



Aplicación Citrix Workspace 2203.1 LTSR para Windows

Contents

Acerca de esta versión	2
Problemas resueltos	3
Problemas conocidos	21
Avisos legales de terceros	23
Requisitos del sistema y compatibilidad	23
Instalación y desinstalación	32
Implementación	45
Actualización	54
Introducción	62
Configurar	82
Configurar Single Sign-On en la aplicación Citrix Workspace	182
Autenticación	185
Proteger comunicaciones	205
Storebrowse	216
Desktop Lock de la aplicación Citrix Workspace	226
Kit de desarrollo de software (SDK) y API	232
Referencia para parámetros ICA	234

Acerca de esta versión

March 6, 2024

Novedades en la versión 2203.1 LTSR

La aplicación Citrix Workspace 2203.1 CU6 es la versión Long Term Service Release (LTSR) más reciente de la aplicación Citrix Workspace para Windows.

Nota:

Esta versión admite las funciones incluidas entre la aplicación Citrix Workspace 2002 para Windows y la aplicación Citrix Workspace 2202 para Windows, excepto aquellas relacionadas con los componentes mencionados en la sección [Exclusiones destacables](#).

Mejora en la redirección de audio

Compatibilidad mejorada con eliminación de eco en todos los códecs de audio, incluidos los códecs de audio adaptable y todos los códecs de audio antiguos.

Optimización de Microsoft Teams

- **Mejora en App Protection y Microsoft Teams:** Microsoft Teams admite el uso compartido de pantallas y vídeos entrantes cuando la aplicación Citrix Workspace para Windows con App Protection habilitada está en modo **Desktop Viewer** únicamente. Las aplicaciones publicadas en modo integrado no representan el vídeo entrante ni las pantallas compartidas.

Continuidad del servicio

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

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

Problemas resueltos

June 14, 2024

Aplicación Citrix Workspace 2203.1 LTSR CU6 parche rápido 1 para Windows

Comparado con: La aplicación Citrix Workspace 2203.1 LTSR CU6

- Es posible que se produzca un error al iniciar si `wfica32.exe` deja de responder al utilizar la aplicación Citrix Workspace para Windows versión 2203.1 LTSR CU6. [CVADHELP-24770]
- Es posible que las claves de controlador virtual personalizadas no se conserven al desinstalar la aplicación Citrix Workspace para Windows. [CVADHELP-24513]

Aplicación Citrix Workspace 2203.1 LTSR CU6 para Windows

Comparado con: aplicación Citrix Workspace 2203.1 LTSR CU5

Sesión/Conexión

- Si se habilitó la concesión de conexiones para un almacén en la nube, la aplicación Citrix Workspace para Windows inicia las sesiones correctamente, incluso después de superar el límite de sesiones. [CVADHELP-23771]
- `qlaunch` puede fallar por primera vez cuando `selfservicemode` se establece en `false`. [CVADHELP-24414]
- Si la configuración del proxy WPAD está configurada en una máquina cliente cuando se produce la confiabilidad de la sesión, el proceso `wfica32.exe` deja de responder. [CVADHELP-23873]
- Si el archivo ICA o la carpeta en la que está presente el archivo ICA tienen caracteres Unicode en el nombre, es posible que no pueda iniciar las sesiones. Este problema solo se produce en el inicio híbrido. [CVADHELP-23843]
- Es posible que la versión 2212 de la aplicación Citrix Workspace para Windows no cumpla las condiciones establecidas en el archivo PAC del proxy. [CVADHELP-22503]

Experiencia de usuario

- Al cambiar la configuración del almacén mediante la plantilla de objetos de directiva de grupo o mediante la línea de comandos, es posible que se muestre una pantalla en blanco. [CVADHELP-23801]

- La funcionalidad de actualización puede fallar con los almacenes en la nube de dominios personalizados. [CVADHELP-23733]
- Cuando se configuran varias cuentas mediante GPO y se habilita cualquier cuenta inhabilitada, la aplicación Citrix Workspace siempre cambia a la vista de todas las cuentas en lugar de a la cuenta única seleccionada. [CVADHELP-24018]
- Si tiene el IME japonés de Google habilitado con el modo IME de experiencia óptima de Citrix, es posible que no pueda eliminar los cuadros de texto en PowerPoint con la tecla de **suprimir**. [CVADHELP-23605]
- Si una sesión de HDX a pantalla completa está enfocada y el punto final está bloqueado mediante **Ctrl+Alt+Del**, es posible que los usuarios no puedan escribir nada después de desbloquearlo. [CVADHELP-24512]
- Es posible que observe que la aplicación se abre incluso después de cerrar la aplicación Citrix Workspace cuando resalta una aplicación mediante la ficha, cierra la aplicación Citrix Workspace y después presione **Intro**. [CVADHELP-22700]

Excepciones del sistema

- Al actualizar el VDA a Citrix Virtual Apps and Desktops 2308 o una versión posterior, es posible que la aplicación Citrix Workspace deje de responder al iniciar ventanas de aplicaciones publicadas en modo integrado. [CVADHELP-23976]
- En máquinas cliente que no estén en inglés, si la aplicación publicada tiene un título Unicode, `wfica32.exe` no es compatible con los componentes de Analytics. [CVADHELP-24471]

Ventanas integradas

- Si mueve una aplicación a otro monitor y la minimiza, es posible que la aplicación no se abra correctamente en la vista maximizada. Puede probar a cerrar la aplicación para después abrirla de nuevo. [CVADHELP-23703]

Instalación, desinstalación y actualización

- Es posible que las claves de controlador virtual personalizadas no se conserven al desinstalar la aplicación Citrix Workspace. [CVADHELP-24513]

Problemas en el dispositivo cliente

- Es posible que el **módulo biométrico Bloomberg Keyboard 5** no se conecte automáticamente incluso cuando la redirección automática de los dispositivos USB del cliente esté activada. [CVADHELP-22673]

Interfaz de usuario

- Es posible que Citrix Workspace no pueda enumerar los recursos publicados durante un breve período de tiempo al conectarse a una URL de Global Server Load Balancing (GSLB). Este problema se produce cuando el servidor StoreFront establecido detecta algún problema que provoca un cambio de dirección IP virtual (VIP) controlada por GSLB en el dispositivo de punto final. [CVADHELP-22467]
- Es posible que no pueda agregar un almacén si el dominio de nivel superior (TLD) de la URL del almacén tiene menos de dos caracteres o cuando no hay ningún TLD. [CVADHELP-23973]

Inicio de sesión/Autenticación

- Es posible que la aplicación Citrix Workspace con autenticación SAML2 y FAS no pueda iniciar sesión automáticamente al desbloquear la sesión, incluso cuando el control del espacio de trabajo **WSCReconnectMode** está establecido en **Reconectarse al iniciar sesión en Windows** y está habilitada la directiva **Autenticación silenciosa para Citrix Workspace**. [CVADHELP-23018]

Aplicación Citrix Workspace 2203.1 LTSR CU5 para Windows

Comparado con: La aplicación Citrix Workspace 2203.1 LTSR CU4

HDX Plug and Play

- Si se configuran dispositivos USB nuevos y existentes para la denegación, es posible que siga apareciendo este mensaje:

Citrix Workspace detectó uno o más dispositivos conectados a su equipo. Para conectar los dispositivos a la sesión, haga clic aquí.

[CVADHELP-23506]

Instalación, desinstalación y actualización

- Tras reiniciar un dispositivo cliente de punto final, es posible que no se pueda realizar la comprobación periódica de actualizaciones automáticas antes de iniciar sesión. [CVADHELP-23054]
- Una vez completada la instalación de la aplicación Citrix Workspace, es posible que aparezca un mensaje de error irrecoverable al configurar un almacén mediante un GPO o una línea de comandos. [CVADHELP-23345]

Teclado

- En un caso de doble salto, es posible que la tecla **Alt+Tab** no funcione en los clientes de macOS. [CVADHELP-23085]

Sesión/Conexión

- Al conectarse a un escritorio mediante el modo [Redirección de caché](#) y si se produce un error en la [Alta disponibilidad](#) de ADC, es posible que no pueda conectarse de nuevo a un escritorio mediante el modo Redirección de caché. [CVADHELP-22881]
- Es posible que no pueda iniciar la aplicación Citrix Workspace con la API del SDK de ICO después de actualizar a una versión más reciente. [CVADHELP-22940]
- Si el modo de autoservicio está establecido en **False** y la función de bloqueo de escritorio está habilitada, es posible que no pueda agregar almacenes ni iniciar escritorios. [CVADHELP-23052]
- Es posible que el contenido de aplicaciones publicadas aparezca congelado para algunos usuarios de forma aleatoria. El problema se produce cuando la conexión TCP se establece antes de la conexión UDP y la detección de MTU de EDT no se activa al cambiar de TDP a UDP. [CVADHELP-23253]
- Al cerrar sesión en un dispositivo de punto final, es posible que el proceso wfica32.exe deje de responder y bloquee el cierre de sesión. [CVADHELP-23617]

Experiencia de usuario

- Es posible que no pueda iniciar sesión en la aplicación Citrix Workspace mediante Single Sign-On o que no vea la solicitud de autenticación en los almacenes de la nube. El problema se produce cuando la cuenta se configura mediante el GPO o la línea de comandos por primera vez y cuando el modo de autoservicio se establece en False y la directiva de autenticación silenciosa en Citrix Workspace está habilitada. [CVADHELP-22641]

- Es posible que la VPN de Citrix cierre sesión cuando usted cierre sesión en la aplicación Citrix Workspace, a pesar de que la VPN se haya desacoplado del valor del Registro **DisableIconHide**, que está establecido en **1**. [CVADHELP-22916]
- Es posible que la incorporación de cuentas de almacén tarde mucho tiempo o que falle en el dispositivo de punto final sin acceso a Internet o cuando no se pueda acceder al servidor de Global App Config. [CVADHELP-22999]
- Es posible que el ejecutable de SelfService se ejecute aunque no se haya agregado ninguna cuenta a la aplicación Citrix Workspace. [CVADHELP-23124]

Interfaz de usuario

- Al abrir un escritorio publicado con caracteres Unicode, es posible que el nombre de Desktop Viewer no se pueda leer bien. El problema solo se produce con el modo Internet Explorer (IE) de Microsoft Edge. [CVADHELP-22925]

Aplicación Citrix Workspace 2203.1 LTSR CU4 para Windows

Comparado con: La aplicación Citrix Workspace 2203.1 LTSR CU3

Redirección de contenido

- Con la corrección, puede evitar la comprobación del ping y permitir el redireccionamiento automático de la URL en una redirección de host a cliente.
 - Para evitar la comprobación del ping en una redirección de host a cliente, establezca la siguiente clave de Registro:
HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Citrix/ICA Client/SFTA
Nombre: OverridePingCheck
Tipo: REG_DWORD
Valor: 1
 - Para permitir la redirección automática de URL en la redirección de host a cliente, establezca la siguiente clave de Registro:
HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Citrix/ICA Client/SFTA
Nombre: OverridePreventAutoRedirect
Tipo: REGREG_DWORD
Valor: 1

[CVADHELP-22824]

Instalación, desinstalación y actualización

- Cuando se intenta actualizar la aplicación Citrix Workspace para Windows a la versión 1912 CU2 o una versión anterior instalada con la opción **Habilitar App Protection**, la operación pueden fallar y puede mostrarse este mensaje de error:

No se pudo iniciar el servicio ‘AppProtection Service’(entryprotectsvc). Compruebe que dispone de suficientes privilegios para iniciar servicios del sistema.

[CVADHELP-22404]

- Es posible que el comando `CitrixReceiverUpdater.exe` no actualice la configuración de **actualización automática**, como **AutoUpdateStream** si la configuración de actualización automática se cambió anteriormente desde **Preferencias avanzadas > Actualizaciones de Citrix Workspace**. [CVADHELP-22840]

Sesión/Conexión

- Es posible que se tarde en agregar almacenes debido a las solicitudes de verificación de revocación de certificados del almacén. Como solución temporal, puede omitir la comprobación de la revocación de certificados mediante este Registro:

- HKEY_LOCAL_MACHINE/Software/wow6432node/Citrix/Receiver

Nombre: SkipStoreCertificateRevocationCheck

Tipo: DWORD

Valor: 1

O bien,

- HKEY_CURRENT_USER/Software/Citrix/Receiver

Nombre: SkipStoreCertificateRevocationCheck

Tipo: DWORD

Valor: 1

[CVADHELP-21931]

- Es posible que la sesión se desconecte si hace clic en **Desktop Viewer** y cambia el tamaño de un escritorio publicado de forma continua. [CVADHELP-22063]

- Los intentos de volver a conectarse a determinadas versiones de escritorio que no estén en inglés mediante la reconexión automática de clientes pueden fallar y mostrarse un mensaje de error. [CVADHELP-22507]
- Es posible que H.265 a pantalla completa de Thinwire recurra a H.264 con la aplicación Citrix Workspace 2203.1 LTSR CU3 para Windows. [CVADHELP-22919]

Excepciones del sistema

- El proceso msedgewebview2.exe puede provocar un uso elevado de la CPU cuando se ejecuta el autoservicio. [CVADHELP-21610]
- El proceso wfica32.exe puede cerrarse de manera imprevista durante una sesión de usuario con redirección de cámaras web HDX. [CVADHELP-22249]
- El proceso wfica32.exe puede cerrarse de manera imprevista al cerrar la sesión. [CVADHELP-22329]

Experiencia de usuario

- La configuración de los accesos directos de escritorio por aplicación puede tener prioridad de forma predeterminada. Además, es posible que establecer los accesos directos de escritorio en **False** en el lado del cliente no surta efecto. Con esta corrección y al establecer la siguiente clave de Registro, la configuración de los accesos directos de escritorio del lado del cliente anula la configuración de los accesos directos de escritorio de cada aplicación.

Configure la siguiente clave de Registro para anular la configuración de accesos directos de escritorio:

HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle

Nombre: ProviderSettingOverride

Tipo: REG_SZ

Valor: True

[CVADHELP-15550]

- En entornos de alta latencia, es posible que se observe un movimiento inestable en el cursor del mouse de la aplicación Citrix Workspace cuando la opción **Usar mouse relativo** está habilitada.

Para habilitar la corrección, modifique el archivo default.ica de StoreFront en C:\inetpub\wwwroot\Citrix\Sto

Agregue `RelMouseSyncTimeout=xxx(min 10 to max 1000)` a la sección [`WFClient`].

O bien,

Establezca la siguiente clave de Registro en el dispositivo punto final:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Mod

Nombre: RelMouseSyncTimeout

Tipo: CADENA

Valor: El valor mínimo es 10 y el valor máximo es 1000

[CVADHELP-21829]

- Es posible que no se puedan copiar y pegar archivos MSG de Microsoft Outlook local en un explorador publicado. [CVADHELP-22542]

Interfaz de usuario

- Al iniciar sesión en la aplicación Citrix Workspace, es posible que no se muestren aplicaciones y escritorios correspondientes a varias cuentas configuradas mediante GPO o la línea de comandos. Este problema se produce cuando el valor **CurrentAccount** de la clave de Registro de se establece en **AllAccount**, en Computer\HKEY_LOCAL_MACHINE\Software\wow6432Node\Citrix\Dazzle. [CVADHELP-21124]

- Es posible que reciba este mensaje de error cuando el valor del parámetro **AllowAddStore** se establece en **N** y se agrega un almacén HTTP mediante un objeto de directiva de grupo (GPO) o la interfaz de línea de comandos:

No se puede conectar con el servidor.

[CVADHELP-22184]

- En el caso de los almacenes de la nube, es posible que no pueda agregar cuentas mediante una URL de redirección. [CVADHELP-22438]
- Es posible que vea un nombre de almacén diferente al nombre que proporcionó en la aplicación Citrix Workspace. [CVADHELP-22452]
- Tras actualizar la versión de la aplicación Citrix Workspace para Windows a 2203 LTSR, es posible que vea una pantalla blanca. Este problema se produce al agregar y configurar un almacén por primera vez y, simultáneamente, actualizar y abrir la interfaz de usuario de autoservicio. [CVADHELP-22696]

Aplicación Citrix Workspace 2203.1 LTSR CU3 para Windows

Comparado con: La aplicación Citrix Workspace 2203.1 LTSR CU2

Problemas en el dispositivo cliente

- Si el valor de la directiva **RemoveOnLock** de dispositivos USB genéricos contiene letras mayúsculas, es posible que la directiva no pueda desconectar el dispositivo USB (por ejemplo, los paneles de firmas) en clientes bloqueados. [CVADHELP-21492]

HDX RealTime

- Cuando aparece un recordatorio de Microsoft Outlook durante una llamada de Microsoft Teams, aparece un cuadrado negro en la pantalla compartida de Microsoft Teams. [CVADHELP-19222]

Instalación, desinstalación y actualización

- Es posible que la función de acceso a aplicaciones locales no funcione en los dispositivos de usuario instalados con el sistema operativo en italiano. [CVADHELP-21986]
- Es posible que se produzca un error al intentar instalar la aplicación Citrix Workspace en Windows Server 2012 R2. Para obtener más información, consulte el artículo [CTX477888](#) de Knowledge Center. [CVADHELP-22116]

Teclado

- Al mantener presionada la tecla **Impr Pant**, es posible que la aplicación publicada en el lado del servidor reciba eventos VK_SNAPSHOT WM_KEYUP (capturas de pantalla tomadas) de forma continua. [CVADHELP-21209]

Inicio de sesión/Autenticación

- Si **Selfservicemode** está configurado en false, es posible que los almacenes agregados no se actualicen correctamente después de abrir la aplicación Citrix Workspace. Como resultado, la ventana de autenticación no aparece. [CVADHELP-20593]
- Es posible que el valor de tiempo de espera por inactividad no caduque si sale de la aplicación Citrix Workspace antes de alcanzar el valor de tiempo de espera establecido. Como resultado, es posible que más adelante pueda iniciar la aplicación Citrix Workspace sin necesidad introducir ninguna credencial. [CVADHELP-20912]
- Es posible que no se puedan enumerar las aplicaciones mediante el comando **storebrowse** si la URL de Citrix Gateway utilizada es `**.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0x2000 -E { NSG_URL }`. [CVADHELP-21910]

Ventanas integradas

- En una sesión integrada, es posible que el mouse y el teclado del dispositivo de usuario se bloqueen de forma intermitente si la aplicación inhabilita y, a continuación, habilita su ventana en esa secuencia. [CVADHELP-21031]
- Al utilizar la función **Aero Snap de Windows** para mover una ventana maximizada de un monitor a otro más grande con Windows 11, es posible que la sesión desaparezca. [CVADHELP-21173]
- Al abrir una aplicación publicada en modo integrado, es posible que otras aplicaciones locales o integradas aparezcan en primer plano y tapen la aplicación publicada. [CVADHELP-20742, CVADHELP-21277]
- Es posible que las aplicaciones publicadas se abran en un estado no visible al iniciar la aplicación. [CVADHELP-21618]

Sesión/Conexión

- Es posible que la redirección del puerto COM esté bloqueada durante la itinerancia de sesiones. [CVADHELP-20959]
- Si la opción **Usar mouse relativo** está habilitada en una sesión de usuario, es posible que el clic principal (izquierdo) no funcione en el panel táctil. [CVADHELP-21223]
- En un entorno aislado, es posible que la aplicación Citrix Workspace intente conectarse al servidor de Global App Config aunque la directiva de **Global App Config Service** esté inhabilitada mediante GPO. Esto provoca una demora al agregar cuentas. [CVADHELP-21319]
- Citrix Analytics no puede recibir métricas relacionadas con la red de los usuarios finales. Este problema se produce incluso cuando se cumplen estos requisitos previos:
 - Las sesiones de aplicación o escritorio permanecen en ejecución durante más de 15 minutos con la aplicación Citrix Workspace.
 - El almacén o la cuenta utilizados están habilitados para CAS.

Nota:

Los eventos de CAS relacionados con la red no se envían para el inicio de aplicaciones o escritorios basado en explorador. Se envían solo cuando se abre una aplicación o un escritorio a través de la web y desde el mismo almacén que se agrega a través de la aplicación Citrix Workspace nativa.

[CVADHELP-21448]

- A veces, es posible que las aplicaciones publicadas en un escritorio publicado no se inicien y la aplicación Citrix Workspace deje de responder. [CVADHELP-21604]

- Es posible que no pueda acceder a la aplicación Citrix Workspace para Windows cuando la VPN se desconecta o se conecta de nuevo. [CVADHELP-21662]
- Es posible que el proceso Windocker.exe genere de forma incorrecta solicitudes de red salientes a varias direcciones IP. [CVADHELP-21728]
- Es posible que, al usar la reconexión automática de clientes, se demore la conexión a una sesión. [CVADHELP-21738]
- Al intentar configurar varios almacenes mediante un objeto de directiva de grupo (GPO) o una línea de comandos, es posible que uno de los almacenes no esté completamente configurado. [CVADHELP-22034]
- Es posible que haya eventos de descarga de archivos de Citrix Analytics, como los atributos de nombre y ruta de archivo, estén vacíos. [CVADHELP-22194]

Excepciones del sistema

- Al iniciar una aplicación publicada con la directiva **Audio adaptable** habilitada, es posible que el proceso wfica32 se cierre de forma inesperada. [CVADHELP-20999]
- Es posible que algunos archivos binarios de la aplicación Citrix Workspace no estén firmados, lo que provoca problemas de seguridad. [CVADHELP-21159]

Experiencia de usuario

- Al minimizar y maximizar un escritorio, es posible que no se conserve la ubicación de la barra de herramientas. [CVADHELP-21258]
- Al desconectarse y reconectarse a una sesión que está configurada en el modo de pantalla completa, es posible que no se conserve la ubicación de la barra de herramientas. [CVADHELP-21324]
- Es posible que experimente demoras a la hora de enumerar aplicaciones e iniciar aplicaciones o escritorios cuando utilice SSON en un entorno que no tiene acceso activo a sitios externos. Este problema se produce a partir de la versión 2210.5 de la aplicación Citrix Workspace y a partir de la versión 2203 CU2 de la aplicación Citrix Workspace. [CVADHELP-21786]

Interfaz de usuario

- Es posible que no pueda agregar un almacén oculto a la aplicación Citrix Workspace. Este problema ocurre cuando se intenta agregar un nombre de dominio completo (FQDN) de Citrix Gateway que requiere autenticación con tarjeta inteligente o cuando el nombre del almacén

de StoreFront contiene espacios; por ejemplo, <https://servername.company.com?StoreService>. [CVADHELP-21516]

- Una vez que se haya agregado un almacén con el token de autenticación del almacén establecido en **true**, es posible que Citrix Workspace deje de responder en la pantalla blanca y que el token de autenticación del almacén pase a estar en **false**. [CVADHELP-21582]
- Es posible que la pantalla muestre la ventana emergente de autenticación en la esquina superior izquierda en lugar de mostrarse en el centro. [CVADHELP-21835]
- Es posible que la barra de estado de WebView aparezca en la parte inferior de la aplicación Citrix Workspace al pasar el mouse por encima de cualquier aplicación o icono de escritorio publicado. [CVADHELP-22108]
- Al abrir una aplicación Citrix Workspace nativa y hacer clic con el botón secundario en la interfaz de usuario de autoservicio, es posible que aparezca un menú contextual. [CVADHELP-22131]

Aplicación Citrix Workspace 2203.1 LTSR CU2 para Windows

Comparado con: La aplicación Citrix Workspace 2203.1 LTSR CU1

Instalación, desinstalación y actualización

- Al instalar la aplicación Citrix Workspace como usuario del sistema mediante determinadas aplicaciones de terceros, es posible que aparezcan mensajes de error incorrectos en los registros de instalación. [CVADHELP-20695]

Teclado

- En un dispositivo Surface Pro, al elegir el teclado en pantalla en Desktop Viewer, es posible que el teclado no aparezca. [CVADHELP-20564]

Inicio de sesión/Autenticación

- Con esta corrección, puede suprimir la solicitud de autenticación de la vista web mientras se usa la autenticación Single Sign-On.

Para habilitar la corrección, establezca la siguiente clave de Registro:

HKEY_LOCAL_MACHINE/SOFTWARE/Wow6432Node/Citrix/AuthManager o HKEY_CURRENT_USER/SOFTWA

Nombre: HideAuthPrompt

Tipo: REG_SZ

Valor: True

[CVADHELP-20799]

Sesión/Conexión

- Es posible que la versión 2109 de la aplicación Citrix Workspace y posteriores omita los parámetros del archivo default.ica del servidor de StoreFront. [CVADHELP-20017]
- Al configurar una baliza interna predeterminada como la URL del almacén de StoreFront (por ejemplo, <https://example.com/Citrix/Store/discovery>) en la aplicación Citrix Workspace, es posible que las solicitudes HTTP HEAD que se envían a estas URL provoquen errores 404. [CVADHELP-20329]
- Es posible que, al iniciar una aplicación publicada a través de la aplicación Citrix Workspace en un dispositivo de punto final con más de ocho monitores, se produzca un error con este mensaje de error:

This version of Workspace doesn't support the selected encryption. Contacte con su administrador.

[CVADHELP-20555]

- Si el nombre del explorador web (BrowserName) de una aplicación publicada contiene caracteres de varios bytes, es posible que la aplicación no se inicie. El problema se produce en la versión 11 de Internet Explorer y con Microsoft Edge cuando se abre en modo Internet Explorer. [CVADHELP-20684]
- Al usar la aplicación Citrix Workspace para Windows 2106 o una versión posterior, es posible que la funcionalidad de proxy ICA saliente no funcione. [CVADHELP-20824]
- La aplicación Citrix Workspace le pide que seleccione un certificado aunque solo exista un certificado. Este problema se produce al autenticarse en el almacén (de la nube) de Workspace.

Para suprimir esta solicitud de certificado, agregue este Registro:

- En sistemas de 32 bits:

HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/Dazzle o HKEY_CURRENT_USER/SOFTWARE/Citrix/Dazzle

Nombre: SuppressCertSelectionPrompt

Tipo: REG_SZ

Valor: True

- En sistemas de 64 bits:

HKEY_LOCAL_MACHINE/Software/Wow6432Node/Citrix/Dazzle o HKEY_CURRENT_USER/Software/Wo

Nombre: SuppressCertSelectionPrompt

Tipo: REG_SZ

Valor: True

[CVADHELP-20844]

- Si la redirección de dispositivos USB del cliente está inhabilitada en una sesión existente e inicia una nueva sesión con la redirección habilitada, es posible que la redirección no funcione. [CVADHELP-20858]

Excepciones del sistema

- Es posible que Citrix Authentication Manager (AuthManSvr.exe) se cierre de forma inesperada durante el inicio de sesión. [CVADHELP-17233]
- Es posible que el proceso de wfica32.exe sufra una infracción de acceso y se cierre de forma inesperada. [CVADHELP-20558]
- Al desconectar un dispositivo de audio, es posible que el proceso wfica32.exe produzca una infracción de acceso y se cierre de forma inesperada. El problema se produce después de actualizar la aplicación Citrix Workspace para Windows a la versión 2203.1 LTSR CU1. [CVADHELP-21123]
- Es posible que Citrix Desktop Viewer (CDViewer.exe) se cierre de forma inesperada cuando el tamaño del archivo ICA es de 4096 bytes. [CVADHELP-21128]

Experiencia de usuario

- Es posible que la aplicación Citrix Workspace muestre una imagen borrosa al presionar Mayús+F2 varias veces en una sesión de usuario con Desktop Viewer inhabilitado. [CVADHELP-20467]
- Al iniciar una máquina VDA e iniciar sesión en una sesión de usuario por primera vez, es posible que deba mover el mouse de forma explícita para ver el cursor. [CVADHELP-20818]
- Al iniciar una aplicación integrada en el modo quiosco de Windows 10, el cursor del mouse no responde correctamente y es posible que las fuentes de texto aparezcan distorsionadas. [CVADHELP-20860]

Interfaz de usuario

- Es posible que la aplicación Citrix Workspace no responda después del inicio. [CVADHELP-20317]

- Es posible que no pueda acceder a la aplicación Citrix Workspace para Windows cuando la VPN se desconecta o se conecta de nuevo [CVADHELP-20376]
- Al agregar dos almacenes del mismo servidor de StoreFront mediante GPO, la configuración del segundo almacén podría fallar de forma intermitente. [CVADHELP-20655]
- Al agregar un almacén inhabilitado a través de un GPO y un almacén diferente del mismo servidor de StoreFront a través de una GUI, es posible que aparezca una pantalla de carga y que no se pueda agregar una cuenta. [CVADHELP-20776]

Aplicación Citrix Workspace 2203.1 LTSR CU1 para Windows

Comparado con: La aplicación Citrix Workspace 2203.1 LTSR

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]

HDX RealTime

- Durante llamadas entre dos usuarios con la optimización HDX de Microsoft Teams, es posible que el uso compartido de la ventana de una aplicación no se detenga después de iniciar y detener el uso compartido muchas veces, y es posible que no pueda compartir la pantalla del escritorio ni la ventana de la aplicación ni llamar ni recibir llamadas hasta que haya reiniciado la aplicación Citrix Workspace. [CVADHELP-20162]

Instalación, desinstalación y actualización

- Citrix Workspace: Es posible que el servicio actualizador no se inicie y se produzca un error de instalación. El problema se produce cuando el cliente no está conectado a Internet. [CVADHELP-19613]

Teclado

- Después de iniciar una sesión HDX, al cambiar de la ventana en primer plano a una ventana de aplicación local, es posible que las teclas del sistema, como **Windows** y **Alt+Tab**, las gestione la

sesión de Citrix en lugar del escritorio del PC local, a pesar de que la sesión de Citrix se ejecute en segundo plano. [CVADHELP-19778]

Inicio de sesión/Autenticación

- Después de iniciar sesión correctamente con la aplicación Citrix Workspace, es posible que aparezca un mensaje de inicio de sesión incorrecto con este mensaje:

Debe iniciar sesión para acceder a Citrix Workspace.

[CVADHELP-19676]

Ventanas integradas

- Al conectar o desconectar un monitor, es posible que la ventana integrada aparezca en una posición incorrecta. [CVADHELP-19168]

Sesión/Conexión

- Es posible que las sesiones RDP no se puedan iniciar en la aplicación Citrix Workspace 1912 LTSR CU6 para Windows cuando está habilitada la redirección de tarjetas inteligentes a través de RDP. [CVADHELP-19430]

- Cuando accede a un VDA por primera vez con la versión 2112 de la aplicación Citrix Workspace para Windows o una posterior, es posible que aparezca este mensaje de seguridad:

Una aplicación conectada está intentando acceder a la información en un dispositivo conectado al acceso a archivos HDX de su equipo.

En versiones anteriores, este mensaje solo aparecía durante el primer acceso a cada recurso publicado en un grupo de entrega y no en todos los VDA.

[CVADHELP-19636]

- Es posible que no se puedan iniciar aplicaciones o escritorios desde una tableta con la aplicación Citrix Workspace. El problema se produce cuando no se puede obtener la dirección IP del cliente. [CVADHELP-19703]
- Es posible que la configuración de almacenes mediante direcciones URL con DNS geográfico a través de un objeto de directiva de grupo o la línea de comandos no funcione si estableció `AllowAddStore=N` durante la instalación de la aplicación Citrix Workspace. [CVADHELP-19853]

- Al usar la aplicación Citrix Workspace 2204.1 o una versión posterior, es posible que la sesión se desconecte. Este problema se produce si hay una restricción para ejecutar binarios sin firmar, como, por ejemplo, wfica.ocx. [CVADHELP-20053]

Excepciones del sistema

- Es posible que, al arrastrar y colocar una ventana en una sesión de HDX, sea lento y provoque que el proceso wfica32.exe se cierre de forma inesperada. [CVADHELP-19482]
- La regla **AppLocker** del objeto de directiva de grupo bloquea la integración del plug-in de Citrix Gateway en Citrix Workspace. Como resultado, se crean varios archivos temporales con el formato VPNXXX.tmp en la carpeta temporal. Los archivos se crean incluso cuando la clave del Registro, HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client, tiene el valor **DisableIconHide**. [CVADHELP-19709]
- Esta corrección resuelve un problema poco frecuente de pérdida de memoria en el proceso wfica32.exe que se produce con la aplicación Citrix Workspace para Windows. [CVADHELP-19904]
- Es posible que las aplicaciones de Microsoft Office se cierren de forma inesperada cuando el servicio de protección de software no se inicia debido a componentes de App Protection defectuosos. [CVADHELP-20667]

Experiencia de usuario

- Es posible que arrastrar archivos desde el dispositivo del usuario y colocarlos en una aplicación publicada funcione la primera vez que se intenta hacerlo. Los intentos posteriores fallan y la aplicación no responde. [CVADHELP-17211]
- Si arrastra y coloca una ventana en una sesión HDX, la ventana tarda en recuperarse y el icono de la barra de tareas tarda en aparecer. [CVADHELP-19440]
- Es posible que la función de arrastrar y colocar no funcione al cerrar un cuadro de diálogo con la tecla **Esc** en una sesión integrada. [CVADHELP-19604]
- Al actualizar la aplicación Citrix Workspace desde la versión 2006 o una anterior, es posible que se eliminen las configuraciones de puerta de enlace y baliza de los almacenes existentes y se agreguen de nuevo las mismas configuraciones aunque las configuraciones de almacén no se modifican en el objeto de directiva de grupo. [CVADHELP-19839]
- El acceso a la URL de un almacén web desde la aplicación Citrix Workspace para Windows puede provocar que la ventana del espacio de trabajo aparezca en primer plano en lugar de aparecer en segundo plano después de cada intervalo de actualización. [CVADHELP-19885]

- Es posible que la aplicación Citrix Workspace siga enviando datos a <https://rttf.citrix.com> incluso después de que se inhabilite el programa Customer Experience Improvement Program (CEIP). [CVADHELP-20016]

Interfaz de usuario

- En la aplicación Citrix Workspace para Windows, al agregar direcciones URL de almacén mediante el objeto de directiva de grupo, es posible que aparezca este mensaje de error:

No se puede conectar con el servidor.

Este problema se produce si uno de los almacenes está inhabilitado y no se puede acceder a él. [CVADHELP-19751]

- Con esta corrección, aparece una página de inicio de sesión al cerrar sesión en la aplicación Citrix Workspace para Windows. Para habilitar la corrección, establezca la siguiente clave de Registro:

- En sistemas de 32 bits:

HKEY/LOCAL/MACHINE/Software/Citrix/Dazzle

Nombre: ShowSignInPageOnLogOff

Tipo: REG_SZ

Valor: True

- En sistemas de 64 bits:

HKEY/LOCAL/Software/Wow6432Node/Citrix/Dazzle

Nombre: ShowSignInPageOnLogOff

Tipo: REG_SZ

Valor: True

[CVADHELP-19967]

- Es posible que la notificación del estado de la batería y el cuadro de diálogo emergente del teclado automático no aparezcan durante la sesión cuando la directiva **Visualización automática del teclado** está habilitada en el DDC. [CVADHELP-19987]
- Al iniciar la aplicación Citrix Workspace por primera vez después de agregar la URL del almacén, aparece este mensaje de error:

Su aplicación Citrix Workspace encontró un error al inicializar Microsoft Edge WebView2. Reinicie la aplicación.

Este problema se produce al agregar la URL del almacén a través de un GPO o la línea de comandos, e incluye “/” tras la detección. Por ejemplo: <https://sales.example.com/Citrix/Store/discovery/;0n;Store>.

[CVADHELP-20214]

- Es posible que la barra de herramientas de **Desktop Viewer** no se vea al abrir el escritorio virtual desde almacenes de portales personalizados. [CVADHELP-20253]

Aplicación Citrix Workspace 2203.1 LTSR para Windows

Sesión/Conexión

- Es posible que el dispositivo Citrix ADC deje de responder cuando se desencadenen ciertas condiciones en la aplicación Citrix Workspace para Windows. [HDX-39683]
- Cuando intenta redirigir hacia la cámara web preferida conforme a la configuración establecida en la aplicación Citrix Workspace para Windows, es posible que no funcione del modo previsto. Con esta corrección, la cámara web preferida es la única cámara web disponible en la sesión de usuario. De esta forma, se logra un mayor control cuando hay varias cámaras web disponibles en la sesión de usuario.

[HDX-38214]

- 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]
- Es posible que, de manera intermitente, no se puedan agregar direcciones URL de Citrix Gateway y se muestre el siguiente mensaje de error:

No se pudo establecer contacto con el servicio de autenticación.

[CVADHELP-19415]

Problemas conocidos

March 6, 2024

Problemas conocidos en la versión 2203.1 LTSR CU6

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 2203.1 LTSR CU5

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 2203.1 LTSR CU4

- Es posible que no pueda iniciar sesiones si el nombre del archivo ICA o la carpeta en la que se descarga el archivo ICA tiene caracteres Unicode o que no estén en el abecedario inglés. Este problema solo se produce cuando accede a un almacén y se autentica mediante un explorador web y, a continuación, inicia aplicaciones o escritorios con la aplicación Citrix Workspace nativa. [CVADHELP-23843]

Problemas conocidos en la versión 2203.1 LTSR CU3

- Es posible que H.265 a pantalla completa de Thinwire recurra a H.264 con la aplicación Citrix Workspace 2203.1 LTSR CU3 para Windows. [CVADHELP-22919]

Problemas conocidos en la versión 2203.1 LTSR CU2

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 2203.1 LTSR CU1

No se han observado nuevos problemas conocidos en esta versión.

Problemas conocidos en la versión 2203.1 LTSR

- La instalación de la aplicación Citrix Workspace para Windows en modo sin conexión puede fallar cuando el instalador no encuentra Microsoft Edge WebView2 en el sistema.

Como solución temporal, instale **MicrosoftEdgeWebView2RuntimeInstallerX86.exe** como administrador y, a continuación, instale la aplicación Citrix Workspace para Windows.

[RFFWIN-26329]

- Es posible que la notificación del estado de la batería y el cuadro de diálogo emergente del teclado automático no aparezcan durante la sesión cuando la directiva **Visualización automática del teclado** está habilitada en el DDC. [HDX-39558]
- Al conectar un dispositivo USB o acceder a archivos, es posible que la aplicación Citrix Workspace muestre el cuadro de diálogo antiguo **Citrix Workspace: Advertencia de seguridad**. [LCM-10369]

Avisos legales de terceros

June 9, 2023

Es posible que la aplicación Citrix Workspace 2203.1 LTSR para Windows incluya software de terceros con licencias definidas en los términos del siguiente documento:

[Avisos legales de terceros de la aplicación Citrix Workspace para Windows](#) (descarga de PDF)

Requisitos del sistema y compatibilidad

April 22, 2024

Requisitos

Requisitos de hardware

- Mínimo 1 GB de RAM.
- En la tabla siguiente se indica el espacio necesario en el disco para instalar la aplicación Citrix Workspace.

	Versión mínima requerida de Microsoft Edge WebView2 Runtime	Versión máxima compatible de Microsoft Edge WebView2 Runtime
Versión del sistema operativo		
Windows 10 y Windows 11	92	No aplicable (compatible con la versión más reciente)
Windows Server 2012R2	92	109

	Versión mínima requerida de Microsoft Edge WebView2 Runtime	Versión máxima compatible de Microsoft Edge WebView2 Runtime
Versión del sistema operativo		
Windows Server 2016, 2019 y 2022	92	No aplicable (compatible con la versión más reciente)

Nota:

- El instalador solo lleva a cabo la comprobación de espacio en el disco después de haberse extraído el paquete de instalación.
- Cuando el sistema tiene poco espacio en el disco durante una instalación silenciosa, no aparece el cuadro de diálogo, pero se registra el mensaje de error en `CTXInstall _TrolleyExpress-*.log`.

Requisitos de software

- Microsoft Edge WebView2 Runtime
- .NET 4.8
- La versión más reciente de Microsoft Visual C++ Redistributable

Requisitos de Microsoft Edge WebView2 En la siguiente tabla se enumeran las versiones mínimas y máximas de Microsoft Edge WebView2 Runtime compatibles con los diferentes sistemas operativos Windows:

	Versión mínima requerida de Microsoft Edge WebView2 Runtime	Versión máxima compatible de Microsoft Edge WebView2 Runtime
Versión del sistema operativo		
Windows 10 y Windows 11	92	No aplicable (compatible con la versión más reciente)
Windows Server 2012R2	92	109
Windows Server 2016, 2019 y 2022	92	No aplicable (compatible con la versión más reciente)

- La aplicación Citrix Workspace viene empaquetada con la versión [Evergreen Bootstrapper](#) de Microsoft Edge WebView2 Runtime.
- El instalador de la aplicación Citrix Workspace puede instalar Microsoft Edge WebView2 Runtime durante la instalación de la aplicación Citrix Workspace. Sin embargo, para realizar esta

instalación, debe tener conexión a Internet. Como alternativa, puede instalar el paquete adecuado sin conexión del [instalador independiente de Microsoft Edge WebView2 Runtime Evergreen](#) antes de instalar la aplicación Citrix Workspace.

- El dispositivo debe tener acceso a estas URL:
 - https://*.dl.delivery.mp.microsoft.com para descargar Microsoft Edge WebView2 Runtime durante la instalación de la aplicación Citrix Workspace. Para obtener más información, consulte [Lista de permitidos para puntos finales de Microsoft Edge](#).
 - <https://msedge.api.cdp.microsoft.com> para comprobar la actualización de Microsoft Edge WebView2 Runtime
- Para administrar la actualización automática de Microsoft Edge WebView2 Runtime, consulte [Directivas de actualización](#) en la documentación de Microsoft. Por ejemplo, la actualización automática es útil en escritorios virtuales no persistentes, donde los escritorios vuelven a su estado original cuando un usuario cierra sesión.

Nota:

Al intentar instalar o actualizar la versión de la aplicación Citrix Workspace con privilegios que no son de administrador y Microsoft Edge WebView2 Runtime no está presente, la instalación se detiene con este mensaje:

“Debe iniciar sesión como administrador para instalar estos paquetes de requisitos previos:
Edge Webview 2 Runtime”

Requisitos de .NET La aplicación Citrix Workspace requiere .NET 4.8. Permite suscribirse e iniciar aplicaciones y escritorios desde la línea de comandos o la interfaz de usuario de la aplicación Citrix Workspace.

Al intentar instalar o actualizar la versión de la aplicación Citrix Workspace a la versión 1904 o a una posterior y la versión requerida de .NET Framework no está disponible en su sistema Windows, el instalador de la aplicación Citrix Workspace descarga e instala la versión requerida de .NET Framework.

Nota:

- Se produce un error en la instalación al intentar instalar o actualizar la versión de la aplicación Citrix Workspace con privilegios que no son de administrador y .NET Framework 4.8 o una versión más reciente no está presente en el sistema.
- **Debe tener conexión a Internet para descargar e instalar .NET Framework. De lo contrario, el administrador puede instalar estos requisitos mediante un método de implementación, como, por ejemplo, SCCM.**

Requisitos de Microsoft Visual C++ Redistributable La aplicación Citrix Workspace requiere 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 instalador de Microsoft Visual C++ Redistributable se empaqueta con el instalador de la aplicación Citrix Workspace. Durante la instalación de la aplicación Citrix Workspace, el instalador comprueba si el paquete de Microsoft Visual C++ Redistributable está presente en el sistema y lo instala si es necesario.

Nota:

Si el paquete de Microsoft Visual C++ Redistributable no existe en el sistema, es posible que falle la instalación de la aplicación Citrix Workspace con privilegios que no son de administrador.

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 Citrix Knowledge Center.

Tabla de compatibilidad

La aplicación Citrix Workspace es compatible con todas las versiones actualmente compatibles de Citrix Virtual Apps and Desktops, 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 para Windows es compatible con los siguientes sistemas operativos Windows:

Nota:

- La aplicación Citrix Workspace 2203.1 LTSR para Windows es la última versión compatible con el sistema operativo Windows Server 2012 R2.
- La aplicación Citrix Workspace 2203.1 LTSR para Windows no es compatible con Windows 7 ni Windows 8.1.
- 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

Windows 11

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

Compatibilidad con Windows 10 Enterprise (LTSC 2021) a partir de la versión 2203.1 LTSR CU1

Windows 10 Enterprise (2016 LTSB 1607, LTSC 2019)

Windows 10 (Home Edition*, Pro)

Windows Server 2022

Windows Server 2019

Windows Server 2016

*No se admite la autenticación PassThrough de dominio, Desktop Lock, la API de FastConnect ni configuraciones que requieran una máquina Windows unida a un dominio.

Compatibilidad de Windows 10 u 11 con la aplicación Citrix Workspace para Windows

Con el sistema operativo Windows 10, Microsoft presentó una nueva forma de crear, implementar y ofrecer servicios a Windows: [Windows como servicio](#). Las nuevas funciones se empaquetan en Actualizaciones de funciones (versiones principales como 20H2, 21H1 o 21H2). Las correcciones de errores y de seguridad se empaquetan en Actualizaciones de calidad. Estas actualizaciones que se pueden implementar mediante herramientas de administración existentes como SCCM.

Nota:

- No se recomienda instalar versiones de software de Citrix anteriores a la versión del Canal semianual.
- 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 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: Windows](#) de Microsoft.

En esta tabla, se muestra el número de la versión de Windows 10 y las correspondientes versiones compatibles de la aplicación Citrix Workspace para Windows.

Número de versión de Windows 10	Número de compilación	Versión de la aplicación Citrix Workspace
22H2	19045	2203.1 CU1 y versiones posteriores
21H2	19044	2112.1 y versiones posteriores
21H1	19043.928	2106 y versiones posteriores
20H2	19042.508	2012 y versiones posteriores
2004	19041.113	2006.1 y versiones posteriores
1909	18363.418	1911 y versiones posteriores
1903	18362.116	1909 y versiones posteriores
1809	17763.107	1812 y versiones posteriores
1803	17134.376	1808 y versiones posteriores

Nota:

Las versiones de Windows 10 son compatibles solamente con las versiones mencionadas de la aplicación Citrix Workspace. Por ejemplo, la versión 21H1 de Windows 10 no es compatible con la versión anterior a 2106.

En esta tabla, se muestra el número de la versión de Windows 11 y las correspondientes versiones compatibles de la aplicación Citrix Workspace para Windows.

Número de versión de Windows 11	Número de compilación	Versión de la aplicación Citrix Workspace
23H2	22631	2203.1 CU6
22H2	22621	2203.1 CU1 y versiones posteriores
21H2	22000	2203.1 y versiones posteriores

Validar el espacio libre en disco En la tabla siguiente se indica el espacio necesario en el disco para instalar la aplicación Citrix Workspace.

Tipo de instalación	Espacio de disco requerido
Instalación nueva	572 MB

Tipo de instalación	Espacio de disco requerido
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.

Nota:

- El instalador solo lleva a cabo la comprobación de 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

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 existe un certificado privado en la puerta de enlace remota, instale el certificado raíz de la entidad de certificación de la organización en el dispositivo de usuario que accede a los recursos de Citrix.

Nota:

Si el certificado de la puerta de enlace remota no se puede verificar durante la conexión, aparece una advertencia de certificado que no es de confianza. Esta advertencia aparece cuando falta el certificado raíz en el almacén de claves local. Cuando un usuario elige ignorar la advertencia y continuar con la conexión, se muestran las aplicaciones, pero no se pueden iniciar.

Certificados raíz

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

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

Certificados comodín

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

La aplicación Citrix Workspace admite certificados comodín. Use certificados comodín de acuerdo con la directiva de seguridad de su organización. Una alternativa a los certificados comodín es un certificado que contenga la lista de nombres de servidor con la extensión del nombre alternativo del sujeto (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

	Workspace para Web	Sitio de servicios de StoreFront (nativo)	StoreFront, Citrix Virtual Apps and Desktops (nativo), Citrix DaaS	De Citrix Gateway a Workspace para Web	Citrix Gateway en el sitio de StoreFront Services (nativo)
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.

Lista de revocación de certificados

La lista de revocación de certificados (CRL) permite a la aplicación Citrix Workspace comprobar si el certificado del servidor está revocado. La comprobación del certificado mejora la autenticación criptográfica del servidor y la seguridad general de la conexión TLS entre el dispositivo de usuario y un servidor.

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

Si quiere configurar la comprobación de certificados en su equipo local, cierre la aplicación Citrix Workspace. Compruebe que todos los componentes de Citrix Workspace, incluida la **Central de conexiones**, estén cerrados.

Para obtener más información, consulte [Transport Layer Security](#).

Instalación y desinstalación

May 23, 2024

Dispone de las siguientes maneras de instalar la aplicación Citrix Workspace:

- Puede descargar el paquete de instalación `CitrixWorkspaceApp.exe` desde la [página Descargas](#).
- O bien desde la página de descargas de la empresa (si está disponible).

Puede instalar el paquete siguiendo estos pasos:

- 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 línea de comandos. Para obtener información sobre cómo instalar la aplicación Citrix Workspace mediante la interfaz de línea de comandos, consulte [Usar parámetros de la línea de comandos](#).

Instalar con y sin privilegios de administrador:

Tanto los usuarios como los administradores 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

	Carpeta de instalación	Tipo de instalación
Usuario	%USERPROFILE%\AppData\Local\Citrix\WorkspaceClient	Instalación por usuario

Nota:

Los administradores pueden supeditar la instancia instalada por el usuario de la aplicación Citrix Workspace y continuar con la instalación correctamente.

Usar un instalador basado en Windows

Para instalar la aplicación Citrix Workspace para Windows, ejecute manualmente el paquete del instalador de [CitrixWorkspaceApp.exe](#) siguiendo estos métodos:

- Medios de instalación
- Recurso compartido de red
- Explorador de Windows
- Interfaz de línea de comandos

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. Cuando se instala en una máquina unida a un dominio con privilegios de administrador, aparece un cuadro de diálogo de inicio de sesión 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.

Cuando se completa la instalación, la aplicación Citrix Workspace solicita que agregue una cuenta. Para obtener información sobre cómo agregar cuentas, consulte [Agregar cuentas o cambiar de servidor](#).

Usar parámetros 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 de instalación se descomprime automáticamente en el directorio temporal del sistema antes de iniciar el programa de instalación. 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 desde la línea de comandos de Windows, inicie el símbolo del sistema y escriba lo siguiente en la misma línea:

- Nombre del archivo del instalador
- Comandos de instalación
- Y propiedades de instalación

Los comandos y las propiedades de instalación disponibles son los siguientes:

`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, no se reconocen aquellos dispositivos USB que estén en estado suspendido. Los dispositivos USB se activan solo después de reiniciar el dispositivo.
- `/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`: El modificador `/rcu` solo es efectivo cuando se actualiza una versión no compatible del software. Indica que la instalación o la actualización de la versión de la aplicación Citrix Workspace se completa al desinstalar la versión existente. El modificador de línea de comandos `/rcu` también borra los parámetros existentes o anteriores.

Nota:

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

- `/forceinstall`: Este modificador es efectivo al limpiar cualquier configuración existente o entradas de la aplicación Citrix Workspace que hubiera en el sistema. Utilice este modificador 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.

Nota:

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

- 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 habilitó la actualización automática, puede elegir la versión que quiere actualizar. 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 cuando haya una actualización disponible. Para obtener más información, consulte [Actualizaciones de Citrix Workspace](#).

- -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 le recuerda de nuevo la actualización. Por ejemplo: `CitrixWorkspaceApp.exe /DeferUpdateCount=0`.
- Cualquier otro número “n”: Permite aplazar las notificaciones “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 hay disponible una nueva versión de la aplicación, Citrix implanta 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 seguridad mejorada porque restringe la posibilidad de que los clientes corran peligro por parte de malware que registra claves y captura pantallas.

- `CitrixWorkspaceApp.exe /includeappprotection`

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

/InstallEmbeddedBrowser

Excluye los binarios de Citrix Enterprise Browser. Ejecute el conmutador `/InstallEmbeddedBrowser=N` para excluir la función Citrix Enterprise Browser.

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,SSON,SELSERVICE,DesktopViewer,WebHelper,WorkspaceHub,USB,AppProtection`.

Nota:

De forma predeterminada, `ReceiverInside`, `ICA_Client` y `AM` se instalan al instalar la aplicación Citrix Workspace.

`ADDLOCAL` instala uno o varios componentes especificados.

`ReceiverInside`, `ICA_Client` y `AM` son requisitos previos, y se instalan de forma predeterminada al instalar la aplicación Citrix Workspace.

- `ReceiverInside`: Instala la experiencia de la aplicación Citrix Workspace (obligatoria), la funcionalidad de la bandeja del sistema y la actualización automática.
- `ICA_Client`: Instala los componentes HDX.
- `AM`: Instala los componentes de Authentication Manager.

También puede instalar estos módulos en función de sus requisitos y su entorno:

- `SSON`: Instala los componentes necesarios para Single Sign-On.
- `SELSERVICE`: Instala Self-Service Plug-in. Esto le permite acceder a aplicaciones y escritorios virtuales desde la ventana de la aplicación Citrix Workspace o desde una línea de comandos. Si `SELSERVICE` no está instalado, puede acceder a las aplicaciones y escritorios a través de la web (Receiver para Web).
- `DesktopViewer`: Instala Desktop Viewer para ver aplicaciones y escritorios virtuales.
- `WebHelper`: Instala el componente WebHelper. Este componente recupera el archivo ICA de StoreFront y lo transfiere a HDX Engine. También verifica los parámetros del entorno y los comparte con StoreFront. Este componente se utiliza durante el inicio de la sesión a través del explorador web.
- `WorkspaceHub`: Componente Citrix Ready Workspace Hub que habilita Citrix Casting.
- `USB`: Instala la compatibilidad con USB.
- `AppProtection`: Instala el componente App Protection.

Parámetros de funciones HDX

ALLOW_BIDIRCONTENTREDIRECTION

Indica si la redirección de contenido bidireccional entre el cliente y el host está habilitada. Para obtener más información, consulte la sección [Configuraciones de directiva de Redirección de contenido bidireccional](#) en la documentación de Citrix Virtual Apps and Desktops.

- 0 (valor predeterminado): Indica que la redirección bidireccional de contenido está inhabilitada. Por ejemplo: `CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=0`.
- 1: Indica que la redirección bidireccional de contenido 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. Instale la aplicación 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 quiere mostrar iconos de documentos o archivos que tienen asociaciones de tipo de archivo con aplicaciones suscritas.

- False (valor predeterminado): Muestra iconos de 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: No muestra iconos de documentos o archivos que tienen asociaciones de tipo de archivo con aplicaciones suscritas. Por ejemplo: `CitrixWorkspaceApp.exe LEGACYFTAICONS=True`.

ALLOW_CLIENHOSTEDAPPSURL

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_CLIENHOSTEDAPPSURL=0`.
- 1: Habilita la función de redirección de URL en el dispositivo del usuario. Por ejemplo: `CitrixWorkspaceApp.exe ALLOW_CLIENHOSTEDAPPSURL=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 su propio almacén. 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 de la aplicación Citrix Workspace.

- 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 el directorio para los 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 el directorio para los accesos directos del 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** y 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): Participar en el programa Citrix Customer Improvement Program (CEIP). Por ejemplo: `CitrixWorkspaceApp.exe EnableCEIP=True`.
- False: Rechazar la participación en el programa Customer Experience Improvement Program (CEIP) de Citrix. 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. Especifique 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 usar la autenticación Kerberos, que solo se requiere cuando se habilita la autenticación Single Sign-On. Para obtener más información, consulte [Autenticación PassThrough de dominio con Kerberos](#).

- Sí: Indica que HDX Engine debe utilizar la autenticación Kerberos. Por ejemplo: `CitrixWorkspaceApp.exe ENABLE_KERBEROS=Yes`.
- No: Indica que HDX Engine no utiliza 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:** Nombre de dominio completo del servidor que aloja el almacén.
- **IISLocation:** 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 instalación mediante la 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.
- En una configuración de varios almacenes, la URL del almacén de Citrix Gateway debe ser la primera en la lista. Solo se permite la configuración de una 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.

Restablecer la aplicación Citrix Workspace

El restablecimiento de la aplicación Citrix Workspace restaura los parámetros predeterminados.

Se restablecen estos elementos al restablecer la aplicación Citrix Workspace:

- Todas las cuentas y almacenes configurados.
- Aplicaciones entregadas por Self-Service Plug-in, sus iconos y claves de Registro.
- Asociaciones de tipos de archivo creadas por Self-Service Plug-in.
- Archivos almacenados en la caché y contraseñas guardadas.
- Parámetros del Registro por usuario.
- Instalaciones por máquina y sus parámetros del Registro.
- Parámetros del Registro de Citrix Gateway para la aplicación Citrix Workspace.

Ejecute este comando desde la interfaz de línea de comandos para restablecer la aplicación Citrix Workspace:

```
C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe -cleanUser
```

Para el restablecimiento silencioso, use este comando:

```
C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe /silent -cleanUser
```

Nota:

Utilice la U mayúscula en el parámetro.

El restablecimiento de la aplicación Citrix Workspace no afecta a lo siguiente:

- Instalación de plug-ins o de la aplicación Citrix Workspace.
- Parámetros de bloqueo de ICA por máquina.
- Configuraciones de plantillas administrativas de objetos de directiva de grupo (GPO) para la aplicación Citrix Workspace.

Desinstalar

Usar un instalador basado en Windows:

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

Nota:

Durante la instalación de la aplicación Citrix Workspace, recibirá un mensaje para desinstalar el paquete Citrix HDX RTME. Haga clic en **Aceptar** para continuar con la desinstalación.

Uso de la interfaz de línea de comandos:

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

```
CitrixWorkspaceApp.exe /uninstall
```

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

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

Nota:

El instalador de la aplicación Citrix Workspace no controla las claves del Registro relacionadas con los GPO, por lo que se conservan después de la desinstalación. Si encuentra alguna entrada, actualícelas mediante `gpedit` o elimínelas manualmente.

Implementación

April 22, 2024

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](#).
- Antes de iniciar Workspace para Web, instale la aplicación Citrix Workspace para Windows. 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](#).
- Use Microsoft Endpoint Manager (Intune). Para obtener más información, consulte [Implementar la aplicación Citrix Workspace en Microsoft Endpoint Manager \(Intune\)](#).

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 en función de la estructura de su organización. 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, configure `DesiredVersion= 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 del instalador de la aplicación Citrix Workspace y no se autentica mediante el script. La carpeta compartida debe tener permisos de lectura para todos (EVERYONE).
- **Script Logging Directory (Directorio de registros del script):** El recurso compartido de la red donde se copian los registros de instalación y los que el script no autentificó. 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.

Tipo de implementación	Para implementar	Para quitar
Por equipo	<code>CheckAndDeployWorkspacePerMachineStartUpScript.bat</code>	<code>CheckAndRemoveWorkspacePerMachineScript.bat</code>
Por usuario	<code>CheckAndDeployWorkspacePerUserScript.bat</code>	<code>CheckAndRemoveWorkspacePerUserScript.bat</code>

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**, copie el script apropiado en la carpeta que se muestra y cierre el cuadro de diálogo.
5. 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 asignados 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 que quiera quitar a la unidad organizativa que creó.
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

Los espacios de trabajo para la web le permiten acceder a almacenes de StoreFront a través de un explorador web mediante una página web.

Antes de conectarse a una aplicación desde un explorador web, haga lo siguiente:

1. Instale la aplicación Citrix Workspace para Windows.
2. Implementar la aplicación Citrix Workspace desde Workspace para Web

Si Workspace para Web detecta que no hay una versión compatible de la aplicación Citrix Workspace, aparece un mensaje. El mensaje muestra que debe descargar e instalar la aplicación Citrix Workspace para Windows.

Nota:

Los espacios de trabajo para la web no admiten la detección de cuentas basada en direcciones de correo electrónico.

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 StoreFront mediante los 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.

Puede implementar la aplicación Citrix Workspace con SCCM mediante las cuatro partes siguientes:

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 la información de la aplicación, como, 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 /silent /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 **4.3.0.65534**.
11. En el panel **Experiencia del usuario**, establezca:
 - **Comportamiento de instalación**: Instalar para el sistema.
 - **Requisito de inicio de sesión**: Si un usuario inició sesión.
 - **Visibilidad del programa de instalación**: NormalHaga clic en **Siguiente**.

Nota:

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

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 configurada. También puede programarla o llevar a cabo la instalación 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** y 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 que indica que la operación se realizó correctamente.

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 recopilación de dispositivos forma parte de las Recopilaciones de dispositivos al buscar en el **asistente para implementar software**.

Nota:

Es posible que la configuración de la aplicación Citrix Workspace mediante SCCM falle cuando el atributo **MSIRESTARTMANAGERCONTROL** se establece en **False**.

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.

Implementar la aplicación Citrix Workspace en Microsoft Endpoint Manager (Intune)

Para implementar la aplicación Citrix Workspace (aplicación Win 32 nativa) en Microsoft Endpoint Manager (Intune), haga lo siguiente:

1. Cree estas carpetas:
 - Una carpeta para almacenar todos los archivos de origen necesarios para la instalación. Por ejemplo: `C:\CitrixWorkspace_Executable`.
 - Una carpeta para el archivo de salida. Los archivos de salida están en el archivo `.intunewin`. Por ejemplo: `C:\Intune_CitrixWorkspaceApp`.
 - Una carpeta para la herramienta Microsoft Win32 Content Prep. Por ejemplo: `C:\Intune_WinAppTool`. Esta herramienta ayuda a convertir los archivos de instalación al formato `.intunewin`. Puede descargar la herramienta de empaquetado en [Microsoft-Win32-Content-Prep-Tool](#).
2. Convierta todos los archivos de origen que se necesitan para la instalación en un archivo `.intunewin`:
 - a) Inicie el símbolo del sistema y vaya a la carpeta donde existe Microsoft Win32 Content Prep Tool. Por ejemplo: `C:\Intune_WinAppTool`.
 - b) Ejecute el comando `IntuneWinAppUtil.exe`.
 - c) En el mensaje, introduzca esta información:
 - **Source folder:** `C:\CitrixWorkspace_Executable`

- **Setup file:** `CitrixWorkspaceApp.exe`
- **Output folder:** `C:\Intune_CitrixWorkspaceApp`
Se crea el archivo `.intunewin`.

3. Agregue el paquete a Microsoft Endpoint Manager (Intune):

- a) Abra la consola de Microsoft Endpoint Manager (Intune): <https://endpoint.microsoft.com/#home>.

Nota:

Esta instrucción solo se puede realizar en <https://endpoint.microsoft.com/#home>. También puede agregar el paquete a través de <https://portal.azure.com>.

- b) Haga clic en **Apps > Windows app** y, a continuación, en **+Add**.
- c) Seleccione **Windows app (Win 32)** en la lista desplegable **App type**.
- d) Haga clic en **App package file**, busque el archivo `CitrixWorkspaceApp.intunewin` y, a continuación, haga clic en **OK**.
- e) Haga clic en **App information** y complete la información obligatoria (Name, Description y Publisher) y, a continuación, haga clic en **OK**.
- f) Haga clic en **Program**, introduzca esta información y haga clic en **OK**:
- Comando de instalación: `CitrixWorkspaceApp.exe /silent`
 - Comando de desinstalación: `CitrixWorkspaceApp.exe /uninstall`
 - Comportamiento de instalación: System
- g) Haga clic en **Requirement**, introduzca la información requerida y, a continuación, haga clic en **OK**.

Nota:

Seleccione x64 y x32 en la lista Operating System Architecture. La versión del sistema operativo puede ser cualquiera con Win 1607 o una versión posterior.

- h) Haga clic en **Detection rules**, seleccione **Manually configure detection rules** bajo **Rules format** y, a continuación, haga clic en **OK**.
- i) Haga clic en **Add**, seleccione el tipo de regla necesario en **Rule type** y, a continuación, haga clic en **OK**.
- Si **Rule type** es **File**, la ruta puede ser, por ejemplo, `C:\Program Files (x86)\Citrix\ICA Client\wfica32.exe`.

- Si **Rule type** es **Registry**, introduzca `HKEY_CURRENT_USER\Software\Citrix` como **Path** y **Key exists** como **Detection method**.
 - j) Haga clic en **Return codes**, compruebe si los códigos de devolución predeterminados son válidos y haga clic en **OK**.
 - k) Haga clic en **Add** para agregar la aplicación a Intune.
4. Compruebe si la implementación se ha realizado correctamente:
- a) Haga clic en **Home > Apps > Windows**.
 - b) Haga clic en **Device install status**.
- El estado del dispositivo muestra la cantidad de dispositivos en los que está instalada la aplicación Citrix Workspace.

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](#). Para obtener información sobre la instalación, consulte [Instalación y desinstalación](#).

Actualización automática

Cuando hay una nueva versión disponible 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 para Windows 2104 ni a la aplicación Citrix Workspace 1912 LTSR CU4.
- El sistema debe tener una conexión a Internet para recibir actualizaciones.
- De forma predeterminada, las actualizaciones de la aplicación Citrix Workspace están in-

- habilitadas en el VDA. Esto incluye máquinas de servidor multiusuario RDS, VDI y máquinas de acceso con Remote PC.
- Las actualizaciones de la aplicación Citrix Workspace están inhabilitadas en las máquinas donde esté instalado Desktop Lock.
 - Los usuarios de Workspace para Web no pueden descargar automáticamente la directiva de StoreFront.
 - Las actualizaciones de la aplicación Citrix Workspace solo se pueden limitar a las actualizaciones LTSR.
 - Citrix HDX RTME para Windows se incluye en las actualizaciones de la aplicación Citrix Workspace. Se muestra una notificación cuando hay actualizaciones disponibles de HDX RTME, tanto en la versión LTSR como en la versión actual de la aplicación Citrix Workspace.
 - A partir de la versión 2105, se modifican las rutas de registros de las actualizaciones de la aplicación Citrix Workspace. Los registros de Actualizaciones de Workspace están en C:\Archivos de programa (x86)\Citrix\Logs. Para obtener información sobre la captura de registros, consulte la sección [Recopilación de registros](#).
 - 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**. La opción **Buscar actualizaciones** está disponible tanto en las instancias instaladas por el usuario como en las instancias instaladas por el administrador de la aplicación Citrix Workspace.

Reinicie la aplicación Citrix Workspace para Windows tras una actualización manual o automática.

Configuración avanzada para actualizaciones automáticas (Actualizaciones de Citrix Workspace)

Puede configurar las actualizaciones de la aplicación Citrix Workspace siguiendo estos métodos:

1. Plantilla administrativa de objetos de directiva de grupo (GPO)
2. Interfaz de línea de comandos
3. Interfaz gráfica (GUI)
4. StoreFront

Configurar Actualizaciones de Citrix Workspace con 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 y vaya al nodo Configuración del equipo.

2. Vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Actualizaciones de Workspace.**

Citrix Workspace Updates

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on: ADMX Migrator encountered a policy that does not have a supportedOn value.

Options:

Enable Citrix Workspace Update Policy

Auto

LTSR ONLY

Citrix-Workspace-Update-DeferUpdate-Count

-1

Help:

Not Configured – Citrix Workspace Updates is enabled. Enabled – Citrix Workspace Updates is enabled with the additional options listed in this dialog. Disabled – Citrix Workspace Updates option is hidden from the Advanced Preferences sheet and you will not receive any update notifications.

Enable Citrix Workspace Update Policy:
Auto = Citrix Workspace checks for updates automatically.
Manual = User checks for updates manually.

LTSR ONLY:
True = Only LTSR updates will be available.

Citrix-Workspace-Update-DeferUpdate-Count:
-1: User can defer any number of times.
0: User would not see remind later option.
number: User would see remind later options with the given count.

OK Cancel Apply

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

Nota:

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

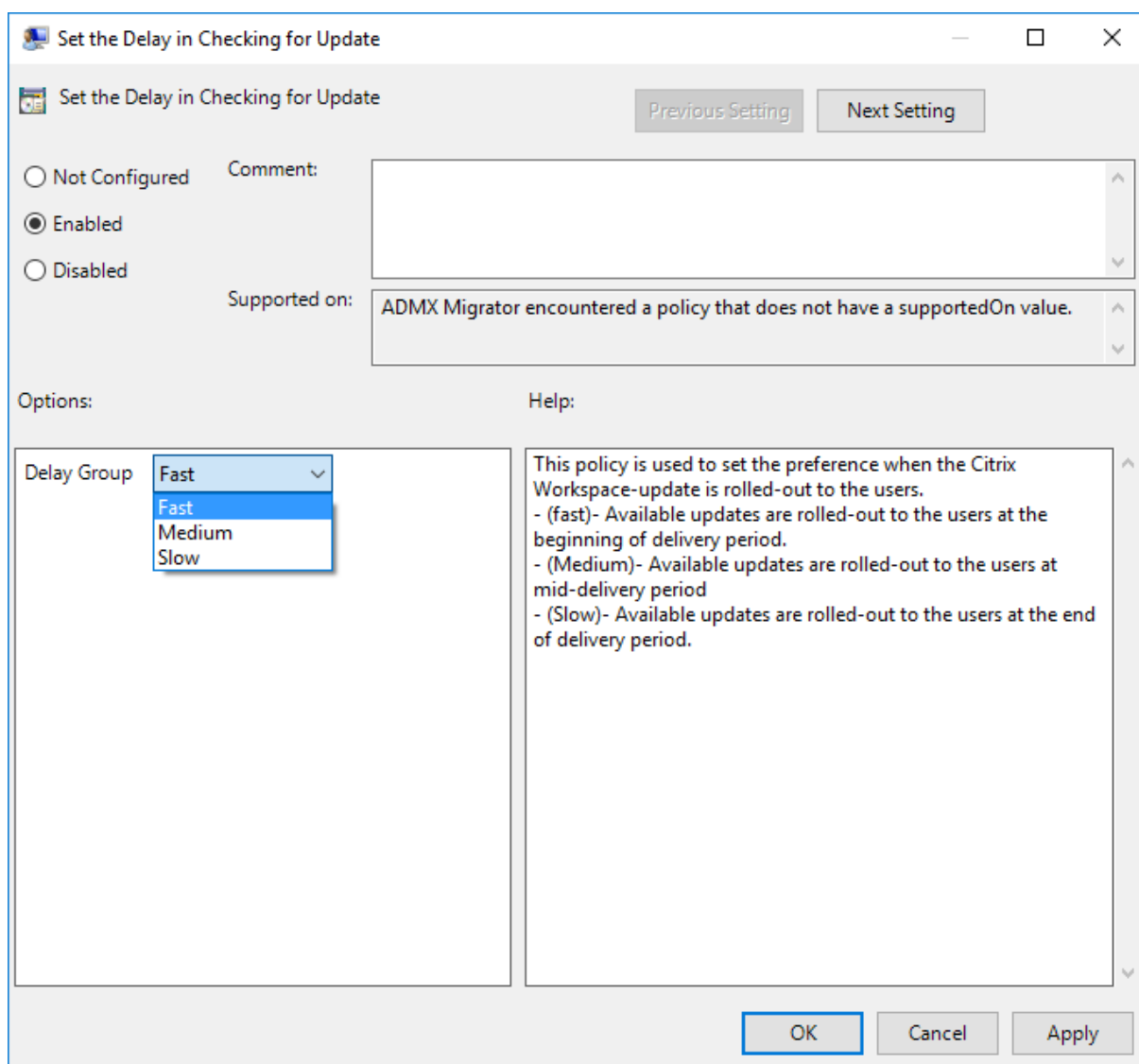
4. **Notificación de actualización.** Cuando haya una actualización disponible, puede optar por recibir una notificación automática o comprobarlo manualmente. Una vez habilitadas las actualizaciones de Workspace, seleccione una de las opciones siguientes en la lista desplegable **Directiva para habilitar 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.
5. Seleccione **SOLO LTSR** para obtener las actualizaciones para LTSR solamente.
 6. En la lista desplegable **Citrix-Workspace-Update-DeferUpdate-Count**, seleccione un valor entre -1 y 30:
 - Si el valor es 0, aparece la opción **Recordármelo más tarde**. El mensaje **Actualización disponible** se muestra tras cada comprobación automática periódica de actualizaciones.
 - Si el valor es -1, aparece la opción **Recordármelo más tarde** con el mensaje **Actualización disponible**. Puede aplazar la notificación de actualizaciones las veces que quiera.
 - Un valor entre 1 y 30 define la cantidad de veces que debe aparecer la opción **Recordármelo más tarde** con el mensaje **Actualización disponible**. Puede aplazar la notificación de actualizaciones en función del valor definido en este campo. Sin embargo, el mensaje **Actualización disponible** sigue apareciendo, pero sin la opción **Recordármelo más tarde**.

Configurar la demora en la comprobación de actualizaciones Cuando hay disponible una nueva versión de la aplicación Citrix Workspace, Citrix implanta 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**.



Habilítela y, en el menú desplegable **Demorar grupo**, seleccione una de estas 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 actualizaciones disponibles. **Inhabilitada** también oculta la opción Actualizaciones de Citrix Workspace en la hoja Preferencias avanzadas.

Configurar las actualizaciones de la aplicación 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. Vaya a la ubicación de `CitrixReceiverUpdater.exe` mediante la línea de comandos de Windows.

Por regla general, `CitrixReceiverUpdater.exe` se encuentra en `CitrixWorkspaceInstallLocation\Citrix\Ica Client\Receiver`. Puede ejecutar el binario `CitrixReceiverUpdater.exe` 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
```

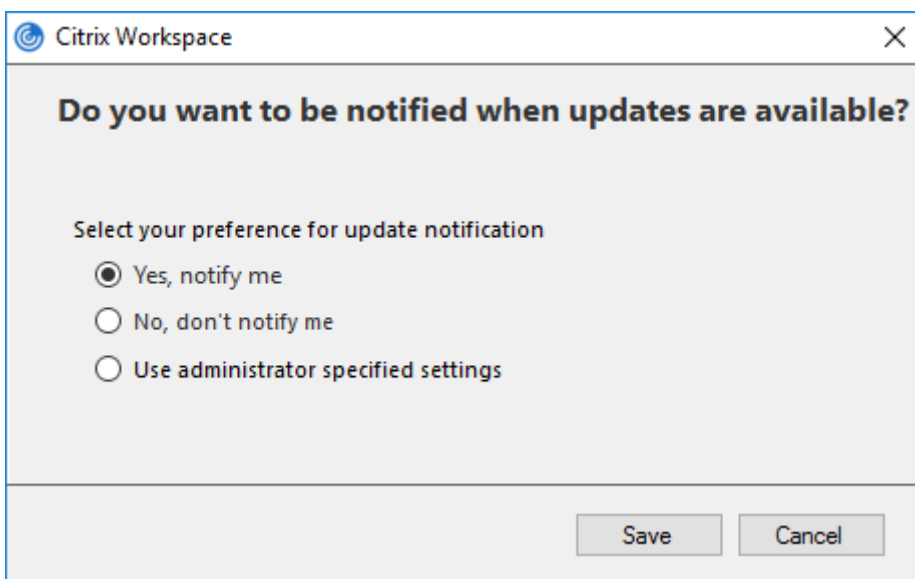
Nota:

`/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.

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 > Actualizaciones de Citrix Workspace**.
3. Seleccione la preferencia de notificación y haga clic en **Guardar**.



Nota:

Puede ocultar una parte o toda la hoja de Preferencias avanzadas disponible en el icono de la aplicación Citrix Workspace. Para obtener más información, consulte la sección [Hoja de Preferencias avanzadas](#).

Configurar las actualizaciones de la aplicación 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 la etiqueta `<clear />`.

```

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

```

7      description="" published="true" updaterType="Citrix"
      remoteAccessType="None">
8
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 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.

Introducción

April 22, 2024

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

Requisitos previos:

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

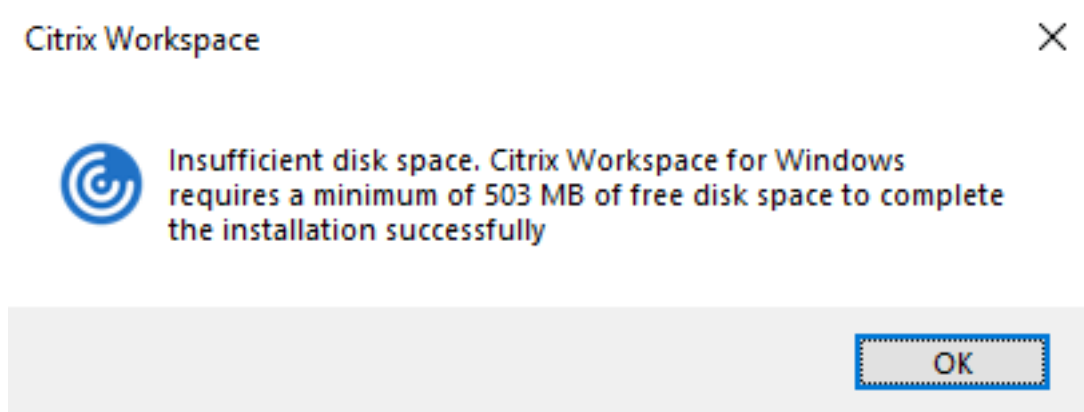
Validar el espacio libre en disco

Consulte la tabla siguiente para obtener información detallada sobre el espacio en disco necesario antes de la instalación:

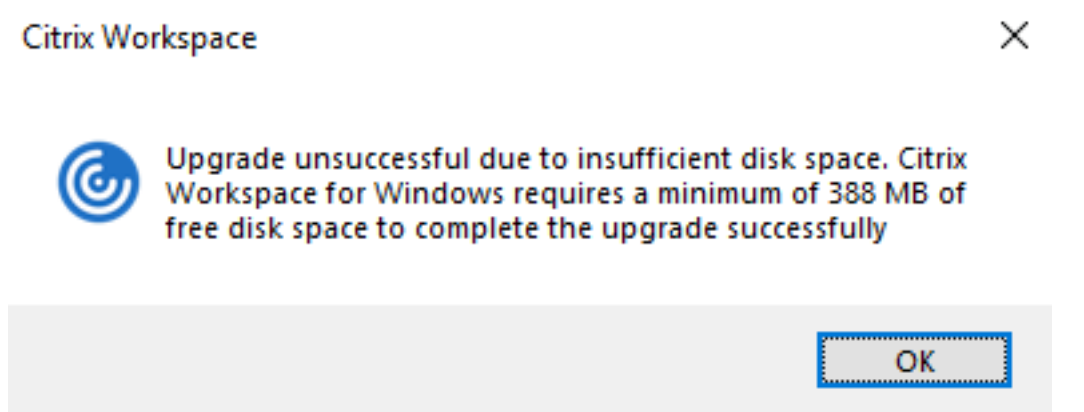
Tipo de instalación	Espacio mínimo requerido en disco
Instalación nueva	572 MB
Actualizaciones	350 MB

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

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



Durante la actualización de la versión de la aplicación Citrix Workspace, la instalación se detiene y aparece el siguiente cuadro de diálogo cuando no hay suficiente espacio en el disco.



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`.

Configure lo siguiente antes de utilizar la aplicación Citrix Workspace:

- [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

Se recomienda utilizar la plantilla administrativa de objetos de directiva de grupo y configurar reglas para:

- Redirección de red
- Servidores proxy
- Configuración del servidor de confianza
- Redirección de usuarios
- Dispositivos de usuarios remotos
- Experiencia del usuario.

Puede utilizar los archivos de plantilla `receiver.admx` o `receiver.adm` 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. La importación es útil al aplicar los parámetros de la aplicación Citrix Workspace a diferentes dispositivos de usuario en la empresa. Para modificar 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.

El directorio de instalación incluye `CitrixBase.admx` y `CitrixBase.adml`, así como los archivos de plantillas administrativas (`receiver.adml` o `receiver.admx` 'receiver.adml').

Nota:

Los archivos ADMX y ADML se usan con Windows Vista, Windows Server 2008 y las demás versiones posteriores de Windows.

Por ejemplo: `<installation directory>\Online Plugin\Configuration`.

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

Consulte la tabla siguiente para obtener información sobre los archivos de plantilla de aplicaciones de Citrix Workspace y sus respectivas ubicaciones.

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.

Tipo de archivo	Ubicación de archivos
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 versión de la aplicación Citrix Workspace, agregue los archivos de plantilla más recientes al GPO local. La configuración anterior se conserva después de la importación. Para obtener más información, consulte el siguiente procedimiento:

Para agregar los archivos de plantilla receiver.admx/adml al objeto de directiva de grupo local:

Puede utilizar archivos de plantilla ADM para configurar los objetos de directiva de grupo locales y 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 estos archivos de plantilla:

Tipo de archivo	Copiar de	Copiar a
receiver.admx	Installation Directory\ICA Client\ Configuration\ receiver.admx	%systemroot%\ policyDefinitions
CitrixBase.admx	Installation Directory\ICA Client\ Configuration\ CitrixBase.admx	%systemroot%\ policyDefinitions
receiver.adml	Installation Directory\ICA Client\ Configuration\ [MUICulture]receiver. adml	%systemroot%\ policyDefinitions\ [MUICulture]
CitrixBase.adml	Installation Directory\ICA Client\ Configuration\ [MUICulture] CitrixBase.adml	%systemroot%\ policyDefinitions\ [MUICulture]

Nota:

Agregue CitrixBase.admx/CitrixBase.adml a la carpeta `\PolicyDefinitions` para ver los archivos de plantilla en **Plantillas administrativas > Componentes de Citrix > Citrix Workspace**.

StoreFront

Configure 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:

Es posible que vea la antigua interfaz de usuario de StoreFront si selecciona la opción para **mostrar todos los almacenes**.

Para configurar StoreFront:

Instale y configure StoreFront como se describe en la documentación de [StoreFront](#). La aplicación

Citrix Workspace requiere una conexión HTTPS. En un almacén de StoreFront configurado en HTTP, defina la clave del Registro como se describe en [Usar parámetros de línea de comandos](#).

Nota:

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 objetos 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 #Storename es el nombre del almacén detrás de Citrix Gateway.

A partir de la versión 1808, los cambios realizados en la directiva **URL de Citrix Gateway/Lista de cuentas de StoreFront** se aplican en una sesión después de reiniciar la aplicación. No es necesario reiniciarla.

Nota:

En una instalación nueva, no es necesario restablecer la aplicación Citrix Workspace 1808 ni versiones posteriores. Si hay una actualización a 1808 o una versión posterior, 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 está disponible la opción de usar varias direcciones 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. Por ejemplo: el control del espacio de trabajo permite a los médicos trasladarse 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. El control de Workspace también se puede realizar para los dispositivos cliente unidos a un dominio mediante la directiva de grupo.

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 de 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

Habilitar control del espacio de trabajo 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:

También puede establecer la clave **WSCReconnectAll** en false si no quiere crear una 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 modificar el período de tiempo de espera, cree un valor de REG_DWORD denominado **SI INACTIVE MS** en [HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\](#). El valor de 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

La función 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. La integración del menú Inicio y la administración de accesos directos del escritorio proporcionan una experiencia de escritorio fluida para grupos de usuarios. También para los usuarios que necesitan acceder a un conjunto básico de aplicaciones de forma continua.

Esta marca se denomina **SelfServiceMode** y está establecida como **True** de forma predeterminada. Cuando el administrador establece el indicador **SelfServiceMode** en **False**, no se puede acceder a la interfaz de usuario de autoservicio. En su lugar, puede acceder a aplicaciones suscritas desde el menú Inicio y accesos directos de escritorio, lo que 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 aplicaciones. Todas las aplicaciones son obligatorias cuando se trabaja con la marca **SelfServiceMode** establecida en False (modo de acceso directo solamente). Si quita un icono de acceso directo que hubiera en el escritorio, el icono vuelve a aparecer cuando selecciona **Actualizar** desde el icono de la aplicación Citrix Workspace situado en el área de notificaciones.
- Los usuarios solo pueden configurar un almacén. Las opciones Cuenta y Preferencias no están disponibles para evitar que el usuario configure más almacenes. El administrador puede otorgar a un usuario privilegios especiales para agregar más de una cuenta mediante la plantilla de objeto de directiva de grupo. Los administradores también pueden proporcionar privilegios especiales al agregar manualmente una clave del Registro (HideEditStoresDialog) en la máquina cliente. Cuando el administrador da este privilegio a un usuario, este usuario tiene la opción Preferencias en el icono del área de notificaciones, 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 modificar 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 individualmente o en la carpeta raíz. No dentro de las subcarpetas de categoría que se definen 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 función de reinstalación automática de aplicaciones modificadas se puede habilitar mediante la clave del Registro `AutoReInstallModifiedApps`. Al habilitar `AutoReInstallModifiedApps`, los cambios en los atributos de aplicaciones y escritorios publicados en el servidor se muestran en la máquina cliente. Al inhabilitar `AutoReInstallModifiedApps`, los atributos de las aplicaciones y escritorios no se actualizan, y los accesos directos no vuelven a aparecer al actualizar si se eliminaron del cliente. De forma predeterminada, `AutoReInstallModifiedApps` está habilitada.

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

Nota:

- De forma predeterminada, las claves del Registro usan el formato de **cadena**.
 - Cambie las claves del Registro antes de configurar un almacén. Si en algún momento usted o un usuario quieren personalizar las claves del Registro, deben hacer lo siguiente:
1. Restablecer la aplicación Citrix Workspace
 2. Configurar las claves del Registro
 3. Y reconfigurar el almacén

Claves de Registro para máquinas de 32 bits

Clave del Registro: WSCSupported Valor: True

Ruta de la clave:

- ```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
 primaryStoreID +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

**Clave del Registro: WSCReconnectAll Valor: True**

**Ruta de la clave:**

- ```
1 - `HKEY_CURRENT_USER\Software\Citrix\Dazzle`
2 - `HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
   primaryStoreID + \Properties`
3 - `HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle`
4 - `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle`
```

Clave del Registro: WSCReconnectMode Valor: 3

Ruta de la clave:

- ```
1 - HKEY_CURRENT_USER\Software\Citrix\Dazzle
2 - HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" +
 primaryStoreID +\Properties
3 - HKEY_LOCAL_MACHINE\Software\Policies\Citrix\Dazzle
4 - HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle
```

**Clave del Registro: WSCReconnectModeUser Valor:** El Registro no se crea durante la instalación.

**Ruta de la clave:**



- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Citrix\Dazzle

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

**Clave del Registro: WSCSupported Valor: True**

**Ruta de la clave:**

- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Citrix\Dazzle

**Clave del Registro: WSCReconnectAll Valor: True**

**Ruta de la clave:**

- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Citrix\Dazzle

**Clave del Registro: WSCReconnectMode Valor: 3**

**Ruta de la clave:**

- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
- 4 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Citrix\Dazzle

**Clave del Registro: WSCReconnectModeUser Valor:** El Registro no se crea durante la instalación.

**Ruta de la clave:**

- 1 - HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- 2 - HKEY\_CURRENT\_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
- 3 - HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle

## 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

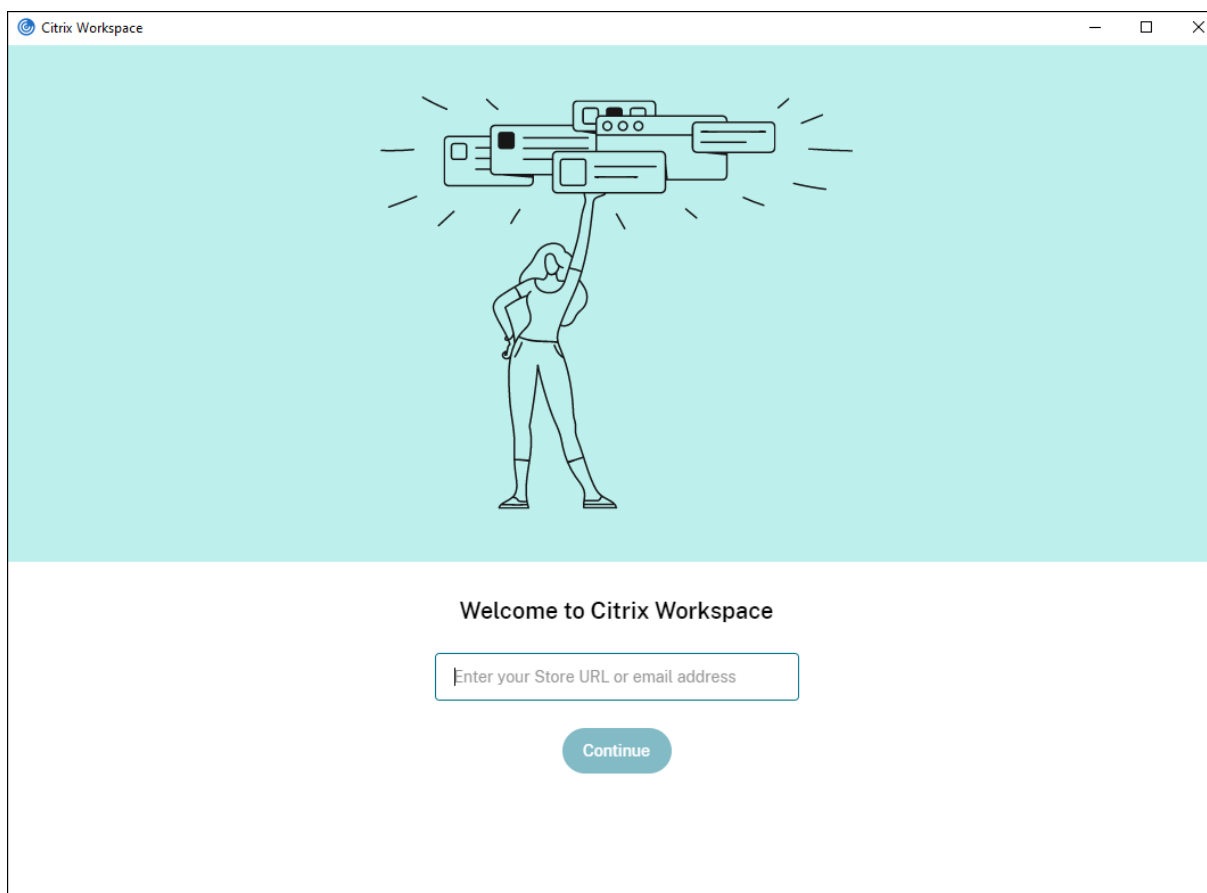
Citrix recomienda que reinicie la aplicación Citrix Workspace después de la instalación para asegurarse de lo siguiente:

- El reinicio garantiza que los usuarios puedan agregar cuentas.
- La aplicación Citrix Workspace puede detectar 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.

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

Tras la instalación correcta de la aplicación Citrix Workspace, aparece esta pantalla. Los usuarios deben introducir una dirección de correo electrónico o de servidor para acceder a las aplicaciones y escritorios. 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 permitir que los usuarios configuren sus cuentas manualmente, distribúyales la información que necesitan para conectarse con sus escritorios y aplicaciones virtuales.

- Para conectarse a un almacén de Workspace, proporcione la URL de Workspace.
- Para conectarse a un almacén de StoreFront, proporcione la dirección URL de ese servidor. Por ejemplo: <https://servername.company.com>.
- Para conectarse 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:

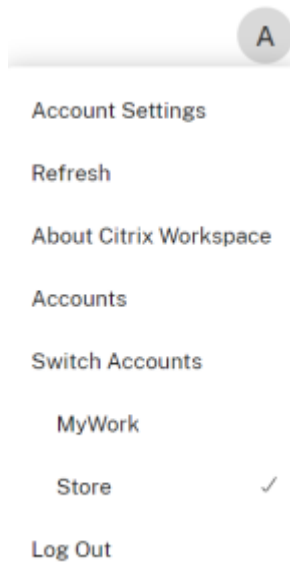
**CitrixGatewayFQDN?MyStoreName:**

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 para acceder a AplicacionesVentas
- \* O servidor2.com?AplicacionesRRHH para acceder a **AplicacionesRRHH**.

La función **CitrixGatewayFQDN?MyStoreName** requiere que un nuevo usuario cree una cuenta mediante una dirección URL, y no está disponible para la detección basada en direcciones de correo electrónico.

Una vez que la aplicación Citrix Workspace se haya configurado con la URL del almacén, la cuenta se puede administrar desde la opción **Cuentas** del menú de perfil.



### 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 asociados a la dirección de correo electrónico en función de los registros de servicios (SRV) del Sistema de nombres de dominio (DNS). A continuación, la aplicación solicita al usuario que inicie sesión para acceder a aplicaciones y escritorios virtuales.

Para obtener más información, consulte [Configurar la detección de cuentas basada en direcciones de correo electrónico](#).

### 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 incluyan 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 conectarse a un almacén de StoreFront, proporcione la dirección URL de ese servidor. Por ejemplo: `https://servername.company.com`.
- Para conectarse 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` para acceder a AplicacionesVentas
- `O servidor2.com?AplicacionesRRHH` para acceder a **AplicacionesRRHH**.

La función **CitrixGatewayFQDN?MyStoreName** requiere que un nuevo usuario cree una cuenta mediante una dirección URL, y no está disponible para la 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 exijan la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de un uso incorrecto 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.

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:

**Ruta de la clave:** `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle`

**Nombre de la clave:** `CurrentAccount`

**Valor:** `AllAccount`

**Tipo:** REG\_SZ

#### Para sistemas de 64 bits:

**Ruta de la clave:** `HKEY_LOCAL_MACHINE\\Software\\Wow6432Node\\Citrix\\Dazzle`

**Nombre de la clave:** `CurrentAccount`

**Valor:** `AllAccount`

**Tipo:** REG\_SZ

## Asignación de unidades de 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.

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, por lo que parece que estén 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.

### **Inhabilitar 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. Al habilitar solamente 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). Al habilitar la redirección de carpetas del cliente en el servidor y el usuario la configura en el dispositivo de usuario, 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 redirige 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 | Accesible por el servidor 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. Por lo tanto, las letras de unidad del servidor se cambian a letras de unidad posteriores. En este 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 | Accesible por el servidor 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 asigna la unidad de red a la misma letra de unidad que la de un servidor, la asignación de unidad de red no es válida.

Al conectar un dispositivo de usuario 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 and Play permite la redirección dinámica de dispositivos multimedia al servidor. Los dispositivos multimedia incluyen cámaras, escáneres, reproductores multimedia y dispositivos de punto de venta (POS). Al mismo tiempo, se puede impedir la redirección de todos los dispositivos o de una parte. 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 supeditar 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 notifique 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 se pueden asignar)
- z es el número del puerto COM del cliente que quiere asignar

4. Para confirmar la operación, escriba:

```
net use
```

El mensaje muestra las unidades asignadas, los puertos LPT y los 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 de 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 el servidor.

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 inhabilitar 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

Es posible que el uso incorrecto del Editor del Registro del sistema cause 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 modifi-

carlo.

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.

## Almacenes web personalizados

Esta función proporciona acceso al almacén web personalizado de su organización desde la aplicación Citrix Workspace para Windows. Para usar esta función, el administrador debe agregar el dominio o el almacén web personalizado a las URL permitidas de Global App Configuration Service.

Para obtener más información sobre cómo configurar las direcciones URL de almacén web para los usuarios finales, consulte [Global App Configuration Service](#).

Ahora puede proporcionar la URL del almacén web personalizado en la pantalla **Agregar cuenta** de la aplicación Citrix Workspace. El almacén web personalizado se abre en la ventana de la aplicación Citrix Workspace nativa.

Para quitar el almacén web personalizado, vaya a **Cuentas > Agregar o quitar cuentas**, seleccione la URL del almacén web personalizado y haga clic en **Quitar**.

## Configurar

May 23, 2024

Al utilizarse la aplicación Citrix Workspace para Windows, los parámetros siguientes permiten a los usuarios acceder a sus aplicaciones y escritorios alojados.

### Microsoft Teams

- [Pantalla compartida](#)
- [Estimador de rendimiento del codificador](#)
- [Eliminación de eco acústico](#)

### Pantalla compartida

A partir de la versión 2006.1, hay nuevas funcionalidades en la función saliente de uso compartido de la pantalla para la aplicación Microsoft Teams que emplea la optimización HDX.

El contenido compartido con Microsoft Teams se limita al contenido de la ventana de **Desktop Viewer**. Todo lo que está fuera de la ventana de **Desktop Viewer** (escritorio local del cliente, aplicaciones) se oscurece.

En un sistema operativo Windows 10, los siguientes elementos no se oscurecen cuando se superponen a la ventana de **Desktop Viewer**:

- El menú Inicio, el menú Buscar y la vista de tareas.
- La barra de notificaciones y las notificaciones que aparecen en el lado derecho de la barra de tareas.
- En una configuración de varios monitores con diferentes parámetros de PPP. Si una aplicación local se superpone en 2 monitores diferentes y su valor de PPP no coincide con el del monitor principal que tiene la ventana de Desktop Viewer.
- La aplicación y la vista previa que se muestran al pasar el mouse sobre el icono de la aplicación en la barra de tareas.

### Estimador de rendimiento del codificador

`HdxRtcEngine.exe` es el motor de medios WebRTC integrado en la aplicación Citrix Workspace que gestiona la redirección de Microsoft Teams. A partir de la aplicación Citrix Workspace 1912 o una versión posterior, `HdxRtcEngine.exe` puede estimar la mejor resolución de codificación que la CPU del dispositivo de punto final puede soportar sin sobrecargarse. Los valores posibles son: 240p, 360p, 480p, 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. La negociación del códec incluye la resolución más alta posible. La negociación del códec puede ser 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 (1920x1080 16:9 @ 30 fps)                     | 3                           |
| medio                                      | 720p (1280x720 16:9 @ 30 fps)                       | 2                           |
| lento                                      | 360p (640x360 16:9 @ 30 fps o 640x480 4:3 @ 30 fps) | 1                           |

| Rendimiento del dispositivo de punto final | Resolución máxima                                   | Valor de clave del Registro |
|--------------------------------------------|-----------------------------------------------------|-----------------------------|
| muy lento                                  | 240p (320x180 16:9 @ 30 fps o 320x240 4:3 @ 30 fps) | 0                           |

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

Vaya a la ruta del Registro HKEY\_CURRENT\_USER\SOFTWARE\Citrix\HDXMediaStream y cree esta clave:

| Nombre              | Tipo  | Valores | Descripción                                                                                                        |
|---------------------|-------|---------|--------------------------------------------------------------------------------------------------------------------|
| OverridePerformance | DWORD | 0;1;2;3 | Fuerza el rendimiento deseado. El valor debe estar en el intervalo entre 0 y 3, donde 0 indica lento, y 3, rápido. |

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

### Eliminación de eco acústico

La eliminación del eco en `HdxRtcEngine.exe` puede inhabilitarse para solucionar problemas de rendimiento de audio o de compatibilidad con periféricos que tienen prestaciones de AEC integradas.

Vaya a la ruta del Registro HKEY\_CURRENT\_USER\SOFTWARE\Citrix\HDXMediaStream y cree esta clave:

Nombre: EnableAEC

Tipo: REG\_DWORD

Datos: 0

(0 inhabilita AEC y 1 habilita AEC; si `Regkey` no está presente, el comportamiento predeterminado en `HdxRtcEngine` es el de habilitar AEC, independientemente de las prestaciones de hardware del periférico).

## Mejoras en la optimización de Microsoft Teams

- A partir de la aplicación Citrix Workspace 2112.1 para Windows, estas funciones solo están disponibles después de la implantación de actualizaciones futuras de Microsoft Teams.

Cuando Microsoft implante la actualización, consulte el artículo de Knowledge Center [CTX253754](#) para obtener información sobre la actualización de la documentación y el anuncio.

- **Reuniones y chats en varias ventanas para Microsoft Teams:** Puede usar varias ventanas para chats y reuniones en Microsoft Teams (1.4.00.16771 o una versión posterior) cuando HDX lo optimiza en Citrix Virtual Apps and Desktops (2112 o una versión posterior). Puede separar las conversaciones o las reuniones de varias maneras. Para obtener más información sobre la función de ventana emergente, consulte [Microsoft Teams Pop-Out Window for Chats and Meetings](#) en el sitio de Microsoft Office 365.

Si ejecuta una versión anterior de la aplicación Citrix Workspace o Virtual Delivery Agent (VDA), es posible que Microsoft retire el código de las ventanas únicas en el futuro. Sin embargo, puede actualizarlos a la versión de VDA o de la aplicación Citrix Workspace que admita varias ventanas (2112 y versiones posteriores) antes de que hayan transcurrido nueve meses de la fecha en que la función se puso a disposición general.

- **Uso compartido de aplicaciones:** Antes no podía compartir aplicaciones mediante la función **Compartir pantalla** en Microsoft Teams al habilitar la directiva HDX 3D Pro en Citrix Studio.

A partir de la aplicación Citrix Workspace 2112.1 para Windows y Citrix Virtual Apps and Desktops 2112, la función de **Pantalla compartida** le permite compartir aplicaciones en Microsoft Teams. Puede compartir aplicaciones cuando la directiva de HDX 3D Pro esté habilitada.

- **Dar control:** Puede usar el botón **Dar control** para otorgar el control de su pantalla compartida a otros usuarios que participan en la reunión. Los otros participantes pueden seleccionar elementos y modificar la pantalla compartida mediante el teclado, el mouse y el portapapeles. Tanto usted como el participante tienen el control de la pantalla compartida y pueden recuperar el control en cualquier momento.
- **Tomar el control:** Durante las sesiones de uso compartido de pantalla, cualquier participante puede solicitar el control mediante el botón **Solicitar el control**. La persona que comparte la pantalla puede aprobar o rechazar la solicitud. Cuando tiene el control, puede controlar el teclado y el mouse en la pantalla compartida y liberar el control para dejar de compartir el control.

### Limitación:

La opción **Solicitar el control** no está disponible durante llamadas entre un usuario optimizado y un usuario en el cliente de escritorio de Microsoft Teams nativo en el dispositivo de punto

final. Como solución temporal, los usuarios pueden unirse a una reunión para obtener la opción **Solicitar el control**.

- **E911 dinámico:** La aplicación Citrix Workspace admite llamadas de emergencia dinámicas. Cuando se usa en los planes de llamadas de Microsoft, Operator Connect y enrutamiento directo, proporciona la opción de:
  - \* configurar y redirigir llamadas de emergencia
  - \* notificar al personal de seguridad

La notificación se envía en función de la ubicación actual de la aplicación Citrix Workspace que se ejecuta en el dispositivo de punto final, en lugar del cliente de Microsoft Teams del VDA.

La ley de Ray Baum exige que la ubicación transmitible de la persona que llama al 911 se transmita al Punto de Respuesta de Seguridad Pública (PSAP) correspondiente. A partir de la aplicación Citrix Workspace 2112.1 para Windows, la optimización para Microsoft Teams con HDX cumple con la ley de Ray Baum.

- A partir de la aplicación Citrix Workspace 2109.1 para Windows, estas funciones solo están disponibles después de la implantación de actualizaciones futuras de Microsoft Teams.

Cuando Microsoft implante la actualización, consulte CTX253754 para obtener información sobre la actualización de la documentación y el anuncio.

- **Compatibilidad con WebRTC:** La aplicación Citrix Workspace 2109.1 para Windows admite WebRTC 1.0 para ofrecer una mejor experiencia en videoconferencias junto en la vista de galería.
- **Mejora del uso compartido de la pantalla:** Puede compartir aplicaciones individuales, ventanas o la pantalla completa mediante la función de uso compartido de la pantalla en Microsoft Teams. Citrix Virtual Delivery Agent 2109 es un requisito previo para esta función.
- **Compatibilidad con App Protection:** Ahora, cuando App Protection está habilitada, puede compartir contenido a través de Microsoft Teams con la optimización de HDX. Con esta función, puede compartir la ventana de aplicaciones que se ejecutan en el escritorio virtual. Citrix Virtual Delivery Agent 2109 es un requisito previo para esta función.

**Nota:**

El uso compartido total del escritorio o de los monitores se inhabilita cuando App Protection se habilita para el grupo de entrega.

- **Subtítulos en directo:** La aplicación Citrix Workspace 2109.1 para Windows ofrece la transcripción en tiempo real de lo que dicen los ponentes cuando Subtítulos en directo esté habilitado en Microsoft Teams.

- La aplicación Citrix Workspace 2109.1 para Windows admite lo siguiente en Microsoft Teams optimizado de aplicaciones alojadas por VM:
  - \* Llamadas de audio y vídeo entre dos usuarios
  - \* Llamada de conferencias
  - \* Pantalla compartida
- A partir de la aplicación Citrix Workspace 2106 para Windows:
  - 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.
- A partir de la aplicación Citrix Workspace 2105 para Windows:
  - 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.
  - Puede inhabilitar el módulo del dispositivo de audio 2 (ADM2) para que se utilice el módulo de dispositivo de audio (ADM) antiguo para micrófonos de cuatro canales. Inhabilitar ADM2 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.
- A partir de la aplicación Citrix Workspace 2103.1 para Windows:
  - Ahora el códec de vídeo VP9 está inhabilitado de forma predeterminada.
  - 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 **DirectWShow** es el generador predeterminado.

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

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

Otros valores posibles:

- \* 0: Media Foundation
- \* 1: DirectShow (predeterminado)

4. Vuelva a iniciar la aplicación Citrix Workspace.

- A partir de la aplicación Citrix Workspace 2012 para Windows:
  - Ahora, los usuarios pueden ver el puntero del presentador en una sesión de pantalla compartida.
  - El motor de medios **WebRTC** ahora tiene en cuenta el servidor proxy configurado en el dispositivo cliente.
- A partir de la aplicación Citrix Workspace 2009.6 para Windows:
  - Microsoft Teams muestra los dispositivos periféricos utilizados anteriormente en la lista **Dispositivos preferidos**.
  - El motor de medios **WebRTC** determina con precisión la resolución máxima de codificación posible en un dispositivo de punto final. El motor de medios **WebRTC** realiza estimaciones varias veces al día y no solo al iniciarse por primera vez.
  - El instalador de la aplicación Citrix Workspace incluye tonos de llamada de Microsoft Teams.
  - Mejoras en la eliminación del eco: Se ha reducido el nivel de eco cuando un compañero tiene un altavoz o un micrófono que generan eco.
  - Mejoras en el uso compartido de la pantalla: Al compartir la pantalla, solo la pantalla de **Desktop Viewer** se captura en formato de mapa de bits nativo. Antes, las ventanas locales del cliente que quedaban se superponían a la ventana de **Desktop Viewer** quedaban oscurecidas.
- A partir de la aplicación Citrix Workspace 2002 para Windows:

- 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.

## Tareas y aspectos relevantes para administradores

En este artículo se describen las tareas y los aspectos que son relevantes para los administradores de la aplicación Citrix Workspace para Windows.

### Administrar marcas de función

Si se produce un problema con la aplicación Citrix Workspace en producción, podemos inhabilitar de manera dinámica una función afectada en la aplicación Citrix Workspace aunque dicha función ya se haya publicado.

Para ello, se utilizan marcas de función y un servicio externo denominado LaunchDarkly. No es necesario que realice ninguna configuración para permitir el tráfico a LaunchDarkly, salvo si tiene un firewall o proxy bloqueando el tráfico saliente. En ese caso, puede habilitar el tráfico a LaunchDarkly a través de direcciones URL o direcciones IP específicas, según sus requisitos de directiva.

Puede habilitar el tráfico y la comunicación en LaunchDarkly de las siguientes formas:

### Permitir el tráfico a las siguientes URL

- [events.launchdarkly.com](https://events.launchdarkly.com)
- [stream.launchdarkly.com](https://stream.launchdarkly.com)
- [clientstream.launchdarkly.com](https://clientstream.launchdarkly.com)
- [Firehose.launchdarkly.com](https://firehose.launchdarkly.com)
- [mobile.launchdarkly.com](https://mobile.launchdarkly.com)

**Incluir direcciones IP en una lista de permitidos** Si necesita incluir las direcciones IP en una lista de permitidos, para obtener una lista de todos los intervalos de direcciones IP actuales, consulte esta [lista de direcciones IP públicas de LaunchDarkly](#). Puede usar esta lista para saber que las configuraciones de su firewall se actualizan automáticamente de acuerdo con las actualizaciones de la infraestructura. Para obtener detalles sobre el estado actual de los cambios en la infraestructura, consulte la [Página de estado de LaunchDarkly](#).

**Requisitos del sistema para LaunchDarkly** Compruebe si las aplicaciones pueden comunicarse con los siguientes servicios si el parámetro de túnel dividido está **desactivado** en Citrix ADC para estos servicios:

- Servicio de LaunchDarkly.
- Servicio de escucha de APNs

**Inhabilitar el servicio de LaunchDarkly** Puede inhabilitar el servicio de LaunchDarkly mediante una directiva de objeto de directiva de grupo (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 > Conformidad**.
3. Seleccione la directiva **Inhabilitar el envío de datos a terceros** y habilítela.
4. Haga clic en **Aplicar** y **Aceptar**.

También puede inhabilitar el servicio de LaunchDarkly mediante el Registro.

1. Abra el Editor del Registro.
2. Vaya a `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix` una máquina de 64 bits y `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix` una máquina de 32 bits.
3. Cree y agregue una cadena de Registro REG\_SZ con el nombre **EnableLDFeature** y establezca su valor como **False**.
4. Salga de la aplicación Citrix Workspace y reiníciela para que los cambios surtan efecto.

## App Protection

### Renuncia de responsabilidades

Las directivas de App Protection filtran el acceso a las funciones requeridas del sistema operativo subyacente (llamadas a API específicas necesarias para capturar pantallas o pulsaciones de teclas). Las directivas de App Protection proporcionan protección incluso contra herramientas de piratas informáticos personalizadas y con un diseño específico. Sin embargo, a medida que los sistemas operativos evolucionan, es posible que surjan 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 en 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 la interfaz de línea de comandos o la GUI.
- Durante el inicio de una aplicación (instalación a demanda).

**Nota:**

- Esta función solo está disponible en sistemas operativos de escritorio como Windows 10 o Windows 8.1.
- A partir de la versión 2006.1, la aplicación Citrix Workspace no se admite en Windows 7. Por lo tanto, App Protection no funciona en Windows 7. Para obtener más información, consulte [Elementos retirados](#).
- Esta función no se puede usar 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 GUI disponible para este propósito.

**Nota:**

A partir de la versión 2103, Citrix DaaS solo ofrece App Protection con StoreFront.

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

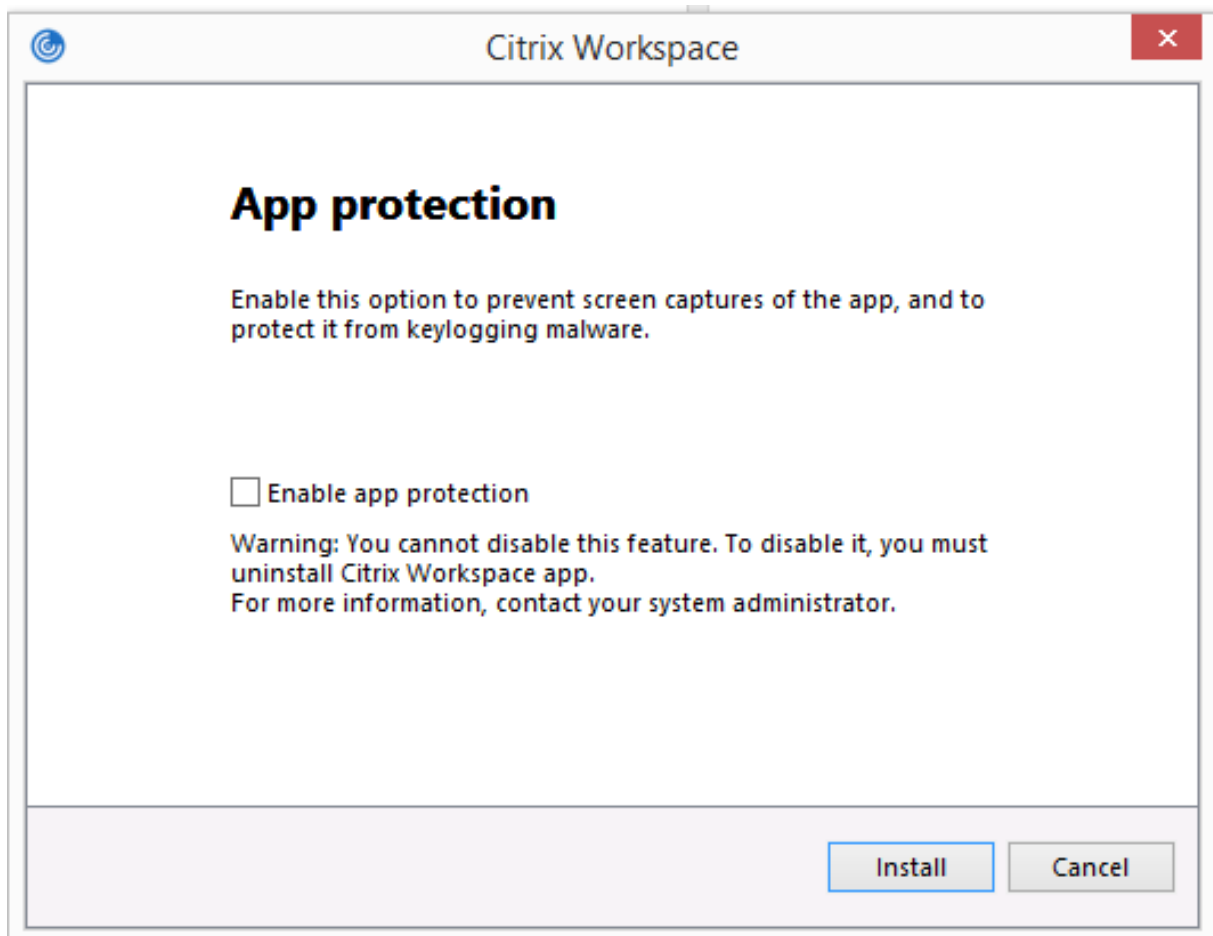
### Nota:

- 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 hecho de agregar el componente de App Protection afecte a la función 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 (GUI)
- Interfaz de línea de comandos

**Interfaz gráfica (GUI)** 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 |

En versiones anteriores, toda la pantalla, incluidas las aplicaciones no protegidas en segundo plano, se oscurecían al tomar una captura de pantalla de una ventana protegida.

A partir de la versión 2008, al tomar una captura de pantalla, solo se oscurece la ventana protegida. Puede hacer una captura de pantalla de la zona que queda fuera de la ventana protegida.

**Comportamiento previsto:**

El comportamiento previsto depende del método por el cual los usuarios acceden al almacén de Store-Front que tiene los recursos protegidos.

**Nota:**

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

sesiones protegidas.

- **Comportamiento en los espacios de trabajo para la web:**

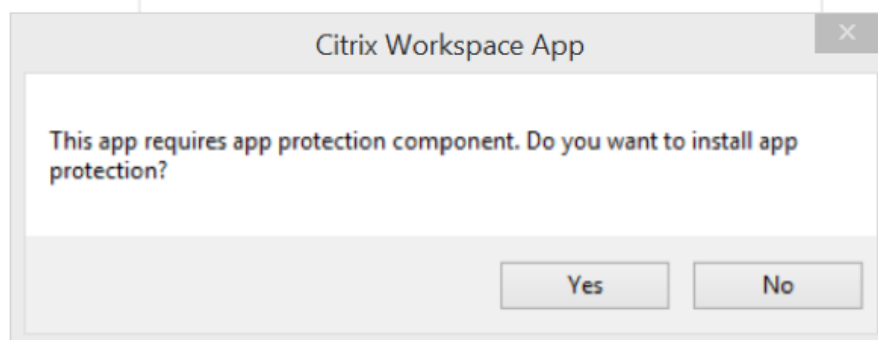
El componente de App Protection no se admite en las configuraciones de espacios de trabajo para la web. Las aplicaciones protegidas por directivas de App Protection no se indican. Para obtener más información acerca de los recursos asignados, póngase en contacto con el administrador del sistema.

- **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:**

En un Controller configurado con App Protection, si intenta iniciar una aplicación protegida, App Protection se instala a demanda. Aparece el siguiente cuadro de diálogo:



Haga clic en **Sí** para instalar el componente de App Protection. A continuación, puede iniciar la aplicación protegida.

- **Comportamiento de la sesión protegida en caso de protocolo de escritorio remoto (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).

## Mejora de la configuración de App Protection

Antes, el administrador de autenticación y los cuadros de diálogo de **Self-Service Plug-in** estaban protegidos de forma predeterminada.

A partir de la versión 2012, puede configurar las funciones de protección contra el registro de teclado y protección contra capturas de pantalla por separado para las interfaces del administrador de autenticación y del Self-Service Plug-in. Puede configurar las funcionalidades mediante una directiva de objeto de directiva de grupo (GPO).

**Nota:**

Esta directiva de GPO no se aplica a las sesiones ICA y SaaS. Las sesiones ICA y SaaS se siguen controlando mediante el Delivery Controller y Citrix Gateway Service.

**Configuración de App Protection para la interfaz del Self-Service Plug-in:**

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**.
3. Para configurar la protección contra el registro de teclado y la protección contra capturas de pantalla para el cuadro de diálogo del Self-Service Plug-in, seleccione **Autoservicio > directiva Administrar App Protection**.
4. Seleccione una de estas opciones o las dos:
  - **Protección contra el registro de teclado:** Evita que programas capturen teclado.
  - **Protección contra capturas de pantalla:** Evita que los usuarios realicen capturas de pantalla y compartan su pantalla.
5. Haga clic en **Aplicar** y **Aceptar**.

**Configuración de App Protection para el administrador de autenticación:**

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**.
3. Para configurar la protección contra el registro de teclado y la protección contra capturas de pantalla para el administrador de autenticación, seleccione **Autenticación de usuarios > directiva Administrar App Protection**.
4. Seleccione una de estas opciones o las dos:
  - **Protección contra el registro de teclado:** Evita que programas capturen teclado.
  - **Protección contra capturas de pantalla:** Evita que los usuarios realicen capturas de pantalla y compartan su pantalla.
5. Haga clic en **Aplicar** y **Aceptar**.

**Registros de errores de App Protection:**



A partir de la versión 2103, los registros de App Protection se recopilan como parte de los registros de la aplicación Citrix Workspace. Para obtener más información sobre la recopilación de registros, consulte [Recopilación de registros](#).

No es necesario instalar ni usar una aplicación de terceros para recopilar específicamente los registros de App Protection. Sin embargo, DebugView todavía se puede seguir utilizando para la recopilación de registros.

Los registros 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:

- Esta función no está disponible en sistemas operativos de Microsoft Server, como Windows Server 2012 R2 y Windows Server 2016.
- 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.

### Categorías de las aplicaciones

Las categorías de las aplicaciones permiten a los usuarios administrar colecciones de aplicaciones en la aplicación Citrix Workspace. Puede crear grupos de aplicaciones para aplicaciones compartidas

en diferentes grupos de entrega o utilizadas por un subconjunto de usuarios dentro de los grupos de entrega.

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

## Seguridad de archivos ICA mejorada

Esta función proporciona una mayor seguridad al gestionar archivos ICA durante el inicio de sesiones de Virtual Apps and Desktops.

Ahora, la aplicación Citrix Workspace le permite almacenar el archivo ICA en la memoria del sistema en lugar de hacerlo en el disco local al iniciar sesiones de aplicaciones y escritorios virtuales.

Esta función tiene como objetivo eliminar los ataques de superficie y cualquier malware que pueda utilizar incorrectamente el archivo ICA al almacenarlo localmente. Esta función también se puede aplicar a las sesiones de aplicaciones y escritorios virtuales que se inician en Workspace para Web

## Configuración

La seguridad de archivos ICA también se ofrece al acceder a Citrix Workspace o a StoreFront desde la web. La detección de clientes es un requisito previo para que la función esté operativa si se accede a través de la web. Si accede a StoreFront mediante un explorador, habilite estos atributos en el archivo web.config de las implementaciones de StoreFront:

---

| Versión de StoreFront | Atributo        |
|-----------------------|-----------------|
| 2.x                   | pluginassistant |
| 3.x                   | protocolHandler |

---

Cuando inicie sesión en el almacén a través del explorador web, haga clic en **Detectar la aplicación Workspace**. Si no aparece la solicitud, borre las cookies del explorador web e inténtelo de nuevo.

Si se trata de una implementación de Workspace, los parámetros de detección de clientes se encuentran en **Parámetros de cuenta > Avanzado > Preferencia de inicio de aplicaciones y escritorios**.

Puede tomar medidas adicionales para que las sesiones se inicien solo con el archivo ICA almacenado en la memoria del sistema. Utilice cualquiera de estos métodos:

- Plantilla administrativa de objetos de directiva de grupo (GPO) en el cliente.
- Global App Config Service
- Workspace para Web.

### Mediante el GPO:

Para bloquear los inicios de sesión desde archivos ICA almacenados en el disco local, haga lo siguiente:

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 > Motor de cliente**.
3. Seleccione la directiva **Proteger inicio de sesiones con archivos ICA y habilítela**.
4. Haga clic en **Aplicar** y **Aceptar**.

### Mediante Global App Config Service:

Para bloquear los inicios de sesión desde archivos ICA almacenados en el disco local, haga lo siguiente:

Establezca el atributo **Bloquear el inicio directo del archivo ICA** en **True**.

Para obtener más información sobre Global App Config Service, consulte la documentación de [Global App Config Service](#).

### Con Workspace para Web:

Para no permitir la descarga de archivos ICA en el disco local al usar Workspace para Web, haga lo siguiente:

Ejecute el módulo de PowerShell. Consulte [Configure DisallowICADownload](#).

#### Nota:

La directiva **DisallowICADownload** no está disponible para implementaciones de StoreFront.

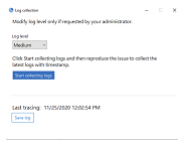
## Recopilación de registros

La recopilación de registros simplifica el proceso de recopilación de registros para la aplicación Citrix Workspace. Los registros ayudan a Citrix a solucionar problemas y, en el caso de problemas complicados, facilitan la asistencia técnica.

Puede recopilar registros mediante la interfaz gráfica de usuario.

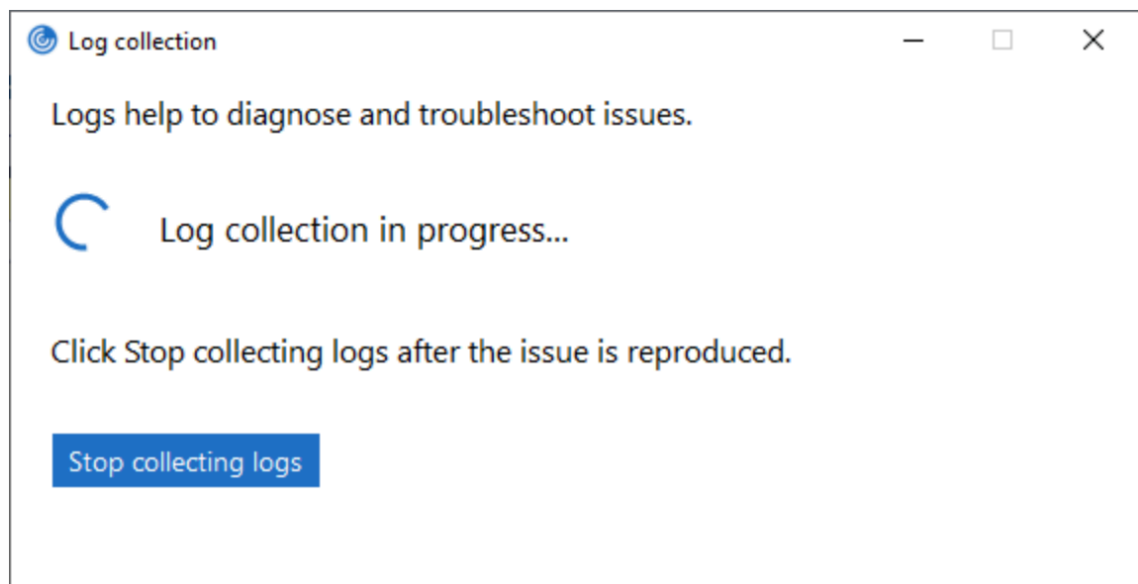
### Recopilación de registros:

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 **Recopilación de registros**.  
Aparecerá el cuadro de diálogo Recopilación de registros.



3. Seleccione uno de los siguientes niveles de registros:
  - Bajo
  - Medio
  - Detallado
4. Haga clic en **Comenzar a recopilar registros** para reproducir el problema y recopilar los registros más recientes.

Se inicia el proceso de recopilación de registros.



5. Haga clic en **Dejar de recopilar registros** una vez reproducido el problema.
6. Haga clic en **Guardar registro** para guardar los registros en la ubicación deseada.

## Rendimiento HDX adaptable

El rendimiento HDX adaptable ajusta de manera inteligente el rendimiento máximo de la sesión ICA porque adapta los búferes de salida. Al principio, la cantidad de búferes de salida se establece en un valor alto. Este valor alto permite que los datos se transmitan al cliente de manera más rápida y eficiente, especialmente en redes de latencia alta.

Ofrece una mejor interactividad, transferencias de archivos más rápidas, reproducciones de vídeo más fluidas, mayor velocidad de fotogramas y mayor resolución en una experiencia de usuario mejorada.

La interactividad de la sesión se mide constantemente para determinar si algún flujo de datos de la sesión ICA está afectando negativamente a la interactividad. Si eso ocurre, el rendimiento se reduce para disminuir el impacto del flujo de datos de gran tamaño en la sesión y permitir que se recupere la interactividad.

Esta función solo se admite en la aplicación Citrix Workspace 1811 para Windows y versiones posteriores.

**Importante:**

El rendimiento HDX adaptable cambia los búferes de salida al transferir el mecanismo del cliente al VDA. Por lo tanto, adaptar la cantidad de búferes de salida presentes en el cliente como se describe en el artículo [CTX125027](#) de Knowledge Center no produce ningún efecto.

## Transporte adaptable

El transporte adaptable es un mecanismo de Citrix Virtual Apps and Desktops y Citrix DaaS que permite utilizar el protocolo Enlightened Data Transport (EDT) para conexiones ICA. Para obtener más información, consulte la sección [Transporte adaptable](#) en la documentación de Citrix Virtual Apps and Desktops.

## Hoja de Preferencias avanzadas

A partir de la versión 4.10, puede personalizar la disponibilidad de la hoja **Preferencias avanzadas** y el contenido que figura en el menú contextual del icono de la aplicación Citrix Workspace del área de notificaciones. Al hacerlo, 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 siguientes parámetros concretos en la hoja:
  - 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 parámetros concretos de la hoja de **Preferencias avanzadas**

Puede ocultar parámetros específicos configurables por el usuario en la hoja **Preferencias avanzadas** mediante la plantilla administrativa de GPO de la aplicación Citrix Workspace. Para ocultar los parámetros:

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 los efectos de cada una de ellas:

| 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**.

### Migración de URL de StoreFront a Workspace

Esta función se halla actualmente en Technical Preview. La migración de URL de StoreFront a Workspace le permite migrar fácilmente a los usuarios finales de un almacén de StoreFront a un almacén de Workspace con una interacción mínima de los usuarios.

Tenga en cuenta que todos los usuarios finales tienen un almacén de StoreFront `storefront.com` agregado a su aplicación Citrix Workspace. Como administrador, puede configurar una asignación de URL de StoreFront a una URL del espacio de trabajo `{'storefront.com':'xyz.cloud.com'}` en Global App Configuration Service. Global App Config Service envía el parámetro a todas las instancias de la aplicación Citrix Workspace, tanto a dispositivos administrados como a no administrados que tienen agregada la URL de StoreFront `storefront.com`.

Tras detectarse este parámetro, la aplicación Citrix Workspace agrega la URL del espacio de trabajo asignada `xyz.cloud.com` como otro almacén. Cuando el usuario final inicia la aplicación Citrix Workspace, se abre el almacén de Citrix Workspace. El almacén de StoreFront `storefront.com` agregado anteriormente se agrega a la aplicación Citrix Workspace. Los usuarios siempre pueden volver al almacén de StoreFront `storefront.com` mediante la opción **Cambiar de cuenta** en la aplicación Citrix Workspace. Los administradores pueden controlar la eliminación del almacén de StoreFront `storefront.com` de la aplicación Citrix Workspace en los dispositivos de punto final. Se puede eliminar a través de Global App Config Service.

Para habilitar la función, siga estos pasos:

1. Configure esta asignación de StoreFront a Workspace mediante Global App Config Service. Para obtener más información sobre Global App Config Service, consulte [Global App Configuration Service](#).
2. Modifique la carga útil en el servicio de configuración de aplicaciones:

```
1 {
2 "serviceURL": Unknown macro: {
3 "url" }
4
5 ,
6 "settings":{
7
8 "name":"Productivity Apps", [New Store Name]
9 "description":"Provides access StoreFront to Workspace Migration",
10 "useForAppConfig":true,
11 "appSettings":
12 {
13 "windows":[Unknown macro: {
14 "category" }
15
16]
17 }
18
19 }
20
21 }
22
23 <!--NeedCopy-->
```



**Nota:**

Si piensa configurar la carga útil por primera vez, use **POST**.

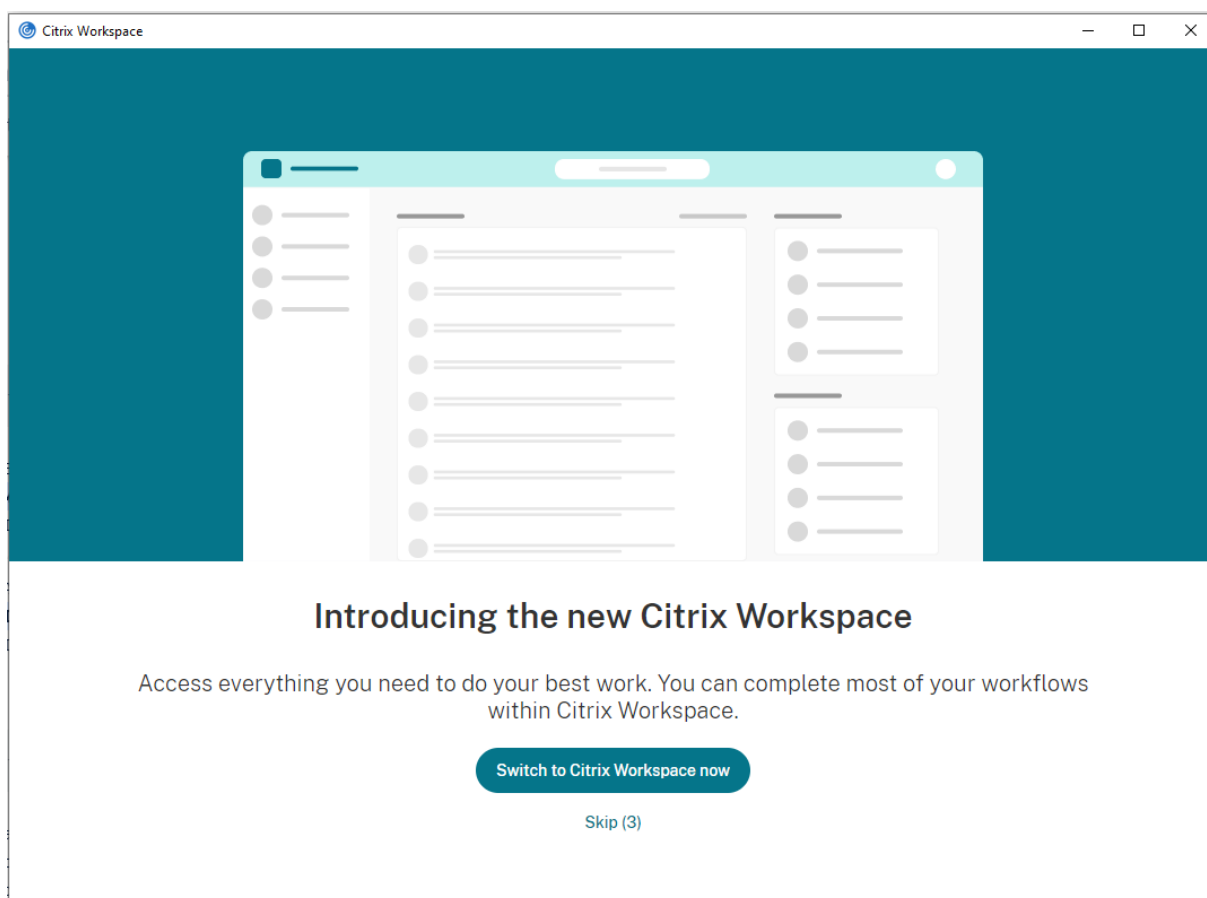
Si piensa modificar la configuración de la carga útil existente, utilice **PUT** y compruebe que tiene una carga útil que consta de todos los parámetros compatibles.

3. Especifique la URL de StoreFront [storefront.com](https://storefront.com) como el valor de **URL** en la sección **serviceURL**.
4. Configure la URL del espacio de trabajo [xyz.cloud.com](https://xyz.cloud.com) en la sección **migrationUrl**.
5. Utilice **storeFrontValidUntil** para establecer el calendario de la eliminación del almacén de StoreFront de la aplicación Citrix Workspace. Este campo es opcional. Puede establecer este valor según lo que necesite:
  - Fecha válida en el formato (AAAA-MM-DD)

**Nota:**

Si proporcionó una fecha anterior, el almacén de StoreFront se quita inmediatamente después de la migración de la URL. Si proporcionó una fecha futura, el almacén de StoreFront se quitará en la fecha establecida.

Una vez enviados los parámetros, se muestra esta pantalla:



Cuando el usuario hace clic en **Cambiar a Citrix Workspace**, la URL del espacio de trabajo se agrega a la aplicación Citrix Workspace y aparece la solicitud de autenticación. Los usuarios tienen una opción limitada de retrasar la transición hasta tres veces.

## 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 abrir un explorador web para ir a un sitio de Workspace para Web y 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*. El modo de autoservicio le permite suscribirse a aplicaciones desde la interfaz de usuario de la aplicación Citrix Workspace. La experiencia de usuario mejorada es similar al uso de una tienda 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:** Los administradores pueden configurar la aplicación Citrix Workspace para que coloque automáticamente accesos directos de aplicaciones y escritorios directamente en el menú Inicio o en el escritorio. La ubicación es similar a la de la aplicación Citrix Workspace Enterprise. El nuevo modo de *accesos directos solamente* permite a los usuarios buscar todas sus aplicaciones publicadas dentro del esquema de navegación de Windows estándar al que están acostumbrados.

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

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

Con solo agregar una cuenta de StoreFront a la aplicación Citrix Workspace o configurar la aplicación Citrix Workspace para que apunte a un sitio de StoreFront, puede configurar el modo de autoservicio. La configuración permite a los usuarios suscribirse a aplicaciones desde la interfaz de usuario de Citrix Workspace. La experiencia de usuario mejorada es similar al uso de una tienda 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 que proporcione para 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, 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. En su lugar, muestra las aplicaciones individualmente o en la carpeta raíz. Las aplicaciones no se encuentran en las subcarpetas de categoría definidas con Citrix Virtual Apps

and Desktops.

- Para establecer un único directorio para todos los accesos directos del 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 ninguna entrada en los clientes “Agregar o quitar programas”, use `DontCreateAddRemoveE`. Parámetros: “true” o “false”(predeterminado: false).
- Para quitar los accesos directos y el icono de Citrix Workspace de una aplicación que estuvo disponible en el almacén, pero ya no lo está, use `SilentlyUninstallRemovedResources`. 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:**

Es posible que los elementos de propiedad agregados antes de la etiqueta `<clear />` los invaliden. 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](#).

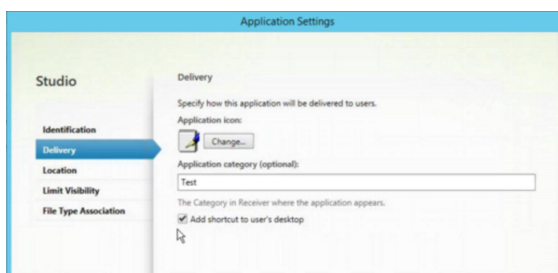
### Usar parámetros por aplicación en Citrix Virtual Apps and Desktops 7.x para personalizar ubicaciones de los accesos directos de las aplicaciones

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. Sin embargo, esta configuración es similar a la de las versiones anteriores de Workspace para Windows. No obstante, la versión 4.2.100 incorporó la capacidad de controlar la ubicación del acceso directo a la aplicación mediante parámetros por aplicación de Citrix Virtual Apps. La función resulta útil en entornos donde hay varias aplicaciones que es necesario mostrar en ubicaciones coherentes.

### 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 necesario.
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

La aplicación Citrix Workspace proporciona la funcionalidad para copiar los códigos auxiliares EXE de un recurso compartido de red si:

- Hay una demora en la enumeración de aplicaciones en cada inicio de sesión
- O es necesario firmar digitalmente los códigos auxiliares de las aplicaciones

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. Use el Editor del Registro 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 crear ejecutables de código auxiliar, agregue todas las aplicaciones a la máquina mediante la aplicación Citrix Workspace; esta aplicación genera los archivos ejecutables.
2. Reúna los ejecutables de código auxiliar de `%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 de la aplicación Citrix Workspace y reiníciela para que los cambios surtan efecto.

### 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 docenas o incluso cientos de aplicaciones, permita a los usuarios seleccionar las aplicaciones para agregarlas al menú **Favoritos e Inicio**:

---

Si quiere que el usuario elija las aplicaciones que prefiere 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 prefiere tener en su menú Inicio, pero también quiere tener 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. 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 coloca aplicaciones en el menú Inicio, ni siquiera en el modo de autoservicio, a menos que usted las 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, coloque todas en el menú Inicio o en el escritorio, o bien 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 `PutShortcutsOnDesktop = true`. Todas las aplicaciones disponibles se muestran en el escritorio.

Si quiere que todos los accesos directos se coloquen en el escritorio dentro de una carpeta.

Configure la aplicación Citrix Workspace con `DesktopDir=Nombre de la carpeta de escritorio 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 `PutShortcutsInStartMenu=false` 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 los usuarios vean aplicaciones mientras otro usuario comparte el dispositivo de punto final, puede quitarlas 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 el equipo de un 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 preferida 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 el equipo de un 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.

**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 preferida 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 y Citrix DaaS.

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
\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.

## Distribución de pantallas virtuales

Esta función le permite definir una distribución de monitores virtuales que se aplica al escritorio remoto. También puede dividir un único monitor de cliente virtualmente en un máximo de ocho monitores en el escritorio remoto. Puede configurar los monitores virtuales en la ficha **Diseño del monitor** en Desktop Viewer. Allí, puede dibujar líneas horizontales o verticales para separar la pantalla en monitores virtuales. La pantalla se divide según el porcentaje especificado en la resolución del monitor de 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.

A partir de Citrix Workspace para Windows 2106, la distribución de pantallas virtuales también está disponible en sesiones de escritorio de pantalla completa y con varios monitores. La distribución de pantallas virtuales está habilitada de forma predeterminada. En casos con varios monitores, se aplica la misma distribución de pantallas virtuales configurada a todos los monitores de la sesión si el total de pantallas virtuales no es superior a ocho pantallas virtuales. Si se supera este límite, la distribución de pantallas virtuales se ignora y no se aplica a ningún monitor de la sesión.

Para inhabilitar la mejora para varios monitores, configure esta clave del Registro:

- `HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer`

Nombre: **SplitAllMonitors**

Tipo: DWORD

Valores:

1: Habilitada

0: Inhabilitada

## 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. La sesión de preinicio se crea cuando un usuario inicia sesión en la aplicación Citrix Workspace o a una hora programada si el usuario ha iniciado sesión.

La 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 surte efecto hasta la siguiente sesión. La aplicación predeterminada `ctxprelaunch.exe` se ejecuta en esta sesión, pero no es visible.

Para obtener más información, consulte las instrucciones para el preinicio de sesiones y la persistencia de sesiones en el artículo de Citrix Virtual Apps and Desktops titulado [Administrar grupos de entrega](#).

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 establezca 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 si reinicia la aplicación Citrix Workspace.
- **Preinicio programado:** El preinicio ocurre a una hora programada. El preinicio programado ocurre solamente 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 compartir la carga de red y del servidor. Por ejemplo, si el preinicio programado está programado para las 13:45, la sesión se inicia realmente entre las 13:15 y las 13:45. Por lo general, se usa en períodos de mucho tráfico.

La configuración del preinicio en un servidor de Citrix Virtual Apps consiste en lo siguiente:

- Crear, modificar o eliminar aplicaciones de preinicio
- Y actualizar los parámetros de directivas de usuario que controlan la aplicación de preinicio

No se puede usar el archivo `receiver.admx` para personalizar la función de preinicio. Sin embargo, puede cambiar la configuración de preinicio al modificar valores del Registro. Los valores del Registro se pueden modificar 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. Puede proporcionar a sus usuarios scripts para cambiar los valores.

#### **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**

Tipo: `REG_DWORD`

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**

Tipo: REG\_DWORD

Valores:

0: Inhabilita el preinicio.

1: Habilite el preinicio a petición. (el preinicio ocurre después de que el usuario autentique las credenciales).

2: Habilite el preinicio programado. (El preinicio comienza a la hora configurada en Programación).

Nombre: **Schedule**

Tipo: REG\_DWORD

Valor:

Hora (en formato de 24 horas) y días de la semana para los preinicios programados, con este formato:

---

HH:MM	M:T:W:TH:F:S:SU, donde HH y MM son las horas y los minutos. M:T:W:TH:F:S:SU son los días 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	1:0:1:0:1:0:0. La sesión se inicia entre las 13:15 y las 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.



Citrix ofrece redirección de host a cliente y acceso a aplicaciones locales para la redirección de cliente a URL. Sin embargo, recomendamos utilizar redirección bidireccional de contenido para los clientes de Windows que se unen 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

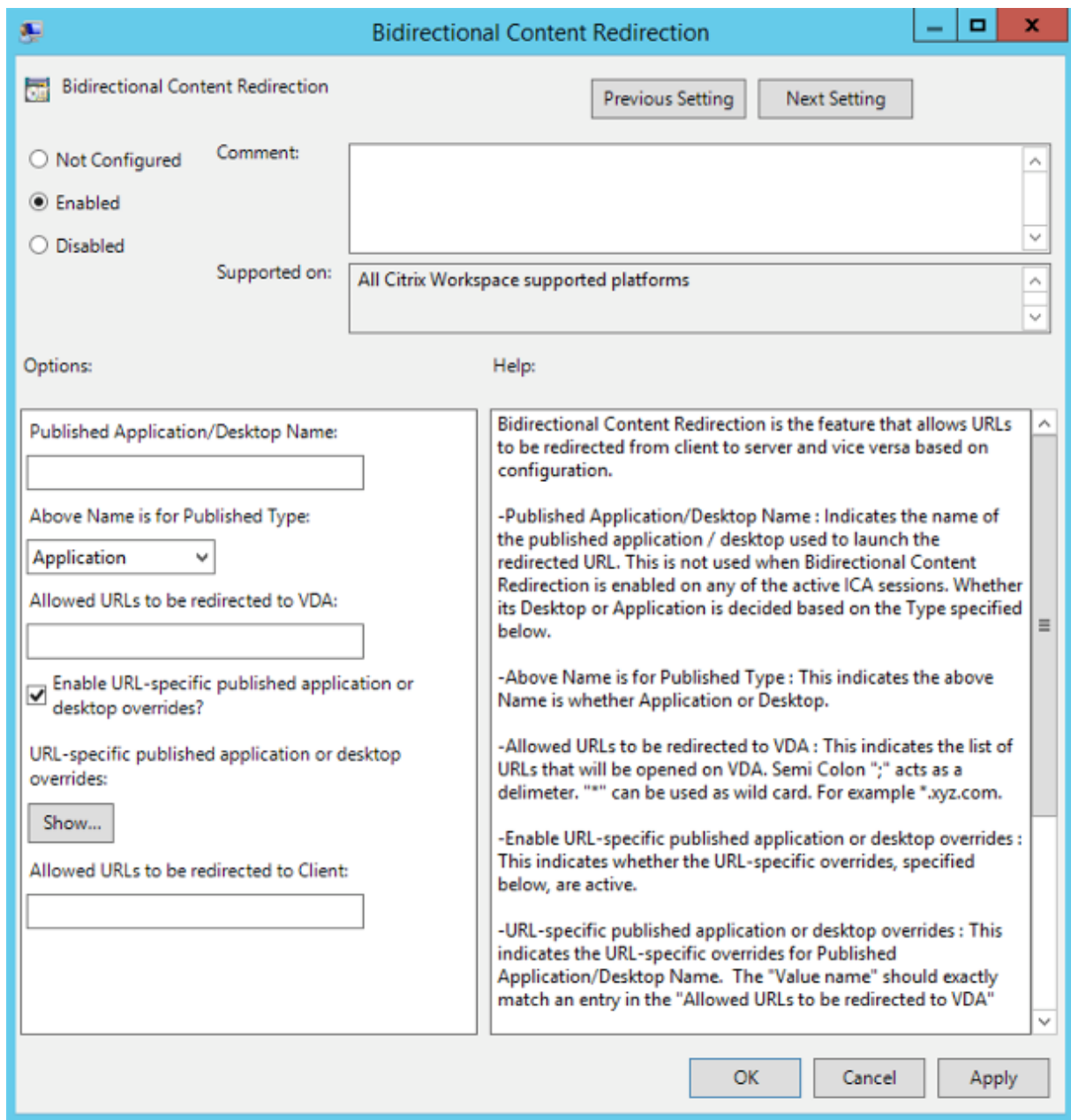
**Nota:**

- La redirección de contenido bidireccional no funciona en las sesiones en las que **Acceso a aplicaciones locales** está habilitado.
- 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**.



1. En el campo **Nombre de aplicación o escritorio publicados**, indique el nombre del recurso utilizado para iniciar la dirección URL redirigida.

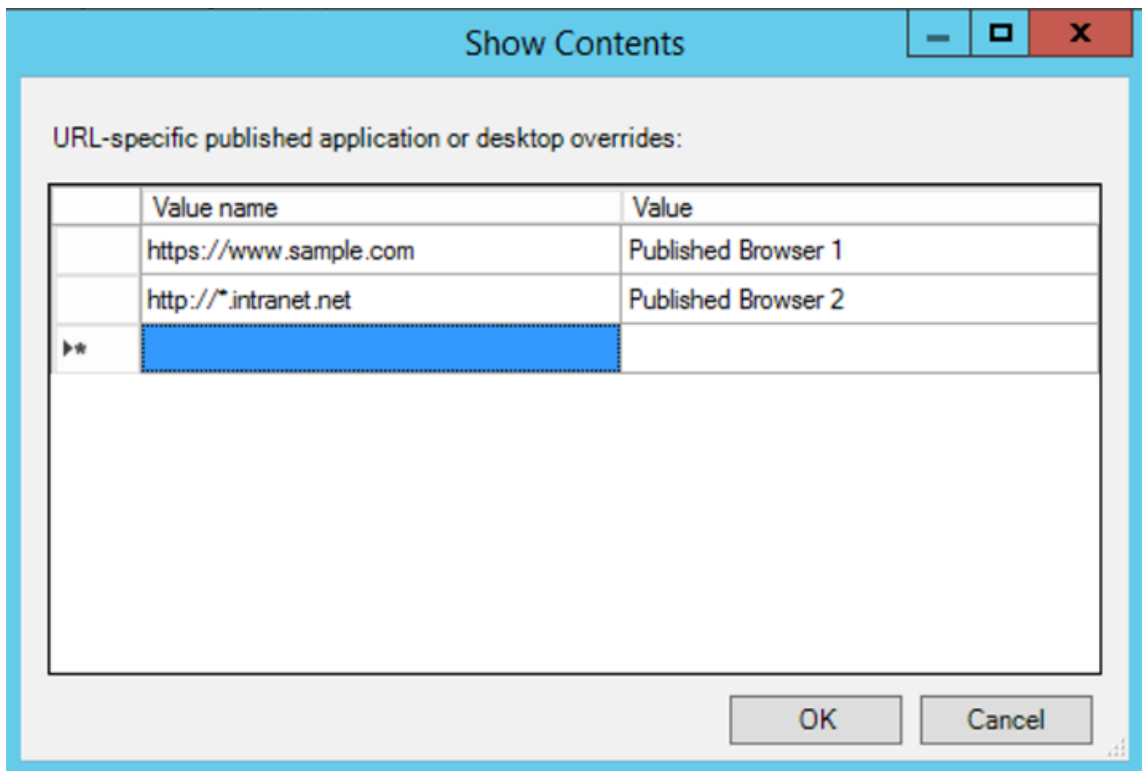
**Nota:**

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 supeditar 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 usan varias cuentas de StoreFront, el nombre simplificado de la cuenta principal de StoreFront se utiliza para iniciar la aplicación o una sesión de escritorio.
- Solo se abre una nueva ventana de explorador web cuando una dirección URL se redirige al cliente. Cuando una 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, hay habilitada una de las directivas de redirección de contenido del host y solamente existe una de las asociaciones de tipos de archivo de servidor. Citrix recomienda inhabilitar la asociación de tipos de archivo de servidor o la función de redirección de contenido de host (URL) para confirmar 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.

**Función de URL bidireccionales con exploradores web basados en Chromium**

La redirección bidireccional de contenido permite configurar direcciones URL para redirigir contenido del cliente al servidor y del servidor al cliente mediante directivas en el servidor y en el cliente.

Las directivas de servidor se establecen en el Delivery Controller, y las directivas de cliente se establecen en la aplicación Citrix Workspace. Las directivas se establecen mediante la plantilla administrativa de objetos de directiva de grupo (GPO).

A partir de la versión 2106, se ofrece la redirección bidireccional de URL para Google Chrome y Microsoft Edge.

**Requisitos previos:**

- Citrix Virtual Apps and Desktops 2106 o una versión posterior.
- Versión 5.0 de la extensión de redirección del explorador web.

Para registrar el explorador web Google Chrome en la redirección bidireccional de URL, ejecute este comando desde la carpeta de instalación de la aplicación Citrix Workspace:

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome /
verbose
```

**Nota:**

Al utilizar estos comandos en exploradores Chrome, la [extensión de redirección de contenido bidireccional](#) se instala automáticamente desde Chrome Web Store.

Para cancelar el registro del explorador web Google Chrome de la redirección bidireccional de URL, ejecute este comando desde la carpeta de instalación de la aplicación Citrix Workspace:

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome /
verbose
```

**Nota:**

Si aparece este error al acceder a la página Extensiones del explorador web, ignórelo:

```
WebSocket connection to wss://... failed.
```

Para obtener información sobre cómo configurar la redirección de URL en la aplicación Citrix Workspace, consulte [Redirección de contenido bidireccional](#).

**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 simultáneamente, es posible que la información que contienen no sea legible. 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. Use el Editor del Registro 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 **DisabledImmung** 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 de 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.

La función Citrix Casting permite acceder de forma instantánea y segura a cualquier aplicación desde un dispositivo móvil y mostrarla 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 está habilitado 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:

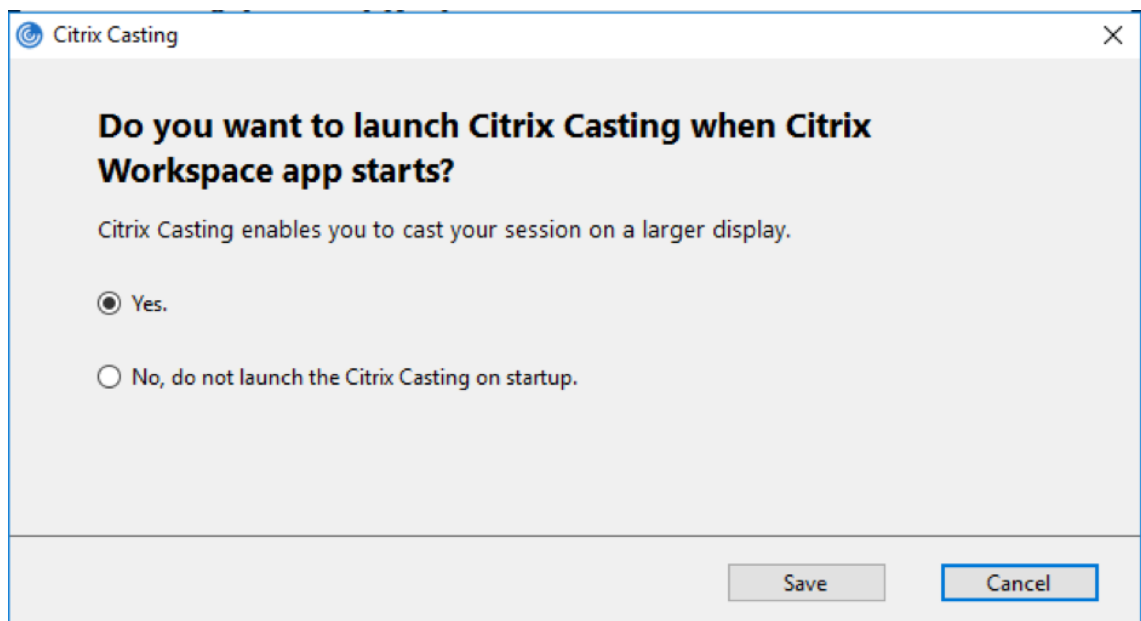
Puede ocultar toda o parte de la hoja Preferencias avanzadas. Para obtener más información, consulte [Hoja de Preferencias avanzadas](#).

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.

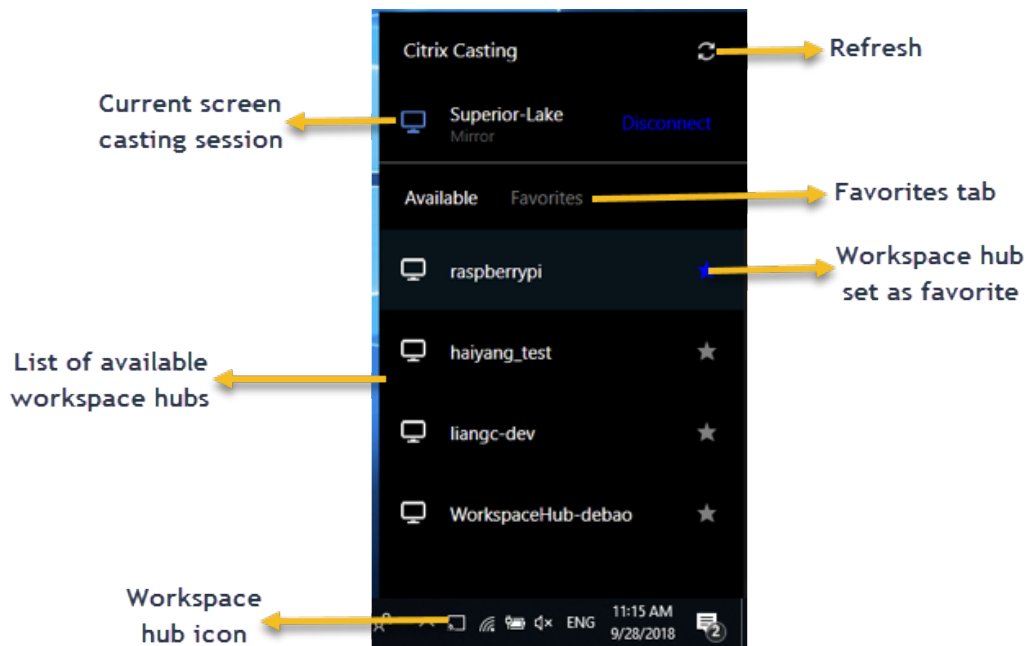
**Nota:**

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](http://<hub_ip>:55555/device-details.xml) para comprobar si muestra 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. Si hay problemas de red, es posible que haya demoras 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.

Para obtener más información sobre Citrix Ready Workspace Hub, consulte la sección [Citrix Ready Workspace Hub](#) en la documentación de Citrix Virtual Apps and Desktops.

## Redirección de dispositivos USB compuestos

USB 2.1 y versiones posteriores admiten la noción de dispositivos USB compuestos donde varios dispositivos secundarios comparten una única conexión con el mismo bus USB. Estos dispositivos emplean un solo espacio de configuración y una conexión de bus compartida, donde se usa un número de interfaz único 00-ff para identificar cada dispositivo secundario. Estos dispositivos no son lo mismo que un concentrador USB que proporciona un nuevo origen de bus USB para otros dispositivos USB con direcciones independientes para la conexión.

Los dispositivos compuestos encontrados en el dispositivo de punto final cliente se pueden reenviar al host virtual como una de estas dos opciones:

- Un solo dispositivo USB compuesto
- Un conjunto de dispositivos secundarios independientes (dispositivos divididos)

Cuando se reenvía un dispositivo USB compuesto, todo el dispositivo deja de estar disponible para el dispositivo de punto final. El reenvío también bloquea el uso local del dispositivo para todas las aplicaciones del dispositivo de punto final, incluido el cliente Citrix Workspace necesario para ofrecer una experiencia remota con HDX optimizado.

Considere un dispositivo con auriculares USB con dispositivo de audio y un botón HID para el control de volumen y silencio. Si todo el dispositivo se reenvía mediante un canal USB genérico, el dispositivo

deja de estar disponible para la redirección por el canal de audio con HDX optimizado. Sin embargo, puede obtener una experiencia óptima cuando el audio se envía a través del canal de audio con HDX optimizado, a diferencia del audio enviado mediante controladores de audio del lado del host a través de la comunicación remota por USB genérico. Este comportamiento se produce porque los protocolos de audio USB suelen provocar ruido.

También nota problemas cuando el teclado del sistema o el dispositivo al que apunta forman parte de un dispositivo compuesto con otras funciones integradas necesarias para admitir sesiones remotas. Cuando se reenvía un dispositivo compuesto completo, el teclado o el mouse del sistema dejan de funcionar en el dispositivo de punto final, excepto en la sesión o la aplicación del escritorio remoto.

Para resolver estos problemas, Citrix recomienda dividir el dispositivo compuesto y reenviar solo las interfaces secundarias que usan un canal USB genérico. Este mecanismo garantiza que los demás dispositivos secundarios estén disponibles para su uso en las aplicaciones del dispositivo de punto final del cliente, incluida la aplicación Citrix Workspace que ofrece experiencias con HDX optimizado, al tiempo que permite que solo los dispositivos requeridos se reenvíen y estén disponibles para la sesión remota.

### **Reglas de dispositivo:**

Al igual que los dispositivos USB normales, las reglas de dispositivo establecidas en la directiva o en la configuración de la aplicación Citrix Workspace del cliente en el dispositivo de punto final seleccionan los dispositivos compuestos para el reenvío. La aplicación Citrix Workspace usa estas reglas para decidir los dispositivos USB para los que permitir o impedir el reenvío a la sesión remota.

Cada regla consta de una palabra clave de acción (Permitir, Conectar o Denegar), dos puntos (:) y cero o más parámetros de filtro que coinciden con dispositivos reales en el subsistema USB de los dispositivos de punto final. Estos parámetros de filtro corresponden a los metadatos descriptores del dispositivo USB que usa cada dispositivo USB para identificarse.

Las reglas de dispositivo son texto no cifrado con cada regla en una sola línea y un comentario opcional precedido de un carácter #. Las reglas se cotejan de arriba a abajo (orden de prioridad descendente). Se aplica la primera regla que coincida con la interfaz del dispositivo o la interfaz secundaria. Se ignoran las reglas subsiguientes que seleccionen el mismo dispositivo o interfaz.

Reglas de dispositivo de ejemplo:

- ALLOW: vid=046D pid=0102 # Permite un dispositivo específico por vid/pid
- ALLOW: vid=0505 class=03 subclass=01 # Permite cualquier pid para el proveedor 0505 cuando subclass=01
- DENY: vid=0850 pid=040C # Deniega un dispositivo específico (incluidos todos los dispositivos secundarios)
- DENY: class=03 subclass=01 prot=01 # Deniega todo dispositivo que coincida con todos los filtros

- CONNECT: vid=0911 pid=0C1C # Permite y se conecta automáticamente a un dispositivo específico
- ALLOW: vid=0286 pid=0101 split=01 # Divide este dispositivo y permite todas las interfaces
- ALLOW: vid=1050 pid=0407 split=01 intf=00,01 # Divide y permite solamente 2 interfaces
- CONNECT: vid=1050 pid=0407 split=01 intf=02 # Divide y se conecta automáticamente a la interfaz 2
- DENY: vid=1050 pid=0407 split=1 intf=03 # Evita que se conecte remotamente a la interfaz 03

Puede usar cualquiera de estos parámetros de filtro para aplicar reglas a los dispositivos detectados:

Parámetro de filtro	Descripción
vid=xxxx	ID de proveedor del dispositivo USB (código hexadecimal de cuatro dígitos)
pid=xxxx	ID de producto del dispositivo USB (código hexadecimal de cuatro dígitos)
rel=xxxx	ID de versión del dispositivo USB (código hexadecimal de cuatro dígitos)
class=xx	Código de clase del dispositivo USB (código hexadecimal de dos dígitos)
subclass=xx	Código de subclase del dispositivo USB (código hexadecimal de dos dígitos)
prot=xx	Código de protocolo del dispositivo USB (código hexadecimal de dos dígitos)
split=1 (o split=0)	Seleccione un dispositivo compuesto que dividir (o no dividir)
intf=xx[,xx,xx,...]	Seleccione un conjunto específico de interfaces secundarias de un dispositivo compuesto (lista separada por comas de códigos hexadecimales de dos dígitos)

Los seis primeros parámetros seleccionan los dispositivos USB a los que se debe aplicar la regla. Si algún parámetro no se especifica, la regla coteja dispositivos con CUALQUIER valor para ese parámetro.

El foro de implementadores de USB mantiene una lista de valores definidos de clase, subclase y protocolo en [Defined Class Codes](#). USB-IF también conserva una lista de los ID de proveedores registrados. Puede comprobar los ID de proveedor, producto, versión e interfaz de un dispositivo específico directamente en el administrador de dispositivos de Windows o con una herramienta gratuita como UsbTreeView.

Cuando están presentes, los dos últimos parámetros solo se aplican a dispositivos USB compuestos. El parámetro de división determina si un dispositivo compuesto debe reenviarse como dispositivos divididos o como un solo dispositivo compuesto.

- *Split=1* indica que las interfaces secundarias seleccionadas de un dispositivo compuesto deben reenviarse como dispositivos divididos.
- *Split=0* indica que el dispositivo compuesto no debe dividirse.

**Nota:**

Si el parámetro de división se omite, se presupone que *Split=0*.

El parámetro *intf* selecciona las interfaces secundarias específicas del dispositivo compuesto al que debe aplicarse la acción. Si se omite, la acción se aplica a todas las interfaces del dispositivo compuesto.

Considere un dispositivo compuesto de auriculares USB con tres interfaces:

- Interfaz 0: Dispositivos de punto final de clase audio
- Interfaz 3: Dispositivos de punto final de clase HID (botones de volumen y silencio)
- Interfaz 5: Interfaz de administración/actualización

Las reglas sugeridas para este tipo de dispositivo son:

- CONNECT: vid=047F pid=C039 split=1 intf=03 # Permite y se conecta automáticamente a un dispositivo HID
- DENY: vid=047F pid=C039 split=1 intf=00 # Deniega dispositivos de punto final de audio
- ALLOW: vid=047F pid=C039 split=1 intf=05 # Permite mgmt *intf*, pero no se conecta automáticamente

**Habilitar la directiva de reglas de dispositivo:**

La aplicación Citrix Workspace para Windows incluye un conjunto de reglas de dispositivo predeterminadas que filtra ciertas clases no deseadas de dispositivos y permiten aquellas que los clientes suelen encontrar.

Puede comprobar estas reglas de dispositivo predeterminadas en el Registro del sistema en uno de estos dos lugares:

- `HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\GenericUSB` (Windows de 32 bits)
- `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\ICA Client\GenericUSB` (Windows de 64 bits), en el valor de multcadena **DeviceRules**.

Sin embargo, en la aplicación Citrix Workspace para Windows, puede aplicar la directiva **Reglas de dispositivos USB** para sobrescribir estas reglas predeterminadas.

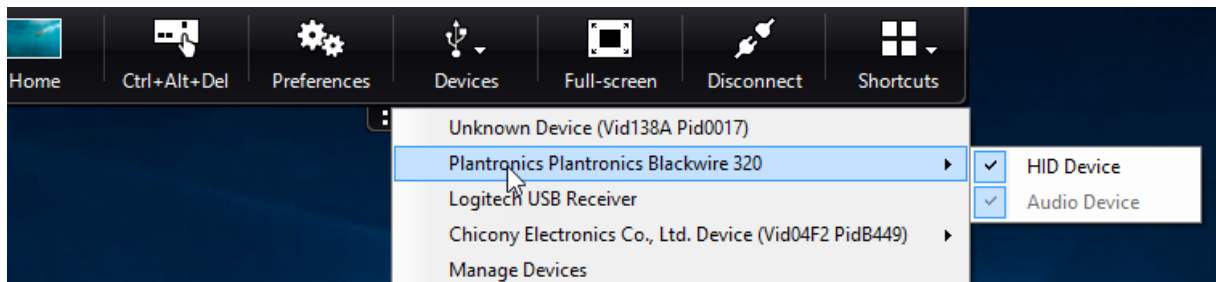
Para habilitar la directiva de reglas de dispositivo para la aplicación Citrix Workspace para Windows:

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 > 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**, pegue (o modifique directamente) las reglas de dispositivos USB que se implementarán.
6. Haga clic en **Aplicar** y **Aceptar**.

Citrix recomienda conservar las reglas predeterminadas que se envían al cliente al crear esta directiva mediante la copia de las reglas originales y la inserción de reglas nuevas para modificar el comportamiento como se quiera.

### Conectar dispositivos USB:

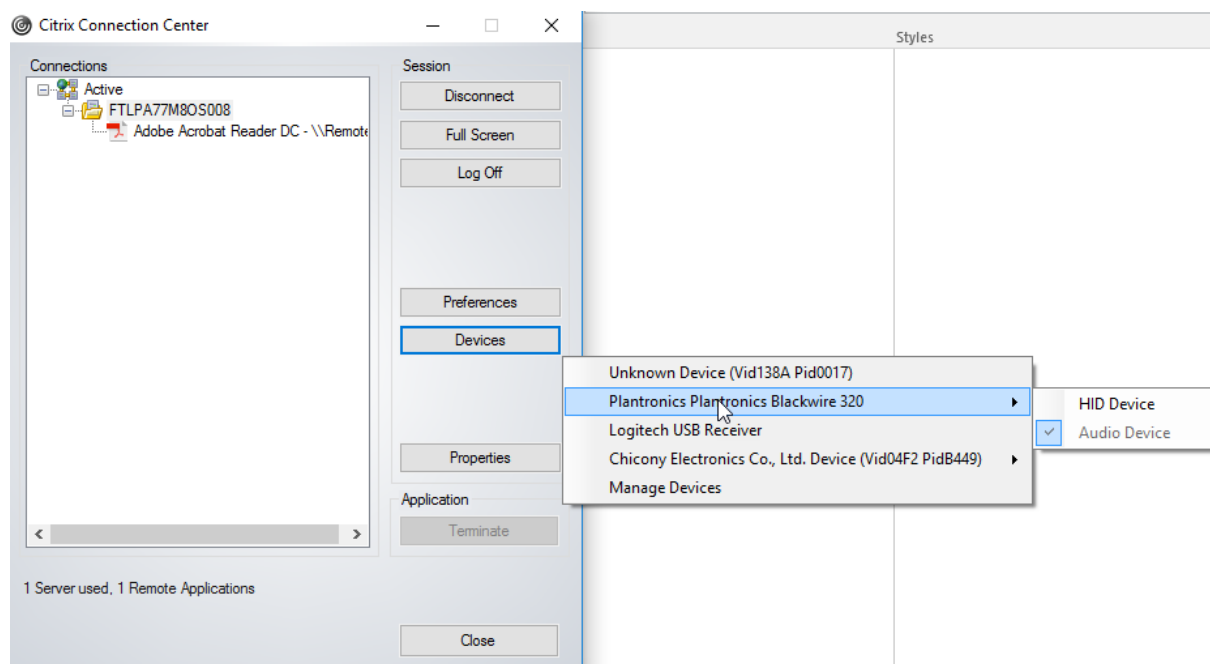
En una sesión de escritorio, los dispositivos USB divididos se muestran en Desktop Viewer, en **Dispositivos**. Además, los dispositivos USB divididos se pueden ver también en **Preferencias > Dispositivos**.



#### Nota:

La palabra clave CONNECT permite la conexión automática de un dispositivo USB. Sin embargo, si la palabra clave CONNECT no se utiliza al dividir un dispositivo USB compuesto para la redirección de USB genérico, debe seleccionar manualmente el dispositivo desde Desktop Viewer o la Central de conexiones para conectar un dispositivo permitido.

En una sesión de aplicación, los dispositivos USB divididos se muestran en la **Central de conexiones**.



### Para conectar automáticamente una interfaz:

La palabra clave CONNECT introducida en la aplicación Citrix Workspace para Windows 2109 permite la redirección automática de dispositivos USB. La regla CONNECT puede reemplazar la regla ALLOW si el administrador permite que el dispositivo o determinadas interfaces se conecten automáticamente en la sesión.

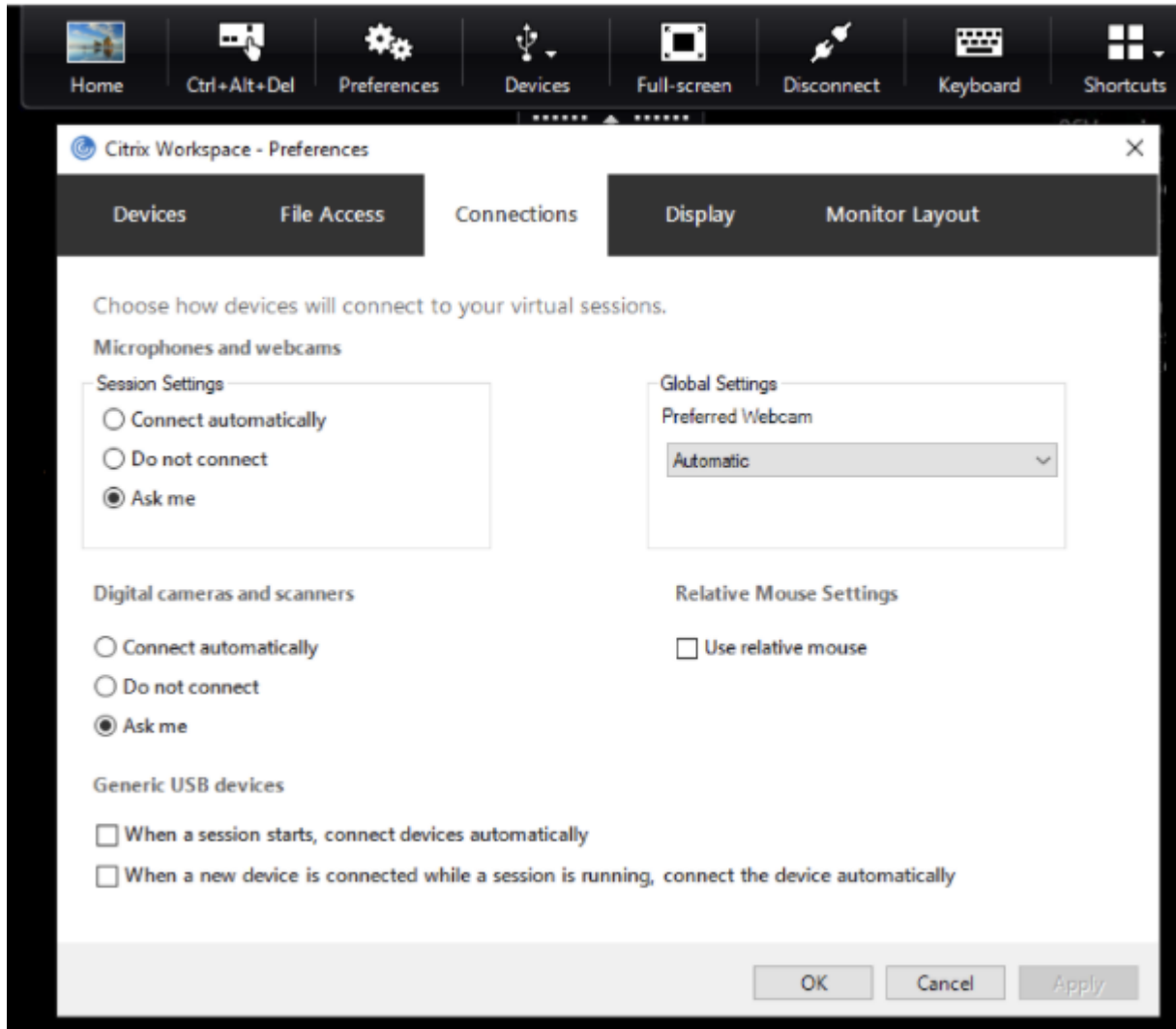
1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del usuario**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Uso remoto de dispositivos cliente > Uso remoto de USB genérico**.
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 que se conecte automáticamente.

Por ejemplo, `CONNECT: vid=047F pid=C039 split=01 intf=00,03:` permite dividir un dispositivo compuesto, la conexión automática de las interfaces 00 y 03, y la restricción de otras interfaces de ese dispositivo.

6. Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.

### Cambiar las preferencias de la conexión automática de los dispositivos USB:

La aplicación Citrix Workspace conecta automáticamente dispositivos USB etiquetados con la acción CONNECT en función de las preferencias establecidas para el recurso de escritorio actual. Puede cambiar las preferencias en la barra de herramientas de **Desktop Viewer**, como se muestra en la siguiente imagen.



Las dos casillas situadas en la parte inferior del panel controlan si los dispositivos deben conectarse automáticamente o esperar conexiones manuales en la sesión. Estos parámetros no están habilitados de forma predeterminada. Puede cambiar las preferencias si los dispositivos USB genéricos deben conectarse automáticamente.

Como alternativa, para invalidar las preferencias de usuario, un administrador puede implementar las directivas correspondientes desde la plantilla administrativa de objetos de directiva de grupo de la aplicación Citrix Workspace. Las directivas de usuario y máquina se pueden encontrar en **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Uso remoto de dispositivos cliente > Uso remoto de USB genérico**. Las directivas correspondientes se etiquetan como Dispositivos USB existentes y Dispositivos USB nuevos, respectivamente.



### **Cambiar la configuración predeterminada de dispositivos divididos:**

De forma predeterminada, la aplicación Citrix Workspace para Windows solo divide dispositivos compuestos que se etiquetan explícitamente como *Split=1* en las reglas de dispositivo. Sin embargo, puede cambiar la disposición predeterminada para dividir todos los dispositivos compuestos que no están etiquetados con *Split=0* en una regla de dispositivo correspondiente.

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.

#### **Nota:**

Citrix recomienda usar reglas de dispositivo explícitas para identificar dispositivos o interfaces específicos que deben dividirse en lugar de cambiar el valor predeterminado. Esta configuración se retirará en una versión futura.

### **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.

### **Teclados Bloomberg**

La aplicación Citrix Workspace admite el uso de teclados Bloomberg en una sesión de Citrix Virtual Apps and Desktops. 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.

Los teclados Bloomberg ofrecen mejor funcionalidad en comparación con los teclados estándar, lo que permite a los usuarios acceder a datos del mercado financiero y realizar transacciones bursátiles.

El teclado Bloomberg consta de varios dispositivos USB integrados en una shell física:

- El teclado
- Un lector de huellas dactilares
- Un dispositivo de audio

- Un concentrador USB para conectar todos estos dispositivos al sistema
- Botones HID, como, por ejemplo, Silenciar, Más volumen y Menos volumen, del dispositivo de audio

Además de la funcionalidad normal de estos dispositivos, el dispositivo de audio permite el uso de algunas teclas, el control del teclado y los LED del teclado.

Para usar la funcionalidad especializada dentro de una sesión, debe redirigir el dispositivo de audio como dispositivo USB. Esta redirección hace que el dispositivo de audio esté disponible para la sesión, pero impide que el dispositivo de audio se utilice localmente. Además, la funcionalidad especializada solo puede utilizarse con una sesión y no se puede compartir entre varias sesiones.

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

### **Para configurar teclados Bloomberg 5:**

Debe configurar varias interfaces del teclado Bloomberg. Desde la aplicación Citrix Workspace para Windows 2109, se presenta una nueva palabra clave CONNECT para permitir la conexión automática de dispositivos USB al iniciar las sesiones y al insertar dispositivos. La palabra clave CONNECT se puede usar para reemplazar la palabra clave ALLOW cuando el usuario quiera que una interfaz o un dispositivo USB se conecten automáticamente. En este ejemplo se utiliza la palabra clave CONNECT.

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 > Uso remoto de dispositivos cliente > Uso remoto de USB genérico**.
3. Seleccione la directiva **Dividir dispositivos**.
4. Seleccione **Habilitada**.
5. En el cuadro de texto **Reglas de dispositivos USB**, agregue estas reglas si no existen.
  - CONNECT: vid=1188 pid=A101 # Módulo biométrico de Bloomberg 5
  - DENY: vid=1188 pid=A001 split=01 intf=00 # Teclado principal Bloomberg 5
  - CONNECT: vid=1188 pid=A001 split=01 intf=01 # HID del teclado Bloomberg 5
  - DENY: vid=1188 pid=A301 split=01 intf=02 # Canal de audio del teclado Bloomberg 5
  - CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # HID del audio del teclado Bloomberg 5

#### **Nota:**

Se pueden utilizar IIRC, líneas nuevas o punto y coma para separar reglas, lo cual permite leer valores del Registro de una línea o de varias líneas.

6. Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.

7. En la ventana **Preferencias**, seleccione la ficha **Conexiones** y después marque una o ambas casillas para conectar los dispositivos automáticamente. Se puede acceder a la ventana **Preferencias** desde la barra de herramientas del escritorio o desde el administrador de conexiones.

Este procedimiento deja el teclado Bloomberg 5 listo para su uso. Las reglas DENY mencionadas en los pasos aplican la redirección del teclado principal y del canal de audio a través de un canal optimizado, pero no de USB genérico. Las reglas CONNECT permiten la redirección automática del módulo de huella digital, las teclas especiales en el teclado y las teclas relacionadas con el control de audio.

### Configurar teclados Bloomberg 4 o 3:

#### 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.

1. Busque las siguientes claves 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.

La funcionalidad para teclados Bloomberg 3 está disponible en el Online Plug-in 11.2 para Windows y versiones posteriores.

La funcionalidad para teclados Bloomberg 4 está disponible para Receiver para Windows 4.8 y versiones posteriores.

### Determinar si la funcionalidad para teclados Bloomberg está habilitada:

- Para comprobar si la funcionalidad para teclados Bloomberg está habilitada en el Online Plug-in, compruebe los informes que genera Desktop Viewer sobre dispositivos de teclado Bloomberg. Si Desktop Viewer no se usa, puede comprobar el Registro en la máquina donde se ejecuta el Online Plug-in.
- Si la funcionalidad para teclados Bloomberg no está habilitada, Desktop Viewer muestra:
  - Dos dispositivos para el teclado Bloomberg 3, que aparece como **Bloomberg Fingerprint Scanner** y **Bloomberg Keyboard Audio**.
  - Un dispositivo redirigido por directiva para el teclado Bloomberg 4. Este dispositivo aparece como **Bloomberg LP Keyboard 2013**.

- Si la funcionalidad para teclados Bloomberg está habilitada, se muestran dos dispositivos en Desktop Viewer. Uno aparece como **Bloomberg Fingerprint Scanner** como antes y el otro como **Bloomberg Keyboard Features**.
- Si el controlador del dispositivo Bloomberg Fingerprint Scanner no está instalado, es posible que la entrada Bloomberg Fingerprint Scanner no aparezca en Desktop Viewer. Si falta la entrada, es posible que Bloomberg Fingerprint Scanner no esté disponible para la redirección. Sigue pudiendo comprobar el nombre del otro dispositivo Bloomberg donde está habilitada la funcionalidad para teclados Bloomberg.
- También puede comprobar el valor en el Registro para saber si la funcionalidad está habilitada:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB\EnableBloombergHID`

Si el valor no existe o es 0 (cero), no se habilita la funcionalidad para teclados Bloomberg. Si el valor es 1, sí se habilita.

### Para habilitar el teclado Bloomberg:

#### Nota:

Citrix Receiver para Windows 4.8 incorporó la compatibilidad con dispositivos compuestos a través de la directiva **Dividir dispositivos**. Sin embargo, para el teclado Bloomberg 4, debe usar la función de teclado Bloomberg en lugar de esta directiva.

La funcionalidad para teclados Bloomberg cambia el modo en que determinados dispositivos USB se redirigen a una sesión. Esta funcionalidad no está habilitada de forma predeterminada.

- Para habilitarla durante la instalación, especifique el valor de la propiedad **ENABLE\_HID\_REDIRECTION** en TRUE en la línea de comandos de instalación. Por ejemplo:

```
CitrixOnlinePluginFull.exe /silent
ADDLOCAL="ICA_CLIENT,PN_AGENT,SSON,USB"
ENABLE_SSON="no"INSTALLDIR="c:\test"
ENABLE_DYNAMIC_CLIENT_NAME="Yes"
DEFAULT_NDSCONTEXT="Context1,Context2"
SERVER_LOCATION="http://testserver.net"ENABLE_HID_REDIRECTION="
TRUE"
```

- Para habilitarla después de instalar el Online Plug-in, modifique el Registro de Windows en el sistema donde se ejecuta el Online Plug-in:
  1. Abra el Editor del Registro.
  2. Vaya a esta clave:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
  3. Si el valor **EnableBloombergHID** existe, modifíquelo para que los datos del valor sean 1.

4. Si el valor **EnableBloombergHID** no existe, cree un valor DWORD con el nombre EnableBloombergHID e indique 1 como datos del valor.

### **Inhabilitar la funcionalidad para el teclado Bloomberg:**

Puede inhabilitar la funcionalidad para teclados Bloomberg en el Online Plug-in de este modo:

1. Abra el Editor del Registro en el sistema donde se ejecuta el software de Online Plug-in.
2. Vaya a esta clave:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
3. Si el valor **EnableBloombergHID** existe, modifíquelo para que los datos del valor sean 0 (cero).

Si el valor **EnableBloombergHID** no existe, indica que la funcionalidad para teclados Bloomberg no está habilitada. En tales casos, no tiene que modificar ningún valor del Registro.

### **Usar teclados Bloomberg sin habilitar la funcionalidad:**

- Puede usar el teclado sin habilitar la funcionalidad para teclados Bloomberg en el Online Plug-in. Sin embargo, no se puede beneficiar del uso compartido de la funcionalidad especializada en varias sesiones y es posible que disponga de un mayor ancho de banda de red para el audio.
- Las teclas normales del teclado Bloomberg están disponibles del mismo modo que cualquier otro teclado. No necesita tomar ninguna acción especial.
- Para usar las teclas Bloomberg especializadas, debe redirigir el dispositivo de audio del teclado Bloomberg a la sesión. Si utiliza Desktop Viewer, aparece el nombre del fabricante y el nombre del dispositivo de los dispositivos USB, y aparece **Bloomberg Keyboard Audio** para el dispositivo de audio del teclado Bloomberg.
- Para usar el lector de huellas digitales, debe redirigir el dispositivo a Bloomberg Fingerprint Scanner. Si los controladores del lector de huellas digitales no están instalados localmente, el dispositivo solo muestra una de estas opciones:
  - Si el Online Plug-in está configurado para conectar dispositivos automáticamente.
  - Permitir al usuario elegir si quiere conectar dispositivos.

Además, si el teclado Bloomberg se conecta antes de establecer la sesión y los controladores del lector de huellas digitales no existen localmente, el lector de huellas digitales no se muestra y no se puede usar dentro de la sesión.

#### **Nota:**

Para Bloomberg 3, una sola sesión o el sistema local puede usar el lector de huellas dactilares y no se puede compartir. La redirección está prohibida en Bloomberg 4.

### **Usar teclados Bloomberg después de habilitar la funcionalidad:**

- Si habilita la funcionalidad para teclados Bloomberg en el Online Plug-in, tiene la ventaja de compartir la funcionalidad especializada del teclado con varias sesiones. También dispone de menos ancho de banda de red para el audio.
- Habilitar la funcionalidad para teclados Bloomberg impide la redirección del dispositivo Bloomberg Keyboard Audio. En vez de ello, un nuevo dispositivo está disponible. Si utiliza Desktop Viewer, este dispositivo se denomina Bloomberg Keyboard Features. La redirección de este dispositivo proporciona las teclas Bloomberg especializadas a la sesión.

Habilitar la funcionalidad para teclados Bloomberg solo afecta a las teclas Bloomberg especializadas y al dispositivo de audio. Esto es porque las teclas normales y el lector de huellas digitales se utilizan de la misma manera que cuando la funcionalidad no está habilitada.

## 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. El escalado de la sesión sigue la resolución del sistema operativo.

Puede configurar el escalado de PPP mediante las siguientes opciones:

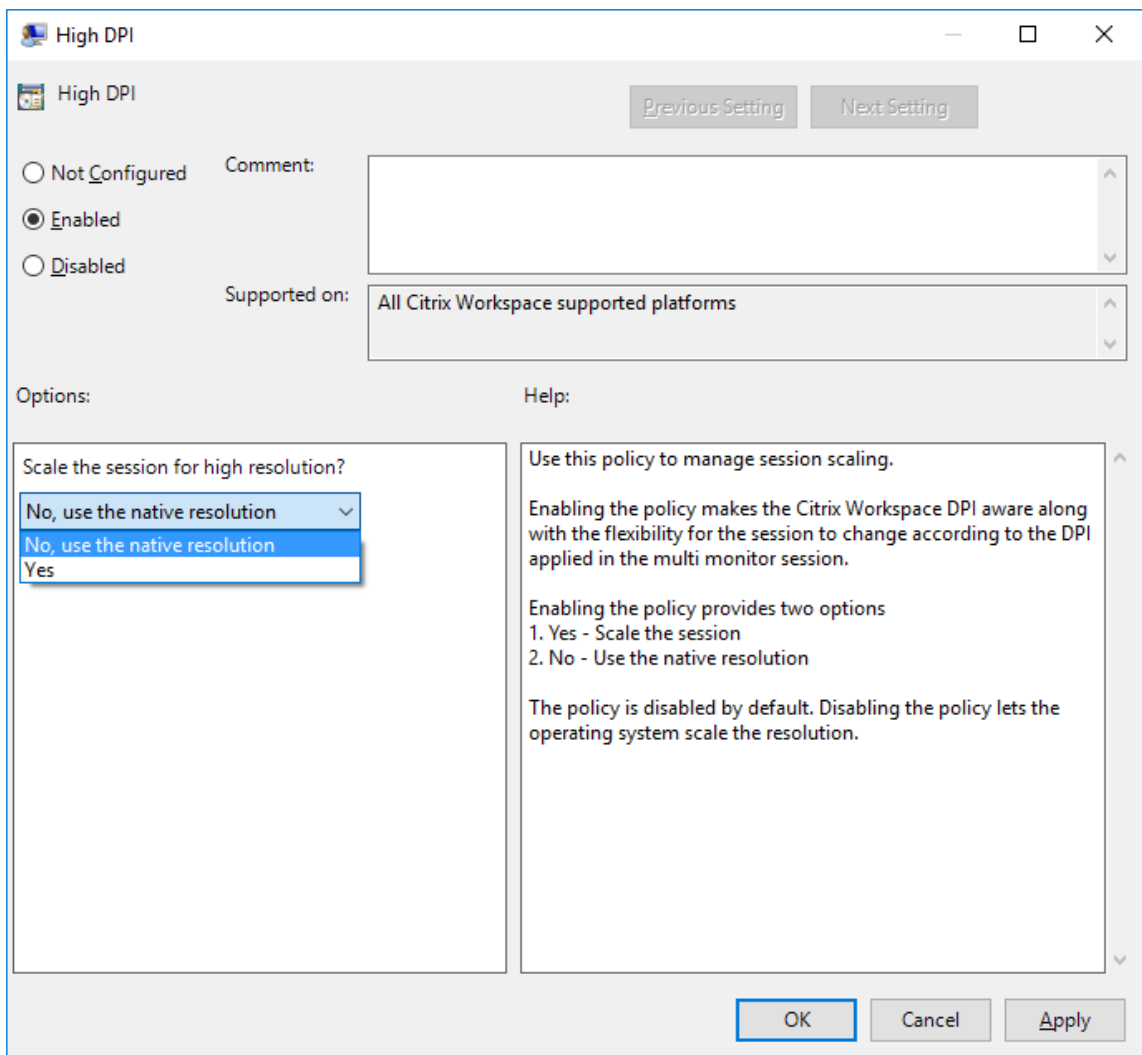
1. Plantilla administrativa de objetos de directiva de grupo (GPO) (configuración por máquina)
2. Preferencias avanzadas (configuración por usuario)

### 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: Indica que se aplica un PPP elevado en una sesión.
- b) No, usar la resolución nativa: Indica que 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.

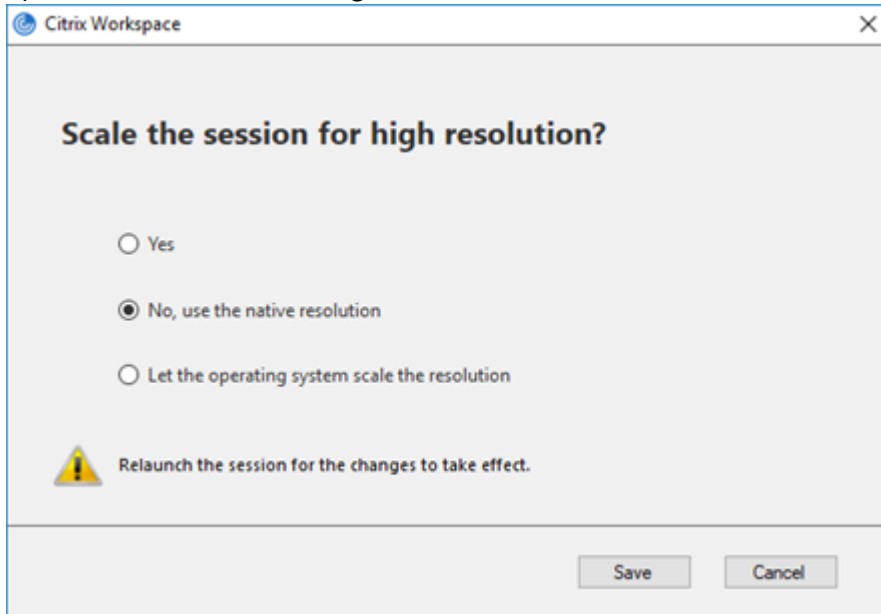
### Configurar el escalado de PPP mediante la interfaz gráfica de usuario:

#### Nota:

Puede ocultar toda o parte de la hoja Preferencias avanzadas. 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: Indica que se aplica un PPP elevado 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. El parámetro de escalado



corresponde al parámetro **Sí** de la interfaz de usuario, o la directiva de PPP elevados habilitada en la directiva de GPO. El parámetro **Sí** de la interfaz de usuario funciona bien en casos de PPP mixtos al conectarse a VDA modernos y permite 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). Es posible las API de Acceso a aplicaciones locales, RTOP y otros plug-ins que utilizan posicionamiento de pantalla no sean compatibles 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. El parámetro Sin escalar corresponde al parámetro **No** de la interfaz de usuario y la directiva de PPP elevados habilitada en el objeto de directiva de grupo (GPO). El parámetro **No** de la IU 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. Sin embargo, este parámetro 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. Según este parámetro, el sistema operativo Windows gestiona el escalado de PPP de 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 desenfoque 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.

Citrix recomienda este parámetro para usuarios de dispositivos de punto final con Windows 7 y para aquellos que se conectan a VDA antiguos. También se puede usar en Windows 10 si no hay PPP mixtos.

## Distribución de pantallas virtuales

Esta función le permite definir una distribución de monitores virtuales para el escritorio remoto. También puede dividir un único monitor de cliente virtualmente en un máximo de ocho monitores en el escritorio remoto. Puede configurar los monitores virtuales en la ficha **Diseño del monitor** en Desktop Viewer. Allí, puede dibujar líneas horizontales o verticales para separar la pantalla en monitores virtuales. La pantalla se divide según el porcentaje especificado en la resolución del monitor de 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.

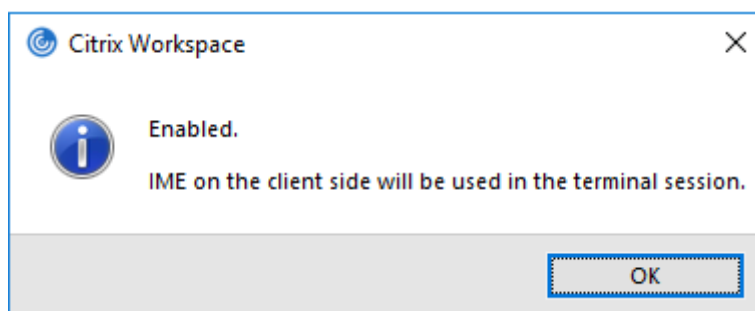
## Editores IME de cliente genérico

### Nota:

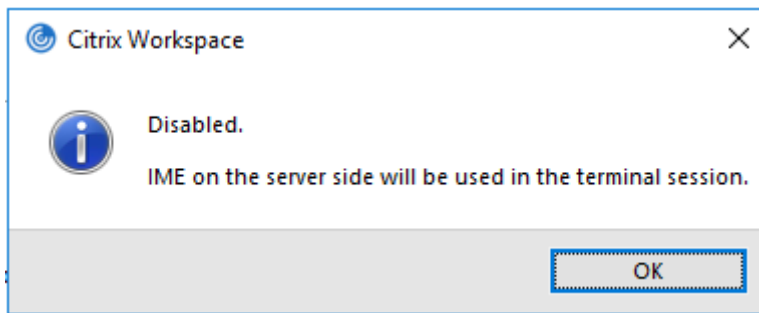
Si utiliza un sistema operativo Windows 10, versión 2004, es posible que tenga problemas técnicos al usar la función IME en una sesión. Esos problemas son el resultado de una limitación de terceros. Para obtener más información, consulte el [artículo de asistencia de Microsoft](#).

### 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`.



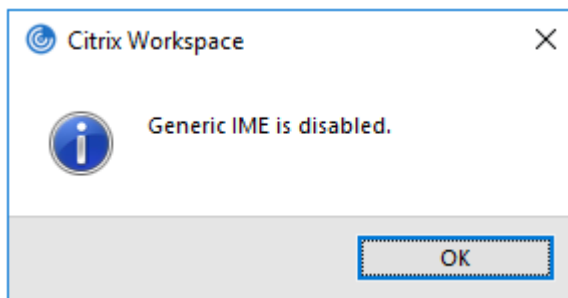
- Para inhabilitar el IME de cliente genérico, ejecute el comando `wfica32.exe /localime:off` desde la carpeta de instalación de la aplicación Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`.



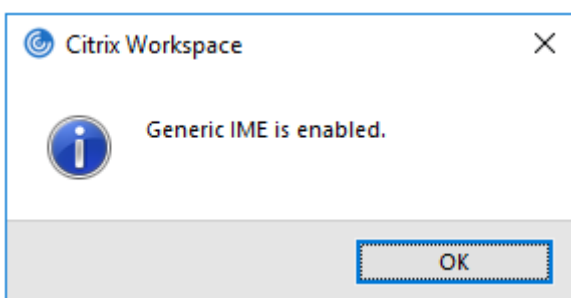
**Nota:**

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 del 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.

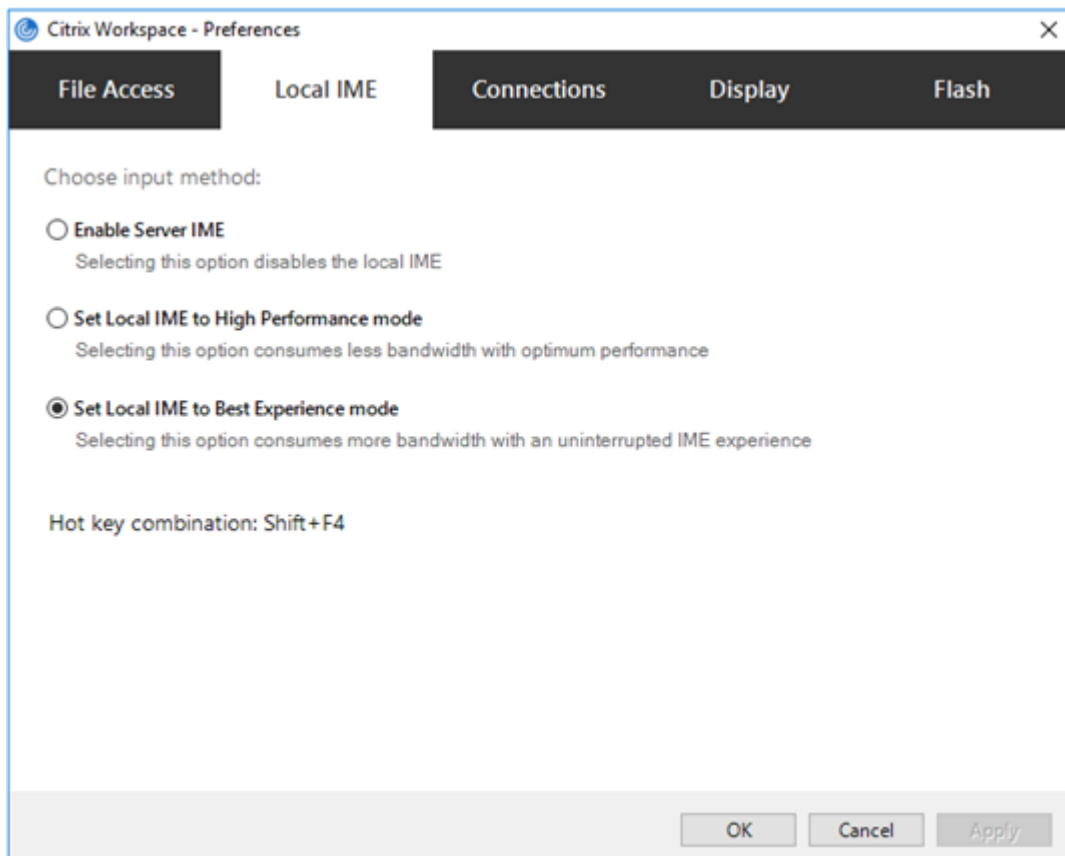
### Configurar el IME de cliente genérico mediante la interfaz gráfica de usuario:

El IME de cliente genérico requiere el VDA 7.13 o una versión más reciente.

Para habilitar las funciones de IME de cliente genérico, se puede habilitar 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. 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.

Los cambios solo se aplican a 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_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Key`.

Seleccione **AllowHotKey** y cambie el valor predeterminado a 1.

Puede utilizar las teclas de acceso rápido **Mayúsc+F4** para seleccionar diferentes modos de IME en las sesiones.

Las diferentes opciones de los modos de IME aparecen en la esquina superior derecha de la sesión al usar este atajo.



#### **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 inhabilitarlo, 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. Es necesario que se admita el códec de vídeo H.265 y que esté habilitado tanto en el VDA como en la aplicación Citrix Workspace. Si la GPU del dispositivo de 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 la 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 le permite cambiar entre distintas distribuciones de teclado preferidas en el dispositivo cliente. Esta función está inhabilitada de forma predeterminada. La sincronización de la distribución del teclado permite que la distribución del teclado del cliente se sincronice automáticamente con la sesión de aplicaciones y escritorios virtuales.

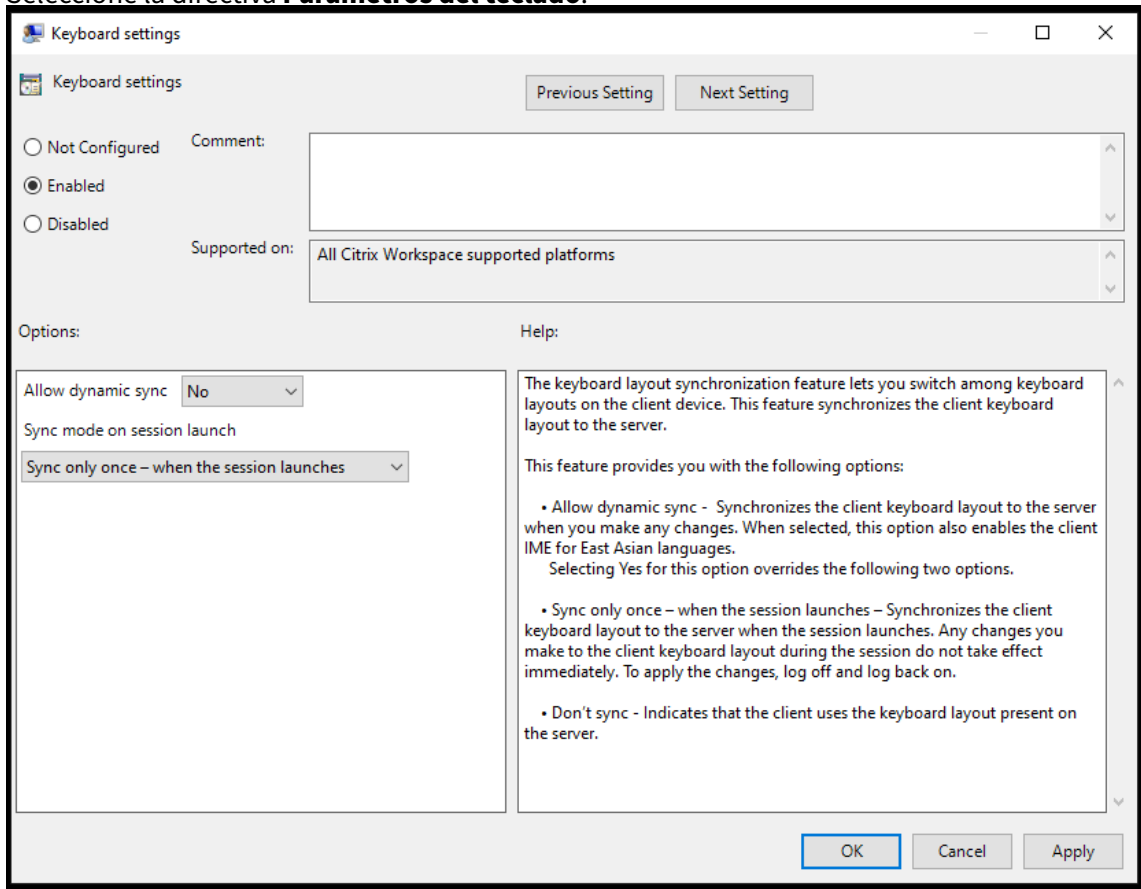
### Para configurar la sincronización de la distribución del teclado mediante la plantilla administrativa de GPO:

**Nota:**

La configuración de GPO tiene prioridad sobre las configuraciones de StoreFront y de la GUI.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. En los nodos **Configuración del equipo** o **Configuración del usuario**, vaya a **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Workspace > Experiencia de usuario**.

3. Seleccione la directiva **Parámetros del teclado**.



4. **Habilítela** y seleccione una de estas opciones:

- **Permitir sincronización dinámica:** En el menú desplegable, seleccione **Sí** o **No**. Esta opción sincroniza la distribución del teclado del cliente con el servidor al cambiar la distribución del teclado del cliente. Al seleccionar esta opción, también se habilita el editor IME del cliente para idiomas de Asia Oriental.

Al seleccionar **Sí** para esta opción, se anulan las dos opciones siguientes.

- **Modo de sincronización al iniciar la sesión:** En el menú desplegable, seleccione una de estas opciones:
  - **Sincronizar solo una vez: cuando se inicia la sesión:** Sincroniza la distribución del teclado del cliente con la del servidor cuando se inicia la sesión. Los cambios que haga en la distribución del teclado del cliente durante la sesión no surtirán efecto inmediatamente. Para aplicar los cambios, cierre la sesión y vuelva a iniciarla.
  - **No sincronizar:** Indica que el cliente utiliza la distribución del teclado presente en el servidor.

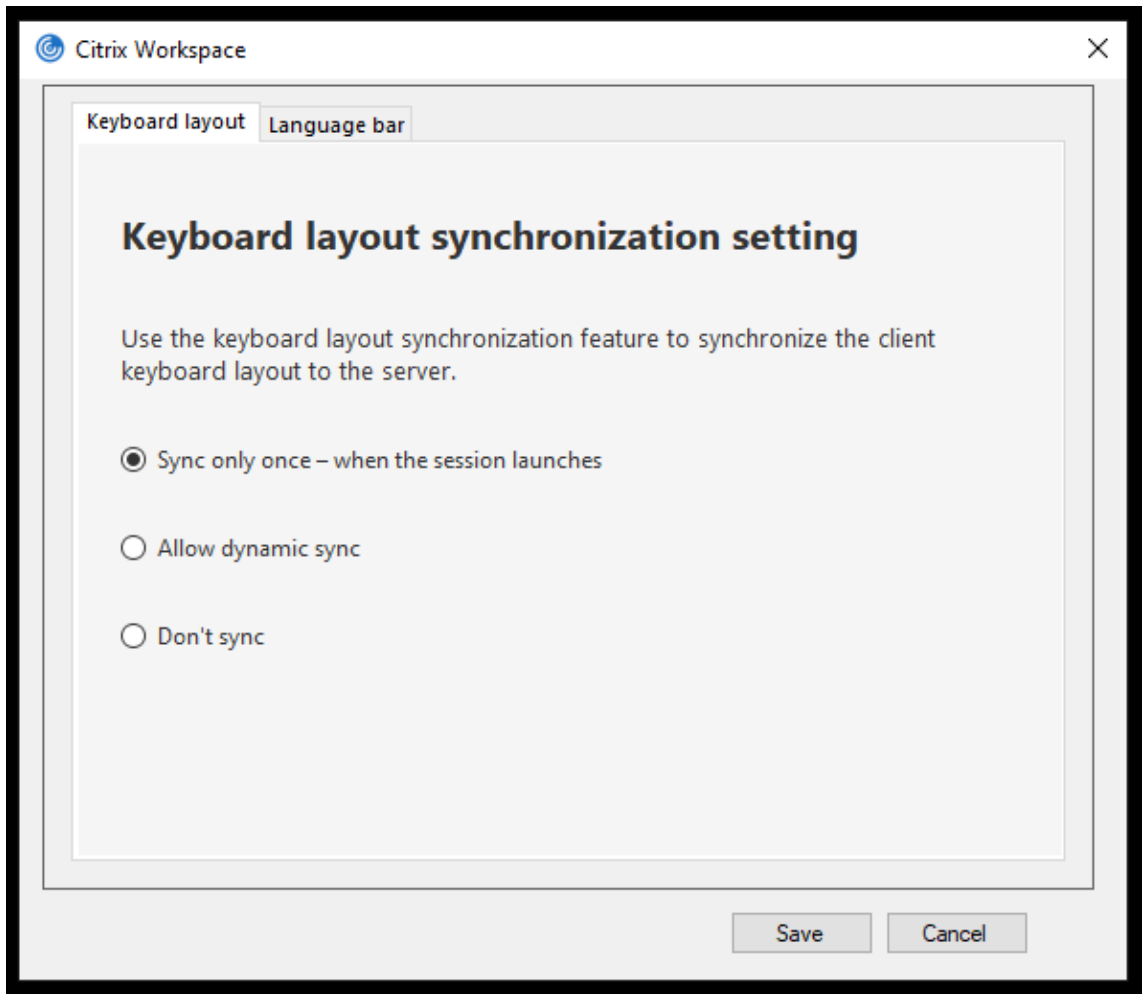
5. Seleccione **Aplicar** y **Aceptar**.

**Para configurar la sincronización de la distribución del teclado mediante la interfaz gráfica de usuario:**



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:

- **Sincronizar solo una vez: cuando se inicia la sesión:** Indica que la distribución del teclado se sincroniza desde el VDA solo una vez al iniciarse la sesión.
- **Permitir sincronización dinámica:** Indica que la distribución del teclado se sincroniza de manera dinámica con el VDA al cambiar el teclado del cliente en una sesión.
- **No sincronizar:** Indica que el cliente usa la distribución del teclado presente en el servidor.

3. Haga clic en **Guardar**.

**Para configurar la sincronización de la distribución del teclado mediante la interfaz de línea de comandos:**

Ejecute este comando desde la carpeta de instalación de la aplicación Citrix Workspace para Windows.

Normalmente, la carpeta de instalación de la aplicación Citrix Workspace se encuentra en `C:\Program files (x86)\Citrix\ICA Client`.

- Para habilitarla: `wfica32.exe /localime:on`
- Para inhabilitarla: `wfica32.exe /localime:off`

La opción de distribución de teclado del cliente activa el editor IME (Input Method Editor) del cliente. Si los usuarios que trabajan en japonés, chino o coreano prefieren usar el editor IME del servidor, deben inhabilitar la opción de distribución del teclado del cliente. Para ello, deben seleccionar **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.

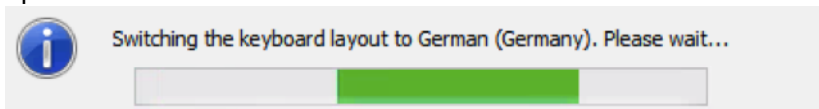
### Configurar la sincronización del teclado en Windows VDA

#### Nota:

Este procedimiento solo se aplica a Windows Server 2016 y versiones posteriores. En Windows Server 2012 R2 y versiones anteriores, la función de sincronización del teclado está habilitada de forma predeterminada.

1. Abra el Editor del Registro y vaya a `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Cree la entrada DWORD `DisableKeyboardSync` y establezca su valor en 0.  
1 inhabilita la función de sincronización de distribución del teclado.
3. Inicie la sesión de nuevo para que los cambios surtan efecto.

Una vez habilitada la distribución del teclado tanto en el VDA como en la aplicación Citrix Workspace, aparece esta ventana al cambiar de distribución del teclado.



Esta ventana indica que la distribución del teclado de la sesión se va a cambiar a la distribución del teclado del cliente.

### Configurar la sincronización del teclado en Linux VDA

Inicie el símbolo del sistema y ejecute este comando:

```
1 /opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\
 CurrentControlSet\Control\Citrix\LanguageBar" -v "SyncKeyboardLayout
 " -d "0x00000001"
2 <!--NeedCopy-->
```

Reinicie el VDA para que los cambios surtan efecto.

Para obtener más información sobre la función de sincronización de distribución del teclado en Linux VDA, consulte [Sincronización de la distribución de teclado dinámico](#).

### 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. Use el Editor del Registro 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 del teclado en el cliente por una distribución que no es compatible en el servidor, la función de sincronización de la distribución del teclado se inhabilita por motivos de seguridad. Una distribución de teclado no reconocida se considera una amenaza potencial para la 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** + **Shift**. Como solución temporal, use la barra de idioma en la sesión RDP para cambiar la distribución del teclado.

## Barra de idioma

La barra de idioma muestra el idioma de entrada preferido en una sesión. 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.

### Configurar la barra de idioma mediante la plantilla administrativa de GPO:

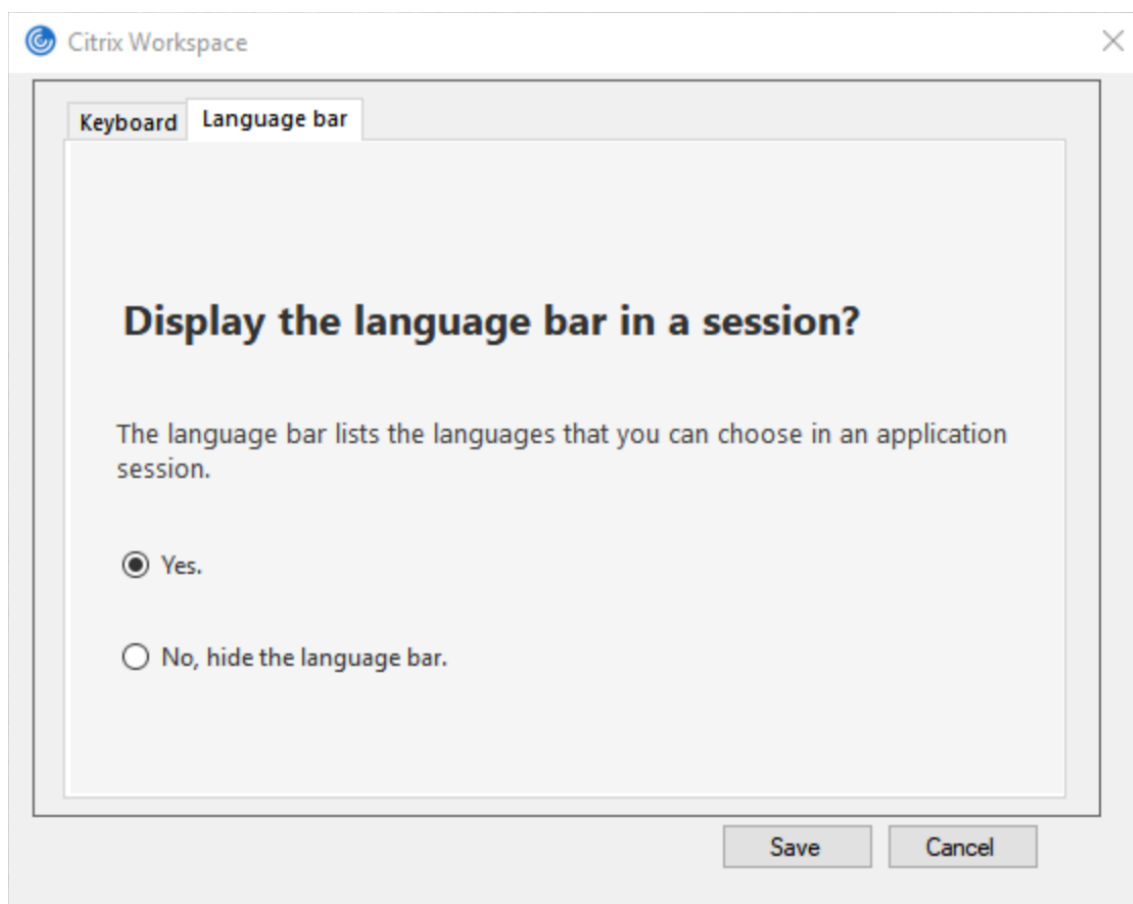
La barra de idioma muestra el idioma de entrada preferido en una sesión de aplicación.

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute `gpedit.msc`.
2. En los nodos **Configuración del equipo** o **Configuración del usuario**, vaya a **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Workspace > Experiencia de usuario**.
3. Seleccione la directiva **Barra de idioma**.
4. **Habilítela** y seleccione una de estas opciones:
  - Sí: Indica que la barra de idioma se muestra en la sesión de una aplicación.
  - No, ocultar la barra de idioma: Indica que la barra de idioma se oculta en la sesión de una aplicación.
5. Haga clic en **Aplicar** y **Aceptar**.

### Configurar la barra de idioma mediante la interfaz gráfica de usuario:

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 o alta velocidad. Este entorno permite que estos dispositivos interactúen con paquetes, 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
- Tarjeta NIC integrada
- 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 aplicaciones virtuales:

- Dispositivos Bluetooth
- Tarjeta NIC integrada
- 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 un 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 seleccionar qué dispositivos USB deben conectarse de forma remota al escritorio virtual 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 en el caso de dispositivos de almacenamiento masivo, además de la compatibilidad con USB, el acceso remoto está disponible a través de la asignación de unidades del cliente. Puede configurarlo a través de la directiva de la aplicación Citrix Workspace para Windows **Uso remoto de dispositivos cliente > Asignación de unidades del cliente**. Al aplicar esta directiva, cuando 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

Función	Asignación de unidades del cliente	Compatibilidad con USB
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 habilita las directivas “USB genérico” y “Asignación de unidades del cliente”, e 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 tenerse en cuenta 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 permiten diferentes 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. Dichas clases de dispositivos USB son las siguientes.

- **Audio (clase 01):** Incluye los dispositivos de entrada de audio (micrófonos), los dispositivos de salida de audio y los controladores MIDI. Los dispositivos de audio modernos suelen utilizar transferencias isócronas compatibles con XenDesktop 4 y versiones posteriores. 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. Es posible configurar una cámara para que utilice cualquiera de las clases desde los menús de configuración que proporciona la propia cámara.



**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 escaneo 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 escaneo) 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 de vídeo abarca los dispositivos que se utilizan para manipular vídeo o material relacionado con vídeo. Dispositivos, como cámaras web, videgrabadoras digitales,

convertidores de vídeo analógico, algunos sintonizadores de televisión y algunas cámaras digitales que admiten la transmisión de video por streaming.

### Importante

La mayoría de los dispositivos de transmisión de vídeo por streaming utilizan transferencias isócronas compatibles con XenDesktop 4 y versiones posteriores. 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 reglas de directivas USB predeterminadas no permiten estas clases diferentes de dispositivos USB:

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

- Concentradores USB (clase 09). Los concentradores USB permiten conectar dispositivos adicionales al equipo local. No es necesario acceder a estos dispositivos de forma remota.
- Tarjeta inteligente (clase 0b). Los lectores de 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 importante o conecten periféricos importantes, como mouse o teclados Bluetooth.

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

- **Varios dispositivos de red (clase ef, subclase 04):** Es posible que algunos de estos dispositivos ofrezcan un acceso peligroso a la red. La directiva USB predeterminada no permite estos dispositivos. No obstante, es posible que, en el caso de dispositivos particulares, sea apropiado proporcionar acceso al uso de USB.

### Actualizar la lista de dispositivos USB disponibles para la comunicación remota

Modifique el archivo de plantilla de Citrix Workspace para Windows para actualizar el rango de dispositivos USB disponibles para la comunicación remota con los escritorios. Esta actualización le permite realizar cambios en la aplicación Citrix Workspace para Windows mediante directivas de grupo. El archivo se halla en esta carpeta de instalación:

`\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. Use el Editor del Registro 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](#). Para la actualización de versiones, los parámetros existentes se conservan 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 este comando  
`gpupdate /force:`

## Iniciar vPrefer

En versiones anteriores, puede 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=application` en **Citrix Studio**.

A partir de la versión 4.11, en casos de doble salto (en los que la aplicación Citrix Workspace se ejecuta en el VDA que aloja la sesión), ya puede controlar si la aplicación Citrix Workspace inicia:

- La instancia local de una aplicación instalada en el VDA (si está disponible como aplicación local)
- O 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. 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 en el VDA, la aplicación Citrix Workspace inicia la aplicación alojada. Para obtener más información sobre cómo StoreFront gestionaba el inicio local, 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](#). Para la actualización de versiones, los parámetros existentes se conservan 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**.
5. En la lista desplegable **Permitir aplicaciones**, seleccione una de estas 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, WordPad y el símbolo del sistema. A continuación, inicia la aplicación en el VDA en lugar de iniciarla en 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 y la Calculadora.
  - **Permitir aplicaciones de red:** Esta opción inicia la instancia de una aplicación que esté publicada en una red compartida.
6. Haga clic en **Aplicar** y **Aceptar**.

7. Inicie la sesión de nuevo para que los cambios surtan efecto.

**Limitación:**

- Workspace para Web no admite esta función.

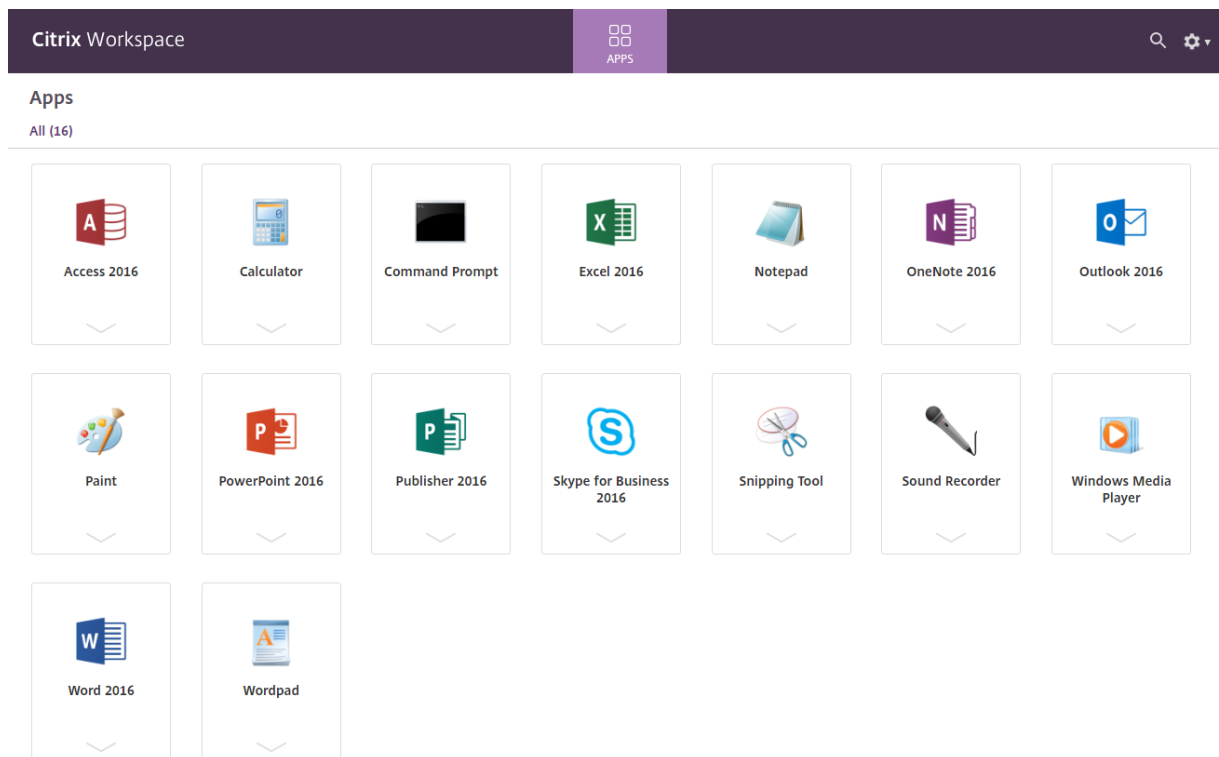
**Configuración de Workspace**

La aplicación Citrix Workspace para Windows admite la configuración de Workspace para los suscriptores, que pueden estar usando uno o varios servicios disponibles en Citrix Cloud.

La aplicación Citrix Workspace muestra de forma inteligente solamente 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 proteger la red de la organización y los dispositivos de los usuarios finales frente al malware y las filtraciones de datos. Para ello, los administradores filtran el acceso a sitios web y categorías de sitios web específicos.

La aplicación Citrix Workspace para Windows admite el uso de aplicaciones SaaS con Citrix Secure Private Access. 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.

La aplicación Citrix Workspace inicia las aplicaciones SaaS en Citrix Enterprise Browser (antes denominado Citrix Workspace Browser). Para obtener información, consulte la documentación de [Citrix Enterprise Browser](#).

### Limitaciones:

1. Cuando inicia una aplicación publicada con la opción de impresión habilitada y la descarga inhabilitada, y emite un comando de impresión en una aplicación iniciada, aún puede guardar el PDF. 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

La aplicación Citrix Workspace para Windows admite la impresión de documentos PDF durante las sesiones. El controlador de impresora universal PDF de Citrix (o Citrix PDF Universal Printer) permite imprimir documentos abiertos con aplicaciones alojadas o aplicaciones ejecutadas en Citrix Virtual Apps and Desktops y Citrix DaaS.

Cuando un usuario selecciona la opción **Citrix PDF Printer** en el cuadro de diálogo **Print**, el controlador convierte el archivo a documento PDF y lo transfiere al dispositivo local. El PDF se abre con el visor de PDF predeterminado para consultarlo y se imprime en una impresora conectada localmente.

Citrix recomienda el explorador Google Chrome o Adobe Acrobat Reader para ver documentos PDF.

Puede habilitar la impresión de PDF de Citrix mediante Citrix Studio en el Delivery Controller.

#### **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. Habilite la directiva **Crear automáticamente la impresora universal de PDF**.

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.

En un dispositivo cliente con función táctil, el VDA de Windows 10 detecta la presencia de un teclado o un mouse 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 incluye un 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 un PC con teclado y mouse.

**Nota:**

Workspace para Web no admite la función Windows Continuum.

## Citrix Analytics

La aplicación Citrix Workspace está equipada para transmitir registros de manera segura a Citrix Analytics. Los registros se analizan y almacenan en los servidores de Citrix Analytics cuando está habilitado. Para obtener más información sobre Citrix Analytics, consulte [Citrix Analytics](#).

## Mouse relativo

La función “mouse relativo” determina hasta dónde se ha movido el cursor desde el último fotograma de una ventana o pantalla.

El mouse relativo utiliza las diferencias píxeles entre los movimientos del cursor. Por ejemplo, cuando se cambia la dirección de la cámara mediante controles del cursor, la función registra el cambio. Las aplicaciones también suelen ocultar el cursor del mouse porque la posición del cursor en relación con las coordenadas de la pantalla no es relevante cuando se manipula una escena o un objeto 3D.

El mouse relativo ofrece una opción para interpretar la posición del mouse de un modo relativo en lugar de hacerlo de un modo absoluto. La interpretación es necesaria para las aplicaciones que exigen una entrada de mouse relativo en lugar de absoluto.

Puede configurar la función tanto por usuario como por sesión, lo que proporciona un control más detallado sobre la disponibilidad de la función.

**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.

## 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

- Nombre: Mouse
- Tipo: REG\_SZ
- Valor: 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. Es posible que, si hay diferentes valores, haya 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 “sitename” es el nombre especificado del sitio cuando se creó. Para los clientes de StoreFront, el archivo default.ica suele estar en `C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica`, donde `storename` es el nombre establecido del almacén cuando se creó.
2. Agregue una clave con el nombre RelativeMouse en la sección WFClient. Defina su valor en la misma configuración 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:**

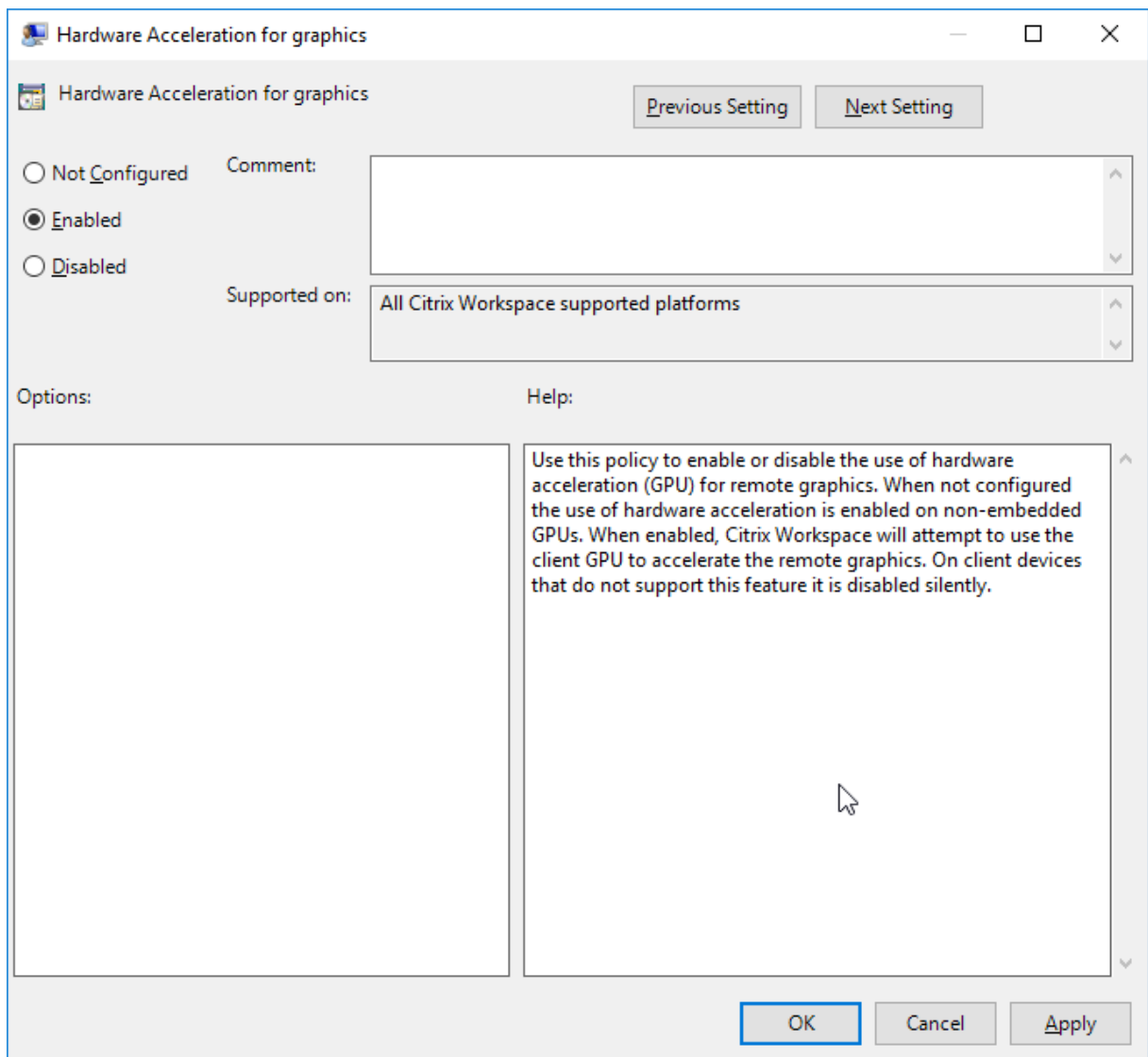
La configuración del mouse relativo desde Desktop Viewer aplica la función solo por sesión.

## **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 está configurada y si se utiliza la aceleración de hardware para sesiones ICA activas, compruebe estas entradas del Registro:

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 uno de los monitores está activo en la segunda GPU, se usa la decodificación basada en CPU.

- Al conectarse a un servidor de Citrix Virtual Apps con Windows Server 2008 R2, no use 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. Puede usar micrófonos instalados localmente 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.

## Asignación de unidades de cliente

La asignación de unidades del cliente admite la transferencia de datos entre el host y el cliente como un flujo. La transferencia de archivos se adapta a las condiciones cambiantes de rendimiento de la red. También utiliza cualquier ancho de banda adicional disponible para ampliar la velocidad de la transferencia de datos.

De manera predeterminada, esta función está habilitada.

Para inhabilitar esta función, configure así la siguiente clave de Registro y reinicie el servidor:

Ruta: `HKEY_LOCAL_MACHINE\System\Currentcontrolset\services\picadm\Parameters`

Nombre: `DisableFullStreamWrite`

Tipo: REG\_DWORD

Valor:

`0x01` = función inhabilitada

`0` o ningún valor = función habilitada

## 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 ventana, con la imagen de un solo monitor para la sesión; las aplicaciones no se acoplan a 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 puede detectar cada uno de los monitores. 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 de 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 de Citrix para el servidor de Citrix Virtual Apps, seleccione la comunidad y, en el panel de tareas, seleccione:
      - **Modify Server Properties > Modify all properties > Server Default > HDX Broadcast > Display**
      - **Modify Server Properties > Modify all properties > Server Default > ICA > Display**

- \* Y establezca la memoria máxima que se utilizará para los gráficos de cada sesión.

Compruebe que el parámetro sea lo bastante 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 calcular 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 modifique las opciones “Compresión de imagen” y “Almacenamiento en caché de imágenes y fuentes”.

### Controlar el teclado en pantalla

Para habilitar el acceso táctil a 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
- Cuando el dispositivo está en modo tienda o tableta

En algunos dispositivos y en algunas circunstancias, la aplicación Citrix Workspace no puede detectar con precisión el modo del dispositivo. Es posible que el teclado en pantalla también aparezca cuando no quiera.

Para evitar que aparezca el teclado en pantalla al usar un dispositivo convertible:

- Cree un valor REG\_DWORD DisableKeyboardPopup 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\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver.

Las claves se pueden configurar en estos 3 modos:

- **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. **Habilítela** y seleccione las opciones necesarias.
5. Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

## Compatibilidad de la aplicación Citrix Workspace con iconos de color de 32 bits:

La aplicación Citrix Workspace admite iconos de color de alta densidad de 32 bits. Para proporcionar aplicaciones integradas, selecciona automáticamente la profundidad del color para:

- Las aplicaciones visibles en el cuadro de diálogo **Central de conexiones**
- El menú Inicio
- La barra de tareas

**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.

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 necesario. 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. Es posible que los requisitos para los usuarios accedan a los escritorios virtuales varíen de un usuario a otro y a medida que evolucionan las necesidades de la empresa. La experiencia de usuario al conectarse a escritorios virtuales y la medida en que el usuario puede configurar las conexiones dependen de la configuración de 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 trabajar en 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 puede cambiar la resolución de pantalla mediante 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 ciertas funciones de accesibilidad de Microsoft, como las Teclas especiales, las Teclas de filtro y las Teclas de alternancia, 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. Las secuencias de accesos directos son, por ejemplo, la secuencia Ctrl+F1, que reproduce las teclas Ctrl+Alt+Supr, y Mayús+F2, que cambia entre el modo de pantalla completa y de ventanas en las aplicaciones.

**Nota:**

No puede usar secuencias de teclas de acceso rápido con escritorios virtuales que se muestran en Desktop Viewer, es decir, con sesiones de aplicaciones y escritorios virtuales. Sin embargo, puede usarlas con aplicaciones publicadas, es decir, con sesiones de aplicaciones virtuales.

## Escritorios virtuales

Los usuarios no pueden conectarse al mismo escritorio virtual desde una sesión de escritorio. Si el usuario lo intenta, desconecta 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.

Un usuario que inicia una sesión localmente en un equipo que actúa como escritorio virtual bloquea la conexión con ese escritorio.

Citrix recomienda trabajar con ellos para definir la asignación de dispositivos:

- Si sus usuarios se conectan a aplicaciones virtuales, publicadas con Citrix Virtual Apps, desde un escritorio virtual
- Si su organización tiene un administrador de Citrix Virtual Apps independiente

La asignación de dispositivos comprueba si los dispositivos de escritorio se asignan de manera coherente en sesiones de escritorio y de aplicación. 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 modificar el tiempo de espera, siga estos pasos:

1. Abra el Editor del Registro.
2. Vaya a la siguiente ruta:
  - En un sistema operativo de 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA_CLIENT\Engine`
  - En un sistema operativo de 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA_CLIENT\Engine\`
3. Cree una clave del Registro de la siguiente manera:
  - Tipo: REG\_DWORD
  - Nombre: `SI_INACTIVE_MS`
  - Valor: 4, si quiere que el indicador de estado desaparezca antes.

Al configurar esta clave, es posible que el indicador de estado aparezca y desaparezca a menudo. Este comportamiento es el esperado. Para suprimir el indicador de estado, haga lo siguiente:

1. Abra el Editor del Registro.
2. Vaya a la siguiente ruta:
  - En un sistema operativo de 64 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA_CLIENT\`
  - En un sistema operativo de 32 bits: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA_CLIENT\`
3. Cree una clave del Registro de la siguiente manera:
  - Tipo: REG\_DWORD
  - Nombre: `NotificationDelay`
  - Valor: Cualquier valor en milisegundos (por ejemplo, 120000)

## Tiempo de espera por inactividad para sesiones de Workspace

Los administradores pueden configurar el valor del tiempo de espera por inactividad para especificar el tiempo de inactividad permitido antes de que se cierre automáticamente la sesión de los usuarios de Citrix Workspace. Se cierra su sesión de Workspace automáticamente si el mouse, el teclado o la función táctil están inactivos durante el intervalo de tiempo especificado. El tiempo de espera por inactividad no afecta a las sesiones de aplicaciones y escritorios virtuales ni a almacenes de Citrix StoreFront que estén activos.

El valor del tiempo de espera por inactividad se puede establecer desde 1 minuto a 1440 minutos. De forma predeterminada, el tiempo de espera por inactividad no está configurado. Los administradores pueden configurar la propiedad `inactivityTimeoutInMinutes` mediante un módulo de PowerShell. Haga clic [aquí](#) para descargar los módulos de PowerShell de la configuración de Citrix Workspace.

La experiencia del usuario final es la siguiente:

- Aparecerá una notificación en la ventana de la sesión tres minutos antes de que se le cierre la sesión, con la opción de mantener la sesión abierta o cerrar la sesión.
- La notificación aparece solamente si el valor del tiempo de espera por inactividad configurado es mayor o igual a cinco minutos.
- Los usuarios pueden hacer clic en **Mantener sesión abierta** para descartar la notificación y seguir utilizando la aplicación. En ese caso, el temporizador de inactividad se restablece a su valor configurado. También puede hacer clic en **Cerrar sesión** para finalizar la sesión del almacén actual.

**Nota:**

Los administradores pueden configurar el tiempo de espera por inactividad solamente para sesiones de Workspace (nube).

### 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.

---

**Nota:**

A partir de la versión 2203.1 LTSR CU4, la aplicación Citrix Workspace no recopila ningún dato de CEIP de los usuarios que se encuentran en la Unión Europea (UE), el Espacio Económico Europeo (EEE), Suiza y el Reino Unido (Reino Unido). Actualice la aplicación Citrix Workspace si quiere

aprovechar esta funcionalidad.

### Información adicional

Citrix gestiona sus datos de acuerdo con las condiciones de su contrato con Citrix y los protege como se especifica en el documento [Citrix Services Security Exhibit](#). El documento Citrix Services Security Exhibit está 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 dejar de enviar datos de CEIP a Citrix y Google Analytics de la siguiente manera:

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**.

#### Nota:

Puede dejar de enviar datos de CEIP excepto para las versiones del sistema operativo y de la aplicación Citrix Workspace que se recopilaron para Google Analytics que se indican con un \* en la segunda tabla.

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** o establecido la clave `Enable_CEIP` en `False`, para dejar de enviar los dos últimos elementos de datos de CEIP, es decir, la versión de la aplicación Citrix Workspace y del sistema operativo, vaya a la siguiente entrada del Registro y defina el valor:

**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	Motivo de la pancarta sin conexión

---

### Parámetros de región

La aplicación Citrix Workspace muestra la fecha, la hora y el número en función de la configuración regional del explorador web o del dispositivo de punto final.

A partir de la aplicación Citrix Workspace 2106, puede personalizar los formatos regionales de fecha, hora y número mediante los Parámetros regionales. Los cambios realizados en estos parámetros se guardan para un usuario individual y se aplican en todos los dispositivos.

**Nota:**

Esta opción solo está disponible en implementaciones de la nube.

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

## Configurar Single Sign-On en la aplicación Citrix Workspace

December 13, 2023

### Single Sign-On mediante Azure Active Directory

En esta sección se explica cómo implementar Single Sign-On (SSO) con Azure Active Directory (AAD) como proveedor de identidades con cargas de trabajo unidas a un dominio en dispositivos de punto final híbridos o inscritos en AAD. Con esta configuración, puede autenticarse en Workspace mediante Windows Hello o FIDO2 en dispositivos de punto final que están inscritos en AAD.

**Nota:**

Si usa Windows Hello como autenticación independiente, puede usar Single Sign-On en la aplicación Citrix Workspace, pero se le solicitará el nombre de usuario y la contraseña al acceder a aplicaciones o escritorios virtuales publicados. Como solución temporal, considere la posibilidad de implementar el Servicio de autenticación federada (FAS).

### Requisitos previos

- Una conexión activa de Azure Active Directory a Citrix Cloud. Para obtener más información, consulte [Conectar Azure Active Directory a Citrix Cloud](#).
- Una autenticación del espacio de trabajo de Azure Active Directory. Para obtener más información, consulte [Habilitar la autenticación de Azure AD para espacios de trabajo](#).
- Compruebe si configuró Azure AD Connect. Para obtener más información, consulte [Introducción a Azure AD Connect mediante la configuración rápida](#).
- Active la autenticación PassThrough en Azure AD Connect. Igualmente, verifique si las opciones de Single Sign-On y PassThrough funcionan en Azure Portal. Para obtener más información, consulte [Autenticación de paso a través de Azure Active Directory: Guía de inicio rápido](#).

## Configuración

Siga estos pasos para configurar SSO en su dispositivo:

1. Instale la aplicación Citrix Workspace mediante la línea de comandos de Windows con la opción `includeSSON`:

`CitrixWorkspaceApp.exe /includeSSON`

1. Reinicie el dispositivo.
2. Ejecute `gpedit.msc` para abrir la plantilla administrativa de GPO de la aplicación Citrix Workspace.
3. Vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Autenticación de usuarios > Nombre de usuario y contraseña locales**.
4. Seleccione **Habilitar autenticación PassThrough**. En función 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.
5. Modifique los parámetros de Autenticación del usuario en Internet Explorer. Para modificar los parámetros:
  - Abra **Propiedades de Internet** en el Panel de control.
  - Vaya a **Propiedades generales > Intranet local** y haga clic en **Sitios**.
  - En la ventana **Intranet local**, haga clic en **Opciones avanzadas > Agregar este sitio a la zona de:**, agregue estos sitios de confianza y haga clic en **Cerrar**:
    - `https://aadg.windows.net.nsatc.net`
    - `https://autologon.microsoftazuread-sso.com`
    - The name of your tenant, **for** example: `https://xxxtenantxxx.cloud.com`
6. Para inhabilitar las solicitudes de autenticación adicionales, inhabilite el atributo `prompt=login` en su arrendatario. Para obtener más información, consulte [User Prompted for Additional Credentials on Workspace URLs When Using Federated Authentication Providers](#). Puede ponerse en contacto con la asistencia técnica de Citrix para inhabilitar el atributo `prompt=login` en su arrendatario y configurar correctamente Single Sign-On.
7. Habilite la autenticación PassThrough de dominio en el cliente de la aplicación Citrix Workspace. Para obtener más información, consulte [Autenticación PassThrough de dominio](#).
8. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.



## Single Sign-On mediante Okta y el Servicio de autenticación federada

En esta sección se explica cómo puede implementar Single Sign-On (SSO) mediante Okta como proveedor de identidades con un dispositivo unido a un dominio y el Servicio de autenticación federada (FAS). Con esta configuración, puede autenticarse en Workspace mediante Okta para habilitar Single Sign-On y evitar que se solicite un segundo inicio de sesión. Para que este mecanismo de autenticación funcione, debe usar el Servicio de autenticación federada de Citrix con Citrix Cloud. Para obtener más información, consulte [Conectar el Servicio de autenticación federada de Citrix con Citrix Cloud](#).

### Requisitos previos

- Cloud Connector. Para obtener más información sobre la instalación de Cloud Connector, consulte [Instalar Cloud Connector](#).
- Un agente de Okta. Para obtener más información sobre la instalación de un agente de Okta, consulte [Install the Okta Active Directory agent](#). Además, puede configurar el agente web de Okta IWA para que inicie sesión desde un dispositivo unido a un dominio de Windows. Para obtener más información, consulte [Install and configure the Okta IWA Web agent for Desktop single sign-on](#).
- Una conexión activa de Azure Active Directory a Citrix Cloud. Para obtener más información, consulte [Conectar Azure Active Directory a Citrix Cloud](#).
- Servicio de autenticación federada. Para obtener más información, consulte [Instalar el Servicio de autenticación federada](#).

### Configuración

Siga estos pasos para configurar SSO en su dispositivo:

#### Conecte Citrix Cloud con su organización de Okta:

1. Descargue e instale el agente de Active Directory para Okta. Para obtener más información, consulte [Install the Okta Active Directory agent](#).
2. Inicie sesión en Citrix Cloud desde <https://citrix.cloud.com>.
3. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
4. Ubique Okta y seleccione **Conectar** en el menú de tres puntos.
5. En **URL de Okta**, introduzca su dominio de Okta.
6. En **Token de API de Okta**, introduzca el token de API de su organización de Okta.

7. En **ID de cliente** y **Secreto del cliente**, introduzca el ID y el secreto del cliente de la integración de la aplicación web OIDC que creó antes. Para copiar estos valores de la consola de Okta, seleccione **Aplicaciones** y busque su aplicación de Okta. En **Credenciales del cliente**, utilice el botón **Copiar al portapapeles** para cada valor.
8. Haga clic en **Probar y finalizar**. Citrix Cloud verifica los detalles de Okta y prueba la conexión.

#### **Habilite la autenticación con Okta para espacios de trabajo:**

1. En el menú de Citrix Cloud, seleccione **Configuración de Workspace > Autenticación**.
2. Seleccione **Okta**. Cuando se le solicite, seleccione **Comprendo los efectos en la experiencia de uso de los suscriptores**.
3. Haga clic en **Aceptar** para aceptar la solicitud de permisos.

#### **Habilite el Servicio de autenticación federada.**

1. En el menú de Citrix Cloud, seleccione **Configuración de Workspace** y, luego, **Autenticación**.
2. Haga clic en **Habilitar FAS**. Este cambio puede tardar hasta cinco minutos en aplicarse a las sesiones de los suscriptores.

Posteriormente, el Servicio de autenticación federada (FAS) se activa para todos los inicios de aplicaciones virtuales y escritorios de Citrix Workspace.

Cuando los suscriptores inician sesión en su espacio de trabajo e inician una aplicación virtual o un escritorio en la misma ubicación de recursos que el servidor FAS, la aplicación o el escritorio se inician sin solicitar credenciales.

#### **Nota:**

Si todos los servidores de FAS de una ubicación de recursos están inactivos o están en modo de mantenimiento, los inicios de aplicación se ejecutan correctamente, pero Single Sign-On no está activo. Se solicita a los suscriptores sus credenciales de AD para acceder a cada aplicación o escritorio.

## **Autenticación**

April 22, 2024

Para maximizar la seguridad del entorno, debe proteger las conexiones entre la aplicación Citrix Workspace y los recursos que publique. Puede configurar diversos tipos de autenticación para la aplicación Citrix Workspace: autenticación con tarjeta inteligente, autenticación PassThrough de dominio y autenticación PassThrough con Kerberos.

## Autenticación PassThrough de dominio

Single Sign-On permite autenticarse en un dominio y usar Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) sin necesidad de volver a autenticarse.

Cuando inicia sesión en la aplicación Citrix Workspace, las credenciales se transfieren a StoreFront, junto con las aplicaciones, los escritorios y los parámetros del menú Inicio. Después de configurar el tipo de inicio de sesión Single Sign-On, puede iniciar sesión en la aplicación Citrix Workspace e iniciar sesiones de aplicaciones y escritorios virtuales sin tener que volver a escribir las credenciales.

Todos los exploradores web necesitarán que configure Single Sign-On mediante la plantilla administrativa de objetos de directiva de grupo (GPO). Para obtener más información sobre cómo configurar Single Sign-On mediante la plantilla administrativa de objetos de directiva de grupo (GPO), 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 (GUI)

## Configurar Single Sign-On durante una instalación nueva

Para configurar Single Sign-On durante una instalación nueva, siga estos pasos:

1. Configuración en StoreFront.
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

Single Sign-On le permite autenticarse en un dominio y usar Citrix Virtual Apps and Desktops y Citrix DaaS desde el mismo dominio sin tener que autenticarse de nuevo para cada aplicación o escritorio.

Cuando agrega un almacén mediante la utilidad **Storebrowse**, las credenciales se transfieren al servidor de Citrix Gateway, junto con las aplicaciones y los escritorios enumerados para usted, incluidos los parámetros del menú Inicio. Después de configurar el inicio Single Sign-On, puede agregar el almacén, enumerar sus aplicaciones y escritorios e iniciar los recursos necesarios sin tener que escribir sus credenciales varias veces.

Según la implementación de Citrix Virtual Apps and Desktops, la autenticación Single Sign-On se puede configurar en StoreFront desde la consola de administración.

Utilice esta tabla para ver los diferentes casos de uso y su configuración respectiva:

Caso de uso	Detalles de configuración	Información adicional
SSON configurado en StoreFront	Inicie Citrix Studio, vaya a <b>Almacenes &gt; Administrar métodos de autenticación - Almacén</b> y habilite <b>PassThrough de dominio</b> .	Cuando la aplicación Citrix Workspace no está configurada con Single Sign-On, 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>Almacenes &gt; Sitios de Workspace para Web &gt; Administrar métodos de autenticación - Almacén</b> y habilite <b>PassThrough de dominio</b> .	Cuando la aplicación Citrix Workspace no está configurada con Single Sign-On, cambia automáticamente el método de autenticación de <b>PassThrough de dominio</b> a <b>Nombre de usuario y contraseña</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 del 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**, y seleccione **Single Sign-On para Citrix Gateway**.
3. Seleccione **Habilitado**.
4. Haga clic en **Aplicar** y **Aceptar**.
5. 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, ejecute el siguiente comando de PowerShell como administrador en el Delivery Controller:

```
asnp Citrix* ; Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True
```

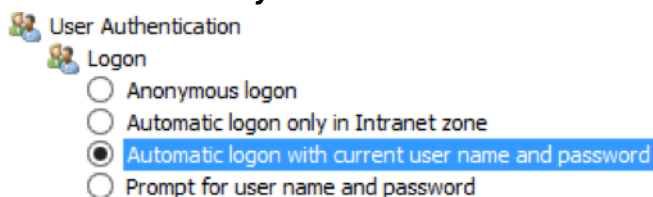
### Modificar los parámetros de Internet Explorer

1. Agregar el servidor de StoreFront a la lista de sitios de confianza mediante Internet Explorer. Para agregarlo:

- 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 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 modificarlos:

- 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**.



- e) Haga clic en **Aplicar** y **Aceptar**.

### Configurar Single Sign-On mediante la interfaz de línea de comandos

Instale la aplicación Citrix Workspace con el modificador de línea de comandos `/includeSSON` y reiníciela para que los cambios surtan efecto.

**Nota:**

Al instalar la aplicación Citrix Workspace para Windows sin el componente Single Sign-On, no se permite actualizarla a la versión más reciente de Citrix Workspace con el modificador de línea de comandos `/includeSSON`.

### Configurar Single Sign-On mediante la GUI

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 en un almacén existente (o configurar un almacén nuevo) mediante la aplicación Citrix Workspace sin introducir 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 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

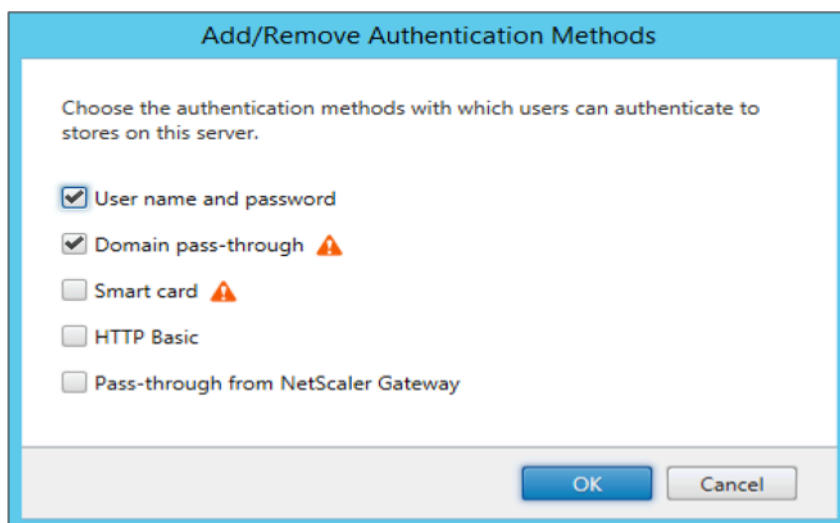
Complete los pasos siguientes para configurar la aplicación Citrix Workspace para la autenticación PassThrough mediante la directiva de grupo de Active Directory. En este caso, puede obtener la autenticación Single Sign-On sin utilizar las herramientas de implementación del software de empresa, como Microsoft System Center Configuration Manager.

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 el contenido para adaptarlo a 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 [receiver.adml](#).
6. Después de agregar la plantilla [receiver.adml](#), vaya a **Configuración del equipo > Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Autenticación de usuarios**. Para obtener más información sobre cómo agregar los archivos de plantilla, consulte [Plantilla administrativa de objeto de directiva de grupo](#).
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

### Configurar StoreFront

1. Inicie **Citrix Studio** en el servidor de StoreFront y seleccione **Almacenes > Administrar métodos de autenticación - Almacén**.
2. Seleccione **PassThrough de dominio**.



## Tokens de autenticación

Los tokens de autenticación se cifran y se almacenan en el disco local para que no tenga que volver a escribir sus credenciales al reiniciar el sistema o la sesión. La aplicación Citrix Workspace ofrece una opción para inhabilitar el almacenamiento de tokens de autenticación en el disco local.

Para mejorar la seguridad, ahora proporcionamos una directiva de objeto de directiva de grupo (GPO) para configurar el almacenamiento de tokens de autenticación.

### Nota:

Esta configuración solo se puede aplicar en implementaciones en la nube.

### Para inhabilitar el almacenamiento de tokens de autenticación mediante la directiva de objeto de directiva de grupo (GPO):

1. Ejecute `gpedit.msc` para abrir la plantilla administrativa de GPO de la aplicación Citrix Workspace.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix > Autoservicio**.
3. En la directiva **Almacenar tokens de autenticación**, seleccione una de estas opciones:
  - **Habilitado**: Indica que los tokens de autenticación se almacenan en el disco. De forma predeterminada, habilítela.
  - **Inhabilitado**: Indica que los tokens de autenticación no se almacenan en el disco. Introduzca de nuevo sus credenciales al reiniciar el sistema o la sesión.
4. Haga clic en **Aplicar** y **Aceptar**.



A partir de la versión 2106, la aplicación Citrix Workspace ofrece otra opción para inhabilitar el almacenamiento de tokens de autenticación en el disco local. Junto con la configuración de GPO existente, también puede inhabilitar el almacenamiento de tokens de autenticación en el disco local mediante Global App Configuration Service.

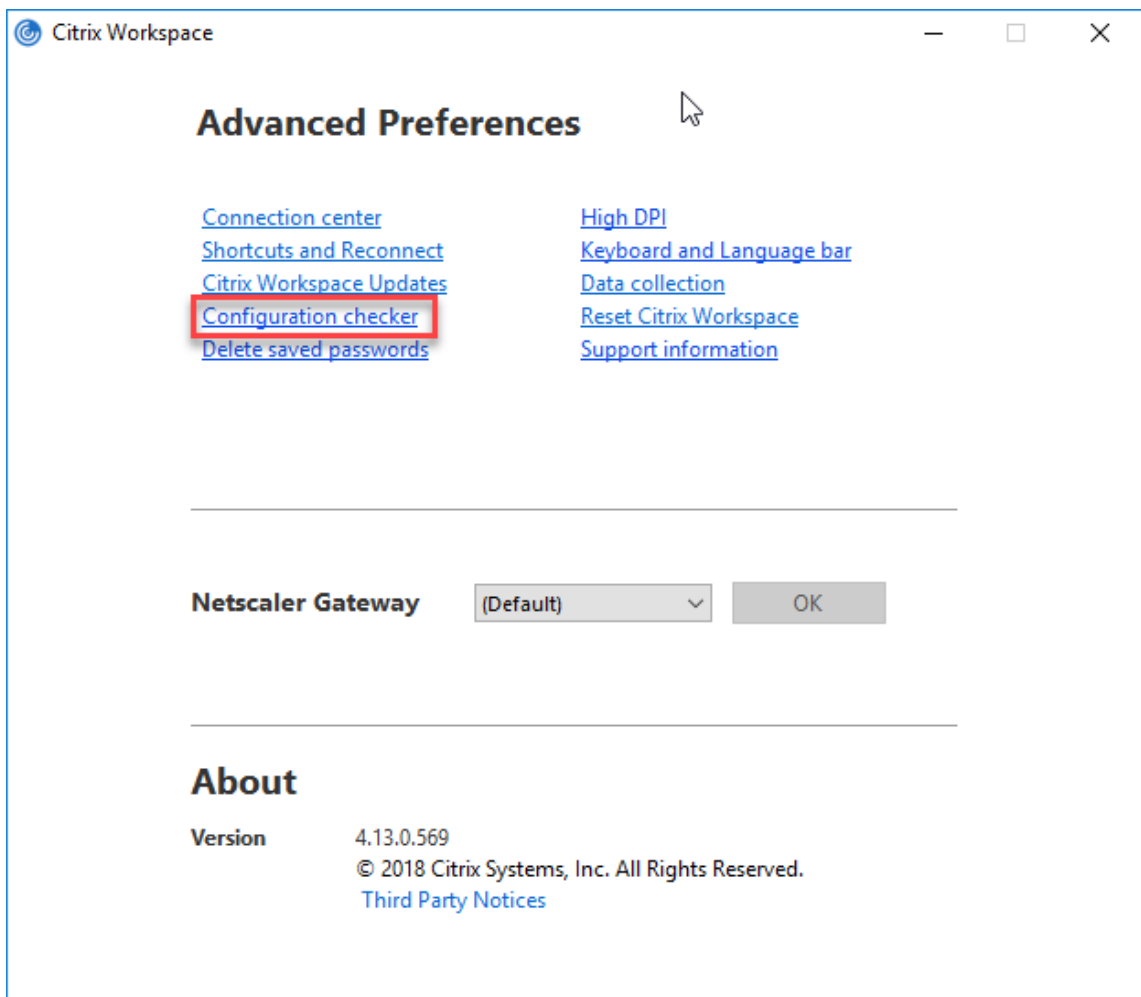
En Global App Configuration Service, establezca el atributo `Store Authentication Tokens` en `False`.

Para obtener más información, consulte la documentación de [Global App Configuration Service](#).

### **Configuration Checker**

Configuration Checker le permite ejecutar pruebas para comprobar si 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:** Proporciona información adicional sobre la prueba, independientemente del resultado de esta.

El usuario puede ver más información sobre cada punto de control y los resultados correspondientes.

Se realizan estas 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 proveedores 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 StoreFront.

**Nota:**

- Si accede a Workspace para Web, los resultados de la prueba no se aplican.
- Si la aplicación Citrix Workspace está configurada con 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 del 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 de confianza en solicitudes enviadas a XML Service en los servidores de Citrix Virtual Apps and Desktops.

**Prueba de baliza** La aplicación Citrix Workspace permite realizar una prueba de baliza mediante la herramienta de comprobación de balizas que está disponible como parte de la herramienta **Configuration Checker**. La prueba de baliza ayuda a confirmar si se puede acceder a la baliza (ping.citrix.com). Con esta prueba de diagnóstico, 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 la opción **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.

### **Nota:**

- Los resultados de la prueba no se aplican a Workspace para Web.
- Puede guardar como informes los resultados de la prueba. El formato predeterminado del informe es TXT.

## **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)**.

Al habilitarse, Kerberos se autentica sin contraseña en la aplicación Citrix Workspace. Así, impide ataques de tipo troyano que intentan acceder a las contraseñas del dispositivo de usuario. Los usuarios pueden iniciar sesión con cualquier método de autenticación y acceder a recursos publicados; por ejemplo, un autenticador biométrico (un lector de huellas digitales).

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. HDX Engine (antes conocido como cliente ICA) 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, compruebe si la configuración de Kerberos cumple estos 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. Se confía en los servidores 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**

Es posible que el uso incorrecto del Editor del Registro del sistema cause problemas graves que puedan obligarle a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de un uso incorrecto 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.

### **Autenticación PassThrough de dominio con Kerberos para usarla con tarjetas inteligentes**

Antes de continuar, consulte la sección [Proteger la implementación](#) en el documento de Citrix Virtual Apps and Desktops.

Cuando instale la aplicación Citrix Workspace para Windows, incluya la opción siguiente en la línea de comandos:

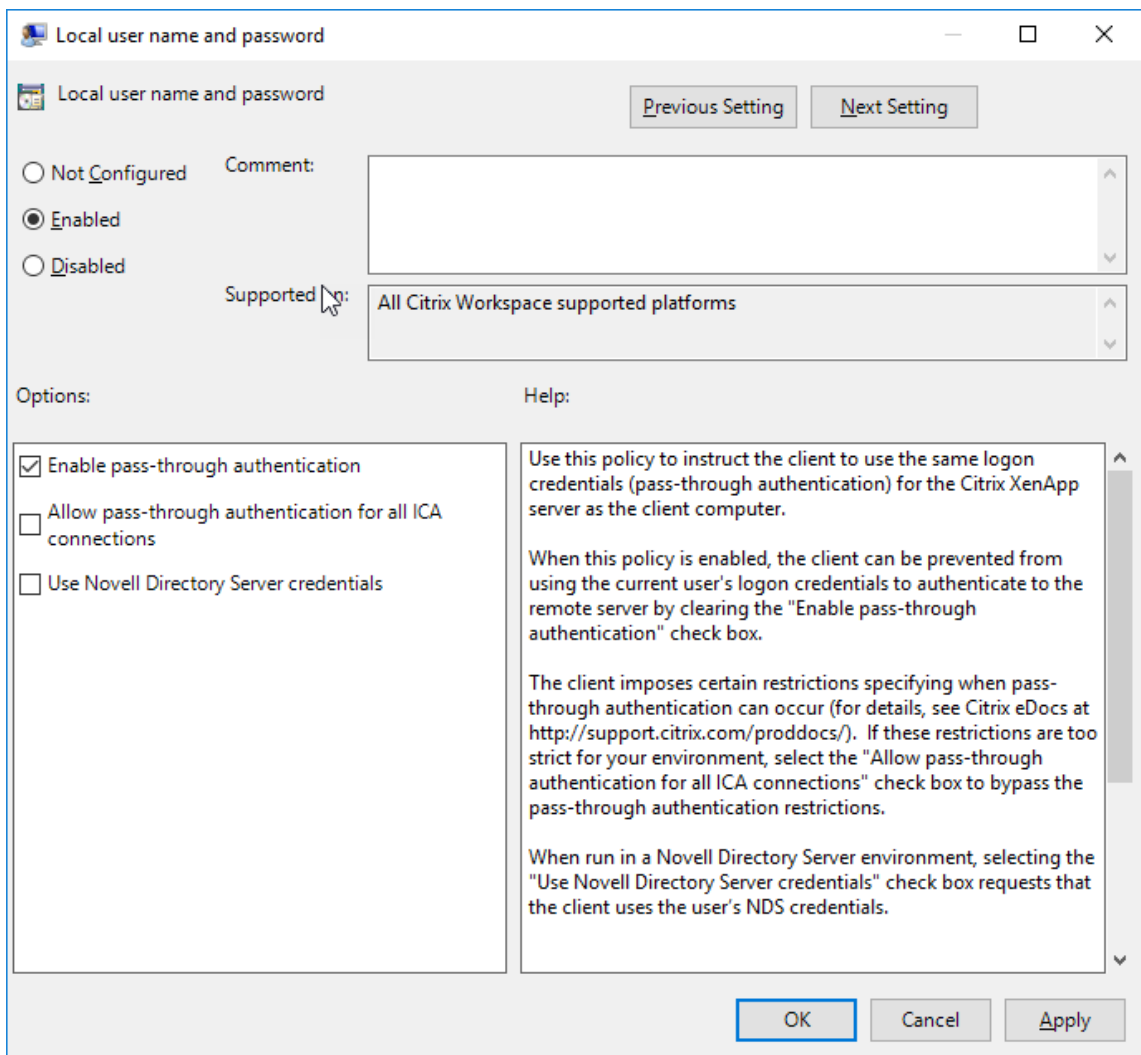
- `/includeSSON`

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 que el motor HDX utiliza 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.

### Compatibilidad del Acceso condicional con Azure Active Directory

El Acceso condicional es una herramienta utilizada por Azure Active Directory para aplicar directivas de organización. Los administradores de Workspace pueden configurar y aplicar directivas de acceso condicional de Azure Active Directory a usuarios que se autentican en la aplicación Citrix Workspace.

La máquina Windows que ejecute la aplicación Citrix Workspace debe tener instalada la versión 92 de Microsoft Edge WebView2 Runtime o una versión posterior.

Para obtener información e instrucciones completas sobre cómo configurar directivas de acceso condicional con Azure Active Directory, consulte la **documentación sobre el Acceso condicional de Azure AD** en [docs.microsoft.com/es-es/azure/active-directory/conditional-access/](https://docs.microsoft.com/es-es/azure/active-directory/conditional-access/).

**Nota:**

Esta función solo está disponible en implementaciones de Workspace (Cloud).

## Otras formas de autenticarse en Citrix Workspace

Puede configurar estos mecanismos de autenticación con la aplicación Citrix Workspace. Para que estos mecanismos de autenticación funcionen como es debido, la máquina Windows que ejecuta la aplicación Citrix Workspace debe tener instalada la versión 92 de Microsoft Edge WebView2 Runtime o una versión posterior.

1. Autenticación por Windows Hello: Para obtener instrucciones sobre cómo configurar la autenticación por Windows Hello, consulte **Configure Windows Hello for Business Policy settings - Certificate Trust** en [\\_docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings](https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings).

**Nota:**

No se admite la autenticación basada en Windows Hello con PassThrough de dominio.

1. Autenticación por claves de seguridad FIDO2: Las claves de seguridad FIDO2 ofrecen un método intuitivo para que los empleados se autenticen sin introducir nombres de usuario ni contraseñas. Puede configurar la autenticación por claves de seguridad FIDO2 en Citrix Workspace. Si quiere que los usuarios se autenticen en Citrix Workspace con su cuenta de Azure AD mediante una clave de seguridad FIDO2, consulte **Habilitación del inicio de sesión con clave de seguridad sin contraseña** en [docs.microsoft.com/es-es/azure/active-directory/authentication/howto-authentication-passwordless-security-key](https://docs.microsoft.com/es-es/azure/active-directory/authentication/howto-authentication-passwordless-security-key).
2. También puede configurar Single Sign-On (SSO) en la aplicación Citrix Workspace desde máquinas unidas a Microsoft Azure Active Directory (AAD) con AAD como un proveedor de identidades. Para obtener más información detallada sobre la configuración de Azure Active Directory Domain Services, consulte **Configurar Azure Active Directory Domain Services** en [docs.microsoft.com/es-es/azure/active-directory-domain-services/overview](https://docs.microsoft.com/es-es/azure/active-directory-domain-services/overview). Para obtener información sobre cómo conectar Azure Active Directory a Citrix Cloud, consulte [Conectar Azure Active Directory a Citrix Cloud](#).



## 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 un dominio que inician sesión en la aplicación Citrix Workspace con una 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 permitir autenticarse tanto con nombre y contraseña como 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:** Pueden emplearse varios certificados para una única tarjeta inteligente, y también si se utilizan varias tarjetas inteligentes. Cuando se inserta una tarjeta inteligente en el lector de tarjetas, los certificados se aplican a todas las aplicaciones ejecutadas en el dispositivo del usuario, incluida la aplicación Citrix Workspace.
- **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, debe 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.
- **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 durante la sesión del usuario. No se guarda 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 una VPN con la autenticación con tarjeta inteligente, instale Citrix Gateway Plug-in. Inicie sesión en una página web con sus tarjetas inteligentes y sus 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. Es posible que el uso incorrecto del Editor del Registro del sistema cause problemas que puedan requerir la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de un uso incorrecto 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.

- En el Editor del Registro, vaya a esta ruta de acceso y establezca la cadena `SSONCheckEnabled` en `False` si no instaló el componente Single Sign-On.

```
HKEY_CURRENT_USER\Software{ Wow6432 } \Citrix\AuthManager\protocols
\integratedwindows\
```

```
HKEY_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\
protocols\integratedwindows\
```

La clave impide que Authentication Manager de la aplicación Citrix Workspace busque el componente Single Sign-On y permite que la aplicación Citrix Workspace se autentique en StoreFront.

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 inicia sesión en el dispositivo de punto final con otro método de autenticación como, por ejemplo, nombre de usuario y contraseña, la línea de comandos es:

```
/includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
```

Este tipo de autenticación evita la captura de las credenciales al iniciar sesión y permite que la aplicación Citrix Workspace almacene el PIN durante el inicio de sesión en la aplicación 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. En su lugar, 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 uso de claves debe incluir la firma digital.
- Las sesiones de Citrix Virtual Apps se cierran al extraer la tarjeta inteligente.
- El campo “Uso mejorado de claves” debe incluir 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) permitidos que haya enviado 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` o `LatestExpiry`, si hay varios certificados que cumplen esos criterios, la aplicación Citrix Workspace pide al usuario que elija un certificado.

---

Agregue el siguiente valor a la clave de Registro `SmartCardDefault` o `LatestExpiry`.

```
HKEY_CURRENT_USER OR
HKEY_LOCAL_MACHINE\
Software\[Wow6432Node
\Citrix\AuthManager:
CertificateSelectionMode=
{Prompt
```

---

•

Los valores definidos en `HKEY_CURRENT_USER` tienen preferencia sobre los valores definidos en `HKEY_LOCAL_MACHINE` para facilitar al usuario la selección de un 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\AuthManager: SmartCardPINEntry=CSP`.

### **Cambios en la extracción y la compatibilidad de tarjetas inteligentes**

Las sesiones de Citrix Virtual Apps se cierran al extraer la tarjeta inteligente. Si la aplicación Citrix Workspace está configurada con tarjeta inteligente como método de autenticación, configure la directiva correspondiente en la aplicación Citrix Workspace para Windows para que se aplique el cierre de las sesiones de Citrix Virtual Apps. La sesión del usuario sigue abierta en la aplicación Citrix Workspace.

#### **Limitación:**

Cuando inicia sesión en el sitio de la aplicación Citrix Workspace mediante la autenticación con tarjeta inteligente, el nombre de usuario aparece como **Conectado**.

**Tarjeta inteligente rápida** La tarjeta inteligente rápida es una mejora con respecto a la redirección HDX existente de tarjetas inteligentes basada en PC/SC. Mejora el rendimiento cuando se usan tarjetas inteligentes en entornos WAN con latencia alta.

Las tarjetas inteligentes rápidas solo son compatibles con Windows VDA.

#### **Para habilitar el inicio de sesión con tarjeta inteligente rápida en la aplicación Citrix Workspace:**

El inicio de sesión con tarjeta inteligente rápida está habilitado de forma predeterminada en VDA e inhabilitado de forma predeterminada en la aplicación Citrix Workspace. Para habilitarlo, incluya el siguiente parámetro en el archivo `default.ica` del sitio asociado de StoreFront:

```
1 copy[WFCClient]
2 SmartCardCryptographicRedirection=On
3 <!--NeedCopy-->
```

### **Para inhabilitar el inicio de sesión con tarjeta inteligente rápida en la aplicación Citrix Workspace:**

Para inhabilitar el inicio de sesión con tarjeta inteligente rápida en la aplicación Citrix Workspace, quite el parámetro `SmartCardCryptographicRedirection` del archivo `default.ica` del sitio asociado de StoreFront.

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

### **Autenticación silenciosa para Citrix Workspace**

La aplicación Citrix Workspace presenta una directiva de objeto de directiva de grupo (GPO) para habilitar la autenticación silenciosa en Citrix Workspace. Esta directiva permite a la aplicación Citrix Workspace iniciar sesión en Citrix Workspace automáticamente al iniciar el sistema. Utilice esta directiva solo cuando la autenticación PassThrough de dominio (Single Sign-On) esté configurada para Citrix Workspace en dispositivos unidos a un dominio.

Para que esta directiva funcione, se deben cumplir los siguientes criterios:

- Single Sign-On debe estar habilitado.
- La clave `SelfServiceMode` debe establecerse en `Off` en el editor del Registro.

#### **Habilitar la autenticación silenciosa:**

1. Ejecute `gpedit.msc` para abrir la plantilla administrativa de GPO de la aplicación Citrix Workspace.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Workspace > Autoservicio**.
3. Haga clic en la directiva **Autenticación silenciosa para Citrix Workspace** y **hábilitela**.
4. Haga clic en **Aplicar** y **Aceptar**.

### **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 todo un abanico de tecnologías de seguridad, como, por ejemplo:

- Citrix Gateway: Para obtener información, consulte los temas de esta sección, además de la documentación de Citrix Gateway y StoreFront.
- 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.
- Se admite desde la versión 1.0 hasta la versión 1.2 de Transport Layer Security (TLS).
- Servidor de confianza para establecer relaciones de confianza en las conexiones de la aplicación Citrix Workspace.
- ICA File Signing
- Protección de la autoridad de seguridad local (LSA)
- Solo para el servidor proxy de implementaciones de Citrix Virtual Apps: un servidor proxy SOCKS o un servidor proxy seguro. Los servidores proxy ayudan a limitar el acceso entrante y saliente de la red. También gestionan las conexiones entre la aplicación Citrix Workspace y el servidor. La aplicación Citrix Workspace admite protocolos de proxy seguro y SOCKS.
- Proxy saliente

## Citrix Gateway

Citrix Gateway (anteriormente Access Gateway) protege las conexiones a los almacenes de StoreFront. Además, permite a los administradores controlar de manera detallada el acceso de los usuarios a los escritorios y las aplicaciones.

Para conectarse a escritorios y aplicaciones a través de Citrix Gateway:

1. Especifique la URL de Citrix Gateway que el administrador proporciona de una de las siguientes maneras:
  - La primera vez que use la interfaz de usuario de autoservicio, se le solicitará que introduzca la dirección URL en el cuadro de diálogo **Agregar cuenta**
  - Cuando utilice más tarde la interfaz de usuario de autoservicio, puede introducir la URL en **Preferencias > Cuentas > Agregar**.
  - Si quiere establecer una conexión mediante el comando storebrowse, escriba la dirección URL en la línea de comandos.

La dirección URL especifica la puerta de enlace y, si quiere, un almacén concreto:

- Para conectarse al primer almacén que encuentra la aplicación Citrix Workspace, use una URL en este formato:
  - <https://puertadeenlace.empresa.com>
- Para conectarse a un almacén específico, use una URL con este formato. Por ejemplo: <https://puertadeenlace.empresa.com?>. Esta dirección URL dinámica no tiene el formato estándar; no incluya = (el signo igual) en la URL. Si quiere establecer una conexión a un almacén

concreto mediante storebrowse, puede que se necesiten comillas alrededor de la dirección URL en el comando storebrowse.

1. Cuando se le solicite, conéctese al almacén (a través de la puerta de enlace) con su nombre de usuario, contraseña y token de seguridad. Para obtener más información sobre este paso, consulte la documentación de Citrix Gateway.

Una vez completado el proceso de autenticación, se muestran los escritorios y las aplicaciones.

## Conectarse a través de 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 un firewall, la aplicación Citrix Workspace para Windows puede comunicarse a través de él con el servidor web y el servidor de Citrix.

## Puertos comunes de comunicación Citrix

Origen	Tipo	Puerto	Detalles
Aplicación Citrix Workspace	TCP	80/443	Comunicación con StoreFront
ICA o HDX	TCP/UDP	1494	Acceso a aplicaciones y escritorios virtuales
ICA o HDX con fiabilidad de la sesión	TCP/UDP	2598	Acceso a aplicaciones y escritorios virtuales
ICA o HDX por TLS	TCP/UDP	443	Acceso a aplicaciones y escritorios virtuales

Para obtener más información sobre los puertos, consulte el artículo [CTX101810](#) de Knowledge Center.

## Transport Layer Security

Transport Layer Security (TLS) es el reemplazo del protocolo SSL (Secure Sockets Layer). La organización Internet Engineering Taskforce (IETF) le cambió el nombre a TLS al asumir la responsabilidad del desarrollo de TLS como un estándar abierto.

TLS protege las comunicaciones de datos mediante la autenticación del servidor, el cifrado del flujo de datos y la comprobación de la integridad de los mensajes. Algunas organizaciones, entre las que se



encuentran organizaciones del gobierno de los EE. UU., requieren el uso de TLS para proteger las comunicaciones de datos. Es posible que estas organizaciones también exijan el uso de cifrado validado, como FIPS 140 (Federal Information Processing Standard). FIPS 140 es un estándar para cifrado.

Para utilizar el cifrado TLS como medio de comunicación, debe configurar el dispositivo de usuario y la aplicación Citrix Workspace. Para obtener información sobre cómo proteger las comunicaciones de StoreFront, consulte la sección [Proteger](#) de la documentación de StoreFront. Para obtener información sobre cómo proteger los VDA, consulte [Transport Layer Security \(TLS\)](#) en la documentación de Citrix Virtual Apps and Desktops.

Puede usar estas directivas para:

- Exigir el uso de TLS: Se recomienda usar TLS para las conexiones a través de redes que no son de confianza, incluido Internet.
- Exigir el uso de FIPS (Federal Information Processing Standards): Criptografía aprobada y seguir 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.
- 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.

La aplicación Citrix Workspace para Windows admite estos conjuntos de cifrado para el protocolo TLS 1.2:

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA

Para obtener información sobre los conjuntos de cifrado admitidos, consulte el artículo [CTX250104](#) de Knowledge Center.

**Importante:**

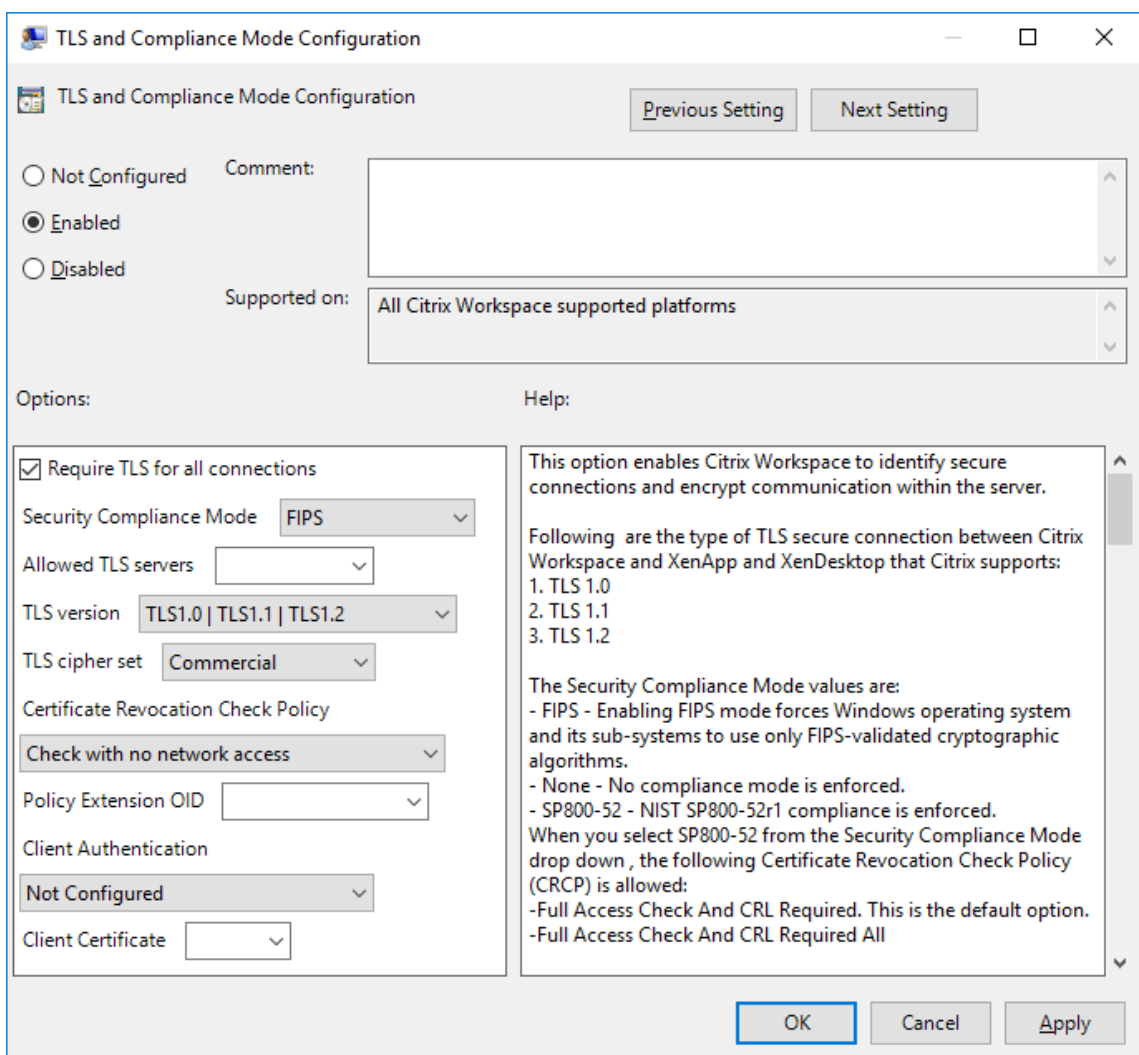
Estos conjuntos de cifrado se han retirado para mejorar la seguridad:

- Conjuntos de cifrado RC4 y 3DES
- Conjuntos de cifrado con el prefijo “TLS\_RSA\_\*\*”
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 (0x009d)
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0x009c)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003d)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002f)
- TLS\_RSA\_WITH\_RC4\_128\_SHA (0x0005)
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x000a)

## 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 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 la puerta de enlace 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**. Asimismo, habilite 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**, establezca la configuración de la directiva **Comprobación de revocación de certificados** en **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 sigue 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. Igualmente, habilite 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 el menú desplegable **Servidores TLS permitidos**, seleccione el número de puerto. Utilice una lista separada por comas para asegurarse de que la aplicación Citrix Workspace solo se conecta a un servidor especificado. 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 o no 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 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 un conjunto de cifrado TLS específico, seleccione Gubernamental (GOV), Comercial (COM) o Todos (ALL). Para obtener más información, consulte el artículo [CTX250104](#) de Knowledge Center.
- b) 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. Una comprobación de la lista de revocación de certificados que verifica el certificado del servidor disponible en el servidor de traspaso SSL o de Citrix Secure Web Gateway de destino no es obligatorio.
  - **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. La comprobación de la lista de revocación de certificados para verificar el certificado de servidor disponible en el servidor de destino no es esencial.
  - **Requerir comprobación con acceso completo y lista de revocación de certificados:** Se hace una comprobación de listas de revocación de certificados, a excepción 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.

Para obtener información sobre la tabla de conexiones de red internas y externas, consulte el artículo [CTX250104](#) de Knowledge Center.

## 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. 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 se halla 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 > Componentes de Citrix > Citrix Workspace > Redirección de red > Configuración de servidores de confianza**.
3. Marque **Habilitado** para obligar a que la aplicación Citrix Workspace identifique la región.
4. Marque **Aplicar configuración de servidor de confianza**. Esta opción obliga al cliente a realizar la identificación mediante un servidor de confianza.
5. Desde el menú 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 de firma de archivos ICA 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.

## 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 quitar 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 se puede iniciar la sesión por la falta de autorización.
    - 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:**

Al seleccionar un certificado de firma digital, recomendamos elegirlo a partir de esta lista de prioridades:

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.
4. Cree un certificado raíz y distribúyalo a los dispositivos de usuario mediante un objeto de directiva de grupo o una instalación manual.

#### **Protección de la autoridad de seguridad local (LSA)**

La aplicación Citrix Workspace ofrece la protección de la autoridad de seguridad local (LSA) de Windows, que conserva información sobre todos los aspectos de la seguridad local de un sistema. Esto proporciona el nivel LSA de protección del sistema para los escritorios alojados.

#### **Conectarse a través de un 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 con Workspace para 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. Configure los parámetros de **Internet** del explorador web predeterminado en el dispositivo de usuario según corresponda.

Para aplicar los parámetros de proxy a través del archivo ICA en StoreFront, consulte el artículo [CTX136516](#) de Citrix Knowledge Center.

## Compatibilidad con proxies salientes

SmartControl permite a los administradores configurar y aplicar directivas que afectan al entorno. Por ejemplo, es posible que quiera prohibir a los usuarios asignar unidades a sus escritorios remotos. Puede lograr la granularidad mediante la función SmartControl en 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 SmartControl porque la puerta de enlace no existe en el dominio. En su lugar, puede utilizar el proxy ICA saliente. La función proxy ICA saliente permite utilizar la función SmartControl 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. Utilice el plug-in de proxy saliente para configurar un único proxy estático o seleccione un servidor proxy en tiempo de ejecución.

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 o 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"
```

## Storebrowse

October 30, 2023

**Storebrowse** es una utilidad de línea de comandos que interactúa entre el cliente y el servidor. Se usa para autenticar todas las operaciones en StoreFront y con Citrix Gateway.

Con la utilidad **Storebrowse**, los administradores pueden automatizar las siguientes operaciones:

- Agregar un almacén.
- Producir una lista de las aplicaciones y los escritorios publicados desde un almacén configurado.
- Generar un archivo ICA manualmente seleccionando cualquier escritorio o aplicación virtual publicados.
- Generar un archivo ICA mediante la línea de comandos de **Storebrowse**.
- Iniciar la aplicación publicada.

La utilidad **Storebrowse** forma parte del componente **Authmanager**. Al completar la instalación de la aplicación Citrix Workspace, la utilidad **Storebrowse** se encuentra en la carpeta de instalación **AuthManager**.

Puede verificar si la utilidad **Storebrowse** está instalada junto con el componente **Authmanager**. Para ello, consulte la siguiente ruta de registro:

#### **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**

- Aplicación Citrix Workspace 1808 para Windows o una versión posterior.
- Mínimo 530 MB de espacio libre en disco.
- 2 GB de RAM.

### **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:

En un almacén HTTP, la utilidad **Storebrowse** no acepta credenciales introducidas desde la línea de comandos.

## 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:** Introduzca las credenciales para autenticarse y acceder a los almacenes. La autenticación explícita está habilitada de forma predeterminada cuando crea el primer almacén.
- **PassThrough de dominio:** Después de autenticarse en los equipos Windows unidos a un dominio, se inicia sesión automáticamente en los almacenes. Para utilizar esta opción, habilite la

autenticación PassThrough al instalar la aplicación Citrix Workspace. Para obtener más información sobre PassThrough de dominios, 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 **Autenticación HTTP básica**.

La utilidad **Storebrowse** permite la autenticación de cualquiera de estas maneras:

- Mediante el componente [AuthManager](#), integrado en la utilidad **Storebrowse**. Nota: Habilite 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.

### 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 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 la devolución falla, se notifica un error.

#### **Nota:**

Con la utilidad **Storebrowse**, es posible configurar varios almacenes.

### **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 recursos.

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 para las aplicaciones y los escritorios publicados mediante la utilidad **Storebrowse**. La opción `quicklaunch` requiere una URL de inicio como entrada, junto con la URL del almacén. La URL de inicio puede ser el 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 si ejecuta el siguiente comando:

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/Second/discovery
```

Las URL de inicio suelen ser así:

```
'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 y la URL del almacén. El nombre puede ser el servidor de StoreFront o la URL de Citrix Gateway. El archivo ICA se genera en el directorio %LocalAppData%\Citrix\Storebrowse\cache.

Ejecute este comando para obtener el nombre simplificado de las aplicaciones y los escritorios publicados:

```
.\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/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

El nombre en negrita del 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:**

Con este comando, puede agregar un almacén y verificar e iniciar los recursos publicados. Esta opción toma los siguientes elementos como parámetros:

- Nombre de usuario
- Contraseña

- Dominio
- Nombre del recurso que se va a iniciar
- URL del almacén

Sin embargo, si el usuario no proporciona las credenciales, **AuthManager** le pide que introduzca las credenciales y, a continuación, se inicia el recurso.

Puede obtener el nombre del recurso de aplicaciones y escritorios publicados con este 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/Q29udHJvbGxlcj5DYWxjdWxhdG9y/launch/ica
```

El nombre en negrita del resultado anterior se usa como el parámetro de entrada de 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 en la ruta personalizada para las aplicaciones y escritorios publicados.

La opción de inicio requiere un nombre de carpeta y el nombre del recurso como entrada con la URL del almacén. La URL del almacén puede ser el 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 el dispositivo Citrix Gateway:

```
.\storebrowse.exe -f "C:\Temp\Launch.ica" -L "Resource_Name" { NSG_URL }
```



## **-t, --traceauthentication**

### **Descripción:**

Genera registros para el componente [AuthManager](#). Los registros se generan solo si la utilidad **Storebrowse** utiliza 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.secondexamplestore.com
```

## **Función Single Sign-On en Citrix Gateway**

Single Sign-On permite autenticarse en un dominio y usar Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) que proporciona el dominio. Puede iniciar sesión sin tener que reautenticarse en cada aplicación o escritorio. Al agregar un almacén, las credenciales se transfieren al servidor de Citrix Gateway, junto con las aplicaciones y los escritorios de Citrix Virtual Apps and Desktops y Citrix DaaS, y los parámetros del menú Inicio.

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).

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 e intenta conectarse al almacén mediante la utilidad para comprobar o iniciar las aplicaciones o escritorios virtuales publicados, no se permite introducir credenciales mediante la opción de línea de comandos. Como solución temporal, utilice el módulo [AuthManager](#) externo si no proporciona 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.

Para habilitar SSON para aplicaciones de terceros que usan ICOSDK, cree este Registro:

- Clave del Registro: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Valor del Registro: Ruta completa de las aplicaciones de terceros
- Tipo de Registro: `reg_multi_sz`

Ejemplo:

- Clave del Registro: `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- Valor del Registro: `C:\temp1\abc.exe; C:\temp2\xyz.exe`
- Tipo de Registro: `reg_multi_sz`

**Nota:**

- Puede proporcionar varias aplicaciones de terceros separadas por puntos y comas.

## 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.

La aplicación Citrix Workspace para Windows con Desktop Lock funciona en máquinas unidas a dominios con Single Sign-On habilitado 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.

Instale la aplicación Citrix Workspace para Windows con el indicador `/includeSSON`. Configure el almacén y Single Sign-On, ya sea mediante el archivo `adm/admx` o con la opción de la línea de comandos. Para obtener más información, consulte [Instalación](#).

A continuación, instale Desktop Lock de la aplicación Citrix Workspace como administrador con el archivo `CitrixWorkspaceDesktopLock.msi` disponible en la página de [descargas de Citrix](#).

### Requisitos del sistema

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. Para obtener más información, consulte la página de [descargas de Microsoft](#).
- Compatible con Windows 8, Windows 8.1, Windows 10 (actualización Anniversary Update incluida) y Windows 11.
- Se conecta a StoreFront solo a través de protocolos nativos.
- Puntos finales unidos a un dominio.
- Los dispositivos de usuario deben estar conectados a una LAN o una WAN.

## Acceso a aplicaciones locales

### Importante

Al habilitar 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 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 este comando:

Por ejemplo:

```
1 CitrixWorkspaceApp.exe
2 /includeSSON
3 STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/
 discovery;on;Desktop Store"
4 <!--NeedCopy-->
```

El comando está disponible en la aplicación Citrix Workspace y en la carpeta **Plug-ins > Windows > Citrix Workspace app** de los medios de instalación. Para obtener información detallada sobre los comandos, consulte la documentación sobre la instalación de la aplicación Citrix Workspace en [Instalación](#).

3. En la misma carpeta de los medios de instalación, haga doble clic en `CitrixWorkspaceDesktopLock.msi`. Aparece el asistente de Desktop Lock. Siga las indicaciones.
4. 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.

Puede permitir la administración del dispositivo de usuario una vez finalizada la instalación. La cuenta que se utilizó para instalar `CitrixWorkspaceDesktopLock.msi` se excluye del shell de sustitución. Si esa cuenta se elimina más tarde, no puede 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

Una vez que haya iniciado sesión como un usuario que no es administrador, Desktop Lock inicia automáticamente una sesión de escritorio asignada.

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 si 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 en

**Configuración de usuario > Plantillas administrativas > Plantillas administrativas clásicas (ADMX) > Componentes de Citrix**). Los archivos ADMX están en %ProgramFiles%\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 y no se requiere ninguna interacción por parte del usuario. El escritorio virtual 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. Agregue la URL en formato escritorio://nombre-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, independientemente de cuál sea la directiva de extracción de tarjeta inteligente configurada en el equipo. Desktop Lock garantiza que el dispositivo del usuario no quede en un estado incoherente. Esto se aplica solo a los dispositivos de usuario con Desktop Lock de la aplicación Citrix Workspace.

## **Eliminar Desktop Lock**

Asegúrese de quitar los dos componentes indicados a continuación:

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.



## Kit de desarrollo de software (SDK) y API

June 9, 2023

### SDK de declaración de identidad de certificado

El SDK de declaración de identidad de certificado (CID) permite a los desarrolladores crear un plug-in. El plug-in permite que la aplicación Citrix Workspace se autentique en el servidor de StoreFront mediante el certificado que está 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 API nativas que le permiten interactuar y realizar operaciones básicas de manera programática. 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. La sesión 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 kit de desarrollo de software (SDK) de Citrix Virtual Channel permite la escritura de aplicaciones del lado del servidor y controladores del lado del cliente para más canales virtuales 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 que proporciona credenciales de usuario a la función Single Sign-On (SSO). Esta función está disponible a partir de la versión 4.2 de la aplicación Citrix Workspace para Windows. Con esta API, los socios de Citrix pueden ofrecer productos de autenticación y SSO que usen StoreFront 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).