.ini y Untrusted\_Regions.ini a los tipos Auto (automático), None (ninguno) y Wpad. Si usa otros tipos (SOCKS, Secure o Script), modifique esos archivos para agregarlos a la lista de permitidos.

### Nota:

Para garantizar una conexión segura, habilite TLS.

## Servidor proxy seguro

La configuración de conexiones para utilizar el protocolo de proxy seguro también habilita la autenticación de desafío y respuesta de Windows NT (NTLM). Si este protocolo está disponible, se detectará y se utilizará en el momento de la ejecución sin ninguna configuración adicional.

### Importante:

La compatibilidad con NTLM requiere las bibliotecas OpenSSL 1.1.1d y libcrypto.so. Instale las bibliotecas en el dispositivo del usuario. Estas bibliotecas se incluyen a menudo en las distribuciones de Linux. También puede descargarlas desde <http://www.openssl.org/>.

## Secure Web Gateway y SSL

Puede integrar la aplicación Citrix Workspace con los servicios Citrix Secure Web Gateway o servicio de Traspaso SSL. La aplicación Citrix Workspace admite el protocolo TLS. TLS (Transport Layer Security) es la versión estándar más reciente del protocolo SSL. La organización Internet Engineering Taskforce (IETF) le cambió el nombre a TLS al asumir la responsabilidad del desarrollo de SSL como un estándar abierto. TLS protege las comunicaciones de datos mediante la autenticación del servidor, el cifrado del flujo de datos y la comprobación de la integridad de los mensajes. Algunas organizaciones, entre las que se encuentran organizaciones del gobierno de los EE. UU., requieren el uso de TLS para proteger las comunicaciones de datos. Estas organizaciones también pueden exigir el uso de cifrado validado, como FIPS 140 (Estándar federal de procesamiento de información). FIPS 140 es un estándar para cifrado.

## Secure Web Gateway

Es posible usar Citrix Secure Web Gateway en modo Normal o en modo Relay (Traspaso) para proporcionar un canal de comunicaciones seguro entre la aplicación Citrix Workspace y el servidor. No es necesario configurar la aplicación Citrix Workspace si se utiliza Citrix Secure Web Gateway en el modo Normal.

Si se instala Citrix Secure Web Gateway Proxy en un servidor de una red segura, se puede utilizar Citrix Secure Web Gateway Proxy en modo de traspaso (Relay). Para obtener más información, consulte la documentación de [Citrix Virtual Apps](#) (Citrix Secure Web Gateway).

Si se utiliza el modo de traspaso, el servidor Citrix Secure Web Gateway funciona como un proxy y es necesario configurar la aplicación Citrix Workspace para que use lo siguiente:

- El nombre de dominio completo (FQDN) del servidor Citrix Secure Web Gateway.
- El número de puerto del servidor Citrix Secure Web Gateway. El modo de traspaso no se ofrece en la versión 2.0 de Citrix Secure Web Gateway.

El nombre de dominio completo (FQDN) debe tener los siguientes tres componentes, consecutivamente:

- Nombre de host
- Dominio intermedio
- Dominio superior

Por ejemplo: `mi_equipo.mi_empresa.com` es un nombre de dominio completo porque contiene el nombre de host (`mi_equipo`), un dominio intermedio (`mi_empresa`) y un dominio superior (`com`). Por lo general, la combinación de nombre de dominio intermedio y dominio superior (`mi_empresa.com`) se conoce como nombre de dominio.

## Traspaso SSL

De forma predeterminada, el Traspaso SSL Citrix utiliza el puerto TCP 443 en el servidor de Citrix Virtual Apps para las comunicaciones protegidas con SSL/TLS. Cuando el Traspaso SSL recibe una conexión TLS, descifra los datos antes de redirigirlos al servidor.

Si configuró el Traspaso SSL para un puerto de escucha distinto a 443, debe especificar en la aplicación Citrix Workspace ese número de puerto de escucha no estándar.

Puede utilizar el Traspaso SSL Citrix para proteger las comunicaciones:

- Entre un dispositivo de usuario habilitado con TLS y un servidor

Para obtener más información sobre la configuración y el uso del Traspaso SSL para proteger la instalación, consulte la documentación de [Citrix Virtual Apps](#).

## TLS

Se puede controlar las versiones del protocolo TLS que se pueden negociar si agrega las siguientes opciones de configuración en la sección [WFClient]:

- MinimumTLS=1.2
- MaximumTLS=1.2

Estos son los valores predeterminados implementados en el código. No obstante, puede ajustarlos según sea necesario.

### Nota:

- Estos valores se leen en el momento de iniciar los programas. Si los cambia después de haber iniciado self-service o storebrowse, debe escribir: **killall AuthManagerDaemon ServiceRecord selfservice storebrowse**.
- La aplicación Citrix Workspace para Linux no permite usar el protocolo SSLv3.

Para seleccionar el conjunto de cifrado, agregue la siguiente opción de configuración en la sección [WFClient]:

- SSLCiphers=GOV

Este es el valor predeterminado. Otros valores reconocidos son COM y ALL.

### Nota:

Al igual que con la configuración de la versión de TLS, si lo cambia después de haber iniciado self-service o storebrowse, debe escribir:

**killall AuthManagerDaemon ServiceRecord selfservice storebrowse**

## Actualización criptográfica

Esta función es un cambio importante en el protocolo de comunicación segura. Los conjuntos de cifrado con el prefijo TLS\_RSA\_ que no ofrecen confidencialidad directa se consideran débiles.

Los conjuntos de cifrado TLS\_RSA\_ se han eliminado por completo. En su lugar, se admiten los conjuntos de cifrado avanzados TLS\_ECDHE\_RSA\_. Si su entorno no está configurado con los conjuntos de cifrado TLS\_ECDHE\_RSA\_, los inicios de sesión clientes no se admiten debido a cifrados débiles. Para la autenticación de clientes, se admiten claves RSA de 1536 bits.

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)

DTLS v1.0 admite los siguientes conjuntos de cifrado:

- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV

DTLS v1.2 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
- TLS\_EMPTY\_RENEGOTIATION\_INFO\_SCSV

**Nota:**

A partir de la versión 1903 y posteriores, DTLS se admite en Citrix Gateway 12.1 y versiones posteriores. Para obtener información sobre los conjuntos de cifrado compatibles con DTLS para Citrix Gateway, consulte [Soporte para el protocolo DTLS](#).

### Conjuntos de cifrado

Para habilitar diferentes conjuntos de cifrado, cambie el valor del parámetro `SSLCiphers` a `ALL`, `COM` o `GOV`. De forma predeterminada, la opción está establecida en `ALL` en el archivo `All_Regions.ini` del directorio `$ICAROOT/config`.

`ALL`, `GOV` y `COM` proporcionan los siguientes conjuntos de conjuntos de cifrado:

- `ALL`
  - Están disponibles los 3 conjuntos de cifrado.
- `GOV`
  - `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)`
  - `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)`
- `COM`
  - `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)`

Para obtener información sobre la solución de problemas, consulte [Conjuntos de cifrado](#).

Los conjuntos de cifrado con el prefijo `TLS_RSA_` no ofrecen confidencialidad directa. Por lo general, estos conjuntos de cifrado se consideran obsoletos en el sector de las TIC. Sin embargo, por compatibilidad con versiones anteriores de Citrix Virtual Apps and Desktops, la aplicación Citrix Workspace para Linux dispone de una opción para utilizar estos conjuntos de cifrado.

Para una mayor seguridad, establezca el indicador `Enable\_\_TLS\_\_RSA\_\_` en `False`.

A continuación, dispone de la lista de conjuntos de cifrado retirados:

- `TLS_RSA_AES256_GCM_SHA384`
- `TLS_RSA_AES128_GCM_SHA256`
- `TLS_RSA_AES256_CBC_SHA256`
- `TLS_RSA_AES256_CBC_SHA`

- TLS\_RSA\_AES128\_CBC\_SHA
- TLS\_RSA\_3DES\_CBC\_EDE\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_MD5
- TLS\_RSA\_WITH\_RC4\_128\_SHA

**Nota:**

Los dos últimos conjuntos de cifrado utilizan el algoritmo RC4 y se han retirado porque no son seguros. El conjunto de cifrado TLS\_RSA\_3DES\_CBC\_EDE\_SHA también se puede considerar retirado. Puede usar estos indicadores para aplicar todos estos elementos retirados.

Para obtener información sobre la configuración de DTLS 1.2, consulte la sección [Transporte adaptable](#) de la documentación de Citrix Virtual Apps and Desktops.

**Requisito previo:**

Si utiliza la versión 1901 o una anterior, siga estos pasos:

Si .ICAClient ya está presente en el directorio de inicio del usuario actual:

- Elimine el archivo `All\_Regions.ini`

O bien

- Para conservar el archivo `AllRegions.ini`, agregue las siguientes líneas al final de la sección [Network\SSL]:
  - Enable\_RC4-MD5=
  - Enable\_RC4\_128\_SHA=
  - Enable\_TLS\_RSA=

Si la carpeta .ICAClient no está presente en la carpeta particular del usuario actual, entonces es que indica una nueva instalación de la aplicación Citrix Workspace. En ese caso, se conserva la configuración predeterminada para la funcionalidad.

En la tabla siguiente se enumeran los conjuntos de cifrado en cada grupo:

Tabla 1: Tabla de compatibilidad de los conjuntos de cifrado



Ciphersuite	Native Crypto Kit mode and cipher set								
	Open			FIPS			SP800-52		
	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y		Y	Y		Y	Y	
TLS_RSA_WITH_AES_256_GCM_SHA384 (1) (2)	X								
TLS_RSA_WITH_AES_128_GCM_SHA256 (1) (2)	X	X							
TLS_RSA_WITH_AES_256_CBC_SHA (2)	X								
TLS_RSA_WITH_AES_128_CBC_SHA (2)	X	X							
TLS_RSA_WITH_RC4_128_CBC_SHA (2) (3)	X	X							
TLS_RSA_WITH_RC4_128_CBC_MD5 (2) (3)	X	X							
TLS_RSA_WITH_3DES_EDE_CBC_SHA (2)	X								
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	Y	Y	Y	Y	Y	Y	Y	Y	Y
<b>Notes</b>									
(1) Ciphersuites that require TLS1.2/DTLS 1.2									
(2) Ciphersuites disabled by default									
(3) Ciphersuites not available for DTLS protocol									
Y - Supported ciphersuites									
X - Deprecated ciphersuites									

**Nota:**

Todos los conjuntos de cifrado anteriores cumplen con FIPS y SP800-52. Los dos primeros están permitidos solo para conexiones (D)TLS1.2. Consulte **Tabla 1: Tabla de compatibilidad de los conjuntos de cifrado** para obtener una representación completa de la compatibilidad con los conjuntos de cifrado.

## Storebrowse

July 6, 2020

Storebrowse es una utilidad ligera de línea de comandos que interactúa entre el cliente y el servidor. Con la utilidad storebrowse, los administradores pueden automatizar las siguientes operaciones cotidianas:

- Agregar un almacén.
- Producir una lista de las aplicaciones y los escritorios publicados desde un almacén configurado.
- Suscribir y cancelar la suscripción de aplicaciones y escritorios de un almacén configurado.
- Habilitar e inhabilitar accesos directos para aplicaciones y escritorios publicados.
- Iniciar aplicaciones publicadas.
- Volver a conectarse a sesiones desconectadas.

La utilidad storebrowse suele estar disponible en la carpeta `/util`. Puede encontrarla en la ubicación de la instalación. Por ejemplo, `/opt/Citrix/ICAClient/util`.

## Requisitos previos

La utilidad storebrowse requiere el paquete de biblioteca **libxml2**.

## Iniciar aplicaciones y escritorios publicados

Hay dos formas de iniciar un recurso:

- Puede utilizar los comandos de la línea de comandos y de storebrowse.
- Puede utilizar la interfaz de usuario para iniciar recursos.

En este artículo se describen los comandos de storebrowse.

## Utilizar comandos

En la siguiente sección se detallan los comandos de storebrowse que puede utilizar desde la utilidad storebrowse.

### **-a, -addstore**

#### **Descripción:**

Agrega un nuevo almacén con detalles sobre la puerta de enlace, la baliza y el proceso de demonio ServiceRecord. Este comando devuelve la URL completa del almacén. Aparece un error si no se puede agregar un almacén.

#### **Ejemplo de comando en StoreFront:**

Comando:

```
./storebrowse -a *URL of StoreFront or a PNAStore*
```

Ejemplo:

```
./storebrowse -a https://my.firstexamplestore.net
```

#### **Nota:**

Puede agregar varios almacenes mediante la utilidad storebrowse.

### **-, -h, -help**

#### **Descripción:**

Ofrece información detallada sobre el uso de la utilidad storebrowse

### **-l --liststore**

#### **Descripción:**

Muestra los almacenes que ha agregado.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -l
```

### **-E --enumerate**

#### **Descripción:**

Muestra los recursos disponibles. De forma predeterminada, aparecen los siguientes valores:

- Nombre del recurso
- Nombre simplificado
- Carpeta del recurso

Para ver más información, adjunte el comando **-M** (`--details`) al comando **-E**.

#### **Nota:**

Al ejecutar el comando **-E**, aparece una ventana de autenticación si antes no proporcionó sus credenciales.

Escriba toda la URL del almacén según lo indicado por **-liststore**.

#### **Ejemplo de comando en StoreFront:**

- `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -E -M https://my.firstexamplestore.net/Citrix/Store/discovery`

### **-S --subscribed**

#### **Descripción:**

Enumera los recursos suscritos. De forma predeterminada, aparecen los siguientes valores:

- Nombre del recurso
- Nombre simplificado
- Carpeta del recurso

Para ver más información, adjunte el comando **-M** (`--details`) al comando **-E**.

#### **Ejemplo de comando en StoreFront:**

- `./storebrowse.exe -S https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse.exe -S -M https://my.firstexamplestore.net/Citrix/Store/discovery`

### **-M -details**

#### **Descripción:**

Este comando devuelve varios atributos de las aplicaciones publicadas. Este comando suele utilizarse con los comandos **-E** y **-S**. Este comando toma un argumento que es la suma de los números correspondientes a los detalles requeridos:

- Publisher(0x1)
- VideoType(0x2)
- SoundType(0x4)
- AppInStartMenu(0x8)
- AppOnDesktop(0x10)
- AppIsDesktop(0x20)
- AppIsDisabled(0x40)
- WindowType(0x80)
- WindowScale(0x100)
- DisplayName(0x200)
- AppIsMandatory(0x10000)
- CreateShortcuts(0x100000)
- RemoveShortcuts(0x200000)

#### **Notas:**

- Para crear entradas de menú para aplicaciones suscritas, utilice el argumento CreateShortcuts(0x100000) con los comandos **-S**, **-s** y **-u**.
- Para eliminar todas las entradas de menú, utilice RemoveShortcuts(0x200000) con el comando **-S**.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse.exe -S -M 0x264 https://my.firstexamplestore.net/Citrix/Store/discovery
```

Donde 0x264 es la combinación de DisplayName(0x200), AppIsDisabled(0x40), AppIsDesktop(0x20) y SoundType(0x4). El resultado muestra los recursos suscritos y sus detalles.

Puede utilizar el comando **-M** para enumerar los recursos con los detalles necesarios:

```
./storebrowse.exe -E -M 0x264 https://my.firstexamplestore.net/Citrix/Store/discovery
```

**Notas:**

- Puede expresar los valores en formato decimal o hexadecimal. Por ejemplo, 512 para 0x200.
- Cuando algunos de los detalles no están disponibles a través de storebrowse, el valor resultante es cero.

**-s -subscribe**

**Descripción:**

Suscribe el recurso especificado de un almacén.

**Ejemplo de comando en StoreFront:**

```
./storebrowse -s <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

**-u -unsubscribe**

**Descripción:**

Cancela la suscripción del recurso especificado de un almacén.

**Ejemplo de comando en StoreFront:**

```
./storebrowse -u <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

**-L -launch**

**Descripción:**

Inicia una conexión con un recurso publicado. A continuación, la utilidad se cierra automáticamente, lo que deja una sesión conectada correctamente.

**Ejemplo de comando en StoreFront:**

```
./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery
```

**-i -icons**

**Descripción:**

Este comando obtiene iconos de escritorio y aplicación en formato PNG. Este comando se utiliza con los comandos **-E** o **-S**.

Para obtener iconos de tamaños y profundidades requeridos, utilice el método del argumento **best** o del argumento **size**.

### Argumento **best**

Con el método del argumento **best**, puede obtener los iconos del mejor tamaño disponibles en el servidor. Más tarde, puede ajustar los iconos a los tamaños requeridos. El método del argumento **best** es la forma más eficiente de almacenar, aplicar ancho de banda y simplificar la creación de scripts. Los archivos se guardan en formato `<nombre del recurso>.PNG`.

### Argumento **size**

Para obtener iconos de tamaños y profundidades especificados, utilice el método del argumento **size**. Aparece un error si el servidor no puede obtener iconos de un tamaño o una profundidad determinados.

El argumento **size** tiene la forma **WxB**, donde:

- **W** es el ancho de los iconos. Todos los iconos son cuadrados, por lo que solo se necesita un valor para especificar el tamaño.
- **B** es la profundidad de color. Es decir, la cantidad de bits por píxel.

#### Nota:

El valor **W** es obligatorio. El valor **B** es opcional.

Si deja los valores sin especificar, aparecerán iconos de todas las profundidades de imagen disponibles. Los archivos se guardan en el formato `<nombre del recurso>_WxWxB.png`.

Los dos métodos guardan iconos en formato **PNG** para cada recurso que devuelven los comandos **-E** o **-S**.

Los iconos se almacenan en la carpeta **.ICAClient/cache/icons**.

### Ejemplo de comando en StoreFront:

- `./storebrowse -E -i best https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -S -i 16x16 https://my.firstexamplestore.net/Citrix/Store/discovery`

### **-W [r|R] --reconnect [r|R]**

#### **Descripción:**

Vuelve a conectar las sesiones desconectadas pero todavía activas del almacén especificado. La opción [r] vuelve a conectar todas las sesiones desconectadas. La opción [R] vuelve a conectar todas las sesiones activas y desconectadas.

#### **Ejemplo de comando en StoreFront:**

- `./storebrowse -Wr https://my.firstexamplestore.net/Citrix/Store/discovery`
- `./storebrowse -WR https://my.firstexamplestore.net/Citrix/Store/discovery`

### **-WD --disconnect**

#### **Descripción:**

Desconecta todas las sesiones del almacén especificado.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -WD https://my.firstexamplestore.net/Citrix/Store/discovery
```

### **-WT --logoff**

#### **Descripción:**

Cierra todas las sesiones del almacén especificado.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -WT https://my.firstexamplestore.net/Citrix/Store/discovery
```

### **-v --version**

#### **Descripción:**

Muestra la versión de la utilidad storebrowse.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -v
```

### **-r -icaroot**

#### **Descripción:**

Especifica el directorio raíz donde está instalada la aplicación Citrix Workspace para Linux. Si no se especifica, el directorio raíz se determina durante la ejecución.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -r /opt/Citrix/ICAClient
```

### **-U -username, -P -password, -D domain**

#### **Descripción:**

Pasa el nombre de usuario, la contraseña y los detalles del dominio al servidor. Este método solo funciona con almacenes PNA. Los almacenes de StoreFront ignoran este comando. Los detalles no se almacenan en la caché. Debe introducir los detalles con cada comando.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -E https://my.firstexamplestore.net/Citrix/Store/discovery -U  
user1 -P password -D domain-name
```

### **-d -deletestore**

#### **Descripción:**

Cancela el registro de un almacén con el demonio de ServiceRecord.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -d https://my.firstexamplestore.net/Citrix/Store/discovery
```

### **-c -configselfservice**

#### **Descripción:**

Obtiene y configura los parámetros de interfaz de usuario de autoservicio que se guardan en Store-Cache.ctx. Toma un argumento con el formato <entrada[=valor]>. Si solo está presente la entrada, se imprime el valor actual del parámetro. Sin embargo, si hay un valor presente, el valor se utiliza para configurar el parámetro.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -c SharedUserMode=True
```



### **-C -addCR**

#### **Descripción:**

Lee el archivo de Citrix Receiver (CR) proporcionado y le solicita que agregue cada almacén. El resultado es el mismo que el del comando **-a**, pero tiene más de un almacén, y estos están separados en líneas nuevas.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -C <path to CR file>
```

### **-K -killdaemon**

#### **Descripción:**

Cierra el demonio de storebrowse. Como consecuencia, se borran todas las credenciales y todos los tokens.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -K
```

### **-e -listerrorcodes**

#### **Descripción:**

Enumera los códigos de error registrados.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -e
```

### **-g -storegateway**

#### **Descripción:**

Establece la puerta de enlace predeterminada para un almacén que ya está registrado en el demonio de ServiceRecord.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -g "<unique gateway name>" https://my.firstexamplestore.net/  
Citrix/Store/discovery
```

#### **Nota:**

El nombre exclusivo de la puerta de enlace debe estar en la lista de puertas de enlace del almacén especificado.

### **-q, -quicklaunch**

#### **Descripción:**

Inicia una aplicación mediante la URL directa. Este comando solo funciona para almacenes de StoreFront.

#### **Ejemplo de comando en StoreFront:**

```
.\storebrowse.exe -q <https://my.firstexamplestore.net/Citrix/Store/resources/v2/Q2hJk0lmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

### **-n -nosingleshot**

#### **Descripción:**

Siempre convierte el proceso storebrowse en demonio.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -n
```

### **-F -fileparam**

#### **Descripción:**

Inicia un archivo con la ruta de acceso del archivo y el recurso especificados.

#### **Ejemplo de comando en StoreFront:**

```
./storebrowse -F "<path to file>" -L <Resource Name> <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

## **Flujo de trabajo**

En este artículo se muestra un sencillo flujo de trabajo sobre cómo iniciar una aplicación mediante los comandos de storebrowse:

1. `./storebrowse -a https://my.firstexamplestore.net`

Agrega un almacén y proporciona la URL completa de dicho almacén. Tome nota de la URL completa porque se utiliza en los comandos posteriores.

2. `./storebrowse.exe -E https://my.firstexamplestore.net/Citrix/Store/discovery`

Enumera todas las aplicaciones y escritorios publicados. Introduzca sus credenciales en la ventana emergente que aparece para el almacén registrado.

3. `./storebrowse -L <Resource_Name> https://my.firstexamplestore.net/Citrix/Store/discovery`

Inicia el recurso. Tome el valor de Resource\_Name del resultado del comando anterior.

4. `./storebrowse -K`

Este comando borra las credenciales introducidas anteriormente y termina el proceso de demonio storebrowse. Si no menciona explícitamente este comando, el proceso storebrowse se cierra una hora después.

## Solución de problemas

July 30, 2021

Este artículo contiene información que ayudará a los administradores a solucionar problemas con la aplicación Citrix Workspace para Linux.

### Conexión

Es posible que se tope con los siguientes problemas de conexión.

#### Inicio de ICA en Fedora 29/30

Es posible que ICA no se pueda iniciar en Fedora 29/30. Como solución temporal, siga estos pasos:

1. Instale openssl10 con el comando

```
1 sudo yum install compat-openssl10.x86_64
```

1. Establezca la variable de entorno en `~/.bashrc` para carga en cada sesión. Esta acción apunta a la biblioteca libcrypto antigua.

```
1 export LD_PRELOAD=/lib64/libcrypto.so.1.0.2o
2
```

```
3 > **Nota:**
4 >
5 > La aplicación funciona bien en el servidor X.Org en comparación con
    el compositor Wayland. Para las distribuciones que tienen Wayland
    como protocolo de gráficos predeterminado, quite la marca de
    comentario de cualquiera de las siguientes opciones:
6 >
7 > `WaylandEnable=false in /etc/gdm/custom.conf` o
8 > ` /et/gdm3/custome.conf`. Cierre sesión e inicie sesión para apuntar
    al servidor X.Org.
```

### **Sesión de escritorio o recurso publicado**

Si, al establecer una conexión con un servidor Windows, aparece un cuadro de diálogo con el mensaje “Connecting to server...”, pero no aparece la subsiguiente ventana de conexión, puede que deba configurar el servidor con una licencia de acceso de cliente (CAL). Para obtener más información sobre las licencias, consulte [Licencias](#).

### **Reconexión de sesión**

A veces, el intento de reconectar con una sesión que tiene una profundidad de color mayor que la solicitada por la aplicación Citrix Workspace hace que la conexión falle. Este error se debe a una falta de memoria disponible en el servidor. Si la reconexión falla, la aplicación Citrix Workspace intenta utilizar la profundidad de color original. En caso contrario, el servidor intenta iniciar una sesión nueva con la profundidad de color solicitada, con lo que deja la sesión original en estado desconectado. Sin embargo, también puede ocurrir un error en la segunda conexión si sigue faltando memoria en el servidor.

### **Nombre completo de Internet**

Citrix recomienda configurar el servidor de nombres de dominio (DNS) en su red para poder resolver los nombres de servidores a los que quiere conectarse. Si el servidor DNS no está configurado, quizás no sea posible resolver el nombre de un servidor en una dirección IP. Como alternativa, puede especificar el servidor por su dirección IP, en lugar de por su nombre. Las conexiones TLS requieren un nombre de dominio completo, no una dirección IP.

### **Error de detección de proxy**

Si su conexión está configurada para utilizar la detección automática del proxy y recibe el mensaje de error “Proxy detection failure: JavaScript error” al intentar conectarse, copie el archivo `wpad.dat` en

`$ICAROOT/util`. Ejecute el siguiente comando, donde host name es el nombre de host del servidor al que intenta conectarse:

```
cat wpad.dat | ./pacexec pac.js FindProxyForURL <http://hostname>  
hostname 2\>&1 | grep "undeclared variable"
```

Si no obtiene resultados, existe un problema grave con el archivo `wpad.dat` en el servidor y debe investigarlo. Sin embargo, si observa un resultado como “assignment to undeclared variable...”, puede solucionar el problema. Abra `pac.js` y, para cada variable mencionada en los resultados, agregue una línea en la parte superior del archivo con el siguiente formato, donde “...” es el nombre de la variable.

```
var ...;
```

### Sesiones lentas

Si una sesión no se inicia hasta que mueva el mouse, puede que haya un problema con la generación del número aleatorio en el kernel de Linux. Como solución temporal, ejecute un demonio que genere entropía, como `rngd` (que está basado en hardware) o `haveged` (de Magic Software).

### Conjuntos de cifrado

Si su conexión falla con el nuevo soporte de cifrado:

1. Puede utilizar varias herramientas para comprobar qué conjuntos de cifrado admite su servidor, entre las que se incluyen:
  - [Sslslabs.com](https://www.ssllabs.com) (requiere que el servidor tenga acceso a Internet)
  - [sslyze](https://github.com/nabla-c0d3/sslyze) (<https://github.com/nabla-c0d3/sslyze>)
2. En Linux Client WireShark busque paquete (Client Hello, Server Hello) con filtro (`ip.addr == VDAIPAddress`) para encontrar la sección SSL. El resultado tiene los conjuntos de cifrado enviados por el cliente y aceptados por el servidor.

### Citrix Optimization SDK incorrecto

El paquete Citrix Optimization SDK contiene una versión incorrecta de `UIDialogLibWebKit.so`. Como solución temporal, siga los siguientes pasos:

1. Descargue el paquete Citrix Optimization SDK versión 18.10 de la página de [Descargas](#).
  - a) Vaya a la ruta `CitrixPluginSDK/UIDialogLib/GTK`:

```
cd CitrixPluginSDK/UIDialogLib/GTK
```
  - b) Elimine todos los archivos objeto:

```
rm -rf *.o
```

c) Vaya a la carpeta WebKit:

```
cd ../WebKit
```

d) Retire el UIDialogLibWebKit.So existente:

```
rm -rf UIDialogLibWebKit.so
```

e) Utilice el siguiente comando en el directorio WebKit:

```
make all
```

Se genera el nuevo UIDialogLibWebKit.so.

f) Copie la nueva biblioteca en el directorio **\$ICAROOT/lib**.

### Conjuntos de cifrado débiles para las conexiones SSL

Al establecer una conexión TLS, la aplicación Citrix Workspace para Linux ofrece una serie de conjuntos de cifrado más moderna y restringida de forma predeterminada. Si se conecta a un servidor que requiere un conjunto de cifrado más antiguo, establezca la opción de configuración SSLCiphers=ALL en la sección [WFClient] de un archivo de configuración.

Se admiten los siguientes conjuntos de cifrado avanzado:

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0xc030), ALL, GOV
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xc028), ALL, GOV
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xc013), ALL, COM

### Pérdida de conexión

Al usar el protocolo EDT, es posible que aparezca este mensaje de error: La conexión con “...” se ha perdido. Este problema puede ocurrir si la conexión pasa a través de un enrutador con una unidad de transmisión máxima para EDT que es inferior al valor predeterminado de 1500 bytes. Haga lo siguiente:

- Defina `edtMSS=1000` en un archivo de configuración.

### Errores de conexión

Los errores de conexión pueden producir varios diálogos de error diferentes. Por ejemplo:

- “Error in connection: A protocol error occurred while communicating with the Authentication Service”
- “The Authentication Service cannot be contacted”
- “Your account cannot be added using this server address”

Estos errores pueden deberse a varios problemas, por ejemplo:

- Cuando el equipo local y el equipo remoto no pueden negociar un protocolo TLS común. Para obtener más información, consulte [TLS](#).
- Cuando el equipo remoto requiere un conjunto de cifrado más antiguo para una conexión TLS. En este caso, puede establecer la opción de configuración `SSLCiphers=ALL` en la sección `\[WFClient\]` de un archivo de configuración y ejecutar `killall AuthManagerDaemon ServiceRecord selfservice storebrowse` antes de reiniciar la conexión.
- Cuando el equipo remoto no pide el certificado de cliente de la manera apropiada. IIS solo debe **aceptar** o **solicitar** certificados para Citrix, Authentication y Certificate.
- Otros problemas.

### Conexiones con ancho de banda reducido

Citrix recomienda utilizar la versión más reciente de Citrix Virtual Apps and Desktops en el servidor y la aplicación Citrix Workspace en el dispositivo del usuario.

Si utiliza una conexión con poco ancho de banda, puede realizar cambios en la configuración de la aplicación Citrix Workspace y en la forma en que la utiliza para mejorar el rendimiento.

- **Configure la conexión de la aplicación Citrix Workspace:** La configuración de las conexiones de la aplicación Citrix Workspace puede reducir el ancho de banda que ICA requiere y, así, mejorar el rendimiento.
- **Cambie la forma en que se utiliza la aplicación Citrix Workspace:** Cambiar la forma en que se utiliza la aplicación Citrix Workspace también puede reducir el ancho de banda requerido para una conexión de alto rendimiento.
- **Habilite el sonido UDP:** Esta función puede mantener un nivel de latencia regular en redes sobrecargadas durante conexiones Voice-over-IP (VoIP).
- **Utilice las versiones más recientes de Citrix Virtual Apps y la aplicación Citrix Workspace para Linux:** Citrix aumenta y mejora constantemente el rendimiento en cada versión, y muchas funcionalidades de rendimiento requieren la versión más reciente de la aplicación Citrix Workspace y el software de servidor.

## Visualización

### Pantalla partida

El problema de pantalla partida se produce cuando dos o más fotogramas distintos aparecen en pantalla al mismo tiempo, en bloques horizontales. Este problema se ve principalmente en áreas grandes de contenido que cambia rápidamente en la pantalla. Aunque los datos se capturan en el VDA de modo que no se partan los fotogramas, y los datos se pasan al cliente de manera que tampoco se introduzca ese problema, X11 (el subsistema de gráficos de Linux/Unix) no ofrece un modo coherente de dibujar en pantalla de forma que se evite este problema.

Para evitar la pantalla partida, Citrix recomienda el enfoque estándar, que sincroniza el dibujo de la aplicación con el dibujo de la pantalla. Es decir, esperar a `vsvnc` para iniciar el dibujo del fotograma siguiente. Dispone de una serie de opciones al utilizar Linux, según el hardware de gráficos que tenga en el cliente y el administrador de ventanas que utilice. Estas opciones se dividen en dos grupos de soluciones:

- Parámetros de GPU de X11
- Usar un administrador de composición

### Parámetros de GPU de X11

Para gráficos Intel HD, cree un archivo llamado **20-intel.conf en la carpeta xorg.conf.d**, con este contenido:

Sección: “Dispositivo”

```
1 Identificador:    "Graphics"
2 Controlador:     "intel"
3 Opción:          "AccelMethod" "sna"
4 Opción:          "TearFree" "true"
```

EndSection

Para gráficos de NVIDIA, busque en la carpeta `xorg.conf.d` el archivo que contenga la opción “MetaModes” para su configuración. Para cada uno de los MetaModes utilizados, separados por comas, agregue lo siguiente:

```
{ForceFullCompositionPipeline = On}
```

Por ejemplo:

Opción: “MetaModes” “DFP-0: 1920x1200 +0+0 {ForceFullCompositionPipeline = On}”

#### Nota:

Las distintas distribuciones de Linux usan rutas diferentes para la carpeta `xorg.conf.d`. Por ejemplo: `/etc/X11/xorg.conf.d` o `/user/share/X11/xorg.conf.d`.

### Administradores de composición

Use lo siguiente:

- Compiz (integrado en Ubuntu Unity). Instale el administrador de parámetros “CompizConfig Settings Manager”.

Ejecute “CompizConfig Settings Manager”.



En “General > Composition”, desmarque la casilla “Undirect Fullscreen Windows”.

**Nota:**

Utilice “CompizConfig Settings Manager” con atención, ya que, si se cambian incorrectamente sus valores, el sistema puede dejar de responder y no iniciarse.

- Compton (una herramienta instalada como complemento). Consulte la documentación o la página man de Compton para ver información detallada. Por ejemplo, ejecute el comando:

```
compton --vsync opengl --vsync -aggressive
```

### **Entradas de teclado incorrectas**

Si utiliza un teclado en un idioma que no sea el inglés, es posible que la presentación en la pantalla no coincida con las entradas del teclado. En este caso, debe especificar el tipo y la distribución del teclado que utiliza. Para obtener más información acerca de la especificación de teclados, consulte [Control del comportamiento del teclado](#).

### **Redibujado excesivo**

Algunos administradores de ventanas informan continuamente de la posición nueva de las ventanas integradas al moverlas, lo que puede producir un redibujado excesivo. Para solucionar este problema, cambie el administrador de ventanas a un modo que solo dibuje los contornos de las ventanas cuando se muevan.

### **Compatibilidad de iconos**

La aplicación Citrix Workspace para Linux crea iconos de ventanas que son compatibles con la mayoría de los administradores de ventanas, pero no son completamente compatibles con la convención de comunicación del protocolo X Inter-Client.

### **Compatibilidad total de iconos**

Para ofrecer una compatibilidad total de iconos:

1. Abra el archivo de configuración wfclient.ini.
2. Modifique la siguiente línea en la sección [WFClient]: UseIconWindow=True
3. Guarde el archivo y ciérrelo.

### **Color del cursor**

Puede ser difícil ver el cursor si tiene el mismo color, o uno similar, al color del fondo. Para solucionar este problema, establezca que las áreas del cursor sean de color negro o blanco.

Para cambiar el color del cursor

1. Abra el archivo de configuración wfclient.ini.
2. Agregue una de las líneas siguientes a la sección [WFClient]:  
CursorStipple=ffff,ffff (para que el cursor sea negro)  
CursorStipple=0,0 (para que el cursor sea blanco)
3. Guarde el archivo y ciérrelo.

### **Flash de color**

Cuando mueva el puntero en una ventana de conexión, o fuera de ella, los colores de la ventana fuera de foco comienzan a parpadear. Este problema es una limitación conocida cuando se utiliza X Windows System con presentaciones en PseudoColor. De ser posible, utilice una profundidad de color mayor para la conexión afectada.

### **Cambios de color en presentaciones en color verdadero**

Los usuarios tienen la opción de utilizar 256 colores cuando se conectan a un servidor. En esta opción se asume que el hardware del vídeo admite paletas, para permitir que las aplicaciones cambien rápidamente los colores de la paleta con el fin de producir presentaciones animadas.

Las presentaciones en color verdadero no tienen ninguna capacidad para emular la habilidad de producir animaciones cambiando rápidamente la paleta. La emulación de software de este recurso es costosa en tiempo y en tráfico de red. Para reducir este coste, la aplicación Citrix Workspace almacena en búfer los cambios rápidos de la paleta y actualiza la paleta real solamente cada pocos segundos.

### **Pantalla incorrecta**

La aplicación Citrix Workspace utiliza la codificación de caracteres EUC-JP o UTF-8 para los caracteres japoneses, mientras que el servidor utiliza la codificación de caracteres SJIS. La aplicación Citrix Workspace no traduce entre estos grupos de caracteres. Esto puede ocasionar problemas al mostrar los archivos que están guardados en el servidor y que se ven localmente, o bien que están guardados localmente y se ven en el servidor. Este problema afecta además a los caracteres japoneses en los parámetros utilizados en el traspaso de parámetros extendidos.

### **Extensión de sesión**

Las sesiones de pantalla completa abarcan todos los monitores, pero también está disponible una opción de línea de comandos para el control de la presentación en entornos de varios monitores, -span. Con esta opción se pueden ejecutar sesiones de pantalla completa y abarcar varios monitores.

La funcionalidad de la barra de herramientas de Desktop Viewer le permite alternar entre una sesión en modo de ventana y una sesión a pantalla completa; además, admite varios monitores para los monitores intersecados.

**Importante:**

Span no tiene ningún efecto en sesiones de ventanas integradas o normales (incluidas aquellas en ventanas maximizadas).

La opción `-span` tiene el siguiente formato:

```
-span [h][o][a|mon1[,mon2[,mon3, mon4]]]
```

Si se especifica `h`, se imprime una lista de monitores en `stdout`. Si `h` es el valor completo de la opción, `wfica` se cierra.

Si se especifica `o`, la ventana de la sesión tendrá el atributo `override-redirect`.

**Precaución:**

No se recomienda el uso del valor de esta opción. Debe considerarse como último recurso, para utilizar con los administradores de ventanas que presenten dificultades de uso. El administrador de ventanas no ve la ventana de la sesión; además, la ventana no tiene icono y no se puede volver a apilar. Solo se podrá quitar finalizando la sesión.

Si se especifica `a`, la aplicación Citrix Workspace intenta crear una sesión que cubra todos los monitores.

La aplicación Citrix Workspace supone que el resto del valor de la opción `-span` es una lista de números de monitores. Un único valor selecciona un monitor específico, dos valores seleccionan los monitores en las esquinas superior izquierda e inferior derecha del área requerida, cuatro valores especifican los monitores en los bordes superior, inferior, izquierdo y derecho del área.

Si no se ha especificado `o`, `wfica` utiliza el mensaje `_NET_WM_FULLSCREEN_MONITORS` para solicitar una disposición de ventanas adecuada desde el administrador de ventanas, en caso de que se admita. De lo contrario, utiliza las directrices de tamaño y posición para solicitar la disposición deseada.

El siguiente comando se puede utilizar para probar la función del administrador de ventanas:

```
xprop -root | grep \_NET\_WM\_FULLSCREEN\_MONITORS
```

Si no obtiene resultados, no hay función disponible. Si no la hay, es posible que necesite una ventana con el atributo `override-redirect`. Puede configurar una ventana con el atributo `override-redirect` mediante `-span o`.

Para realizar una sesión que abarque varios monitores desde la línea de comandos:

1. Escriba lo siguiente en una interfaz de comandos:

```
/opt/Citrix/ICAClient/wfica -span h
```

Se imprime una lista de los números de los monitores actualmente conectados al dispositivo del usuario en stdout y wfica se cierra.

2. Tome nota de estos números de monitores.
3. Escriba lo siguiente en una interfaz de comandos:

```
/opt/Citrix/ICAclient/wfica -span \[w\[,x\[,y,z\]\]\]
```

donde [w], [x], [y] y [z] son los números de monitores obtenidos en el paso 1 mencionado anteriormente, y un único valor [w] especifica un monitor en particular, dos valores [w] y [x] especifican monitores en las esquinas superior izquierda e inferior derecha del área requerida, y los cuatro valores (w, x, y, z) especifican monitores en los bordes superior, inferior, izquierdo y derecho del área.

### Importante:

Defina la variable WFICA\_OPTS antes de iniciar el autoservicio a través de un explorador web. Para hacer esto, modifique su archivo de perfil que, por lo general, se encuentra en \$HOME/.bash\_profile o \$HOME/.profile, y agregue una línea para definir la variable WFICA\_OPTS. Por ejemplo:

```
export WFICA_OPTS="--span a"
```

Este cambio afecta tanto a las sesiones de Citrix Virtual Apps como a las de Virtual Desktops.

Si ha iniciado self-service o storebrowse, quite los procesos que estos iniciaron para que la nueva variable de entorno tenga efecto. Quítelos con:

```
killall AuthManagerDaemon ServiceRecord storebrowse
```

## Aplicaciones locales

Es posible que no pueda salir de una sesión a pantalla completa para utilizar aplicaciones locales u otras sesiones, ya que la IU del sistema del cliente está oculta y la función de transparencia del teclado inhabilita el comando habitual del teclado, por ejemplo, Alt + Tab, y, en su lugar, envía el comando al servidor.

Como solución temporal, presione Ctrl+F2 para desactivar temporalmente la función de teclado transparente hasta que la ventana de la sesión vuelva a estar activa y en primer plano. Otra solución temporal es establecer TransparentKeyPassthrough en No en \$ICAROOT/config/module.ini. Así, se inhabilita la función de transparencia de teclado. Sin embargo, puede que deba anular el archivo ICA. Para ello, agregue este parámetro al archivo All\_regions.ini.

## Explorador web

### Explorador local

Cuando hace clic en un vínculo en una sesión de Windows, el contenido aparece en un explorador local. La redirección de contenido servidor-cliente está habilitada en `wfclient.ini`. Esto provoca que se ejecute una aplicación local. Para inhabilitar la redirección de contenido cliente-servidor, consulte [Redirección de contenido servidor-cliente](#).

### Acceso a los recursos publicados

Cuando accede a recursos publicados, el explorador le pide que guarde un archivo. Los exploradores web distintos de Firefox y Chrome pueden requerir cierta configuración para poder conectar con un recurso publicado. Sin embargo, al intentar acceder a un recurso con un clic en su icono en la página, el explorador web le solicitará guardar el archivo ICA.

### Explorador específico

Si tiene problemas para utilizar un explorador web específico, configure la variable de entorno `BROWSER` para especificar la ruta local y el nombre del explorador web requerido antes de ejecutar `setupwfc`.

### Explorador Firefox

Cuando inicie escritorios o aplicaciones en Firefox, si la página no responde, pruebe a habilitar el plug-in ICA.

### Plug-in ICA en Firefox

Cuando el plug-in ICA está habilitado en Firefox, es posible que no se inicien ni las sesiones de escritorio ni las sesiones de aplicación. En este caso, pruebe a inhabilitar el plug-in ICA.

### Errores de configuración

Estos errores pueden producirse si configuró incorrectamente una entrada de conexión.

**E\_MISSING\_INI\_SECTION. Verifique el archivo de configuración: “..”. Falta la sección “..” en el archivo de configuración.**

El archivo de configuración se modificó incorrectamente o está dañado.

**E\_MISSING\_INI\_ENTRY. Verifique el archivo de configuración: “..”. La sección “..” debe contener una entrada “..”.**

El archivo de configuración se modificó incorrectamente o está dañado.

**E\_INI\_VENDOR\_RANGE. Verifique el archivo de configuración: "...". El rango de proveedores de servidor X "... en el archivo de configuración no es válido.**

La información sobre el proveedor del servidor X en el archivo de configuración está dañada. Comuníquese con Citrix.

### **Errores de configuración de wfclient.ini**

Estos errores pueden producirse si ha modificado incorrectamente wfclient.ini.

E\_CANNOT\_WRITE\_FILE - No se puede escribir el archivo: "..."

Se produjo un problema al guardar la base de datos de la conexión; por ejemplo, no hay espacio en el disco.

E\_CANNOT\_CREATE\_FILE - No se puede crear el archivo: "..."

Se produjo un problema al crear una base de datos de la conexión.

**E\_PNAGENT\_FILE\_UNREADABLE. No se puede leer el archivo Citrix Virtual Apps "...": No existe tal archivo o directorio.**

O bien:

**No se puede leer el archivo de Citrix Virtual Apps "...": permiso denegado.**

Está intentando acceder a un recurso a través de un menú o un elemento de escritorio, pero el archivo Citrix Virtual Apps del recurso no está disponible. Actualice la lista de los recursos publicados. Para hacerlo, seleccione Application Refresh en el menú View e intente acceder nuevamente al recurso. Si el error persiste, compruebe las propiedades del elemento de menú o del icono del escritorio y también del archivo Citrix Virtual Apps al que se refiere el icono o el elemento.

### **Errores de archivos PAC**

Estos errores pueden producirse si el entorno utiliza archivos PAC (configuración automática del proxy) para especificar configuraciones del proxy.

**Error de detección de proxy: La URL de configuración automática no es válida.**

Se especificó una dirección en el explorador con un tipo de URL no válido. Los tipos válidos son <http://> y <https://>. No se admite ningún otro tipo. Cambie la dirección a un tipo de URL válido e inténtelo nuevamente.

**Fallo de detección de proxy: La descarga HTTP del script .PAC falló: la conexión falló.**

Compruebe que no se haya introducido una dirección o un nombre incorrecto. En caso afirmativo, corrija la entrada e inténtelo nuevamente. En caso contrario, es posible que el servidor esté inactivo. Inténtelo nuevamente más tarde.

**Error de detección de proxy: Falló la descarga HTTP del script PAC. Ruta no encontrada.**

El archivo PAC solicitado no se encuentra en el servidor. Cambie esta opción en el servidor o vuelva a configurar el explorador.

**Error de detección de proxy: Falló la descarga HTTP del script PAC.**

Ocurrió un fallo de conexión al descargar el archivo PAC. Vuelva a conectarse e inténtelo nuevamente.

**Error de detección de proxy: El script de configuración automática está vacío.**

El archivo PAC está vacío. Cambie esta opción en el servidor o vuelva a configurar el explorador.

**Error de detección de proxy: No se admite JavaScript.**

Falta el archivo ejecutable PAC o el archivo de texto pac.js. Vuelva a instalar la aplicación Citrix Workspace.

**Error de detección de proxy: Error de JavaScript.**

El archivo PAC contiene código JavaScript no válido. Corrija el archivo PAC en el servidor. Consulte también [Conexión](#).

**Error de detección de proxy: Resultados no válidos del script de configuración automática del proxy.**

Se recibió una respuesta con formato incorrecto por parte del servidor. Corrija esto en el servidor o vuelva a configurar el explorador.

## Certificados

Cuando utiliza un almacén con autenticación SAML (con el protocolo AUTHv3), aparece el siguiente mensaje de error: “Unacceptable TLS Certificate”.

El problema se produce cuando se utiliza la aplicación Citrix Workspace para Linux 1906 y versiones posteriores. Para obtener instrucciones sobre la solución de problemas, consulte el artículo [CTX260336](#) en Knowledge Center.

Si el servidor de StoreFront no puede proporcionar los certificados intermedios que coincidan con el certificado que está utilizando, o si instala certificados intermedios para admitir usuarios de tarjetas inteligentes, siga estas instrucciones antes de agregar un almacén de StoreFront:

1. Obtenga uno o varios certificados intermedios por separado en formato PEM.

**Sugerencia:**

Si no puede encontrar un certificado en formato PEM, use la utilidad `openssl` para convertir un certificado en formato CRT a un archivo PEM.

2. Como el usuario que instala el paquete (normalmente root):
  - a) Copie uno o varios archivos a `$ICAROOT/keystore/intcerts`.
  - b) Ejecute el siguiente comando como usuario que instaló el paquete:

```
$ICAROOT/util/ctx_rehash
```

Si autentica un certificado de servidor que fue emitido por una entidad de certificación, pero el dispositivo de usuario todavía no confía en él, siga estas instrucciones antes de agregar un almacén de StoreFront.

1. Obtenga el certificado raíz en formato PEM.  
Sugerencia: Si no puede encontrar un certificado en este formato, use la utilidad `openssl` para convertir un certificado en formato CRT a un archivo PEM.
2. Mediante la cuenta de usuario con la que instaló el paquete (normalmente root):
  - a) Copie el archivo en `$ICAROOT/keystore/cacerts`.
  - b) Ejecute el comando siguiente:  

```
$ICAROOT/util/ctx_rehash
```

## Otros

### Problemas de conexión

Puede que se den los siguientes problemas.

### Cerrar una sesión

Si quiere saber si el servidor ha indicado a la aplicación Citrix Workspace que cierre una sesión, puede utilizar el programa `wfica` para que capture un registro cuando reciba un comando desde el servidor para terminar una sesión.

Para grabar esta información en el sistema de `syslog`, agregue `SyslogThreshold` con el valor 6 a la sección [WFClient] del archivo de configuración. Esto habilita la captura de registros de mensajes que tienen una prioridad de `LOG_INFO` o mayor. El valor predeterminado para `SyslogThreshold` es 4 (=LOG\_WARNING).

Igualmente, para que `wfica` envíe la información a la salida de “standard error”, agregue `PrintLogThreshold` con el valor 6 a la sección [WFClient]. El valor predeterminado de `PrintLogThreshold` es 0 (=LOG\_EMERG).



Para obtener más información sobre cómo iniciar sesión, consulte [Captura de registros](#) y, para obtener más información sobre la configuración syslog, consulte [configuración de syslog](#).

### **Parámetros del archivo de configuración**

Para cada entrada de wfclient.ini, debe haber una entrada correspondiente en All\_Regions.ini para que el parámetro tenga efecto. Además, para cada entrada en las secciones [Thinwire3.0], [Client-Drive] y [TCP/IP] de wfclient.ini, debe haber una entrada correspondiente en canonicalization.ini para que el parámetro tenga efecto. Consulte los archivos All\_Regions.ini y canonicalization.ini en el directorio \$ICAROOT/config para obtener más información.

### **Aplicaciones publicadas**

Si tiene problemas al ejecutar una aplicación publicada que accede a un puerto serie, es posible que falle (con o sin mensajes de error, según la aplicación propiamente dicha) si otra aplicación bloqueó el puerto. En tales circunstancias, verifique si hay alguna aplicación que haya bloqueado temporalmente el puerto serie, o bien, que haya bloqueado el puerto serie y que se haya cerrado sin desbloquearlo.

Para solucionar este problema, detenga la aplicación que está bloqueando el puerto serie. En cuanto a bloqueos del tipo UUCP, puede que se haya dejado un archivo de bloqueo después de que la aplicación finalice. La ubicación de estos archivos de bloqueo depende del sistema operativo que utilice.

### **Inicio de la aplicación Citrix Workspace**

Si la aplicación Citrix Workspace no se inicia, aparece el mensaje de error “Application default file could not be found or is out of date”. Eso puede ocurrir porque la variable de entorno ICAROOT no se definió correctamente. Esto es un requisito si instaló la aplicación Citrix Workspace en una ubicación no predeterminada. Para solucionar este problema, Citrix recomienda que realice alguna de las siguientes acciones:

- Defina ICAROOT como el directorio de instalación.

Para verificar que la variable de entorno ICAROOT está definida correctamente, intente iniciar la aplicación Citrix Workspace desde una sesión de terminal. Si el mensaje de error continúa, es probable que la variable de entorno ICAROOT no esté definida correctamente.

- Vuelva a instalar la aplicación Citrix Workspace en la ubicación predeterminada. Para obtener más información acerca de cómo instalar la aplicación Citrix Workspace, consulte [Instalación y configuración](#).

Si la aplicación Citrix Workspace se ha instalado anteriormente en la ubicación predeterminada, elimine el directorio `/opt/Citrix/ICAClient` o `$HOME/ICAClient/platform` antes de volver a instalarla.

### **Citrix CryptoKit (anteriormente, SSLSDK)**

Para encontrar el número de versión de Citrix CryptoKit (anteriormente SSLSDK) o de OpenSSL que se está utilizando, puede utilizar el siguiente comando:

```
strings libctxssl.so | grep "Citrix SSLSDK"
```

También puede ejecutar este comando en AuthManagerDaemon o en PrimaryAuthManager.

### **Teclas de acceso rápido**

Si el administrador de ventanas utiliza las mismas combinaciones de teclas para proporcionar funcionalidad nativa, las combinaciones de teclas podrían no funcionar correctamente. Por ejemplo, el administrador de ventanas KDE utiliza las combinaciones de teclas desde CTRL+MAYÚS+F1 a CTRL+MAYÚS+F4 para cambiar entre los escritorios 13 a 16. Si observa este problema, intente alguna de estas soluciones:

- El modo traducido en el teclado asigna un conjunto de combinaciones de teclas locales a combinaciones de teclas en el lado del servidor. Por ejemplo, de forma predeterminada en el modo traducido, la combinación CTRL+MAYÚS+F1 está asignada a la combinación ALT+F1 en el lado del servidor. Para reconfigurar esta asignación a una combinación de teclas local alternativa, actualice esta entrada de la sección [WFClient] del archivo \$HOME/.ICAClient/wfclient.ini. Esto asigna la combinación de teclas local ALT+CTRL+F1 a ALT+F1:
  - Cambie Hotkey1Shift=Ctrl+Shift por Hotkey1Shift=Alt+Ctrl.
- El modo directo en el teclado envía todas las combinaciones de teclas directamente al servidor. Es decir, no se procesan localmente. Para configurar el modo directo, en la sección [WFClient] de \$HOME/.ICAClient/wfclient.ini, defina TransparentKeyPassthrough con el valor Remote.
- Reconfigure el administrador de ventanas de modo que suprima las combinaciones de teclado predeterminadas.

### **Teclado croata remoto**

Este procedimiento garantiza que los caracteres ASCII se envíen correctamente a los escritorios virtuales remotos con distribuciones de teclado croatas.

1. En la sección WFClient del archivo de configuración apropiado, establezca UseEUKSforASCII con el valor True.
2. Establezca UseEUKS con el valor 2.

### **Teclado japonés**

Para configurar el uso del teclado japonés, actualice la siguiente entrada en el archivo de configuración wfclient.ini:

KeyboardLayout=Japanese (JIS)

### **Teclado ABNT2**

Para configurar el uso del teclado ABNT2, actualice la siguiente entrada en el archivo de configuración wfclient.ini:

KeyboardLayout=Brazilian (ABNT2)

### **Teclado local**

Si algunas teclas del teclado local no funcionan de la manera prevista, elija la mejor distribución de servidores de la lista que hay en \$ICAROOT/config/module.ini.

### **Reproductor de Windows Media**

Es posible que la aplicación Citrix Workspace no tenga los plug-ins de GStreamer para gestionar un formato solicitado. Normalmente, esto hace que el servidor solicite un formato distinto. Algunas veces, la comprobación inicial de plug-ins adecuados indica, incorrectamente, que sí existen. Esto debería detectarse y debe aparecer un diálogo de error en el servidor para indicar que el Reproductor de Windows Media encontró un problema al reproducir el archivo. Al volver a intentar reproducir el archivo dentro de la sesión, la operación funciona porque la aplicación Citrix Workspace ha rechazado el formato y, como resultado de ello, el servidor ha solicitado un formato distinto o bien lo ha generado él mismo.

En algunas circunstancias, la inexistencia de un plug-in adecuado no se detecta y el archivo no se reproduce correctamente, a pesar de que el indicador de progreso se mueve en el Reproductor de Windows Media.

Para evitar ver este error o evitar el fallo de reproducción en futuras sesiones:

1. Como solución temporal, agregue la opción de configuración “SpeedScreenMMAVerbose=On” en la sección [WFClient] del archivo \$Home/.ICAClient/wfclient.ini, por ejemplo.
2. Reinicie WFICA desde un autoservicio que se haya iniciado desde un terminal.
3. Reproduzca un vídeo que pueda generar este error.
4. Tome nota (en la salida de seguimiento) del tipo MIME asociado al plug-in que falta, o el tipo MIME que debería ser compatible pero no se reproduce (por ejemplo, “video/x-h264...”).
5. Modifique \$ICAROOT/config/MediaStreamingConfig.tbl. En la línea con el tipo MIME anotado, introduzca un signo “?” entre los dos puntos (:) y el tipo MIME. Esto inhabilita el formato.
6. Repita los pasos anteriores del 2 al 5 para otros formatos de medios que provoquen este error.

7. Distribuya el archivo `MediaStreamingConfig.tbl` modificado a otras máquinas con el mismo conjunto de plug-ins GStreamer.

**Nota:**

Como alternativa, después de identificar el tipo MIME puede ser posible instalar un plug-in GStreamer para descifrarlo.

### Configuración de un puerto serie

Para configurar un único puerto serie, agregue las siguientes entradas en el archivo de configuración `$ICAROOT/config/module.ini`:

```
LastComPortNum=1
```

```
ComPort1=device
```

Para configurar dos puertos serie o más, agregue las siguientes entradas en el archivo de configuración `$ICAROOT/config/module.ini`:

```
LastComPortNum=2
```

```
ComPort1=device1
```

```
ComPort2=device2
```

### Errores

Este tema contiene una lista de otros mensajes de error comunes que pueden aparecer al utilizar la aplicación Citrix Workspace.

**Ha ocurrido un error. El código del error es 11 (E\_MISSING\_INI\_SECTION). Consulte la documentación. Cerrándose.**

Al ejecutar la aplicación Citrix Workspace desde la línea de comandos, esto normalmente significa que la descripción otorgada en la línea de comandos no se ha encontrado en el archivo `appsrv.ini`.

**E\_BAD\_OPTION. La opción “..” no es válida.**

Falta el argumento para la opción “..”.

**E\_BAD\_ARG. La opción “..” tiene un argumento no válido: “..”.**

Se especificó un argumento no válido para la opción “..”.

**E\_INI\_KEY\_SYNTAX - La clave “..” en el archivo de configuración “..” no es válida.**

La información sobre el proveedor del servidor X en el archivo de configuración está dañada. Cree un archivo de configuración.

**E\_INI\_VALUE\_SYNTAX - El valor “..” en el archivo de configuración “..” no es válido.**

La información sobre el proveedor del servidor X en el archivo de configuración está dañada. Cree un archivo de configuración.

**E\_SERVER\_NAMELOOKUP\_FAILURE - No se puede conectar con el servidor “...”.**

No puede resolverse el nombre del servidor.

**No se puede escribir en uno o varios archivos: “...”. Corrija los problemas de disco lleno o de permisos, y vuelva a intentarlo.**

Verifique si existen problemas de disco lleno o problemas de permisos. Si se detecta y corrige un problema, vuelva a intentar la operación que originó el mensaje de error.

**Se perdió la conexión con el servidor. Vuelva a conectarse e inténtelo nuevamente. Puede que falten datos en estos archivos: “...”.**

Vuelva a conectarse y vuelva a intentar la operación que originó el error.

### **Información de diagnóstico**

Si tiene problemas con la aplicación Citrix Workspace, es posible que la asistencia técnica de Citrix le pida información de diagnóstico. Esta información permite al equipo diagnosticar el problema y ofrecer la ayuda necesaria para solucionarlo.

Para obtener información de diagnóstico sobre la aplicación Citrix Workspace

1. En el directorio de instalación, escriba `util/lurdump`. Se recomienda que haga esto en una sesión abierta y, si es posible, mientras el problema siga activo.

Se genera un archivo que contiene información de diagnóstico detallada, incluidos los detalles de la versión, el contenido de los archivos de configuración de la aplicación Citrix Workspace y los valores de diversas variables del sistema.

2. Revise el archivo para ver si contiene información confidencial antes de enviarlo al departamento de asistencia técnica de Citrix.

### **Solución de problemas en las conexiones con recursos**

Los usuarios pueden administrar sus conexiones activas con la Central de conexiones. La Central de conexiones es una herramienta de productividad que permite a usuarios y administradores solucionar inconvenientes en conexiones lentas o problemáticas. Con la Central de conexiones, los usuarios pueden administrar las conexiones de este modo:

- Cerrar aplicaciones.
- Cerrar la sesión. Este paso finaliza la sesión y cierra todas las aplicaciones que hubiera abiertas.

- Desconectarse de una sesión. Este paso interrumpe la conexión seleccionada con el servidor sin cerrar ninguna aplicación que haya abierta (a menos que el servidor esté configurado para cerrar aplicaciones en caso de desconexión).
- Ver estadísticas de transporte de la conexión.

## SDK y API

July 6, 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. 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:

- La API para Citrix Virtual Driver (VD-API), que se usa con las funciones de canal virtual en el SDK de WF-API (Citrix Server API SDK) para crear nuevos canales virtuales. El soporte para canales virtuales proporcionado por VD-API está diseñado para hacer más sencilla la creación de sus propios canales virtuales.
- Código fuente operacional de varios ejemplos de programas de canales virtuales, que demuestran varias técnicas de programación.
- El Virtual Channel SDK requiere el SDK de WF-API para escribir la parte del lado del servidor del canal virtual.

Para obtener más información, consulte [Citrix Virtual Channel SDK para la aplicación Citrix Workspace para Linux](#).

### Referencia de línea de comandos

Para obtener información sobre las referencias y los parámetros de la línea de comandos, consulte [Referencia de comandos de la aplicación Citrix Workspace para Linux](#).

### SDK de optimización de plataforma

Como parte de la iniciativa HDX SoC para la aplicación Citrix Workspace para Linux, hemos creado el “Platform Optimization SDK” (SDK para la optimización de plataforma), para facilitar un ecosistema de dispositivos de bajo coste, bajo consumo y alto rendimiento con factores de forma innovadores.

El Platform Optimization SDK puede ser útil para los desarrolladores que buscan mejorar el rendimiento de los dispositivos basados en Linux, ya que les permite crear extensiones de plug-in para el componente de motor ICA (wfica) de la aplicación Citrix Workspace para Linux. Los plug-ins se crean como bibliotecas compatibles que se wfica carga dinámicamente. Estos plug-ins pueden ayudarle a optimizar el rendimiento de los dispositivos Linux, mediante la habilitación de las siguientes funciones:

- Proporcionar la decodificación acelerada de datos JPEG y H.264 que se utilizan para dibujar la imagen de la sesión
- Controlar la asignación de memoria utilizada para dibujar la imagen de la sesión
- Mejorar el rendimiento, tomando el control del dibujo de bajo nivel de la imagen de la sesión
- Proporcionar servicios de salida de gráficos y entradas de usuario para entornos de sistema operativo que no admiten X11

Para obtener información, consulte [Aplicación Citrix Workspace para Linux - Platform Optimization SDK](#).

**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).