



# **Aplicación Citrix Workspace 1912 LTSR para Windows**

## Contents

<b>Acerca de esta versión</b>	<b>2</b>
<b>Problemas resueltos</b>	<b>8</b>
<b>Problemas conocidos</b>	<b>24</b>
<b>Avisos legales de terceros</b>	<b>25</b>
<b>Requisitos del sistema y compatibilidad</b>	<b>26</b>
<b>Instalación y desinstalación</b>	<b>34</b>
<b>Implementación</b>	<b>45</b>
<b>Actualización</b>	<b>52</b>
<b>Introducción</b>	<b>60</b>
<b>Configurar</b>	<b>81</b>
<b>Autenticación</b>	<b>156</b>
<b>Proteger comunicaciones</b>	<b>173</b>
<b>Storebrowse</b>	<b>185</b>
<b>Desktop Lock de la aplicación Citrix Workspace</b>	<b>194</b>
<b>SDK y API</b>	<b>200</b>
<b>Referencia para parámetros ICA</b>	<b>202</b>

## Acerca de esta versión

October 30, 2023

### Novedades en la versión 1912

Cumulative Update 7 (CU7) es la actualización más reciente de la versión 1912 LTSR.

#### Mejora para Microsoft Teams

Esta mejora de Microsoft Teams se ofrece en CU6 y en versiones posteriores:

Cuando Desktop Viewer se halla en modo de pantalla completa, el usuario puede seleccionar una de todas las pantallas que cubren Desktop Viewer para compartirla. En el modo de ventana, el usuario puede compartir la ventana de Desktop Viewer. En el modo integrado, el usuario puede seleccionar una de todas las pantallas para compartirla. Cuando Desktop Viewer cambia el modo de ventana (maximizada, restaurada o minimizada), la pantalla compartida se detiene.

Estas mejoras de Microsoft Teams se admiten en CU5 y versiones posteriores:

- Mejoras en el uso compartido de la pantalla: Ahora, al compartir la pantalla, solo la pantalla de Desktop Viewer se captura en formato de mapa de bits nativo.
- Ahora, los usuarios pueden ver el puntero del presentador en una sesión de pantalla compartida.
- Generación de vídeo mejorada.
- Mejoras en el rendimiento y la fiabilidad.
- El motor de medios WebRTC ahora tiene en cuenta el servidor proxy configurado en el dispositivo cliente.
- Mejora en la eliminación de eco, el control automático de ganancias y configuraciones de supresión de ruido: Si Microsoft Teams configura estas opciones, la instancia de Microsoft Teams redirigida por Citrix respeta los valores tal y como están configurados. De lo contrario, estas opciones se establecen en True de forma predeterminada.
- Ahora puede configurar una interfaz de red preferida para el tráfico multimedia.

Vaya a `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` y cree una clave llamada `NetworkPreference(REG_DWORD)`.

Seleccione uno de estos valores según corresponda:

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

De forma predeterminada y si no se establece ningún valor, el motor de medios WebRTC elige la mejor ruta disponible.

- Ahora puede inhabilitar el módulo del dispositivo de audio 2 (ADM2) para que el módulo de dispositivo de audio (ADM) heredado se utilice para micrófonos de cuatro canales. Esto ayuda a resolver problemas relacionados con los micrófonos en las llamadas.

Para inhabilitar ADM2, vaya a `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`, cree una clave denominada `DisableADM2` (REG\_DWORD) y establezca el valor en 1.

- Ahora `DirectWShow` es el generador predeterminado.

**Para cambiar el generador predeterminado, haga esto:**

- Abra el Editor del Registro.
- Vaya a esta ubicación de clave: `HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`.
- Actualice este valor: `"UseDirectShowRendererAsPrimary"=dword:00000000`

Otros valores posibles:

- \* 0: Media Foundation
  - \* 1: DirectShow (predeterminado)
- Vuelva a iniciar la aplicación Citrix Workspace.

**Nota:**

- Las mejoras solo se admiten en dispositivos de punto final con sistema operativo de escritorio Microsoft Windows 10.
- Las mejoras no se admiten en dispositivos de punto final con los sistemas operativos Microsoft Windows 7 ni 8.
- La compatibilidad con las mejoras se determina durante la instalación del paquete de la aplicación Citrix Workspace. Se recomienda desinstalar Citrix Workspace al actualizar la versión 7 del sistema operativo de Microsoft Windows a la versión 10.

## App Protection

### Renuncia de responsabilidades

Las directivas de App Protection funcionan mediante el filtrado del acceso a las funciones requeridas del sistema operativo subyacente (llamadas a API específicas necesarias para capturar pantallas o pulsaciones de teclas). Esto significa que las directivas de App Protection pueden proporcionar protección incluso contra herramientas de piratas informáticos personalizadas y con un diseño específico. Sin embargo, a medida que los sistemas operativos evolucionan, pueden surgir nuevas formas de capturar pantallas y registrar pulsaciones de teclas. Si bien seguimos identificándolas y abordándolas, no podemos garantizar una protección completa en configuraciones e implementaciones específicas.

App Protection 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. App Protection 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.

#### Nota:

Citrix recomienda que utilice la aplicación Citrix Workspace nativa únicamente para iniciar sesiones protegidas.

App Protection se configura entre StoreFront y el Controller mediante el Controller. Para obtener información sobre cómo configurar App Protection en el Controller, consulte la documentación de [App Protection](#). Esta configuración se aplica a la aplicación Citrix Workspace; para ello, se incluye el componente de App Protection mediante cualquiera de los métodos siguientes:

- Interfaz gráfica de usuario
- Interfaz de la línea de comandos

Puede incluir el componente de App Protection durante la instalación de la aplicación Citrix Workspace o la instalación a demanda.

#### Nota:

- Esta función solo se admite en sistemas operativos de escritorio de Microsoft Windows, como Windows 10, Windows 8.1 y Windows 7.
- Esta función no es compatible con el Protocolo de escritorio remoto (RDP).

Para obtener información sobre cómo configurar App Protection en la aplicación Citrix Workspace, consulte [App Protection](#).

**Mejora en App Protection** Antes, al intentar hacer una captura de pantalla de una ventana protegida, toda la pantalla, incluidas las aplicaciones no protegidas en segundo plano, se oscurecía.

Ahora, al hacer capturas de pantalla con una herramienta de recortes, solo se oscurece o se oculta la ventana protegida. Puede tomar una captura de pantalla de la zona externa a la ventana protegida, excepto en modo no Aero, donde toda la pantalla está oscurecida.

Sin embargo, si utiliza la tecla **Impr Pant** para hacer una captura de pantalla, debe salir de la aplicación Citrix Workspace.

Además, esta versión soluciona problemas para mejorar la función de App Protection.

### **Mejora del instalador**

En versiones anteriores, si un administrador intentaba instalar la aplicación Citrix Workspace en un sistema que tiene una instancia de la aplicación instalada por el usuario, la instalación se bloqueaba.

Ahora, en esta versión, los administradores pueden supeditar la instancia instalada por el usuario de la aplicación Citrix Workspace y continuar con la instalación correctamente.

### **Mejora en Actualizaciones de Citrix Workspace**

En versiones anteriores, si un administrador instalaba la aplicación Citrix Workspace, un usuario que no fuera administrador no podía actualizarla.

En esta versión, los usuarios que no sean administradores pueden actualizar la aplicación Citrix Workspace en instancias instaladas por un administrador. Para ello, haga clic con el botón secundario en el icono de la aplicación Citrix Workspace, en el área de notificaciones, y seleccione Buscar actualizaciones.

#### **Nota:**

La opción **Buscar actualizaciones** ahora está disponible tanto en las instancias instaladas por el usuario como en las instancias instaladas por el administrador de la aplicación Citrix Workspace.

### **Compatibilidad con proxies salientes**

Smart Control permite a los administradores definir directivas granulares con el objetivo de configurar y aplicar atributos de entorno de usuario para aplicaciones y escritorios virtuales mediante Citrix Gateway. Por ejemplo, es posible que quiera prohibir a los usuarios asignar unidades a sus escritorios remotos. Esto se puede lograr con la función Smart Control de Citrix Gateway.

Sin embargo, la situación cambia cuando la aplicación Citrix Workspace y Citrix Gateway pertenecen a cuentas empresariales distintas. En tales casos, el dominio del cliente no puede aplicar la función Smart Control porque la puerta de enlace no existe en el dominio del cliente. En su lugar, puede utilizar el proxy ICA saliente. El proxy ICA saliente le permite utilizar la función Smart Control incluso cuando la aplicación Citrix Workspace y Citrix Gateway se implementan en organizaciones distintas.

La aplicación Citrix Workspace admite inicios de sesión mediante el proxy de LAN de Citrix ADC. Se puede configurar un único proxy estático o se puede seleccionar el servidor proxy en ejecución mediante el plug-in del proxy saliente.

Puede configurar proxies salientes a través de los métodos siguientes:

- Proxy estático: El servidor proxy se configura al proporcionarle un nombre de host y un número de puerto.
- Proxy dinámico: Se puede seleccionar un servidor proxy único entre uno o más servidores proxy mediante la DLL del plug-in de proxy.

Puede configurar el proxy saliente mediante la plantilla administrativa de objetos de directiva de grupo y el Editor del Registro.

Para obtener más información acerca del proxy saliente, consulte [Compatibilidad con proxies ICA salientes](#) en la documentación de Citrix Gateway.

Para obtener más información acerca de la configuración del proxy saliente en la aplicación Citrix Workspace, consulte [Proxy saliente](#).

### **Binarios del explorador integrado de Citrix**

Esta versión ya no instala el explorador integrado de Citrix. En los casos en que actualice a la versión 1912, se quita el explorador integrado de Citrix.

En ausencia del explorador integrado de Citrix, cambian las siguientes funcionalidades:

- La redirección de contenido del explorador web no funciona.
- Las aplicaciones SaaS y web no se inician con el explorador integrado de Citrix. En su lugar, se inician en Citrix Secure Browser Service.

### **Mejora para compartir escritorios con Microsoft Teams**

Cuando comparte el espacio de trabajo mediante Microsoft Teams, la aplicación Citrix Workspace muestra un borde rojo que rodea el área del monitor que se está compartiendo. Solo se puede compartir la ventana de Desktop Viewer o cualquier ventana local superpuesta encima de este. Cuando se minimiza la ventana de Desktop Viewer, el uso compartido de pantalla se pausa.

## Estimador de rendimiento del codificador de dispositivos de punto final en Microsoft Teams

Cuando se inicia el proceso HdxTeams.exe (el motor de medios WebRTC incluido en la aplicación Citrix Workspace que controla la redirección de Microsoft Teams), se calcula la mejor resolución de codificación que puede acomodar la CPU del dispositivo del punto final sin sobrecargarse. Los valores posibles son: 240p, 360p, 720p y 1080p.

El proceso de estimación del rendimiento (también llamado `webrtcapi.EndpointPerformance`) se ejecuta cuando se inicializa HdxTeams.exe. El código de macrobloque determina la mejor resolución que se puede lograr en ese dispositivo de punto final en cuestión. A continuación, se incluye la resolución más alta posible durante la negociación del códec entre los pares o entre el par y el servidor de conferencias.

Para obtener información sobre cómo configurar el codificador de dispositivos de punto final, consulte [Estimador de rendimiento del codificador de dispositivos de punto final en Microsoft Teams](#).

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

## Mejora en Citrix Analytics Service

Con esta versión, la aplicación Citrix Workspace está destinada a transmitir de forma segura la dirección IP pública del salto de red más reciente a Citrix Analytics Service. Estos datos se recopilan por inicio de sesión. Ayuda a Citrix Analytics Service a analizar si los problemas de rendimiento deficiente están vinculados a áreas geográficas específicas. De forma predeterminada, los registros de direcciones IP se envían a Citrix Analytics Service. Sin embargo, puede inhabilitar esta opción en la aplicación Citrix Workspace mediante el Editor del Registro.

Para inhabilitar las transmisiones de registros de direcciones IP, vaya a la siguiente ruta del Registro y **desactive** la clave `SendPublicIPAddress`.

- En máquinas con Windows de 64 bits, vaya a: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`.
- En máquinas con Windows de 32 bits, vaya a: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`.

### Nota:

- Aunque la aplicación Citrix Workspace transmite todas las direcciones IP en las que se inicia, la transmisión de direcciones IP se produce en el mejor de los casos. Es posible que algunas de las direcciones no sean exactas.
- En entornos de clientes cerrados, donde los dispositivos de punto final operan dentro de una intranet, compruebe que la URL `https://locus.analytics.cloud.com/api`

`/locate ip` se halla en la lista de permitidos del dispositivo de punto final en cuestión.

Para obtener más información sobre cómo utiliza esta información Performance Analytics, consulte [Autoservicio para el rendimiento](#).

## Problemas resueltos

October 30, 2023

### Aplicación Citrix Workspace 1912 LTSR CU7 para Windows

Comparado con: Aplicación Citrix Workspace 1912 LTSR CU6

#### Redirección de contenido

- Cuando Desktop Viewer está configurado en el modo de pantalla completa y el explorador predeterminado se maximiza en el dispositivo de punto final, es posible que la función Redirección de contenido bidireccional no ponga en primer plano la ventana del explorador web predeterminado local. El problema se produce con exploradores web predeterminados locales que no sean Internet Explorer. [CVADHELP-19041]

#### Inicio de sesión/Autenticación

- Es posible que, de manera intermitente, no se puedan agregar direcciones URL de Citrix Gateway y que muestren este mensaje de error:

**No se pudo establecer contacto con el servicio de autenticación.**

[CVADHELP-19415]

#### Sesión/Conexión

- Es posible que la utilidad Storebrowse para enumerar recursos de la URL de Citrix Gateway falle cuando no se puede acceder a al menos uno de los Delivery Controllers configurados. [CVADHELP-15416]
- Cuando IME de Citrix está habilitado, es posible que ciertas aplicaciones de terceros no respondan y que no se inicien aplicaciones en las sesiones de usuario. El problema se produce por un error en el módulo CtxIme. [CVADHELP-18511]

- Es posible que, al intentar actualizar o iniciar una aplicación, aparezca un mensaje de error que indica que **no se puede contactar con el almacén**. Este problema se produce cuando no se consigue obtener la descripción del acceso directo para aplicaciones suscritas concretas.

**Sus aplicaciones no están disponibles en este momento. Inténtelo de nuevo en unos minutos o póngase en contacto con el servicio de asistencia técnica con esta información: No se puede contactar con el almacén.**

[CVADHELP-18736]

- Es posible que no se puedan iniciar sesiones de usuario después de usar el comando **selfservice.exe –init –ipoll –exit**. [CVADHELP-19095]
- Con esta corrección, puede configurar **TWITaskbarGroupingMode** en **GroupNone**, tanto en **HKEY\_CURRENT\_USER** como en **HKEY\_LOCAL\_MACHINE**. La clave **TWITaskbarGroupingMode** está disponible, por ejemplo, en **HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows**. [CVADHELP-19106]

### Experiencia de usuario

- Cuando la directiva de gráficos Gradual sin pérdida está habilitada en un entorno con varios monitores, es posible que, cuando la pantalla abarca un equipo portátil y un monitor externo, la imagen quede distorsionada. [CVADHELP-19065]

## Aplicación Citrix Workspace 1912 LTSR CU6 para Windows

Comparado con: Aplicación Citrix Workspace 1912 LTSR CU5

### Problemas en el dispositivo cliente

- En una sesión de la aplicación Citrix Workspace, es posible que, al iniciar un vídeo de YouTube o una llamada de Microsoft Teams y, a continuación, desconectar los auriculares, la sesión deje de responder. [CVADHELP-17629]

### Instalación, desinstalación y actualización

- Al actualizar la aplicación Citrix Workspace para Windows de la versión CU4 a la versión CU5 sin instalar el autoservicio, es posible que aparezca este mensaje:

**Actualización de una versión no compatible**

**Citrix Workspace desinstalará automáticamente la versión anterior y eliminará todos los parámetros, aunque podrá restaurarlos más adelante. De lo contrario, deberá eliminarlo todo manualmente. Haga clic en Aceptar para continuar.**

[CVADHELP-18790]

### **Inicio de sesión/Autenticación**

- Es posible que, al iniciar sesión en Citrix Gateway con una contraseña incorrecta, Storebrowse realice varios intentos de autenticación que bloqueen la cuenta de usuario. [CVADHELP-17467]
- Es posible que la autenticación de la aplicación Citrix Workspace falle tras la inicialización al intentar usar una tarjeta inteligente a través de Citrix Gateway. Si actualiza el proceso de autenticación después de 15 minutos, es posible que aparezca un mensaje de error 404 en el explorador integrado de Citrix Workspace. Esto hace que la aplicación se quede atascada en el bucle de autenticación hasta que cierre la aplicación y la abra de nuevo. [CVADHELP-18305]

### **Sesión/Conexión**

- Es posible que, al abrir una aplicación publicada mediante la redirección de carpetas cuando el recurso compartido de redirección de carpetas no está conectado, aparezca este mensaje de error.

**No se puede iniciar la aplicación.**

[CVADHELP-16387]

- Es posible que, al intentar abrir una aplicación mediante el acceso directo con las opciones **Limitar a una sola instancia por usuario** y **vPrefer** habilitadas, aparezca un error de conexión en Citrix Director. [CVADHELP-17372]
- Durante una conferencia telefónica, cuando se utiliza Microsoft Teams en modo optimizado HDX, es posible que la parte del vídeo de las llamadas entrantes parpadee. [CVADHELP-17398]
- Es posible que la aplicación Citrix Workspace sondee balizas externas para los almacenes internos. Con esta corrección, las balizas externas no se sondean cuando el almacén se usa sin la puerta de enlace. [CVADHELP-18275]
- No se pueden crear accesos directos para aplicaciones publicadas a través de la aplicación Citrix Workspace sin los permisos adecuados. Como resultado, es posible que los iconos se descarguen en el perfil de usuario en cada actualización, lo que aumenta el tamaño de la memoria caché en los dispositivos de punto final y el consumo de CPU en el lado de StoreFront. [CVADHELP-18609]

- Es posible que las llamadas optimizadas de Microsoft Teams entre dos usuarios realizadas desde la aplicación Citrix Workspace para Mac a la aplicación Citrix Workspace para Windows se desconecten. [CVADHELP-18696]
- Es posible que no se puedan iniciar sesiones desde grupos de entrega con una regla de directiva de acceso que especifique la dirección IP del cliente si el cliente tiene varias tarjetas NIC.

```
Rule: Set-BrokerAccessPolicyRule -Name <rulename> -includedClientIPs  
<Client ip address>
```

[CVADHELP-18783]

### Excepciones del sistema

- Es posible que Citrix Authentication Manager (AuthManSvr.exe) se cierre de forma inesperada durante el inicio de sesión. [CVADHELP-17233]

### Experiencia de usuario

- Es posible que, al abrir una ventana de escritorio en modo de ventana en un entorno con varios monitores, se dé este comportamiento.

Es posible que la ventana abierta en el monitor 1 y arrastrada al monitor 2 aparezca maximizada en el monitor 1 y no en el monitor 2.

[CVADHELP-17373]

### Interfaz de usuario

- Con esta corrección, puede cambiar a la cuenta requerida al configurar varias cuentas y el Registro de la cuenta actual. [CVADHELP-17718]
- Es posible que, al configurar un almacén habilitado y uno inhabilitado juntos mediante un objeto de directiva de grupo, aparezca una interfaz de usuario que no sea X1 o en forma de burbuja verde en lugar de una interfaz de usuario X1 por primera vez en el almacén habilitado. [CVADHELP-17942]
- Es posible que, al inhabilitar la cuenta de almacén de la aplicación Citrix Workspace, no se eliminen accesos directos de aplicaciones del menú **Inicio** o del escritorio. [CVADHELP-18260]

## Aplicación Citrix Workspace 1912 LTSR CU5 para Windows

Comparado con: Aplicación Citrix Workspace 1912 LTSR CU4

### **Problemas en el dispositivo cliente**

- Al usar la aplicación Citrix Workspace 1912 LTSR CU4, es posible que los dispositivos conectados con puertos COM superiores a 9 no se asignen en la sesión. [CVADHELP-17734]

### **Instalación, desinstalación y actualización**

- Es posible que no se pueda actualizar la aplicación Citrix Workspace para Windows mediante el parámetro **/forceinstall**. El problema se produce cuando la utilidad de limpieza de Receiver no puede iniciar el proceso de limpieza. [CVADHELP-17656]

### **Inicio de sesión/Autenticación**

- Si se agota el tiempo de espera en una sesión de Citrix Gateway, es posible que Citrix Workspace no solicite la autenticación al iniciar una aplicación. [CVADHELP-17187]

### **Ventanas integradas**

- Es posible que algunas aplicaciones de terceros permanezcan en primer plano y dejen otras aplicaciones iniciadas en segundo plano. [CVADHELP-16897]

### **Problemas de seguridad**

- Es posible que la aplicación Citrix Workspace 1912 LTSR para Windows falle cuando los archivos CAT USB están firmados con un certificado SHA-1. [CVADHELP-17679]

### **Sesión/Conexión**

- Al navegar por páginas web en algunos exploradores web con HTML o animaciones en un cliente ligero de GPU, es posible que Citrix Workspace para Windows deje de responder. El problema ocurre cuando el proceso wfica32 consume una gran cantidad de memoria. [CVADHELP-16172]
- Después de actualizar la aplicación Citrix Workspace para Windows a la versión 1912 LTSR CU1 o CU2, es posible que se produzca un error en la fiabilidad de las sesiones. El problema se produce cuando el protocolo Enlightened Data Transport (EDT) está habilitado y la conexión pasa por Citrix Gateway. [CVADHELP-16694]
- Es posible que no se puedan iniciar sesiones mediante Citrix Workspace para Windows cuando el puerto CGP (2598) está bloqueado en el dispositivo de punto final. [CVADHELP-17632]

### Experiencia de usuario

- Esta corrección elimina la ventana emergente de la cuenta de confianza mediante un nuevo parámetro de objeto de directiva de grupo: **Lista de cuentas de almacén de confianza**. [CVADHELP-16597]
- Al utilizar algunas aplicaciones de terceros en un VDA, es posible que haya un retraso en el movimiento del mouse. [CVADHELP-16737]

### Interfaz de usuario

- Al usar la aplicación Citrix Workspace 1912 LTSR CU2 para Windows, es posible que los accesos directos del menú Inicio no se actualicen automáticamente. El problema ocurre al agregar una nueva aplicación o al realizar un cambio en el back-end. [CVADHELP-17122]
- Es posible que, al establecer el valor **CurrentAccount** en **AllAccount** en el Registro HKEY\_LOCAL\_MACHINE\Software\Citrix\Dazzle, este no surta efecto. El problema se produce cuando hay al menos una cuenta de almacén presente. [CVADHELP-17229]
- Al intentar iniciar sesión en dispositivos de cliente ligero de Wyse mediante la aplicación Citrix Workspace para Windows, es posible que aparezca la solicitud de autorización detrás de la pantalla de **Desktop Lock**. Como resultado, no puede iniciar sesión hasta que traiga al frente la ventana de la solicitud de autorización. [CVADHELP-17880]

## Aplicación Citrix Workspace 1912 LTSR CU4 para Windows

Comparado con: Aplicación Citrix Workspace 1912 LTSR CU3

### Problemas en el dispositivo cliente

- Con la directiva **Redirección de puertos COM del cliente** habilitada, es posible que se produzca un error al intentar acceder al puerto COM del dispositivo Bluetooth. [CVADHELP-14939]

### Inicio de sesión/Autenticación

- Es posible que no se pueda iniciar sesión en la versión 1912 LTSR CU3 de la aplicación Citrix Workspace para Windows cuando el nombre de usuario contiene caracteres con diéresis. [CVADHELP-17267]

## Problemas de seguridad

- Es posible que falte la protección binaria de flujo de control en los binarios. [CVADHELP-16531]

## Sesión/Conexión

- Al utilizar la función para compartir pantalla en Microsoft Teams durante una llamada entre dos usuarios, es posible que aparezca una pantalla negra. [CVADHELP-15605]
- Si la directiva **Transporte adaptable HDX** está establecida en **Preferido** y **Detección de MTU en EDT** está habilitada, al intentar iniciar aplicaciones o escritorios, es posible que aparezca una pantalla gris o negra con un mensaje de advertencia. [CVADHELP-15805]
- Es posible que el acceso directo creado para una aplicación no se elimine ni siquiera después de inhabilitar la aplicación o de cambiar la ruta del acceso directo. [[CVADHELP-16448]
- Es posible que no se puedan iniciar aplicaciones a través de la aplicación Citrix Workspace para Windows al establecer o cancelar una conexión VPN que pasa por Citrix Gateway. [CVADHELP-16714]
- En casos de doble salto, es posible que los nombres de cliente de los dispositivos de punto final no pasen a un Delivery Controller o a Director. El problema se produce con la versión 2003 de VDA y versiones posteriores. [CVADHELP-16783]
- Después de actualizar la aplicación Citrix Workspace para Windows a la versión 1912 LTSR CU1 o CU2, es posible que se produzca un error en la fiabilidad de las sesiones. El problema se produce cuando el protocolo Enlightened Data Transport (EDT) está habilitado y la conexión pasa por Citrix Gateway. [CVADHELP-16694]

## Experiencia de usuario

- Al utilizar la versión 1912 LTSR CU2 de la aplicación Citrix Workspace para Windows, es posible que las sesiones muestren artefactos gráficos que tapan el contenido de la pantalla. [CVADHELP-16451]
- Después de actualizar la versión 4.9.6 de Citrix Receiver para Windows a la versión 1912 LTSR CU2 o CU3 de la aplicación Citrix Workspace, al intentar iniciar el acceso directo de una aplicación, es posible que los iconos de acceso directo parpadeen en algunos escritorios. [CVADHELP-16967]

## Interfaz de usuario

- Si selecciona **Cerrar sesión** cuando se está ejecutando una sesión, aparecerá la **solicitud de cierre de sesión** para confirmar la acción. Al presionar **Cancelar**, se producirá un error.

[CVADHELP-15516]

- Al actualizar la versión 4.9 LTSR CU7 de Citrix Receiver para Windows a la versión CU2 o CU3 de la aplicación Citrix Workspace para Windows e intentar establecer la cuenta de almacén predeterminada, es posible que el comportamiento resultante no sea coherente. Por ejemplo, la cuenta de almacén predeterminada siempre opta, de manera predeterminada, la opción Todas las cuentas. Con este cambio, al asignar la cuenta de almacén principal a otro nombre de almacén, dicha asignación se conserva incluso después de salir y reiniciar la aplicación Citrix Workspace. [CVADHELP-16903]

## Aplicación Citrix Workspace 1912 LTSR CU3 para Windows

Comparado con: Aplicación Citrix Workspace 1912 LTSR CU2

### Instalación, desinstalación y actualización

- Al intentar actualizar la aplicación Citrix Workspace mediante el acceso directo creado manualmente, es posible que este se elimine y vuelva a crearse. [CVADHELP-15397]

### Teclado

- Al utilizar un teclado japonés, es posible que el modo de entrada de ancho completo no funcione con Microsoft Excel iniciado mediante Acceso a aplicaciones locales. El problema se produce con la aplicación Citrix Workspace para Windows que tiene habilitada la función de App Protection. [CVADHELP-15410]

### Inicio de sesión/Autenticación

- Incluso después de habilitar las directivas **Mantener mi sesión conectada** y **No volver a preguntar durante 60 días**, es posible que la autenticación de varios factores de Microsoft Azure aún solicite la autenticación.

#### Nota:

Recomendamos que los usuarios salgan de los almacenes en lugar de cerrar la sesión de los almacenes. Si los usuarios cierran la sesión de los almacenes mediante la autenticación de WebView, es posible que se les pida la autenticación de nuevo porque las cookies de Internet Explorer se borran en casos así. De forma predeterminada, la corrección está habilitada (se almacenan las cookies). Para inhabilitar la corrección, habilite la directiva de GPO **Evitar el almacenamiento de cookies persistentes** en **Componentes de Citrix**

> **Citrix Workspace > Autenticación de usuarios.** Si inhabilita la corrección, las cookies no se almacenan y se borran al cerrar la sesión. Si inhabilita la corrección, las cookies no se almacenan y se borran al cerrar la sesión.

[CVADHELP-14814]

- En dispositivos unidos a Azure Active Directory (AD), cuando la aplicación Citrix Workspace intenta acceder a un almacén y, a continuación, pasa por las credenciales de inicio de sesión del dispositivo de punto final, es posible que los usuarios no estén autorizados para iniciar sesión. Además, no hay ninguna opción para iniciar sesión con otra cuenta de usuario. [CVADHELP-14844]

## Impresión

- Al enviar un documento como datos sin procesar a la cola de impresión, es posible que el documento no se imprima. El problema se produce al usar el controlador de impresora XPS. [CVADHELP-14497]

## Sesión/Conexión

- En algunos casos, el uso de licencias de productos Citrix que se muestra en Citrix Studio no coincide con el uso de licencias que se muestra en Citrix License Manager. [CVADHELP-14950]
- Con la opción **vPrefer** habilitada, es posible que las aplicaciones de App-V se inicien en un servidor remoto en lugar de iniciarse en un servidor local. [CVADHELP-15356]
- Al iniciar un escritorio publicado a través de una aplicación Citrix Workspace para Windows nativa, la aplicación Citrix Workspace nativa se ejecuta automáticamente en primer plano dentro del escritorio. El problema se produce cuando la función **Acceso a aplicaciones locales** está habilitada. [CVADHELP-15654]
- Es posible que el proceso Selfservice.exe deje de responder y aparezca un mensaje de **.NET-BroadcastEventWindow.4.0.0.0.1**. El problema se produce al intentar cerrar la sesión desde un sistema con la versión 1909 de Windows 10. [CVADHELP-15700]
- Configure la aplicación Citrix Workspace para Windows para conectarse a todas las cuentas de almacén al establecer una sesión. Si cierra sesión en la aplicación Citrix Workspace y vuelve a iniciar sesión, la configuración de la cuenta de almacén cambia a una cuenta de almacén en lugar de establecerse de forma predeterminada en todas las cuentas. [CVADHELP-15728]
- Con la directiva de redirección de contenido bidireccional habilitada, es posible que no se puedan redirigir direcciones URL de un cliente a un VDA. [CVADHELP-15739]

- En situaciones en las que los servidores proxy no usan el puerto 8080, es posible que la aplicación Citrix Workspace no se pueda conectar a aplicaciones y escritorios publicados. El problema se produce porque es posible que la aplicación Citrix Workspace para Windows no use el puerto del proxy y, en su lugar, use el puerto 8080 predeterminado. [CVADHELP-15977]
- Es posible que la aplicación Citrix Workspace para Windows ignore los parámetros del tipo de proxy. El problema se produce en versiones no inglesas del sistema operativo Microsoft Windows. [CVADHELP-16017]
- Cuando el parámetro del Registro **EnableFactoryReset** está establecido en **False**, es posible que no se pueda desinstalar la aplicación Citrix Workspace y que aparezca este mensaje de error:

**Esta función ha sido inhabilitada.**

[CVADHELP-16114]

- Con Microsoft Teams en modo optimizado, al unirse a una conferencia, es posible que el audio se distorsione. [CVADHELP-16232]

### Excepciones del sistema

- Con la directiva **Eliminación de eco** habilitada y la calidad de audio establecida en Media, es posible que el proceso wfica32.exe se cierre de manera intermitente, lo que provoca que las sesiones acaben desconectándose. [CVADHELP-14568]
- Es posible que el proceso Receiver.exe se cierre de manera inesperada. [CVADHELP-15669]

## Aplicación Citrix Workspace 1912 LTSR CU2 para Windows

Comparado con: Aplicación Citrix Workspace 1912 LTSR CU1

### Instalación, desinstalación y actualización

- Puede que la aplicación Citrix Workspace para Windows no se actualice desde la versión 190x a la versión 1912. El problema se produce cuando un archivo incorrecto está presente en algún punto de la ruta a la carpeta ejecutable. [CVADHELP-15277]
- Cuando intenta actualizar la aplicación Citrix Workspace desde la versión 1912 a la versión 1912 CU1 o 2006, puede que la función de actualización de la aplicación Citrix Workspace no funcione en sistemas operativos cuyo idioma no sea el inglés. [CVADHELP-15357]

## Teclado

- Cuando se utiliza el editor de métodos de entrada (IME) chino llamado Wuxiami, puede que la tecla Mayús se quede atascada en la posición pulsada. El problema se produce si la hora local genérica está **activada**. [CVADHELP-15243]

## Problemas de seguridad

- Esta corrección soluciona un problema de seguridad. Para obtener más información, consulte el artículo [CTX277662](#) de Knowledge Center. [CVADHELP-15613]

## Sesión/Conexión

- Con la herramienta de modificación del Registro inhabilitada, puede que las claves de Registro de la instalación anterior no se conserven después de realizar una actualización. Como resultado, no se inician los escritorios. [CVADHELP-15104]
- Puede que la aplicación Citrix Workspace muestre un error de script en las versiones anteriores a 1911 y una página vacía en las versiones 1911 y posteriores. El problema se produce con los almacenes que utilizan Internet Explorer WebBrowser Control para mostrar las páginas de inicio de sesión cuando se aplican directivas de GPO de referencia de seguridad de Microsoft. [CVADHELP-15475]
- En un caso de doble salto, es posible que no se pueda iniciar una aplicación mediante el acceso directo del menú **Inicio**. El problema se produce si se habilita el límite de una instancia de aplicación por usuario. [CVADHELP-15576]
- Cuando se inicia sesión en un almacén desde la versión 1912 o posterior de la aplicación Citrix Workspace, es posible que las aplicaciones no se enumeren. [CVADHELP-15597]

## Experiencia de usuario

- Si se conecta al Self-Service Plug-in (SSP) a través de una VPN, el SSP podría no actualizarse. [CVADHELP-14418]
- Puede que falle el comando **SelfService.exe -init -ipoll -exit** para cerrar el proceso SelfService.exe. [CVADHELP-15126]
- Cuando utiliza un lápiz óptico HP Active para escribir en una aplicación publicada, la funcionalidad de escritura puede experimentar de tres a cuatro segundos de retraso. [CVADHELP-15203]

- Puede que falle el inicio de sesión después de instalar o actualizar la aplicación Citrix Workspace para Windows. El inicio de sesión se atasca en la pantalla **Preparando el escritorio**. El problema se produce al configurar Desktop Lock desde una URL de Citrix Gateway.

**Nota:**

Aparece una pantalla en negro durante algún tiempo antes de que aparezca Desktop Lock la primera vez que se configura la aplicación Citrix Workspace para Windows desde una URL de Citrix Gateway y Desktop Lock. Si la pantalla negra sigue mostrándose durante mucho tiempo, cierre la sesión con **Ctrl+Alt+Supr** para máquinas físicas y **Ctrl+Alt+Fin** para máquinas virtuales.

[CVADHELP-15334]

- Después de actualizar la aplicación Citrix Workspace a la versión 1912 CU1 desde la versión 1912, la enumeración de aplicaciones puede ser lenta y tardar unos 10 minutos en completarse.

[CVADHELP-15766]

## **Parche rápido 1 de la aplicación Citrix Workspace 1912 LTSR CU1 para Windows (19.12.1001)**

Comparado con: Aplicación Citrix Workspace 1912 LTSR CU1 para Windows

### **Problemas de seguridad**

- Esta corrección soluciona un problema de seguridad. Para obtener más información, consulte el artículo [CTX277662](#) de Knowledge Center. [CVADHELP-15613]

## **Aplicación Citrix Workspace 1912 LTSR CU1 para Windows**

Comparado con: La aplicación Citrix Workspace 1912 LTSR

### **Redirección de contenido**

- Cuando intenta redirigir una URL larga, es posible que la URL no se redirija a un VDA y el proceso Redirector.exe se cierre inesperadamente con la siguiente excepción:

**INVALID\_CRUNTIME\_PARAMETER**

[CVADHELP-13197]

## Instalación, desinstalación y actualización

- Puede que la aplicación Citrix Workspace no se instale o actualice en un VDA con Windows 10. El problema se produce al realizar los siguientes pasos:
  1. Al instalar la aplicación Citrix Workspace.
  2. Al instalar un VDA.
  3. Al actualizar la versión de la aplicación Citrix Workspace.

El problema se produce porque la actualización o instalación provocan la desinstalación de los adaptadores de pantalla de Citrix. [CVADHELP-13764]

- Podrían fallar los intentos de utilizar la funcionalidad de actualización automática para actualizar automáticamente HDX RealTime Media Engine (RTME) junto con la aplicación Citrix Workspace. El RTME no puede actualizarse a la versión más reciente. [CVADHELP-15047]

## Inicio de sesión/Autenticación

- Si agrega dos almacenes a la aplicación Citrix Workspace para Windows con dos cuentas diferentes, es posible que el botón Iniciar sesión no funcione en el almacén secundario después de quitar el almacén principal. [CVADHELP-13805]
- Al habilitarse la autenticación de varios factores y utilizarse el cuadro de diálogo Seguridad de Windows para iniciar sesión, el cuadro de diálogo Servicios de federación de Active Directory (ADFS) no aparece al autenticarse en almacenes. [CVADHELP-14316]
- Al configurar Citrix Gateway para que admita el inicio de sesión único (SSO) a través de la aplicación Citrix Workspace, es posible que el inicio SSO falle. El problema se produce cuando un nombre de usuario o una contraseña contienen caracteres especiales, como %, = o &. [CVADHELP-14564]

## SDK

- Esta corrección proporciona una compatibilidad mejorada para los antiguos identificadores de clave privada. [CVADHELP-14530]

## Sesión/Conexión

- Con las funciones Acceso a aplicaciones locales y Desktop Lock habilitadas, al emplear la función Cambiar usuario después de presionar Ctrl+Alt+Supr, es posible que la sesión local de usuario vuelva a conectarse. Sin embargo, cuando la sesión del servidor intenta volver a conectarse, el VDA se queda atascado en una pantalla blanca que muestra el mensaje “Conectado a su escritorio”. El escritorio nunca aparece. [CVADHELP-13046]

- En un entorno de varios monitores, puede que una sesión de usuario no se maximice. El problema se produce al volver a acoplar el portátil. [CVADHELP-13614]
- En un caso de salto doble, es posible que Citrix HDX Engine se cierre de forma inesperada cuando intenta iniciar una sesión. [CVADHELP-13915]
- Con la opción **vPrefer** habilitada en la aplicación Citrix Workspace, es posible que no se pueda iniciar la aplicación de App-V y aparezca este mensaje de error:

**No se puede iniciar**

[CVADHELP-14039]

- Después de agregar aplicaciones publicadas a **Favoritos**, solo se puede abrir una aplicación. El problema se produce cuando esas aplicaciones publicadas utilizan el mismo nombre ejecutable, como se indica en **KEYWORDS:prefer="<application\_name>**. [CVADHELP-14098]
- Es posible que los valores del Registro relacionados con la función obsoleta **HDX MediaStream para Flash** (por ejemplo, Flash y Flash2) no se quiten de la configuración del Registro HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Mod 3.0\VirtualDriver después de actualizar la aplicación Citrix Workspace. Este problema puede causar un error de conexión. [CVADHELP-14850]

### Excepciones del sistema

- Es posible que el proceso wfica32.exe se cierre de forma inesperada al intentar volver a conectarse a una sesión. El problema se produce con la versión 1904.1 de la aplicación Citrix Workspace para Windows. [CVADHELP-12807]
- Con el acceso a aplicaciones locales habilitado, una sesión podría dejar de responder y mostrar el siguiente mensaje de error:

**Citrix HDX Engine no responde**

[CVADHELP-14058]

- Si intenta instalar la aplicación Citrix Workspace sin configurar el modo de autoservicio, puede producirse una excepción. El problema se produce al abrir el menú **Accesos directos y reconexión** desde la hoja **Preferencias avanzadas**. El problema se produce con la aplicación Citrix Workspace desde las versiones 1907 a 2002. [CVADHELP-14940]

### TWAIN

- Puede que no se realicen detecciones desde un dispositivo TWAIN. La columna **Estado** de la ficha **Aplicaciones** del Administrador de tareas de Windows muestra “No responde” para Citrix HDX Engine. [CVADHELP-14782]

## Experiencia de usuario

- En casos de doble salto en los que los VDA para SO multisesión se ejecutan en el primer salto y las aplicaciones publicadas se ejecutan en el segundo salto, puede que no funcione la opción Actualizar aplicaciones del menú de cuenta de la aplicación Citrix Workspace. [CVADHELP-13230]
- Cuando agrega una cuenta desde una URL de almacén en la aplicación Citrix Workspace para Windows, es posible que tarde mucho tiempo en completarse. El problema se produce cuando la dirección URL contiene un número de puerto. [CVADHELP-14051]
- Se ven dos iconos de la aplicación Citrix Workspace en la bandeja del sistema. El problema se produce con la versión 1912 de la aplicación Citrix Workspace. [CVADHELP-14577]
- Cuando se utiliza el inicio SSO en un entorno de VDA, puede aparecer una pantalla de presentación. El problema se produce al actualizar la aplicación Citrix Workspace para Windows a la versión 1911 o posterior. [CVADHELP-14590]

## Interfaz de usuario

- Es posible que haya aplicaciones se pongan en primer plano de forma intermitente y que desplacen la aplicación que esté usando en ese momento. Es posible que su icono en la barra de tareas parpadee para informar al usuario de que la aplicación intenta pasar al primer plano. [CVADHELP-13071]

## Aplicación Citrix Workspace 1912 LTSR para Windows

### Nota:

Si actualmente es cliente de la aplicación Citrix Workspace 1911 Current Release y quiere pasar a las versiones LTSR:

Esta versión contiene las siguientes correcciones en comparación con la aplicación 1911 de Citrix Workspace.

Si actualmente es cliente de Citrix Receiver 4.9 para Windows y quiere permanecer en las versiones LTSR:

Esta versión contiene todas las correcciones incluidas desde Citrix Receiver para Windows 4.9, incluidas sus CU, hasta 4.12, y todas las correcciones incluidas desde la aplicación Citrix Workspace 1808 a 1911, además de la siguiente lista de correcciones incluidas en la aplicación Citrix Workspace 2002 (en comparación con la aplicación Citrix Workspace 1911): La versión 1912 contiene todas las correcciones que hubo entre [Citrix Receiver for Windows 4.9 LTSR CU9](#) y la aplicación Citrix Workspace 1911, además de las siguientes correcciones:

## Redirección de HDX MediaStream para Windows Media

- En un entorno de varios monitores, cuando reproduce un vídeo MP4 con el Reproductor de Windows Media en una sesión de usuario, el vídeo se reproduce correctamente en el monitor principal. Sin embargo, cuando mueve el reproductor a otra pantalla, es posible que aparezca una pantalla negra en el monitor secundario o extendido conectado a través de DisplayLink mediante una base de acoplamiento. [CVADHELP-11848]

## Sesión/Conexión

- Al intentar volver a conectarse a una sesión desde HDX RealTime Media Engine mediante una tarjeta inteligente rápida, es posible que HDX RealTime Media Engine se cierre de manera inesperada. [CVADHELP-12605]
- Cuando las aplicaciones publicadas reciben muchas solicitudes para reproducir sonidos cortos durante un corto período de tiempo, el proceso wfica32.exe podría cerrarse inesperadamente. [CVADHELP-12855]
- Una vez agotado el tiempo de espera de la sesión, es posible que la sesión se cierre automáticamente. Cuando intenta iniciar la sesión de nuevo, esta tarda más de lo normal en iniciarse. El problema se produce cuando hay una interrupción de la red. [CVADHELP-13017]
- Es posible que la ventana de una aplicación integrada se represente parcialmente cortada y permanezca así hasta que cambie manualmente el tamaño de la ventana. [CVADHELP-13108]
- Ahora la aplicación Citrix Workspace comprueba la presencia de iconos de acceso directo cada vez que se actualiza o se inicia. Si un icono no está disponible, la aplicación Citrix Workspace recupera el icono. Al hacerlo, se garantiza que los accesos directos aparezcan correctamente. [RFWIN-15501]
- Al intentar habilitar la directiva Redirección bidireccional de contenido (en **Configuración del equipo > Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Workspace > Experiencia de usuario**), se le pide que introduzca una URL específica, aunque no habilite la supeditación de aplicaciones o escritorios por URL. [RFWIN-15867]

## Excepciones del sistema

- El proceso Receiver.exe puede cerrarse inesperadamente mientras captura rastreos CDF. [CVADHELP-13077]

## Problemas conocidos

June 9, 2023

### Problemas conocidos en la aplicación Citrix Workspace 1912 LTSR CU7 para Windows

No se han observado nuevos problemas en esta versión.

### Problemas conocidos en la aplicación Citrix Workspace 1912 LTSR CU6 para Windows

- Al compartir la pantalla en Microsoft Teams como aplicación publicada, no aparece el borde rojo en la parte inferior de la pantalla compartida. [LCMRFWIN-4194]

### Problemas conocidos en la aplicación Citrix Workspace 1912 LTSR CU5 para Windows

- Al conectar ciertas aplicaciones remotas de terceros, como mRemoteNG, a un dispositivo de punto final y acoplar la barra de herramientas de la aplicación publicada en los laterales, es posible que el sistema deje de responder con un uso del 100 % de la CPU. [LCMRFWIN-4164]
- Al intentar detener el uso compartido de la pantalla durante llamadas optimizadas de Microsoft Teams, es posible que la sesión deje de responder de forma intermitente. [LCMRFWIN-4184]

### Problemas conocidos en la aplicación Citrix Workspace 1912 LTSR CU4 para Windows

- Durante una sesión, al hacer clic en **Buscar actualizaciones** y las actualizaciones se descargan correctamente, la sesión actual no aparece en el cuadro de diálogo **Descarga correcta**. [RFWIN-23152]

### Problemas conocidos en la aplicación Citrix Workspace 1912 LTSR CU3 para Windows

No se han observado nuevos problemas en esta versión.

### Problemas conocidos en la aplicación Citrix Workspace 1912 LTSR CU2 para Windows

No se han observado nuevos problemas en esta versión.

## Problemas conocidos en la aplicación Citrix Workspace 1912 LTSR CU1 para Windows

- Es posible que, al intentar usar la cámara web en una reunión de WebEx, la aplicación Citrix Workspace deje de responder. El problema se produce al configurar el audio UDP en **Medio**.

Como solución temporal, vaya a esta ruta en el Editor del Registro y configure lo siguiente:

**Ruta:** HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advance

**Nombre:** EchoCancellation

**Tipo:** REG\_SZ

**Valor:** FALSE

[DOCFB-3805]

## Problemas conocidos en la aplicación Citrix Workspace 1912 LTSR para Windows

- Es posible que la captura de pantalla con la tecla **Imprimir pantalla** falle. Este problema se produce al minimizar una sesión protegida de la aplicación Citrix Workspace. [RFFWIN-15155]
- Al iniciar Microsoft Word en una sesión publicada y en su dispositivo local y eliminar el almacén de **Cuentas**, aparece el siguiente mensaje de error al iniciar la aplicación en el dispositivo local:

**¿Quiere buscar una aplicación en Citrix Workspace para abrir este archivo?**

[RFFWIN-15884]

- Es posible que no se pueda iniciar sesión en un VDA habilitado para SSL. [RFFWIN-16129]
- En una sesión de escritorio protegida, es posible que no se puedan realizar capturas de pantalla de sesiones no protegidas. [RFFWIN-16704]
- Es posible que no pueda quitar los detalles del almacén agregados a través de la plantilla administrativa de objetos de directiva de grupo (GPO) mediante la interfaz gráfica de usuario. [RFFWIN-16754]
- Al intentar cambiar la pantalla en una sesión protegida, la sesión se cierra. [RFFWIN-16784]

## Avisos legales de terceros

June 9, 2023

Es posible que la aplicación Citrix Workspace 1912 LTSR para Windows incluya software de terceros con licencias definidas en los términos del siguiente documento:

[Citrix Workspace app for Windows Third Party Notices](#) (descarga en PDF)

## Requisitos del sistema y compatibilidad

April 22, 2024

### Requisitos

- 1 GB de RAM.
- Requisitos de .NET Framework
  - Self-Service Plug-in requiere NET 4.6.2. Permite suscribirse e iniciar aplicaciones y escritorios desde la línea de comandos o la interfaz de usuario de la aplicación Citrix Workspace para Windows. Para obtener más información, consulte [Usar parámetros de línea de comandos](#).
- La versión más reciente de Microsoft Visual C++ Redistributable.

**Nota:**

Citrix recomienda utilizar la versión más reciente de Microsoft Visual C++ Redistributable. De lo contrario, es posible que aparezca un mensaje de reinicio durante la actualización de versiones.

A partir de la versión 1904, el paquete del instalador de la aplicación Citrix Workspace no contiene los binarios individuales de Microsoft Visual C++ Redistributable, sino que incluye el instalador de Microsoft Visual C++ Redistributable. El instalador de la aplicación Citrix Workspace comprueba si el paquete de Microsoft Visual C++ Redistributable está presente en el sistema durante la instalación y lo instala si es necesario. La versión 1912 y versiones posteriores de la aplicación Citrix Workspace requieren como mínimo la versión 14.24.28127.4 de Microsoft Visual C++ Redistributable.

**Nota:**

Es posible que no se pueda instalar la aplicación Citrix Workspace con privilegios que no son de administrador en un sistema sin el paquete de Microsoft Visual C++ Redistributable.

Solamente un administrador puede instalar el paquete Microsoft Visual C++ Redistributable.

Para solucionar problemas con la instalación de .NET Framework o Microsoft Visual C++ Redistributable, consulte el artículo [CTX250044](#) de Knowledge Center.

## Tabla de compatibilidad

La aplicación Citrix Workspace es compatible con todas las versiones actualmente compatibles de Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) y Citrix Gateway, según se indica en la tabla [Citrix Product Lifecycle Matrix](#).

La aplicación Citrix Workspace es compatible con los siguientes sistemas operativos Windows:

### Nota:

El plug-in del análisis de punto final (EPA) de Citrix Gateway está disponible en Citrix Workspace. En la aplicación nativa de Citrix Workspace, solo se ofrece al utilizar la autenticación nFactor. Para obtener más información, consulte [Configure pre-auth and post-auth EPA scan as a factor in nFactor authentication](#) en la documentación de Citrix ADC.

---

## Sistema operativo

Enterprise Edition de 32 y 64 bits de Windows 10. Para obtener más información sobre las versiones compatibles del sistema operativo Windows 10, consulte [Compatibilidad de Windows 10 con la aplicación Citrix Workspace para Windows](#).

Las ediciones de 32 y 64 bits de Windows 10 Pro (compatibles a partir de la versión 1912 LTSR CU5 de la aplicación Citrix Workspace para Windows)

Windows 8.1, ediciones de 32 y 64 bits (y Embedded)

Windows 7, ediciones de 32 bits y 64 bits (actualización de seguridad ampliada o ESU)

Windows 7 Embedded Standard (actualización de seguridad ampliada o ESU)

Windows Thin PC

Windows Server 2016

Windows Server 2012 R2, ediciones Standard y Datacenter

Windows Server 2019

Windows Server 2008 R2

Windows 10 Enterprise LTSC 2019

Windows 10 Enterprise 2016 LTSB 1607

---

## Compatibilidad de Windows 10 con la aplicación Citrix Workspace para Windows

### Nota:

- No se recomienda instalar versiones de software de Citrix publicadas anteriormente en la

versión del Canal semianual. Los clientes que opten por hacerlo deberán corroborar que cualquier problema que genere una llamada a la asistencia técnica no se haya solucionado ya con una versión de software de Citrix más reciente, si está disponible, y es posible que deban actualizar su software de Citrix a una versión más reciente.

- Una vez que una versión de Windows 10 haya alcanzado la finalización del servicio, Microsoft ya no ofrece desarrollo adicional ni servicios para dicha versión. Citrix ofrece asistencia para el uso de su software solamente en sistemas operativos que su fabricante siga manteniendo. Para obtener información sobre la finalización del servicio de Windows 10, consulte las [Preguntas frecuentes sobre el ciclo de vida de Microsoft Windows](#).

---

Versión de la aplicación Citrix Workspace	Número de versión de Windows 10 Enterprise Edition	Número de compilación
1912 CU7 y versiones posteriores	LTSC 2021	19044
1912 CU6 y versiones posteriores	21H2	19044
1912 CU6 y versiones posteriores	21H2	19044
1912 CU5 y versiones posteriores	21H1	19043.1165
1912 CU2 y versiones posteriores	20H2	19042.685
1912 CU1 y versiones posteriores	2004	19041.329
1911 y versiones posteriores	1909	18363.418
1909 y versiones posteriores	1903	18362.116
1812 y versiones posteriores	1809	17763.107
1808 y versiones posteriores	10 1803	17134.376

---

### Exploradores web compatibles

Para obtener una lista de exploradores web compatibles, consulte [Acceder a almacenes a través de los sitios de Citrix Receiver para Web](#).

### Tabla de sistemas operativos

---

### **Sistema operativo compatible en dispositivos táctiles**

---

Windows 10

Windows 8

Windows 7

---

---

### **Sistema operativo compatible en agentes VDA**

---

Windows 10

Windows 8

Windows 7

Windows 2012 R2

Windows Server 2016

Windows 2008 R2

---

### **Validar el espacio libre en disco**

En la tabla siguiente se indica el espacio necesario en el disco para instalar la aplicación Citrix Workspace para Windows:

---

<b>Tipo de instalación</b>	<b>Espacio de disco requerido</b>
Instalación nueva	572 MB
Actualizaciones	350 MB

---

La aplicación Citrix Workspace comprueba el espacio en disco necesario para completar la instalación. La verificación se lleva a cabo tanto si se trata de una instalación nueva como si es una actualización.

En una instalación nueva, esta se detiene cuando no hay suficiente espacio en el disco y aparece el siguiente diálogo.

Citrix Workspace



Insufficient disk space. Citrix Workspace for Windows requires a minimum of 503 MB of free disk space to complete the installation successfully

OK

Durante la actualización de una versión, la instalación termina cuando no hay suficiente espacio en el disco, tras lo cual aparece el siguiente cuadro de diálogo.

Citrix Workspace



Upgrade unsuccessful due to insufficient disk space. Citrix Workspace for Windows requires a minimum of 388 MB of free disk space to complete the upgrade successfully

OK

**Nota:**

- El instalador solo comprueba el espacio en el disco después de haberse extraído el paquete de instalación.
- Cuando el sistema tiene poco espacio en el disco y la instalación es silenciosa, no aparece el cuadro de diálogo, pero se registra el mensaje de error en `CTXInstall\*_TrolleyExpress-\*.log`.

## Conexiones, certificados y autenticación

### Conexiones

- Almacén HTTP
- Almacén HTTPS
- Citrix Gateway 10.5 y versiones posteriores
- Interfaz Web 5.4

## Certificados

### Nota:

La aplicación Citrix Workspace para Windows está firmada digitalmente. La firma digital contiene una marca de tiempo. Por lo tanto, el certificado es válido incluso después de haber caducado.

- Privados (autofirmados)
- Raíz
- Carácter comodín
- Intermedios

### Certificados privados (autofirmados)

Si se ha instalado un certificado privado en la puerta de enlace remota, el certificado raíz de la entidad de certificación de la organización debe estar instalado en el dispositivo de usuario desde el que se accede a los recursos de Citrix.

### 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.

### Certificados raíz

Para equipos unidos a dominios, puede utilizar la plantilla administrativa de objetos 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.

### Certificados comodín

Se usan certificados comodín en un servidor dentro del mismo dominio.

La aplicación Citrix Workspace admite el uso de certificados comodín, aunque deben usarse solo de acuerdo con las directivas de seguridad de su organización. En la práctica, se pueden usar alternativas a certificados comodines, como un certificado que contenga la lista de nombres de servidor con la extensión de nombre de sujeto alternativo (Subject Alternative Name o SAN). Las entidades de certificación privadas o públicas emiten esos certificados.

## Certificados intermedios

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

## Autenticación

### Autenticación en StoreFront

	<b>Workspace para Web con exploradores web</b>	<b>Sitio de servicios de StoreFront (nativo)</b>	<b>StoreFront, Citrix Virtual Apps and Desktops (nativo), Citrix DaaS</b>	<b>De Citrix Gateway a Workspace para Web (explorador web)</b>	<b>Citrix Gateway en el sitio de StoreFront Services (nativo)</b>
Anónimo	Sí	Sí			
Dominio	Sí	Sí	Sí	Sí*	Sí*
PassThrough de dominio	Sí	Sí	Sí		
Token de seguridad				Sí*	Sí*
Autenticación de dos factores (dominio con token de seguridad)				Sí*	Sí*
SMS				Sí*	Sí*
Tarjeta inteligente	Sí	Sí		Sí	Sí
Certificado de usuario				Sí (plug-in de Citrix Gateway)	Sí (plug-in de Citrix Gateway)

\* Con o sin el plug-in de Citrix Gateway instalado en el dispositivo.

**Nota:**

La aplicación Citrix Workspace admite la autenticación de dos factores (dominio y token de seguridad) a través de Citrix Gateway en el servicio nativo de StoreFront.

**Autenticarse en la Interfaz Web** La aplicación Citrix Workspace admite los siguientes métodos de autenticación (en la Interfaz Web, se usa el término **Explícita** para la autenticación de dominio y token de seguridad):

	<b>Interfaz Web (exploradores web)</b>	<b>Sitio de Citrix Gateway de la Interfaz Web</b>	<b>De Citrix Gateway a la Interfaz Web (explorador web)</b>	<b>De Citrix Gateway al sitio de Citrix Gateway de la Interfaz Web</b>
Anónimo	Sí			
Dominio	Sí	Sí	Sí*	
PassThrough de dominio	Sí	Sí		
Token de seguridad			Sí*	
Autenticación de dos factores (dominio con token de seguridad)			Sí*	
SMS			Sí*	
Tarjeta inteligente	Sí	Sí		
Certificado de usuario			Sí (plug-in de Citrix Gateway)	

\* Disponible solo en implementaciones que incluyen Citrix Gateway, con o sin el plug-in asociado instalado en el dispositivo.

Para obtener información acerca de la autenticación, consulte:

- [Configuring Authentication and Authorization](#) en la documentación de Citrix Gateway.
- [Configurar la autenticación y la delegación](#) en la documentación de StoreFront.

## Lista de revocación de certificados

Cuando está habilitada la comprobación de la lista de revocación de certificados (CRL), la aplicación Citrix Workspace verifica si el certificado del servidor se ha revocado. Con esta verificación, mejora la autenticación criptográfica en el servidor y la seguridad general de la conexión TLS entre el dispositivo de usuario y un servidor.

La comprobación de la lista de revocación de certificados (CRL) se puede habilitar en varios niveles. Por ejemplo, se puede configurar que la aplicación Citrix Workspace verifique solo la lista local de certificados, o que verifique las listas de certificados locales y las de red. Además, se puede configurar la verificación de la lista de revocación de certificados para permitir que los usuarios inicien sesiones solo cuando se verifiquen todas las listas de revocación de certificados.

Salga de la aplicación Citrix Workspace y cierre todos los componentes de Citrix Workspace, incluida la **Central de conexiones**.

Para obtener más información, consulte la sección [TLS](#).

## Instalación y desinstalación

May 23, 2024

### Notas para los administradores antes de instalar la aplicación Citrix Workspace 1912 LTSR para Windows

- La aplicación Citrix Workspace 1912 LTSR para Windows requiere la versión 4.6.2 de .NET Framework o una posterior. El instalador de la aplicación Citrix Workspace descarga e instala .NET Framework, si no está presente en el sistema. Sin embargo, se recomienda instalar manualmente la versión de .NET Framework requerida antes de instalar o actualizar la aplicación Citrix Workspace.
- Si intenta realizar una instalación desatendida, consulte el artículo [CTX257546](#) de Knowledge Center.
- Para ver la información más reciente acerca de los conjuntos de cifrado compatibles y no compatibles, consulte el artículo [CTX250104](#) de Knowledge Center.

Para instalar la aplicación Citrix Workspace, descargue el paquete de instalación [CitrixWorkspaceApp.exe](#) desde la [página Descargas](#) o desde la página de descargas de su empresa (si está disponible). Puede instalar el paquete de la siguiente manera:

- Ejecute un asistente de instalación interactivo basado en Windows, o bien,

- Escriba el nombre de archivo del instalador, los comandos de instalación y las propiedades de instalación en la interfaz de la línea de comandos. Para obtener información sobre cómo instalar la aplicación Citrix Workspace mediante la interfaz de la línea de comandos, consulte [Usar parámetros de la línea de comandos](#).

### Instalar con y sin privilegios de administrador:

Tanto el usuario como el administrador pueden instalar la aplicación Citrix Workspace. Los privilegios de administrador solo se requieren cuando se usa la [autenticación PassThrough](#) y [Citrix Ready Workspace Hub](#) con la aplicación Citrix Workspace para Windows.

En la siguiente tabla se describen las diferencias cuando un administrador o usuario instalan la aplicación Citrix Workspace:

	Carpeta de instalación	Tipo de instalación
Administrador	C:\Archivos de programa (x86)\Citrix\ICA Client	Instalación por sistema
Usuario	%USERPROFILE%\AppData\Local\Citrix\ICA Client	Instalación por usuario

#### Nota:

Si existe una instancia de la aplicación Citrix Workspace para Windows instalada por el usuario en el sistema y un administrador instala la aplicación Citrix Workspace para Windows en el mismo sistema, habrá un conflicto. Citrix recomienda desinstalar todas las instancias de la aplicación Citrix Workspace para Windows instaladas por el usuario antes de instalar la aplicación Citrix Workspace para Windows como administrador.

### Usar un instalador basado en Windows

La aplicación Citrix Workspace para Windows puede instalarse mediante los medios de instalación, un recurso compartido de red, Windows Explorer o la línea de comandos ejecutando manualmente el paquete de instalación `CitrixWorkspaceApp.exe`.

De forma predeterminada, los registros del instalador se encuentran en `%temp%\CTXReceiverInstallLogs*.logs`.

1. Inicie el archivo `CitrixWorkspaceApp.exe` y haga clic en **Inicio**.
2. Lea y acepte el Contrato de licencia de usuario final y continúe con la instalación.
3. Si está intentando llevar a cabo la instalación en un equipo unido a un dominio con privilegios de administrador, aparece un cuadro de diálogo adicional para habilitar o inhabilitar Single Sign-On. Consulte [Autenticación PassThrough de dominio](#) para obtener más información.
4. Siga las instrucciones del instalador basado en Windows para completar la instalación.

## Usar parámetros de línea de comandos

Para instalar la aplicación Citrix Workspace, escriba el nombre de archivo del instalador, los comandos de instalación y las propiedades de instalación desde la interfaz de línea de comandos. Puede personalizar el instalador de la aplicación Citrix Workspace. Para ello, especifique las opciones pertinentes en la línea de comandos. El paquete del instalador se descomprime automáticamente a la carpeta temporal del sistema antes de iniciar el instalador. El requisito de espacio incluye espacio para archivos de programa, datos de usuarios y directorios temporales después de iniciar varias aplicaciones.

Para instalar la aplicación Citrix Workspace mediante la línea de comandos de Windows, inicie el símbolo del sistema y, a continuación, escriba el nombre de archivo del instalador, los comandos de instalación y las propiedades de instalación en una sola línea. Los comandos y propiedades de instalación disponibles se enumeran a continuación:

```
CitrixWorkspaceApp.exe [commands] [properties]
```

## Lista de parámetros de la línea de comandos

Los parámetros se pueden clasificar, a grandes rasgos, de la siguiente manera:

- [Parámetros comunes](#)
- [Parámetros de instalación](#)
- [Parámetros de funciones HDX](#)
- [Parámetros de preferencias e interfaz de usuario](#)
- [Parámetros de autenticación](#)

### Parámetros comunes

- `/?` o `/help`: Enumera todos los comandos y propiedades de instalación.
- `/silent`: Inhabilita los cuadros de diálogo y solicitudes de instalación durante la instalación.
- `/noreboot`: Suprime las solicitudes de reinicio durante la instalación. Cuando elimina las solicitudes de reinicio, la aplicación Citrix Workspace no reconoce aquellos dispositivos USB que estén en estado suspendido hasta que se reinicie el dispositivo del usuario.
- `/includeSSON`: Requiere que lleve a cabo la instalación como administrador. Indica que la aplicación Citrix Workspace se instalará con el componente Single Sign-On. Consulte [Autenticación PassThrough de dominio](#) para obtener más información.
- `/rcu`: Este cambio solo es efectivo cuando se actualiza una versión no compatible del software. Indica que la aplicación Citrix Workspace se instalará o actualizará al desinstalar la versión existente. Esto también borra los parámetros existentes.

Nota:

El modificador `/rcu` se retiró en la versión 1909. Para obtener más información, consulte [Elementos retirados](#).

- `/forceinstall`: Este modificador es útil para limpiar cualquier configuración o entradas existentes de la aplicación Citrix Workspace que hubiera en el sistema en los siguientes casos:
  - Al actualizar una versión de la aplicación Citrix Workspace no compatible.
  - La instalación o la actualización no se han realizado correctamente.

## Parámetros de instalación

### **`/AutoUpdateCheck`**

Indica que la aplicación Citrix Workspace detecta si hay una actualización disponible.

- Automático (predeterminado): Se le notificará cuando haya una actualización disponible. Por ejemplo: `CitrixWorkspaceApp.exe /AutoUpdateCheck=auto`.
- Manual: No se le notificará cuando haya actualizaciones disponibles. Compruebe manualmente si hay actualizaciones. Por ejemplo: `CitrixWorkspaceApp.exe /AutoUpdateCheck=manual`.
- Disabled: Inhabilita las actualizaciones automáticas. Por ejemplo: `CitrixWorkspaceApp.exe /AutoUpdateCheck=disabled`.

### **`/AutoUpdateStream`**

Si ha habilitado la actualización automática, puede elegir la versión que quiera en el calendario de publicación de versiones. Consulte [Hitos del ciclo de vida](#) para obtener más información.

- LTSR: Actualizaciones automáticas solamente para actualizaciones Long Term Service Release Cumulative Updates. Por ejemplo: `CitrixWorkspaceApp.exe /AutoUpdateStream=LTSR`.
- Current: Actualizaciones automáticas para la versión más reciente de la aplicación Citrix Workspace. Por ejemplo: `CitrixWorkspaceApp.exe /AutoUpdateStream=Current`.

### **`/DeferUpdateCount`**

Indica las veces que puede aplazar las notificaciones de actualización cuando haya una disponible. Consulte [Actualizaciones de Citrix Workspace](#) para obtener más información.

- -1 (valor predeterminado): Permite aplazar las notificaciones tantas veces como quiera. Por ejemplo: `CitrixWorkspaceApp.exe /DeferUpdateCount=-1`.
- 0: Indica que recibirá (solo) una notificación por cada actualización disponible. No se le volverá a recordar la actualización. Por ejemplo: `CitrixWorkspaceApp.exe /DeferUpdateCount=0`.
- Cualquier otro número “n”: Permite aplazar las notificaciones de actualización “n” veces. La opción **Recordármelo más tarde** se podrá mostrar tantas veces como indique el valor “n”. Por ejemplo: `CitrixWorkspaceApp.exe /DeferUpdateCount=<n>`.

### **/AURolloutPriority**

Cuando se publica una nueva versión de la aplicación, Citrix implementa la actualización durante un período de entrega específico. Con este parámetro, puede controlar el momento del período de entrega en que puede recibir la actualización.

- Auto (valor predeterminado): Recibe las actualizaciones durante el período de entrega configurado por Citrix. Por ejemplo: `CitrixWorkspaceApp.exe /AURolloutPriority=Auto`.
- Fast: Recibe las actualizaciones al comienzo del período de entrega. Por ejemplo: `CitrixWorkspaceApp.exe /AURolloutPriority=Fast`.
- Medium: Recibe las actualizaciones a mitad del período de entrega. Por ejemplo: `CitrixWorkspaceApp.exe /AURolloutPriority=Medium`.
- Slow: Recibe las actualizaciones al final del período de entrega. Por ejemplo: `CitrixWorkspaceApp.exe /AURolloutPriority=Slow`.

### **/includeappprotection**

Proporciona una mayor seguridad al usar Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service), ya que restringe la posibilidad de que los clientes corran peligro por causa de malware que registra pulsaciones de teclas y captura pantallas..

- `CitrixWorkspaceApp.exe /includeappprotection`

Consulte [App Protection](#) para obtener más información.

### **INSTALLDIR**

Especifica el directorio de instalación personalizado para la instalación de la aplicación Citrix Workspace. La ruta predeterminada es `C:\Program Files\Citrix`. Por ejemplo: `CitrixWorkspaceApp.exe INSTALLDIR=C:\Program Files\Citrix`.

## **ADDLOCAL**

Instala uno o varios componentes especificados. Por ejemplo: `CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,AM,SELSERVICE,DesktopViewer,Flash,Vd3d,WebHelper,BrowserEngine,WorkspaceHub,USB`.

## **Parámetros de funciones HDX**

### **ALLOW\_BIDIRCONTENTREDIRECTION**

Indica que la redirección de contenido bidireccional del cliente al host y del host al cliente está habilitada. Consulte la sección [Configuraciones de directiva de Redirección de contenido bidireccional](#) en la documentación de Citrix Virtual Apps and Desktops para obtener más información.

- 0 (valor predeterminado): Indica que la redirección de contenido bidireccional está inhabilitada. Por ejemplo: `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=0`.
- 1: Indica que la redirección de contenido bidireccional está habilitada. Por ejemplo: `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=1`.

### **FORCE\_LAA**

Indica que la aplicación Citrix Workspace está instalada con el componente de acceso a aplicaciones locales del cliente. Debe instalar la aplicación Citrix Workspace con privilegios de administrador para que este componente funcione. Consulte la sección [Acceso a aplicaciones locales](#) en la documentación de Citrix Virtual Apps and Desktops para obtener más información.

- 0 (predeterminado): Indica que el componente de acceso a aplicaciones locales no está instalado. Por ejemplo: `CitrixWorkspaceApp.exe FORCE_LAA=0`.
- 1: Indica que el componente de acceso a aplicaciones locales del cliente está instalado. Por ejemplo: `CitrixWorkspaceApp.exe FORCE_LAA=1`.

### **LEGACYFTAICONS**

Especifica si se muestran los iconos de aplicación para aquellos documentos o archivos que tienen asociaciones de tipo de archivo con aplicaciones suscritas.

- False (valor predeterminado): Indica que los iconos de la aplicación se muestran para documentos o archivos que tienen asociaciones de tipo de archivo con aplicaciones suscritas. Cuando se establece en “false”, el sistema operativo genera un icono para el documento que no tiene asignado un icono específico. El icono generado por el sistema operativo es un icono

genérico superpuesto con una versión más pequeña del icono de la aplicación. Por ejemplo: `CitrixWorkspaceApp.exe LEGACYFTAICONS=False`.

- True: Indica que los iconos de la aplicación no se muestran para documentos o archivos que tienen asociaciones de tipo de archivo con aplicaciones suscritas. Por ejemplo: `CitrixWorkspaceApp.exe LEGACYFTAICONS=True`.

## **ALLOW\_CLIENTHOSTEDAPPSURL**

Habilita la función de redirección de URL en el dispositivo del usuario. Consulte la sección [Acceso a aplicaciones locales](#) en la documentación de Citrix Virtual Apps and Desktops para obtener más información.

- 0 (predeterminado): Inhabilita la función de redirección de URL en el dispositivo del usuario. Por ejemplo: `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=0`.
- 1: Habilita la función de redirección de URL en el dispositivo del usuario. Por ejemplo: `CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=1`.

## **Parámetros de preferencias e interfaz de usuario**

### **ALLOWADDSTORE**

Permite configurar los almacenes (http o https) en función del parámetro especificado.

- S (predeterminado): Permite agregar o quitar solamente almacenes seguros (configurados con HTTPS). Por ejemplo: `CitrixWorkspaceApp.exe ALLOWADDSTORE=S`.
- A: Permite agregar o quitar tanto almacenes seguros (HTTPS) como no seguros (HTTP). No se aplica si la aplicación Citrix Workspace está instalada por usuario. Por ejemplo: `CitrixWorkspaceApp.exe ALLOWADDSTORE=A`.
- N: No permite nunca que los usuarios agreguen o quiten sus propios almacenes. Por ejemplo: `CitrixWorkspaceApp.exe ALLOWADDSTORE=N`.

### **ALLOWSAVEPWD**

Permite guardar las credenciales del almacén de forma local. Este parámetro solo se aplica a los almacenes que utilizan el protocolo PNAgent.

- S (predeterminado): Permite guardar contraseñas solamente para almacenes seguros (configurados con HTTPS). Por ejemplo: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=S`.
- N: No permite guardar contraseñas. Por ejemplo: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=N`.

- A: Permite que los usuarios guarden contraseñas tanto para almacenes seguros (HTTPS) como no seguros (HTTP). Por ejemplo: `CitrixWorkspaceApp.exe ALLOWSAVEPWD=A`.

## STARTMENUDIR

Especifica la carpeta de accesos directos en el menú Inicio.

- <Directory Name>: De forma predeterminada, las aplicaciones aparecen en **Inicio > Todos los programas**. Puede especificar la ruta relativa de los accesos directos en la carpeta `\Programs`. Por ejemplo, para colocar accesos directos en Inicio > Todos los programas > Workspace, especifique `STARTMENUDIR=\Workspace`.

## DESKTOPDIR

Especifica la carpeta de accesos directos en el Escritorio.

### Nota:

Cuando utilice la opción DESKTOPDIR, establezca la clave `PutShortcutsOnDesktop` en `True`.

- <Directory Name>: Puede especificar la ruta relativa de los accesos directos. Por ejemplo, para colocar accesos directos en Inicio > Todos los programas > Workspace, especifique `DESKTOPDIR=\Workspace`.

## SELFSERVICEMODE

Controla el acceso a la interfaz de usuario de la aplicación Citrix Workspace en modo autoservicio.

- True: Indica que el usuario tiene acceso a la interfaz de usuario de autoservicio. Por ejemplo: `CitrixWorkspaceApp.exe SELFSERVICEMODE=True`.
- False: Indica que el usuario no tiene acceso a la interfaz de usuario de autoservicio. Por ejemplo: `CitrixWorkspaceApp.exe SELFSERVICEMODE=False`.

## ENABLEPRELAUNCH

Controla el preinicio de sesiones. Consulte [Tiempo de inicio de aplicaciones](#) para obtener más información.

- True: Indica que el preinicio de sesiones está habilitado. Por ejemplo: `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True`.
- False: Indica que el preinicio de sesiones está inhabilitado. Por ejemplo: `CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False`.

## DisableSetting

Oculto la opción **Accesos directos y reconexión** para que no se muestre en la hoja **Preferencias avanzadas**. Consulte [Ocultar parámetros concretos de la hoja de Preferencias avanzadas](#) para obtener más información.

- 0 (predeterminado): Muestra tanto la opción de **Accesos directos** como la de **Reconexión** en la hoja Preferencias avanzadas. Por ejemplo: `CitrixWorkspaceApp.exe DisableSetting=0`.
- 1: Muestra solo la opción **Reconexión** en la hoja Preferencias avanzadas. Por ejemplo: `CitrixWorkspaceApp.exe DisableSetting=1`.
- 2: Muestra solo la opción **Accesos directos** en la hoja Preferencias avanzadas. Por ejemplo: `CitrixWorkspaceApp.exe DisableSetting=2`.
- 3: Oculta tanto la opción de **Accesos directos** como la de **Reconexión** en la hoja Preferencias avanzadas. Por ejemplo: `CitrixWorkspaceApp.exe DisableSetting=3`.

## EnableCEIP

Indica su participación en el programa CEIP de mejora de la experiencia del cliente. Consulte [CEIP](#) para obtener más información.

- True (predeterminado): Indica que participa en el programa CEIP. Por ejemplo: `CitrixWorkspaceApp.exe EnableCEIP=True`.
- False: Indica que no participa en el programa CEIP. Por ejemplo: `CitrixWorkspaceApp.exe EnableCEIP=False`.

## EnableTracing

Controla la función de **Seguimiento permanente (Always-on tracing)**.

- True (valor predeterminado): Habilita la función de **Seguimiento permanente (Always-on tracing)**. Ejemplo. `CitrixWorkspaceApp.exe EnableTracing=true`.
- False: Inhabilita la función de **Seguimiento permanente (Always-on tracing)**. Por ejemplo: `CitrixWorkspaceApp.exe EnableTracing=false`.

## CLIENT\_NAME

Especifica el nombre utilizado para identificar el dispositivo de usuario en el servidor.

- `<ClientName>`: Especifica el nombre utilizado para identificar el dispositivo de usuario en el servidor. El nombre predeterminado es `%COMPUTERNAME%`. Por ejemplo: `CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%`.

## **ENABLE\_DYNAMIC\_CLIENT\_NAME**

Permite que el nombre del cliente sea el mismo que el nombre del equipo. Cuando los usuarios cambian el nombre de su equipo, el nombre de cliente también cambia.

- Sí (valor predeterminado): Permite que el nombre del cliente sea el mismo que el nombre del equipo. Por ejemplo: `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=Yes`.
- No: No permite que el nombre del cliente sea el mismo que el nombre del equipo. Debe especificar un valor para la propiedad `CLIENT_NAME`. Por ejemplo: `CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No`.

## **Parámetros de autenticación**

### **ENABLE\_SSON**

Habilita Single Sign-On cuando se instala la aplicación Citrix Workspace con el comando `/includeSSON`. Consulte [Autenticación PassThrough de dominio](#) para obtener más información.

- Sí (valor predeterminado): Indica que Single Sign-On está habilitado. Por ejemplo: `CitrixWorkspaceApp.exe /ENABLE_SSON=Yes`.
- No: Indica que Single Sign-On está inhabilitado. Por ejemplo: `CitrixWorkspaceApp.exe /ENABLE_SSON=No`.

### **ENABLE\_KERBEROS**

Especifica si HDX Engine debe utilizar la autenticación Kerberos. Esto solo se aplica cuando la autenticación por Single Sign-On está habilitada. Para obtener más información, consulte [Autenticación PassThrough de dominio con Kerberos](#).

- Sí: Indica que HDX Engine utilizará la autenticación Kerberos. Por ejemplo: `CitrixWorkspaceApp.exe ENABLE_KERBEROS=Yes`.
- No: Indica que HDX Engine no utilizará la autenticación Kerberos. Por ejemplo: `CitrixWorkspaceApp.exe ENABLE_KERBEROS=No`.

Además de las propiedades anteriores, también puede especificar la URL del almacén que se utiliza con la aplicación Citrix Workspace. Puede agregar hasta 10 almacenes. Utilice la siguiente propiedad para hacerlo:

```
STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[On, Off]; [storedescription]"
```

#### **Valores:**

- x: Los enteros del 0 al 9 se utilizan para identificar un almacén.
- storename: Nombre del almacén. Este valor debe coincidir con el nombre configurado en el servidor de StoreFront.
- servername.domain: El nombre de dominio completo del servidor que aloja el almacén.
- IISLocation: La ruta al almacén en IIS. La URL del almacén debe coincidir con la URL en el archivo de aprovisionamiento de StoreFront. La URL del almacén tiene el formato `/Citrix/store/discovery`. Para obtener la dirección URL, exporte un archivo de aprovisionamiento desde StoreFront, ábralo en el Bloc de notas y copie la dirección URL desde el elemento **Address**.
- 
- storedescription: Una descripción del almacén; por ejemplo, `HR App Store`.

### Ejemplos de una instalación de línea de comandos

#### Para especificar la URL de almacén de Citrix Gateway:

```
CitrixWorkspaceApp.exe STORE0=HRStore;https://ag.mycompany.com#  
Storename;0n;Store
```

donde *Storename* indica el nombre del almacén que debe configurarse.

#### Nota:

- La URL de almacén de Citrix Gateway configurada con este método no admite los sitios de servicios de PNA que utilicen Citrix Gateway.
- Si configura más de un almacén, coloque la URL del almacén de Citrix Gateway al principio de la lista. Solo se permite una configuración de URL del almacén de Citrix Gateway.

#### Para instalar todos los componentes de manera silenciosa y especificar dos almacenes de aplicaciones:

```
CitrixWorkspaceApp.exe /silent  
STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;  
HR App Store"  
STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/  
discovery;on;Backup HR App Store"
```

#### Nota:

- Es obligatorio incluir `/discovery` en la URL del almacén para que la autenticación PassThrough se lleve a cabo correctamente.
- La URL de almacén de Citrix Gateway debe ser la primera entrada en la lista de direcciones URL configuradas de almacén.

## Desinstalar

### Usar un instalador basado en Windows:

Puede desinstalar la aplicación Citrix Workspace para Windows con la herramienta Programas y características (Agregar o quitar programas) de Windows.

#### Nota:

Recibirá un mensaje para desinstalar el paquete Citrix HDX RTME para poder continuar con la instalación de la aplicación Citrix Workspace para Windows. Haga clic en Aceptar para continuar con la desinstalación.

### Instalar mediante la interfaz de línea de comandos:

Puede desinstalar la aplicación Citrix Workspace para Windows desde una línea de comandos con el comando siguiente:

```
CitrixWorkspaceApp.exe /uninstall
```

Para una desinstalación silenciosa de la aplicación Citrix Workspace para Windows, ejecute el siguiente modificador de línea de comandos:

```
CitrixWorkspaceApp.exe /silent /uninstall
```

#### Nota:

- Las claves de Registro que crean receiver.adm/receiver.adml o receiver.admx permanecen después de la desinstalación.
- Si encuentra alguna entrada en el Editor del Registro después de la desinstalación, elimínela manualmente.

## Implementación

October 30, 2023

Puede implementar la aplicación Citrix Workspace con los siguientes métodos:

- Use Active Directory y los scripts de inicio de ejemplo para implementar la aplicación Citrix Workspace para Windows. Para obtener más información acerca de Active Directory, consulte [Usar Active Directory y scripts de ejemplo](#).
- Usar Workspace para Web para asegurarse de que los usuarios tengan instalada la aplicación Citrix Workspace para Windows antes de iniciar una aplicación desde un explorador web. Para obtener más información, consulte [Usar Workspace para Web](#).

- Utilice una herramienta ESD (Electronic Software Distribution) como Microsoft System Center Configuration Manager 2012 R2. Para obtener más información, consulte [Usar System Center Configuration Manager 2012 R2](#).

## Usar Active Directory y scripts de ejemplo

Se pueden usar los scripts de directiva de grupo de Active Directory para implementar la aplicación Citrix Workspace para Windows en sistemas basados en la estructura organizativa de Active Directory. Citrix recomienda usar los scripts en lugar de extraer los archivos MSI. Para obtener información general acerca de los scripts de inicio, consulte la [documentación de Microsoft](#).

### Para usar los scripts con Active Directory:

1. Cree la unidad organizativa (UO) para cada script.
2. Cree un objeto de directiva de grupo (GPO) para la unidad organizativa recién creada.

## Modificar scripts

Modifique estos parámetros de los scripts en la sección del encabezado de cada archivo:

- **Current Version of package (Versión actual del paquete):** El número de versión especificado se valida y, si no existe, se lleva a cabo la implementación. Por ejemplo, establezca DesiredVersion en 3.3.0.XXXX para que coincida exactamente con la versión especificada. Por ejemplo, si especifica la versión parcial 3.3.0, esa versión coincidirá con cualquier versión que contenga ese prefijo (3.3.0.1111, 3.3.0.7777 y así sucesivamente).
- **Package Location/Deployment directory (Ubicación del paquete/directorio de distribución):** Especifica el recurso compartido de red que contiene los paquetes (el script no realiza la autenticación). La carpeta compartida debe tener permisos de lectura para todos (EVERYONE).
- **Script Logging Directory (Directorio de registros del script):** Especifica el recurso compartido de red donde se copiarán los registros de instalación (el script no realiza la autenticación). La carpeta compartida debe tener permisos de lectura y escritura para todos (EVERYONE).
- **Package Installer Command Line Options (Opciones de línea de comandos del instalador):** Estas opciones de línea de comandos se envían al instalador. Para obtener información sobre la sintaxis de la línea de comandos, consulte [Usar parámetros de línea de comandos](#).

## Scripts

El instalador de la aplicación Citrix Workspace incluye scripts de ejemplo por equipos y por usuarios para instalar y desinstalar dicha aplicación. Los scripts se encuentran en la página [Descargas](#) de la aplicación Citrix Workspace para Windows.

---

<b>Tipo de implementación</b>	<b>Para implementar</b>	<b>Para quitar</b>
Por equipo	CheckAndDeployWorkspacePerMachineSetupScriptWork	CheckAndRemoveWorkspacePerMachineSta
Por usuario	CheckAndDeployWorkspacePerUserLoginScript.bat	CheckAndRemoveWorkspacePerUserLogonS

---

#### **Para agregar los scripts de inicio:**

1. Abra la Consola de administración de directivas de grupo.
2. Seleccione **Configuración del equipo** o **Configuración del usuario** > **Directivas** > **Configuración de Windows** > **Scripts**.
3. En el panel derecho de la Consola de administración de directivas de grupo, seleccione **Inicio de sesión**.
4. Seleccione **Mostrar archivos** y copie el script correspondiente en la carpeta mostrada.
5. Cierre el cuadro de diálogo.
6. En el menú **Propiedades**, haga clic en **Agregar** y use la opción **Examinar** para buscar y agregar los scripts recientemente creados.

#### **Para implementar la aplicación Citrix Workspace para Windows:**

1. Mueva los dispositivos de usuario designados para recibir esta implementación a la unidad organizativa creada.
2. Reinicie el dispositivo de usuario e inicie sesión.
3. Verifique que el paquete recién instalado esté listado en **Programa y características**.

#### **Para quitar la aplicación Citrix Workspace para Windows:**

1. Mueva los dispositivos de usuario designados para la eliminación a la unidad organizativa creada.
2. Reinicie el dispositivo de usuario e inicie sesión.
3. Verifique que el paquete recién instalado no aparezca en Programas y características.

### **Usar Workspace para Web**

Puede implementar la aplicación Citrix Workspace para Windows desde Workspace para Web si quiere que los usuarios lo tengan instalado antes de que intenten conectarse a una aplicación desde un explorador. El sitio de Workspace para Web permite que los usuarios accedan a almacenes de StoreFront a través de una página web. Si el sitio de Workspace para Web detecta que un usuario no dispone de una versión compatible de la aplicación Citrix Workspace para Windows, se le solicita que descargue e instale la aplicación Citrix Workspace para Windows.

La detección de cuentas basada en correo electrónico no está disponible cuando la aplicación Citrix Workspace para Windows se implementa desde Workspace para Web. Si la detección de cuentas

basada en correo electrónico está configurada y un usuario nuevo instala la aplicación Citrix Workspace para Windows desde Citrix.com, la aplicación Citrix Workspace para Windows pide al usuario una dirección de correo electrónico o de servidor. Al introducir una dirección de correo electrónico, se recibe un mensaje de error similar al siguiente: “Su dirección de correo electrónico no puede usarse para agregar una cuenta”.

Use la siguiente configuración para que solo se pida la dirección del servidor.

1. Descargue [CitrixWorkspaceApp.exe](#) en el equipo local.
2. Cambie el nombre de [CitrixWorkspaceApp.exe](#) a [CitrixWorkspaceAppWeb.exe](#).
3. Distribuya el ejecutable con el nuevo nombre con su método de distribución habitual. Si usa StoreFront, consulte [Configurar sitios de Workspace para Web mediante archivos de configuración](#) en la documentación de StoreFront.

## Usar System Center Configuration Manager 2012 R2

Puede usar Microsoft System Center Configuration Manager (SCCM) para implementar la aplicación Citrix Workspace.

### Nota:

Solo Citrix Receiver para Windows 4.5 y las versiones posteriores admiten la implementación con SCCM.

Hay cuatro partes a completar en la implementación de la aplicación Citrix Workspace para Windows mediante SCCM:

1. Agregar la aplicación Citrix Workspace a la implementación SCCM
2. Agregar puntos de distribución
3. Implementar la aplicación Citrix Workspace en el centro de software
4. Crear colecciones de dispositivos

## Agregar la aplicación Citrix Workspace a la implementación SCCM

1. Copie la carpeta de instalación de la aplicación Citrix Workspace descargada a una carpeta en el servidor de Configuration Manager e inicie la consola de Configuration Manager.
2. Seleccione **Biblioteca de Software > Administración de aplicaciones**. Haga clic con el botón secundario en **Aplicación** y haga clic en **Crear aplicación**.  
Se abrirá el Asistente para crear aplicaciones.
3. En el panel **General**, haga clic en **Especificar manualmente la información de la aplicación** y, a continuación, haga clic en **Siguiente**.

4. En el panel **Información general**, especifique información acerca de la aplicación (por ejemplo, el nombre, el fabricante o la versión de software).
5. En el asistente Catálogo de aplicaciones, especifique información adicional, como el idioma, el nombre de la aplicación o la categoría de usuario, y haga clic en **Siguiente**.

**Nota:**

Los usuarios pueden ver la información que especifique aquí.

6. En el panel **Tipo de implementación**, haga clic en **Agregar** para configurar el tipo de implementación para la instalación de la aplicación Citrix Workspace.  
Aparecerá el Asistente para crear tipos de implementación.
7. En el panel **General**, establezca el tipo de implementación en el valor Windows Installer (archivo \*.msi), seleccione **Especificar manualmente la información del tipo de implementación** y haga clic en **Siguiente**.
8. En el panel **Información General**, especifique los detalles del tipo de implementación (por ejemplo, Implementación de Workspace) y haga clic en **Siguiente**.
9. En el panel **Contenido**:
  - a) Suministre la ruta donde se encuentra el archivo de instalación de la aplicación Citrix Workspace. Por ejemplo: Herramientas en el servidor SCCM.
  - b) Especifique el **programa de instalación** como uno de los siguientes:
    - `CitrixWorkspaceApp.exe /silent` para establecer la instalación silenciosa como instalación predeterminada.
    - `CitrixWorkspaceApp.exe /silent /includeSSON` para habilitar el PassThrough de dominio
    - `CitrixWorkspaceApp.exe /silent SELFSERVICEMODE=false` para instalar la aplicación Citrix Workspace en un modo que no sea de autoservicio.
  - c) Especifique **Programa de desinstalación** como `CitrixWorkspaceApp.exe /uninstall` (para habilitar la desinstalación a través de SCCM).
10. En el panel **Método de detección**, seleccione **Configurar reglas para detectar la presencia de este tipo de implementación** y haga clic en **Agregar cláusula**.  
Aparece el cuadro de diálogo Regla de actualización.
  - Establezca **Tipo de configuración** en “Sistema de archivos”.
  - En **Especificar el archivo o la carpeta para detectar esta aplicación**, establezca las siguientes opciones:
    - **Tipo**: En el menú desplegable, seleccione **Archivo**.
    - **Ruta**: `%ProgramFiles(x86)%\Citrix\ICA Client\Receiver\`

- **Nombre de archivo o carpeta:** `receiver.exe`
- **Propiedad:** En el menú desplegable, seleccione **Versión**.
- **Operador:** En el menú desplegable, seleccione **Mayor o igual que**.
- **Valor:** Escriba el número de versión de la aplicación Citrix Workspace que se va a implementar.

**Nota:**

Esta combinación de reglas también es aplicable a actualizaciones de la aplicación Citrix Workspace para Windows.

11. En el panel **Experiencia del usuario**, establezca:

- **Comportamiento de instalación:** Instalar para el sistema.
  - **Requisito de inicio de sesión:** Tanto si un usuario inició sesión como si no.
  - **Visibilidad del programa de instalación:** Normal
- Haga clic en **Siguiente**.

**Nota:**

No especifique requisitos ni dependencias para este tipo de implementación.

12. En el panel **Resumen**, verifique los parámetros de este tipo de implementación. Haga clic en **Siguiente**.

Aparecerá un mensaje indicando que la conexión tuvo lugar.

13. En el **panel Finalización**, aparece listado un nuevo tipo de implementación (Implementación de Workspace) en Tipos de implementación.

14. Haga clic en **Siguiente** y **Cerrar**.

### Agregar puntos de distribución

1. Haga clic con el botón secundario en la aplicación Citrix Workspace desde la consola de Configuration Manager y seleccione **Distribuir contenido**.

Aparecerá el asistente para distribuir contenido.

2. En el panel “Distribución de contenido”, haga clic en **Agregar > Puntos de distribución**.

Aparecerá el cuadro de diálogo para agregar puntos de distribución.

3. Vaya al servidor de SCCM donde está disponible el contenido y haga clic en **Aceptar**.

En el panel “Finalización”, se muestra un mensaje indicando que la operación es correcta.

4. Haga clic en **Cerrar**.

## Implementar la aplicación Citrix Workspace en el centro de software

1. Haga clic con el botón secundario en la aplicación Citrix Workspace en la consola de Configuration Manager y seleccione **Implementar**.  
Aparece el asistente para implementar software.
2. Seleccione **Examinar** y vaya a la colección (puede ser “Recopilación de dispositivo” o “Recopilación de usuario”) donde la aplicación va a implementarse y haga clic en **Siguiente**.
3. En el panel **Configuración de implementación**, establezca **Acción** en “Instalar” y **Propósito** en “Requerido” (permite la instalación sin supervisión). Haga clic en **Siguiente**.
4. En el panel **Programación**, especifique la programación para implementar el software en los dispositivos de destino.
5. En el panel **Experiencia del usuario**, establezca el comportamiento de las **Notificaciones de usuario**; seleccione **Confirmar cambios dentro de la fecha límite o en una ventana de mantenimiento (reinicio necesario)** y haga clic en **Siguiente** para completar el asistente para implementar software.

En el panel Finalización, se muestra un mensaje que indica que la operación se realizó correctamente.

Reinicie los dispositivos de punto final de destino (requerido solo para iniciar la instalación inmediatamente).

En los dispositivos de punto final, la aplicación Citrix Workspace está visible en el Centro de software, en **Software disponible**. La instalación se activa automáticamente en función de la programación que se configure. Si lo prefiere, también puede programarla o instalarla a demanda. Una vez comenzada la instalación, se muestra el estado de esta en el Centro de software.

## Crear colecciones de dispositivos

1. Abra la consola de Configuration Manager, haga clic en **Activos y compatibilidad > Resumen > Dispositivos**.
2. Haga clic con el botón secundario en **Recopilaciones de dispositivos** y seleccione **Crear recopilación de dispositivos**.  
Se abrirá el asistente para crear recopilaciones de dispositivos.
3. En el panel General, escriba el **Nombre** del dispositivo y haga clic en **Examinar** para “Recopilación de restricción”.  
Esto determina el ámbito de los dispositivos, que puede ser una de las recopilaciones de dispositivos predeterminadas creadas por SCCM.  
Haga clic en **Siguiente**.

4. En el panel Reglas de pertenencia, haga clic en **Agregar regla** para filtrar los dispositivos.  
Aparecerá el asistente para crear reglas de pertenencia directa.
  - En el panel Buscar recursos, seleccione el **Nombre del atributo** en función de los dispositivos que quiere filtrar y suministre el valor del Nombre del atributo para seleccionar los dispositivos.
5. Haga clic en **Siguiente**. En el panel Seleccionar recursos, seleccione los dispositivos que deben formar parte de la colección de dispositivos.  
En el panel “Finalización”, se muestra un mensaje indicando que la operación es correcta.
6. Haga clic en **Cerrar**.
7. En el panel Reglas de pertenencia, aparecerá una nueva regla. Haga clic en Siguiente.
8. En el panel Finalización, se muestra un mensaje que indica que la operación se realizó correctamente. Haga clic en **Cerrar** para completar el Asistente para crear una recopilación de dispositivos.

La nueva colección de dispositivos aparece en **Recopilaciones de dispositivos**. La nueva colección de dispositivos forma parte de las Recopilaciones de dispositivos al buscar en el Asistente para implementar software.

**Nota:**

Cuando se establece el atributo **MSIRESTARTMANAGERCONTROL** en **Falso**, la implementación de la aplicación Citrix Workspace para Windows con SCCM puede fallar.

Según nuestros análisis, la aplicación Citrix Workspace para Windows no es la causa de este fallo. Además, la implementación puede ser correcta en el siguiente intento.

## Actualización

April 22, 2024

### Actualización manual

Si ya instaló la aplicación Citrix Workspace para Windows, descargue e instale la versión más reciente de la aplicación desde la [página Descargas de Citrix](#).

## Actualización automática

A partir de la versión 1912 Cumulative Update 4 (CU4), se modifican las rutas de registros de Actualizaciones de Citrix Workspace. En el caso de las actualizaciones de toda la máquina, los registros de Actualizaciones de Workspace están presentes en C:\Archivos de programa (x86)\Citrix\Logs. En el caso de las actualizaciones de todos los usuarios, los registros están en la carpeta temporal del usuario.

Cuando se publica una nueva versión de la aplicación Citrix Workspace, Citrix envía una actualización al sistema que tiene instalada la aplicación Citrix Workspace.

### Nota:

- Si configuró un proxy SSL interceptor de salida, agregue una excepción al servidor de actualización automática de Workspace <https://downloadplugins.citrix.com/> para recibir actualizaciones de Citrix.
- La actualización automática no está disponible para las versiones anteriores a la aplicación Citrix Workspace 2104 ni a la aplicación Citrix Workspace 1912 LTSR CU4.
- Si ha configurado un proxy SSL interceptor de salida, agregue una excepción al servicio de firma de actualización automática de Workspace <https://citrixupdates.cloud.com/> y la ubicación de descarga <https://downloadplugins.citrix.com/> para recibir actualizaciones de Citrix.
- El sistema debe tener una conexión a Internet para recibir actualizaciones.
- De forma predeterminada, la función Actualizaciones de Citrix Workspace está inhabilitada en el VDA. Esto incluye máquinas de servidor multiusuario RDS, máquinas VDI y máquinas de acceso con Remote PC.
- La función Actualizaciones de Citrix Workspace está inhabilitada en máquinas donde esté instalado Desktop Lock.
- Los usuarios de Workspace para Web no pueden descargar automáticamente la directiva de StoreFront.
- La función Actualizaciones de Citrix Workspace solo se puede limitar a las actualizaciones LTSR.
- Citrix HDX RTME para Windows se incluye en Actualizaciones de Citrix Workspace. Se le notifica sobre la actualización de HDX RTME disponible tanto en versión LTSR como en la versión Current Release de la aplicación Citrix Workspace.

## Configuración avanzada para actualizaciones automáticas (Actualizaciones de Citrix Workspace)

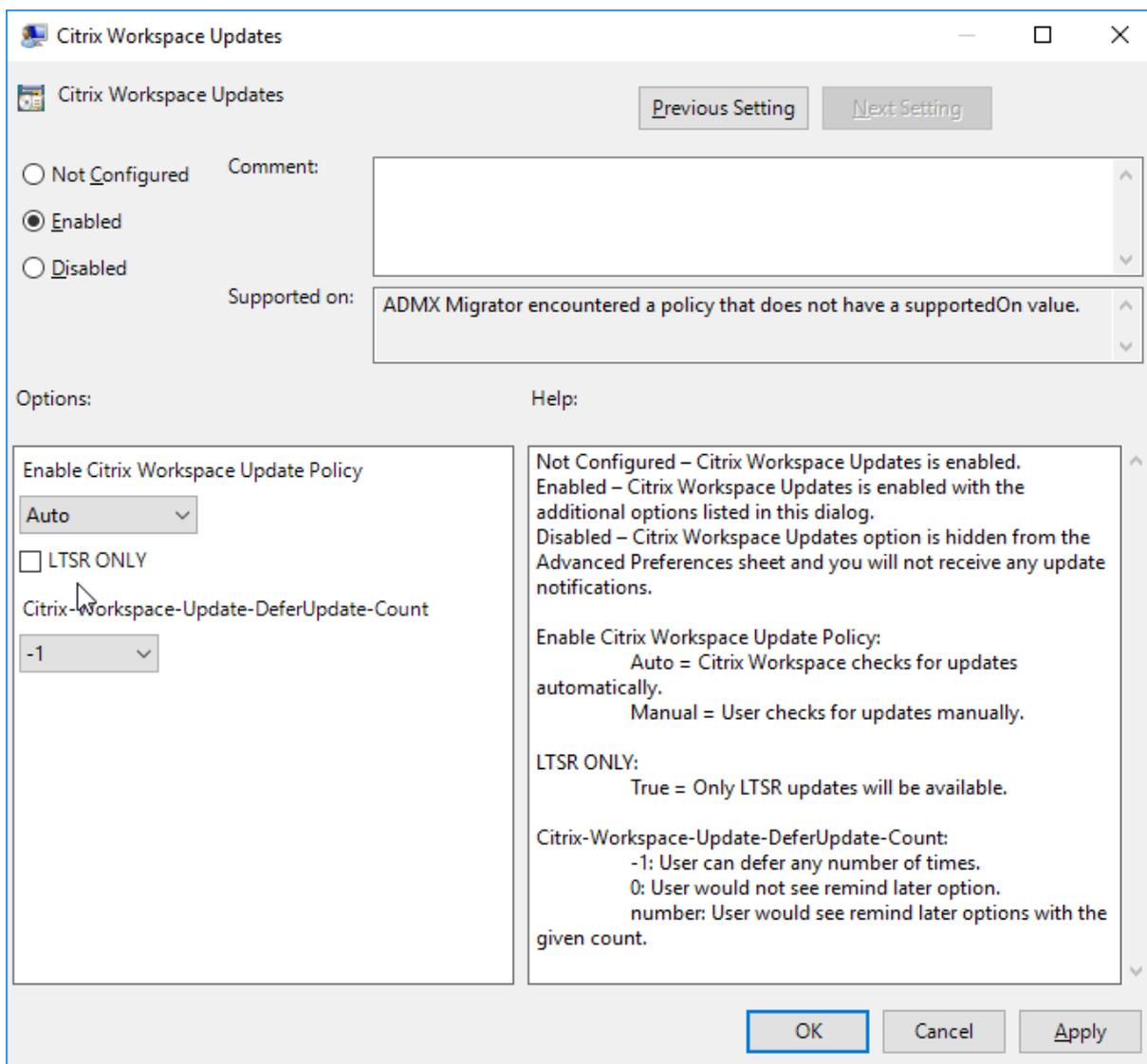
Puede configurar Actualizaciones de Citrix Workspace con estos métodos:

1. Plantilla administrativa de objetos de directiva de grupo (GPO)

- 2. Interfaz de la línea de comandos
- 3. Interfaz gráfica de usuario
- 4. StoreFront

### Configurar Actualizaciones de Citrix Workspace con la plantilla administrativa de objeto de directiva de grupo

Para abrir la plantilla administrativa de objeto de directiva de grupo de la aplicación Citrix Workspace, ejecute gpedit.msc y, en el nodo Configuración del equipo, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Actualizaciones de Workspace**.



- 1. **Habilitar o inhabilitar actualizaciones.** Seleccione **Habilitado** o **Inhabilitado** para habilitar o inhabilitar Actualizaciones de Workspace.

**Nota:**

Si marca **Inhabilitado**, no se le notificará de las nuevas actualizaciones disponibles. También se oculta la opción Actualizaciones de Citrix Workspace en la hoja Preferencias avanzadas.

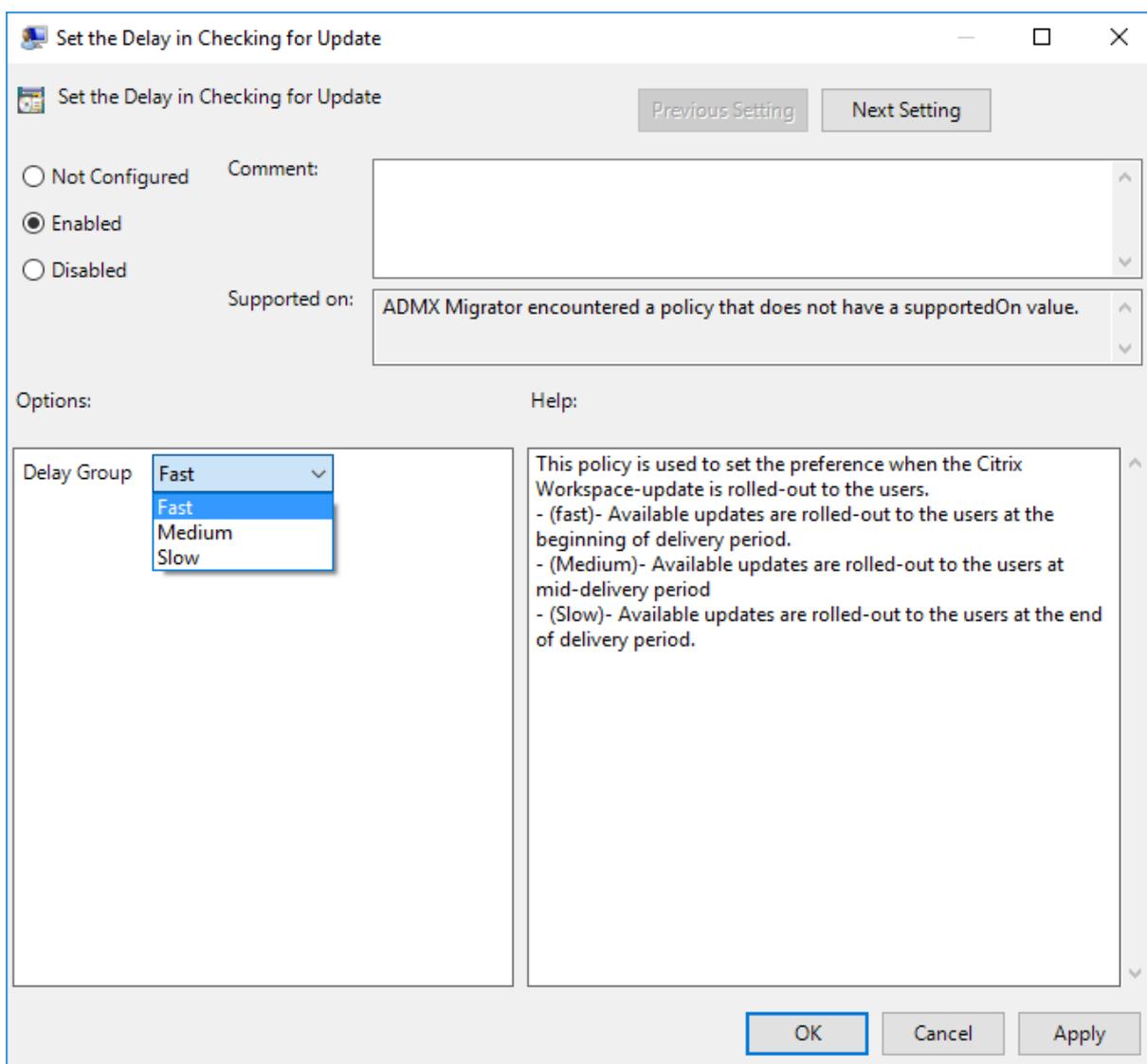
2. **Notificación de actualización.** Cuando haya una actualización disponible, puede optar por recibir una notificación automática o comprobarlo manualmente. Una vez habilitadas las actualizaciones de Workspace, seleccione una de las opciones siguientes en la lista desplegable

**Directiva para habilitar la actualización de Citrix Workspace:**

- Auto: Se le notificará cuando haya una actualización disponible (predeterminado).
  - Manual: No se le notificará cuando haya actualizaciones disponibles. Compruebe manualmente si hay actualizaciones.
3. Seleccione **SOLO LTSR** para obtener las actualizaciones para LTSR solamente.
  4. En la lista desplegable **Citrix-Workspace-Update-DeferUpdate-Count**, seleccione un valor entre -1 y 30, donde
    - 1: Permite aplazar la notificación tantas veces como quiera (valor predeterminado).
    - 0: Recibirá solo una notificación con respecto a la actualización.

**Configurar la demora en la comprobación de actualizaciones** Cuando hay disponible una nueva versión de la aplicación Citrix Workspace, Citrix implementa la actualización durante un período de entrega específico. Con esta propiedad, puede controlar el momento del período de entrega en que puede recibir la actualización.

Para configurar el período de entrega, ejecute `gpedit.msc` para iniciar la plantilla administrativa de objeto de directiva de grupo. En el nodo Configuración del equipo, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Definir demora para comprobar actualizaciones**.



Seleccione **Habilitado** y, en el menú desplegable **Demorar grupo**, seleccione una de las siguientes opciones:

- **Fast (Rápido):** La implantación de la actualización tiene lugar al comienzo del período de entrega.
- **Medium (Medio):** La implantación de la actualización tiene lugar hacia la mitad del período de entrega.
- **Slow (Lento):** La implantación de la actualización tiene lugar al final del período de entrega.

**Nota:**

Si marca **Inhabilitada**, no se le notificará de las actualizaciones disponibles. También se oculta la opción Actualizaciones de Citrix Workspace en la hoja Preferencias avanzadas.

## Configurar Actualizaciones de Citrix Workspace mediante la interfaz de línea de comandos

### Especificando parámetros de línea de comandos al instalar la aplicación Citrix Workspace:

Puede configurar las actualizaciones de Workspace especificando parámetros de línea de comandos durante la instalación de la aplicación Citrix Workspace. Consulte [Parámetros de instalación](#) para obtener más información.

### Mediante parámetros de línea de comandos después de instalar la aplicación Citrix Workspace:

Actualizaciones de Citrix Workspace se puede configurar después de instalar la aplicación Citrix Workspace para Windows. Diríjase a la ubicación de CitrixReceiverUpdater.exe desde la línea de comandos de Windows.

Normalmente, CitrixWorkspaceUpdater.exe está en `CitrixWorkspaceInstallLocation\Citrix\ICA Client\Receiver`. Puede ejecutar este binario junto con los parámetros de línea de comandos que se indican en la sección [Parámetros de instalación](#).

Por ejemplo:

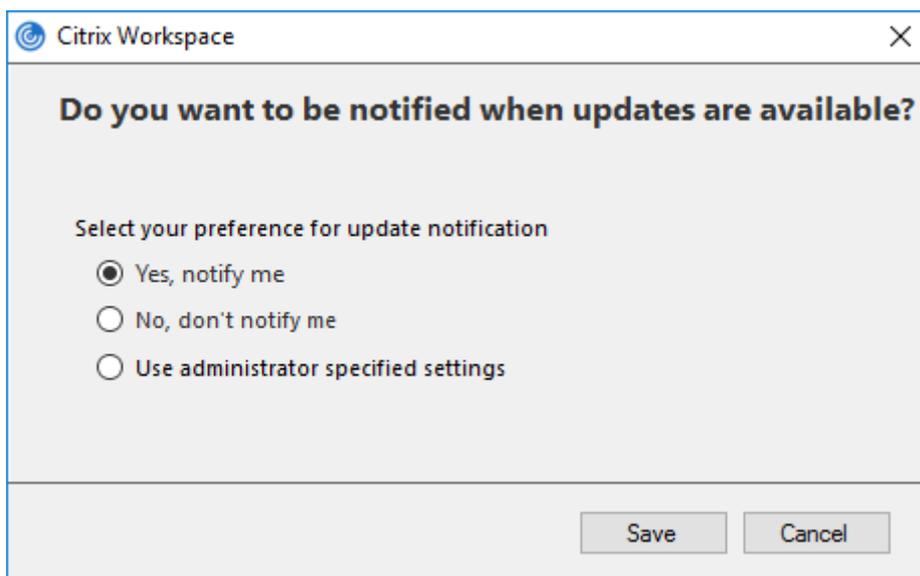
```
CitrixReceiverUpdater.exe /AutoUpdateCheck=auto /AutoUpdateStream=Current /DeferUpdateCount=-1 /AURolloutPriority=fast
```

#### Nota:

`/AutoUpdateCheck` es un parámetro obligatorio que debe definir para configurar otros parámetros como `AutoUpdateStream`, `/DeferUpdateCount` o `/AURolloutPriority`.

## Configurar Actualizaciones de Citrix Workspace mediante la interfaz gráfica de usuario

Un usuario individual puede supeditar el parámetro Actualizaciones de Citrix Workspace desde el cuadro de diálogo Preferencias avanzadas. Se trata de una configuración específica de usuario y los parámetros se aplican solamente al usuario actual. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace situado en el área de notificaciones. Seleccione **Preferencias avanzadas > Actualizaciones de Citrix Workspace**. Seleccione la preferencia de notificación y haga clic en **Guardar**.



**Nota:**

Puede ocultar total o parcialmente las opciones de la hoja de Preferencias avanzadas, disponible en el icono de la aplicación Citrix Workspace del área de notificaciones. Para obtener más información, consulte la sección [Hoja de Preferencias avanzadas](#).

### Configurar Actualizaciones de Citrix Workspace mediante StoreFront

1. Utilice un editor de texto para abrir el archivo `web.config`, que normalmente se encuentra en `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Localice el elemento de la cuenta de usuario en el archivo (Store es el nombre de cuenta de la implementación)

Por ejemplo: `<account id=... name="Store">`

Antes de la etiqueta `</account>`, vaya a las propiedades de esa cuenta de usuario:

```
1 <properties>
2     <clear/>
3 </properties>
4 <!--NeedCopy-->
```

3. Agregue la etiqueta de actualización automática después de `<clear />`.

```
1 <account>
2
3     <clear />
4
5     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
6         F84Store"
```

```
7      description="" published="true" updaterType="Citrix"
8          remoteAccessType="None">
9      <annotatedServices>
10
11      <clear />
12
13      <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
14
15      <metadata>
16
17      <plugins>
18
19      <clear />
20
21      </plugins>
22
23      <trustSettings>
24
25      <clear />
26
27      </trustSettings>
28
29      <properties>
30
31      <property name="Auto-Update-Check" value="auto" />
32
33      <property name="Auto-Update-DeferUpdate-Count" value
34          ="1" />
35
36      <property name="Auto-Update-LTSR-Only" value
37          ="FALSE" />
38
39      <property name="Auto-Update-Rollout-Priority" value=
40          "fast" />
41
42      </properties>
43
44      </metadata>
45
46      </annotatedServiceRecord>
47
48      </annotatedServices>
49
50      <metadata>
51
52      <plugins>
53
54      <clear />
55
56      </plugins>
57
58      <trustSettings>
```

```
56
57     <clear />
58
59 </trustSettings>
60
61 <properties>
62
63     <clear />
64
65 </properties>
66
67 </metadata>
68
69 </account>
70
71 <!--NeedCopy-->
```

El significado de las propiedades y sus posibles valores se detallan a continuación:

- **Auto-update-Check:** Indica que la aplicación Citrix Workspace detecta automáticamente cuándo hay una actualización disponible.
- **Auto-Update-LTSR-Only:** Indica que la actualización de la versión es solamente para LTSR.
- **Auto-Update-Rollout-Priority:** Indica el período de entrega en el que puede recibir la actualización.
- **Auto-update-DeferUpdate-Count:** Indica el número de veces que puede aplazar las notificaciones relativas a las actualizaciones de la versión.

## Introducción

April 22, 2024

Este es un documento de referencia para configurar el entorno después de instalar la aplicación Citrix Workspace.

### Requisitos previos:

Compruebe que todos los requisitos del sistema se cumplen según se indica en la sección [Requisitos del sistema](#).

Debe configurar lo siguiente antes de comenzar a utilizar la aplicación Citrix Workspace:

- [Plantilla administrativa de objetos de directiva de grupo](#)
- [StoreFront](#)
- [Almacén de Citrix Gateway](#)
- [Agregar URL de almacén a la aplicación Citrix Workspace](#)

- [Asignación de unidades del cliente](#)
- [Resolución de nombres de DNS](#)

## Plantilla administrativa de objetos de directiva de grupo

Citrix recomienda usar la plantilla administrativa de objetos de directiva de grupo (GPO) para definir reglas para la redirección de red, servidores proxy, la configuración de servidores de confianza, la redirección de usuarios, dispositivos de usuario remotos y la experiencia de usuario.

Puede utilizar los archivos de plantilla `receiver.admx` o `receiver.adml` con directivas de dominio y de equipos locales. Para las directivas de dominio, importe el archivo de plantilla mediante la Consola de administración de directivas de grupo. Es útil para aplicar los parámetros de la aplicación Citrix Workspace a diferentes dispositivos de usuario en la empresa. Para afectar un solo dispositivo de usuario, importe el archivo de plantilla mediante el Editor de directivas de grupo local del dispositivo.

Citrix recomienda utilizar la plantilla administrativa de GPO de Windows para configurar la aplicación Citrix Workspace.

A partir de Citrix Receiver para Windows 4.6, el directorio de instalación incluye `CitrixBase.admx` y `CitrixBase.adml`, así como los archivos de plantilla administrativa (`receiver.adm`, `receiver.admx` o `receiver.adml`, según el sistema operativo).

### Nota:

El archivo ADM solo se usa para plataformas Windows XP Embedded. Los archivos `.adm`/`.adml` se usan con Windows Vista/Windows Server 2008 y todas las versiones posteriores de Windows.

Si la aplicación Citrix Workspace se instala con el VDA, los archivos `adm`/`adml` se encuentran en el directorio de instalación de la aplicación Citrix Workspace. Por ejemplo: `<directorio de instalación>\Online Plugin\Configuration`.

Si la aplicación Citrix Workspace se instala sin el VDA, los archivos `adm`/`adml` suelen encontrarse en el directorio `C:\Program Files\Citrix\ICA Client\Configuration`.

Consulte la tabla siguiente para ver información sobre los archivos de plantillas de la aplicación Citrix Workspace y su ubicación respectiva.

### Nota:

Citrix recomienda usar los archivos de plantilla de objetos de directiva de grupo (GPO) proporcionados con la versión más reciente de la aplicación Citrix Workspace.

<b>Tipo de archivo</b>	<b>Ubicación de archivos</b>
receiver.adm	<Directorio de instalación>\ICA Client\Configuration
receiver.admx	<Directorio de instalación>\ICA Client\Configuration
receiver.adml	\ICA Client\Configuration\[[MUIculture]
CitrixBase.admx	<Directorio de instalación>\ICA Client\Configuration
CitrixBase.adml	\ICA Client\Configuration\[[MUIculture]

---

**Nota:**

- Si no se agrega CitrixBase.admx\adml al GPO local, se puede perder la directiva **Habilitar ICA File Signing**.
- Al actualizar la aplicación Citrix Workspace, debe agregar los archivos de plantilla más recientes al GPO local, según se describe en el siguiente procedimiento. Los parámetros anteriores se conservan aunque importe archivos de versiones más recientes.

**Para agregar el archivo de la plantilla receiver.adm al objeto de directiva de grupo local (solo para el sistema operativo Windows XP Embedded):**

Citrix recomienda usar los archivos CitrixBase.admx y CitrixBase.adml para asegurarse de que las opciones se organizan y se muestran correctamente en el Editor de objetos de directiva de grupo.

Puede utilizar archivos de plantilla ADM para configurar los objetos de directiva de grupo locales y/o aquellos que utilizan dominios.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta **Plantillas administrativas**.
3. En el menú **Acción**, seleccione **Agregar o quitar plantillas**.
4. Seleccione **Agregar** y busque la ubicación del archivo de plantilla `<Installation Directory>\ICA Client\Configuration\receiver.adm`.
5. Seleccione **Abrir** para agregar la plantilla y luego haga clic en Cerrar para regresar al Editor de directivas de grupo.

El archivo de plantilla de la aplicación Citrix Workspace está disponible en el GPO local, en **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Workspace**.

Una vez que los archivos de plantilla .adm se agreguen al objeto de directiva de grupo local, aparecerá el siguiente mensaje:

“The following entry in the [strings] section is too long and has been truncated”(La siguiente entrada en la sección [cadenas] es demasiado larga y se ha cortado):

Haga clic en **OK** para ignorar el mensaje.

**Para agregar los archivos de plantilla receiver.admx/adml al objeto de directiva de grupo local (en versiones más recientes del sistema operativo Windows):**

Puede utilizar archivos de plantilla ADM para configurar los objetos de directiva de grupo locales y/o aquellos que utilizan dominios. Consulte [aquí](#) el artículo de Microsoft MSDN acerca de la administración de archivos ADMX.

Después de instalar la aplicación Citrix Workspace, copie los archivos de plantilla como se indica en la siguiente tabla:

Tipo de archivo	Copiar de	Copiar a
receiver.admx	Directorio de instalación\ICA Client\Configuration\receiver.admx	%systemroot%\policyDefinitions
CitrixBase.admx	Directorio de instalación\ICA Client\Configuration\CitrixBase.admx	%systemroot%\policyDefinitions
receiver.adml	Directorio de instalación\ICA Client\Configuration[MUIculture]receiver.adml	%systemroot%\policyDefinitions[MUIculture]
CitrixBase.adml	Directorio de instalación\ICA Client\Configuration[MUIculture]\CitrixBase.adml	%systemroot%\policyDefinitions[MUIculture]

**Nota:**

Los archivos de plantilla de la aplicación Citrix Workspace están disponibles en el GPO local, en la carpeta **Plantillas administrativas > Componentes de Citrix > Citrix Workspace** solo si se agrega el archivo CitrixBase.admx o CitrixBase.adml a la carpeta `\PolicyDefinitions`.

## StoreFront

Citrix StoreFront autentica una conexión a Citrix Virtual Apps and Desktops, Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) y VDI-in-a-Box, y enumera y agrupa los escritorios y

las aplicaciones disponibles en unos almacenes a los que los usuarios acceden mediante la aplicación Citrix Workspace.

Además de la configuración resumida en esta sección, es necesario configurar Citrix Gateway para permitir que los usuarios se conecten desde fuera de la red interna (por ejemplo, usuarios que se conectan desde Internet o ubicaciones remotas).

**Nota:**

Cuando se selecciona la opción para mostrar todos los almacenes, es posible que vea la antigua interfaz de usuario de StoreFront.

**Para configurar StoreFront:**

Instale y configure StoreFront como se describe en la documentación de [StoreFront](#). La aplicación Citrix Workspace requiere una conexión HTTPS. Si el servidor de StoreFront está configurado para HTTP, es necesario definir una clave de Registro en el dispositivo de usuario, según se describe en [Usar parámetros de línea de comandos](#), en la descripción de la propiedad **ALLOWADDSTORE**.

**Nota:**

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

## Almacén de Citrix Gateway

**Para agregar o especificar un Citrix Gateway mediante la plantilla administrativa de objeto de directiva de grupo:**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Workspace > StoreFront**.
3. Seleccione **Lista de cuentas de StoreFront/URL de Citrix Gateway**.
4. Modifique los parámetros.
  - Nombre del almacén: El nombre de almacén que verá el usuario.
  - URL del almacén: La dirección URL del almacén.
  - #Store name: El nombre del almacén detrás de Citrix Gateway.
  - Habilitación del almacén: El estado del almacén (Habilitado o Inhabilitado).
  - Descripción del almacén: Una descripción del almacén.
5. Agregue o especifique la URL de Citrix Gateway. Introduzca el nombre de la dirección URL separada por punto y coma:

**Ejemplo:** `CitrixWorkspaceApp.exe STORE0= HRStore;https://ag.mycompany.com#Storename;On;Store`

Donde #Store name es el nombre del almacén detrás de Citrix Gateway.

En versiones anteriores, cuando se agregaba o eliminaba una cuenta mediante la directiva **Lista de cuentas de StoreFront/URL de Citrix Gateway** en el GPO, debía restablecer Citrix Receiver para que los cambios surtieran efecto.

A partir de la versión 1808, todos los cambios realizados en la directiva **Lista de cuentas de StoreFront/URL de Citrix Gateway** se aplican en una sesión cuando se reinicia la aplicación Citrix Workspace. No se requiere ningún restablecimiento.

**Nota:**

Restablecer la aplicación Citrix Workspace no es necesario en una nueva instalación de la aplicación Citrix Workspace 1808 y versiones posteriores. En caso de una actualización a 1808 y versiones posteriores, debe restablecer la aplicación Citrix Workspace para que los cambios surtan efecto.

**Limitaciones:**

- La URL de Citrix Gateway debe incluirse la primera, seguida de direcciones URL de StoreFront.
- No se admiten varias URL de Citrix Gateway.
- La URL de Citrix Gateway configurada con este método no admite el sitio de servicios de PNA detrás de Citrix Gateway.

**Administrar la reconexión del control del espacio de trabajo**

El control del espacio de trabajo permite que las aplicaciones sigan disponibles para los usuarios cuando estos cambian de dispositivo. Esto permite, por ejemplo, que los médicos, en los hospitales, se trasladen de una estación de trabajo a otra sin tener que reiniciar sus aplicaciones en cada dispositivo. En la aplicación Citrix Workspace, el control del espacio de trabajo en los dispositivos cliente se administra mediante la modificación del Registro. Esto también puede llevarse a cabo con Directivas de grupo en dispositivos que pertenecen a dominios.

**Precaución**

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Cree **WSCReconnectModeUser** y modifique la clave de Registro existente **WSCReconnectMode** en la imagen maestra de escritorio o en el servidor Citrix Virtual Apps. El escritorio publicado puede cambiar el comportamiento de la aplicación Citrix Workspace.

Parámetros posibles para la clave WSCReconnectMode de la aplicación Citrix Workspace:

- 0 = No reconectar ninguna sesión existente
- 1 = Reconectarse al iniciar una aplicación
- 2 = Reconectarse al actualizar una aplicación
- 3 = Reconectarse al iniciar o actualizar una aplicación
- 4 = Reconectarse cuando se abra la interfaz de Citrix Workspace
- 8 = Reconectarse al iniciar sesión en Windows
- 11 = Combinación de las opciones 3 y 8

**Inhabilitar el control del espacio de trabajo para la aplicación Citrix Workspace** Para inhabilitar el control del espacio de trabajo, cree la siguiente clave:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 bits)

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Dazzle (32 bits)

Nombre: **WSCReconnectModeUser**

Tipo: REG\_SZ

Información del valor: 0

Modifique la clave siguiente desde el valor predeterminado de 3 a cero

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 bits)

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Dazzle (32 bits)

Nombre: **WSCReconnectMode**

Tipo: REG\_SZ

Información del valor: 0

**Nota:**

Si lo prefiere, puede definir el valor REG\_SZ de WSCReconnectAll como “false” para no crear ninguna clave.

### **Cambiar el tiempo de espera del indicador de estado**

Puede cambiar el tiempo que se muestra el indicador de estado cuando el usuario inicia una sesión. Para cambiar el tiempo de espera, cree el valor REG\_DWORD SI INACTIVE MS en HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\. El valor REG\_DWORD puede establecerse en 4 si quiere que el indicador de estado desaparezca más pronto.

## Personalizar la ubicación del acceso directo de la aplicación mediante la línea de comandos

El modo de integración de accesos directos en el menú Inicio y en el escritorio solamente permite colocar los accesos directos de las aplicaciones publicadas en el menú **Inicio** de Windows y en el escritorio. No es necesario que los usuarios se suscriban a las aplicaciones desde la interfaz de usuario de Citrix Workspace. Administrar la integración de accesos directos en el menú Inicio y en el escritorio proporciona una experiencia de escritorio perfecta para grupos de usuarios, que necesitan acceder a un conjunto básico de aplicaciones de manera uniforme.

Como administrador de la aplicación Citrix Workspace, puede usar marcas de instalación en la línea de comandos, objetos de directiva de grupo, servicios de cuenta o parámetros de Registro para inhabilitar la interfaz habitual de “autoservicio” que ofrece la aplicación Citrix Workspace y sustituirla por un menú Inicio preconfigurado. Esta marca se denomina **SelfServiceMode** y está establecida como True de manera predeterminada. Cuando el administrador establece la marca **SelfServiceMode** en False, el usuario deja de tener acceso a la interfaz de usuario de autoservicio de la aplicación Citrix Workspace. En su lugar, el usuario puede acceder a las aplicaciones suscritas desde el menú Inicio y a través de accesos directos de escritorio, lo que aquí se conoce como “modo de acceso directo solamente”.

Los usuarios y los administradores pueden usar una serie de parámetros de Registro para personalizar el modo en que se configuran los accesos directos.

## Trabajar con accesos directos

- Los usuarios no pueden quitar las aplicaciones. Todas las aplicaciones son obligatorias cuando se trabaja con la marca **SelfServiceMode** establecida en False (modo de acceso directo solamente). Si el usuario quita un icono de acceso directo en el escritorio, el icono vuelve a aparecer cuando selecciona “Actualizar” en el icono de la aplicación Citrix Workspace situado en la bandeja del sistema.
- Los usuarios solo pueden configurar un almacén. Las opciones Cuenta y Preferencias no están disponibles. Esto es para evitar que el usuario pueda configurar más almacenes. El administrador puede dar a un usuario privilegios especiales para agregar más de una cuenta mediante la plantilla de objeto de directiva de grupo o al agregar manualmente una clave de Registro (HideEditStoresDialog) en la máquina cliente. Cuando el administrador da este privilegio a un usuario, el usuario tiene la opción Preferencias en el icono de la bandeja del sistema, desde donde puede agregar y quitar cuentas.
- Los usuarios no pueden quitar las aplicaciones mediante el **Panel de control** de Windows.
- Puede agregar accesos directos de escritorio a través de un parámetro de Registro personalizable. Los accesos directos de escritorio no se agregan de forma predeterminada. Después de realizar cualquier cambio en los parámetros del Registro, reinicie la aplicación Citrix Workspace.

- Los accesos directos se crean en el menú Inicio con una ruta de categoría predeterminada, Use-CategoryAsStartMenuPath.

**Nota:**

Windows 8, Windows 8.1 y Windows 10 no permiten la creación de carpetas anidadas dentro del menú Inicio. Las aplicaciones se muestran de forma individual o bajo la carpeta raíz, pero no en las subcarpetas de categorías definidas con Citrix Virtual Apps.

- Puede agregar una marca [/DESKTOPDIR="Dir\_name"] durante la instalación para reunir todos los accesos directos en una misma carpeta. Se admite el uso de CategoryPath para los accesos directos de escritorio.
- La reinstalación automática de aplicaciones modificadas es una función que se puede habilitar mediante la clave de Registro AutoReInstallModifiedApps. Cuando AutoReInstallModifiedApps está habilitada, los cambios que se hagan en los atributos de aplicaciones y escritorios publicados en el servidor se reflejarán en la máquina cliente. Cuando AutoReInstallModifiedApps está inhabilitada, los atributos de las aplicaciones y escritorios no se actualizan y los accesos directos no vuelven a aparecer al actualizar si han sido eliminados del cliente. De manera predeterminada, AutoReInstallModifiedApps está habilitada. Consulte "Usar claves del Registro para personalizar las ubicaciones de los accesos directos de las aplicaciones".

### **Personalizar la ubicación del acceso directo de la aplicación mediante el Editor del Registro**

**Nota:**

- De forma predeterminada, las claves del Registro usan un formato de cadena.
- Debe realizar cambios en las claves de Registro para configurar un almacén. Siempre que usted o un usuario quieran personalizar las claves de Registro, deben restablecer la aplicación Citrix Workspace, configurar las claves de Registro y luego reconfigurar el almacén.

### **Claves de Registro para máquinas de 32 bits:**

Registry key	Value	Key path
WSSupported	True	<ul style="list-style-type: none"> <li>HKEY_CURRENT_USER \ SOFTWARE \ Citrix \ Dazzle</li> <li>HKEY_CURRENT_USER \ SOFTWARE \ Citrix \ Receiver \ SR \ Store \ " + primaryStoreID + \ Properties</li> <li>HKEY_LOCAL_MACHINE \ SOFTWARE \ Policies \ Citrix \ Dazzle</li> <li>HKEY_LOCAL_MACHINE \ SOFTWARE \ Citrix \ Dazzle</li> </ul>
WSReconnectAll	True	<ul style="list-style-type: none"> <li>HKEY_CURRENT_USER \ SOFTWARE \ Citrix \ Dazzle</li> <li>HKEY_CURRENT_USER \ SOFTWARE \ Citrix \ Receiver \ SR \ Store \ " + primaryStoreID + \ Properties</li> <li>HKEY_LOCAL_MACHINE \ SOFTWARE \ Policies \ Citrix \ Dazzle</li> <li>HKEY_LOCAL_MACHINE \ SOFTWARE \ Citrix \ Dazzle</li> </ul>
WSReconnectMode	3	<ul style="list-style-type: none"> <li>HKEY_CURRENT_USER \ SOFTWARE \ Citrix \ Dazzle</li> <li>HKEY_CURRENT_USER \ SOFTWARE \ Citrix \ Receiver \ SR \ Store \ " + primaryStoreID + \ Properties</li> <li>HKLM \ SOFTWARE \ Policies \ Citrix \ Dazzle</li> <li>HKLM \ SOFTWARE \ Citrix \ Dazzle</li> </ul>
WSReconnectModeUser	Registry is not created during installation	<ul style="list-style-type: none"> <li>HKEY_CURRENT_USER \ SOFTWARE \ Citrix \ Dazzle</li> <li>HKEY_CURRENT_USER \ SOFTWARE \ Citrix \ Receiver \ SR \ Store \ " + primaryStoreID + \ Properties</li> <li>HKEY_LOCAL_MACHINE \ SOFTWARE \ Policies \ Citrix \ Dazzle</li> <li>HKEY_LOCAL_MACHINE \ SOFTWARE \ Citrix \ Dazzle</li> </ul>

**Claves de Registro para máquinas de 64 bits:**

Registry key	Value	Key path
WSSupported	True	<ul style="list-style-type: none"> <li>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle</li> <li>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Dazzle</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\</li> </ul>
WSSReconnectAll	True	<ul style="list-style-type: none"> <li>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle</li> <li>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Dazzle</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\</li> </ul>
WSSreconnectMode	3	<ul style="list-style-type: none"> <li>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle</li> <li>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store\"+ primaryStoreID +"\Properties</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle</li> </ul>
WSSReconnectModeUser	Registry is not created during installation.	<ul style="list-style-type: none"> <li>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle</li> <li>• HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store\"+ primaryStoreID+\Properties</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle</li> <li>• HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle</li> </ul>

**Cuentas de usuario**

Puede hacer lo siguiente para proporcionar a los usuarios la información de cuenta que necesitan para acceder a sus escritorios y aplicaciones virtuales:

- Configurar la detección de cuentas basada en direcciones de correo electrónico
- Archivo de aprovisionamiento
- Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente

### **Importante**

Citrix recomienda que reinicie la aplicación Citrix Workspace después de la instalación. El objetivo es garantizar que los usuarios puedan agregar cuentas, y la aplicación Citrix Workspace pueda detectar los dispositivos USB que estaban suspendidos durante la instalación.

Aparece un diálogo donde se indica que la instalación fue correcta, seguido de la pantalla **Agregar cuenta**. Para los usuarios nuevos, el diálogo **Agregar cuenta** requiere la introducción de una dirección de servidor o de correo electrónico para configurar una cuenta.

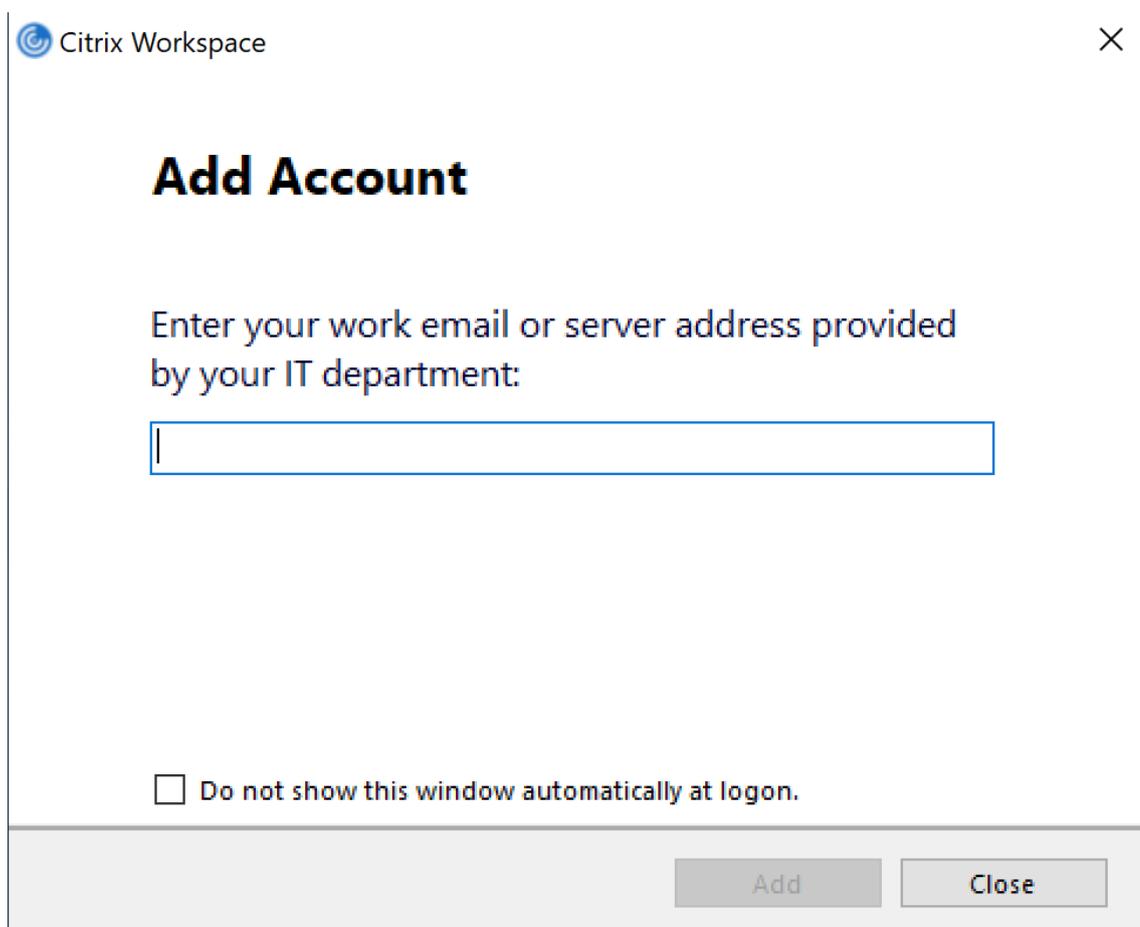
### **Quitar el cuadro de diálogo Agregar cuenta**

El cuadro de diálogo **Agregar cuenta** aparece cuando el almacén no está configurado. Desde el cuadro de diálogo **Agregar cuenta**, puede configurar una cuenta de la aplicación Citrix Workspace. Para ello, escriba una dirección de correo electrónico o una URL de servidor.

La aplicación Citrix Workspace determina el Citrix Gateway, el servidor de StoreFront o el dispositivo virtual App Controller asociado a la dirección de correo electrónico y pide al usuario que inicie sesión para la enumeración.

El cuadro de diálogo Agregar cuenta se puede suprimir de las siguientes formas:

1. **Durante el inicio de sesión del sistema**



Seleccione **No mostrar esta ventana automáticamente al iniciar la sesión** para evitar que la ventana **Agregar cuenta** aparezca como elemento emergente en el siguiente inicio de sesión. Esta es una configuración por usuario y se restablece durante el restablecimiento de la aplicación Citrix Workspace para Windows.

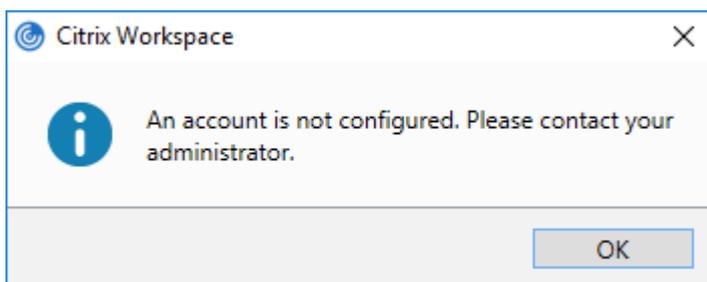
## 2. Instalar desde la línea de comandos

Instale la aplicación Citrix Workspace para Windows como administrador a partir de la interfaz de línea de comandos con el siguiente modificador de línea de comandos.

```
CitrixWorkspaceApp.exe /ALLOWADDSTORE=N
```

Este es un parámetro por máquina; por tanto, el comportamiento se aplicará a todos los usuarios.

Aparecerá el siguiente mensaje si el almacén no está configurado.



Además, el diálogo **Agregar cuenta** se puede quitar de las siguientes formas.

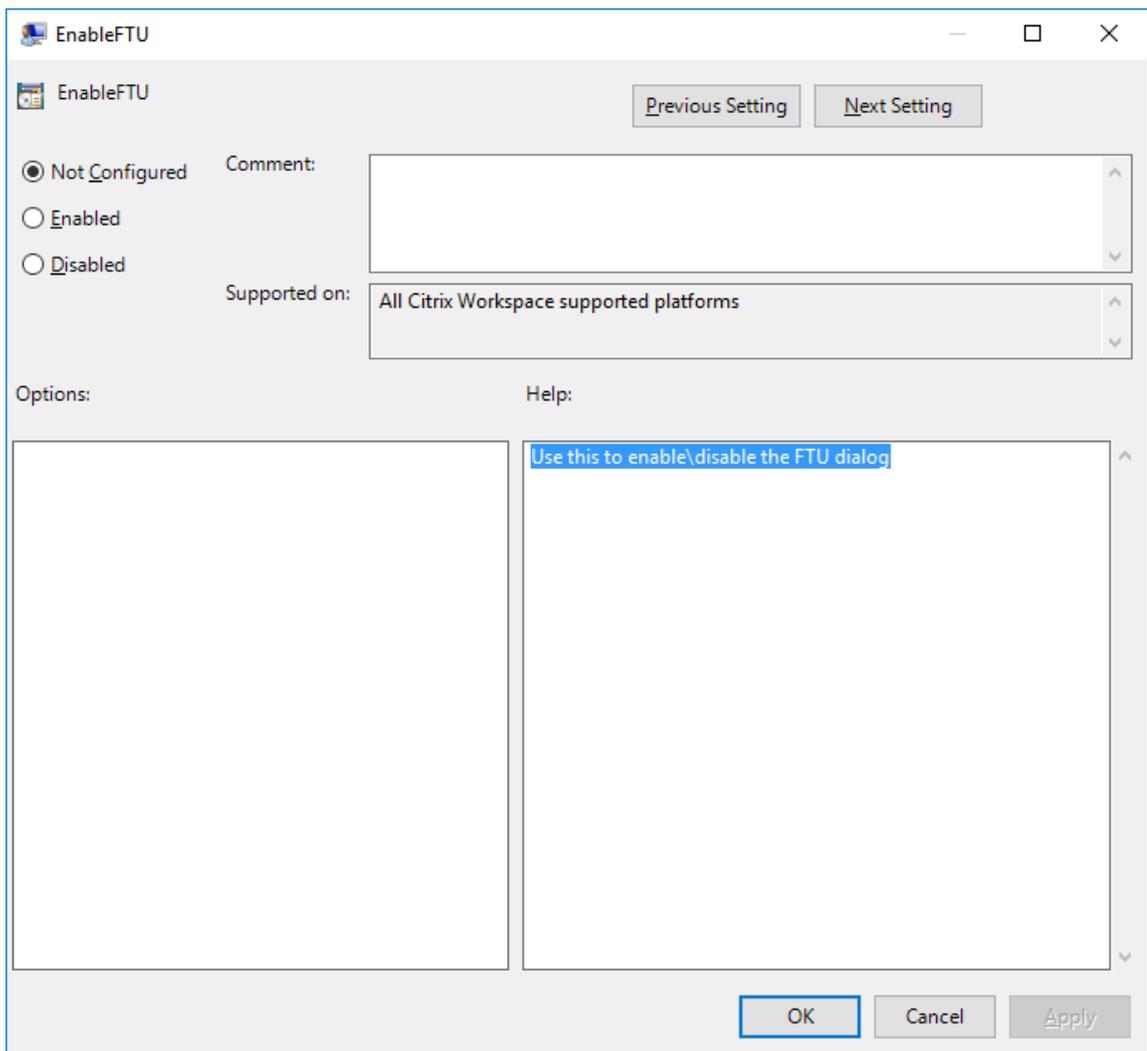
- **Cambiar el nombre del archivo de ejecución de Citrix:**

Cambie el nombre de **CitrixWorkspaceApp.exe** a **CitrixWorkspaceAppWeb.exe** para modificar el comportamiento del cuadro de diálogo **Agregar cuenta**. Al cambiar el nombre del archivo, el diálogo **Agregar cuenta** no aparece en el menú Inicio.

- **Plantilla administrativa de GPO:**

Para ocultar la opción **Agregar cuenta** en el asistente de instalación de la aplicación Citrix Workspace, inhabilite **EnableFTUpolicy** en el nodo Autoservicio de la plantilla administrativa de GPO, como se muestra a continuación.

Como este es un parámetro por máquina, el comportamiento se aplica a todos los usuarios.



### Configurar la detección de cuentas basada en direcciones de correo electrónico

Cuando se configura la aplicación Citrix Workspace para la detección de cuentas basada en direcciones de correo electrónico, los usuarios introducen su dirección de correo electrónico (en lugar de una dirección URL de servidor) durante la instalación y configuración inicial de la aplicación Citrix Workspace. La aplicación Citrix Workspace determina el dispositivo Citrix Gateway o el servidor de StoreFront que está asociado a esa dirección de correo electrónico en función de los registros de servicio (SRV) del sistema de nombres de dominio (DNS). Tras ello, solicita al usuario que inicie sesión para acceder a sus aplicaciones y escritorios virtuales.

**Nota:**

La detección de cuentas basada en correo electrónico no se admite en implementaciones con la Interfaz Web.

Para obtener más información sobre cómo configurar la detección de cuentas basada en direcciones

de correo electrónico, consulte [Global App Configuration Service](#).

### **Proporcionar archivos de aprovisionamiento a los usuarios**

StoreFront proporciona los archivos de aprovisionamiento que los usuarios pueden abrir para conectar con almacenes.

Es posible utilizar StoreFront para crear archivos de aprovisionamiento que contengan los detalles de conexión de las cuentas. Estos archivos se ponen a disposición de los usuarios para que puedan configurar automáticamente la aplicación Citrix Workspace. Después de instalar la aplicación Citrix Workspace, los usuarios no tienen más que abrir el archivo para configurarla. Si configura sitios de Workspace para Web, los usuarios también podrán obtener los archivos de aprovisionamiento para la aplicación Citrix Workspace desde esos sitios.

Para obtener más información, consulte [Para exportar archivos de aprovisionamiento del almacén para los usuarios](#) en la documentación de StoreFront.

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

Para permitir que los usuarios configuren sus cuentas manualmente, distribúyales la información que necesitan para conectarse con sus escritorios y aplicaciones virtuales.

- Para las conexiones con un almacén de StoreFront, proporcione la dirección URL de ese servidor. Por ejemplo: `https://servername.company.com`.  
Para implementaciones con interfaz web, proporcione la dirección URL del sitio de Citrix DaaS.
- Para conexiones a través de Citrix Gateway, primero determine si el usuario necesita ver todos los almacenes configurados o solo el almacén que tiene habilitado el acceso remoto para un dispositivo Citrix Gateway concreto.
  - Para presentarles todos los almacenes configurados, proporcione a sus usuarios el nombre de dominio completo de Citrix Gateway.
  - Para limitar el acceso a un almacén en concreto, proporcione a sus usuarios el nombre de dominio completo de Citrix Gateway y el nombre del almacén, con el formato:

#### **CitrixGatewayFQDN?MyStoreName:**

Por ejemplo, si tiene un almacén llamado “AplicacionesVentas” con acceso remoto habilitado para servidor1.com, y un almacén llamado “AplicacionesRRHH” con acceso remoto habilitado para servidor2.com, el usuario deberá introducir `servidor1.com?AplicacionesVentas` si quiere acceder a AplicacionesVentas, o introducir `servidor2.com?AplicacionesRRHH` si quiere acceder a AplicacionesRRHH. Esta función requiere que un nuevo usuario cree una cuenta introduciendo una dirección URL y no está disponible para detección basada en direcciones de correo electrónico.

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

Para administrar las cuentas, abra la página de inicio de la aplicación Citrix Workspace, haga clic en el  y luego haga clic en **Cuentas**.

## Compartir automáticamente varias cuentas de almacén

### Advertencia

El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden hacer necesaria la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Si dispone de más de una cuenta de almacén, puede configurar la aplicación Citrix Workspace para Windows para que se conecte automáticamente a todas las cuentas al establecer una sesión. Para ver automáticamente todas las cuentas tras abrir la aplicación Citrix Workspace:

### En sistemas de 32 bits, cree la clave “CurrentAccount”:

Ubicación: HKEY\_LOCAL\_MACHINE\Software\Citrix\Dazzle

Nombre de la clave: CurrentAccount

Valor: AllAccount

Tipo: REG\_SZ

### En sistemas de 64 bits, cree la clave “CurrentAccount”:

Ubicación: HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Citrix\Dazzle

Nombre de la clave: CurrentAccount

Valor: AllAccount

Tipo: REG\_SZ

## Asignación de unidades del cliente

La aplicación Citrix Workspace para Windows admite la asignación de dispositivos en los dispositivos de usuario de manera que estén disponibles desde una sesión. Los usuarios pueden:

- Tener acceso imperceptible a las unidades locales, impresoras y puertos COM.
- Cortar y pegar entre sesiones y el portapapeles de Windows local.

- Escuchar sonido (sonidos del sistema y archivos WAV) reproducido en la sesión.

Durante el inicio de sesión, la aplicación Citrix Workspace informa al servidor sobre las unidades cliente, los puertos COM y los puertos LPT disponibles. De forma predeterminada, a las unidades del cliente se les asignan letras de unidad del servidor y se crean colas de impresión de servidor para impresoras cliente de manera que parezca que están directamente conectadas a la sesión. Estas asignaciones están disponibles solamente para el usuario durante la sesión actual. Se las elimina cuando el usuario cierra la sesión y se vuelven a crear la próxima vez que el usuario inicia una sesión.

Puede usar las configuraciones de directiva de redirección de Citrix para asignar los dispositivos de usuario que no se hayan asignado automáticamente al iniciar la sesión. Para obtener más información, consulte la documentación de Citrix Virtual Apps and Desktops.

### **Desactivar asignaciones de dispositivos de usuario**

Es posible configurar las opciones de asignación de dispositivos de usuario para controladores, impresoras y puertos con la herramienta **Administrador del servidor de Windows**. Para obtener más información sobre las opciones disponibles, consulte la documentación de Servicios de Escritorio remoto.

### **Redirigir carpetas del cliente**

La redirección de carpetas del cliente cambia el modo en que los archivos del lado del cliente son accesibles desde la sesión en el host. Cuando se habilita solo la asignación de unidades del cliente en el servidor, se asignan automáticamente volúmenes completos del cliente a las sesiones como enlaces UNC (Universal Naming Convention). Cuando se habilita la redirección de carpetas del cliente en el servidor y, a continuación, el usuario lo configura en el dispositivo de usuario, solo se redirige la parte del volumen local que especifique el usuario.

Solo las carpetas especificadas por el usuario aparecerán como enlaces UNC dentro de las sesiones, en lugar de aparecer todo el sistema de archivos del dispositivo del usuario. Si se inhabilitan los enlaces UNC mediante el Registro, las carpetas del cliente aparecen como unidades asignadas dentro de la sesión. Para obtener más información y conocer cómo configurar la redirección de carpetas del cliente para los dispositivos de usuario, consulte la documentación de Citrix Virtual Apps and Desktops.

### **Asignar unidades del cliente a letras de unidad del host**

La asignación de unidades del cliente permite redirigir letras de unidad del host a unidades existentes en el dispositivo del usuario. Por ejemplo, la unidad H de una sesión de usuario Citrix se puede asignar a la unidad C del dispositivo del usuario que ejecuta la aplicación Citrix Workspace para Windows.

La asignación de unidades del cliente está incorporada de forma imperceptible en las funciones estándar de redirección de dispositivos de Citrix. Para el Administrador de archivos, el Explorador de Windows y sus aplicaciones se ven como cualquier otra asignación de red.

El servidor que aloja las aplicaciones y los escritorios virtuales se puede configurar durante la instalación para que asigne unidades del cliente automáticamente a un grupo determinado de letras de unidad. La instalación predeterminada asigna letras de unidad a las unidades del cliente comenzando por la V y letras subsiguientes en orden descendente, asignando una letra de unidad a cada unidad de disco fija y de CD-ROM (a las unidades de disquete se les asignan las letras de unidad existentes). Este método da como resultado las siguientes asignaciones de unidad en la sesión:

---

Letra de unidad del cliente	El servidor accede a ella como
A	A
B	B
C	V
D	U

---

El servidor se puede configurar para que sus respectivas letras de unidad no entren en conflicto con las del cliente; en este caso, las letras de unidad del servidor se cambian por otras posteriores en orden alfabético. Por ejemplo, si se cambian las unidades C y D del servidor por M y N, respectivamente, los equipos cliente pueden acceder a sus unidades C y D directamente. Este método proporciona las siguientes asignaciones de unidad en una sesión:

---

Letra de unidad del cliente	El servidor accede a ella como
A	A
B	B
C	C
D	D

---

La letra de unidad utilizada para sustituir la unidad C del servidor se define durante la configuración. El resto de las letras de unidad de disco duro y de CD-ROM se sustituyen por letras de unidad secuenciales (por ejemplo; C > M, D > N, E > O). Estas letras de unidad no deben entrar en conflicto con otras asignaciones de unidad de red existentes. Si a una unidad de red se le asigna la misma letra de unidad que la de un servidor, la asignación de unidad de red no será válida.

Cuando un dispositivo cliente se conecta con un servidor, se restablecen las asignaciones del cliente a menos que la asignación automática de dispositivos del cliente esté inhabilitada. La asignación de

unidades del cliente está habilitada de forma predeterminada. Para cambiar esta configuración, use la herramienta de Configuración de Servicios de Escritorio remoto (Servicios de Terminal Server). Es también posible usar directivas para tener mayor control sobre cómo se aplica la asignación de dispositivos del cliente. Para obtener más información sobre las directivas, consulte la documentación de Citrix Virtual Apps and Desktops.

### **Redirigir dispositivos USB de HDX Plug and Play**

La redirección de dispositivos USB de HDX Plug-n-Play permite la redirección dinámica de varios dispositivos, incluyendo cámaras, escáneres, reproductores multimedia y dispositivos de punto de venta (POS) al servidor. Al mismo tiempo, se puede impedir la redirección de todos o algunos dispositivos. Modifique las directivas en el servidor o aplique directivas de grupo en el dispositivo de usuario para configurar los parámetros de la redirección. Para obtener más información, consulte [Consideraciones sobre unidades del cliente y USB](#) en la documentación de Citrix Virtual Apps and Desktops.

#### **Importante**

Si se prohíbe la redirección de dispositivos USB Plug-n-Play en una directiva de servidor, el usuario no podrá anular dicha configuración de directiva.

Un usuario puede definir permisos en la aplicación Citrix Workspace para permitir o rechazar siempre la redirección de dispositivos, o bien para que se le pregunte cada vez que se conecta un dispositivo. El parámetro solo afecta a los dispositivos que se conectan después de que el usuario cambia el parámetro.

### **Para asignar un puerto COM del cliente a un puerto COM del servidor:**

La asignación de puertos COM del cliente permite utilizar los dispositivos conectados a los puertos COM del dispositivo de usuario durante las sesiones. Estas asignaciones se pueden utilizar de la misma forma que cualquier otra asignación de red.

Es posible asignar puertos COM de cliente desde una interfaz de comandos. También se puede controlar la asignación de puertos COM de cliente desde la herramienta Configuración de Escritorio remoto (Servicios de Terminal Server) o a través de directivas. Para obtener información sobre las directivas, consulte la documentación de Citrix Virtual Apps and Desktops.

#### **Importante**

La asignación de puertos COM no es compatible con TAPI.

1. En implementaciones de Citrix Virtual Apps and Desktops, habilite la configuración de directiva Redirección de puertos COM del cliente.
2. Inicie sesión en la aplicación Citrix Workspace.

3. Escriba lo siguiente en una interfaz de comandos:

```
net use comx: \\client\comz:
```

donde x es el número del puerto COM en el servidor (los puertos del 1 al 9 están disponibles para ser asignados) y z es el número del puerto COM del cliente que se quiere asignar.

4. Para confirmar la operación, escriba:

```
net use
```

en la interfaz de comandos. Aparecerá la lista de las unidades, puertos LPT y puertos COM asignados.

Para utilizar este puerto COM en una sesión de aplicación o escritorio virtual, instale el dispositivo con el nombre asignado. Por ejemplo, si asigna COM1 en el cliente a COM5 en el servidor, instale el dispositivo de puerto COM en COM5 durante la sesión. Utilice este puerto COM asignado del mismo modo que lo haría con un puerto COM del dispositivo del usuario.

## Resolución de nombres DNS

Puede configurar la aplicación Citrix Workspace para Windows de modo que use Citrix XML Service para solicitar un nombre DNS de un servidor en lugar de una dirección IP.

### Importante:

A menos que el entorno DNS esté configurado específicamente para utilizar esta función, Citrix recomienda no habilitar la resolución de nombres DNS en la comunidad de servidores.

La aplicación Citrix Workspace que se conecta a aplicaciones publicadas a través de la Interfaz Web también usa Citrix XML Service. Para la aplicación Citrix Workspace que se conecta a través de la Interfaz Web, el servidor web resuelve el nombre DNS en nombre de la aplicación Citrix Workspace.

De forma predeterminada, la resolución de nombres DNS está inhabilitada en el servidor y habilitada en la aplicación Citrix Workspace. Cuando la resolución de nombres DNS está inhabilitada en el servidor, todas las solicitudes de la aplicación Citrix Workspace de un nombre DNS devuelven una dirección IP. No es necesario desactivar la resolución de nombres DNS en la aplicación Citrix Workspace.

### Para inhabilitar la resolución de nombres DNS para dispositivos cliente específicos:

Si su implementación de servidores usa DNS para la resolución de nombres y tiene problemas con algunos dispositivos de usuario, puede inhabilitar la resolución de nombres DNS para esos dispositivos.

### Precaución

El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden hacer necesaria la reinstalación del sistema operativo. Citrix no puede garantizar que los proble-

mas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. Agregue una cadena de clave de Registro **xmlAddressResolutionType** a `HKEY\LOCAL_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing`.
2. El valor debe ser **IPv4-Port**.
3. Repita el proceso para cada usuario de los dispositivos de usuario.

## Configurar

May 23, 2024

### App Protection

#### Renuncia de responsabilidades

Las directivas de App Protection funcionan mediante el filtrado del acceso a las funciones requeridas del sistema operativo subyacente (llamadas a API específicas necesarias para capturar pantallas o pulsaciones de teclas). Esto significa que las directivas de App Protection pueden proporcionar protección incluso contra herramientas de piratas informáticos personalizadas y con un diseño específico. Sin embargo, a medida que los sistemas operativos evolucionan, pueden surgir nuevas formas de capturar pantallas y registrar pulsaciones de teclas. Si bien seguimos identificándolas y abordándolas, no podemos garantizar una protección completa en configuraciones e implementaciones específicas.

App Protection es una función complementaria que proporciona una mayor seguridad al usar Citrix Virtual Apps and Desktops y Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service). 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. App Protection 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.

App Protection requiere instalar una licencia adicional en el servidor de licencias. También debe haber presente una licencia de Citrix Virtual Desktops. Para obtener información sobre las licencias, consulte la sección [Configurar](#) de la documentación de App Protection.

#### Requisitos:

- Citrix Virtual Apps and Desktops 1912 o versiones posteriores.
- StoreFront 1912.
- Aplicación Citrix Workspace 1912 o versiones posteriores.

#### **Requisitos previos:**

- La función de App Protection debe estar habilitada en el Controller. Para obtener más información, consulte la documentación de [App Protection](#).

Puede incluir el componente de App Protection con la aplicación Citrix Workspace en una de estas dos situaciones:

- Durante la instalación de la aplicación Citrix Workspace mediante una interfaz de línea de comandos o una interfaz gráfica de usuario. O BIEN:
- Durante el inicio de una aplicación (instalación a demanda).

#### **Nota:**

- Esta función solo se admite en sistemas operativos de escritorio de Microsoft Windows, como Windows 10, Windows 8.1 y Windows 7.
- Esta función no es compatible con el Protocolo de escritorio remoto (RDP).

#### **Protección de sesiones HDX locales:**

Dos directivas proporcionan funciones contra el registro de tecleo y las capturas de pantalla en las sesiones. Estas directivas deben configurarse a través de PowerShell. No hay ninguna interfaz gráfica de usuario disponible para este propósito.

#### **Nota:**

Citrix DaaS no ofrece la función de App Protection.

Para obtener información sobre la configuración de App Protection en Citrix Virtual Apps and Desktops, consulte la documentación de [App Protection](#).

#### **App Protection: Configuración en la aplicación Citrix Workspace**

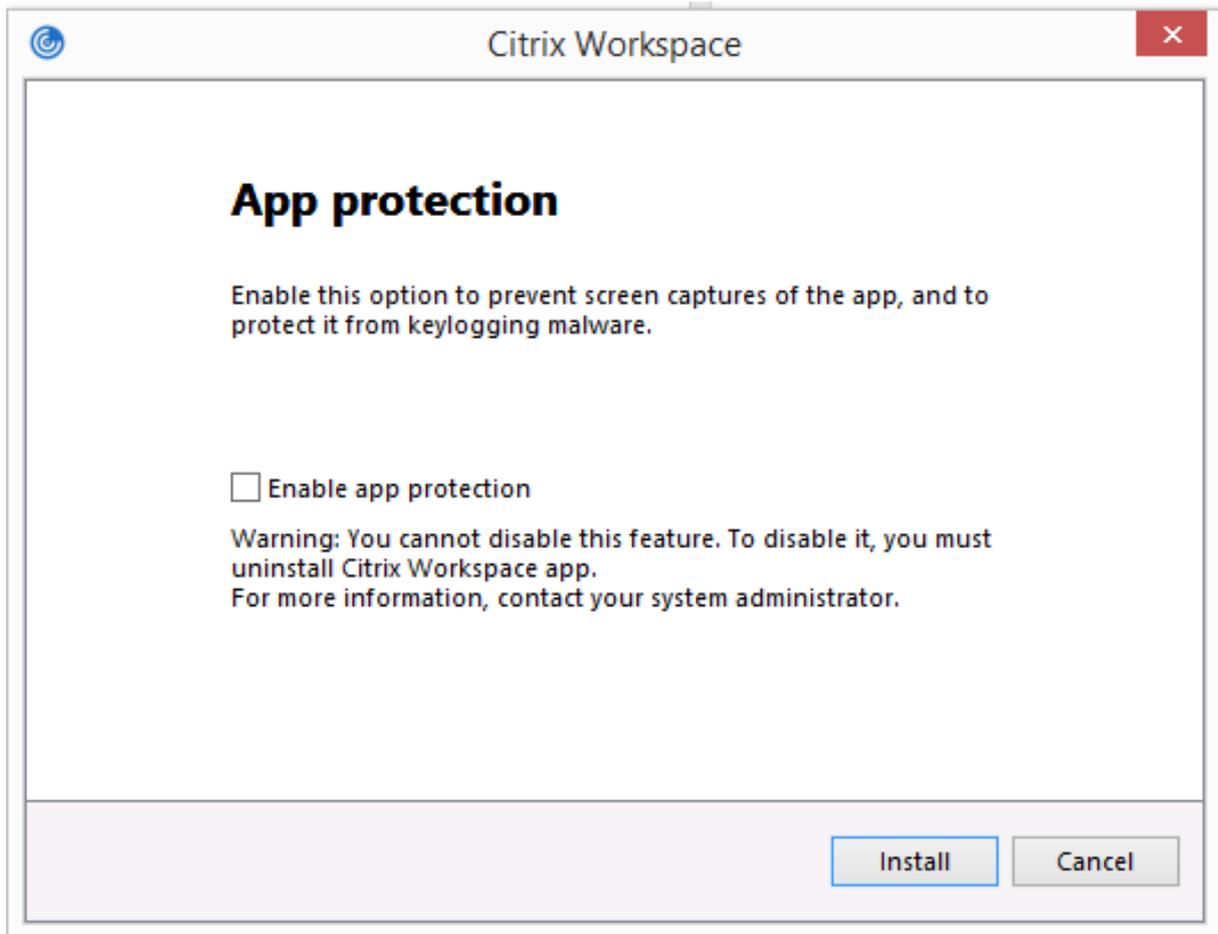
#### **Nota:**

- Incluya el componente de App Protection con la aplicación Citrix Workspace solo si el administrador le ha indicado que lo haga.
- Es posible que el componente de App Protection afecte a las prestaciones de captura de pantalla del dispositivo.

Durante la instalación de la aplicación Citrix Workspace, puede incluir App Protection mediante uno de estos métodos:

- Interfaz gráfica de usuario
- Interfaz de línea de comandos

**Interfaz gráfica de usuario** Durante la instalación de la aplicación Citrix Workspace, utilice este cuadro de diálogo para incluir el componente de App Protection. Seleccione **Habilitar App Protection** y, a continuación, haga clic en **Instalar** para continuar con la instalación.



**Nota:**

Si no se habilita App Protection durante la instalación, aparecerá un mensaje al iniciar una aplicación protegida. Siga las instrucciones del mensaje para instalar el componente de App Protection.

**Interfaz de línea de comandos** Utilice el modificador de línea de comandos `/includeappprotection` durante la instalación de la aplicación Citrix Workspace para agregar el componente de App Protection.

La tabla siguiente proporciona información sobre las pantallas protegidas en función de la implementación:

Implementación de App Protection	Pantallas protegidas	Pantallas no protegidas
Se incluye en la aplicación Citrix Workspace	Cuadro de diálogo de credenciales de usuario / administrador de autenticación y Self-Service Plug-in	Central de conexiones, Dispositivos, cualquier mensaje de error de la aplicación Citrix Workspace, Reconexión automática de clientes, Agregar cuenta
Se ha configurado en el Controller	Pantalla de sesión ICA (tanto aplicaciones como escritorios)	Central de conexiones, Dispositivos, cualquier mensaje de error de la aplicación Citrix Workspace, Reconexión automática de clientes, Agregar cuenta

### Comportamiento previsto:

El comportamiento previsto depende del método por el cual los usuarios acceden al almacén de StoreFront que contiene recursos protegidos.

#### Nota:

- Citrix recomienda que utilice la aplicación Citrix Workspace nativa únicamente para iniciar sesiones protegidas.

- **Comportamiento en Workspace para Web:**

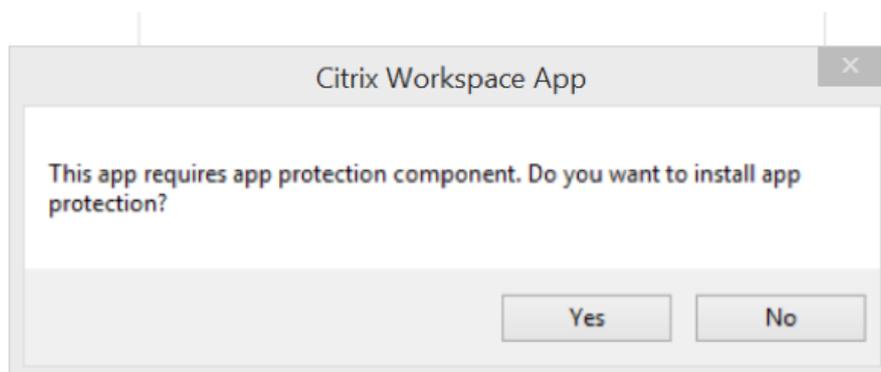
El componente de App Protection no se admite en las configuraciones de Workspace para Web. Las aplicaciones protegidas por directivas de App Protection no se indican. Para obtener más información acerca de los recursos asignados, póngase en contacto con el administrador del sistema.

- **Comportamiento de las versiones de la aplicación Citrix Workspace que no ofrecen App Protection:**

En la versión 1911 de la aplicación Citrix Workspace y en versiones anteriores, las aplicaciones protegidas por directivas de App Protection no se indican en StoreFront.

- **Comportamiento de las aplicaciones que tienen configurada la función de App Protection en el Controller:**

Si la protección de la aplicación está configurada en el Controller y usted intenta iniciar una aplicación protegida, App Protection se instala a demanda. Aparece el siguiente cuadro de diálogo:



Después de hacer clic en **Sí**, se instala el componente de App Protection y el usuario puede iniciar la aplicación protegida.

- **Comportamiento de la sesión protegida con el protocolo RDP**

- La sesión protegida activa se desconecta si se inicia una sesión de protocolo RDP.
- No puede iniciar sesiones protegidas en sesiones con Protocolo de escritorio remoto (RDP).

#### **Registros de errores de App Protection:**

Los registros del componente de App Protection se guardan en el archivo de depuración generado. Para recopilar estos registros, haga lo siguiente:

1. Descargue la aplicación [DebugView](#) del sitio web de Microsoft e instálela.
2. Inicie el símbolo del sistema y ejecute este comando:

```
Dbgview.exe /t /k /v /l C:\logs.txt
```

En el ejemplo anterior, puede ver los registros en el archivo log.txt.

El comando indica lo siguiente:

- `/t`: La aplicación DebugView se inicia minimizada en el área de notificaciones.
- `/k`: Habilita la captura de kernel.
- `/v`: Habilita la captura detallada de kernel.
- `/l`: Registra los datos de salida en un archivo específico.

#### **Desinstalar el componente de App Protection:**

Para desinstalar el componente de App Protection, debe desinstalar la aplicación Citrix Workspace del sistema. Reinicie el sistema para que los cambios surtan efecto.

**Nota:**

App Protection solo se ofrece en la actualización que hay a partir de la versión 1912.

**Problemas conocidos y limitaciones:**

- La función no está disponible en los sistemas operativos de Microsoft Server, como Windows Server 2012 R2 y Windows Server 2016.
- Para realizar una captura de pantalla del dispositivo local, se deben minimizar las ventanas relacionadas con la aplicación Citrix Workspace. De lo contrario, no podrá realizar capturas de pantalla de su dispositivo local.
- Esta función no está disponible en casos de doble salto.
- Para que esta función opere correctamente, inhabilite la directiva **Redirección del portapapeles del cliente** del VDA.

**Estimador de rendimiento del codificador de dispositivos de punto final en Microsoft Teams**

Cuando se inicia el proceso HdxTeams.exe (el motor de medios WebRTC incluido en la aplicación Citrix Workspace que controla la redirección de Microsoft Teams), se calcula la mejor resolución de codificación que puede acomodar la CPU del dispositivo del punto final sin sobrecargarse. Los valores posibles son: 240p, 360p, 720p y 1080p.

El proceso de estimación del rendimiento (también llamado `webrtcapi.EndpointPerformance`) se ejecuta cuando se inicializa HdxTeams.exe. El código de macrobloque determina la mejor resolución que se puede lograr en ese dispositivo de punto final en cuestión. A continuación, se incluye la resolución más alta posible durante la negociación del códec entre los pares o entre el par y el servidor de conferencias.

Existen cuatro categorías de rendimiento para los dispositivos de punto final que tienen su propia resolución máxima disponible:

Rendimiento del dispositivo de punto final	Resolución máxima	Valor de clave del Registro
rápido	1080p	3
medio	720p	2
lento	360p	1
muy lento	240p	0

Hay indicadores de configuración para inhabilitar el códec VP9 o H264.

El códec H264 es más ligero en la CPU, pero consume más ancho de banda. En cambio, el códec VP9 consume más potencia de CPU, pero menos ancho de banda.

#### **Ruta al Registro en la aplicación Citrix Workspace:**

Vaya a la ruta del Registro HKEY\_CURRENT\_USER\SOFTWARE\Citrix\HDXMediaStream y cree las siguientes claves:\

---

Nombre	Tipo	Valores	Descripción
DisableVP9	DWORD	1; 0	1: Inhabilitar el códec VP9. 0: Habilitarlo.
DisableH264	DWORD	1;0	1: Inhabilitar el códec H.264. 0: Habilitarlo.
OverridePerformance	DWORD	0;1;2;3	Fuerza el rendimiento deseado. El valor debe estar en el rango entre 0 y 3, donde 0 indica muy lento y 3 muy rápido.

---

Para obtener más información sobre la optimización de Microsoft Teams, consulte [Optimización para Microsoft Teams](#).

### **Transporte adaptable**

El transporte adaptable es un mecanismo de transporte de datos para Citrix Virtual Apps and Desktops y Citrix DaaS. Es más rápido y escalable, mejora la interactividad de las aplicaciones y es más interactivo en conexiones de Internet y WAN difíciles de largo recorrido. El transporte adaptable mantiene la alta escalabilidad de servidores y un uso eficiente del ancho de banda. Al usar el transporte adaptable, los canales virtuales ICA responden automáticamente a las cambiantes condiciones de red. Cambian de forma inteligente el protocolo subyacente entre el protocolo de Citrix (denominado Enlightened Data Transport o EDT) y TCP para conseguir el mejor rendimiento. Mejora el rendimiento de datos en todos los canales virtuales ICA, incluida la tecnología de pantallas remotas Thinwire, la transferencia de archivos (asignación de unidades del cliente), la impresión y la redirección multimedia. Se aplica la misma configuración a las condiciones de WAN y LAN.

En versiones anteriores, cuando **HDXoverUDP** se establece en **Preferido**, los datos se transportan por EDT siempre que sea posible (cuando no sea posible, se recurre a TCP).

Cuando se habilita la fiabilidad de la sesión, EDT y TCP intentan conectarse en paralelo, reconexión de la fiabilidad de la sesión y 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 usar EDT cada cinco minutos.

**Requisitos:**

- Citrix Virtual Apps and Desktops 7.12 o una versión más reciente.
- StoreFront 3.8.
- Solo agentes VDA IPv4. No se admiten configuraciones de IPv6 ni mixtas (de IPv4 e IPv6).
- Agregue reglas de firewall para permitir el tráfico entrante en los puertos UDP 1494 y 2598 del VDA.

**Nota:**

Los puertos TCP 1494 y 2598 son necesarios y se abren automáticamente cuando se instala el VDA. Sin embargo, los puertos UDP 1494 y 2598 no se abren automáticamente. Debe **habilitarlos**.

La aplicación Citrix Workspace permite el transporte adaptable de forma predeterminada. También de forma predeterminada, el cliente intenta utilizar el transporte adaptable solo si el VDA está configurado como **Preferido** en el Delivery Controller y si la configuración se ha aplicado en el VDA.

Puede habilitar el transporte adaptable mediante la configuración de directiva **Transporte adaptable HDX**. Establezca la nueva configuración de directiva con el valor **Preferido** si quiere usar el transporte adaptable cuando sea posible, y usar TCP como alternativa.

Utilice la plantilla administrativa de objeto de directiva de grupo (GPO) para inhabilitar el transporte adaptable en el cliente.

**Para configurar el transporte adaptable mediante la plantilla administrativa de GPO de Citrix Workspace**

A continuación, se describen pasos de configuración opcionales para personalizar el entorno. Por ejemplo, puede optar por inhabilitar la función para un determinado cliente por motivos de seguridad.

**Nota:**

De forma predeterminada, el transporte adaptable está inhabilitado y se usa siempre TCP.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Workspace > Redirección de red**.

3. **Habilite** la directiva **Protocolo de transporte para Citrix Workspace**.
4. Seleccione el **protocolo de comunicación para la aplicación Citrix Workspace** como convenga.
  - **Desactivado:** Se usará TCP para la transferencia de datos.
  - **Preferido:** Indica que el cliente intenta conectarse al servidor mediante UDP al principio. Si UDP no está disponible, la conexión cambia a TCP como alternativa.
  - **Activado:** La aplicación Citrix Workspace para Windows se conecta con el servidor solo mediante el protocolo UDP. Con esta opción, no existe la alternativa de recurrir a TCP.
5. Haga clic en **Aplicar** y **Aceptar**.
6. Desde la línea de comandos, ejecute el comando `gpupdate /force`.

Para utilizar el transporte adaptable, agregue los archivos de plantilla de la aplicación Citrix Workspace a la carpeta de **definiciones de directivas**. Para obtener información sobre cómo agregar los archivos de plantilla al GPO local, consulte la sección [Plantilla de objeto de directiva de grupo](#).

Para confirmar que la configuración de directiva surte efecto:

Vaya a `HKEY\LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT` y verifique que la clave **HDXOverUDP** está incluida.

Para obtener más información, consulte la sección [Transporte adaptable](#) en la documentación de Citrix Virtual Apps and Desktops.

## Hoja de Preferencias avanzadas

Puede personalizar la disponibilidad y el contenido de la hoja **Preferencias avanzadas** que figura en el menú contextual del icono de la aplicación Citrix Workspace en el área de notificaciones. Al personalizar, se garantiza que los usuarios puedan aplicar solo los parámetros especificados por el administrador en sus sistemas. Específicamente, puede:

- Ocultar la hoja entera de Preferencias avanzadas
- Ocultar los parámetros siguientes:
  - Recopilación de datos
  - Central de conexiones
  - Configuration Checker
  - Barra de idioma y teclado
  - PPP elevados
  - Información de asistencia
  - Accesos directos y reconexión
  - Citrix Casting

### Ocultar la opción **Preferencias avanzadas** en el menú contextual

Puede ocultar la hoja “Preferencias avanzadas” mediante la plantilla administrativa de objetos de directiva de grupo (GPO) de la aplicación Citrix Workspace:

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Workspace > Autoservicio > Opciones de Preferencias avanzadas**.
3. Seleccione la directiva **Inhabilitar Preferencias avanzadas**.
4. Seleccione **Habilitada** para ocultar la opción “Preferencias avanzadas” en el menú contextual del icono de la aplicación Citrix Workspace en el área de notificaciones.

**Nota:**

De forma predeterminada, está seleccionada la opción **No configurada**.

### Ocultar configuraciones específicas de la hoja **Preferencias avanzadas** mediante la plantilla administrativa de GPO

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Workspace > Autoservicio > Opciones de Preferencias avanzadas**.
3. Seleccione la directiva para el parámetro que quiere ocultar.

La tabla siguiente contiene las opciones que puede seleccionar y el efecto de cada una:

Opciones	Acción
No configurado	Muestra el parámetro
Habilitado	Oculto el parámetro
Inhabilitado	Muestra el parámetro

Puede ocultar los siguientes parámetros concretos en la hoja de Preferencias avanzadas:

- Configuration Checker
- Central de conexiones
- PPP elevados
- Recopilación de datos
- Eliminar contraseñas guardadas

- Barra de idioma y teclado
- Accesos directos y reconexión
- Información de asistencia
- Citrix Casting

### **Ocultar la opción de Restablecer Workspace en la hoja de Preferencias avanzadas mediante el Editor del Registro**

Puede ocultar opción **Restablecer Workspace** en la hoja “Preferencias avanzadas” solamente mediante el Editor del Registro.

1. Abra el Editor del Registro.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`.
3. Cree una clave de valor de cadena **EnableFactoryReset** y configúrela con cualquiera de las siguientes opciones:
  - True: Muestra la opción “Restablecer Workspace” en la hoja “Preferencias avanzadas”
  - False: Oculta la opción “Restablecer Workspace” en la hoja “Preferencias avanzadas”

### **Ocultar la opción de Actualizaciones de Citrix Workspace en la hoja de Preferencias avanzadas**

#### **Nota:**

La ruta de la directiva para la opción “Actualizaciones de Citrix Workspace” es diferente de la de otras opciones presentes en la hoja “Preferencias avanzadas”.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Actualizaciones de Citrix Workspace**.
3. Seleccione la directiva **Actualizaciones de Citrix Workspace**.
4. Seleccione **Inhabilitada** para ocultar los parámetros de las actualizaciones de Citrix Workspace en la hoja **Preferencias avanzadas**.

### **Entrega de aplicaciones**

Cuando entregue aplicaciones con Citrix Virtual Apps and Desktops y Citrix DaaS, tenga en cuenta las siguientes opciones para mejorar la experiencia de los usuarios:

- Modo de acceso web: Sin configuración necesaria, la aplicación Citrix Workspace ofrece acceso web a las aplicaciones y los escritorios. Puede ir a un sitio de Workspace para Web o un sitio de

la Interfaz Web para seleccionar y usar las aplicaciones que quiera. En este modo, no se colocan accesos directos en el escritorio del usuario.

- **Modo de autoservicio:** Cuando agrega una cuenta de StoreFront a la aplicación Citrix Workspace o configura esta aplicación para que apunte a un sitio web de StoreFront, puede definir un *modo de autoservicio*. Este modo permite a los usuarios suscribirse a las aplicaciones desde la interfaz de usuario de la aplicación Citrix Workspace. Esta experiencia de usuario mejorada es similar al uso de un almacén de aplicaciones móviles. En el modo de autoservicio, se pueden configurar parámetros de palabra clave para aplicaciones aprovisionadas automáticamente, destacadas y obligatorias.

**Nota:**

De forma predeterminada, la aplicación Citrix Workspace permite seleccionar las aplicaciones que aparecerán en su menú Inicio.

- **Modo de acceso directo solamente:** Puede configurar la aplicación Citrix Workspace para que coloque automáticamente accesos directos de aplicaciones y escritorios directamente en el menú Inicio o en el escritorio. El nuevo modo de *accesos directos solamente* permite buscar las aplicaciones publicadas dentro del esquema familiar de navegación de Windows.

Para obtener información, consulte la sección [Crear grupos de entrega](#) de la documentación de Citrix Virtual Apps and Desktops.

### **Configurar el modo de autoservicio**

Agregue una cuenta de StoreFront a la aplicación Citrix Workspace o configure la aplicación Citrix Workspace para que apunte a un sitio de StoreFront para usar el modo autoservicio. El autoservicio permite a los usuarios suscribirse a las aplicaciones desde la interfaz de usuario de Citrix Workspace. Esta experiencia de usuario mejorada es similar al uso de un almacén de aplicaciones móviles.

**Nota:**

De forma predeterminada, la aplicación Citrix Workspace permite a los usuarios seleccionar las aplicaciones que quieran ver en su menú Inicio.

En el modo de autoservicio, se pueden configurar parámetros de palabra clave para aplicaciones aprovisionadas automáticamente, destacadas y obligatorias.

Agregue palabras clave en las descripciones de las aplicaciones de los grupos de entrega:

- Para hacer obligatoria una aplicación concreta (de forma que no pueda quitarse de la aplicación Citrix Workspace), agregue la cadena **KEYWORDS: Mandatory** a la descripción de la aplicación. Los usuarios no tienen la opción **Quitar** para cancelar la suscripción a las aplicaciones obligatorias.

- Para suscribir automáticamente a todos los usuarios de un almacén a una aplicación, agregue la cadena **KEYWORDS: Auto** a la descripción. Cuando los usuarios inicien sesión en el almacén, la aplicación se aprovisionará automáticamente sin que los usuarios tengan que suscribirse de forma manual a la aplicación.
- Para anunciar aplicaciones a los usuarios o facilitar la búsqueda de las aplicaciones más utilizadas incorporándolas a la lista Destacados de Citrix Workspace, agregue la cadena **KEYWORDS: Featured** a la descripción de cada aplicación.

### **Personalizar las ubicaciones de los accesos directos de aplicaciones mediante la plantilla de objeto de directiva de grupo**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Autoservicio**.
3. Seleccione la directiva **Administrar modo Self-Service**.
  - a) **Habilítela** para ver la interfaz de usuario que ofrece la directiva de autoservicio.
  - b) **Inhabilítela** si quiere suscribirse manualmente a las aplicaciones. Esta opción oculta la interfaz de usuario de autoservicio.
4. Seleccione la directiva **Administrar accesos directos de aplicaciones**.
5. Seleccione las opciones según sea necesario.
6. Haga clic en **Aplicar y Aceptar**.
7. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

### **Usar parámetros de cuenta de StoreFront para personalizar las ubicaciones de los accesos directos de aplicaciones**

Puede configurar accesos directos en el menú Inicio y en el escritorio desde el sitio de StoreFront. Se puede agregar esta configuración al archivo `web.config` en `C:\inetpub\wwwroot\Citrix\Roaming`, en la sección **<annotatedServices>**:

- Para poner los accesos directos en el escritorio, use `PutShortcutsOnDesktop`. Parámetros: `“true”` o `“false”`(predeterminado: `false`).
- Para poner los accesos directos en el menú Inicio, use `PutShortcutsInStartMenu`. Parámetros: `“true”` o `“false”`(predeterminado: `true`).
- Para usar la ruta de categoría en el menú Inicio, use `UseCategoryAsStartMenuPath`. Parámetros: `“true”` o `“false”`(predeterminado: `true`).

**Nota:**

Windows 8, Windows 8.1 y Windows 10 no permiten la creación de carpetas anidadas dentro del menú Inicio. Las aplicaciones se muestran de forma individual o bajo la carpeta raíz, pero no en las subcarpetas de categorías definidas con Citrix Virtual Apps and Desktops.

- Para establecer un único directorio para todos los accesos directos en el menú Inicio, use StartMenuDir. Parámetro: Valor de cadena, correspondiente al nombre de la carpeta donde se van a incluir los accesos directos.
- Para volver a instalar aplicaciones modificadas, use AutoReinstallModifiedApps. Parámetros: “true” o “false”(predeterminado: true).
- Para mostrar un único directorio para todos los accesos directos en el escritorio, use DesktopDir. Parámetro: Valor de cadena, correspondiente al nombre de la carpeta donde se van a incluir los accesos directos.
- Para no crear una entrada en el panel “Agregar o quitar programas” del cliente, use DontCreateAddRemoveEntry. Parámetros: “true” o “false”(predeterminado: false).
- Para quitar los accesos directos y el icono de Citrix Workspace de una aplicación que previamente estuvo disponible en el almacén, pero ya no lo está, use SilentlyUninstallRemoveResources. Parámetros: “true” o “false”(predeterminado: false).

En el archivo web.config, los cambios se deben agregar en la sección **XML** de la cuenta. Para encontrar esta sección, busque la etiqueta de apertura:

```
<account id=... name="Store"
```

La sección termina con la etiqueta </account>.

Antes del final de la sección sobre cuentas, en la primera sección sobre propiedades:

```
<properties> <clear> <properties>
```

Se pueden agregar propiedades a esta sección después de la etiqueta <clear />, una por línea, mediante el nombre y el valor. Por ejemplo:

```
<property name="PutShortcutsOnDesktop" value="True"/>
```

**Nota:**

Los elementos de propiedad agregados antes de la etiqueta <clear /> pueden invalidarlos. Si quiere, puede optar por quitar la etiqueta <clear /> al agregar un nombre y un valor de propiedad.

El siguiente es un ejemplo ampliado para esta sección:

```
<properties <property name="PutShortcutsOnDesktop" value="True"<  
property name="DesktopDir" value="Citrix Applications">
```

### Importante

En implementaciones con varios servidores, use solo un servidor a la vez para hacer cambios en la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen. Para obtener más información, consulte la documentación de [StoreFront](#).

## Usar parámetros por aplicación en Citrix Virtual Apps and Desktops 7.x para personalizar ubicaciones de los accesos directos de las aplicaciones

La aplicación Citrix Workspace puede configurarse para que coloque automáticamente los accesos directos de los escritorios y las aplicaciones directamente en el menú Inicio o en el escritorio. Esta función era similar a las versiones anteriores de Citrix Workspace para Windows. Sin embargo, la versión 4.2.100 incluía la capacidad de controlar la ubicación de los accesos directos de las aplicaciones mediante los parámetros por aplicación de Citrix Virtual Apps. Esta función resulta útil en entornos donde hay unas cuantas aplicaciones que es necesario mostrar en ubicaciones coherentes.

Si quiere establecer la ubicación de los accesos directos de modo que cada usuario las encuentre en el mismo lugar, use los parámetros por aplicación de Citrix Virtual Apps:

---

Si quiere usar parámetros por aplicación para determinar dónde se colocarán las aplicaciones, independientemente de si se usa el modo de autoservicio o el modo de menú Inicio.

Configure la aplicación Citrix Workspace para Windows con **PutShortcutsInStartMenu=false** y habilite los parámetros por aplicación. Nota: Este parámetro solo es aplicable a sitios de la Interfaz Web.

---

### Nota:

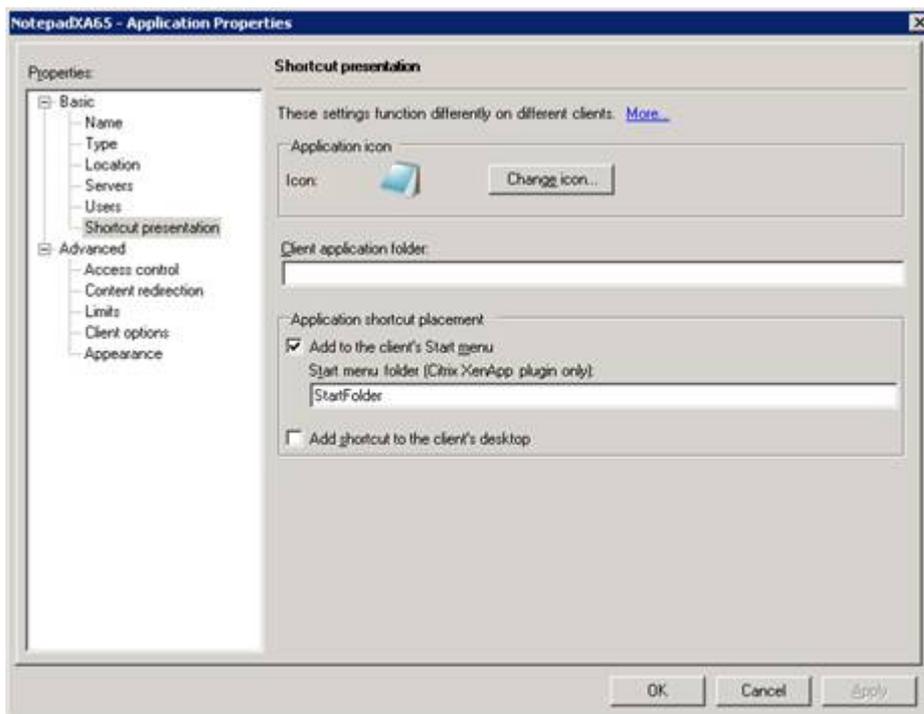
El parámetro **PutShortcutsInStartMenu=false** se aplica a XenApp 6.5 y XenDesktop 7.x.

## Configurar parámetros por aplicación en XenApp 6.5

Para configurar un acceso directo de publicación para cada aplicación en XenApp 6.5:

1. En la pantalla **Propiedades de la aplicación** de XenApp, expanda las propiedades **Básicas**.
2. Seleccione la opción “Presentación del acceso directo”.

3. En la sección “Ubicación del acceso directo de la aplicación” en la pantalla **Presentación del acceso directo**, seleccione **Agregar** al menú Inicio del cliente. Después de marcar esta casilla, escriba el nombre de la carpeta donde desea colocar el acceso directo. Si no se especifica un nombre de carpeta, XenApp coloca el acceso directo en el menú Inicio, sin carpeta.
4. Seleccione Agregar un acceso directo en el escritorio del cliente para incluir el acceso directo en el escritorio de la máquina cliente.
5. Haga clic en **Aplicar**.
6. Haga clic en **Aceptar**.



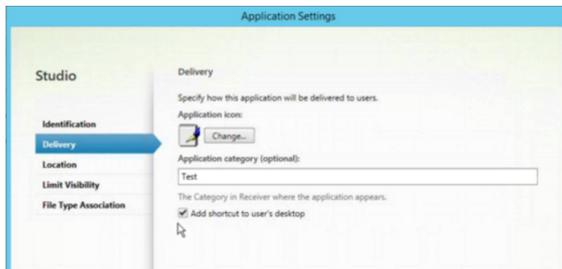
### Usar parámetros por aplicación en XenApp 7.6 para personalizar las ubicaciones de los accesos directos de las aplicaciones

Para configurar un acceso directo de publicación para cada aplicación en XenApp 7.6:

1. En Citrix Studio, busque la pantalla **Parámetros de la aplicación**.
2. En la pantalla **Parámetros de la aplicación**, seleccione **Entrega**. En esta pantalla, puede especificar cómo se entregarán las aplicaciones a los usuarios.
3. Seleccione el icono adecuado para la aplicación. Haga clic en **Cambiar** para ir a la ubicación del icono pertinente.
4. En el campo **Categoría de la aplicación**, opcionalmente, puede especificar la categoría en que

aparece la aplicación dentro de Citrix Workspace. Por ejemplo, si está agregando accesos directos a aplicaciones de Microsoft Office, escriba Microsoft Office.

5. Marque la casilla “Agregar acceso directo al escritorio del usuario”.
6. Haga clic en Aceptar.



### Disminuir las demoras de enumeración o firma digital de código auxiliar de aplicaciones

Si los usuarios notan demoras en la enumeración de aplicaciones en cada inicio de sesión, o si hay necesidad de firmar digitalmente código auxiliar (stubs) de aplicaciones, la aplicación Citrix Workspace ofrece una funcionalidad para copiar los EXE de código auxiliar desde un recurso compartido de red.

Esta funcionalidad requiere varios pasos a seguir:

1. Cree el código auxiliar de cada aplicación en la máquina cliente.
2. Copie el código auxiliar de las aplicaciones en una ubicación común, accesible desde un recurso compartido de red.
3. Si es necesario, prepare una lista de permitidos o firme el código auxiliar con un certificado de empresa.
4. Agregue una clave de Registro para dejar que Citrix Workspace para Windows cree el código auxiliar copiándolo desde el recurso compartido de red.

Si **RemoveappsOnLogoff** y **RemoveAppsonExit** están habilitados, y los usuarios notan demoras en la enumeración de aplicaciones cada vez que inician una sesión, use la siguiente solución para reducir las demoras:

1. Use `regedit` para agregar `HKEY_CURRENT_USER\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"`.
2. Use `regedit` para agregar `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"`. `HKEY_CURRENT_USER` prevalece sobre `HKEY_LOCAL_MACHINE`.

#### Precaución

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados

de la utilización inadecuada del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Permita que una máquina use archivos ejecutables de código auxiliar almacenados en el recurso compartido de red:

1. En una máquina cliente cree ejecutables de código auxiliar para todas las aplicaciones. Para lograr eso, agregue todas las aplicaciones a la máquina mediante la aplicación Citrix Workspace; esta aplicación genera los archivos ejecutables.
2. Después, tome los archivos stub de los ejecutables que encontrará en %APPDATA%\Citrix\SelfService. Solamente necesita los archivos EXE.
3. Copie los archivos ejecutables a un recurso compartido de red.
4. Para cada máquina cliente que está bloqueada, establezca las siguientes claves de Registro:
  - a) `Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\WorkspaceStubs"`
  - b) `Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v`
  - c) `CopyStubsFromCommonStubDirectory /t REG_SZ /d "true"`. También es posible configurar estos parámetros en HKEY\_CURRENT\_USER, si lo prefiere. HKEY\_CURRENT\_USER prevalece sobre HKEY\_LOCAL\_MACHINE.
  - d) Salga y reinicie la aplicación Citrix Workspace para probar la configuración.

### **Ejemplo de casos de uso:**

Este tema proporciona casos de uso para los accesos directos de aplicaciones.

### **Permitir a los usuarios elegir lo que quieran ver en el menú Inicio (Autoservicio)**

Si tiene decenas (o incluso cientos) de aplicaciones, es mejor permitir que los usuarios seleccionen qué aplicaciones quieren ver como favoritas y agregarlas al menú Inicio:

---

Si quiere que el usuario elija las aplicaciones que desea tener en su menú Inicio...

Configure la aplicación Citrix Workspace en el modo de autoservicio. En este modo, también deberá configurar los parámetros de palabra clave *auto* (aprovisionada automáticamente) y *mandatory* (obligatoria) para las aplicaciones, según sea necesario.

Si quiere que el usuario elija las aplicaciones que quiera colocar en su menú Inicio, pero también quiere colocar accesos directos específicos en el escritorio...

Configure la aplicación Citrix Workspace sin opciones y, a continuación, use parámetros para cada una de las aplicaciones que quiera mostrar en el escritorio. Use aplicaciones aprovisionadas automáticamente (*auto*) y obligatorias (*mandatory*), según sea necesario.

---

### **Menú Inicio sin accesos directos de aplicaciones**

Si el usuario utiliza un equipo doméstico que usa toda la familia, es posible que no sea necesario o conveniente colocar accesos directos. En tales casos, lo más sencillo es usar el acceso por explorador web; instale la aplicación Citrix Workspace sin configuración alguna y vaya a Citrix Workspace para Web o a la Interfaz Web. También puede configurar la aplicación Citrix Workspace para el acceso de autoservicio sin colocar accesos directos en ningún lugar.

---

Si quiere evitar que la aplicación Citrix Workspace coloque accesos directos de aplicaciones en el menú Inicio automáticamente.

Configure la aplicación Citrix Workspace con `PutShortcutsInStartMenu=False`. La aplicación Citrix Workspace no colocará aplicaciones en el menú Inicio, incluso en el modo de autoservicio, a menos que usted los coloque mediante los parámetros de cada aplicación.

---

### **Todos los accesos directos de aplicaciones en el menú Inicio o en el escritorio**

Si el usuario tiene pocas aplicaciones, puede colocarlas todas en el menú Inicio o todas en el escritorio, o en una carpeta del escritorio.

---

Si quiere que la aplicación Citrix Workspace coloque todos los accesos directos de las aplicaciones en el menú Inicio automáticamente

Configure la aplicación Citrix Workspace con `SelfServiceMode=False`. Todas las aplicaciones disponibles aparecen en el menú Inicio.

---

...

---

Si quiere que se coloquen accesos directos de todas las aplicaciones en el escritorio...	Configure la aplicación Citrix Workspace con <code>PutShortcutsOnDesktop = true</code> . Todas las aplicaciones disponibles aparecen en el escritorio.
Si quiere que todos los accesos directos se coloquen dentro de una carpeta en el escritorio ...	Configure la aplicación Citrix Workspace con <code>DesktopDir=Nombre de la carpeta de escritorio</code> donde quiera las aplicaciones.

---

### Parámetros por aplicación en XenApp 6.5 o 7.x

Si quiere establecer la ubicación de los accesos directos de modo que cada usuario las encuentre en el mismo lugar, use los parámetros de aplicación de XenApp:

---

Si quiere usar parámetros por aplicación para determinar dónde se colocarán las aplicaciones, independientemente de si se usa el modo de autoservicio o el modo de menú Inicio.	Configure la aplicación Citrix Workspace con <code>PutShortcutsInStartMenu=false</code> y habilite los parámetros por aplicación.
---	---

---

### Aplicaciones en carpetas de categorías o en carpetas específicas

Si quiere mostrar las aplicaciones en carpetas específicas, use las siguientes opciones:

---

Si quiere que los accesos directos de las aplicaciones que la aplicación Citrix Workspace coloca en el menú Inicio aparezcan en su categoría (carpeta) asociada...	Configure la aplicación Citrix Workspace con <code>UseCategoryAsStartMenuPath=True</code> .
Si quiere que las aplicaciones que la aplicación Citrix Workspace coloca en el menú Inicio aparezcan en una carpeta específica...	Configure la aplicación Citrix Workspace con <code>StartMenuDir=el nombre de la carpeta del menú Inicio</code> .

---

## Quitar aplicaciones al cerrar la sesión o al salir

Si no quiere que un usuario vea las aplicaciones de otro usuario cuando van a compartir un dispositivo de punto final, puede hacer que las aplicaciones se eliminen cuando el usuario cierre sesión y salga.

---

Si quiere que la aplicación Citrix Workspace quite todas las aplicaciones al cerrar sesión...	Configure la aplicación Citrix Workspace con <code>RemoveAppsOnLogoff=True</code> .
Si quiere que la aplicación Citrix Workspace quite las aplicaciones al salir...	Configure la aplicación Citrix Workspace con <code>RemoveAppsOnExit=True</code> .

---

## Configurar aplicaciones para el acceso a aplicaciones locales

Al configurar aplicaciones para el acceso a aplicaciones locales:

- Para especificar que se debe usar una aplicación instalada localmente en lugar de una aplicación disponible en la aplicación Citrix Workspace, agregue la cadena de texto `KEYWORDS:prefer="pattern"`. Esta función se conoce como Acceso a aplicaciones locales.

Antes de instalar una aplicación en un equipo de usuario, la aplicación Citrix Workspace busca los patrones especificados para ver si la aplicación está instalada localmente. Si lo está, la aplicación Citrix Workspace se suscribe a la aplicación y no crea ningún acceso directo. Cuando el usuario inicia la aplicación desde la ventana de la aplicación Citrix Workspace, la aplicación Citrix Workspace inicia la aplicación instalada localmente (preferida).

Si un usuario desinstala una aplicación preferida desde fuera de la aplicación Citrix Workspace, la próxima vez que la aplicación Citrix Workspace se actualice, cancelará la suscripción a la aplicación. Si un usuario desinstala una aplicación preferida desde el cuadro de diálogo de la aplicación Citrix Workspace, la aplicación Citrix Workspace cancela la suscripción a la aplicación, pero no la desinstala.

### Nota:

La palabra clave “prefer” se aplica cuando la aplicación Citrix Workspace se suscribe a una aplicación. Si se agrega la palabra clave después de haberse suscrito a la aplicación, esto no tiene efecto alguno.

Puede especificar la palabra clave `prefer` varias veces para una aplicación. Solo se necesita una vez para aplicar la palabra clave a una aplicación. Estos patrones pueden usarse en cualquier combinación:

- Para especificar que se debe usar una aplicación instalada localmente en lugar de una aplicación disponible en la aplicación Citrix Workspace, agregue la cadena de texto KEYWORDS:prefer="pattern". Esta función se conoce como Acceso a aplicaciones locales.

Antes de instalar una aplicación en un equipo de usuario, la aplicación Citrix Workspace busca los patrones especificados para ver si la aplicación está instalada localmente. Si lo está, la aplicación Citrix Workspace se suscribe a la aplicación y no crea ningún acceso directo. Cuando el usuario inicia la aplicación desde el cuadro de diálogo de la aplicación Citrix Workspace, la aplicación Citrix Workspace inicia la aplicación instalada localmente (preferida).

Si un usuario desinstala una aplicación preferida desde fuera de la aplicación Citrix Workspace, la próxima vez que la aplicación Citrix Workspace se actualice, cancelará la suscripción a la aplicación. Si un usuario desinstala una aplicación preferida desde la aplicación Citrix Workspace, la aplicación Citrix Workspace cancela la suscripción a la aplicación, pero no la desinstala.

A partir de 1912, puede configurar el comportamiento de la actualización automática en la aplicación Citrix Workspace mediante el Editor del Registro.

En versiones anteriores, al reiniciar la aplicación Citrix Workspace, la actualización automática se produce incluso cuando los datos de la caché están disponibles.

**Nota:**

No se puede configurar esta opción en cuentas de tienda que no sean X1.

**Para configurar la actualización automática mediante el Editor del Registro:**

1. Inicie el Editor del Registro y vaya a HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle.
2. Cree las siguientes claves de valor de cadena:

---

Clave del Registro	Valor
InitialRefreshMinMs	10000 (10 segundos)
InitialRefreshMaxMs	15000 (15 segundos)
SuppressRefreshMs	1000 (1 segundo)

---

3. Guarde y cierre el editor.

**Nota:**

La palabra clave "prefer" se aplica cuando la aplicación Citrix Workspace se suscribe a una aplicación. Si se agrega la palabra clave después de haberse suscrito a la aplicación, esto no tiene efecto alguno.

Puede especificar la palabra clave prefer varias veces para una aplicación. Solo se necesita una vez para aplicar la palabra clave a una aplicación. Estos patrones pueden usarse en cualquier combinación:

- prefer="NombreDeAplicación"

El patrón del nombre de la aplicación hará coincidir cualquier aplicación que contenga dicho nombre en el nombre del archivo de acceso directo. El nombre de aplicación puede ser una palabra o una frase. Para introducir frases hay que usar comillas. No se hacen coincidir palabras o rutas de archivo incompletas, y la coincidencia no distingue entre mayúsculas y minúsculas. El patrón de coincidencia de nombre de aplicación resulta útil para sobrescritura de parámetros realizadas manualmente por un administrador.

KEYWORDS:prefer=	Acceso directo en Programas	¿Coincide?
Word	\Microsoft Office\Microsoft Word 2010	Sí
Microsoft Word	\Microsoft Office\Microsoft Word 2010	Sí
Consola	McAfee\VirusScan Console	Sí
Virus	McAfee\VirusScan Console	No
Consola	McAfee\VirusScan Console	Sí

- prefer="\\Carpeta1\Carpeta2\...\NombreDeAplicación"

El patrón de la ruta absoluta coincide con la ruta completa del archivo de acceso directo, además del nombre completo de la aplicación en el menú Inicio. La carpeta Programas es una subcarpeta del directorio del menú Inicio, de modo que hay que incluirla en la ruta absoluta si el destino es una aplicación de esa carpeta. Si la ruta contiene espacios hay que usar comillas. La coincidencia distingue entre mayúsculas y minúsculas. El patrón de coincidencia de la ruta absoluta es útil para sobrescrituras implementadas mediante programación en Citrix Virtual Apps and Desktops.

KEYWORDS:prefer=	Acceso directo en Programas	¿Coincide?
\Programs\Microsoft Office\Microsoft Word 2010	\Programs\Microsoft Office\Microsoft Word 2010	Sí
\Microsoft Office	\Programs\Microsoft Office\Microsoft Word 2010	No
\Microsoft Word 2010	\Programs\Microsoft Office\Microsoft Word 2010	No

KEYWORDS:prefer=	Acceso directo en Programas	¿Coincide?
\Programs\Microsoft Word 2010	\Programs\Microsoft Word 2010	Sí

- prefer="\"Carpeta1\Carpeta2\...\NombreDeAplicación"

El patrón de la ruta relativa coincide con la ruta relativa del archivo de acceso directo en el menú Inicio. La ruta relativa suministrada debe contener el nombre de la aplicación y puede, de manera optativa, incluir las carpetas donde reside el acceso directo. La coincidencia es correcta si la ruta del archivo de acceso directo termina con la ruta relativa suministrada. Si la ruta contiene espacios hay que usar comillas. La coincidencia distingue entre mayúsculas y minúsculas. El patrón de coincidencia de la ruta absoluta es útil para sobrescrituras implementadas mediante programación.

KEYWORDS:prefer=	Acceso directo en Programas	¿Coincide?
\Microsoft Office\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Sí
\Microsoft Office	\Microsoft Office\Microsoft Word 2010	No
\Microsoft Word 2010	\Microsoft Office\Microsoft Word 2010	Sí
\Microsoft Word	\Microsoft Word 2010	No

Para obtener más información sobre otras palabras clave, consulte “Recomendaciones adicionales” en [Optimizar la experiencia de usuario](#), en la documentación de StoreFront.

## Tiempo de inicio de las aplicaciones

La función de preinicio de sesiones permite reducir el tiempo que tardan en abrirse las aplicaciones durante los períodos de mucho tráfico o tráfico normal, mejorando así la experiencia del usuario. La función de preinicio permite crear una sesión de preinicio cuando un usuario inicia una sesión en la aplicación Citrix Workspace o en un momento específico programado si el usuario ya ha iniciado una sesión.

Esta sesión de preinicio reduce el tiempo que tarda en iniciarse la primera aplicación. Cuando un usuario agrega una nueva conexión de cuenta a la aplicación Citrix Workspace para Windows, el preinicio de sesiones no tiene efecto hasta la siguiente sesión. La aplicación predeterminada ctxprelaunch.exe se ejecuta en esta sesión, pero no es visible.

En implementaciones de StoreFront, se admite el preinicio de sesiones. En implementaciones de la Interfaz Web, debe usar la opción **Guardar contraseña** para evitar que aparezcan diálogos de inicio de sesión. El preinicio de sesiones no se admite en implementaciones de Citrix Virtual Apps and Desktops.

Para obtener más información, consulte [Preinicio de sesiones y persistencia de sesiones en un grupo de entrega](#) en la documentación de Citrix Virtual Apps and Desktops.

El preinicio de sesiones está inhabilitado de forma predeterminada. Para habilitar el preinicio de sesiones, especifique el parámetro `ENABLEPRELAUNCH=true` en la línea de comandos de Workspace o defina la clave de Registro `EnablePreLaunch` en true. El parámetro predeterminado es Null y significa que el preinicio está inhabilitado.

**Nota:**

Si la máquina cliente se ha configurado para admitir la autenticación PassThrough de dominio (SSON), el preinicio está habilitado automáticamente. Si quiere usar la autenticación PassThrough de dominio (Single Sign-On) sin la función de preinicio, establezca el valor de la clave de Registro `EnablePreLaunch` en false.

Las ubicaciones en el Registro son:

- HKEY\_LOCAL\_MACHINE\Software\[Wow6432Node\Citrix\Dazzle
- HKEY\_CURRENT\_USER\Software\Citrix\Dazzle

Existen dos tipos de preinicio:

- **Preinicio a petición:** El preinicio se lleva a cabo inmediatamente después de autenticarse las credenciales del usuario, independientemente del tráfico de la red. Por lo general, se usa en períodos de tráfico normal. Un usuario puede provocar el preinicio reiniciando la aplicación Citrix Workspace.
- **Preinicio programado:** El preinicio ocurre a una hora programada. El preinicio programado ocurre solo cuando el dispositivo de usuario ya se está ejecutando y se ha autenticado. Si no se cumplen estas dos condiciones cuando llega la hora del preinicio programado, no se inicia la sesión. La sesión se inicia en una ventana a la hora programada lo que permite distribuir la carga de red y del servidor. Por ejemplo, si el preinicio se ha programado para las 13:45, la sesión en realidad se inicia entre las 13:15 y las 13:45. Esto se utiliza, por lo general, en períodos de mucho tráfico.

La configuración del preinicio en el servidor Citrix Virtual Apps consiste en crear, modificar o eliminar aplicaciones de preinicio, así como actualizar las configuraciones de directivas de usuario que controlan el preinicio de aplicaciones.

No se puede usar el archivo receiver.admx para personalizar la función de preinicio. No obstante, se puede cambiar la configuración del preinicio modificando valores de Registro durante o después de la instalación de la aplicación Citrix Workspace para Windows.

- Los valores HKEY\_LOCAL\_MACHINE se escriben durante la instalación del cliente.
- Los valores HKEY\_CURRENT\_USER permiten dar diferentes parámetros a los distintos usuarios de una misma máquina. Los usuarios pueden cambiar los valores HKEY\_CURRENT\_USER sin necesidad de permisos de administrador. Se pueden proporcionar scripts a los usuarios para lograr este resultado.

#### **Valores de Registro HKEY\_LOCAL\_MACHINE:**

Para sistemas operativos Windows de 64 bits: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

Para sistemas operativos Windows de 32 bits: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch

Nombre: **UserOverride**

Valores:

0: Usa los valores de HKEY\_LOCAL\_MACHINE, incluso si ya existen valores de HKEY\_CURRENT\_USER.

1: Usa los valores de HKEY\_CURRENT\_USER si ya existen; de lo contrario, usa los valores de HKEY\_LOCAL\_MACHINE.

Nombre: **State**

Valores:

0: Inhabilita el preinicio.

1: Habilita el preinicio a petición (el preinicio ocurre después de autenticar las credenciales).

2: Habilita el preinicio programado (el preinicio comienza a la hora configurada en Programar).

Nombre: **Schedule**

Valor:

Hora (en formato de 24 horas) y días de la semana para los inicios previos programados, con el formato siguiente:

`HH:MM | M:T:W:TH:F:S:SU` - donde `HH` y `MM` son horas y minutos; `M:T:W:TH:F:S:SU` es el día de la semana. Por ejemplo, para habilitar el preinicio programado los lunes, miércoles y viernes a las 13:45, configure Schedule en `Schedule=13:45`

---

### Valores de Registro HKEY\_CURRENT\_USER:

HKEY\_CURRENT\_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

Las claves State y Schedule tienen los mismos valores que para HKEY\_LOCAL\_MACHINE.

### Redirección bidireccional de contenido

La directiva “Redirección bidireccional de contenido” permite habilitar o inhabilitar la redirección de direcciones URL entre el host y el cliente y viceversa. Las directivas de servidor se configuran en Citrix Studio, y las directivas de cliente se configuran en la plantilla administrativa de objetos de directiva de grupo de la aplicación Citrix Workspace.

A pesar de que Citrix también ofrece la redirección del host al cliente y el Acceso a aplicaciones locales para la redirección del cliente a la URL, le recomendamos usar la redirección bidireccional de contenido para clientes de Windows unidos a un dominio.

Es posible habilitar la redirección bidireccional de contenido mediante uno de los siguientes métodos:

1. Plantilla administrativa de objetos de directiva de grupo (GPO)
2. Editor del Registro

#### Nota:

- La redirección bidireccional de contenido no funciona en las sesiones donde está habilitado el **Acceso a aplicaciones locales**.
- La redirección bidireccional de contenido debe estar habilitada tanto en el servidor como en el cliente. Cuando esté inhabilitada en alguna de las partes, ya sea el servidor o el cliente, la funcionalidad estará inhabilitada.
- Al incluir direcciones URL, puede especificar una sola dirección URL o una lista de direcciones URL, delimitadas por punto y coma. Puede utilizar un asterisco (\*) como comodín.

### Para habilitar la redirección bidireccional de contenido mediante la plantilla administrativa de GPO:

Use la configuración de la plantilla administrativa de GPO solo para la primera instalación de la aplicación Citrix Workspace para Windows.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del usuario**, vaya a **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Workspace > Experiencia de usuario**.
3. Seleccione la directiva **Redirección bidireccional de contenido**.

**Bidirectional Content Redirection**

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on: All Citrix Workspace supported platforms

Options:

Published Application/Desktop Name:

Above Name is for Published Type: Application

Allowed URLs to be redirected to VDA:

Enable URL-specific published application or desktop overrides?

URL-specific published application or desktop overrides:

Allowed URLs to be redirected to Client:

Help:

Bidirectional Content Redirection is the feature that allows URLs to be redirected from client to server and vice versa based on configuration.

- Published Application/Desktop Name : Indicates the name of the published application / desktop used to launch the redirected URL. This is not used when Bidirectional Content Redirection is enabled on any of the active ICA sessions. Whether its Desktop or Application is decided based on the Type specified below.
- Above Name is for Published Type : This indicates the above Name is whether Application or Desktop.
- Allowed URLs to be redirected to VDA : This indicates the list of URLs that will be opened on VDA. Semi Colon ";" acts as a delimiter. "\*" can be used as wild card. For example \*.xyz.com.
- Enable URL-specific published application or desktop overrides : This indicates whether the URL-specific overrides, specified below, are active.
- URL-specific published application or desktop overrides : This indicates the URL-specific overrides for Published Application/Desktop Name. The "Value name" should exactly match an entry in the "Allowed URLs to be redirected to VDA"

OK Cancel Apply

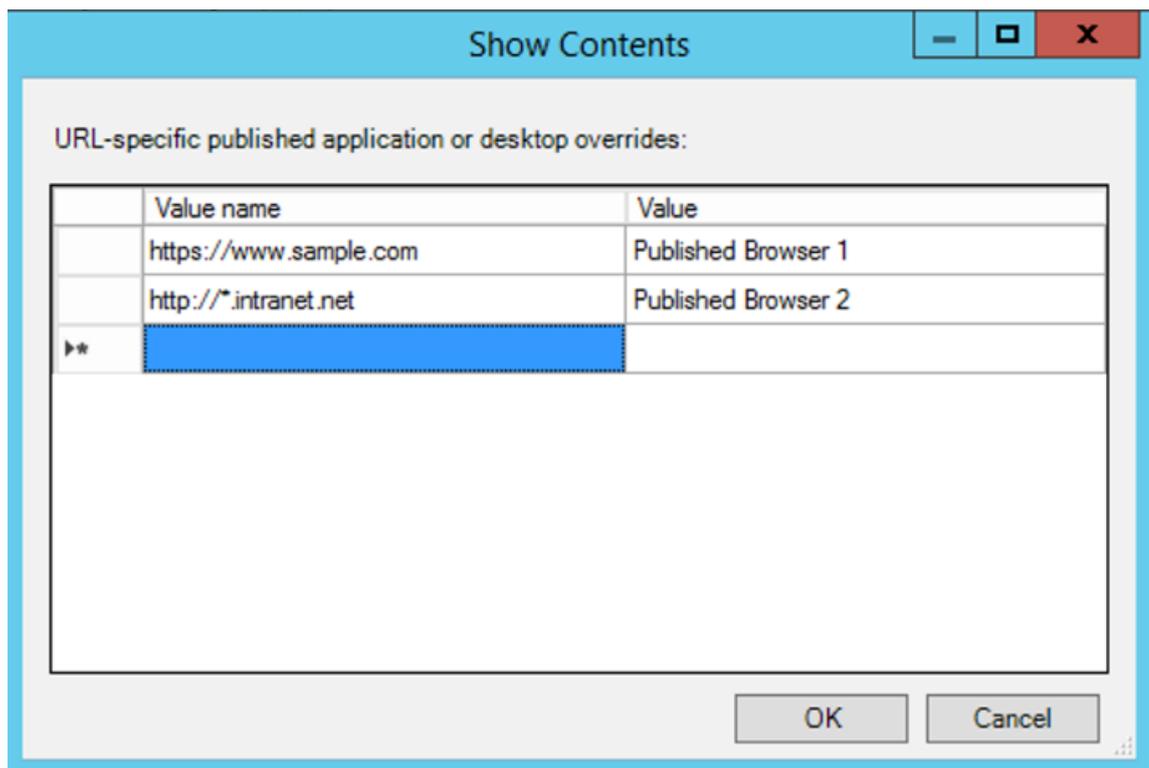
1. En el campo **Nombre de aplicación/escritorio publicado**, indique el nombre del recurso uti-

lizado para iniciar la dirección URL redirigida.

**Nota:**

Al incluir direcciones URL, especifique una sola dirección URL o una lista de direcciones URL, delimitadas por punto y coma. Puede utilizar un asterisco (\*) como comodín.

2. En **Tipo de recurso publicado**, seleccione **Aplicación** o **Escritorio** del recurso según corresponda.
3. En el campo **Direcciones URL permitidas para redirigir al VDA**, introduzca las direcciones URL que se deben redirigir. Separe cada dirección de la lista con un punto y coma.
4. Seleccione la opción **Habilitar el reemplazo de aplicaciones o escritorios publicados con direcciones URL específicas** para reemplazar una URL.
5. Haga clic en **Mostrar** para ver una lista en la que el nombre del valor debe coincidir con cualquiera de las direcciones URL indicadas en el campo **Direcciones URL permitidas para redirigir al VDA**. El valor debe coincidir con el nombre de una aplicación publicada.



6. En el campo **Direcciones URL permitidas para redirigir al cliente**, introduzca las direcciones URL que se deben redirigir del servidor al cliente. Separe cada dirección de la lista con un punto y coma.

**Nota:**

Al incluir direcciones URL, especifique una sola dirección URL o una lista de direcciones URL, delimitadas por punto y coma. Puede utilizar un asterisco (\*) como comodín.

7. Haga clic en **Aplicar** y **Aceptar**.
8. Desde la línea de comandos, ejecute el comando `gpupdate /force`.

**Para habilitar la redirección bidireccional de contenido mediante el Registro:**

Para habilitar la redirección bidireccional de contenido, ejecute el comando `redirector.exe /RegIE` desde la carpeta de instalación de la aplicación Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`.

**Importante:**

- Compruebe que la regla de redirección no resulta en un bucle. Cuando las reglas del VDA se definen para que la URL `https://www.my\_company.com` se redirija, por ejemplo, al cliente y también para que la misma URL se redirija al VDA, el resultado es un bucle.
- La función de redirección de URL solo admite direcciones URL explícitas (aquellas que aparecen en la barra de direcciones del explorador o las que se encuentran navegando dentro del explorador, según el explorador que se esté usando).
- Si hay dos aplicaciones con el mismo nombre simplificado que están configuradas para usar varias cuentas de StoreFront, el nombre simplificado de la cuenta principal de StoreFront se utiliza para lanzar la sesión de escritorio o de aplicación.
- Solo se abre una nueva ventana de explorador web cuando la dirección URL se redirige al cliente. Cuando la dirección URL se redirige al VDA, si el explorador web ya está abierto, la URL redirigida se abre en una nueva ficha.
- Se admiten enlaces incrustados en archivos como documentos, mensajes de correo electrónico y archivos PDF.
- Compruebe que, en una máquina, solamente hay habilitada una de las directivas de redirección de contenido del host y de la asociación de tipos de archivo del servidor. Citrix recomienda inhabilitar la función de asociación de tipos de archivo de servidor o la función de redirección de contenido de host (URL) para asegurarse de que la redirección de URL funciona correctamente.

**Limitación:**

Si la redirección falla debido a problemas de lanzamiento de la sesión, no hay ningún mecanismo alternativo.

## Teclados Bloomberg

La aplicación Citrix Workspace admite el uso de teclados Bloomberg en una sesión de aplicaciones y escritorios virtuales. Los componentes necesarios se instalan con el plug-in. Puede activar la función de teclado Bloomberg durante la instalación de la aplicación Citrix Workspace para Windows o mediante el Editor del Registro.

No se recomienda tener varias sesiones con teclados Bloomberg. El teclado solo funciona en entornos de sesión única.

### Configurar teclados Bloomberg:

#### Precaución

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. Busque la siguiente clave en el Registro:

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`

2. Lleve a cabo una de las siguientes acciones:

- Para habilitar esta función, configure una entrada de tipo DWORD y el nombre **Enable-BloombergHID** con el valor 1.
- Para inhabilitar esta función, establezca el valor en 0.

Para obtener más información sobre la configuración de teclados Bloomberg, consulte el artículo [CTX122615](#) de Knowledge Center.

### Para impedir que la ventana de Desktop Viewer se atenúe:

Si utiliza varias ventanas de Desktop Viewer, de manera predeterminada se atenúan los escritorios que no están activos. Si los usuarios quieren ver varios escritorios de forma simultánea, esto puede hacer que la información que se incluye en ellos sea ilegible. Para inhabilitar el comportamiento predeterminado e impedir que la ventana de Desktop Viewer se atenúe, modifique el Editor del Registro.

#### Precaución

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de

modificarlo.

- En el dispositivo de usuario, cree una entrada de Registro REG\_DWORD denominada **DisableDimming** en una de las siguientes claves, dependiendo de si quiere impedir la atenuación solo para el usuario actual del dispositivo, o para el dispositivo propiamente dicho. Existe un registro si Desktop Viewer se ha utilizado en el dispositivo:
  - HKEY\_CURRENT\_USER\Software\Citrix\XenDesktop\DesktopViewer
  - HKEY\_LOCAL\_MACHINE\Software\Citrix\XenDesktop\DesktopViewer

O bien, en lugar de controlar la atenuación, puede definir una directiva local creando la misma entrada REG\_WORD en una de las siguientes claves:

- HKEY\_CURRENT\_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer
- HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\XenDesktop\DesktopViewer

Antes de utilizar estas claves, compruebe si el administrador de Citrix Virtual Apps and Desktops y Citrix DaaS ha establecido una directiva para esta función.

Establezca la entrada en cualquier valor distinto de cero, como 1 o true (verdadero).

Si no se especifican entradas o si esta se establece en 0, la ventana de Desktop Viewer se atenúa. Si se especifican varios registros, se utiliza la siguiente prioridad. El primer registro que se ubica en esta lista, y su valor, determinan si la ventana se atenúa:

1. HKEY\_CURRENT\_USER\Software\Policies\Citrix\...
2. HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\...
3. HKEY\_CURRENT\_USER\Software\Citrix\...
4. HKEY\_LOCAL\_MACHINE\Software\Citrix\...

## Citrix Casting

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

Citrix Ready Workspace Hub se ha construido sobre la plataforma Raspberry Pi 3. El dispositivo que ejecuta la aplicación Citrix Workspace se conecta a Citrix Ready Workspace Hub y transmite las aplicaciones o los escritorios hacia una pantalla más grande. Citrix Casting solo se admite en la versión 1607 de Microsoft Windows 10 y en versiones posteriores o en Windows Server 2016.

Citrix Casting es una función pensada para permitirle acceder de forma instantánea y segura a cualquier aplicación desde un dispositivo móvil y mostrar el contenido en una pantalla grande.

**Nota:**

- Citrix Casting para Windows admite la versión 2.40.3839 de Citrix Ready Workspace Hub y versiones posteriores. Es posible que las versiones anteriores de Citrix Ready Workspace Hub no se detecten o causen un error de proyección.
- La función Citrix Casting no está disponible en la aplicación Citrix Workspace para Windows (Store).

**Requisitos previos:**

- Bluetooth está habilitado en el dispositivo para detectar hubs.
- Tanto Citrix Ready Workspace Hub como la aplicación Citrix Workspace deben estar en la misma red.
- El puerto 55555 no debe estar bloqueado entre el dispositivo que ejecuta la aplicación Citrix Workspace y Citrix Ready Workspace Hub.
- Para Citrix Casting, el puerto 1494 no se debe bloquear.
- El puerto 55556 es el puerto predeterminado para las conexiones SSL entre los dispositivos móviles y Citrix Ready Workspace Hub. Puede configurar otro puerto SSL en la página de parámetros de Raspberry Pi. Si el puerto SSL está bloqueado, los usuarios no pueden establecer conexiones SSL con Workspace Hub.
- Citrix Casting solo se admite en la versión 1607 de Microsoft Windows 10 y en versiones posteriores o en Windows Server 2016.

**Configurar el inicio de Citrix Casting**

**Nota:**

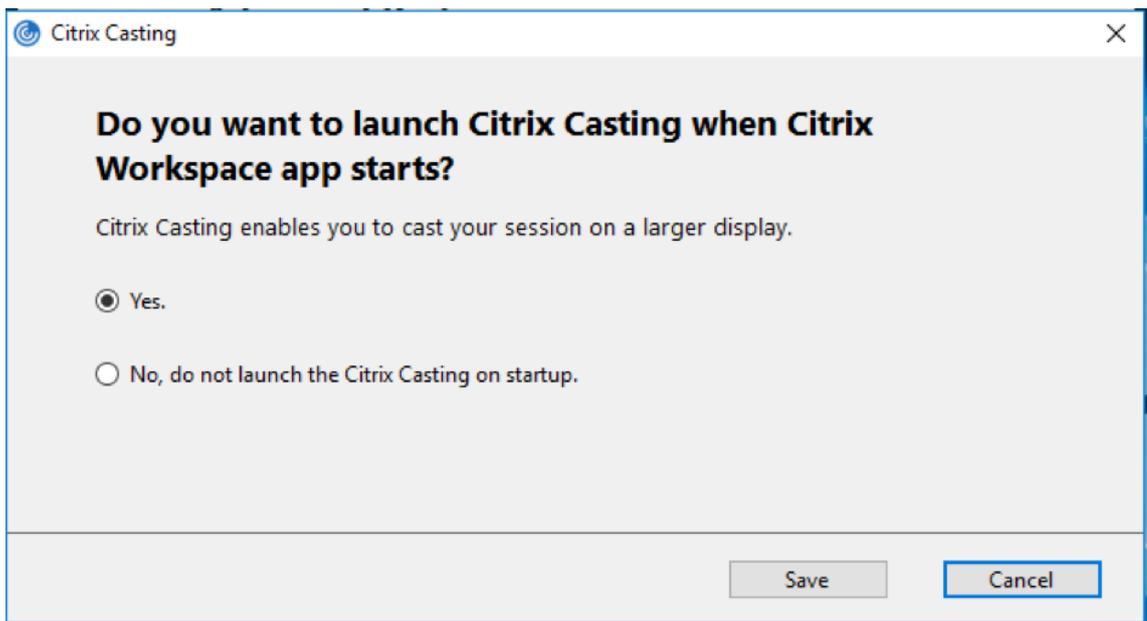
Puede ocultar total o parcialmente las opciones de la hoja de Preferencias avanzadas, disponible en el icono de la aplicación Citrix Workspace del área de notificaciones. Para obtener más información, consulte [Hoja de Preferencias avanzadas](#).

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace en el área de notificaciones y seleccione **Preferencias avanzadas**.

Se mostrará el cuadro de diálogo **Preferencias avanzadas**.

2. Seleccione **Citrix Casting**.

Aparece el cuadro de diálogo **Citrix Casting**.



3. Seleccione una de estas opciones:

- **Sí:** Indica que Citrix Casting se inicia cuando se inicia la aplicación Citrix Workspace.
- **No,** no abrir Citrix Casting al iniciar: Citrix Casting no se inicia al iniciar la aplicación Citrix Workspace.

**Nota:**

Seleccionar la opción **No** no finaliza la sesión actual de proyección de pantalla. La configuración se aplica solo en el próximo inicio de la aplicación Citrix Workspace.

4. Haga clic en **Guardar** para aplicar los cambios.

### Cómo usar Citrix Casting con la aplicación Citrix Workspace

1. Inicie sesión en la aplicación Citrix Workspace y active Bluetooth en el dispositivo.

Se muestra la lista de hubs disponibles. La lista está ordenada por el valor RSSI del paquete de baliza de Workspace Hub.

2. Seleccione el dispositivo Workspace Hub para proyectar su pantalla y elija una de las siguientes opciones:

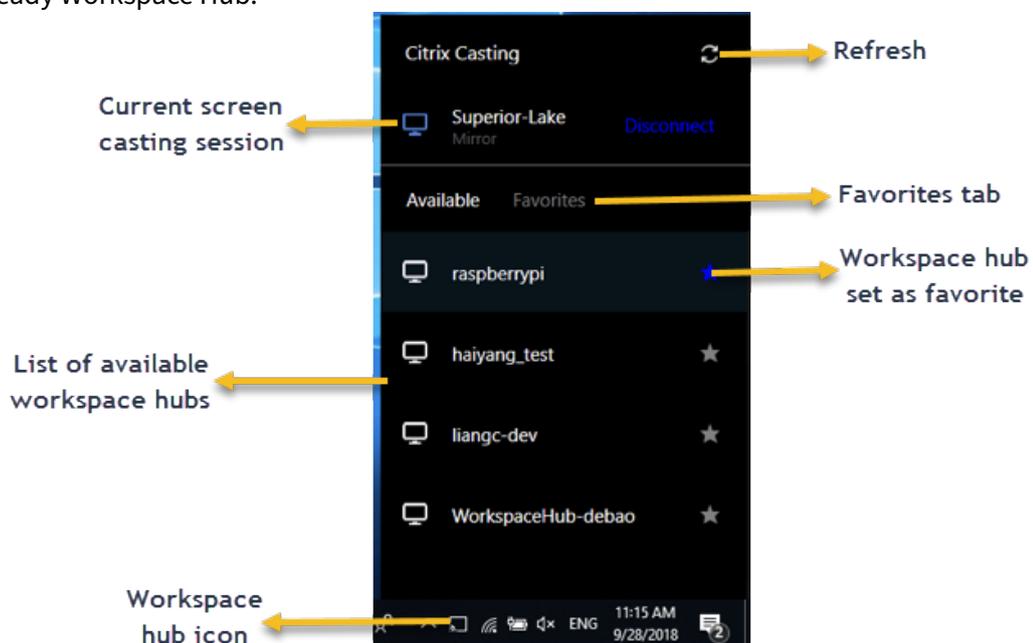
- **Mirror** (reflejar) para duplicar la pantalla principal y proyectarla en el dispositivo Workspace Hub conectado.
- **Extend** (extender) para usar la pantalla del dispositivo Workspace Hub como pantalla secundaria.

**Nota:**

Salir de la aplicación Citrix Workspace no implica salir de Citrix Casting.

En el cuadro de diálogo de **notificación de Citrix Casting**, están disponibles las siguientes opciones:

1. La sesión de proyección de pantalla actual se muestra en la parte superior.
2. Icono **Actualizar**.
3. **Desconectar** para detener la sesión de proyección de pantalla actual.
4. Icono con forma de estrella para agregar el Workspace Hub a los **favoritos**.
5. Haga clic con el botón secundario en el icono de Workspace Hub situado en el área de notificaciones y seleccione **Salir** para desconectar la sesión de proyección de pantalla y salir de Citrix Ready Workspace Hub.



### Lista de autocomprobación

Si la aplicación Citrix Workspace no puede detectar ni comunicarse con ningún Workspace Hub disponible dentro del alcance, debe llevar a cabo lo siguiente como parte de la autocomprobación:

1. La aplicación Citrix Workspace y Citrix Ready Workspace Hub están conectados a la misma red.
2. Bluetooth está habilitado y funciona correctamente en el dispositivo donde se ha iniciado la aplicación Citrix Workspace.
3. El dispositivo en el que se ha iniciado la aplicación Citrix Workspace se encuentra al alcance (a menos de 10 metros y sin ningún obstáculo, como paredes) de Citrix Ready Workspace Hub.

4. Inicie un explorador web en la aplicación Citrix Workspace y escriba `http://<hub_ip>:55555/device-details.xml` para comprobar que se muestran datos del dispositivo Workspace Hub.
5. Haga clic en el icono de **actualización** en Citrix Ready Workspace Hub e intente volver a conectarse al Workspace Hub.

### Problemas conocidos y limitaciones

1. Citrix Casting no funciona a menos que el dispositivo esté conectado a la misma red que Citrix Ready Workspace Hub.
2. En caso de problemas de red, puede haber una demora en la pantalla del dispositivo Workspace Hub.
3. Cuando selecciona **Extender**, la pantalla principal donde esté iniciada la aplicación Citrix Ready Workspace parpadea varias veces.
4. En el modo **Extender**, no se puede configurar la pantalla secundaria como pantalla principal.
5. La sesión de proyección de pantalla se desconecta automáticamente cuando hay algún cambio en la configuración de visualización en el dispositivo. Por ejemplo, un cambio en la resolución de la pantalla o un cambio en la orientación de la pantalla.
6. Durante la sesión de proyección de pantalla, si el dispositivo que ejecuta la aplicación Citrix Workspace se bloquea, se suspende o hiberna, aparece un error al iniciar sesión.
7. No se admiten las sesiones de proyección en varias pantallas.
8. La resolución de pantalla máxima admitida por Citrix Casting es 1920 x 1440.
9. Citrix Casting admite la versión 2.40.3839 de Citrix Ready Workspace Hub y versiones posteriores. Es posible que las versiones anteriores de Citrix Ready Workspace Hub no se detecten o causen un error de proyección.
10. Esta función no se ofrece en la aplicación Citrix Workspace para la Tienda Windows.
11. Puede que Citrix Casting en modo **Extender** no esté posicionado correctamente en Windows 10, compilación 1607.

### Redirección de dispositivos USB compuestos

#### Configurar la redirección de dispositivos USB compuestos:

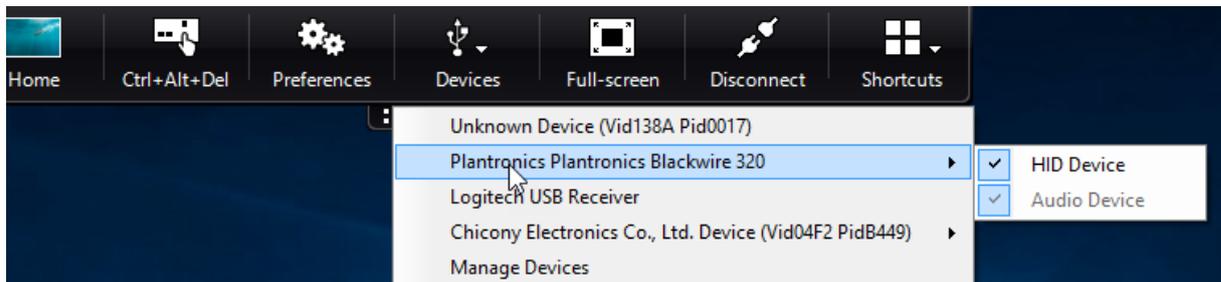
1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. En el nodo **Configuración del usuario**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Uso remoto de dispositivos cliente > Uso remoto de USB genérico**.
3. Seleccione la directiva **Dividir dispositivos**.
4. Seleccione **Habilitada**.

5. Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.

**Para permitir o denegar una interfaz:**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del usuario**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Uso remoto de dispositivos cliente > Uso remoto de USB genérico**.
3. Seleccione la directiva **Reglas de dispositivos USB**.
4. Seleccione **Habilitada**.
5. En el cuadro de texto **Reglas de dispositivos USB**, agregue el dispositivo USB que quiere permitir o denegar.  
Por ejemplo, `ALLOW: vid=047F pid=C039 split=01 intf=00,03` permite la interfaz 00 y 03, pero restringe las demás.
6. Haga clic en **Aplicar** y **Aceptar**.

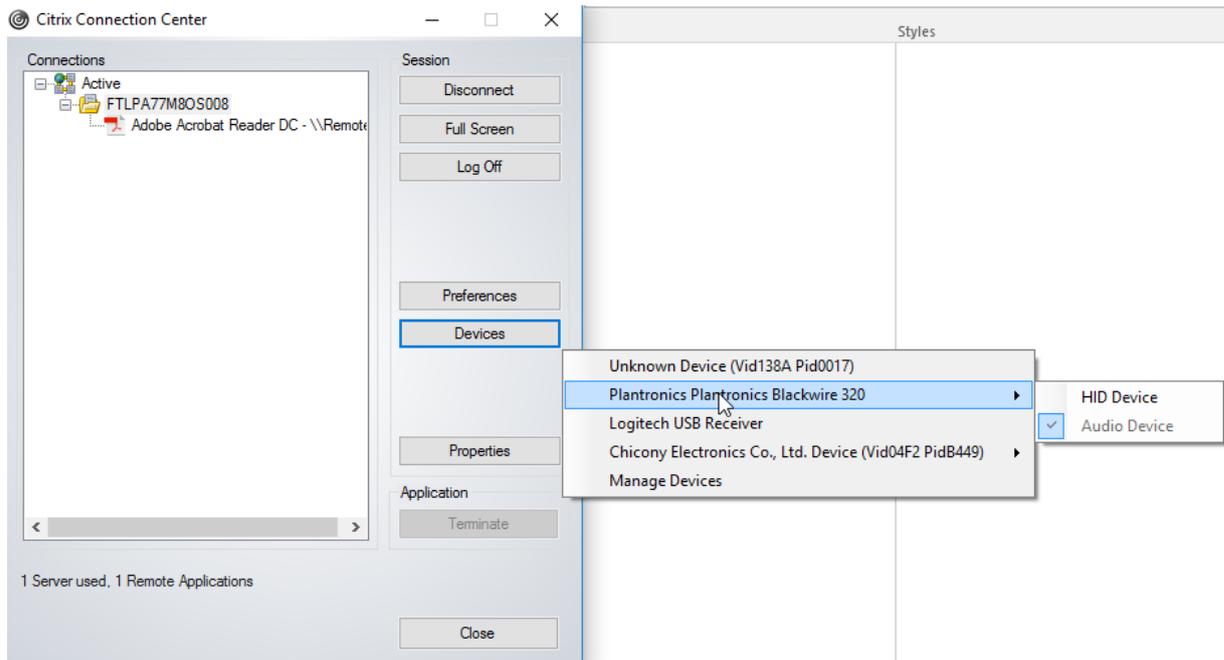
En una sesión de escritorio, los dispositivos USB divididos se muestran en Desktop Viewer, en **Dispositivos**. Además, los dispositivos USB divididos se pueden ver también en **Preferencias > Dispositivos**.



**Nota:**

Al dividir un dispositivo USB compuesto para la redirección de dispositivos USB genéricos, debe seleccionar el dispositivo desde Desktop Viewer o desde la Central de conexiones para redirigirlo.

En una sesión de aplicación, los dispositivos USB divididos se muestran en la **Central de conexiones**.



La siguiente tabla proporciona detalles sobre el comportamiento cuando se permite o se deniega una interfaz de USB.

**Para permitir una interfaz:**

Dividido	Interfaz	Acción
TRUE	Número válido 0 - n	Permitir la interfaz especificada
TRUE	Número no válido	Permitir todas las interfaces
FALSE	Cualquier valor	Permitir USB genérico del dispositivo principal
No especificada	Cualquier valor	Permitir USB genérico del dispositivo principal

Por ejemplo, SplitDevices- *true* indica que todos los dispositivos se dividen.

**Para denegar una interfaz:**

Dividido	Interfaz	Acción
TRUE	Número válido 0 - n	Denegar la interfaz especificada
TRUE	Número no válido	Denegar todas las interfaces

Dividido	Interfaz	Acción
FALSE	Cualquier valor	Denegar USB genérico del dispositivo principal
No especificada	Cualquier valor	Denegar USB genérico del dispositivo principal

Por ejemplo, `SplitDevices- false` indica que los dispositivos no se dividen con el número de la interfaz especificado.

Ejemplo: Mis auriculares *Plantronics*

#### Número de interfaz:

- Clase de interfaz de audio-0
- Clase de interfaz HID-3

Ejemplo de reglas que se usan para Mis auriculares *Plantronics*:

- PERMITIR: `vid=047F pid= C039 split=01 intf=00,03 /Allowed 00 and 03 interface, restrict others`
- DENEGAR: `vid=047F pid= C039 split=01 intf=00,03 / deny 00 and 03`

#### Limitación:

Citrix recomienda que no divida interfaces para una cámara web. Como solución alternativa, se puede redirigir el dispositivo a un dispositivo único mediante la redirección de USB genérico. Para obtener un mejor rendimiento, use el canal virtual optimizado.

#### Escalado de PPP

La aplicación Citrix Workspace permite que el sistema operativo controle la resolución de la sesión.

Puede aplicar PPP elevados en una sesión, pero la función está inhabilitada de forma predeterminada. Esto significa que el escalado de la sesión sigue la resolución del sistema operativo.

Puede configurar el escalado de PPP mediante las siguientes opciones:

1. Plantilla administrativa de objetos de directiva de grupo (configuración por equipo)
2. Preferencias avanzadas (configuración por usuario)

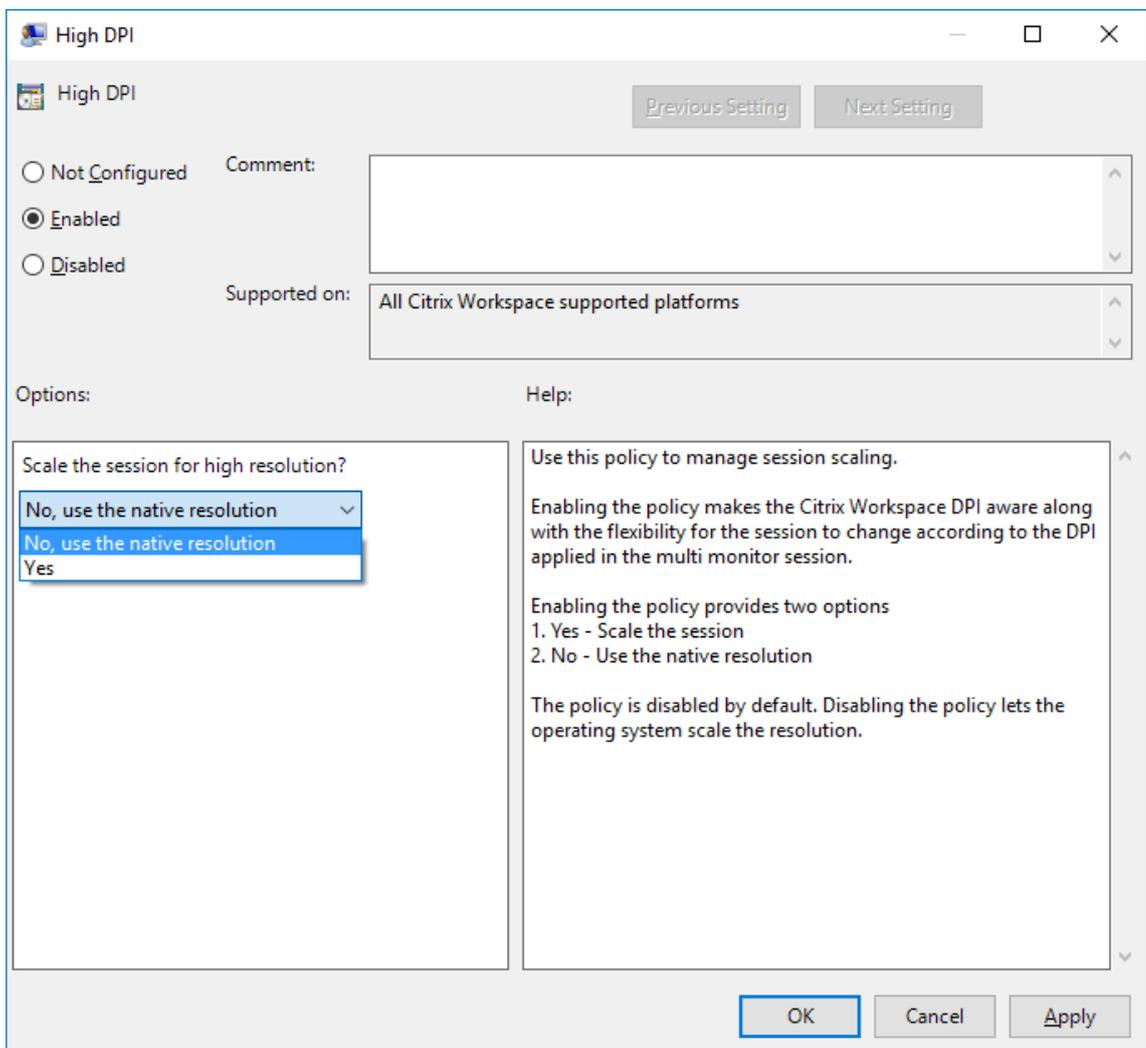
#### Limitaciones:

- Incluso con esta función habilitada, se ha observado una leve falta de definición en Desktop Viewer.

- En una sesión, cuando cambian los parámetros de PPP y se vuelve a iniciar la sesión, es posible que el tamaño de la ventana de la sesión no sea el adecuado. Como solución temporal, cambie el tamaño de la ventana de la sesión.

**Para configurar el ajuste de escala de PPP mediante la plantilla administrativa de GPO:**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > PPP**.
3. Seleccione la directiva **PPP elevados**.



4. Seleccione una de estas opciones:
  - a) Sí: Se aplican PPP elevados en una sesión.
  - b) No, usar la resolución nativa: El sistema operativo se encarga de configurar la resolución.

5. Haga clic en **Aplicar y Aceptar**.
6. Desde la línea de comandos, ejecute el comando `gpupdate /force` para aplicar los cambios.

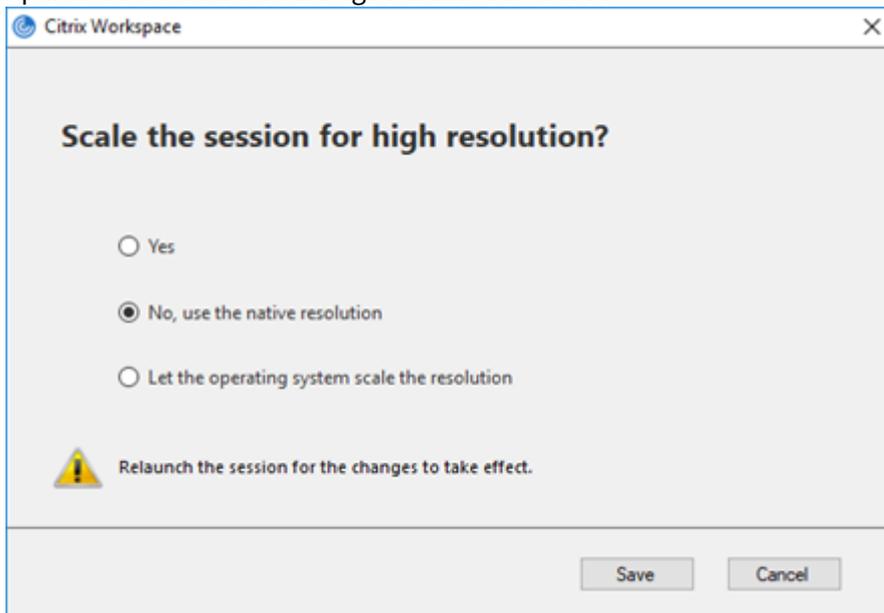
### Configurar el escalado de PPP mediante la interfaz gráfica de usuario:

#### Nota:

Puede ocultar total o parcialmente las opciones de la hoja “Preferencias avanzadas”, disponible desde el icono de la aplicación Citrix Workspace para Windows en el área de notificaciones. Para obtener más información, consulte [Hoja de Preferencias avanzadas](#).

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace situado en el área de notificaciones.
2. Seleccione **Preferencias avanzadas** y haga clic en **Parámetros de PPP**.

Aparecerá el cuadro de diálogo Parámetros de PPP.



3. Seleccione una de estas opciones:
  - a) Sí: Se aplican PPP elevados en una sesión.
  - b) No, usar la resolución nativa: La aplicación Citrix Workspace detecta los PPP en el VDA y los aplica.
  - c) De forma predeterminada está seleccionada la opción Dejar que el sistema operativo ajuste la resolución. Permite a Windows encargarse del escalado de PPP. Esta opción también significa que se inhabilita la directiva PPP elevados.
4. Haga clic en **Guardar**.
5. Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

## Opciones de escalado de PPP

Hay tres configuraciones posibles para el escalado de PPP en la aplicación Citrix Workspace: Escalado, Sin escalar y Escalado del sistema operativo. Los casos de uso para las diferentes configuraciones son los siguientes.

### **Escalado:**

El parámetro de escalado escala la resolución en el VDA de manera similar a la escala del sistema operativo, sin embargo, esta configuración admite escenarios mixtos de PPP. Esto corresponde al parámetro Sí de la interfaz de usuario, o la directiva de PPP elevados habilitada en la directiva de GPO. Este parámetro funciona bien para escenarios de PPP mixtos cuando se conecta a VDA modernos. Esta es la única forma de escalar sesiones integradas. El escalado puede causar un desenfoque en las imágenes, especialmente en el texto. Puede haber un bajo rendimiento al conectarse a VDA antiguos (6.5 o configurados para Gráficos antiguos). El Acceso a aplicaciones locales, RTOP y otros plug-ins que utilizan el posicionamiento de pantalla también puede presentar un rendimiento bajo. Las API no funcionan con el escalado. Por diseño, en este modo las aplicaciones integradas saltan de un monitor a otro para mantener la escala correcta.

Esta configuración se recomienda para usuarios en Windows 10 que se conectan a VDA modernos. Admite PPP mixtos sin ningún impacto adicional en los recursos del servidor.

### **Sin escalar:**

El parámetro Sin escalar envía la resolución completa de todos los monitores en la sesión. Estas resoluciones no tienen escala y puede dar como resultado texto e iconos pequeños en las aplicaciones y escritorios. Esto corresponde al parámetro No de la interfaz de usuario y la directiva de PPP elevados habilitada en el objeto de directiva de grupo (GPO). Este parámetro no causa ningún desenfoque debido al escalado, pero puede dar como resultado texto e iconos pequeños. Al conectarse a una sesión de escritorio, los PPP se pueden establecer dentro del VDA, lo que da como resultado el escalado que se busca. Esto no es posible en escritorios RDS ni en aplicaciones integradas. La habilitación de este parámetro provoca sesiones con mayor resolución que pueden afectar al rendimiento y la escalabilidad del servidor.

Este parámetro se recomienda para sesiones de escritorio que requieren la mejor calidad de imagen, donde se aceptan los recursos adicionales del servidor. También se puede utilizar en los casos en que el texto y los iconos pequeños no sean un problema para el usuario.

### **Escalado del sistema operativo:**

El escalado del sistema operativo es el predeterminada y corresponde al parámetro de la interfaz de usuario “Dejar que el sistema operativo ajuste la resolución”. La directiva de PPP elevados está inhabilitada en este caso. Esto permite que el sistema operativo Windows gestione el escalado de PPP para la sesión. La resolución del VDA se ajusta según los PPP, lo que resulta en una resolución más pequeña que el dispositivo cliente. Esto funciona bien para sesiones de un solo monitor y es eficiente cuando se conecta a 6.5 VDA o VDA configurados para Gráficos antiguos. Este método no es compatible con

PPP mixtos; todos los monitores deben tener los mismos PPP o la sesión no funciona. El escalado puede causar desenfoco en las imágenes, especialmente en el caso de texto. También puede haber problemas con el tamaño de los cursores en el sistema operativo Windows 10.

Esta configuración se recomienda para usuarios en dispositivos de punto final Windows 7 que se conectan a VDA antiguos. También se puede usar en Windows 10 si no hay PPP mixtos.

### Distribución de pantallas virtuales

Esta función permite definir un diseño de monitor virtual que se aplica al escritorio remoto. Asimismo, permite dividir virtualmente un solo monitor de cliente en hasta ocho monitores en el escritorio remoto. Puede configurar los monitores virtuales en la ficha **Distribución del monitor** en Desktop Viewer. Allí, puede dibujar líneas horizontales o verticales para separar la pantalla en monitores virtuales. La pantalla se divide en función de porcentajes especificados en la resolución del monitor cliente.

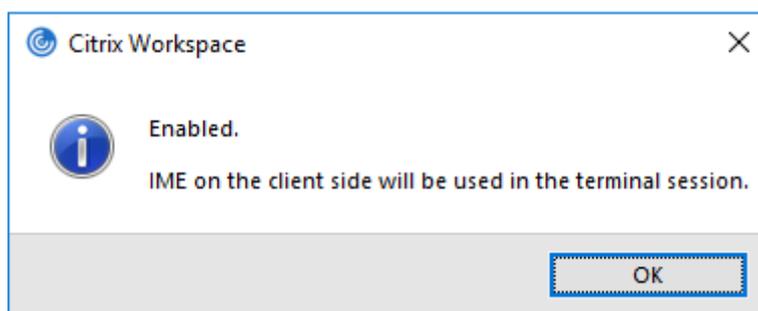
Puede establecer los PPP en los monitores virtuales que se utilizarán para el escalado de PPP o la correspondencia de PPP. Después de aplicar una distribución de monitores virtuales, cambie el tamaño o vuelva a conectarse a la sesión.

Esta configuración se aplica solo a sesiones de escritorio de un solo monitor y sesiones en pantalla completa, y no afecta a ninguna aplicación publicada. Esta configuración se aplica a todas las conexiones posteriores de ese cliente.

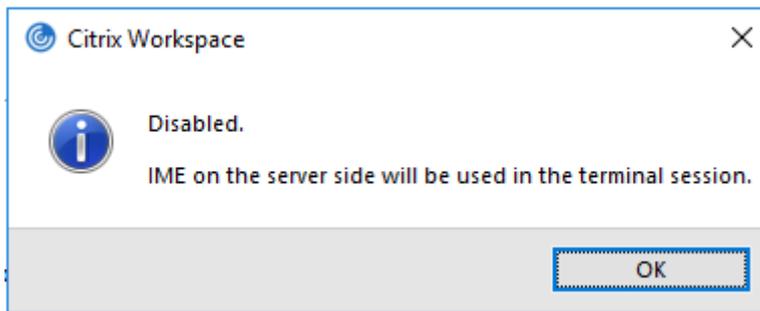
### Editores IME de cliente genérico

#### Configurar el IME de cliente genérico mediante la interfaz de línea de comandos:

- Para habilitar el IME de cliente genérico, ejecute el comando `wfica32.exe /localime:on` desde la carpeta de instalación de la aplicación Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`.



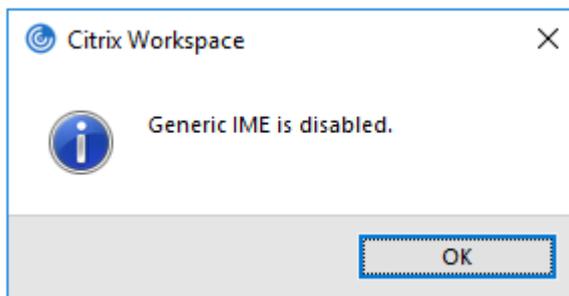
- Para inhabilitar el IME de cliente genérico, ejecute el comando `wfica32.exe /localime:off` desde la carpeta de instalación de la aplicación Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`.



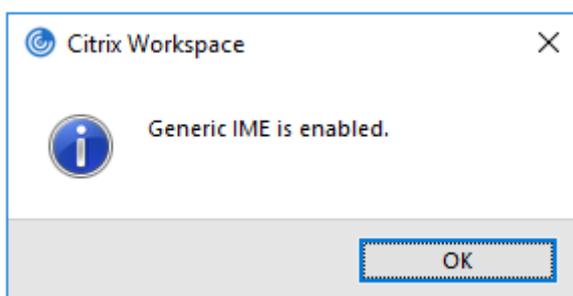
**Nota:**

Puede usar el modificador de línea de comandos `wfica32.exe /localime:on` para habilitar tanto el IME de cliente genérico como la sincronización de la distribución de teclado.

- Para inhabilitar el IME de cliente genérico, ejecute el comando `wfica32.exe /localgenericime:off` desde la carpeta de instalación de la aplicación Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`. Este comando no afecta a los parámetros de sincronización de distribución de teclado.



Si ha inhabilitado el IME de cliente genérico desde la interfaz de línea de comandos, puede habilitar la función de nuevo mediante el comando `wfica32.exe /localgenericime:on`.



**Activar/desactivar:**

La aplicación Citrix Workspace admite la activación o desactivación de esta función. Ejecute `wfica32.exe /localgenericime:on` para habilitarla o inhabilitarla. Sin embargo, los parámetros de sincronización de distribución de teclado tienen prioridad sobre este comando modificador. Si la sincronización de la distribución de teclado está **desactivada**, la activación con el conmutador no habilita el IME de cliente genérico.

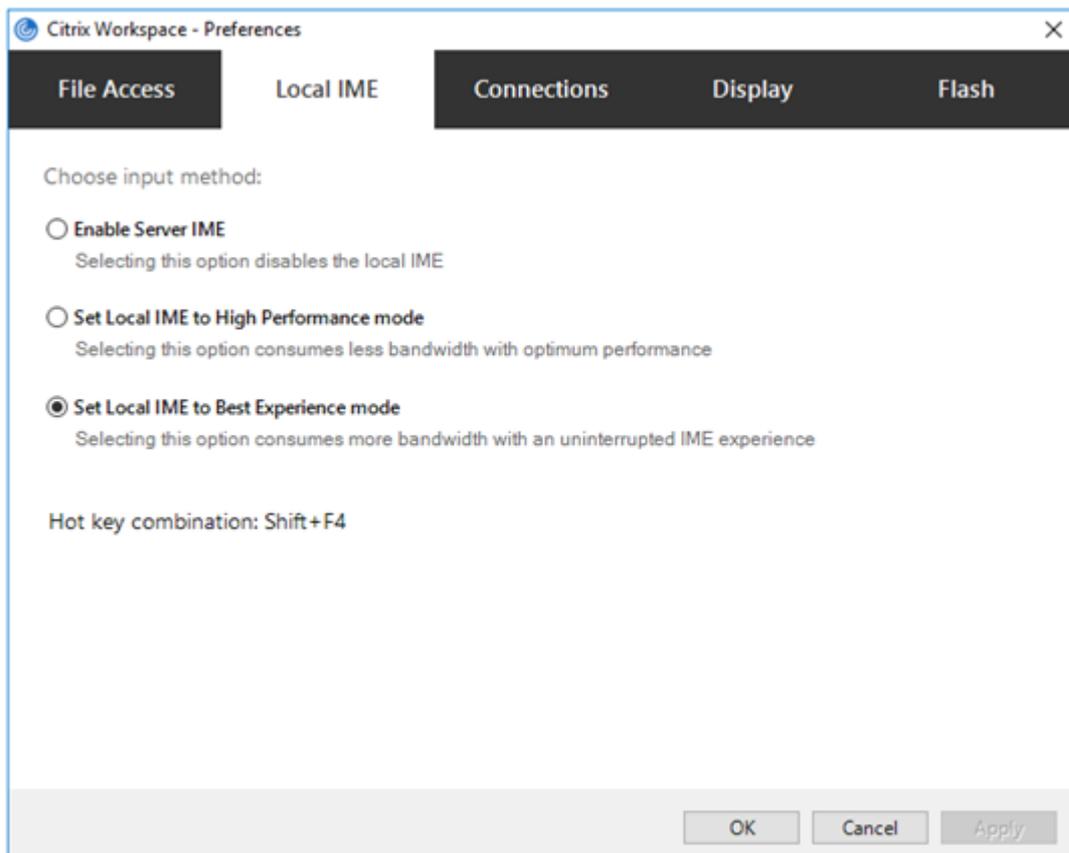
### Configurar el IME de cliente genérico mediante la interfaz gráfica de usuario:

El IME de cliente genérico requiere el VDA 7.13 o una versión más reciente.

La función de IME de cliente genérico se puede habilitar mediante la habilitación de la sincronización de la distribución de teclado. Para obtener más información, consulte [Sincronizar la distribución del teclado](#).

La aplicación Citrix Workspace permite configurar diferentes opciones para usar el IME de cliente genérico. Se puede seleccionar alguna de estas opciones en función de los requisitos y el uso.

1. En una sesión activa de aplicación, haga clic con el botón secundario en el icono de la aplicación Citrix Workspace en el área de notificaciones y seleccione **Central de conexiones**.
2. Seleccione **Preferencias** y haga clic en **IME local**.



Las siguientes opciones están disponibles para los distintos modos de IME:

1. **Habilitar IME del servidor:** Inhabilita el IME local y solo se pueden utilizar los idiomas establecidos en el servidor.
2. **Definir IME local en modo de alto rendimiento:** Usa el IME local con ancho de banda limitado. Esta opción restringe la funcionalidad de la ventana de candidatos.

3. **Definir IME local en modo de experiencia óptima:** Usa el IME local con la mejor experiencia de usuario. Esta opción consume mucho ancho de banda. De forma predeterminada, se selecciona esta opción cuando se habilita el IME de cliente genérico.

El cambio de parámetro se aplica solo en la sesión actual.

#### **Habilitar la configuración de teclas de acceso rápido mediante un editor del Registro:**

Cuando el IME de cliente genérico está habilitado, se puede usar **MAYÚS + F4** para seleccionar distintos modos de IME. Las diferentes opciones de modos IME aparecen en la esquina superior derecha de la sesión.

De forma predeterminada, la tecla de acceso rápido para el IME de cliente genérico está inhabilitada.

En el Editor del Registro, vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys`.

Seleccione **AllowHotKey** y cambie el valor predeterminado a 1.



#### **Limitaciones:**

- El IME de cliente genérico no admite las aplicaciones UWP (Universal Windows Platform) tales como IU de búsqueda y el explorador Edge del sistema operativo Windows 10. Como solución temporal, use el editor IME del servidor en su lugar.
- El editor IME genérico del cliente no es compatible con Internet Explorer 11 en **modo protegido**. Como solución temporal, puede inhabilitar el modo protegido en las **Opciones de Internet**. Para ello, haga clic en **Seguridad** y desmarque la casilla **Habilitar modo protegido**.

#### **Codificación de vídeo H.265**

La aplicación Citrix Workspace admite el uso del códec de vídeo H.265 para la aceleración de hardware de vídeos y gráficos remotos. Para utilizar esta función, es necesario que se admita y esté habilitada

tanto en el VDA como en la aplicación Citrix Workspace. Si la GPU en el punto final no admite la decodificación H.265 mediante la interfaz DXVA, la configuración de directiva “Decodificación H265 para gráficos” se ignora y la sesión recurre al códec de vídeo H.264.

#### Requisitos previos:

1. VDA 7.16 y versiones posteriores.
2. Habilite la directiva **Optimizar para cargas de trabajo de gráficos 3D** en el VDA.
3. Habilite la directiva **Usar codificación por hardware para códec de vídeo** en el VDA.

#### Nota:

La codificación H.265 solo se admite en las GPU de NVIDIA.

Esta función está **Inhabilitada** de forma predeterminada en la aplicación Citrix Workspace para Windows.

#### Configurar la aplicación Citrix Workspace para usar la codificación de vídeo H.265 mediante la plantilla administrativa de GPO de Citrix:

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Workspace > Experiencia de usuario**.
3. Seleccione la directiva **Decodificación H265 para gráficos**.
4. Seleccione **Habilitada**.
5. Haga clic en **Aplicar** y **Aceptar**.

#### Configurar la codificación de vídeo H.265 mediante el Editor del Registro:

##### Habilitar la codificación de vídeo H.265 en una red no unida a un dominio en un sistema operativo de 32 bits:

1. Abra el Editor del Registro mediante `regedit` en el comando Ejecutar.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Graphics Engine`.
3. Cree una clave DWORD con el nombre **EnableH265** y establezca el valor de esa clave en 1.

##### Habilitar la codificación de vídeo H.265 en una red no unida a un dominio en un sistema operativo de 64 bits:

1. Abra el Editor del Registro mediante `regedit` en el comando Ejecutar.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine`.
3. Cree una clave DWORD con el nombre `EnableH265` y establezca el valor de esa clave en 1.

Inicie la sesión de nuevo para que los cambios surtan efecto.

**Nota:**

- Si la directiva **Aceleración de hardware para gráficos** está inhabilitada en la plantilla administrativa de GPO de la aplicación Citrix Workspace para Windows, la configuración de directiva **Decodificación H265 para gráficos** se ignora y esta función no funciona.
- Ejecute la herramienta HDX Monitor 3.x para saber si el codificador de vídeo H.265 está habilitado dentro de las sesiones. Para obtener más información acerca de la herramienta HDX Monitor 3.x, consulte el artículo [CTX135817](#) de Knowledge Center.

## Barra de idioma y distribución del teclado

### Distribución del teclado

**Nota:**

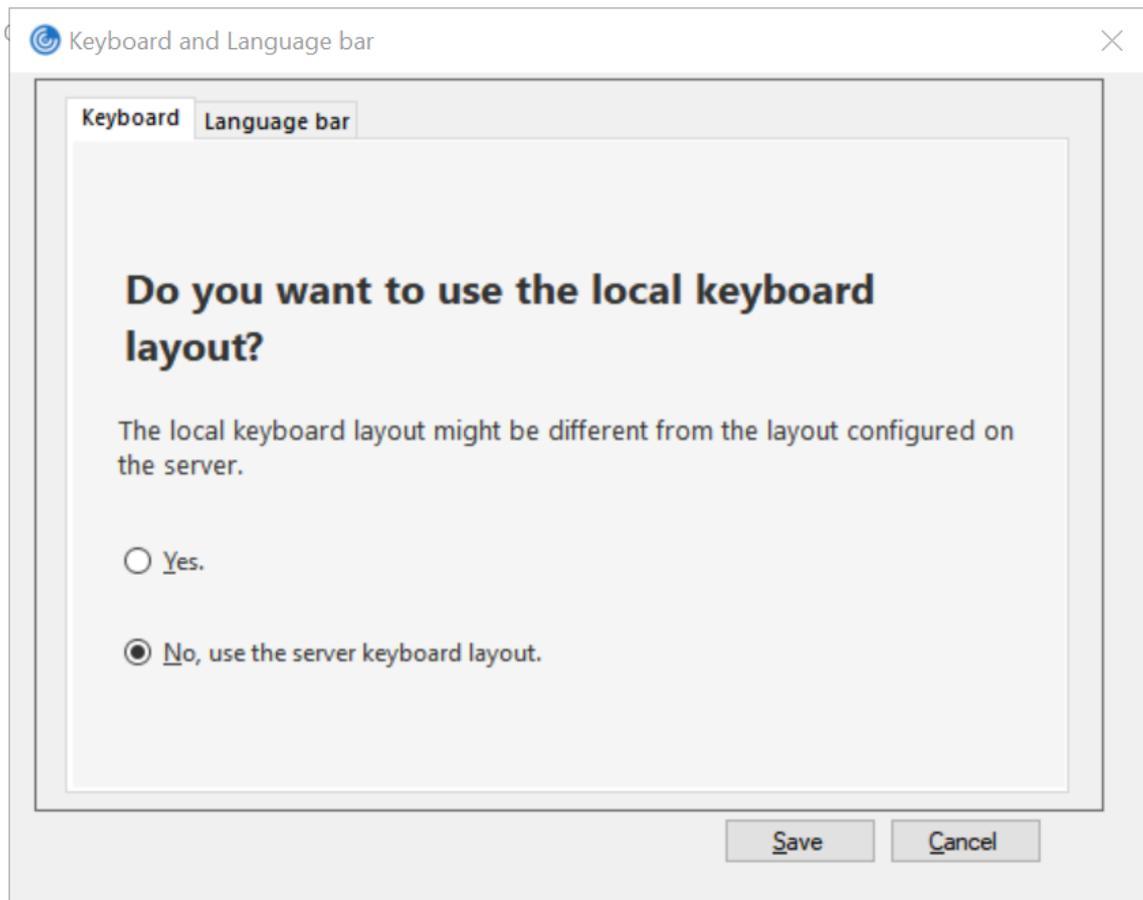
Puede ocultar total o parcialmente las opciones de la hoja de Preferencias avanzadas, disponible en el icono de la aplicación Citrix Workspace del área de notificaciones. Para obtener más información, consulte [Hoja de Preferencias avanzadas](#).

La sincronización de la distribución del teclado permite a los usuarios cambiar entre distintas distribuciones de teclado preferidas en el dispositivo cliente. Esta función está inhabilitada de forma predeterminada.

#### Para habilitar la sincronización de la distribución del teclado:

1. Desde el icono de la aplicación Citrix Workspace del área de notificaciones, seleccione **Preferencias avanzadas > Barra de idioma y teclado**.

Aparecerá el cuadro de diálogo Barra de idioma y teclado.



2. Seleccione una de estas opciones:

- Sí: Se usa la distribución del teclado local en una sesión.
- No; usar la distribución de teclado del servidor: Se aplica a la sesión la distribución del teclado utilizado en el VDA. Esta opción inhabilita la función de distribución del teclado local.

3. Haga clic en **Guardar**.

También puede habilitar e inhabilitar la sincronización de la distribución del teclado mediante la línea de comandos. Para ello, ejecute `wfica32:exe /localime:on` o `wfica32:exe /localime:off` desde la carpeta de instalación de la aplicación Citrix Workspace para Windows `C:\Program files (x86)\Citrix\ICA Client`.

La opción de distribución de teclado local activa el IME (Input Method Editor) del cliente. Si los usuarios que trabajan en japonés, chino y coreano prefieren usar el editor IME del servidor, deben inhabilitar la opción de distribución del teclado local. Para ello, pueden seleccionar la opción **No** o ejecutar `wfica32:exe /localime:off`. La sesión recurrirá a la distribución de teclado que suministre el servidor remoto cuando se conecten a la sesión siguiente.

En ocasiones, el cambio a la distribución de teclado del cliente no tiene efecto en una sesión activa.

Para resolver este problema, cierre la sesión en la aplicación Citrix Workspace y vuelva a iniciarla.

### **Ocultar el diálogo de notificación del cambio de distribución del teclado:**

El diálogo de notificación de cambio de distribución del teclado permite saber si la sesión VDA cambia la distribución del teclado. Para que el cambio de distribución del teclado se efectúe, se necesitan aproximadamente dos segundos. Tras ocultar el cuadro de diálogo de notificación, espere un tiempo antes de comenzar a escribir para evitar la introducción de caracteres incorrectos.

#### **Advertencia**

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

### **Ocultar el diálogo de notificación del cambio de distribución del teclado mediante el Editor del Registro:**

1. Abra el Editor del Registro y vaya a `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Cree una clave de valor de cadena con el nombre **HideNotificationWindow**.
3. Establezca DWORD con el valor **1**.
4. Haga clic en **Aceptar**.
5. Inicie la sesión de nuevo para que los cambios surtan efecto.

#### **Limitaciones:**

- Las aplicaciones remotas que se ejecutan con privilegios elevados (por ejemplo, hacer clic con el botón secundario en el icono de una aplicación y elegir la opción “Ejecutar como administrador”) no se pueden sincronizar con la distribución de teclado del cliente. Como solución temporal, cambie manualmente la distribución del teclado en el lado del servidor (VDA) o inhabilite el Control de cuentas de usuario (UAC).
- Si el usuario cambia la distribución de teclado en el cliente por una distribución que no se admite en el servidor, la función de sincronización de la distribución del teclado se inhabilitará por razones de seguridad, ya que una distribución de teclado no reconocida se trata como una potencial amenaza de seguridad. Para restaurar la función de la sincronización de distribución del teclado, cierre la sesión y vuelva a iniciarla.
- En una sesión RDP, no se puede cambiar la distribución del teclado con los accesos directos Alt + Mayús. Como solución temporal, use la barra de idioma en la sesión RDP para cambiar la distribución del teclado.
- Esta función está inhabilitada en Windows Server 2016 debido a un problema de terceros que podría introducir un riesgo para el rendimiento. La función se puede habilitar mediante un

parámetro de Registro en el VDA: en `HKEY_LOCAL_MACHINE\Software\Citrix\ICA\IcaIme`, agregue una nueva clave llamada **DisableKeyboardSync** y establezca el valor en 0.

## Barra de idioma

La barra de idioma muestra el idioma de entrada preferido en una sesión. En versiones anteriores, solo podía cambiar esta configuración mediante las claves de Registro en el VDA. A partir de Citrix Receiver para Windows 4.11, puede cambiar la configuración desde el cuadro de diálogo **Preferencias avanzadas**. La barra de idioma aparece en una sesión de forma predeterminada.

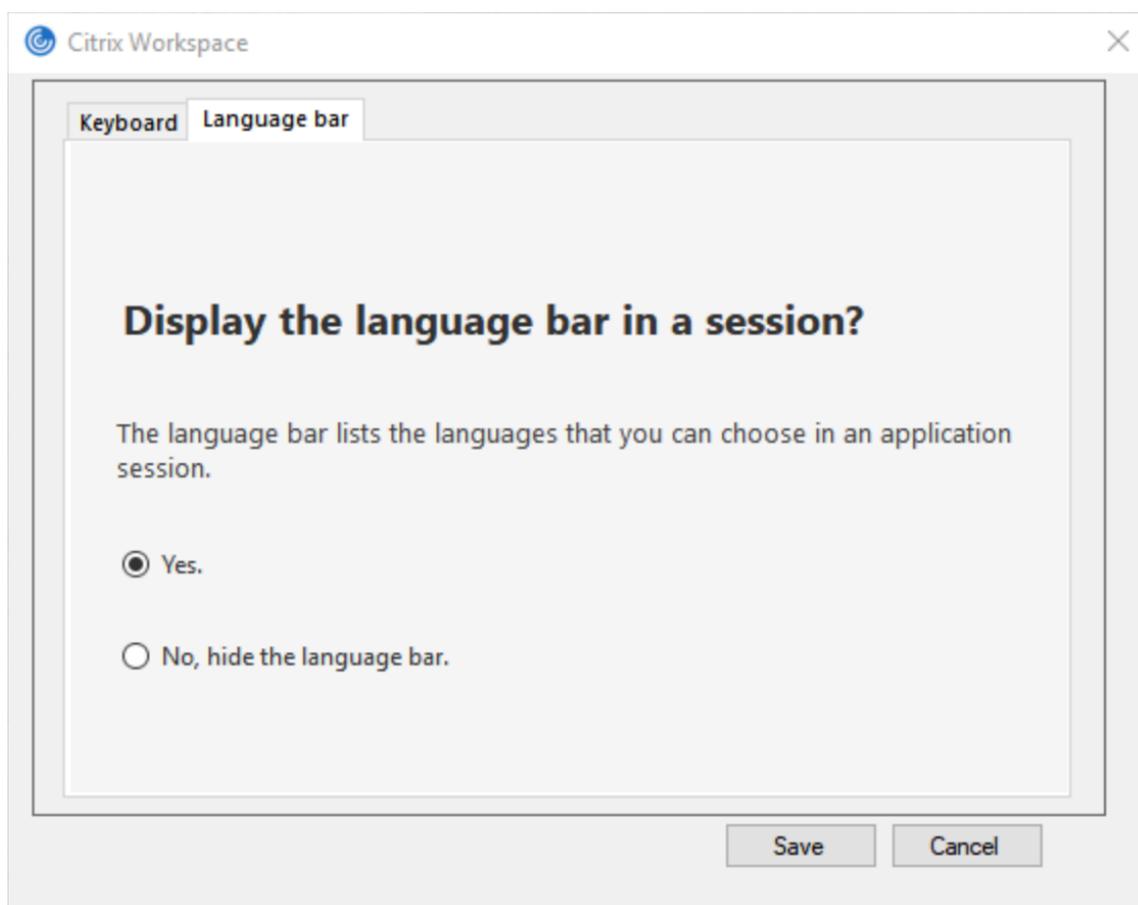
### Nota:

Esta función está disponible en sesiones con VDA 7.17 y versiones posteriores.

### Definir si mostrar u ocultar la barra de idioma remota:

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace en el área de notificaciones y seleccione **Preferencias avanzadas**.
2. Seleccione **Barra de idioma y teclado**.
3. Seleccione la ficha **Barra de idioma**.
4. Seleccione una de estas opciones:
  - a) Sí: La barra de idioma se muestra en una sesión.
  - b) No; ocultar la barra de idioma: La barra de idioma se oculta en una sesión.
5. Haga clic en **Guardar**.

Los cambios de configuración surten efecto de inmediato.



**Nota:**

- Puede cambiar la configuración en una sesión activa.
- La barra de idioma remota no aparece en una sesión si solo hay un idioma de entrada.

**Ocultar la barra de idioma en la hoja de Preferencias avanzadas:**

Puede utilizar el Registro para ocultar la ficha de la barra de idioma a fin de que esta no aparezca en la hoja **Preferencias avanzadas**.

1. Abra el Editor del Registro.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LocalIME`.
3. Cree una clave de valor DWORD, **ToggleOffLanguageBarFeature**, y establézcala en **1** para ocultar la opción de barra de idioma en la hoja “Preferencias avanzadas”.

**Compatibilidad con USB**

Si se admite USB, se permite interactuar con una amplia variedad de dispositivos USB en una conexión a Citrix Virtual Apps and Desktops y Citrix DaaS. Puede conectar dispositivos USB a sus

equipos y esos dispositivos se pueden usar de manera remota en el escritorio virtual. 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. Mediante una preferencia de la barra de herramientas, los usuarios de Desktop Viewer pueden controlar si los dispositivos USB se encuentran disponibles en aplicaciones y escritorios de Citrix Virtual Apps and Desktops y Citrix DaaS.

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. Esto permite a estos dispositivos interactuar con paquetes tales como Microsoft Office Communicator y Skype.

Los siguientes tipos de dispositivos se admiten directamente en una sesión de aplicaciones y escritorios virtuales, y por lo tanto no ofrecen la funcionalidad USB:

- Teclados
- Mouse
- Tarjetas inteligentes

Los dispositivos USB especializados (por ejemplo, los teclados Bloomberg y mouse 3D) pueden configurarse para utilizar la funcionalidad USB. Para obtener información sobre cómo configurar los teclados Bloomberg, consulte

[Configurar teclados Bloomberg](#).

Para obtener información sobre cómo configurar reglas de directivas para otros dispositivos USB especializados, consulte el artículo [CTX122615](#) en Knowledge Center.

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 y Citrix DaaS. 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 aplicaciones y escritorios virtuales:

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

Los dispositivos USB conectados a un concentrador se pueden conectar remotamente pero no se puede conectar el concentrador propiamente dicho.

Los siguientes tipos de dispositivos USB no se admiten de forma predeterminada en sesiones de Citrix Virtual Apps:

- Dispositivos Bluetooth
- Tarjetas de interfaz de red integradas
- Hubs USB
- Adaptadores gráficos USB
- Dispositivos de sonido
- Dispositivos de almacenamiento masivo

### **Funcionamiento de la compatibilidad con USB:**

Cuando un usuario conecta un dispositivo USB, éste se comprueba con la directiva USB y, si se lo admite, se lo coloca en comunicación remota con el escritorio virtual. Si la directiva predeterminada rechaza el dispositivo, solo estará disponible para el escritorio local.

Cuando un usuario conecta un dispositivo USB, se muestra una notificación para informar al usuario sobre el nuevo dispositivo. El usuario puede decidir qué dispositivos USB se comunican de forma remota con el escritorio virtual seleccionando los dispositivos de la lista cada vez que se conectan. También, el usuario puede configurar la compatibilidad con USB para que todos los dispositivos USB que se conecten antes o durante una sesión se comuniquen automáticamente de forma remota con el escritorio virtual que esté en primer plano.

### **Dispositivos de almacenamiento masivo**

Solo para dispositivos de almacenamiento masivo, además de la funcionalidad USB, el acceso remoto está disponible mediante la asignación de unidades del cliente. Esta asignación se configura a través de la siguiente directiva de la aplicación Citrix Workspace para Windows: **Comunicación remota de dispositivos cliente > Asignación de unidades de cliente**. Cuando se aplica esta directiva, en el momento en que los usuarios inician sesión, las unidades del dispositivo del usuario se asignan automáticamente a las letras de las unidades del escritorio virtual. Las unidades se muestran como carpetas compartidas con letras de unidades asignadas.

Las principales diferencias entre los dos tipos de directivas de comunicación remota son las siguientes:

---

Función	Asignación de unidades del cliente	Compatibilidad con USB
Habilitada de forma predeterminada	Sí	No
Configuración para acceso de solo lectura	Sí	No
Dispositivo para quitar con seguridad durante una sesión	No	Sí, si un usuario hace clic en Quitar hardware con seguridad en el área de notificaciones

---

Si se habilitan las directivas “USB genérico” y “Asignación de unidades del cliente”, y se inserta un dispositivo de almacenamiento masivo antes del inicio de una sesión, ese dispositivo se redirigirá primero mediante la asignación de unidades del cliente, antes de ser considerado para la redirección de USB genérico. Si se inserta después del inicio de una sesión, se redirigirá a través de la compatibilidad con USB antes de la asignación de unidades del cliente.

### **Clases de dispositivos USB que se admiten de manera predeterminada:**

Las reglas de directivas USB predeterminadas admiten distintas clases de dispositivos USB:

A pesar de incluirse en esta lista, algunas clases están solo disponibles de forma remota en las sesiones de aplicaciones y escritorios virtuales después de una configuración adicional. Estos parámetros no se pueden configurar.

- **Audio (clase 01):** Incluye los dispositivos de entrada de audio (micrófonos), los dispositivos de salida de audio y los controladores MIDI. Los dispositivos de sonido modernos generalmente utilizan transferencias isócronas, que son compatibles con XenDesktop 4 o posterior. El audio (clase 01) no es aplicable a Citrix Virtual Apps, ya que estos dispositivos no están disponibles para la comunicación remota en Citrix Virtual Apps mediante la funcionalidad USB.

#### **Nota:**

Algunos dispositivos específicos (por ejemplo, teléfonos VOIP) requieren una configuración adicional. Para obtener más información, consulte el artículo [CTX123015](#) de Knowledge Center.

- **Dispositivos de interfaz física (clase 05):** Estos dispositivos son similares a los dispositivos de interfaz de usuario (HID) pero, en general, proporcionan respuesta o información en “tiempo real”. Pueden ser joysticks con fuerza de respuesta, plataformas de movimiento y exoesqueletos con fuerza de respuesta.
- **Digitalización de imágenes fijas (clase 06):** Escáneres y 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 y puede ser posible configurar una cámara para que utilice cualquiera de las clases mediante los menús de configuración que proporciona la cámara propiamente dicha.

#### **Nota:**

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

#### Nota

Esta clase de dispositivo (en particular, impresoras con funciones de escaneado) requiere configuración adicional. Para obtener instrucciones, consulte el artículo [CTX123015](#) de Knowledge Center.

- **Almacenamiento masivo (clase 08):** Los dispositivos de almacenamiento masivo más comunes son las unidades flash USB. Otros son 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 y que incluyen los reproductores multimedia, las cámaras digitales y los teléfonos celulares. El almacenamiento masivo (clase 08) no es aplicable a Citrix Virtual Apps, ya que estos dispositivos no están disponibles para la comunicación remota en Citrix Virtual Apps mediante la funcionalidad USB. 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 usa 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.

- **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.
- **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, convertidores de vídeo analógico, algunos sintonizadores de televisión y algunas cámaras digitales que admiten el streaming de vídeo.

#### Importante

La mayoría de los dispositivos de streaming por vídeo utilizan transferencias isócronas, que son compatibles con XenDesktop 4 o posterior. Algunos dispositivos de vídeo (por ejemplo, cámaras

web con detección de movimiento) requieren una configuración adicional. Para obtener instrucciones, consulte el artículo [CTX123015](#) de Knowledge Center.

- **Atención médica personal (clase 0f):** 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 que se rechazan de manera predeterminada

Las siguientes clases de dispositivo USB se rechazan por las reglas de directiva de USB predeterminadas:

- Comunicaciones y control CDC (clases 02 y 0a). La directiva USB predeterminada no permite estos dispositivos porque es posible que uno de ellos proporcione la conexión al propio escritorio virtual.
- 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 mouse.

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 gestionan de manera apropiada sin funcionalidad USB y a que normalmente es necesario utilizar estos dispositivos de forma local y de forma remota cuando se conecta con 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 tarjeta inteligente abarcan los lectores de tarjeta inteligente con contacto y sin contacto, y los tokens USB con un chip inteligente incluido que equivale a la tarjeta.

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

- Controlador inalámbrico (clase e0). Es posible que algunos de estos dispositivos proporcionen acceso de red crítico o conecten periféricos importantes, tales como mouse o teclados Bluetooth.

La directiva USB predeterminada no permite estos dispositivos. No obstante, es posible que haya dispositivos concretos para los que sea apropiado dar acceso mediante la funcionalidad USB.

- **Varios dispositivos de red (clase ef, subclase 04):** Algunos de estos dispositivos pueden ofrecer un acceso peligroso a la red. La directiva USB predeterminada no permite estos dispositivos. No obstante, es posible que haya dispositivos concretos para los que sea apropiado dar acceso mediante la funcionalidad USB.

### Actualizar la lista de dispositivos USB disponibles para la comunicación remota

Puede actualizar el rango de dispositivos USB disponibles para la comunicación remota con los escritorios. Para ello, deberá modificar el archivo de plantilla de Citrix Workspace para Windows. Con ello, puede realizar cambios en Citrix Workspace para Windows mediante la directiva de grupo. El archivo se localiza en la carpeta de instalación siguiente:

```
\C:\Program Files\Citrix\ICA Client\Configuration\en.
```

También puede modificar el Registro en cada dispositivo de usuario y agregar la siguiente clave de Registro:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB  
Type=String Name="DeviceRules"Value=
```

#### Importante

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Las reglas predeterminadas del producto se almacenan en:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB Tipo=MultiSz Nombre="DeviceRules"Valor=
```

No modifique las reglas predeterminadas del producto.

Para obtener más información acerca de la configuración de directivas de dispositivos USB, consulte [Configuraciones de directiva de Dispositivos USB](#) en la documentación de Citrix Virtual Apps and Desktops.

## Configurar el sonido USB

### Nota:

- Si instala o actualiza la versión de la aplicación Citrix Workspace para Windows por primera vez, agregue los archivos de plantilla más recientes al GPO local. Para obtener más información sobre cómo agregar los archivos de plantilla al GPO local, consulte [Plantilla administrativa de objeto de directiva de grupo](#). En caso de una actualización de versión, la configuración existente se conserva al importar los archivos más recientes.
- Esta función solo está disponible en el servidor Citrix Virtual Apps.

### Para configurar dispositivos de audio USB:

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Workspace > Experiencia de usuario** y seleccione **Audio a través de redirección de USB genérico**.
3. Modifique los parámetros.
4. Haga clic en **Aplicar** y **Aceptar**.
5. Abra el símbolo del sistema en modo de administrador.
6. Ejecute el comando siguiente  
`gpupdate /force`.

## Iniciar vPrefer

En las versiones anteriores, podía especificar que se iniciara preferentemente la instancia de una aplicación instalada en el VDA (denominada “instancia local” en este documento) antes que la aplicación publicada. Para ello, configuraba el atributo `KEYWORDS:prefer=` atributo “application” en **Citrix Studio**.

A partir de la versión 4.11, en una situación de doble salto (donde la aplicación Citrix Workspace se ejecuta en el VDA que aloja su sesión), puede controlar si Workspace inicia la instancia local de una aplicación instalada en el VDA (si está disponible como aplicación local) en lugar de iniciar una instancia alojada de la aplicación.

vPrefer está disponible en StoreFront 3.14, Citrix Virtual Desktops 7.17 y versiones posteriores.

Al iniciar la aplicación, la aplicación Citrix Workspace lee los datos de los recursos presentes en el servidor de StoreFront y aplica la configuración en función del indicador **vPrefer** en el momento de la enumeración. La aplicación Citrix Workspace busca la ruta de instalación de la aplicación en el Registro de Windows del VDA y, si está presente, inicia la instancia local de la aplicación. De lo contrario, se inicia una instancia alojada de la aplicación.

Si inicia una aplicación que no está instalada en el VDA, se inicia la aplicación alojada. Para obtener más información sobre cómo se gestiona el inicio local en StoreFront, consulte [Controlar el inicio de aplicaciones locales en escritorios publicados](#) en la documentación de Citrix Virtual Apps and Desktops.

Si no quiere que la instancia local de la aplicación se inicie en el VDA, establezca **LocalLaunchDisabled** en **True** mediante PowerShell en el Delivery Controller. Para obtener más información, consulte la documentación de [Citrix Virtual Apps and Desktops](#).

Esta función ayuda a iniciar aplicaciones más rápido, proporcionando así una mejor experiencia de usuario. Puede configurarla mediante la plantilla administrativa del objeto de directiva de grupo (GPO). De forma predeterminada, vPrefer se habilita solo en una situación de doble salto.

**Nota:**

Si instala o actualiza la versión de la aplicación Citrix Workspace por primera vez, agregue los archivos de plantilla más recientes al GPO local. Para obtener más información sobre cómo agregar los archivos de plantilla al GPO local, consulte [Plantilla administrativa de objeto de directiva de grupo](#). En caso de una actualización de versión, la configuración existente se conserva al importar los archivos más recientes.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Autoservicio**.
3. Seleccione la directiva **vPrefer**.
4. Seleccione **Habilitada** y, en el menú desplegable **Permitir aplicaciones**, seleccione una de las siguientes opciones:
  - **Permitir todas las aplicaciones:** Esta opción inicia la instancia local de todas las aplicaciones presentes en el VDA. La aplicación Citrix Workspace busca la aplicación instalada (incluidas las aplicaciones nativas de Windows, como el Bloc de notas, la Calculadora, el WordPad, el símbolo del sistema) e inicia la aplicación que haya en el VDA, en lugar de iniciar la aplicación alojada.
  - **Permitir aplicaciones instaladas:** Esta opción inicia la instancia local de las aplicaciones instaladas que haya presentes en el VDA. Si la aplicación no está instalada en el VDA, se inicia la aplicación alojada. De forma predeterminada, se selecciona la opción **Permitir aplicaciones instaladas** cuando se **habilita** la directiva **vPrefer**. Esta opción excluye las aplicaciones nativas del sistema operativo Windows, como el Bloc de notas, la Calculadora, etc.
  - **Permitir aplicaciones de red:** Esta opción inicia la instancia de una aplicación que esté publicada en una red compartida.
5. Haga clic en **Aplicar** y **Aceptar**.

6. Inicie la sesión de nuevo para que los cambios surtan efecto.

**Limitación:**

- Workspace para Web no admite esta función.

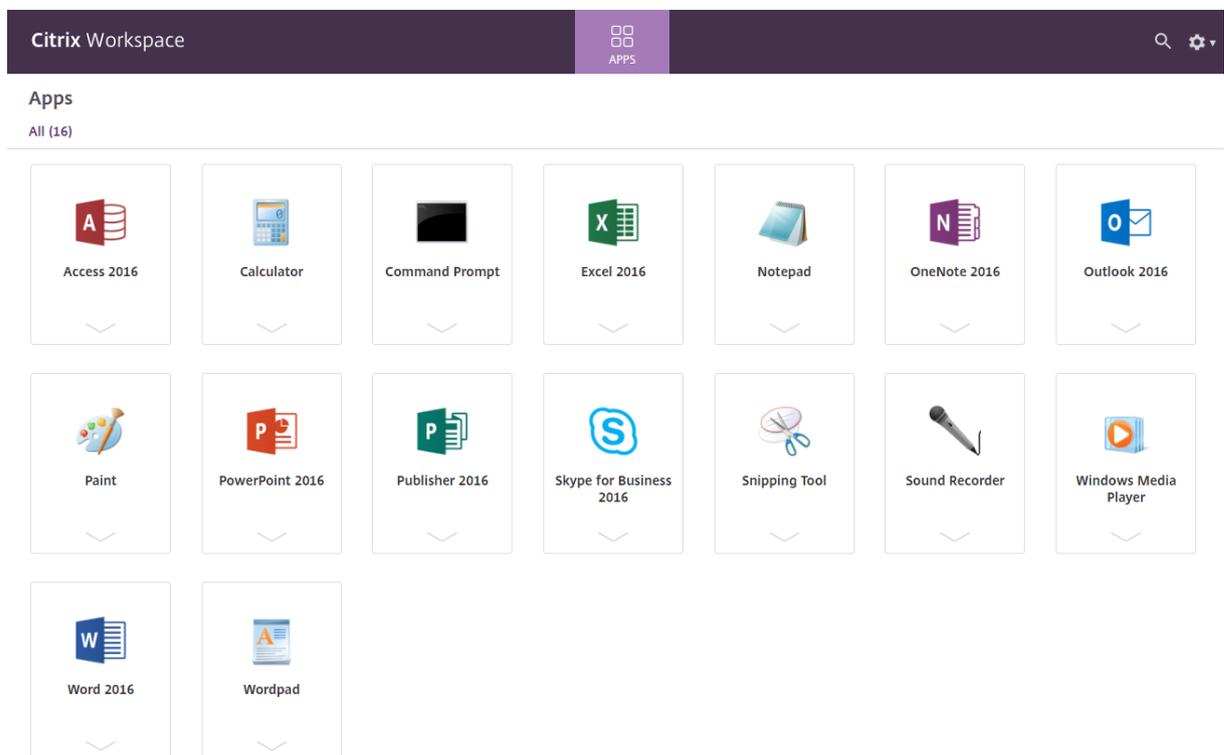
**Configuración de Workspace**

La aplicación Citrix Workspace para Windows admite la configuración de espacios de trabajo (Workspace) para los suscriptores, que pueden estar usando uno o varios servicios disponibles en Citrix Cloud.

La aplicación Citrix Workspace mostrará de forma inteligente solo los recursos específicos del espacio de trabajo a los que tienen derecho los usuarios. Todos los recursos del espacio de trabajo digital disponibles en la aplicación Citrix Workspace son alimentados por el servicio de experiencia de Citrix Cloud Workspace.

Un espacio de trabajo (Workspace) forma parte de una solución de espacio de trabajo digital que permite a los departamentos de TI entregar de manera segura un acceso a aplicaciones desde cualquier dispositivo.

Esta captura de pantalla es un ejemplo de un espacio de trabajo tal y como lo ven los suscriptores. El diseño de esta interfaz está evolucionando y es posible que no sea exactamente igual a la interfaz que estén usando actualmente sus suscriptores. Por ejemplo, puede figurar “StoreFront” en la parte superior de la página en lugar de “Workspace”.



## Aplicaciones SaaS

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 Windows 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.

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.

### Requisitos previos:

- La aplicación SaaS debe admitir la autenticación SAML 2.0 para poder aplicar la función Single Sign-On.
- La opción **Habilitar seguridad mejorada** debe estar habilitada en el servicio de control de acceso (Access Control Service) para que Citrix Enterprise Browser (antes denominado Citrix Workspace Browser) para generar la aplicación SaaS. Si esta opción no está habilitada, las aplicaciones SaaS se inician con el explorador predeterminado tal y como se ha establecido en el cliente.

#### Nota:

La aplicación Citrix Workspace agrega las aplicaciones y los escritorios que se publican tanto en entornos locales como en la nube para una experiencia de usuario unificada.

La aplicación Citrix Workspace incluye el explorador Citrix Secure Browser para iniciar las aplicaciones SaaS. El framework incrustado de Chromium sobre el que se construyó Citrix Secure Browser se ha actualizado a la versión 70. Eso se traduce en una mejor experiencia de usuario al acceder a aplicaciones SaaS seguras.

#### Nota:

- En el caso de Workspace para Web, las aplicaciones SaaS solo se inician en el explorador predeterminado como se haya establecido en el cliente, no en el explorador Citrix Secure Browser.
- La experiencia del usuario entre una aplicación de sesión ICA y una aplicación SaaS segura

puede variar.

El explorador Citrix Secure Browser admite operaciones como la barra de herramientas, el portapapeles, Imprimir, Descargar y Marca de agua. Estas operaciones se aplican en la aplicación Citrix Workspace como se define en la configuración de directivas en el servicio de control de acceso (ACS).

### **Operaciones que puede realizar mediante el explorador Citrix Secure Browser:**

**Barra de herramientas:** Cuando la opción de barra de herramientas está habilitada en una aplicación, verá las opciones “Atrás”, “Adelante” y “Actualizar” en la aplicación iniciada. La barra de herramientas también muestra puntos suspensivos, donde se incluyen las operaciones del portapapeles.

**Portapapeles:** Cuando el acceso al portapapeles está habilitado en una aplicación, puede utilizar las opciones “Cortar”, “Copiar” y “Pegar” que aparecen en la barra de herramientas de la aplicación iniciada. Cuando la opción está inhabilitada, las opciones “Cortar”, “Copiar” y “Pegar” aparecen atenuadas.

**Imprimir:** Puede ejecutar un comando de impresión en la aplicación iniciada si la opción de impresión está habilitada. Cuando está inhabilitada, la opción de impresión no aparece en la aplicación iniciada.

**Navegación:** El icono siguiente y el icono anterior aparecen en la barra de herramientas de la aplicación iniciada si la opción de navegación está habilitada.

**Descargar:** Puede descargar archivos de la aplicación iniciada si la opción de descarga está habilitada. Haga clic con el botón secundario en la aplicación iniciada y seleccione **Guardar como**. Vaya a la ubicación conveniente y haga clic en **Descargar**.

#### **Nota:**

Cuando descarga un archivo, no se muestra una barra de progreso para indicar el estado de la descarga. Sin embargo, la descarga se lleva a cabo.

**Marca de agua:** Cuando la opción de marca de agua está habilitada, aparece una marca de agua que contiene el nombre de usuario y la dirección IP de la máquina cliente en la aplicación iniciada. La marca de agua es semitransparente y no se puede modificar para mostrar ninguna otra información.

### **Configurar la caché mediante el GPO:**

Cuando varios usuarios utilizan el mismo dispositivo para iniciar sesión y acceder a las aplicaciones SaaS de Secure, la caché se transfiere al siguiente usuario, por lo que se comparte la información de navegación entre los usuarios.

Para solucionar este problema, la aplicación Citrix Workspace presenta una nueva directiva administrativa de objetos de directiva de grupo (GPO). Esta directiva no permitirá el almacenamiento de la caché del explorador en el dispositivo local.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Workspace > Citrix Secure Browser**.
3. Seleccione la directiva de **caché**.  
Nota: De forma predeterminada, esta directiva se establece en **Habilitada**.
4. Para inhabilitarla, seleccione **Inhabilitada** y haga clic en **Aplicar** y **Aceptar**.
5. Reinicie la aplicación Citrix Workspace para que el cambio surta efecto.

#### **Limitaciones:**

1. Cuando inicia una aplicación publicada con la opción de impresión habilitada y la descarga inhabilitada, y emite un comando de impresión en la aplicación iniciada, es posible que pueda guardar el documento PDF incluso cuando la funcionalidad de descarga esté restringida. Como solución temporal, para inhabilitar estrictamente la funcionalidad de descarga, inhabilite la opción de impresión.
2. Es posible que los vídeos incrustados en una aplicación no funcionen.

Para obtener más información sobre cómo configurar espacios de trabajo, consulte [Configurar el espacio de trabajo](#) en Citrix Cloud.

## **Impresión de PDF**

#### **Requisitos previos:**

- Aplicación Citrix Workspace 1808 o una versión más reciente.
- Citrix Virtual Apps and Desktops 7 1808 o una versión más reciente.
- Debe haber instalado al menos un visor de PDF en el equipo.

#### **Para habilitar la impresión de documentos PDF:**

1. En el Delivery Controller, use Citrix Studio para seleccionar el nodo **Directiva** en el panel de la izquierda. Puede crear una directiva o modificar una existente.
2. Establezca la directiva **Crear automáticamente la impresora universal de PDF** en **Habilitada**.

Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

#### **Limitación:**

- El explorador Microsoft Edge no admite la visualización ni la impresión de documentos PDF.

## Modo de tableta expandida en Windows 10 cuando se usa Windows Continuum

Windows Continuum es una función de Windows 10 que se adapta al uso que se le da al dispositivo cliente. La aplicación Citrix Workspace para Windows 4.10 y versiones posteriores admite el uso de Windows Continuum, incluido el cambio dinámico de modo.

Para los dispositivos cliente táctiles, el VDA de Windows 10 se inicia en modo tableta cuando no hay teclado ni mouse conectados. En cambio, se inicia en modo escritorio cuando se le conecta un teclado, un mouse o ambos. Cuando se conecta o se desconecta el teclado a cualquier dispositivo cliente, o se conecta o desconecta la pantalla en un dispositivo 2-en-1 (como Surface Pro), el modo pasa de tableta a escritorio y viceversa. Para obtener más información, consulte [Modo tableta para dispositivos de pantalla táctil](#) en la documentación de Citrix Virtual Apps and Desktops.

El VDA de Windows 10 detecta la presencia de un teclado o un mouse en un dispositivo cliente con función táctil cuando se conecta o se reconecta a una sesión. También detecta cuando se conecta o desconecta un teclado o mouse durante la sesión. Esta función está habilitada de forma predeterminada. Para inhabilitar la función, modifique la directiva **Cambiar modo tableta** mediante Citrix Studio.

El modo tableta ofrece una interfaz de usuario que se adapta mejor a las pantallas táctiles:

- Botones ligeramente más grandes.
- La pantalla **Inicio** y todas las aplicaciones que inicie se abren en modo de pantalla completa.
- La barra de tareas contiene el botón Atrás.
- Los iconos desaparecen de la barra de tareas.

El modo escritorio ofrece la interfaz de usuario tradicional, donde se interactúa de la misma manera que con el PC con teclado y mouse.

### Nota:

Workspace para Web no admite la función Windows Continuum.

## Mouse relativo

El mouse relativo ofrece una opción para interpretar la posición del mouse 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 se puede aplicar en una sesión de escritorio publicado.

La configuración de la función mediante el Editor del Registro o el archivo default.ica permite que la configuración sea persistente incluso después de finalizar la sesión.

Puede controlar la disponibilidad de la función por usuario y por equipo mediante el Registro de la siguiente manera:

### Configurar el mouse relativo mediante el Editor del Registro

Para configurar la función, establezca las siguientes claves del Registro según corresponda y, a continuación, reinicie la sesión para que los cambios surtan efecto:

#### Para que la función esté disponible por sesión:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse

#### Para que la función esté disponible por usuario:

HKEY\_CURRENT\_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse

- ```
1 - Name: Mouse
2 - Type: REG_SZ
3 - Value: True
```

#### Nota:

- Los valores establecidos en el Editor del Registro tienen prioridad sobre la configuración del archivo ICA.
- Los valores establecidos en HKEY\_LOCAL\_MACHINE y HKEY\_CURRENT\_USER deben ser los mismos. Si tienen diferentes valores esto podría causar conflictos.

### Configurar el mouse relativo mediante el archivo default.ica

1. Abra el archivo default.ica, ubicado normalmente en `C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica`, donde nombre del sitio es el nombre especificado para el sitio cuando fue creado. En el caso de clientes de StoreFront, el archivo default.ica se encuentra normalmente en `C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica`, donde storename es el nombre especificado para el almacén cuando este se creó.
2. Agregue una nueva clave con el nombre de RelativeMouse en la sección WFClient, configurado con el mismo valor que el objeto JSON.
3. Establezca el valor según sea necesario:
  - true: Para habilitar el mouse relativo
  - false: Para inhabilitar el mouse relativo
4. Inicie la sesión de nuevo para que los cambios surtan efecto.

**Nota:**

Los valores establecidos en el Editor del Registro tienen prioridad sobre la configuración del archivo ICA.

### **Habilitar el mouse relativo desde Desktop Viewer**

1. Inicie sesión en la aplicación Citrix Workspace.
2. Lance una sesión de escritorio publicado.
3. En la barra de herramientas de Desktop Viewer, seleccione **Preferencias**.  
Aparecerá la ventana “Citrix Workspace - Preferencias”.
4. Seleccione **Conexiones**.
5. En los parámetros de **Mouse relativo**, habilite **Usar mouse relativo**.
6. Haga clic en **Aplicar** y **Aceptar**.

**Nota:**

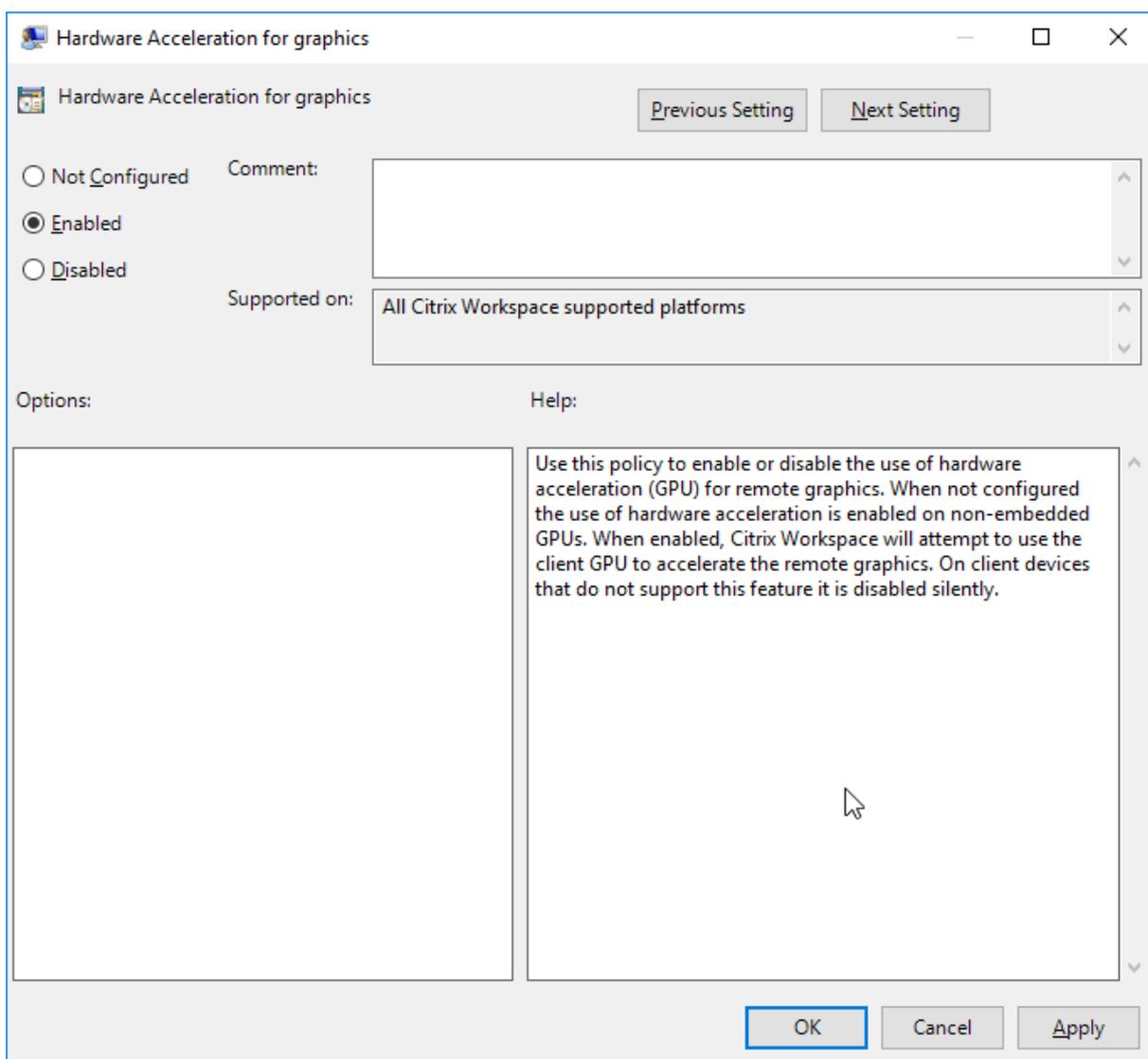
La configuración del mouse relativo desde Desktop Viewer aplica la función solo por sesión.

### **Decodificación por hardware**

Cuando se usa la aplicación Citrix Workspace (con HDX Engine 14.4), la GPU se puede usar para la decodificación H.264 donde esté disponible en el cliente. La capa de API utilizada para la decodificación por GPU es DirectX Video Acceleration.

#### **Para habilitar la decodificación por hardware con la plantilla administrativa de GPO de la aplicación Citrix Workspace:**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Workspace > Experiencia de usuario**.
3. Seleccione **Aceleración de hardware para gráficos**.
4. Seleccione **Habilitada** y haga clic en **Aplicar** y luego en **Aceptar**.



Para validar si la directiva se ha aplicado y la aceleración por hardware se está utilizando en una sesión ICA activa, busque las entradas de Registro siguientes:

Ruta del Registro: `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender`.

#### Sugerencia

El valor de **Graphics\_GfxRender\_Decoder** y **Graphics\_GfxRender\_Renderer** debe ser 2. Si el valor es 1, esto significa que se está usando la decodificación por CPU.

Cuando use la función de decodificación por hardware, tenga en cuenta que existen las limitaciones siguientes:

- Si el cliente tiene dos unidades GPU y si uno de los monitores está activo en la segunda GPU, se usará la decodificación basada en CPU.

- Al conectarse a un servidor Citrix Virtual Apps que ejecuta Windows Server 2008 R2, Citrix recomienda no usar la decodificación por hardware en el dispositivo Windows del usuario. Si se habilita, pueden observarse problemas, como un rendimiento lento al resaltar texto y un parpadeo de pantalla.

## Entrada de micrófono

La aplicación Citrix Workspace admite varias entradas de micrófono en el cliente. Los micrófonos instalados localmente se pueden usar para:

- Actividades en tiempo real, como llamadas desde sistemas de telefonía integrada en el equipo y conferencias web.
- Aplicaciones de grabación en el servidor, como programas de dictado.
- Grabaciones de vídeo y sonido.

Los usuarios de la aplicación Citrix Workspace pueden seleccionar si quieren usar los micrófonos conectados a sus dispositivos mediante un parámetro en la Central de conexiones. Los usuarios de Citrix Virtual Apps and Desktops y Citrix DaaS también pueden usar las Preferencias del visor de Citrix Virtual Apps and Desktops para inhabilitar sus micrófonos y cámaras web.

## Admitir varios monitores

Puede usar un máximo de ocho monitores con la aplicación Citrix Workspace para Windows.

Cada monitor en una configuración de varios monitores tiene su propia resolución, configurada por el fabricante. Los monitores pueden ofrecer diferentes resoluciones y orientaciones durante las sesiones.

Las sesiones pueden distribuirse entre varios monitores de dos formas:

- En modo de pantalla completa, con varios monitores en la sesión; las aplicaciones se presentan en los monitores como lo harían localmente.

**Citrix Virtual Apps and Desktops y Citrix DaaS:** Puede mostrar la ventana de Desktop Viewer en cualquier subconjunto de rectángulos de monitores; para ello, cambie el tamaño de la ventana en cualquier parte de esos monitores y haga clic en **Maximizar**.

- En modo de ventanas, con una única imagen de monitor para la sesión; las aplicaciones no se muestran en monitores individuales.

**Citrix Virtual Apps and Desktops y Citrix DaaS:** Cuando posteriormente se inicia cualquier escritorio en la misma asignación (anteriormente “grupo de escritorios”), se mantiene el parámetro de ventana y se muestra el escritorio en los mismos monitores. En la medida en que la distribución de monitores

sea rectangular, se pueden mostrar varios escritorios virtuales en un dispositivo. Si la sesión de aplicaciones y escritorios virtuales usa el monitor principal en el dispositivo, este será el monitor principal de la sesión. De lo contrario, el monitor con el número más bajo en la sesión se convierte en el monitor principal.

Para habilitar la compatibilidad con varios monitores, compruebe lo siguiente:

- El dispositivo de usuario está configurado para admitir el uso de varios monitores.
- El sistema operativo debe ser capaz de detectar cada monitor. En plataformas con Windows, para verificar que esta detección tiene lugar, vaya a **Configuración > Sistema**, haga clic en **Pantalla** y confirme que cada monitor aparezca por separado.
- Después de detectar los monitores:
  - **Citrix Virtual Desktops:** Defina el límite de memoria gráfica con la configuración **Límite de memoria de presentación** de las directivas de máquina de Citrix.
  - **Citrix Virtual Apps:** Según la versión del servidor Citrix Virtual Apps que haya instalado:
    - \* Defina el límite de memoria de gráficos con la configuración Límite de memoria de presentación en la **directiva de equipo de Citrix**.
    - \* En la consola de administración Citrix del servidor Citrix Virtual Apps, seleccione la comunidad y, en el panel de tareas, seleccione **Modificar las propiedades del servidor > Modificar todas las propiedades > Predeterminadas del servidor > HDX Broadcast > Presentación** (o Modificar las propiedades del servidor > Modificar todas las propiedades > Predeterminadas del servidor > ICA > Presentación) y defina la configuración “Memoria máxima” que se puede utilizar en cada uno de los gráficos de las sesiones.

Asegúrese de que el parámetro es lo suficientemente amplio (en kilobytes) para ofrecer suficiente memoria gráfica. Si este parámetro no es lo suficientemente grande, el recurso publicado se restringirá al subconjunto de monitores que cubra el tamaño especificado.

#### **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.

Para obtener información sobre el cálculo de los requisitos de memoria gráfica para Citrix Virtual Apps and Desktops y Citrix DaaS, consulte el artículo [CTX115637](#) en Knowledge Center.

## Impresora

Para sobrescribir los parámetros de la impresora en el dispositivo de usuario

1. En el menú **Imprimir** de la aplicación del dispositivo de usuario, elija **Propiedades**.
2. En la ficha **Parámetros del cliente**, haga clic en **Optimizaciones avanzadas** y realice cambios en las opciones “Compresión de imagen” y “Almacenamiento en caché de imágenes y fuentes”.

## Controlar el teclado en pantalla

Para habilitar el acceso táctil a las aplicaciones y escritorios virtuales desde tabletas Windows, la aplicación Citrix Workspace muestra automáticamente el teclado en pantalla al activar un campo de entrada de texto, y cuando el dispositivo está en modo tienda o tableta.

En algunos dispositivos y en algunas circunstancias, la aplicación Citrix Workspace no puede detectar el modo en que se encuentra un dispositivo, y es posible que el teclado en pantalla aparezca cuando no sea necesario.

Para evitar que aparezca el teclado en pantalla cuando se utiliza un dispositivo convertible, cree un valor `DisableKeyboardPopup` de REG\_DWORD en `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver` y establezca el valor en 1.

### Nota:

En una máquina x64, cree el valor en `HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver`.

Las claves se pueden establecer en 3 modos diferentes, como se muestra a continuación:

- **Automatic:** `AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 0`
- **Always popup** (teclado en pantalla): `AlwaysKeyboardPopup = 1; DisableKeyboardPopup = 0`
- **Never popup** (teclado en pantalla): `AlwaysKeyboardPopup = 0; DisableKeyboardPopup = 1`

## Teclas de acceso rápido

Se pueden configurar combinaciones de teclas para que la aplicación Citrix Workspace las interprete como una funcionalidad especial. Cuando se habilita la directiva de teclas de acceso directo, se pueden especificar las teclas de acceso directo de Citrix, el comportamiento de las teclas de acceso directo de Windows y la disposición del teclado para las sesiones.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Experiencia de usuario**.
3. Seleccione la directiva **Accesos directos de teclado**.
4. **Actívela** y defina las opciones pertinentes.
5. Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

### Compatibilidad con iconos de color de 32 bits:

La aplicación Citrix Workspace admite los iconos de color de alta densidad (de 32 bits) y selecciona automáticamente la profundidad de color de las aplicaciones que se muestran en el cuadro de diálogo **Central de conexiones de Citrix**, en el menú Inicio y en la barra de tareas para proporcionar una integración total.

#### Precaución

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si usa el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Para establecer una profundidad preferida, puede agregar una cadena de clave de Registro llamada `TWIDesiredIconColor` a `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences` y establecerla en el valor pertinente. Las profundidades de color posibles son 4, 8, 16, 24 y 32 bits por píxel. Si la conexión de la red es lenta, los usuarios pueden seleccionar valores de profundidad de color menores para los iconos.

### Desktop Viewer

Cada empresa tiene sus propias necesidades de negocio. 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. La experiencia del usuario a la hora de conectarse a los escritorios virtuales, así como su interacción en la configuración de las conexiones depende de cómo se configure la aplicación Citrix Workspace para Windows.

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 modo de acceso, las funciones de la barra de herramientas de Desktop Viewer permiten al usuario abrir un escritorio virtual en una ventana, desplazar y cambiar el tamaño de ese

escritorio dentro del escritorio local. Los usuarios pueden definir preferencias y conectarse a más de un escritorio mediante varias conexiones de Citrix Virtual Apps and Desktops y Citrix DaaS en el mismo dispositivo de usuario.

**Nota:**

Use la aplicación Citrix Workspace para cambiar la resolución de pantalla en los escritorios virtuales. No se puede cambiar la resolución de pantalla desde el Panel de control de Windows.

### **Entrada de teclado en Desktop Viewer**

En las sesiones de Desktop Viewer, la combinación de la tecla con el **logotipo de Windows** + L se transfiere al equipo local.

Ctrl+Alt+Supr se transfiere al equipo local.

Las pulsaciones de teclas que activan Teclas especiales, Teclas de filtro y Teclas de alternancia (funciones de accesibilidad de Microsoft) siempre se transfieren al equipo local.

Como una función de accesibilidad de Desktop Viewer, al presionar Ctrl+Alt+Interrumpir se muestran los botones de la barra de herramientas de Desktop Viewer en una ventana emergente.

Ctrl+Esc se envía al escritorio virtual remoto.

**Nota:**

De forma predeterminada, Alt+Tab transfiere el foco entre las ventanas de la sesión si Desktop Viewer está maximizado. Si Desktop Viewer se muestra en una ventana, Alt+Tab transfiere el foco entre las ventanas fuera de la sesión.

Las secuencias de teclas de acceso rápido son combinaciones de teclas diseñadas por Citrix. Por ejemplo, la secuencia Ctrl+F1 reproduce las teclas Ctrl+Alt+Supr, y Mayús+F2 cambia entre el modo de pantalla completa y de ventanas en las aplicaciones. No se pueden usar las secuencias de teclas de acceso rápido con escritorios virtuales que se muestran en Desktop Viewer (en sesiones de aplicaciones y escritorios virtuales), pero sí se pueden usar con aplicaciones publicadas (en sesiones de Citrix Virtual Apps).

### **Escritorios virtuales**

Los usuarios no pueden conectarse al mismo escritorio virtual desde una sesión de escritorio. Si se intenta, se desconectará la sesión de escritorio existente. Por lo tanto, Citrix recomienda lo siguiente:

- Los administradores no deben configurar a los clientes de un escritorio para que se conecten con un sitio que publica el mismo escritorio.

- Los usuarios no deben buscar un sitio que aloje el mismo escritorio si el sitio se configura para reconectar a los usuarios automáticamente con las sesiones existentes.
- Los usuarios no deben buscar un sitio que aloje el mismo escritorio e intentar ejecutarlo.

Tenga en cuenta que un usuario que inicia una sesión localmente en un equipo que actúa como escritorio virtual bloquea la conexión con ese escritorio.

Si los usuarios se conectan a aplicaciones virtuales (publicadas con Citrix Virtual Apps) desde un escritorio virtual y la organización dispone de un administrador de Citrix Virtual Apps independiente, Citrix recomienda aunar esfuerzos para definir la asignación de dispositivos para que los dispositivos de escritorio se asignen siempre dentro de las sesiones de aplicación y escritorio. Debido a que las unidades locales se muestran como unidades de red en las sesiones de escritorio, el administrador de Citrix Virtual Apps debe modificar la directiva de asignación de unidades para que incluya las unidades de red.

### **Tiempo de espera del indicador de estado**

Puede cambiar el tiempo que se muestra el indicador de estado cuando el usuario inicia una sesión. Para cambiar el tiempo de espera, cree el valor REG\_DWORD SI\_INACTIVE\_MS en HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA\_CLIENT\Engine\. El valor REG\_DWORD puede establecerse en 4 si quiere que el indicador de estado desaparezca más pronto.

### **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 Windows y envía esos datos automáticamente a Citrix y 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 según se especifica en el [documento de prueba acerca de la seguridad de Citrix Services](#), disponible en el [Centro de confianza de Citrix](#).

Citrix también usa 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. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace situado en el área de notificaciones.
2. Seleccione **Preferencias avanzadas**.  
Se mostrará el cuadro de diálogo **Preferencias avanzadas**.
3. Seleccione **Recopilación de datos**.
4. Seleccione **No, gracias** para inhabilitar CEIP o dejar de participar en el programa.
5. Haga clic en **Guardar**.

También puede ir a la siguiente entrada del Registro y establecer el valor como se sugiere:

**Ruta:** `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

**Clave:** `Enable_CEIP`

**Valor:** `False`

**Nota:**

Una vez que haya seleccionado **No, gracias** en el cuadro de diálogo de la recopilación de datos o haya establecido la clave `Enable_CEIP` en `False`, si quiere inhabilitar el envío de los dos últimos elementos de datos de CEIP recopilados por Google Analytics (es decir, la versión de sistema operativo y la versión de la aplicación Citrix Workspace) vaya a la siguiente entrada del Registro y establezca el valor como se sugiere:

**Ruta:** `HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

**Clave:** `DisableHeartbeat`

**Valor:** `True`

Elementos concretos de datos CEIP recopilados por Citrix:

|                               |                                           |                                          |                                   |
|-------------------------------|-------------------------------------------|------------------------------------------|-----------------------------------|
| Versión del sistema operativo | Versión de la aplicación Citrix Workspace | Dispositivos externos conectados         | Resolución de pantalla            |
| Versión de Flash              | Configuración de Desktop Lock             | Uso táctil                               | Configuración de la autenticación |
| Método de inicio de sesiones  | Configuración de gráficos                 | Configuración de Desktop Viewer          | Impresión                         |
| Error de conexión             | Tiempo restante para el inicio            | Idioma de la aplicación Citrix Workspace | Información de VDA                |
| Estado de SSON                | Estado del instalador                     | Tiempo restante para la instalación      | Protocolo de conexión             |
| Versión de Internet Explorer  |                                           |                                          |                                   |

Elementos concretos de datos CEIP recopilados por Google Analytics:

|                                         |                                            |                                      |                                          |
|-----------------------------------------|--------------------------------------------|--------------------------------------|------------------------------------------|
| Versión del sistema operativo*          | Versión de la aplicación Citrix Workspace* | Configuración de la autenticación    | Idioma de la aplicación Citrix Workspace |
| Método de inicio de sesiones            | Error de conexión                          | Protocolo de conexión                | Información de VDA                       |
| Configuración del instalador            | Estado del instalador                      | Distribución del teclado del cliente | Configuración del almacén                |
| Preferencia de actualización automática | Uso de la Central de conexiones            | Configuración de App Protection      |                                          |

## Autenticación

October 30, 2023

Proteja las conexiones entre la aplicación Citrix Workspace y los recursos publicados para maximizar la seguridad. Puede configurar los siguientes tipos de autenticación:

- PassThrough de dominio
- Tarjeta inteligente
- PassThrough de Kerberos

## **Autenticación PassThrough de dominio**

Single Sign-On permite autenticarse y usar las aplicaciones y los escritorios virtuales sin necesidad de volver a autenticarse.

El inicio de sesión en la aplicación Citrix Workspace permite que las credenciales y los recursos enumerados se transfieran a StoreFront.

En versiones anteriores, al usar Google Chrome, Microsoft Edge o Mozilla Firefox, se podían iniciar sesiones Single Sign-On, aunque la función no estuviera habilitada.

A partir de la versión 1905, todos los exploradores web necesitarán que configure Single Sign-On mediante la plantilla administrativa de objeto de directiva de grupo. Para obtener más información sobre cómo configurar Single Sign-On mediante la plantilla administrativa de objetos de directiva de grupo, consulte [Configurar Single Sign-On en Citrix Gateway](#).

Puede configurar el inicio Single Sign-On tanto en una instalación nueva como en una actualización mediante cualquiera de las siguientes opciones:

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

## **Configurar Single Sign-On durante una instalación nueva**

### **Configurar Single Sign-On durante una instalación nueva:**

1. Configure Single Sign-On en StoreFront o la Interfaz Web.
2. Configure servicios XML de confianza en el Delivery Controller.
3. Modifique parámetros de Internet Explorer.
4. Instale la aplicación Citrix Workspace con Single Sign-On.

## **Configurar Single Sign-On en StoreFront o la Interfaz Web**

Según el tipo de implementación de Citrix Virtual Apps and Desktops, Single Sign-On se puede configurar en StoreFront o la Interfaz Web desde la consola de administración.

Utilice la siguiente tabla para los diferentes casos de uso y su configuración respectiva:

| Caso de uso                                      | Detalles de configuración                                                                                                                            | Información adicional                                                                                                                                                                                                      |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SSON configurado en StoreFront y la Interfaz Web | Inicie Citrix Studio, vaya a <b>Almacén &gt; Administrar métodos de autenticación</b> y habilite <b>PassThrough de dominio</b> .                     | Cuando Single Sign-On no está configurado, la aplicación Citrix Workspace cambia automáticamente el método de autenticación de <b>PassThrough de dominio</b> a <b>Nombre de usuario y contraseña</b> , si está disponible. |
| Cuando se necesita Workspace para Web            | Inicie <b>Almacén &gt; Workspace para Web &gt; Administrar métodos de autenticación</b> y habilite <b>PassThrough de dominio</b> .                   | Cuando Single Sign-On no está configurado, la aplicación Citrix Workspace cambia automáticamente el método de autenticación de <b>PassThrough de dominio</b> a <b>Nombre de usuario y contraseña</b> , si está disponible. |
| Cuando StoreFront no está configurado            | Si la Interfaz Web está configurada en el VDA, inicie el sitio de servicios XenApp > <b>Métodos de autenticación</b> y habilite <b>PassThrough</b> . | Cuando el inicio Single Sign-On no está configurado, la aplicación Citrix Workspace cambia automáticamente el método de autenticación de <b>PassThrough</b> a <b>Explícita</b> , si está disponible.                       |

### Configurar Single Sign-On en Citrix Gateway

El inicio Single Sign-On en Citrix Gateway se habilita a través de la plantilla administrativa del GPO.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Autenticación de usuarios**.
3. Seleccione la directiva **Single Sign-On para Citrix Gateway**.
4. Seleccione **Habilitado**.
5. Haga clic en **Aplicar** y **Aceptar**.
6. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

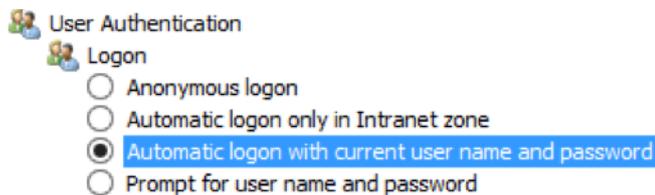
## Configurar servicios XML de confianza en el Delivery Controller

En Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service), ejecute el siguiente comando de PowerShell como administrador del Delivery Controller:

```
asnp Citrix* Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True
```

## Modificar los parámetros de Internet Explorer

1. Agregar el servidor de StoreFront a la lista de sitios de confianza mediante Internet Explorer. Para hacerlo:
  - a) Inicie **Opciones de Internet** desde el Panel de control.
  - b) Haga clic en **Seguridad > Internet local** y, a continuación, haga clic en **Sitios**. Aparecerá la ventana **Intranet local**.
  - c) Seleccione **Opciones avanzadas**.
  - d) Agregue la URL del FQDN de StoreFront o de la Interfaz Web con los protocolos HTTP o HTTPS correspondientes.
  - e) Haga clic en **Aplicar** y **Aceptar**.
2. Modifique los parámetros de **Autenticación del usuario** en **Internet Explorer**. Para hacerlo:
  - a) Inicie **Opciones de Internet** desde el Panel de control.
  - b) Haga clic en la ficha **Seguridad > Sitios de confianza**.
  - c) Haga clic en **Nivel personalizado**. Aparecerá la ventana **Configuración de seguridad: zona de sitios de confianza**.
  - d) En el panel **Autenticación del usuario**, seleccione **Inicio de sesión automático con el nombre de usuario y contraseña actuales**.



- a) Haga clic en **Aplicar** y **Aceptar**.

## Configurar Single Sign-On mediante la interfaz de línea de comandos

Instale la aplicación Citrix Workspace para Windows con el modificador de línea de comandos `/includeSSON` y reiníciela para que los cambios surtan efecto.

**Nota:**

Si la aplicación Citrix Workspace para Windows se instala sin el componente Single Sign-On, no se admite actualizar a la versión más reciente de Citrix Workspace con el modificador de línea de comandos `/includeSSON`.

### Configurar Single Sign-On mediante la interfaz gráfica de usuario

1. Busque el archivo de instalación de la aplicación Citrix Workspace (`CitrixWorkspaceApp.exe`).
2. Haga doble clic en `CitrixWorkspaceApp.exe` para iniciar el instalador.
3. En el asistente de instalación **Habilitar Single Sign-On**, seleccione la opción **Habilitar Single Sign-On**.
4. Haga clic en **Siguiente** y siga las instrucciones para completar la instalación.

Ahora puede iniciar sesión mediante la aplicación Citrix Workspace sin proporcionar credenciales de usuario.

### Configurar Single Sign-On en Citrix Workspace para Web

Puede configurar Single Sign-On en Workspace para Web mediante la plantilla administrativa del objeto de directiva de grupo.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace para Web. Para ello, ejecute `gpedit.msc`.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Autenticación de usuarios**.
3. Seleccione la directiva **Nombre de usuario y contraseña locales y habilítela**.
4. Haga clic en **Habilitar autenticación PassThrough**. Esta opción permite a la aplicación Citrix Workspace para Web usar las credenciales de inicio de sesión para autenticarse en el servidor remoto.
5. Haga clic en **Permitir autenticación PassThrough para todas las conexiones ICA**. Esta opción omite las restricciones de autenticación y permite que las credenciales se transfieran en todas las conexiones.
6. Haga clic en **Aplicar y Aceptar**.
7. Reinicie Citrix Workspace para Web para que los cambios surtan efecto.

Verifique si Single Sign-On está habilitado. Para ello, inicie el **Administrador de tareas** y compruebe que el proceso `ssonsvr.exe` se está ejecutando.

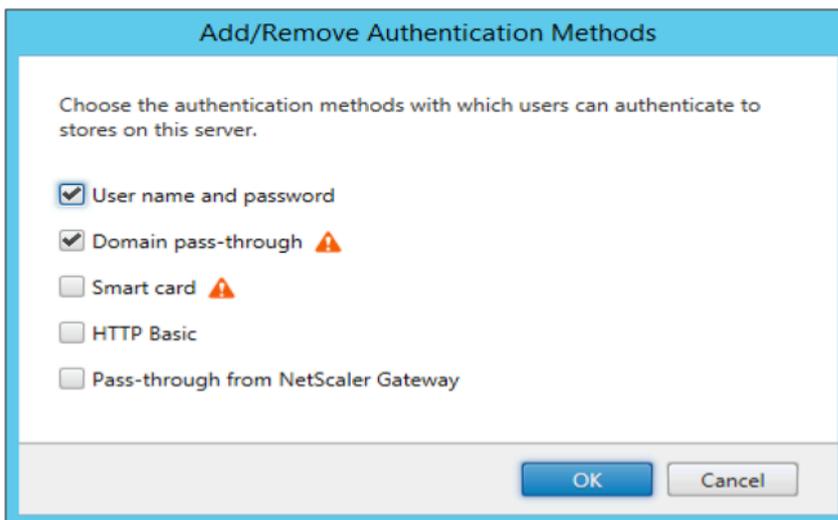
## Configurar Single Sign-On mediante Active Directory

Puede configurar la autenticación Single Sign-On mediante Active Directory. No es necesario utilizar herramientas de implementación, como Microsoft System Center Configuration Manager en este caso.

1. Descargue el archivo de instalación de la aplicación Citrix Workspace ([CitrixWorkspaceApp.exe](#)) y colóquelo en un recurso compartido de red adecuado. Se debe poder acceder a ese recurso desde las máquinas de destino en las que instale la aplicación Citrix Workspace.
2. Puede obtener la [CheckAndDeployWorkspacePerMachineStartupScript.bat](#) plantilla desde la página de [descargas de la aplicación Citrix Workspace para Windows](#).
3. Modifique la ubicación y la versión de [CitrixWorkspaceApp.exe](#).
4. En la **Consola de administración de directivas de grupo de Active Directory**, escriba [CheckAndDeployWorkspacePerMachineStartupScript.bat](#) como script de inicio. Para obtener más información sobre cómo implementar los script de inicio, consulte la sección [Active Directory](#).
5. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Agregar o quitar plantillas** para agregar el archivo [icaclient.adm](#).
6. Después de agregar la plantilla [icaclient.adm](#), vaya a **Configuración del equipo > Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Autenticación de usuarios**.
7. Seleccione la directiva **Nombre de usuario y contraseña locales y habilítela**.
8. Seleccione **Habilitar autenticación PassThrough** y haga clic en **Aplicar**.
9. Reinicie la máquina para que los cambios surtan efecto.

## Configurar Single Sign-On en StoreFront y la Interfaz Web

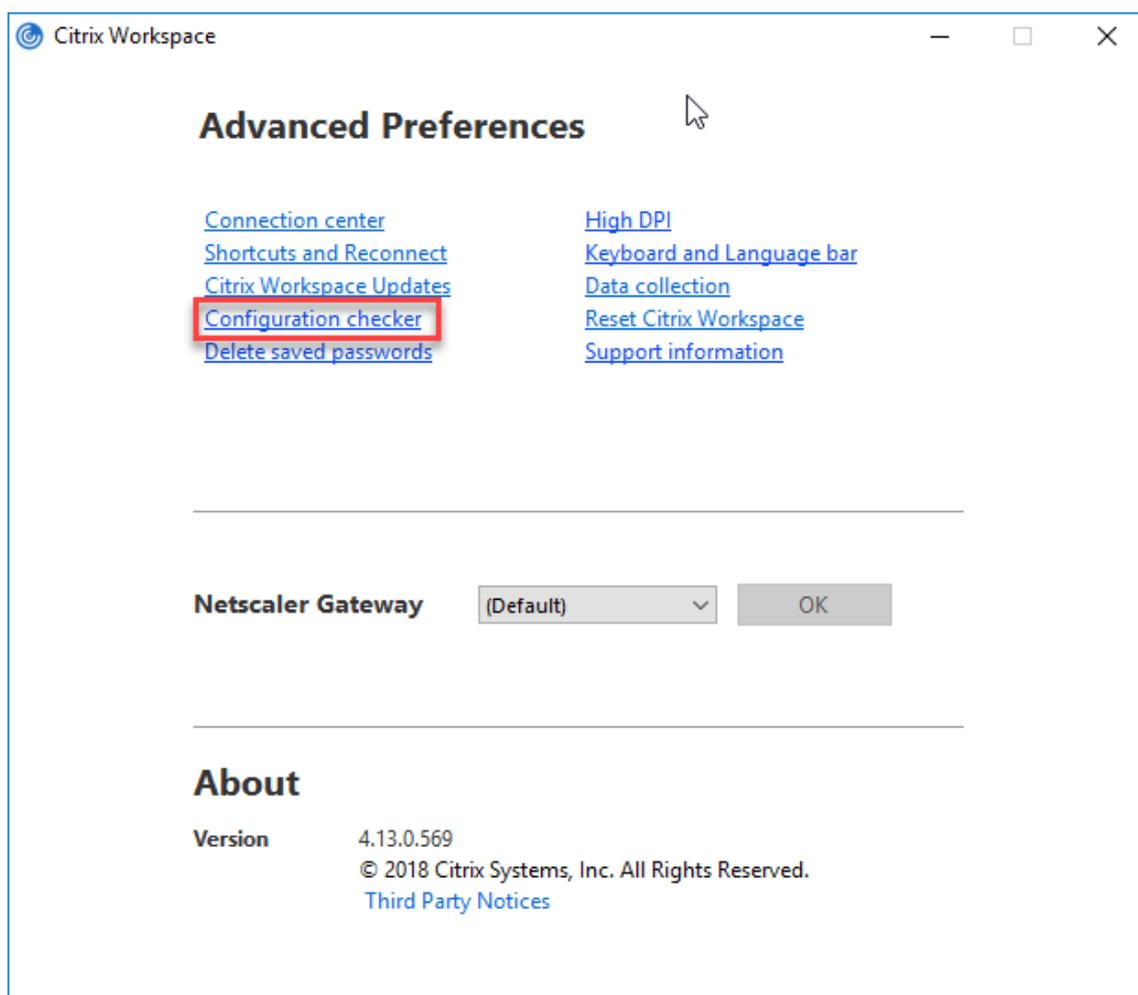
**Configurar StoreFront** Abra **Citrix Studio** en el servidor de StoreFront y seleccione **Autenticación > Agregar o quitar métodos de autenticación**. Seleccione **PassThrough de dominio**.



### Configuration Checker

Configuration Checker permite ejecutar pruebas para comprobar que Single Sign-On está configurado correctamente. Las pruebas se ejecutan en varios puntos de control de la configuración de Single Sign-On y muestran los resultados de la configuración.

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace situado en el área de notificaciones y, a continuación, haga clic en **Preferencias avanzadas**. Aparecerá el cuadro de diálogo **Preferencias avanzadas**.
2. Haga clic en **Configuration Checker**. Aparecerá la ventana **Citrix Configuration Checker**.



3. Seleccione **SSONChecker** desde el panel **Seleccionar**.
4. Haga clic en **Ejecutar**. Aparecerá la barra de progreso, que muestra el estado de la prueba.

La ventana de **Configuration Checker** consta de las siguientes columnas:

1. **Estado:** Muestra el resultado de una prueba en un punto de control concreto.
  - Una marca de verificación (✓) verde indica que el punto de control está configurado correctamente.
  - Una I azul indica información sobre el punto de control.
  - Una X roja indica que ese punto de control no está configurado correctamente.
2. **Proveedor:** Muestra el nombre del módulo en que se ejecuta la prueba. En este caso, Single Sign-On.
3. **Suite:** Indica la categoría de la prueba. Por ejemplo, Instalación.
4. **Prueba:** Indica el nombre de la prueba específica que se ejecuta.
5. **Detalles:** Ofrece información adicional acerca de la prueba.

El usuario puede ver más información sobre cada punto de control y los resultados correspondientes.

Se realizan las siguientes pruebas:

1. Instalado con Single Sign-On.
2. Captura de credenciales de inicio de sesión.
3. Registro de proveedores de red: El resultado de la prueba de registro de proveedor de red muestra una marca de verificación verde solo cuando “Citrix Single Sign-On” figura en primer lugar en la lista de proveedores de red. Si Citrix Single Sign-On aparece en algún otro lugar de la lista, el resultado de la prueba Registro de proveedores de red es una barra azul y se ofrece información adicional.
4. Proceso de Single Sign-On en ejecución.
5. Directiva de grupo: De manera predeterminada, esta directiva está configurada en el cliente.
6. Parámetros de Internet para zonas de seguridad: Compruebe que ha agregado la URL del almacén o del servicio XenApp a la lista de zonas de seguridad en las Opciones de Internet. Si las zonas de seguridad están configuradas mediante una directiva de grupo, cualquier cambio en la directiva requiere que la ventana **Preferencias avanzadas** se vuelva a abrir para que los cambios surtan efecto y para mostrar el estado correcto de la prueba.
7. Método de autenticación para la Interfaz Web o StoreFront.

**Nota:**

- Los resultados de la prueba no se aplican a configuraciones de Workspace para Web.
- En una configuración de varios almacenes, la prueba del método de autenticación se ejecuta en todos los almacenes configurados.
- Puede guardar como informes los resultados de la prueba. El formato predeterminado del informe es TXT.

### **Ocultar la opción Configuration Checker de la ventana Preferencias avanzadas**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. Vaya a **Componentes de Citrix > Citrix Workspace > Autoservicio > DisableConfigChecker**.
3. Haga clic en **Habilitado** para ocultar la opción Configuration Checker de la ventana **Preferencias avanzadas**.
4. Haga clic en **Aplicar** y **Aceptar**.
5. Ejecute el comando `gpupdate /force`.

### **Limitación:**

Configuration Checker no incluye el punto de control de la configuración “Confiar en las solicitudes enviadas a XML Service” en el VDA.

**Prueba de baliza** La prueba de baliza forma parte de la utilidad **Configuration Checker**. Permite realizar una prueba de baliza para confirmar si se puede acceder a la baliza (ping.citrix.com). Con esta prueba, se puede descartar una de las muchas causas posibles para la enumeración lenta de recursos (es decir, que la baliza no esté disponible). Para ejecutar la prueba, haga clic con el botón secundario en la aplicación Citrix Workspace en el área de notificaciones y seleccione **Preferencias avanzadas > Configuration Checker**. Seleccione **Beacon Checker** de la lista “Pruebas” y haga clic en **Ejecutar**.

Los resultados de la prueba pueden ser uno de los siguientes:

- **Accesible:** La aplicación Citrix Workspace puede contactar con la baliza.
- **No accesible:** La aplicación Citrix Workspace no puede contactar con la baliza.
- **Parcialmente accesible:** La aplicación Citrix Workspace puede contactar intermitentemente con la baliza.

## Autenticación PassThrough de dominio con Kerberos

Lo descrito en este artículo se aplica solo a conexiones entre la aplicación Citrix Workspace para Windows y StoreFront, Citrix Virtual Apps and Desktops y Citrix DaaS.

La aplicación Citrix Workspace admite Kerberos para la autenticación PassThrough de dominio en implementaciones que usan tarjetas inteligentes. Kerberos es uno de los métodos de autenticación incluidos en la autenticación de Windows integrada (IWA).

Kerberos autentica sin contraseña en la aplicación Citrix Workspace, y así impide ataques de tipo troyano que intentan obtener acceso a las contraseñas del dispositivo de usuario. Los usuarios pueden iniciar sesión mediante cualquier método de autenticación y acceder a los recursos publicados. Por ejemplo, pueden usar un autenticador biométrico como un lector de huellas dactilares.

Cuando inicie sesión con una tarjeta inteligente en la aplicación Citrix Workspace, StoreFront, Citrix Virtual Apps and Desktops y Citrix DaaS configurados para la autenticación con tarjeta inteligente, la aplicación Citrix Workspace:

1. Captura el PIN de la tarjeta inteligente durante Single Sign-On.
2. Usa IWA (Kerberos) para autenticar al usuario en StoreFront. A continuación, StoreFront proporciona a la aplicación Citrix Workspace información sobre las instancias disponibles de Citrix Virtual Apps and Desktops y Citrix DaaS.

### Nota

Habilite Kerberos para evitar una solicitud extra de PIN. Si no se usa la autenticación Kerberos, la aplicación Citrix Workspace se autentica en StoreFront con las credenciales de la tarjeta inteligente.

3. El motor de HDX pasa el PIN de la tarjeta inteligente al VDA para iniciar la sesión del usuario en la aplicación Citrix Workspace. A continuación, Citrix Virtual Apps and Desktops y Citrix DaaS entregan los recursos solicitados.

Para usar la autenticación Kerberos en la aplicación Citrix Workspace, la configuración de Kerberos debe cumplir los siguientes requisitos.

- Kerberos solo funciona entre la aplicación Citrix Workspace y los servidores que pertenecen a los mismos dominios de Windows o a dominios que son de confianza. Los servidores también deben ser de confianza para la delegación, una opción que se configura a través de la herramienta de administración de usuarios y equipos de Active Directory.
- Kerberos debe estar habilitado tanto en el dominio como en Citrix Virtual Apps and Desktops y en Citrix DaaS. Para mayor seguridad y para asegurarse de que se utiliza Kerberos, inhabilite las demás opciones que no sean Kerberos IWA en el dominio.
- El inicio de sesión con Kerberos no está disponible para conexiones de Servicios de escritorio remoto configuradas para usar la autenticación básica, para usar siempre la información de inicio de sesión especificada o para pedir siempre una contraseña.

#### Advertencia

El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden hacer necesaria la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

### Autenticación PassThrough de dominio con Kerberos para usarla con tarjetas inteligentes

Antes de continuar, consulte la información de tarjeta inteligente que se indica en la sección [Proteger la implementación](#) en la documentación de Citrix Virtual Apps and Desktops.

Cuando instale la aplicación Citrix Workspace para Windows, incluya la opción siguiente en la línea de comandos:

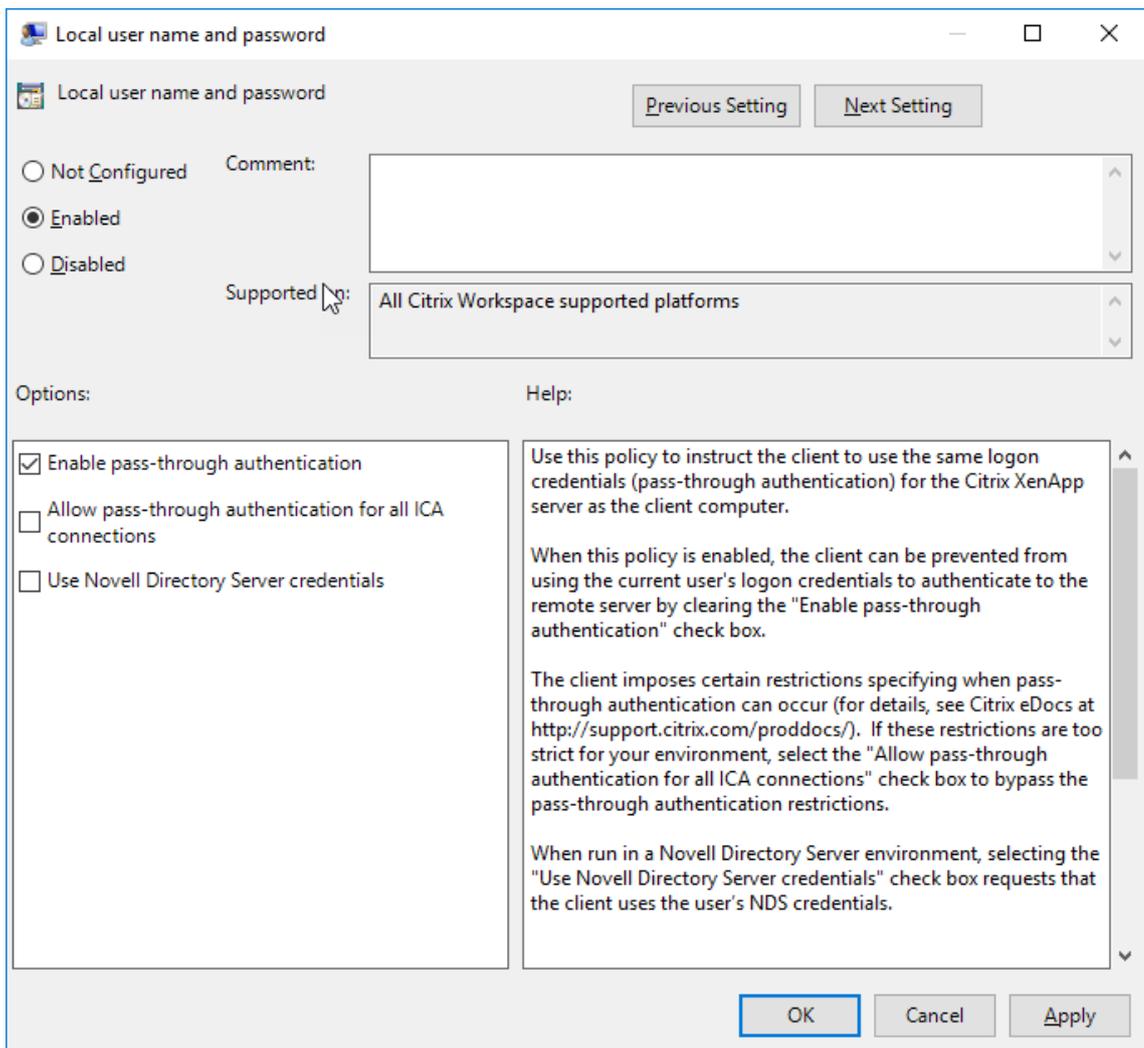
- `/includeSSON`

Esta opción instala el componente Single Sign-On en el equipo unido a un dominio, lo que habilita a Citrix Workspace para autenticarse en StoreFront mediante IWA (Kerberos). El componente Single Sign-On guarda el PIN de la tarjeta inteligente. El motor HDX utiliza ese PIN cuando comunica de forma remota el hardware de la tarjeta inteligente y las credenciales a Citrix Virtual Apps and Desktops y Citrix DaaS. Citrix Virtual Apps and Desktops y Citrix DaaS seleccionan automáticamente un certificado desde la tarjeta inteligente y obtienen el PIN desde el motor HDX.

La opción relacionada `ENABLE\ \_SSON` está habilitada de forma predeterminada.

Si una directiva de seguridad le impide habilitar el inicio Single Sign-On en un dispositivo, configure la aplicación Citrix Workspace mediante la plantilla administrativa del objeto de directiva de grupo.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. Elija **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Autenticación de usuarios > Nombre de usuario y contraseña locales**.
3. Seleccione **Habilitar autenticación PassThrough**.
4. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.



### Para configurar StoreFront:

Durante la configuración del servicio de autenticación en el servidor de StoreFront, seleccione la opción PassThrough de dominio. Este parámetro habilita la autenticación de Windows integrada (IWA). No es necesario seleccionar la opción “Tarjeta inteligente” a menos que también tenga clientes que no estén unidos a un dominio conectándose a StoreFront con tarjeta inteligente.

Para obtener más información sobre el uso de tarjetas inteligentes con StoreFront, consulte [Configurar el servicio de autenticación](#) en la documentación de StoreFront.

## Tarjeta inteligente

La aplicación Citrix Workspace para Windows admite la siguiente autenticación con tarjeta inteligente:

- **Autenticación PassThrough (Single Sign-On):** La autenticación PassThrough captura las credenciales de la tarjeta inteligente cuando los usuarios inician sesión en la aplicación Citrix Workspace. La aplicación Citrix Workspace usa las credenciales capturadas de la siguiente manera:
  - Los usuarios de dispositivos unidos a dominio que inician sesión en la aplicación Citrix Workspace con tarjeta inteligente pueden iniciar aplicaciones y escritorios virtuales sin necesidad de volver a autenticarse.
  - Los usuarios de dispositivos no unidos a ningún dominio que inician sesión en la aplicación Citrix Workspace con credenciales de tarjeta inteligente deben escribir de nuevo sus credenciales para poder iniciar una aplicación o escritorio virtual.

La autenticación PassThrough debe configurarse tanto en StoreFront como en la aplicación Citrix Workspace.

- **Autenticación bimodal:** La autenticación bimodal ofrece a los usuarios la opción de usar una tarjeta inteligente o escribir su nombre de usuario y contraseña. Esta función es efectiva cuando no se puede usar la tarjeta inteligente; por ejemplo, cuando el certificado de inicio de sesión ha caducado. Para permitir la autenticación bimodal, deben configurarse almacenes dedicados para cada sitio siguiendo el método de **DisableCtrlAltDel** establecido en el valor **False** para permitir el uso de tarjetas inteligentes. La autenticación bimodal requiere una configuración de StoreFront.

Con la autenticación bimodal, el administrador de StoreFront puede ofrecer al usuario la posibilidad de autenticarse con nombre y contraseña o con tarjeta inteligente en un mismo almacén. Para ello, el administrador debe seleccionar estas dos opciones en la consola de StoreFront. Consulte la documentación de [StoreFront](#).

- **Varios certificados:** Puede haber varios certificados disponibles para una única tarjeta inteligente y si se utilizan varias tarjetas inteligentes.
- **Autenticación por certificado del cliente:** La autenticación por certificado del cliente requiere la configuración de Citrix Gateway y StoreFront.
  - Para acceder a StoreFront a través de Citrix Gateway, puede que deba volver a autenticarse después de extraer la tarjeta inteligente.

- Cuando la configuración SSL de Citrix Gateway está definida como autenticación por certificado de cliente obligatoria, la operación es más segura. No obstante, la autenticación por certificado de cliente obligatoria no es compatible con la autenticación bimodal.
- **Sesiones de doble salto:** Si es necesario el doble salto, se establece una conexión entre la aplicación Citrix Workspace y el escritorio virtual del usuario. Las implementaciones que ofrecen la funcionalidad de doble salto se describen en la documentación de Citrix Virtual Apps and Desktops.
- **Aplicaciones habilitadas para tarjeta inteligente:** Las aplicaciones habilitadas para tarjeta inteligente, como Microsoft Outlook y Microsoft Office, permiten a los usuarios cifrar o firmar digitalmente los documentos disponibles en las sesiones de aplicaciones y escritorios virtuales.

### Limitaciones:

- Los certificados deben guardarse en una tarjeta inteligente, no en el dispositivo del usuario.
- La aplicación Citrix Workspace no guarda la elección de certificado del usuario, pero guarda el PIN si se configura así. El PIN se almacena en caché solo en la memoria no paginada. No se almacena en el disco.
- La aplicación Citrix Workspace no se reconecta a sesiones cuando se inserta una tarjeta inteligente.
- Cuando está configurada para la autenticación con tarjeta inteligente, la aplicación Citrix Workspace no admite ni el Preinicio de sesiones ni Single Sign-On en redes privadas virtuales (VPN). Para usar la red VPN con la autenticación por tarjeta inteligente, instale Citrix Gateway Plug-in e inicie sesión a través de una página web mediante la tarjeta inteligente y los PIN para autenticarse en cada paso. La autenticación PassThrough en StoreFront con Citrix Gateway Plug-in no está disponible para los usuarios de tarjeta inteligente.
- Las comunicaciones de Citrix Workspace Updater con citrix.com y Merchandising Server no son compatibles con la autenticación por tarjeta inteligente en Citrix Gateway.

### Advertencia

Algunas configuraciones requieren modificaciones del Registro. El uso incorrecto del Editor del Registro del sistema puede causar problemas que pueden hacer necesaria la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Haga una copia de seguridad del Registro antes de modificarlo.

### Para habilitar la autenticación Single Sign-On para tarjeta inteligente:

Para configurar la aplicación Citrix Workspace para Windows, incluya la siguiente opción de línea de comandos cuando la instale:

- `ENABLE\_SSON=Yes`

Single Sign-On es otro término para el paso de credenciales/autenticación PassThrough. Habilitar este parámetro impide que la aplicación Citrix Workspace muestre una segunda solicitud de PIN.

- Defina **SSONCheckEnabled** como “false” si el componente Single Sign-On no está instalado. La clave impide que Authentication Manager de la aplicación Citrix Workspace busque el componente Single Sign-On, lo que permite que la aplicación Citrix Workspace se autentique en StoreFront.

```
HKEY\\_CURRENT\\_USER\\Software\\Citrix\\AuthManager\\protocols\\integratedwindows\\
```

```
HKEY\\_LOCAL\\_MACHINE\\Software\\Citrix\\AuthManager\\protocols\\integratedwindows\\
```

Para habilitar la autenticación en StoreFront con tarjeta inteligente en lugar de Kerberos, instale la aplicación Citrix Workspace para Windows con las siguientes opciones de la línea de comandos.

- `/includeSSON` instala Single Sign-On (autenticación PassThrough). Habilita el almacenamiento en caché de credenciales y el uso de la autenticación PassThrough de dominio.
- Si el usuario está iniciando sesión en el punto final con otro método distinto de la tarjeta inteligente para autenticarse en la aplicación Citrix Workspace para Windows (por ejemplo, con nombre de usuario y contraseña), la línea de comandos es:

```
/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
```

Lo que evita que se capturen credenciales al iniciar sesión, al mismo tiempo que permite que la aplicación Citrix Workspace almacene el PIN al iniciar sesión en Citrix Workspace.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. Vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Autenticación de usuarios > Nombre de usuario y contraseña locales**.
3. Seleccione **Habilitar autenticación PassThrough**. Dependiendo de la configuración y los parámetros de seguridad, seleccione la opción **Permitir autenticación PassThrough para todas las conexiones ICA** para que la autenticación PassThrough funcione.

#### Para configurar StoreFront:

- Al configurar el servicio de autenticación, marque la casilla **Tarjeta inteligente**.

Para obtener más información sobre el uso de tarjetas inteligentes con StoreFront, consulte [Configurar el servicio de autenticación](#) en la documentación de StoreFront.

#### Para habilitar los dispositivos de los usuarios para el uso de tarjetas inteligentes:

1. Importe el certificado raíz de la entidad de certificación en el almacén de claves del dispositivo.
2. Instale el middleware de su proveedor de servicios criptográficos.
3. Instale y configure la aplicación Citrix Workspace.

**Para cambiar cómo se seleccionan los certificados:**

De manera predeterminada, si hay varios certificados válidos, la aplicación Citrix Workspace pide al usuario que elija uno de la lista. Como alternativa, puede configurar la aplicación Citrix Workspace para que use el certificado predeterminado (por proveedor de tarjeta inteligente) o el certificado con la fecha de caducidad más lejana. Si no hay certificados de inicio de sesión válidos, se notifica esto al usuario y se le da la opción de usar un método de inicio de sesión alternativo, si hay alguno disponible.

Un certificado válido debe reunir estas características:

- La fecha y hora actuales según el reloj del equipo local está dentro del período de validez del certificado.
- La clave pública **Sujeto** debe usar el algoritmo de RSA y tener una longitud de 1024, 2048 o 4096 bits.
- El campo Uso de la clave debe contener Firma digital.
- El Nombre alternativo del sujeto debe contener el nombre principal del usuario (UPN).
- El campo “Uso mejorado de claves” debe contener Inicio de sesión de tarjeta inteligente y Autenticación del cliente o Todos los usos de la clave.
- Una de las entidades de certificación en la cadena de emisores del certificado debe coincidir con uno de los nombres distintivos (DN) enviado por el servidor durante el protocolo de enlace TLS.

Cambie el modo en que se seleccionan los certificados mediante uno de estos métodos:

- En la línea de comandos de la aplicación Citrix Workspace, especifique la opción `AM\\_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }`.

La opción predeterminada es “Prompt”(Preguntar). Para SmartCardDefault (predeterminado de la tarjeta inteligente) o LatestExpiry (fecha de caducidad más lejana), si hay varios certificados que cumplen esos criterios, la aplicación Citrix Workspace pide al usuario que elija uno.

---

Agregue este valor a la clave de `SmartCardDefault` `LatestExpiry` }.

Registro en  
HKEY\_CURRENT\_USER or  
HKEY\_LOCAL\_MACHINE\SoftwareWow6432Node\Citrix\AuthManager:  
CertificateSelectionMode={  
Prompt

---

•

Los valores definidos en HKEY\_CURRENT\_USER prevalecen sobre los valores definidos en HKEY\_LOCAL\_MACHINE para facilitar al usuario la selección de certificado.

#### **Para usar solicitudes de PIN del proveedor de servicios criptográficos (CSP):**

De manera predeterminada, los diálogos de PIN que se presentan a los usuarios provienen de la aplicación Citrix Workspace para Windows, en lugar de venir del proveedor CSP (Cryptographic Service Provider) de la tarjeta inteligente. La aplicación Citrix Workspace pide a los usuarios que escriban un PIN cuando es necesario, y luego pasa el PIN al proveedor CSP de la tarjeta inteligente. Si el sitio o la tarjeta inteligente tienen unos requisitos de seguridad más estrictos (por ejemplo, prohibir el almacenamiento del PIN en caché por proceso o por sesión), puede configurar la aplicación Citrix Workspace para que use los componentes del CSP para gestionar las entradas de PIN, incluida la solicitud del PIN.

Cambie el modo en que se gestiona la introducción de PIN mediante uno de estos métodos:

- En la línea de comandos de la aplicación Citrix Workspace, especifique la opción `AM\ \_SMARTCARDPINENTRY=CSP`.
- Agregue el siguiente valor a la clave de Registro `HKEY_LOCAL_MACHINE\Software\[Wow6432Node]\Citrix\AutoSmartCardPINEntry=CSP`.

#### **Cambios en la extracción y la compatibilidad de tarjetas inteligentes**

Tenga en cuenta lo siguiente cuando se conecte a un sitio PNAgent de XenApp 6.5:

- El inicio de sesión con tarjeta inteligente se admite en los inicios de sesión del sitio PNAgent.
- La directiva de extracción de tarjetas inteligentes ha cambiado en el sitio PNAgent:

Una sesión de Citrix Virtual Apps se cierra cuando se extrae la tarjeta inteligente: si el sitio PNAgent está configurado con la tarjeta inteligente como método de autenticación, la directiva correspondiente debe configurarse explícitamente en la aplicación Citrix Workspace para Windows para aplicar el cierre de la sesión de Citrix Virtual Apps. Habilite la itinerancia para la autenticación con tarjeta inteligente en el sitio PNAgent de XenApp y habilite la directiva de extracción de tarjetas inteligentes, la cual cierra la sesión de Citrix Virtual Apps en la sesión de la aplicación Citrix Workspace. La sesión del usuario sigue abierta en la aplicación Citrix Workspace.

#### **Limitación:**

Cuando inicia sesión en el sitio PNAgent mediante la autenticación con tarjeta inteligente, el nombre de usuario aparece como **Conectado**.

## Proteger comunicaciones

April 22, 2024

Para proteger la comunicación entre el servidor Citrix Virtual Apps and Desktops y la aplicación Citrix Workspace, se pueden integrar las conexiones de la aplicación Citrix Workspace a través de tecnologías de seguridad como las siguientes:

- Citrix Gateway: Para obtener información, consulte los temas de esta sección, además de la documentación de Citrix Gateway y StoreFront.

**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.
- Solamente para implementaciones de Citrix Virtual Apps o la Interfaz Web (no se aplica a XenDesktop 7): un servidor proxy SOCKS o un servidor proxy seguro (también conocido como servidor proxy de seguridad o servidor proxy HTTPS). Se pueden utilizar servidores proxy para limitar el acceso hacia y desde la red, y para gestionar las conexiones entre Citrix Workspace y el servidor. La aplicación Citrix Workspace admite protocolos de proxy seguro y SOCKS.
- Solamente para implementaciones de Citrix Virtual Apps o la Interfaz Web; no se aplica a XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 ni XenApp 7.5: Soluciones de Traspaso SSL con protocolos TLS (Transport Layer Security).
- Para Citrix Virtual Apps and Desktops 7.6, puede habilitar una conexión SSL directamente entre los usuarios y los VDA.

## Compatibilidad con proxies salientes

Smart Control permite a los administradores definir directivas granulares con el objetivo de configurar y aplicar atributos de entorno de usuario para Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) mediante Citrix Gateway. Por ejemplo, es posible que quiera prohibir a los usuarios asignar unidades a sus escritorios remotos. Esto se puede lograr con la función Smart Control de Citrix Gateway.

Sin embargo, la situación cambia cuando la aplicación Citrix Workspace y Citrix Gateway pertenecen a cuentas empresariales distintas. En tales casos, el dominio del cliente no puede aplicar la función Smart Control porque la puerta de enlace no existe en el dominio del cliente. En su lugar, puede aprovechar el proxy ICA saliente. El proxy ICA saliente le permite utilizar la función Smart Control incluso cuando la aplicación Citrix Workspace y Citrix Gateway se implementan en organizaciones distintas.

La aplicación Citrix Workspace admite inicios de sesión mediante el proxy de LAN de NetScaler. Se puede configurar un único proxy estático o se puede seleccionar el servidor proxy en ejecución mediante el plug-in del proxy saliente.

Puede configurar proxies salientes a través de los métodos siguientes:

- Proxy estático: El servidor proxy se configura al proporcionarle un nombre de host y un número de puerto.
- Proxy dinámico: Se puede seleccionar un servidor proxy único entre uno o más servidores proxy mediante la DLL del plug-in de proxy.

Puede configurar el proxy saliente mediante la plantilla administrativa de objetos de directiva de grupo y el Editor del Registro.

Para obtener más información acerca del proxy saliente, consulte [Compatibilidad con proxies ICA salientes](#) en la documentación de Citrix Gateway.

## Compatibilidad con proxies salientes: Configuración

### Nota:

Si se configuran tanto proxies estáticos como proxies dinámicos, la configuración de proxies dinámicos tiene prioridad.

### Configurar el proxy saliente mediante la plantilla administrativa de GPO:

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Workspace > Redirección de red**.
3. Seleccione una de estas opciones:
  - Para proxies estáticos: Seleccione la directiva **Configurar el proxy de LAN de NetScaler manualmente**. Seleccione **Habilitado** y, a continuación, indique el nombre de host y el número de puerto.
  - Para proxies dinámicos: Seleccione la directiva **Configurar el proxy de LAN de NetScaler con DLL**. Seleccione **Habilitado** y, a continuación, indique la ruta de acceso completa al archivo DLL. Por ejemplo: `C:\Workspace\Proxy\ProxyChooser.dll`.

4. Haga clic en **Aplicar** y **Aceptar**.

#### **Configurar el proxy saliente mediante el Editor del Registro:**

- **Para proxies estáticos:**

- Abra el Editor del Registro y vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler`.

- Cree claves de valor DWORD de la siguiente manera:

```
"StaticProxyEnabled"=dword:00000001
```

```
"ProxyHost"="testproxy1.testdomain.com
```

```
"ProxyPort"=dword:000001bb
```

- **Para proxies dinámicos:**

- Abra el Editor del Registro y vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler LAN Proxy`.

- Cree claves de valor DWORD de la siguiente manera:

```
"DynamicProxyEnabled"=dword:00000001
```

```
"ProxyChooserDLL"="c:\Workspace\Proxy\ProxyChooser.dll"
```

## **TLS**

Este tema se aplica a Citrix Virtual Apps and Desktops 7.6 y versiones posteriores.

Para usar el cifrado TLS para todas las comunicaciones de la aplicación Citrix Workspace con el servidor, configure el dispositivo de usuario, la aplicación Citrix Workspace y, si usa la Interfaz Web, el servidor que ejecuta la Interfaz Web. Para obtener información sobre cómo proteger las comunicaciones con StoreFront, consulte los temas de [Proteger](#) en la documentación de StoreFront.

#### **Requisitos previos:**

Los dispositivos de los usuarios deben cumplir los requisitos especificados en los [Requisitos del sistema](#).

Use esta directiva para configurar las opciones de TLS que garantizan que la aplicación Citrix Workspace identifique de forma segura el servidor al que se está conectando y pueda cifrar todas las comunicaciones con el servidor.

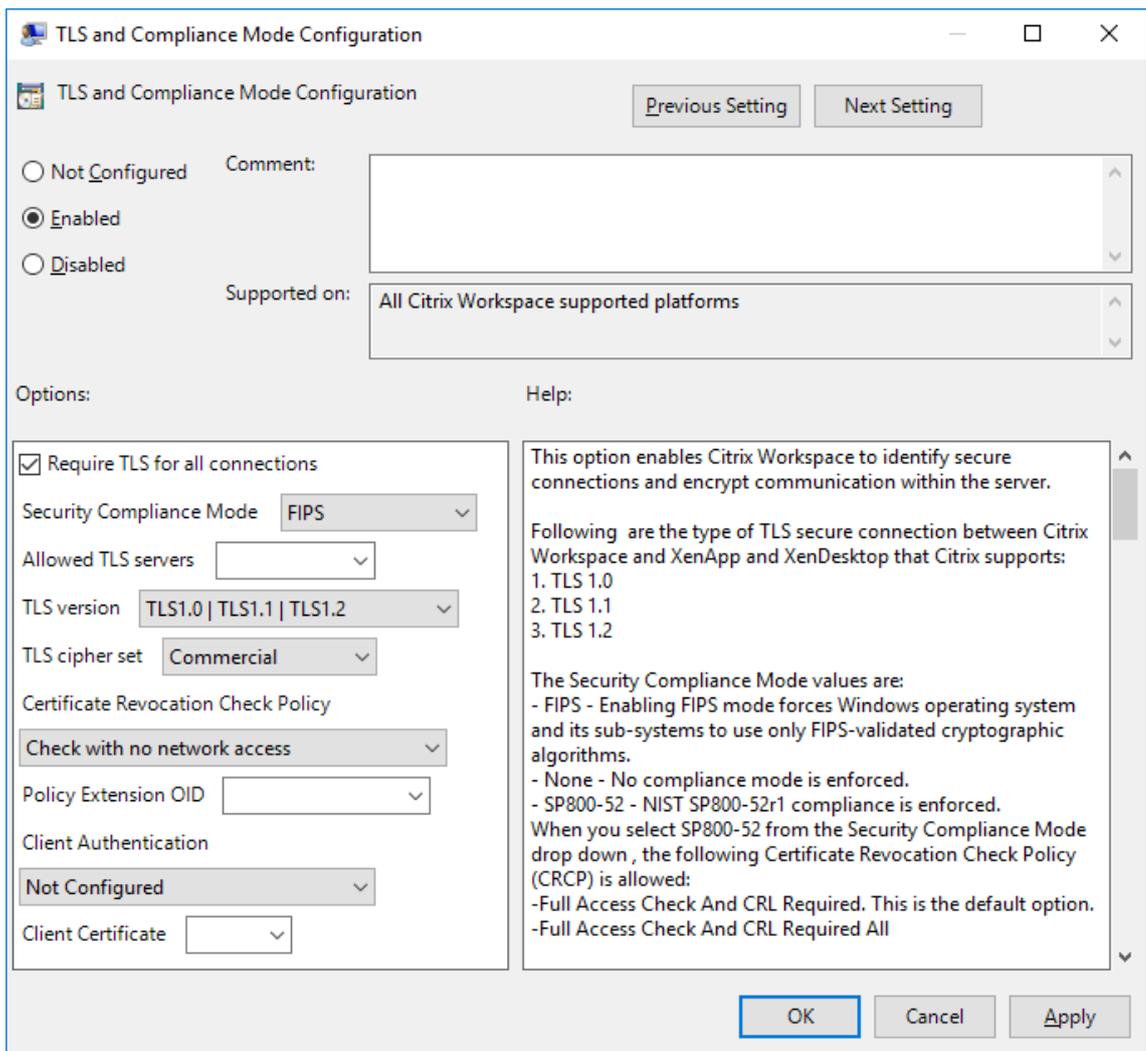
Puede usar estas opciones para:

- Exigir el uso de TLS: Citrix recomienda usar TLS para todas las conexiones a través de redes que no son de confianza, como Internet.

- Exigir el uso de la criptografía aprobada por FIPS (Federal Information Processing Standards): Para cumplir las recomendaciones de NIST SP 800-52. Estas opciones están inhabilitadas de forma predeterminada.
- Exigir el uso de una versión específica de TLS y de conjuntos de cifrado TLS específicos: Citrix admite los protocolos TLS 1.0, TLS 1.1 y TLS 1.2 entre la aplicación Citrix Workspace para Windows y Citrix Virtual Apps and Desktops y Citrix DaaS.
- Conectarse solamente a servidores específicos.
- Comprobar si el certificado del servidor se ha revocado.
- Comprobar si existe alguna directiva de emisión de certificados de servidor específica.
- Seleccionar un certificado de cliente concreto, si el servidor está configurado para solicitar uno.

### **Compatibilidad con TLS**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Workspace > Redirección de red** y seleccione la directiva **Configuración del modo de conformidad y TLS**.



3. Seleccione **Habilitada** para habilitar las conexiones seguras y para cifrar la comunicación en el servidor. Configure estas opciones:

**Nota:**

Citrix recomienda usar TLS para proteger las conexiones.

- a) Seleccione **Requerir TLS para todas las conexiones** si quiere obligar a la aplicación Citrix Workspace a usar TLS en todas las conexiones con aplicaciones y escritorios publicados.
- b) En el menú **Modo de conformidad para la seguridad**, seleccione la opción correspondiente:
  - i. **Ninguno:** No se impone ningún modo de conformidad.
  - ii. **SP800-52:** Seleccione **SP800-52** para la conformidad con NIST SP 800-52. Seleccione esta opción solo si los servidores o las puertas de enlace también cumplen las recomendaciones de NIST SP 800-52.

**Nota:**

Si selecciona **SP800-52**, se usará automáticamente la criptografía aprobada por FIPS, incluso aunque no esté seleccionada la opción **Habilitar FIPS**. También debe habilitar la opción de seguridad de Windows **Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash**. De lo contrario, la aplicación Citrix Workspace puede fallar al intentar conectarse a aplicaciones y escritorios publicados.

Si selecciona **SP800-52**, también debe seleccionar el parámetro **Directiva de comprobación de revocación de certificados** con el valor **Comprobar con acceso completo** o con el valor **Requerir comprobación con acceso completo y lista de revocación de certificados**.

Cuando selecciona **SP 800-52**, la aplicación Citrix Workspace verifica si el certificado de servidor cumple las recomendaciones de NIST SP 800-52. Si el certificado de servidor no las cumple, la aplicación Citrix Workspace no se podrá conectar.

- i. **Habilitar FIPS:** Seleccione esta opción para exigir el uso de la criptografía aprobada por FIPS. También debe habilitar la opción de seguridad de Windows **Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash** en la directiva de grupo del sistema operativo. De lo contrario, la aplicación Citrix Workspace puede fallar al intentar conectarse a aplicaciones y escritorios publicados.
- c) En la lista desplegable **Servidores TLS permitidos**, seleccione el número de puerto. Con una lista separada por comas, la aplicación Citrix Workspace para Windows se conectará solo a los servidores especificados. Se pueden especificar comodines y números de puerto. Por ejemplo, \*.citrix.com: 4433 permite la conexión a un servidor cuyo nombre común termine en .citrix.com en el puerto 4433. La precisión de la información que contenga un certificado de seguridad es responsabilidad del emisor del certificado. Si Citrix Workspace no reconoce ni confía en el emisor de un certificado, se rechaza la conexión.
- d) En el menú **Versión de TLS**, seleccione una de las siguientes opciones:
  - **TLS 1.0, TLS 1.1 o TLS 1.2:** Este es el parámetro predeterminado. Esta opción solo se recomienda si es un requisito del negocio usar TLS 1.0 para la compatibilidad.
  - **TLS 1.1 o TLS 1.2:** Use esta opción para que las conexiones ICA usen TLS 1.1 o TLS 1.2.
  - **TLS 1.2:** Esta opción se recomienda si TLS 1.2 es un requisito del negocio.
- a) **Conjunto de cifrado TLS:** Para obligar el uso de conjuntos de cifrado TLS específicos, seleccione Gubernamental (GOV), Comercial (COM) o Todos (ALL). Para determinadas config-

uraciones de Citrix Gateway, puede que deba seleccionar **COM**. La aplicación Citrix Workspace admite claves RSA de 1024, 2048 y 3072 bits. También se admiten certificados raíz con claves RSA de 4096 bits.

**Nota:**

Citrix no recomienda el uso de claves RSA de 1024 bits.

- **Cualquiera:** Cuando tiene el valor “Cualquiera”, la directiva no está configurada y se permite cualquiera de los siguientes conjuntos de cifrado:
  - a) TLS\_RSA\_WITH\_RC4\_128\_MD5
  - b) TLS\_RSA\_WITH\_RC4\_128\_SHA
  - c) TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
  - d) TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
  - e) TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
  - f) TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
  - g) TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- **Comercial:** Cuando tiene el valor “Comercial”, se permiten solo los conjuntos de cifrado siguientes:
  - a) TLS\_RSA\_WITH\_RC4\_128\_MD5
  - b) TLS\_RSA\_WITH\_RC4\_128\_SHA
  - c) TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
  - d) TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- **Gubernamental:** Cuando tiene el valor “Gubernamental”, se permiten solo los conjuntos de cifrado siguientes:
  - a) TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
  - b) TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
  - c) TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
  - d) TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- a) En el menú **Directiva de comprobación de revocación de certificados**, seleccione alguna de las siguientes opciones:
  - **Comprobar sin acceso a red:** Se lleva a cabo una comprobación de la lista de revocación de certificados. Solo se usan almacenes locales de listas de revocación de certificados. Se ignoran todos los puntos de distribución. No es obligatorio encontrar la lista de revocación de certificados para verificar el certificado que presenta el servidor de Traspaso SSL/Citrix Secure Web Gateway de destino.
  - **Comprobar con acceso completo:** Se lleva a cabo una comprobación de la lista de revocación de certificados. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Si se encuentra información de revocación de

un certificado, se rechaza la conexión. No es obligatorio encontrar una lista de revocación de certificados para la verificación del certificado del servidor presentado por el servidor de destino.

- **Requerir comprobación con acceso completo y lista de revocación de certificados:** Se hace una comprobación de listas de revocación de certificados, con exclusión de la entidad de certificación (CA) raíz. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Si se encuentra información de revocación de un certificado, se rechaza la conexión. Para la verificación, es necesario encontrar todas las listas de revocación de certificados requeridas.
  - **Requerir comprobación con acceso completo y todas las listas de revocación de certificados:** Se hace una comprobación de listas de revocación de certificados, incluida la entidad de certificación (CA) raíz. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Si se encuentra información de revocación de un certificado, se rechaza la conexión. Para la verificación, es necesario encontrar todas las listas de revocación de certificados requeridas.
  - **No comprobar:** No se comprueban listas de revocación de certificados.
- a) Puede restringir la aplicación Citrix Workspace para que solo pueda conectarse a servidores con una directiva de emisión de certificados concreta, mediante un **OID de extensión de directiva**. Cuando se selecciona **OID de extensión de directiva**, la aplicación Citrix Workspace solamente acepta certificados de servidor que contienen ese OID de extensión de directiva.
- b) En el menú **Autenticación del cliente**, seleccione alguna de las siguientes opciones:
- **Inhabilitada:** La autenticación de cliente está inhabilitada.
  - **Mostrar selector de certificados:** Pedir siempre al usuario que seleccione un certificado.
  - **Seleccionar automáticamente, si es posible:** Pedir al usuario que seleccione un certificado solo si hay varios para elegir.
  - **No configurado:** La autenticación del cliente no está configurada.
  - **Usar un certificado especificado:** Usar el certificado de cliente que esté definido en la opción “Certificado del cliente”.
- a) Use el parámetro **Certificado del cliente** para especificar la huella digital del certificado de identificación y evitar tener que preguntar al usuario innecesariamente.
- b) Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.

La tabla siguiente muestra los conjuntos de cifrado en cada grupo:

| 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 <sup>(1)</sup> | Y                                     |          | Y        | Y        |          | Y        | Y            |              | Y            |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 <sup>(1)</sup> | 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 <sup>(1) (2)</sup>   | X                                     |          |          |          |          |          |              |              |              |
| TLS_RSA_WITH_AES_128_GCM_SHA256 <sup>(1) (2)</sup>   | X                                     | X        |          |          |          |          |              |              |              |
| TLS_RSA_WITH_AES_256_CBC_SHA <sup>(2)</sup>          | X                                     |          |          |          |          |          |              |              |              |
| TLS_RSA_WITH_AES_128_CBC_SHA <sup>(2)</sup>          | X                                     | X        |          |          |          |          |              |              |              |
| TLS_RSA_WITH_RC4_128_SHA <sup>(2) (3)</sup>          | X                                     | X        |          |          |          |          |              |              |              |
| TLS_RSA_WITH_RC4_128_MD5 <sup>(2) (3)</sup>          | X                                     | X        |          |          |          |          |              |              |              |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA <sup>(2)</sup>         | 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                            |                                       |          |          |          |          |          |              |              |              |

## 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 un firewall en la implementación, la aplicación Citrix Workspace para Windows debe poder comunicarse a través de él con el servidor web y el servidor Citrix.

## Puertos comunes de comunicación Citrix

| Origen                              | Tipo | Puerto | Detalles                                      |
|-------------------------------------|------|--------|-----------------------------------------------|
| Aplicación Citrix Workspace         | TCP  | 80/443 | Comunicación con StoreFront                   |
| ICA/HDX                             | TCP  | 1494   | Acceso a aplicaciones y escritorios virtuales |
| ICA/HDX con fiabilidad de la sesión | TCP  | 2598   | Acceso a aplicaciones y escritorios virtuales |
| ICA/HDX por SSL                     | TCP  | 443    | Acceso a aplicaciones y escritorios virtuales |

Para obtener más información sobre los puertos, consulte el artículo [CTX101810](#) de Knowledge Center.

Si el firewall se ha configurado para la traducción de direcciones de red (NAT), use la Interfaz Web para definir las asignaciones desde las direcciones internas hacia las direcciones externas y los puertos.

Por ejemplo, si el servidor Citrix Virtual Apps and Desktops no se ha configurado con una dirección alternativa, puede configurar la Interfaz Web para proporcionar una dirección alternativa a la aplicación Citrix Workspace. Entonces, la aplicación Citrix Workspace se conecta al servidor mediante la dirección externa y el número de puerto.

## Servidor proxy

Se usan servidores proxy para limitar el acceso hacia y desde la red, así como para administrar las conexiones entre los servidores y la aplicación Citrix Workspace para Windows. La aplicación Citrix Workspace admite protocolos de proxy seguro y SOCKS.

En la comunicación con el servidor, la aplicación Citrix Workspace utiliza los parámetros del servidor proxy configurados de forma remota en el servidor que ejecuta Workspace para Web o la Interfaz Web. Para obtener más información sobre la configuración de servidores proxy, consulte la documentación de StoreFront o de la Interfaz Web.

En la comunicación con el servidor web, la aplicación Citrix Workspace utiliza los parámetros de servidor proxy configurados a través de la opción **Internet** del explorador web predeterminado en el dispositivo de usuario. Se deben configurar los parámetros de **Internet** del explorador web predeterminado en el dispositivo de usuario según corresponda.

Configure el proxy con el Editor del Registro para indicar a la aplicación Citrix Workspace que acepte o descarte el servidor proxy durante las conexiones.

### Advertencia

Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse.

1. Vaya a `\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\AuthManager`.
2. Defina **ProxyEnabled** (REG\_SZ).
  - True: La aplicación Citrix Workspace acepta al servidor proxy durante las conexiones.
  - False: La aplicación Citrix Workspace descarta al servidor proxy durante las conexiones.
3. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

## Servidor de confianza

El parámetro “Servidor de confianza” identifica y aplica relaciones de confianza en las conexiones de la aplicación Citrix Workspace.

Cuando se habilita “Servidor de confianza”, la aplicación Citrix Workspace especifica los requisitos y decide si la conexión con el servidor es de confianza o no. Por ejemplo, si la aplicación Citrix Workspace se conecta a una dirección determinada (como [https://\\\*.citrix.com](https://\*.citrix.com)) a través de un tipo de conexión específico (como TLS), se redirige a una zona de confianza en el servidor.

Al habilitar esta función, el servidor conectado reside en la zona **Sitios de confianza** de Windows. Para ver instrucciones detalladas sobre cómo agregar servidores a la zona **Sitios de confianza** de Windows, consulte la ayuda en línea de Internet Explorer.

Para habilitar la configuración de servidor de confianza mediante la plantilla administrativa de objetos de directiva de grupo

#### **Requisito previo:**

Debe salir de los componentes de la aplicación Citrix Workspace, incluida la Central de conexiones.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Workspace > Redirección de red > Configuración de servidores de confianza**.
3. Marque **Habilitado** para obligar a que la aplicación Citrix Workspace realice la identificación de la región.
4. Marque **Aplicar configuración de servidor de confianza**. Eso obliga al cliente a realizar la identificación mediante un servidor de confianza.
5. Desde la lista desplegable **Zona de Internet de Windows**, seleccione la dirección del servidor de cliente. Esta configuración solo se aplica a la zona “Sitios de confianza” de Windows.
6. En el campo **Dirección**, establezca la dirección del servidor de cliente en una zona “Sitios de confianza” que no sea Windows. Puede utilizar una lista separada por comas.
7. Haga clic en **Aceptar** y **Aplicar**.

#### **ICA File Signing**

La función ICA File Signing (firma de archivos ICA) permite protegerse ante inicios no autorizados de escritorios y aplicaciones. La aplicación Citrix Workspace verifica si el inicio de la aplicación o del escritorio fue generado desde una fuente de confianza, basándose en una directiva de administración, y protege al usuario frente a inicios originados en servidores que no son de confianza. Puede configurar ICA File Signing mediante la plantilla administrativa de objetos de directiva de grupo o StoreFront. La función ICA File Signing no está habilitada de forma predeterminada.

Para obtener información sobre cómo habilitar ICA File Signing para StoreFront, consulte [Habilitar ICA File Signing](#) en la documentación de StoreFront.

Para la implementación de Interfaz Web, la Interfaz Web habilita y configura los inicios de escritorios y aplicaciones para incluir una firma durante el proceso de inicio mediante el servicio Citrix ICA File Signing. Este servicio permite firmar los archivos ICA con un certificado proveniente del almacén de certificados personal del equipo.

## Configurar la firma del archivo ICA

### Nota:

Si no se agrega CitrixBase.admx\adml al objeto de directiva de grupo (GPO) local, la directiva **Habilitar ICA File Signing** puede no estar presente.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix**.
3. Seleccione la directiva **Habilitar ICA File Signing** y seleccione una de las opciones según sea necesario:
  - a) **Habilitada**: Indica que puede agregar el sello del certificado con firma a la lista de sellos de certificados de confianza permitidos.
  - b) **Certificados de confianza**: Haga clic en **Mostrar** para eliminar el sello del certificado con firma existente en la lista de permitidos. Puede copiar y pegar los sellos de certificados con firma desde las propiedades de los certificados.
  - c) **Directiva de seguridad**: Seleccione una de las siguientes opciones en el menú.
    - i. **Permitir inicios con firma solamente (más seguro)**: Permite los inicios de solamente escritorios o aplicaciones con firma desde servidores de confianza. Aparece una advertencia de seguridad en caso de una firma no válida. No puede iniciar la sesión debido a que no se autoriza.
    - ii. **Preguntar al usuario en inicios sin firma (menos seguro)**: Aparece un mensaje cuando se inicia una sesión sin firma o sin firma válida. Puede optar por continuar el inicio o cancelarlo (opción predeterminada).
4. Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.
5. Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

### Para seleccionar y distribuir un certificado de firma digital:

Cuando se seleccione un certificado de firma digital, Citrix recomienda elegir a partir de la lista siguiente, en el orden siguiente:

1. Adquiera un certificado con firma de código o un certificado con firma SSL a partir de una entidad de certificados (CA) pública.

2. Si su empresa dispone de una entidad de certificados privada, cree un certificado con firma de código o un certificado con firma SSL a través de la entidad de certificados privada.
3. Utilice un certificado SSL existente, como el certificado del servidor de la Interfaz Web.
4. Cree un certificado raíz y distribúyalo a los dispositivos de usuario mediante un objeto de directiva de grupo o una instalación manual.

## Storebrowse

April 22, 2024

Storebrowse es una utilidad ligera de línea de comandos que se usa para interactuar entre el cliente y el servidor. Se usa para autenticar todas las operaciones en StoreFront y Citrix Gateway.

Para obtener información sobre la versión anterior de la utilidad Storebrowse para Citrix Receiver para Windows, consulte la documentación de [Storebrowse para Citrix Receiver para Windows](#).

Con la utilidad Storebrowse, los administradores pueden automatizar las siguientes operaciones cotidianas:

- Agregar un almacén.
- Enumerar las aplicaciones y los escritorios publicados de Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) desde un almacén configurado.
- Generar un archivo ICA manualmente seleccionando cualquier escritorio o aplicación publicados de Citrix Virtual Apps and Desktops y Citrix DaaS.
- Generar un archivo ICA mediante la línea de comandos de Storebrowse.
- Iniciar la aplicación publicada.

A partir de ahora, la utilidad Storebrowse forma parte del componente Authmanager. Después de instalar la aplicación Citrix Workspace, la utilidad Storebrowse se encuentra en la carpeta de instalación [AuthManager](#).

Puede confirmar si la utilidad Storebrowse está instalada junto con el componente [Authmanager](#). Para ello, consulte la ruta de registro de las siguientes maneras:

### **Cuando los administradores instalan la aplicación Citrix Workspace:**

---

En una máquina de 32 bits

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\AuthManager\Inst

En una máquina de 64 bits

[HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\A

---

### **Cuando los usuarios (no los administradores) instalan la aplicación Citrix Workspace:**

---

---

|                           |                                                      |
|---------------------------|------------------------------------------------------|
| En una máquina de 32 bits | [HKEY_CURRENT_USER\SOFTWARE\Citrix\AuthManager\Insta |
| En una máquina de 64 bits | [HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\Au    |

---

### **Requisitos**

Instale la aplicación Citrix Workspace para Windows 1808 o posterior para que la utilidad Storebrowse funcione sin problemas entre StoreFront y Citrix Gateway. La versión 1809 de Citrix Workspace requiere un mínimo de 530 MB de espacio libre en disco y 2 GB de RAM para su instalación.

### **Tabla de compatibilidad**

La utilidad Storebrowse es compatible con estos sistemas operativos:

---

#### Sistema operativo

---

- Windows 10 (ediciones de 32 y 64 bits)
  - Windows 8.1 (ediciones de 32 y 64 bits)
  - Windows 7 SP1 (ediciones de 32 y 64 bits)
  - Windows Thin PC
  - Windows Server 2016
  - Windows Server 2012 R2, ediciones Standard y Datacenter
  - Windows Server 2012, ediciones Standard y Datacenter
  - Windows Server 2008 R2, edición de 64 bits
  - Windows Server 2008 R2, edición de 64 bits
- 

### **Conexiones**

La utilidad Storebrowse admite estos tipos de conexiones:

- Almacén HTTP
- Almacén HTTPS
- Citrix Gateway 11.0 y versiones posteriores

**Nota:**

La utilidad Storebrowse no acepta credenciales introducidas desde la línea de comandos cuando se tiene un almacén HTTP.

## Métodos de autenticación

**Servidores de StoreFront** StoreFront admite diferentes métodos de autenticación para acceder a los almacenes; sin embargo, no todos se recomiendan. Por motivos de seguridad, algunos de los métodos de autenticación están inhabilitados de forma predeterminada cuando se crea un almacén.

- **Nombre de usuario y contraseña:** Los usuarios pueden introducir sus credenciales y autenticarse cuando acceden a los almacenes. La autenticación explícita está habilitada de forma predeterminada cuando crea su primer almacén. Todos los métodos de acceso de usuario son compatibles con la autenticación explícita.
- **PassThrough de dominio:** Los usuarios realizan la autenticación en los equipos unidos a un dominio de Windows y su sesión se inicia automáticamente cuando acceden a los almacenes. Para poder usar esta opción, la autenticación PassThrough debe estar habilitada cuando se instala la aplicación Citrix Workspace en los dispositivos de los usuarios. Para obtener más información sobre cómo configurar la autenticación PassThrough de dominio, consulte [Configurar la autenticación PassThrough](#).
- **Autenticación HTTP básica:** La utilidad Storebrowse requiere que la autenticación HTTP básica esté habilitada para poder comunicarse con los servidores de StoreFront. Esta opción está inhabilitada de forma predeterminada en el servidor de StoreFront. Debe habilitar el método de autenticación HTTP básica.

La utilidad Storebrowse permite la autenticación de cualquiera de estas maneras:

- Mediante el componente [AuthManager](#), integrado en la utilidad Storebrowse. Nota: Debe habilitar el método de autenticación HTTP básica en StoreFront mientras trabaje con la utilidad Storebrowse. Esto es aplicable cuando el usuario proporciona las credenciales mediante los comandos de Storebrowse.
- Componente [Authmanager](#) externo que se puede incluir con la aplicación Citrix Workspace para Windows.

## Citrix Gateway

A partir de la versión más reciente de la utilidad Storebrowse, puede agregar una URL de Citrix Gateway. No se requiere configuración adicional en la utilidad Storebrowse para comunicarse con Citrix Gateway.

## Single Sign-On en Citrix Gateway

Además de la recién agregada compatibilidad con Citrix Gateway, ahora puede usar Single Sign-On en él. Puede agregar un nuevo almacén y enumerar los recursos publicados sin tener que proporcionar sus credenciales de usuario.

Para obtener más información sobre la disponibilidad de Single Sign-On en Citrix Gateway, consulte [Disponibilidad de Single Sign-On en Citrix Gateway](#).

### Nota:

Esta función solo se admite en máquinas unidas a dominio en las que Citrix Gateway está configurado con el método de autenticación Single Sign-On.

## Iniciar una aplicación o un escritorio publicado

Ahora puede iniciar un recurso directamente desde el almacén, sin tener que usar ningún archivo ICA.

## Uso de comandos

En la siguiente sección se ofrece información detallada sobre los comandos que se pueden usar desde la utilidad Storebrowse.

### -a, -addstore

#### Descripción:

Agrega un nuevo almacén. Devuelve la dirección URL completa del almacén. Si esto falla, se notifica un error.

### Nota:

Puede agregar varios almacenes mediante la utilidad Storebrowse.

#### Ejemplo de comando en StoreFront:

Comando:

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of Storefront*
```

Ejemplo:

```
'\storebrowse.exe -U {nombre de usuario} -P {contraseña} -D {dominio} -a https://mi.primeralmacéndeejemplo.n
```

### **Ejemplo de comando en Citrix Gateway:**

Comando:

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of CitrixGateway*
```

Ejemplo:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -a <https://mysecondexample.com>
```

/?

### **Descripción:**

Ofrece información detallada sobre el uso de la utilidad Storebrowse

### **(-l), -liststore**

#### **Descripción:**

Ofrece una lista de los almacenes que agrega el usuario.

#### **Ejemplo de comando en StoreFront:**

```
.\storebrowse.exe -l
```

#### **Ejemplo de comando en Citrix Gateway:**

```
.\storebrowse.exe -l
```

### **(-M 0x2000 -E)**

#### **Descripción:**

Enumera los recursos disponibles

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Ejemplo de comando en Citrix Gateway:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E <https://my.secondexample.net>
```

## **-q, –quicklaunch**

### **Descripción:**

Genera el archivo ICA requerido para las aplicaciones y los escritorios publicados mediante la utilidad Storebrowse. La opción de inicio rápido requiere una URL de inicio como entrada junto con la URL del almacén, que puede ser la URL del servidor de StoreFront o la URL de Citrix Gateway. El archivo ICA se genera en el directorio %LocalAppData%\Citrix\Storebrowse\cache.

Puede obtener la URL de inicio para cualquier aplicación y escritorio publicados ejecutando el siguiente comando:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

Una URL de inicio típica es similar a la siguiente:

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/Stress/resources/v2/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q { Launch_URL_of_published_apps_and_desktops } <https://my.firstexamplestore.net/Citrix/Store/resources/v2/Q2hJk0lmNoPQrSTV9y/launch/ica> <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Ejemplo de comando en Citrix Gateway:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q { Launch_URL_of_published_apps_and_desktops } <https://my.secondexamplestore.com>
```

## **-L, –launch**

### **Descripción:**

Genera el archivo ICA requerido para las aplicaciones y los escritorios publicados mediante la utilidad Storebrowse. La opción de inicio requiere el nombre del recurso junto con la URL del almacén, que puede ser la URL del servidor de StoreFront o la URL de Citrix Gateway. El archivo ICA se genera en el directorio %LocalAppData%\Citrix\Storebrowse\cache.

Puede obtener el nombre simplificado de las aplicaciones y los escritorios publicados ejecutando el siguiente comando:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

Este comando da como resultado lo siguiente:

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/
/Stress/resources/v2/Q29udHJvbGxlc5DYWxjdWxhdG9y/launch/ica
```

El nombre en negrita en el resultado anterior se usa como parámetro de entrada para la opción de inicio.

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L
“{ Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/
discovery>
```

Ejemplo de comando en Citrix Gateway:

```
<.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L {
Resource_Name } https://my.secondexamplestore.com>
```

## **-S, -sessionlaunch**

### **Descripción:**

Puede agregar el almacén, enumerar los recursos publicados (aplicaciones y escritorios) e iniciar el recurso con un solo comando. Esta opción toma lo siguiente como parámetros: nombre de usuario, contraseña, dominio, nombre descriptivo del recurso que se iniciará y la URL del almacén. Sin embargo, si el usuario no proporciona las credenciales, se inicia una solicitud de **AuthManager** que insta a escribir las credenciales a fin de poder iniciar el recurso.

Puede obtener el nombre del recurso de aplicaciones y escritorios publicados ejecutando el siguiente comando:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/
Second/discovery
```

Este comando da como resultado lo siguiente:

```
'Controller.Calculator' 'Calculator' '\ ' 'http://abc-sf.xyz.com/Citrix/
/Stress/resources/v2/Q29udHJvbGxlc5DYWxjdWxhdG9y/launch/ica
```

El nombre en negrita en el resultado anterior se usa como parámetro de entrada para la opción **-S**.

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S “
{ Friendly_Resource_Name } <https://my.firstexamplestore.net/Citrix/
Store/discovery >
```

Ejemplo de comando en Citrix Gateway:

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S { Friendly_Resource_Name } <https://my.secondeXamplestore.com>
```

### **-f, -filefolder**

#### **Descripción:**

Genera el archivo ICA requerido en la ruta personalizada definida en la opción -f para las aplicaciones y los escritorios publicados que utilizan la utilidad Storebrowse.

La opción de inicio requiere un nombre de carpeta junto con el nombre del recurso como entrada con la URL del almacén, que es la URL del servidor de StoreFront o la URL de Citrix Gateway.

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -f "C:\Temp\Launch.ica" -L "Resource_Name" { Store }
```

Ejemplo de comando en Citrix Gateway:

```
.\storebrowse.exe -f "C:\Temp\Launch.ica" -L "Resource_Name" { NSG_URL }
```

### **-t, -traceauthentication**

#### **Descripción:**

Genera registros para el componente integrado `AuthManager` de la utilidad Storebrowse. Los registros se generan solo si la utilidad Storebrowse está utilizando un `AuthManager` integrado. Los registros se generan en el directorio `localappdata%\Citrix\Storebrowse\logs`.

Nota: Esta opción no puede ser el último parámetro que aparece en la línea de comandos del usuario.

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a { StoreURL }
```

Ejemplo de comando en Citrix Gateway:

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a { NSG_URL }
```

## **-d, –deletestore**

### **Descripción:**

Elimina el almacén StoreFront o Citrix Gateway existente.

Ejemplo de comando en StoreFront:

```
.\storebrowse.exe -d https://my.firstexamplestore.net/Citrix/Store/discovery
```

Ejemplo de comando en Citrix Gateway:

```
.\storebrowse.exe -d https://my.seconexamplstore.com
```

## **Función Single Sign-On en Citrix Gateway**

Single Sign-On permite autenticarse en un dominio y usar las aplicaciones y los escritorios de Citrix Virtual Apps and Desktops y Citrix DaaS entregados por ese dominio sin necesidad de volver a autenticarse para cada aplicación o escritorio. Cuando agrega un almacén mediante la utilidad Storebrowse, las credenciales se transfieren al servidor Citrix Gateway, junto con las aplicaciones y los escritorios virtuales enumerados para usted, incluidos los parámetros del menú Inicio. Después de configurar el inicio Single Sign-On, puede agregar el almacén, enumerar las aplicaciones y los escritorios virtuales e iniciar los recursos necesarios sin tener que escribir sus credenciales varias veces.

Esta función es compatible con Citrix Gateway versión 11 y posteriores.

### **Requisitos previos:**

Si quiere ver los requisitos previos necesarios para configurar el inicio Single Sign-On en Citrix Gateway, consulte [Configurar la autenticación PassThrough de dominio](#).

La función Single Sign-On con Citrix Gateway puede habilitarse mediante la plantilla administrativa de objeto de directiva de grupo (GPO).

#### **Nota:**

Cuando actualice de Citrix Receiver a la aplicación Citrix Workspace o instale de cero la aplicación Citrix Workspace por primera vez, debe agregar los archivos de plantilla más recientes al GPO local. Para obtener más información sobre cómo agregar los archivos de plantilla al GPO local, consulte [Configurar la plantilla administrativa de objeto de directiva de grupo](#). En caso de una actualización, la configuración existente se conserva si se importan los archivos más recientes.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Autenticación de usuarios > Single Sign-On para Citrix Gateway**.

3. Utilice las opciones de activación o desactivación para habilitar o inhabilitar la opción Single Sign-On.
4. Haga clic en **Aplicar** y **Aceptar**.
5. Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

#### **Limitaciones:**

- El método de autenticación HTTP básica debe estar habilitado en el servidor de StoreFront para las operaciones de introducción de credenciales con la utilidad Storebrowse.
- Si tiene un almacén HTTP, la introducción de credenciales mediante la opción de línea de comandos no es posible cuando intenta conectarse al almacén mediante la utilidad para enumerar o iniciar las aplicaciones y los escritorios virtuales publicados. Como solución temporal, utilice el módulo [AuthManager](#) externo que se activa cuando no se proporcionan credenciales mediante la línea de comandos.
- Actualmente, la utilidad Storebrowse solo admite Citrix Gateway configurado en un único almacén en el servidor de StoreFront.
- La introducción de credenciales en la utilidad Storebrowse solo funciona si Citrix Gateway está configurado con el método de autenticación con factor único.
- Las opciones de línea de comandos [Username \(-U\)](#), [Password \(-P\)](#) y [Domain \(-D\)](#) de la utilidad Storebrowse distinguen entre mayúsculas y minúsculas, y deben contener solo mayúsculas.

## **Desktop Lock de la aplicación Citrix Workspace**

January 18, 2024

Puede usar Desktop Lock de la aplicación Citrix Workspace cuando no necesite interactuar con el escritorio local. Puede seguir usando Desktop Viewer (si está habilitado), pero solo verá el siguiente conjunto de opciones en la barra de herramientas:

- Ctrl+Alt+Supr
- Preferencias
- Dispositivos
- Desconectar.

Desktop Lock de la aplicación Citrix Workspace para Windows funciona en máquinas unidas a dominios que están habilitadas para el inicio de sesión SSON (Single Sign-On) y configuradas con un almacén. No admite sitios de PNA. Las versiones anteriores de Desktop Lock no se admiten después de actualizar a Citrix Receiver para Windows 4.2 o una versión posterior.

## Instalación de Desktop Lock mediante la interfaz de línea de comandos

### Requisitos previos:

- Debe ser administrador en un equipo unido al dominio.
- Single Sign-On debe estar habilitado.
- El almacén debe estar configurado.

1. Instale la aplicación Citrix Workspace con el siguiente comando:

```
1 `CitrixWorkspaceApp.exe /includeSSON /Silent STORE0= " AppStore;  
https://testserver.net/Citrix/MyStore/discover;on;Desktop App  
Store" `
```

2. Descargue el archivo `CitrixWorkspaceDesktopLock.msi` disponible en la página [Descargas de Citrix](#).
3. Instale Desktop Lock con el siguiente comando:

```
installationSilent : msexec /i CitrixWorkspaceDesktopLock.msi /  
qn
```

El escritorio publicado se inicia automáticamente después de iniciar sesión como usuario.

### Requisitos del sistema

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. Para obtener más información, consulte la página de [descargas de Microsoft](#).
- Se admite en Windows 7 (incluida Embedded Edition), Windows 7 Thin PC, Windows 8, Windows 8.1 y Windows 10 (incluida la actualización Anniversary Update).
- Se conecta a StoreFront solo a través de protocolos nativos.
- Los dispositivos de usuario deben estar conectados a una red de área local (LAN) o a una red de área extensa (WAN).

### Acceso a aplicaciones locales

#### Importante

Si se habilita el Acceso a aplicaciones locales se puede permitir el acceso al escritorio local, a menos que se haya aplicado un bloqueo completo mediante una plantilla de objeto de directiva de grupo o una directiva similar. Para obtener más información, consulte la sección [Configurar el acceso a aplicaciones locales y la redirección de URL](#) en la documentación de Citrix Virtual Apps and Desktops.

## Funcionamiento de Desktop Lock en la aplicación Citrix Workspace

- Puede usar Desktop Lock de la aplicación Citrix Workspace con las siguientes funcionalidades de la aplicación Citrix Workspace:
  - 3Dpro, Flash, USB, HDX Insight, plug-in de Microsoft Lync 2013 y acceso a aplicaciones locales
  - Solo autenticación de dominio, autenticación de dos factores o autenticación con tarjeta inteligente.
- Al desconectar la sesión de Desktop Lock de la aplicación Citrix Workspace, se cierra la sesión del dispositivo final.
- La redirección de Flash está inhabilitada en Windows 8 y versiones posteriores. La redirección de Flash está habilitada en Windows 7.
- Desktop Viewer está optimizado para Desktop Lock de la aplicación Citrix Workspace y no incluye las propiedades Inicio, Restaurar, Maximizar ni Pantalla.
- Ctrl+Alt+Supr está disponible en la barra de herramientas de Desktop Viewer.
- La mayoría de las teclas de acceso directo de Windows se pasan a la sesión remota, excepto Windows+L
- Ctrl+F1 activa Ctrl+Alt+Supr cuando se inhabilita la conexión o Desktop Viewer para conexiones de escritorio.

### Nota:

Con Desktop Lock instalado y `LiveInDesktopDisconnectOnLock` establecido en **False** en la ruta del Registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` o en `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`, la sesión activa se desconecta cuando el dispositivo de punto final sale de la hibernación o del modo de espera.

## Instalar Desktop Lock de la aplicación Citrix Workspace

Con este procedimiento, se instala la aplicación Citrix Workspace para Windows de forma que los escritorios virtuales aparezcan mediante Desktop Lock de la aplicación Citrix Workspace. En el caso de implementaciones que utilizan tarjetas inteligentes, consulte [Tarjeta inteligente](#).

1. Inicie sesión con una cuenta de administrador local.
2. En el símbolo del sistema, ejecute el siguiente comando (ubicado en los medios de instalación, en la carpeta Aplicación Citrix Workspace y Plug-ins > Windows > Aplicación Citrix Workspace).

Por ejemplo:

```
CitrixWorkspaceApp.exe /includeSSON STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/discovery;on;Desktop Store"
```

Para obtener información detallada sobre los comandos, consulte [Instalación](#).

1. En la misma carpeta de los medios de instalación, haga doble clic en `CitrixWorkspaceDesktopLock.msi`. Aparece el asistente de Desktop Lock. Siga las indicaciones.
2. Cuando se complete la instalación, reinicie el dispositivo de usuario. Si dispone de permisos para acceder a un escritorio e inicia sesión como un usuario de dominio, el dispositivo se muestra mediante Desktop Lock de la aplicación Citrix Workspace.

Para poder administrar el dispositivo de usuario una vez finalizada la instalación, la cuenta que se utilizó para instalar `CitrixWorkspaceDesktopLock.msi` se excluye del shell sustituto. Si, más adelante, esa cuenta se elimina, no podrá iniciar sesión ni administrar el dispositivo.

Para ejecutar una **instalación silenciosa** de Citrix Workspace Desktop Lock, use la siguiente línea de comandos:

```
msiexec /i CitrixWorkspaceDesktopLock.msi /qn
```

## Configurar Desktop Lock de la aplicación Citrix Workspace

Otorgue acceso solamente a un escritorio virtual que ejecute Desktop Lock de la aplicación Citrix Workspace por usuario.

Mediante directivas de Active Directory, impida que los usuarios pongan a hibernar los escritorios virtuales.

Para configurar Desktop Lock de la aplicación Citrix Workspace, use la misma cuenta de administrador que utilizó para instalarlo.

- Compruebe que los archivos `receiver.admx` (o `receiver.adml`) y `receiver_usb.admx` (.adml) se han cargado en las Directivas de grupo (las directivas aparecen en: Configuración del equipo o Configuración de usuario > Plantillas administrativas > Plantillas administrativas clásicas (ADMX) > Componentes de Citrix). Los archivos .admx están ubicados en `%Program-Files%\Citrix\ICA Client\Configuration\`.
- Preferencias de USB. Cuando un usuario conecta un dispositivo USB, ese dispositivo se comunica automáticamente de forma remota con el escritorio virtual, por lo que no se requiere ninguna interacción por parte del usuario. El escritorio virtual es el que controla el dispositivo USB y lo muestra en la interfaz de usuario.
  - Habilite la regla de directivas USB.
  - En Aplicación Citrix Workspace > Uso remoto de dispositivos cliente > Uso remoto de USB genérico, habilite y configure las directivas Dispositivos USB existentes y Dispositivos USB nuevos.
- Asignación de unidades: En Aplicación Citrix Workspace > Uso remoto de dispositivos cliente, habilite y configure la directiva Asignación de unidades del cliente.

- **Micrófono:** En Aplicación Citrix Workspace > Uso remoto de dispositivos cliente, habilite y configure la directiva Micrófono del cliente.

## **Configurar tarjetas inteligentes para su uso con Desktop Lock para Windows**

1. Configure StoreFront.
  - a) Configure XML Service para usar resolución de direcciones DNS para poder usar Kerberos.
  - b) Configure los sitios de StoreFront para el acceso mediante HTTPS, cree un certificado de servidor firmado por la entidad de certificación de su dominio y agregue un enlace HTTPS al sitio web predeterminado.
  - c) Compruebe que está habilitada la autenticación PassThrough con tarjeta inteligente (está habilitada de manera predeterminada).
  - d) Habilite Kerberos.
  - e) Habilite Kerberos y la autenticación PassThrough con tarjeta inteligente.
  - f) Habilite el Acceso anónimo en el sitio web predeterminado de IIS y use la Autenticación de Windows integrada.
  - g) Asegúrese de que el sitio web predeterminado de IIS no requiera SSL e ignore los certificados de cliente.
2. Use la Consola de administración de directivas de grupo para configurar las directivas de equipo local en el dispositivo de usuario.
  - a) Importe la plantilla Receiver.admx desde %ProgramFiles%\Citrix\ICA Client\Configuration\.
  - b) Expanda Plantillas administrativas > Plantillas administrativas clásicas (ADMX) > Componentes de Citrix > Citrix Workspace > Autenticación de usuarios.
  - c) Habilite Autenticación con tarjeta inteligente.
  - d) Habilite Nombre de usuario y contraseña locales.
3. Configure el dispositivo del usuario antes de instalar Desktop Lock de la aplicación Citrix Workspace.
  - a) Agregue la dirección URL de Delivery Controller en la lista de Sitios de confianza de Internet Explorer en Windows.
  - b) Agregue la URL del primer grupo de entrega a la lista de sitios de confianza de Internet Explorer en el formato escritorio://nombre-de-grupo-de-entrega.
  - c) Permita a Internet Explorer que utilice el inicio de sesión automático en caso de sitios de confianza.

Cuando Desktop Lock de la aplicación Citrix Workspace se instala en el dispositivo de usuario, se aplica una directiva de extracción de tarjetas inteligentes coherente. Por ejemplo, si la directiva de extracción de tarjetas inteligentes de Windows se establece en Forzar cierre de sesión para el escritorio, el usuario debe cerrar la sesión del dispositivo de usuario también, independientemente de cuál

sea la directiva de extracción de tarjeta inteligente configurada en el equipo. Esto garantiza que el dispositivo de usuario no quede en un estado inconsistente. Esto se aplica solo a los dispositivos de usuario con Desktop Lock de la aplicación Citrix Workspace.

## Eliminar Desktop Lock

Quite los dos componentes de la siguiente lista.

1. Inicie sesión con la misma cuenta de administrador local que usó para instalar y configurar Desktop Lock de la aplicación Citrix Workspace.
2. Con la función de Windows para quitar o cambiar programas:
  - Quite Desktop Lock de la aplicación Citrix Workspace.
  - Quite la aplicación Citrix Workspace para Windows.

## Pasar teclas de acceso directo de Windows a la sesión remota

La mayoría de las teclas de acceso directo de Windows se pasan a la sesión remota. Esta sección describe algunas de las más comunes.

### Windows

- Win+D: Minimizar todas las ventanas en el escritorio.
- Alt+Tab: Cambiar la ventana activa.
- Ctrl+Alt+Supr: A través de Ctrl+F1 y la barra de herramientas de Desktop Viewer.
- Alt+Mayús+Tab
- Windows+Tab
- Windows+Mayús+Tab
- Windows+Todas las teclas de caracteres

### Windows 8

- Win+C: Abrir accesos.
- Win+Q: Acceso Buscar.
- Win+H: Acceso Compartir.
- Win+K: Acceso Dispositivos.
- Win+I: Acceso Configuración.
- Win+Q: Buscar en Aplicaciones.
- Win+W: Buscar en Configuración.
- Win+F: Buscar archivos.

## Aplicaciones de Windows 8

- Win+Z: Ir a opciones de la aplicación.
- Win+. : Acoplar aplicación a la izquierda.
- Win+Mayús+. : Acoplar aplicación a la derecha.
- Ctrl+Tab: Navegar en ciclo por el historial de aplicaciones.
- Alt+F4: Cerrar una aplicación.

## Escritorio

- Win+D: Abrir escritorio.
- Win+,: Vistazo de escritorio.
- Win+B: Volver al escritorio.

## Otros

- Win+U: Abrir el Centro de accesibilidad.
- Ctrl+Esc: Pantalla Inicio.
- Win+Entrar: Abrir el Narrador de Windows.
- Win+X: Abrir el menú de configuración de herramientas del sistema.
- Win+Impr Pant: Toma una captura de pantalla y la guarda en Imágenes.
- Win+Tab: Abre una lista de cambio de ventana.
- Win+T: Vista previa de ventanas abiertas en la barra de tareas.

## SDK y API

June 9, 2023

### SDK de declaración de identidad de certificado

La declaración de identidad de certificado (CID SDK) permite a los desarrolladores crear un plug-in mediante el que la aplicación Citrix Workspace pueda autenticarse en el servidor de StoreFront con el certificado instalado en la máquina cliente. CID declara la identidad de la tarjeta inteligente del usuario en un servidor de StoreFront sin realizar una autenticación basada en tarjeta inteligente.

Para obtener más información, consulte la documentación de [CID SDK para la aplicación Citrix Workspace para Windows](#).

## Citrix Common Connection Manager SDK

Common Connection Manager (CCM) SDK proporciona un conjunto de interfaces API nativas que le permiten interactuar y realizar operaciones básicas mediante programación. Este SDK no requiere una descarga por separado porque forma parte del paquete de instalación de la aplicación Citrix Workspace para Windows.

### Nota:

Algunas de las API que están relacionadas con el inicio de sesiones requieren que el archivo ICA comience el proceso de inicio de las sesiones de aplicaciones y escritorios virtuales.

Las capacidades del CCM SDK incluyen:

- Lanzamiento de sesiones
  - Permite iniciar aplicaciones y escritorios, mediante el archivo ICA generado.
- Desconexión de sesiones
  - Similar a la operación de desconexión mediante la Central de conexiones. La desconexión puede hacerse para todas las sesiones o para un usuario concreto.
- Cierre de sesiones
  - Similar a la operación de cierre de sesión mediante la Central de conexiones. Se pueden cerrar todas las sesiones o la sesión de un usuario concreto.
- Información de la sesión
  - Proporciona diferentes métodos para obtener información relacionada con la conexión de las sesiones iniciadas. Esto incluye sesiones de escritorio, sesiones de aplicación y sesiones de aplicación integrada

Para obtener más información acerca del SDK, consulte la guía [Programmers guide to Citrix CCM SDK](#).

## 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 que usan 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) se usa con las funciones de canal virtual en el SDK de WF-API (Citrix Server API SDK) para crear nuevos canales virtuales. La función de canales virtuales proporcionada por VD-API está diseñada para simplificar la creación de sus propios canales virtuales.
- La API de Windows Monitoring, que mejora la experiencia visual y la compatibilidad con aplicaciones de terceros integradas con ICA.
- Código fuente operacional de 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, consulte la documentación de [Citrix Virtual Channel SDK para la aplicación Citrix Workspace para Windows](#).

### **API Credential Insertion de Fast Connect 3**

La API Credential Insertion de Fast Connect 3 ofrece una interfaz para suministrar credenciales de usuario a la función de inicio de sesión único o Single Sign-On (SSO) en la aplicación Citrix Workspace para Windows 4.2 y versiones posteriores. Con esta API, los socios de Citrix pueden ofrecer productos de autenticación y SSO que usen StoreFront o la Interfaz Web para iniciar sesiones de usuarios en aplicaciones o escritorios virtuales y luego desconectar a los usuarios de esas sesiones.

Para obtener más información, consulte la documentación [Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows](#).

### **Referencia para parámetros ICA**

June 9, 2023

En el archivo de referencia para parámetros ICA se ofrecen listas de parámetros de Registro y parámetros de archivos ICA, lo que permite a los administradores personalizar el comportamiento de la aplicación Citrix Workspace. También puede usar la Referencia para parámetros ICA a fin de solucionar problemas relacionados con un comportamiento inesperado de la aplicación Citrix Workspace.

[Referencia para parámetros ICA \(descarga en PDF\)](#)



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, 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).