



# Aplicación Citrix Workspace 2402 LTSR para Windows

## Contents

<b>Acerca de la aplicación Citrix Workspace 2402 LTSR para Windows</b>	<b>4</b>
<b>Aplicación Citrix Workspace 2402 LTSR para Windows</b>	<b>7</b>
<b>Problemas resueltos</b>	<b>61</b>
<b>Problemas conocidos</b>	<b>63</b>
<b>Requisitos del sistema y compatibilidad</b>	<b>64</b>
<b>Instalación y desinstalación</b>	<b>71</b>
<b>Implementación</b>	<b>93</b>
<b>Configuración del almacén</b>	<b>102</b>
<b>Administración de actualizaciones y plug-ins</b>	<b>115</b>
<b>Actualización</b>	<b>115</b>
<b>Administración de plug-ins</b>	<b>128</b>
<b>Experiencia en la aplicación</b>	<b>139</b>
<b>Entrega de aplicaciones</b>	<b>139</b>
<b>Experiencia mejorada al iniciar aplicaciones y escritorios virtuales</b>	<b>152</b>
<b>Preferencias de la aplicación</b>	<b>152</b>
<b>Aplicaciones SaaS</b>	<b>160</b>
<b>Recopilación y supervisión de datos</b>	<b>161</b>
<b>Seguridad y autenticación</b>	<b>165</b>
<b>Seguridad</b>	<b>165</b>
<b>Proteger comunicaciones</b>	<b>168</b>
<b>Autenticación</b>	<b>184</b>
<b>Tabla de acceso de PassThrough de dominio</b>	<b>210</b>

<b>PassThrough de dominio a Citrix Workspace con Citrix Gateway local como proveedor de identidades</b>	<b>217</b>
<b>PassThrough de dominio a Citrix Workspace con Azure Active Directory como proveedor de identidades</b>	<b>232</b>
<b>PassThrough de dominio a Citrix Workspace con Okta como proveedor de identidades</b>	<b>237</b>
<b>PassThrough de dominio mejorado para Single Sign-On (SSO mejorado)</b>	<b>239</b>
<b>HDX</b>	<b>244</b>
<b>Gráficos y pantalla</b>	<b>244</b>
<b>Microsoft Teams optimizado</b>	<b>256</b>
<b>Transporte HDX</b>	<b>260</b>
<b>Redirección de contenido del explorador web</b>	<b>261</b>
<b>Redirección bidireccional de contenido</b>	<b>264</b>
<b>Referencia para parámetros ICA</b>	<b>270</b>
<b>Dispositivos</b>	<b>271</b>
<b>Puntero</b>	<b>271</b>
<b>Teclado</b>	<b>273</b>
<b>Impresión</b>	<b>291</b>
<b>USB</b>	<b>293</b>
<b>Asignación de unidades de cliente</b>	<b>314</b>
<b>Micrófono</b>	<b>317</b>
<b>Directiva de grupo</b>	<b>317</b>
<b>Experiencia en las sesiones</b>	<b>320</b>
<b>Desktop Lock de la aplicación Citrix Workspace</b>	<b>331</b>
<b>Kit de desarrollo de software (SDK) y API</b>	<b>337</b>
<b>Storebrowse</b>	<b>340</b>

<b>Storebrowse para Workspace</b>	<b>350</b>
<b>Solucionar problemas técnicos</b>	<b>352</b>
<b>Elementos retirados</b>	<b>359</b>

## Acerca de la aplicación Citrix Workspace 2402 LTSR para Windows

June 14, 2024

En esta documentación se describen las funciones y la configuración de la aplicación Citrix Workspace 2402 LTSR para Windows. Esta versión es la versión de servicio a largo plazo (Long Term Service Release, LTSR) más reciente de la aplicación Citrix Workspace para Windows y solo es relevante para los clientes de LTSR.

La documentación de la versión actual (Current Release, CR) de la aplicación Citrix Workspace para Windows está disponible en [Aplicación Citrix Workspace para Windows](#). Para obtener más información sobre los ciclos de vida de las versiones LTSR y CR, consulte [Lifecycle Milestones for Citrix Workspace app](#).

### Nota:

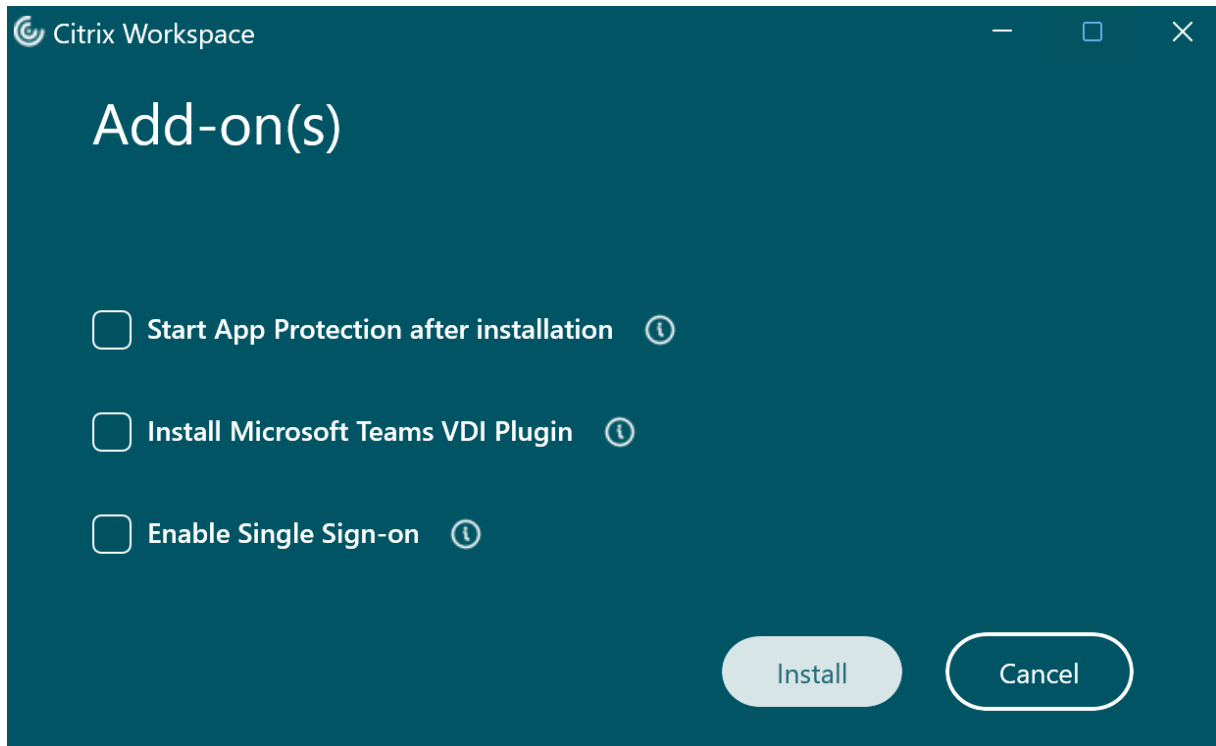
- Si ha habilitado la actualización automática en la aplicación Citrix Workspace y ha optado por el programa LTSR, la aplicación Citrix Workspace 2203.1 LTSR para Windows se actualiza automáticamente a la aplicación Citrix Workspace 2402 LTSR para Windows.
- Si ha habilitado la actualización automática en la aplicación Citrix Workspace y ha optado por el programa Current Release (CR), la versión CR de la aplicación Citrix Workspace se actualiza automáticamente a la aplicación Citrix Workspace 2311.1 para Windows.

## Descargas

[Aplicación Citrix Workspace 2402 LTSR para Windows](#)

## Nuevos complementos y paquetes

Para la aplicación Citrix Workspace para 2402 LTSR, puede instalar el plug-in de optimización de Microsoft Teams, Citrix Enterprise Browser y App Protection desde la página de complementos durante la instalación de la aplicación Citrix Workspace. Puede administrar estos complementos de forma independiente desde la aplicación Citrix Workspace. Por ejemplo, puede actualizarlos o desinstalarlos independientemente de la aplicación Citrix Workspace.



### Redirección de contenido del explorador web (BCR)

Para la versión 2402 LTSR de la aplicación Citrix Workspace:

- Los componentes del cliente BCR no se instalan de forma predeterminada con la interfaz de usuario del instalador de la aplicación Citrix Workspace ni desde la línea de comandos.
- Para las nuevas instalaciones desde la línea de comandos de la aplicación Citrix Workspace, los componentes del cliente BCR con otros componentes necesarios deben especificarse mediante el parámetro de línea de comandos `ADDLOCAL`. Para obtener más información, consulte [Instalar al menos uno de los componentes específicos](#).
- Para la nueva interfaz de usuario del instalador de la aplicación Citrix Workspace, se pueden instalar los componentes del cliente BCR, después de la instalación de {page.cwa}, ejecutando el `BCR_Client.msi` que se encuentra en el directorio `%ProgramFiles(x86)%\Citrix\Citrix Workspace 2402`.
- Si los componentes del BCR se instalaron anteriormente, se actualizarán durante el proceso de instalación.

### Cambio de comportamiento de la optimización de Microsoft Teams

Con la publicación de la aplicación Citrix Workspace 2402 LTSR, los usuarios ahora tienen la opción de instalar el nuevo plug-in de VDI de Microsoft Teams durante la instalación de la aplicación Citrix

Workspace, directamente desde la pantalla de complementos.

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

También puede consultar [Microsoft Teams 2.1 compatible con VDI/DaaS](#).

## Nuevas funciones y mejoras

Para obtener más información sobre las nuevas funciones, los problemas resueltos y los problemas conocidos de esta versión, consulte las secciones a continuación.

- [Novedades de la versión 2402 LTSR](#)
- [Problemas resueltos en la versión 2402 LTSR](#)
- [Problemas conocidos en la versión 2402 LTSR](#)

## Enlaces útiles

- [Tabla de funciones de la aplicación Citrix Workspace](#)
- [Hitos del ciclo de vida para la aplicación Citrix Workspace](#)
- [Información adicional sobre el ciclo de vida de Citrix Receiver para Windows](#)

## Cambios en el nombre y el número de versión de los productos Citrix

Para obtener información sobre los cambios efectuados en 2018 en nombres de producto y números de versión, consulte [Nuevos nombres y números](#).

## Componentes base

---

Componentes base de 2402 LTSR	Versión
Citrix Virtual Apps and Desktops 7 LTSR con CU	1912 LTSR
Citrix Virtual Apps and Desktops 7 LTSR con CU	2203.1 LTSR
Citrix Virtual Apps and Desktops 7 Current Release	2402 CR

---

## Componentes compatibles

Los siguientes componentes son compatibles con los entornos LTSR. Estos componentes no dan derecho a las ventajas de LTSR (ciclo de vida ampliado y actualizaciones acumulativas de correcciones solamente).

---

## Componentes y funciones compatibles

---

Citrix Endpoint Analysis

Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)

Redirección de contenido del explorador web

Citrix Enterprise Browser

---

## Aplicación Citrix Workspace 2402 LTSR para Windows

June 14, 2024

Obtenga información sobre las nuevas funciones y mejoras disponibles para la aplicación Citrix Workspace 2402 LTSR para Windows.

### Importante:

- Citrix Enterprise Browser se puede usar con Citrix Workspace LTSR como componente compatible. No obstante, no se instala de forma predeterminada.

Para instalar Citrix Enterprise Browser, agregue el modificador de instalación `InstallEmbeddedBrowser=Y` o el parámetro `Addlocal` de `CitrixEnterpriseBrowser` como parte de la instalación desde la línea de comandos.

- Para obtener información sobre la instalación del redireccionamiento de contenido del explorador, consulte [Redirección de contenido del explorador web](#).

## Novedades de la versión 2402 LTSR

La siguiente lista muestra las funciones disponibles en la aplicación Citrix Workspace 2402 LTSR para Windows.

### Nota:

Para obtener información sobre los nuevos complementos y cambios en los paquetes, consulte [Nuevos complementos y paquetes](#).

- 2402
  - Iniciativa de sostenibilidad para el inicio híbrido en la nube
  - PassThrough de dominio mejorado para Single Sign-On (SSO mejorado)



- Compatibilidad con directivas avanzadas de NetScaler para Storebrowse en Windows
- Actualización de versión para Chromium Embedded Framework
- Instalar el plug-in VDI de Microsoft Teams para Citrix
- Compartir el audio del sistema en las reuniones (Technical Preview)
- Ocultar la opción de solución de problemas para los usuarios finales
- App Protection
  - \* Lista de permitidos para capturas de pantalla
  - \* Lista de exclusión de procesos
  - \* Lista de exclusión de controladores de filtro USB
- Citrix Endpoint Analysis
- Citrix Enterprise Browser
  - \* Indicador de seguridad al visitar sitios web
  - \* [Citrix Enterprise Browser presenta parámetros adicionales en el servicio Global App Configuration Service] (#Citrix Enterprise Browser presenta parámetros adicionales en Global App Configuration Service)
- 2311.1
  - Presentación del nuevo instalador de la aplicación Citrix Workspace
  - Función de Administrador de actividades en almacenes de la nube
  - Selección automática del códec de vídeo
  - Modo tolerante a pérdidas para audio
  - Sincronice varios teclados al inicio de la sesión
  - Mejora del rendimiento de BCR
  - Actualización de versión para Chromium Embedded Framework
  - Actualización importante sobre los nombres de los archivos y controladores de App Protection
  - Mejora de los efectos y del desenfoco de fondo para la optimización de Microsoft Teams con HDX
  - Citrix Enterprise Browser
    - \* [Experiencia de usuario y tiempo de recarga de sesión mejorados](#)
    - \* [Diseño de marca de agua mejorado](#)
    - \* [Compatibilidad con extensiones de explorador personalizadas](#)
    - \* SSO simplificado para aplicaciones web y SaaS a través de Global App Configuration Service
    - \* [Administrar la autenticación PassThrough en Citrix Enterprise Browser](#)
    - \* [Funciones mejoradas para supervisar las actividades de los usuarios finales](#)

- 2309
  - Requisitos previos adicionales de .NET
  - Experiencia mejorada al iniciar aplicaciones y escritorios virtuales
  - Incorporación de la opción Solución de problemas en la bandeja del sistema de la aplicación Citrix Workspace
  - Iniciativa de sostenibilidad de la aplicación Citrix Workspace
  - Comandos para configurar la sincronización de la distribución del teclado mediante la interfaz de línea de comandos
  - Comando para borrar e instalar la aplicación Citrix Workspace
  - Actualizaciones para Microsoft Teams optimizado
  - App Protection
    - \* Actualización importante sobre los nombres de los archivos
    - \* Detección de manipulación de directivas
    - \* App Protection con escenario de doble salto
  - Citrix Enterprise Browser
    - \* [Autenticación mediante Citrix Enterprise Browser](#)
- 2307
  - Se agregó una función para reproducir tonos cortos en Microsoft Teams optimizado
  - Citrix Enterprise Browser
    - \* [Acceso directo de Citrix Enterprise Browser](#)
- 2305.1
  - Experiencia mejorada al iniciar aplicaciones y escritorios virtuales
  - Seguimiento del estado de los comandos de Storebrowse
  - Compatibilidad con métodos de autenticación modernos para almacenes de StoreFront
  - Compatibilidad con más de 200 grupos en Azure AD
  - App Protection
    - \* Mejora en la protección contra el registro de tecleo
  - Citrix Enterprise Browser
    - \* Compatibilidad con extensiones de explorador
    - \* Modificación en la implementación de directivas de SPA en aplicaciones web y SaaS internas
    - \* Usar Global App Config Service para administrar Citrix Enterprise Browser
- 2303
  - Configurar la ruta para el almacenamiento de datos temporales del explorador web superpuesto de la redirección de contenido del explorador web

- Compatibilidad con métodos de autenticación modernos para almacenes de StoreFront
- Experiencia mejorada para llamadas de videoconferencia en Microsoft Teams optimizado
- Mejora de App Protection: Antiinyección de DLL
- Citrix Enterprise Browser
  - \* Compatibilidad de Secure Private Access con StoreFront
- 2302
  - Experiencia mejorada al reconectar aplicaciones y escritorios virtuales
  - Administración de aplicaciones cliente para el plug-in de Zoom
  - Se ha actualizado el modo de selección de dispositivos de audio para Microsoft Teams optimizado
  - Mejora en App Protection
  - Citrix Enterprise Browser
    - \* Abrir todas las aplicaciones web y SaaS a través de Citrix Enterprise Browser
    - \* Opción para iniciar Citrix Enterprise Browser desde la aplicación Citrix Workspace
- 2212
  - Administración de aplicaciones cliente
  - Control de versiones con actualización automática
  - Forzar solicitud de inicio de sesión para el proveedor de identidades federadas
  - Mejora de la experiencia de reconexión tras la caducidad del archivo de concesión de conexiones
  - Compatibilidad con la instalación predeterminada de App Protection
  - Mejora de App Protection: Detección y notificación de capturas de pantalla
  - Optimización de Desktop Viewer
  - Citrix Enterprise Browser
    - \* [Configurar Citrix Enterprise Browser como explorador de trabajo](#)
- 2210.5
  - Mejora de la actualización automática
- 2210
  - Desenfocado de fondo para la redirección de cámaras web
  - Mejoras en App Protection para aplicaciones web y SaaS en Windows 11
  - Limitar resoluciones de vídeo
  - Cambio de nombre de Citrix Workspace Browser
  - Abrir todas las aplicaciones web y SaaS a través de Citrix Enterprise Browser
  - Función de actualización automática de la aplicación Citrix Workspace en VDA
  - Citrix Enterprise Browser (anteriormente, Citrix Workspace Browser)

- 2207
  - Efectos y desenfoque de fondo para la optimización de Microsoft Teams con HDX
  - Experiencia de actualización automática mejorada
  - Nota sobre la actualización de la aplicación Citrix Workspace
- 2206
  - Rendimiento gráfico mejorado
  - Habilitar la correspondencia de PPP
- 2205
  - Cambio en Citrix Casting
  - Acceso rápido a recursos
  - Cerrar sesión en el almacén web personalizado al salir de la aplicación Citrix Workspace
  - Función para abrir la aplicación Citrix Workspace en modo maximizado
  - Función Storebrowse para Workspace
- 2204.1
  - Mejora en la redirección de audio
  - Optimización de Microsoft Teams

## 2402 LTSR (versión inicial)

### Iniciativa de sostenibilidad para el inicio híbrido en la nube

**Nota:**

Anteriormente, esta función estaba disponible para los inicios nativos (en la nube y locales) a partir de la versión 2309 de la aplicación Citrix Workspace.

Desde la versión 2402 de la aplicación Citrix Workspace, esta función está disponible para inicios híbridos en la nube. Después de habilitar esta función, se muestra un mensaje para cerrar sesión en la sesión de escritorio cuando un usuario cierra un escritorio virtual. Esta función ayuda a ahorrar energía si hay directivas de sistema operativo Windows que se usen para apagar máquinas virtuales cuando estas no tengan usuarios conectados. También puede personalizar el texto que se muestra en la pantalla de **ahorro de energía**. Para obtener más información, consulte [Iniciativa de sostenibilidad para el inicio híbrido en la nube](#).

### PassThrough de dominio mejorado para Single Sign-On (SSO mejorado)

Antes, la aplicación Citrix Workspace para Windows solo permitía la autenticación SSON o la autenticación PassThrough de dominio para Single Sign-On en entornos de Citrix Virtual Apps and Desktops

mediante credenciales de usuario. Esta autenticación permite al usuario autenticarse en el dominio de su dispositivo y usar sus aplicaciones y escritorios virtuales sin tener que autenticarse de nuevo.

Con esta versión, la aplicación Citrix Workspace ofrece un PassThrough de dominio mejorado, que es un nuevo método de SSO. Aprovecha la autenticación de Kerberos en lugar de las credenciales de usuario. Los usuarios ahora pueden iniciar sesión en Citrix Virtual Apps and Desktops y en StoreFront mediante la autenticación de Windows integrada. Para obtener más información, consulte [PassThrough de dominio mejorado para Single Sign-On \(SSO mejorado\)](#).

### Compatibilidad con directivas avanzadas de NetScaler para Storebrowse en Windows

La aplicación Citrix Workspace para Windows ahora admite directivas avanzadas en NetScaler Gateway con Storebrowse. El protocolo de autenticación admitido es la autenticación LDAP. 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. Para obtener más información, consulte [Storebrowse](#).

**Nota:**

El protocolo de autenticación nFactor no es compatible con Storebrowse en Windows.

### Instale el plug-in VDI de Microsoft Teams para Citrix

Ahora puede instalar el plug-in VDI de Microsoft Teams durante la instalación de la aplicación Citrix Workspace mediante una de las siguientes opciones.

- [Uso de la interfaz de usuario](#)
- [Uso de la línea de comandos](#)

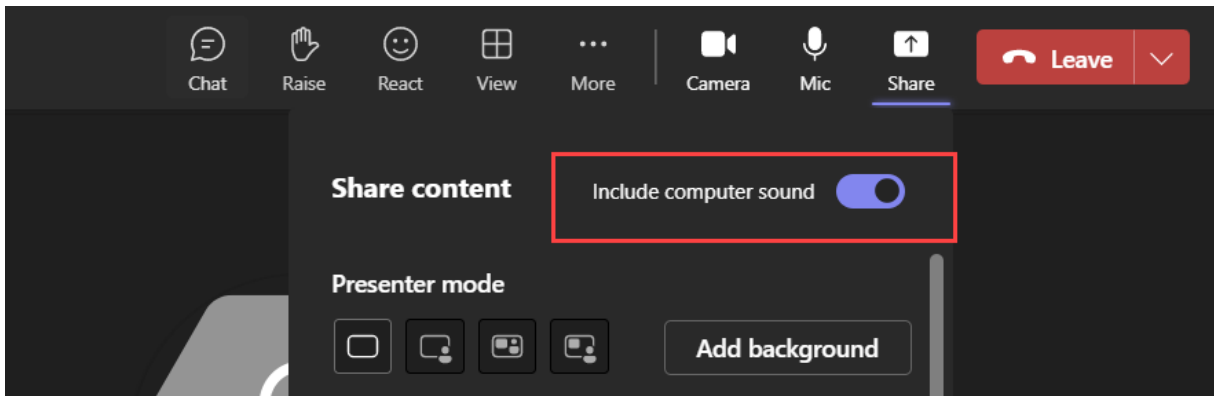
**Nota:**

Para conocer la compatibilidad de las versiones con VDI y los detalles de configuración, consulte [Microsoft Teams 2.1 compatible con VDI/DaaS](#) y [Nuevos requisitos para VDI de Teams](#).

### Compartir el audio del sistema [Technical Preview]

Ahora puede compartir el audio que se reproduce en su VDA con los participantes de una reunión. Seleccione la opción **Incluir sonido del equipo** para que sus reuniones sean más atractivas. Debe habilitar esta función a través del registro estableciendo `HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream\EnableSystemAudio` (DWORD) en 1.

Para los usuarios finales, esta opción no está habilitada de forma predeterminada, sino que deben activarla antes de compartir la pantalla.



### Limitaciones

- El audio no se puede compartir usando esta función cuando se comparte la pantalla con aplicaciones o fichas redirigidas de RAVE y BCR.
- Esta función solo se admite en los escritorios publicados.

#### Nota:

Esta función estará disponible solamente después de la implantación de una futura actualización de Microsoft Teams.

### Ocultar la opción de solución de problemas para los usuarios finales

Los administradores ahora pueden ocultar las opciones de solución de problemas para sus usuarios finales mediante el editor de GPO. Una vez habilitado este parámetro, se oculta la opción de solución de problemas que antes estaba visible para los usuarios finales en la bandeja del sistema. Para obtener más información, consulte [Ocultar la opción de solución de problemas para los usuarios finales](#).

### Retirada de la compatibilidad con PNAgent

A partir de esta versión, se ha retirado la compatibilidad con las URL de XenApp Services (también conocido como PNAgent) para conectarse a almacenes. Use la aplicación Citrix Workspace para conectarse a almacenes mediante la URL de almacén. Para referencia, consulte:

- Página [Elementos retirados](#) en la documentación de la aplicación Citrix Workspace para Windows.
- Página [Avisos de obsolescencia](#) en la documentación de StoreFront.

## **Actualización de versión para Chromium Embedded Framework**

La versión de Chromium Embedded Framework (CEF) se actualizó a la 120. Esta nueva versión ayuda a resolver vulnerabilidades de seguridad.

## **App Protection**

**Lista de permitidos para capturas de pantalla** Si la aplicación Citrix Workspace, las aplicaciones y escritorios virtuales o las aplicaciones SaaS están habilitadas con la directiva anticaptura de pantalla de App Protection, no podrá capturar sus pantallas con ninguna herramienta diseñada para tal fin.

Sin embargo, a partir de la versión 2402 de la aplicación Citrix Workspace para Windows, la función Lista de permitidos para capturas de pantalla le permite agregar una aplicación a la lista de permitidos para capturas de pantalla. Esta función le permite usar la aplicación de la lista de permitidos y capturar la pantalla del recurso habilitado con la directiva anticaptura de pantalla de App Protection. Para obtener más información, consulte [Lista de permitidos para capturas de pantalla](#).

**Lista de exclusión de procesos** Al iniciar cualquier proceso o aplicación en el dispositivo, las DLL de App Protection se inyectan en cada proceso si App Protection está habilitada. En ocasiones, esto puede provocar que el proceso o la aplicación no funcionen debido a problemas de compatibilidad con la DLL.

A partir de la versión 24.02 de la aplicación Citrix Workspace para Windows, puede agregar cualquier proceso a la lista de exclusión de procesos para evitar que las DLL de App Protection se incorporen a ese proceso en particular y evitar problemas de compatibilidad causados por la presencia de las DLL de App Protection. Para obtener más información, consulte [Lista de exclusiones de procesos](#).

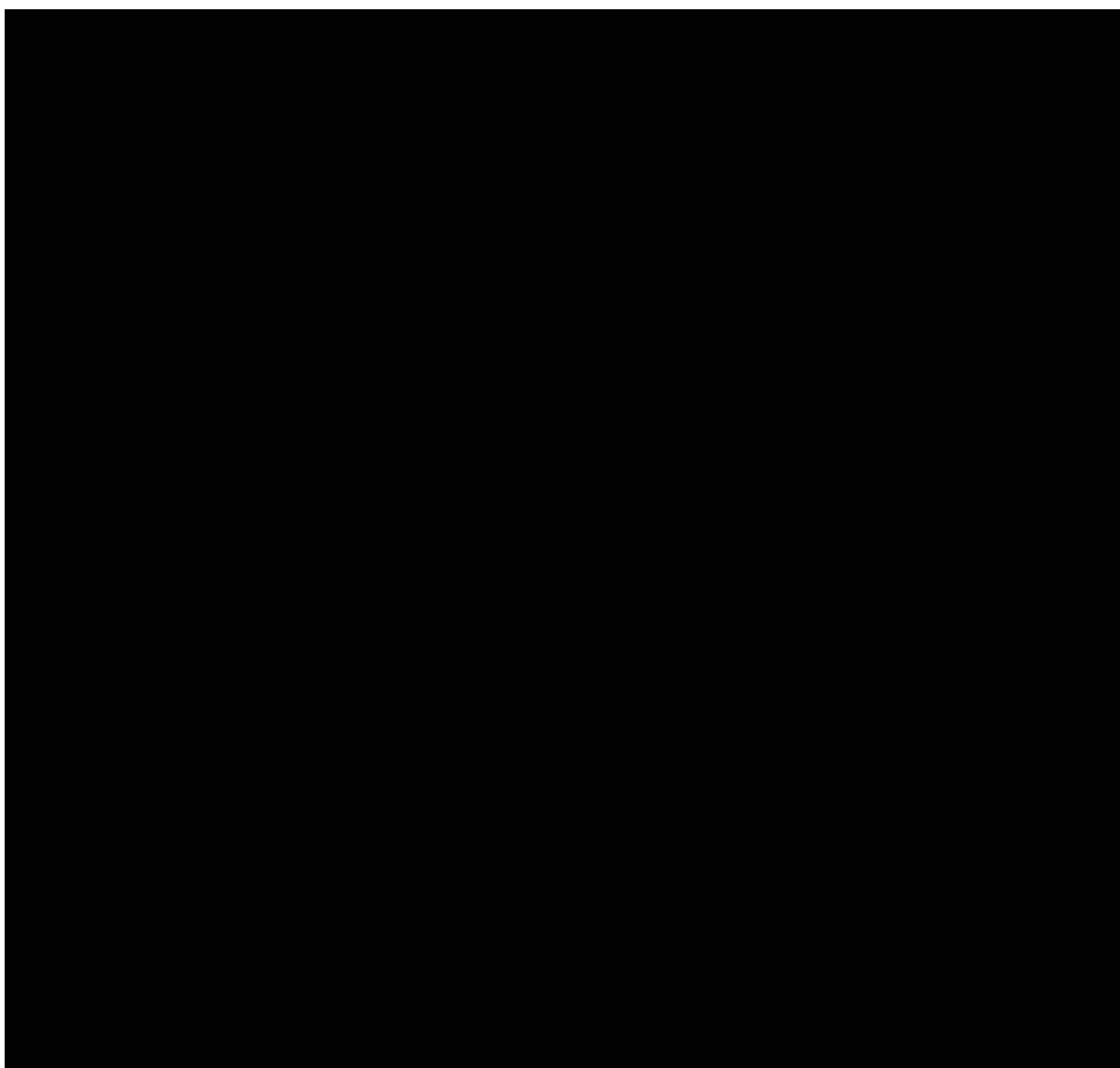
**Lista de exclusión de controladores de filtro USB** A veces, cuando se usan teclados externos especializados, como teclados para juegos, con la aplicación Citrix Workspace, el controlador de filtros USB de App Protection puede provocar problemas de compatibilidad e impedir que el uso del teclado.

A partir de la versión 2402 de la aplicación Citrix Workspace para Windows, la función Lista de exclusión de controladores de filtro USB le permite excluir cualquier dispositivo USB que presente problemas de compatibilidad con la aplicación Citrix Workspace mediante el ID de proveedor y el ID de producto del dispositivo. Para obtener más información, consulte [Lista de exclusiones de controladores de filtro USB](#).

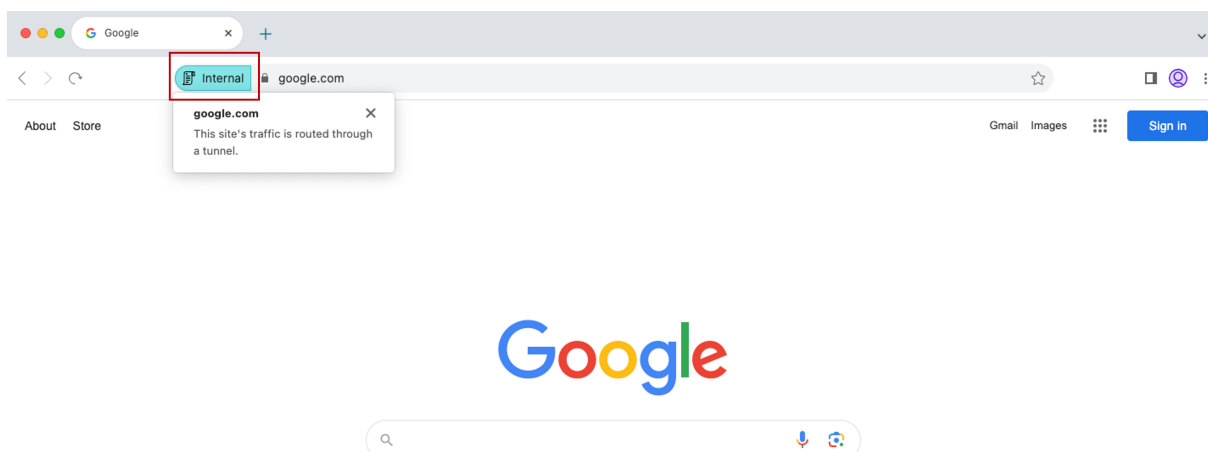
## **Citrix Enterprise Browser**

Esta versión de Citrix Enterprise Browser se instala con la aplicación Citrix Workspace para Windows 2402 y se basa en la versión 122 de Chromium.

**Indicador de seguridad al visitar sitios web** Citrix Enterprise Browser ahora muestra un indicador de seguridad en la barra de direcciones cuando los usuarios visitan cualquier sitio web. El indicador tiene como objetivo informar a los usuarios sobre los aspectos de seguridad de los sitios web, por ejemplo, si se trata de un sitio interno o si existen posibles restricciones de seguridad. El indicador proporciona información adicional al hacer clic en él. El indicador se muestra en Citrix Enterprise Browser de forma predeterminada y mejora la experiencia del usuario.







### **Citrix Enterprise Browser presenta parámetros adicionales en Global App Configuration Service**

Se han agregado parámetros adicionales al Global App Configuration Service (GACS) para configurar Citrix Enterprise Browser.

- Habilitar el relleno automático de la dirección: permite a los administradores habilitar o inhabilitar las sugerencias de relleno automático de la dirección.
- Habilitar el relleno automático de la tarjeta de crédito: permite a los administradores habilitar o inhabilitar las sugerencias de relleno automático de la información de la tarjeta de crédito.
- Iniciar protocolos automáticamente desde los orígenes: permite a los administradores especificar una lista de protocolos que pueden iniciar una aplicación externa desde los orígenes indicados sin preguntar al usuario.
- Habilitar advertencias de seguridad por marcas de línea de comandos: permite a los administradores mostrar u ocultar advertencias de seguridad que se muestran cuando hay marcas de línea de comandos potencialmente peligrosas que intentan iniciar el Enterprise Browser.
- Administrar el parámetro de cookies predeterminadas: permite a los administradores administrar las cookies de un sitio web.
- Administrar el parámetro de ventanas emergentes predeterminadas: permite a los administradores administrar las ventanas emergentes de un sitio web.
- Fuentes de instalación de extensiones: permite a los administradores especificar fuentes válidas para que los usuarios instalen extensiones, aplicaciones y temas.
- Inhabilitar las páginas de advertencia similares: permite a los administradores especificar los dominios preferidos en los que no se muestran páginas de advertencia similares cuando el usuario visita las páginas de ese dominio.
- Habilitar la consulta de métodos de pago: permite a los administradores habilitar sitios web para comprobar si los usuarios han guardado métodos de pago.
- Administrar el almacenamiento del historial del explorador: permite a los administradores gestionar el almacenamiento del historial de Citrix Enterprise Browser.

- Administrar sugerencias de búsqueda: permite a los administradores habilitar o inhabilitar las sugerencias de búsqueda en la barra de direcciones de Citrix Enterprise Browser.
- Habilitar la exportación de marcadores: permite a los administradores habilitar una opción para exportar los marcadores de Enterprise Browser.
- Forzar perfiles efímeros: permite a los administradores borrar o conservar los datos del perfil de usuario cuando los usuarios cierran Citrix Enterprise Browser.

Para obtener más información, consulte la página [Administrar Citrix Enterprise Browser mediante Global App Configuration Service](#) en la documentación de Citrix Enterprise Browser.

Para obtener más información sobre ejemplos de datos JSON, consulte [Ejemplos de datos JSON](#).

### **Citrix Endpoint Analysis**

En esta versión, el cliente EPA se incluye con el instalador de la aplicación Citrix Workspace. Para instalar el cliente, la aplicación Citrix Workspace debe instalarse usando la opción de línea de comandos `InstallePAClient`.

Ejemplo: `./CitrixworkspaceApp.exe InstallePAClient`

**Nota:**

EPA no se instala de forma predeterminada.

En esta versión, la versión de EPA empaquetada es la 23.11.1.20.

### **Función incluida en versiones anteriores**

Esta versión admite algunas funciones que se incluyeron en las versiones 2204.1 a 2311.1 de la aplicación Citrix Workspace para Windows, tal y como se indica a continuación.

#### **2311.1**

En esta versión se agregaron estas funciones:

- [Presentación del nuevo instalador de la aplicación Citrix Workspace](#)
- [Función de Administrador de actividades en almacenes de la nube](#)
- [Selección automática del códec de vídeo](#)
- [Modo tolerante a pérdidas para audio](#)
- [Sincronice varios teclados al inicio de la sesión](#)
- [Mejora del rendimiento de BCR](#)
- [Actualización de versión para Chromium Embedded Framework](#)

- [Actualización importante sobre los nombres de los archivos de App Protection](#)
- [Citrix Enterprise Browser](#)
  - [Experiencia de usuario y tiempo de recarga de sesión mejorados](#)
  - [Diseño de marca de agua mejorado](#)
  - [Compatibilidad con extensiones de explorador personalizadas](#)
  - [SSO simplificado para aplicaciones web y SaaS a través de Global App Configuration Service](#)
  - [Administrar la autenticación PassThrough en Citrix Enterprise Browser](#)
  - [Funciones mejoradas para supervisar las actividades de los usuarios finales](#)

**Nota:**

A partir de la versión 2311.1 de la aplicación Citrix Workspace para Windows, se retiró la redirección de contenido de explorador basada en Internet Explorer. La opción alternativa es utilizar la redirección de contenido de explorador basada en Google Chrome.

## **Presentación del nuevo instalador de la aplicación Citrix Workspace**

La interfaz de usuario del instalador de la aplicación Citrix Workspace se ha renovado para ofrecer un aspecto moderno e intuitivo, y una mejor experiencia de usuario. De forma predeterminada, el nuevo instalador está habilitado.

### **Requisitos previos:**

.Net Desktop Runtime 6.0.20 o posterior es un requisito previo adicional para el nuevo instalador. Para conocer otros requisitos, consulte la sección [Requisitos del sistema](#).

El nuevo instalador está habilitado de forma predeterminada. Para obtener más información, consulte [Instalación basada en la interfaz de usuario](#).

**Nota:**

A partir de la versión 2311.1 de la aplicación Citrix Workspace para Windows, el `TrolleyExpress` se reemplaza por `CWAInstaller-<date and timestamp>`. Por ejemplo, el registro se graba en `C:\Program Files (x86)\Citrix\Logs\CTXWorkspaceInstallLogs-20231225-093441`.

## **Función de Administrador de actividades en almacenes de la nube**

La aplicación Citrix Workspace para Windows es compatible con la función Activity Manager. Esta función permite a los usuarios finales ver todas sus aplicaciones y sesiones de escritorio activas e interactuar con ellas en un solo lugar. Para ver las sesiones activas en el **Administrador de actividades**, haga clic en el icono del **Administrador de actividades**. Puede realizar las siguientes acciones en

una aplicación o un escritorio al hacer clic en el botón de puntos suspensivos (...) correspondiente del Administrador de actividades:

- **Cerrar sesión:** Cierra la sesión en curso. Se cierran todas las aplicaciones de la sesión, y se pierden los archivos no guardados.
- **Desconectar:** La sesión remota se desconecta, pero las aplicaciones y los escritorios están activos en segundo plano.
- **Reiniciar:** Apaga el escritorio y lo inicia de nuevo.
- **Apagar:** Cierra los escritorios desconectados.
- **Forzar cierre:** apaga el escritorio por la fuerza si hay algún problema técnico.
- Haga clic en el botón **X** para terminar la sesión activa de la aplicación desde el Administrador de actividades.

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

**Nota:**

Esta función solo está disponible en la aplicación Citrix Workspace para Windows si la [nueva experiencia del espacio de trabajo](#) está habilitada.

### Selección automática del códec de vídeo

Con esta versión, la aplicación Citrix Workspace para Windows ahora detecta automáticamente el mejor códec de vídeo que se puede usar. Durante la instalación de la aplicación Citrix Workspace para Windows, se evalúan las capacidades de decodificación del dispositivo de punto final. En función de esta información, la aplicación Citrix Workspace para Windows selecciona el mejor códec para usar con el VDA cuando se inicia la sesión. Este es el orden en el que se evalúan los códecs de vídeo:

1. AV1
2. H.265
3. H.264

Esta función está disponible cuando la directiva **Usar códec de vídeo para compresión** está establecida en una de las siguientes opciones:

- **Usar si se prefiere**
- **Para la pantalla entera**
- **Para áreas en cambio constante**

Para obtener más información sobre la directiva **Usar códec de vídeo para la compresión**, consulte [Usar códec de vídeo para la compresión](#).

La selección automática solo se aplica a las variantes YUV 4:2:0 de estos códecs. YUV 4:2:0 utiliza menos ancho de banda, lo que puede afectar la calidad. Si la configuración de la directiva de **Calidad visual** está establecida en **Gradual sin pérdida** o **Siempre sin pérdida** y si la directiva **Permitir**

**sin pérdida visual** está establecida en **habilitada**, la selección automática del códec de vídeo está inhabilitada y, en su lugar, se utiliza YUV 4:4:4 H.264 o H.265.

Para obtener más información sobre estas directivas, consulte lo siguiente:

- [Calidad visual](#)
- [Permitir compresión sin pérdida visual](#)

Esta función está habilitada de manera predeterminada.

Para obtener más información, consulte [Selección automática del códec 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. El códec de vídeo H.265 debe ser compatible y estar habilitado tanto en el VDA como en la aplicación Citrix Workspace.

A partir de la versión 2311.1 de la aplicación Citrix Workspace, esta función se habilita automáticamente con la introducción de la función de **selección automática de códec de vídeo**.

Para obtener más información, consulte la documentación de [H.265](#).

**AV1** La aplicación Citrix Workspace es compatible con el uso del códec de vídeo AV1 para la aceleración de hardware de vídeos y gráficos remotos. El códec de vídeo AV1 debe ser compatible y estar habilitado tanto en el VDA como en la aplicación Citrix Workspace.

A partir de la versión 2311.1 de la aplicación Citrix Workspace, esta función se habilita automáticamente con la introducción de la función de **selección automática de códec de vídeo**.

Para obtener más información, consulte la documentación de [AV1](#).

### **Modo tolerante a pérdidas para audio**

Con esta versión, la aplicación Citrix Workspace incluye el modo tolerante a pérdidas (EDT con pérdidas) para la redirección de audio. Esta función mejora la experiencia del usuario para la transmisión en tiempo real cuando los usuarios se conectan a través de redes con alta latencia y pérdida de paquetes.

Debe usar la versión del VDA 2311 o posterior. De forma predeterminada, esta función está habilitada en la aplicación Citrix Workspace para Windows. Sin embargo, está inhabilitada en el VDA.

Para obtener más información, consulte la documentación sobre el [Modo tolerante a pérdidas para audio](#).

### **Sincronice varios teclados al inicio de la sesión**

Antes, solo el teclado activo del cliente se sincronizaba con el VDA una vez iniciada la sesión en modo de pantalla completa. En este caso, si configuró **Sincronizar solo una vez - cuando se inicia la sesión** en la aplicación Citrix Workspace y tuvo que cambiar a un teclado diferente, debe instalar manualmente el teclado en el escritorio remoto. Del mismo modo, si configuró **Permitir sincronización dinámica** en la aplicación Citrix Workspace, debe pasar al modo de ventana, cambiar el teclado del cliente y, a continuación, volver al modo de pantalla completa.

Con esta versión, todos los teclados disponibles en el cliente se sincronizan con el VDA una vez que se inicia la sesión en modo de pantalla completa. Puede seleccionar el teclado necesario de la lista de teclados instalados o disponibles en el cliente una vez que se inicie la sesión en modo de pantalla completa.

Para obtener más información, consulte la documentación [Sincronizar varios teclados al iniciar la sesión](#).

### **Mejora del rendimiento de BCR**

Antes, BCR utilizaba la caché de espacio en disco del lado del cliente y la información almacenada en caché no se eliminaba durante una actualización de versión. Este parámetro tuvo como resultado un mayor uso del espacio en disco a lo largo del tiempo y un comportamiento incoherente al redireccionar una página mediante BCR.

En esta versión, para resolver este problema, BCR usa una caché en memoria. Esta mejora ayuda a mejorar el rendimiento del BCR.

Esta función está inhabilitada de forma predeterminada.

Para obtener más información, consulte [Mejora del rendimiento del BCR](#).

### **Actualización de versión para Chromium Embedded Framework**

La versión de Chromium Embedded Framework (CEF) se actualizó a la 117. Esta nueva versión ayuda a resolver vulnerabilidades de seguridad.

### **Actualización importante sobre los nombres de los archivos y controladores de App Protection**

A partir de la aplicación Citrix Workspace para Windows 2311.1, los siguientes nombres de archivos y controladores se actualizan así:

Nombre existente	Nuevo nombre
EntryProtect.dll	ctxapdotnet.dll
entryprotect.sys	ctxapdriver.sys
epclient32.dll	ctxapclient32.dll
epclient64.dll	ctxapclient64.dll
epinject.sys	ctxapinject.sys
epusbfilter.sys	ctxapusbfilter.sys
entryprotectdrv	ctxapdriver
epinject6	ctxapinject

Estos archivos se instalan en %ProgramFiles(x86)%\Citrix\ICA Client de forma predefinida.

Si agregó alguno de los nombres de archivo o controlador anteriores a la lista de permitidos de su entorno, actualice la lista de permitidos.

### **Mejora de los efectos y del desenfoco de fondo para la optimización de Microsoft Teams con HDX**

A partir de la versión 2311.1 de la aplicación Citrix Workspace, puede seleccionar las siguientes opciones para el desenfoco y los efectos de fondo:

- Sin efectos de fondo
- Seleccione el desenfoco de fondo
- Seleccione la imagen de fondo

### **Citrix Enterprise Browser**

Esta versión incluye la versión 119.1.1.60 de Citrix Enterprise Browser, basada en la versión 115 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de [Citrix Enterprise Browser](#)

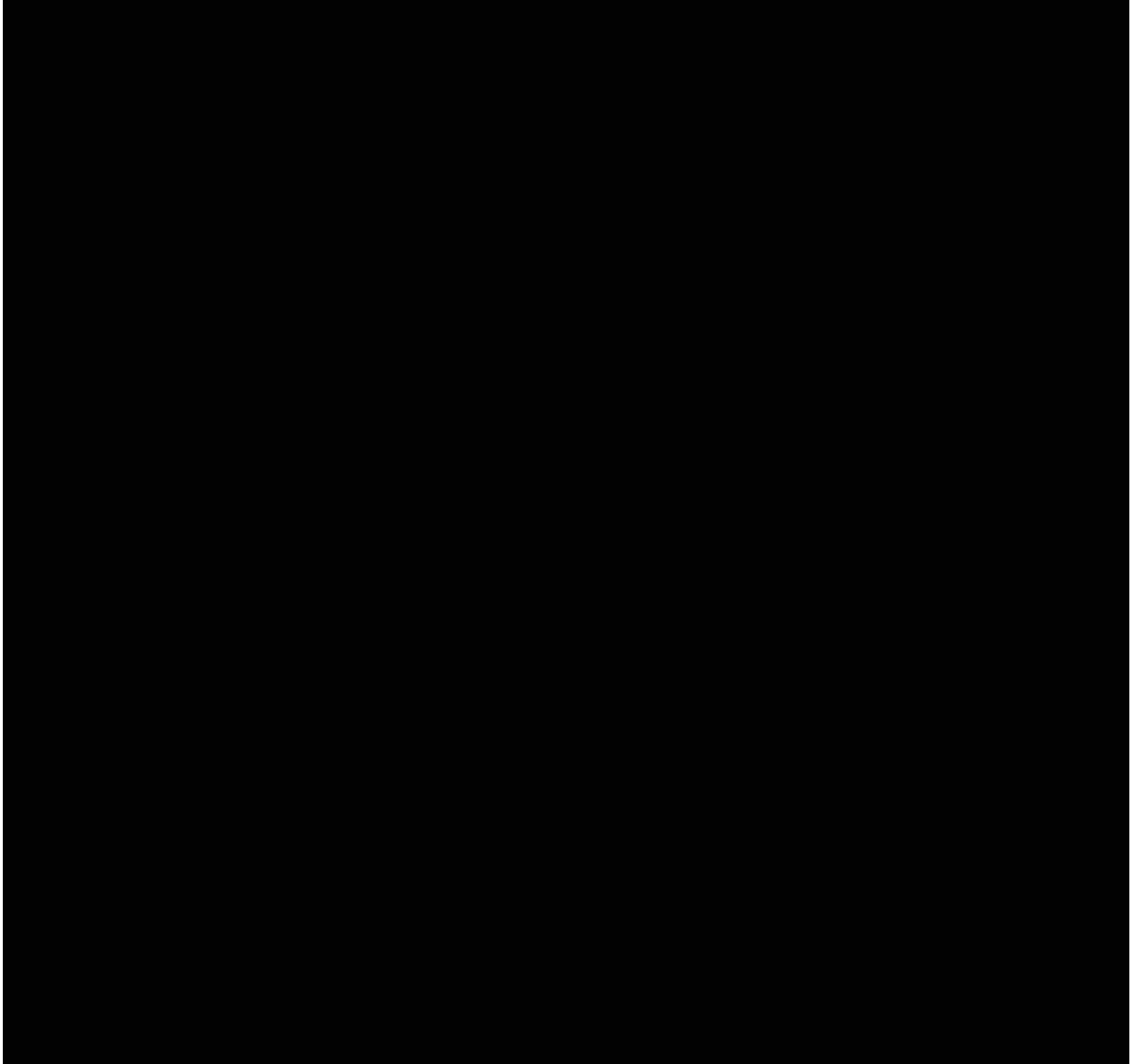
.

### **Citrix Enterprise Browser presenta parámetros adicionales en Global App Configuration Service**

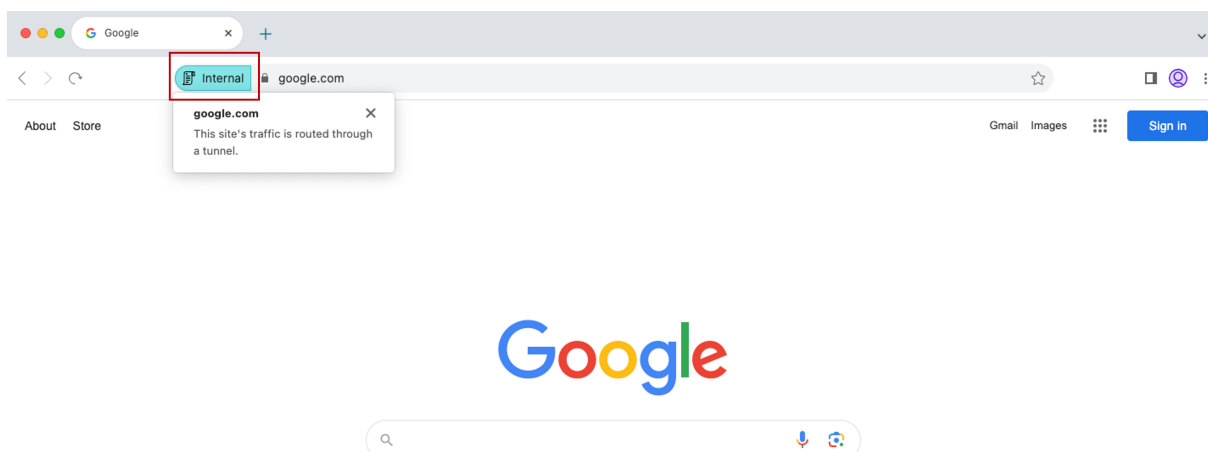
Se han agregado parámetros adicionales al Global App Configuration Service (GACS) para configurar Citrix Enterprise Browser. Para obtener más información, consulte [Administrar Citrix Enterprise Browser mediante GACS](#).

### **Indicador de seguridad al visitar sitios web**

Citrix Enterprise Browser ahora muestra un indicador de seguridad en la barra de direcciones cuando los usuarios visitan cualquier sitio web. Este indicador tiene como objetivo informar a los usuarios acerca de los aspectos de seguridad de los sitios web, por ejemplo, si se trata de un sitio interno o si existen posibles restricciones de seguridad. El indicador proporciona información adicional al hacer clic en él. El indicador se muestra en Citrix Enterprise Browser de forma predeterminada y mejora la experiencia del usuario.







**Experiencia de usuario mejorada** Anteriormente, Citrix Enterprise Browser mostraba un modal de reconexión cuando intentaba realizar una acción después de que caducara la sesión. A partir de la versión 2311.1 de la aplicación Citrix Workspace para Windows (que corresponde a la versión 119.1.1.60 de Chromium), ya no existe la reconexión modal. En su lugar, ahora aparece un icono de carga en la ficha del explorador cuando intentas realizar cualquier acción después de que caduque la sesión.

**Diseño de marca de agua mejorado** Citrix Enterprise Browser ahora tiene un nuevo diseño de marca de agua que es menos intrusivo y proporciona una mejor experiencia de usuario.

**Compatibilidad con extensiones de explorador personalizadas** Citrix Enterprise Browser ha ampliado sus capacidades de extensión. Antes solo se permitían las extensiones de Chrome Web Store. Citrix Enterprise Browser ahora le permite agregar extensiones personalizadas de forma segura. Los administradores pueden configurar extensiones personalizadas como parte de la lista obligatoria. Los usuarios finales pueden acceder a estas extensiones y utilizarlas mediante `citrixbrowser://extensiones` o haciendo clic en la opción **Extensiones** situada debajo del botón **Más**, según sea necesario. Para obtener más información sobre cómo configurar las extensiones personalizadas, consulte [Extensión personalizada obligatoria](#).

### **SSO simplificado para aplicaciones web y SaaS a través de Global App Configuration Service**

Antes el Single Sign-On (SSO) se configuraba para Citrix Enterprise Browser mediante el módulo PowerShell. Ahora, esta función de SSO simplificada le permite configurar el SSO en Citrix Enterprise Browser mediante un parámetro recientemente introducido en el Global App Configuration Service (GACS). Los administradores pueden usar este nuevo parámetro para habilitar el SSO en todas las aplicaciones web y SaaS en Citrix Enterprise Browser. Este método elimina la necesidad del complejo módulo PowerShell. Para obtener más información sobre cómo administrar el Single Sign-On a través del GACS, consulte [Administrar el Single Sign-On para aplicaciones web y SaaS a través del Global App Configuration Service](#).

**Nota:**

Es recomendable que reinicie la aplicación Citrix Workspace cuando modifique los parámetros del Citrix Enterprise Browser en GACS. No obstante, también puede esperar a que finalice la actualización automática. Para obtener más información sobre la duración de la sincronización de las directivas obtenidas de GACS, consulte [Frecuencia de actualización de los parámetros](#).

**Ampliación de la funcionalidad simplificada de Single Sign-On a StoreFront** La función de Single Sign-On (SSO) ya está disponible para StoreFront, lo que garantiza una experiencia de SSO unificada. Esta nueva función elimina la necesidad de que los usuarios se autenticuen por separado cuando acceden a las aplicaciones a través de StoreFront. Para facilitar esta función de SSO, utilice el mismo proveedor de identidades (IdP) para las aplicaciones web y SaaS y para StoreFront. Para obtener más información sobre cómo administrar el Single Sign-On a través del GACS, consulte [Administrar el Single Sign-On para aplicaciones web y SaaS a través del Global App Configuration Service](#).

**Administrar la autenticación PassThrough en Citrix Enterprise Browser** La autenticación PassThrough (PTA) es una función de Azure AD Connect. La PTA es un método de autenticación en el que las credenciales de usuario se pasan de la máquina cliente al servidor. Nunca lo ve tal como sucede en el back-end. En este método, la máquina cliente se comunica directamente con el servidor de autenticación para validar las credenciales del usuario. La PTA se utiliza normalmente cuando el equipo cliente y el servidor de autenticación confían el uno en el otro, y el equipo cliente se considera seguro. Para obtener más información sobre la autenticación PassThrough de Microsoft Azure AD, consulte el [Single Sign-On de conexión directa de Microsoft Entra](#).

Para facilitar la autenticación PassThrough, necesita la extensión Cuentas de Windows para interactuar con las aplicaciones que requieren acceso basado en Azure AD en Enterprise Browser. El administrador debe configurar esta extensión de [cuentas de Windows](#) como parte de la lista obligatoria de **ExtensionInstallForcelist**. Para obtener más información sobre la configuración de las extensiones obligatorias, consulte [Extensión obligatoria](#).

**Funciones mejoradas para supervisar las actividades de los usuarios finales** Antes los administradores no podían supervisar las actividades de los usuarios finales, como el acceso a aplicaciones y el tipo de tráfico. A partir de la versión 2311.1 de la aplicación Citrix Workspace para Windows (correspondiente a la versión 119.1.1.60 de Chromium), ahora también puede supervisar estos detalles.

- **Acceso a aplicaciones:** Enterprise Browser proporciona información sobre todas las aplicaciones a las que accedió el usuario final, siempre que la aplicación aparezca en el documento de directiva.

- **Tipo de tráfico:** Enterprise Browser proporciona información sobre si los datos se envían directamente o mediante la autenticación de Secure Private Access.

Para supervisar las actividades de los usuarios finales desde Enterprise Browser, utilice el servicio Citrix Analytics con su cuenta de Citrix Cloud. Tras iniciar sesión en Citrix Cloud, vaya a **Analytics > Seguridad > Búsqueda**. Allí, puede consultar **Aplicaciones y escritorios** en la sección **Búsqueda de autoservicio**. Para obtener más información sobre Citrix Analytics, consulte [Primeros pasos](#).

## 2309.1

### Novedades

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

### Citrix Enterprise Browser

Esta versión incluye la versión 117.1.1.13 de Citrix Enterprise Browser, basada en la versión 117 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de [Citrix Enterprise Browser](#).

## 2309

### Novedades

#### Nota:

A partir de esta versión, asegúrese de que la versión de Microsoft Edge WebView2 Runtime sea 117 o una posterior. Le recomendamos instalar la versión más reciente para obtener nuevas funcionalidades y correcciones relacionadas con la seguridad.

En esta versión se agregaron estas funciones:

- [Requisitos previos adicionales de .NET](#)
- [Experiencia mejorada al iniciar aplicaciones y escritorios virtuales](#)
- [Incorporación de la opción Solución de problemas en la bandeja del sistema de la aplicación Citrix Workspace](#)
  - [Enviar comentarios sobre la aplicación Citrix Workspace](#)
- [Iniciativa de sostenibilidad de la aplicación Citrix Workspace](#)
- [Configurar la sincronización de la distribución del teclado mediante la interfaz de línea de comandos](#)

- [Comando para borrar e instalar la aplicación Citrix Workspace](#)
- [App Protection](#)
  - [Actualización importante sobre los nombres de los archivos](#)
  - [Detección de manipulación de directivas](#)
  - [Caso de App Protection con DoubleHop](#)
- [Citrix Enterprise Browser](#)
  - [Autenticación mediante Citrix Enterprise Browser](#)

**Requisitos previos adicionales de .NET** Además de .NET Framework 4.8, la aplicación Citrix Workspace requiere la versión x86 de .NET Desktop Runtime 6.0 para los sistemas x86 y x64 con privilegios de administrador. Para obtener más información, consulte [Requisitos de .NET](#).

### Experiencia mejorada al iniciar aplicaciones y escritorios virtuales

**Nota:**

A partir de la versión 2305.1 y posteriores de la aplicación Citrix Workspace, esta función está disponible de forma general para almacenes de la nube y, a partir de la versión 2309, para almacenes locales.

Antes, el cuadro de diálogo de progreso del inicio no era intuitivo para los usuarios. Les hacía creer que el proceso de inicio no respondía, y estos cerraban el cuadro de diálogo, ya que los mensajes de notificación eran estáticos.

La experiencia mejorada al iniciar aplicaciones y escritorios es más informativa, moderna e intuitiva en la aplicación Citrix Workspace para Windows. Esta funcionalidad ayuda a mantener a los usuarios informados con datos relevantes y oportunos sobre el estado del inicio.

Para obtener más información, consulte [Experiencia mejorada al iniciar aplicaciones y escritorios virtuales](#).

**Incorporación de la opción Solución de problemas en la bandeja del sistema de la aplicación Citrix Workspace** Presentamos la opción **Solución de problemas** para mejorar la experiencia del usuario y proceder fácilmente a la solución de problemas. Puede hacer clic con el botón secundario en el icono de la aplicación Citrix Workspace de la bandeja del sistema que se encuentra en la esquina inferior derecha de la pantalla y, a continuación, seleccionar **Solución de problemas** para acceder a ella.

Las opciones disponibles en Solución de problemas son:

- Enviar comentarios
- Recopilar registros

- Comprobar configuración
- Restablecer datos de la aplicación
- Ayuda

**Enviar comentarios sobre la aplicación Citrix Workspace** La opción **Enviar comentarios** le permite informar a Citrix de cualquier problema que pueda surgir al usar la aplicación Citrix Workspace. También puede enviar sugerencias para ayudarnos a mejorar su experiencia en la aplicación Citrix Workspace.

Para obtener más información, consulte [Incorporación de la opción Solución de problemas en la bandeja del sistema de la aplicación Citrix Workspace](#).

**Iniciativa de sostenibilidad de la aplicación Citrix Workspace** Cuando esta función está habilitada, se muestra un mensaje para cerrar sesión en la sesión de escritorio cuando un usuario cierra un escritorio virtual. Es posible que esta función ayude a ahorrar energía si hay directivas de sistema operativo Windows que se usen para apagar máquinas virtuales cuando estas no tengan usuarios conectados.

Para obtener más información, consulte [Iniciativa de sostenibilidad de la aplicación Citrix Workspace](#).

**Comandos para configurar la sincronización de la distribución del teclado mediante la interfaz de línea de comandos** Antes, solo podía configurar la sincronización de la distribución del teclado mediante la GUI o tras actualizar el archivo de configuración. En esta versión, presentamos los nuevos comandos para configurar la sincronización de la distribución del teclado mediante la interfaz de línea de comandos.

Para obtener más información, consulte [Configurar la sincronización de la distribución del teclado mediante la interfaz de línea de comandos](#).

**Comando para borrar e instalar la aplicación Citrix Workspace** Use el comando `/CleanInstall` para borrar rastros que hayan quedado, como archivos y valores del Registro, de una desinstalación anterior y, a continuación, instale de nuevo la nueva versión de la aplicación Citrix Workspace.

Por ejemplo:

```
1 CitrixWorkspaceApp.exe /CleanInstall
2 <!--NeedCopy-->
```

## Actualizaciones para Microsoft Teams optimizado

**Próximo fin de vida (EOL) de la función de ventana única en Microsoft Teams** El 31 de enero de 2024, Microsoft retirará la compatibilidad de Microsoft Teams con la interfaz de usuario de ventana única cuando se utilice la optimización de Microsoft Teams en entornos de imagen de disco virtual (VDI) y solo admitirá la experiencia multiventana. Debe usar una versión de Citrix Virtual Apps and Desktops y de la aplicación Citrix Workspace que admita la función de ventanas múltiples para seguir usando determinadas funcionalidades de Microsoft Teams optimizado. Para obtener más información, consulte [Próximo fin de vida \(EOL\) de la función de ventana única en Microsoft Teams](#).

**Anuncio de obsolescencia del formato SDP (Plan B) en WebRTC** Citrix tiene previsto retirar la compatibilidad con el formato SDP (Plan B) en WebRTC en versiones futuras. Debe usar una versión de la aplicación Citrix Workspace que sea compatible con el plan Unified para seguir usando determinadas funcionalidades de Microsoft Teams optimizado. Para obtener más información, consulte [Anuncio de obsolescencia del formato SDP \(Plan B\) en WebRTC](#).

## App Protection

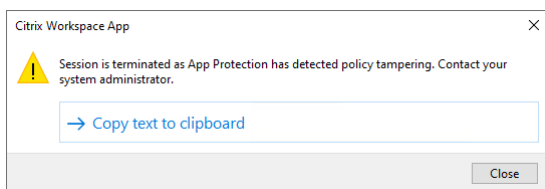
**Actualización importante sobre los nombres de los archivos** En una versión futura de la aplicación Citrix Workspace para Windows, se actualizarán estos nombres de archivo de esta manera:

Nombre de archivo existente	Nombre de archivo nuevo
EntryProtect.dll	ctxapdotnet.dll
entryprotect.sys	ctxapdriver.sys
epclient32.dll	ctxapclient32.dll
epclient64.dll	ctxapclient64.dll
epinject.sys	ctxapinject.sys
epusbfilter.sys	ctxapusbfilter.sys
entryprotectdrv	ctxapdriver
epinject6	ctxapinject

Estos archivos se instalan en %ProgramFiles(x86)%\Citrix\ICA Client de forma predefinida.

Si agregó alguno de los nombres de archivo anteriores a la lista de permitidos de su entorno, actualice la lista de permitidos.

**Detección de manipulación de directivas** La función de detección de manipulación de directivas impide que el usuario acceda a sesiones de escritorio o de aplicación virtual si se alteran las directivas de App Protection de protección contra capturas de pantalla y el registro de teclado. Si se detecta una alteración de las directivas, la sesión de escritorio o aplicación virtual finalizará y mostrará este mensaje de error:



**Nota:**

Esta función solo estará disponible después de la publicación de la próxima versión de Citrix Virtual Apps and Desktops.

Para obtener más información sobre la función de detección de manipulación de directivas, consulte [Detección de manipulación de directivas](#).

**Función total de uso compartido de escritorios desde VDA con la aplicación Citrix Workspace**

Antes, cuando App Protection estaba habilitada, el uso compartido del escritorio estaba inhabilitado para Microsoft Teams optimizado, ya que App Protection no le permitía hacer capturas de la pantalla.

A partir de la versión 2309 y posteriores de la aplicación Citrix Workspace para Windows, el uso compartido del escritorio está habilitado para Microsoft Teams optimizado aunque App Protection esté habilitada.

Para obtener más información, consulte [Compatibilidad con la optimización de HDX para Microsoft Teams](#).

**Caso de App Protection con DoubleHop** Las funciones de App Protection no están disponibles en casos de doble salto. “Doble salto” significa una sesión de Citrix Virtual Apps o Virtual Desktops que se ejecuta dentro de una sesión de Citrix Virtual Desktops. Antes, podía iniciar aplicaciones y escritorios virtuales habilitados con directivas de App Protection en casos de doble salto. No obstante, las funciones de App Protection no se aplicaban.

Ahora, presentamos una directiva de grupos de Windows que permite bloquear el inicio de aplicaciones y escritorios virtuales habilitados con directivas de App Protection en casos de doble salto. Para obtener más información sobre cómo habilitar el parámetro **Bloquear inicio de doble salto**, consulte [Habilitar el parámetro Bloquear inicio de doble salto](#).

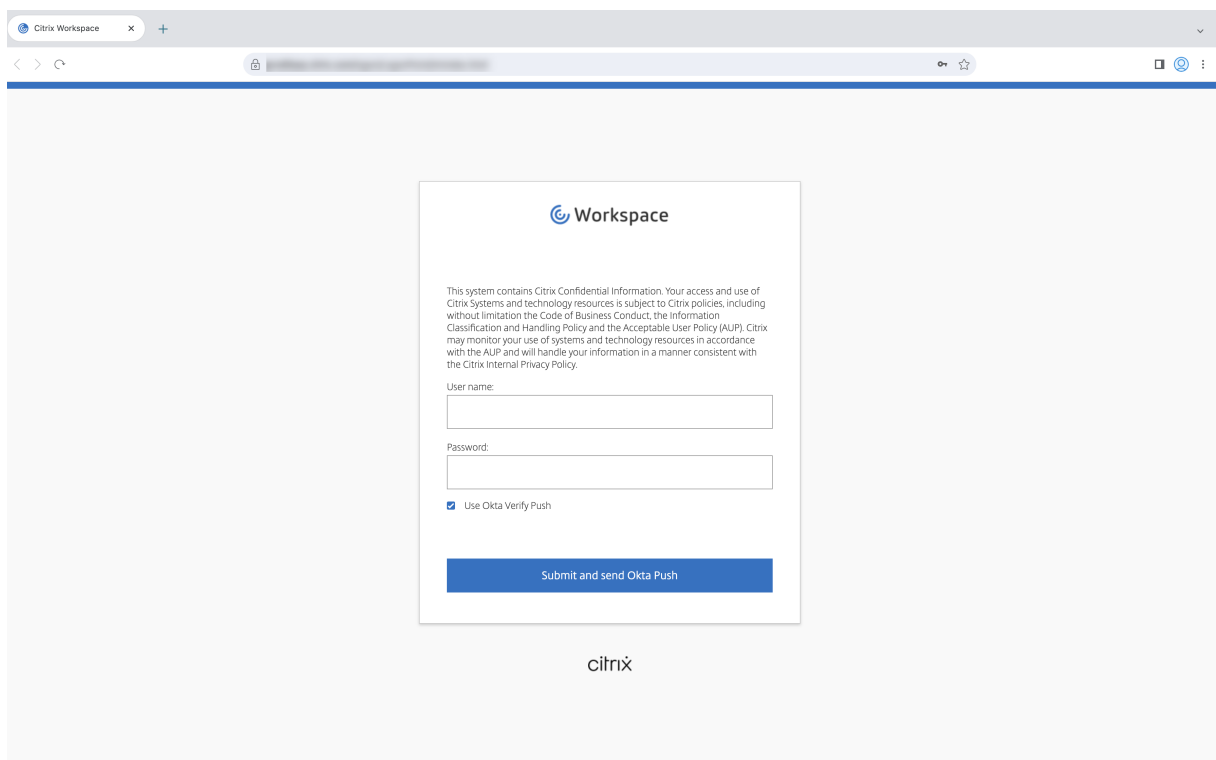
**Citrix Enterprise Browser** Esta versión incluye la versión 117.1.1.9 de Citrix Enterprise Browser, basada en la versión 117 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de [Citrix Enterprise Browser](#).

**Autenticación mediante Citrix Enterprise Browser** Antes, si el token de autenticación de la aplicación Citrix Workspace caducaba, no se podía usar Enterprise Browser. Tenía que cambiar a la aplicación Citrix Workspace y autenticarse de nuevo para seguir utilizando Enterprise Browser.

A partir de la versión 2309 de la aplicación Citrix Workspace para Windows (que corresponde a la versión 117.1.1.9 de Chromium), puede autenticarse en el propio Enterprise Browser solo cuando el almacén siga siendo el mismo. También garantiza la autenticación en la aplicación Citrix Workspace. Además, esta función proporciona una experiencia de inicio de sesión fluida.

**Nota:**

- Esta función se aplica a los almacenes de Workspace.





## 2307.1

### Novedades

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

## 2307

### Novedades

**Se agregó una función para reproducir tonos cortos en Microsoft Teams optimizado** Antes, con la función de tono de llamada secundario habilitada, los tonos cortos, como los pitidos o las notificaciones, se reproducían una y otra vez. Por ejemplo, se repetía el tono que se escuchaba cuando se unían invitados a las reuniones de Microsoft Teams. La única alternativa era cerrar y reiniciar Microsoft Teams. Este problema provocaba una mala experiencia para el usuario final.

Con esta versión, la aplicación Citrix Workspace permite reproducir los tonos cortos como quiera. Esta función también habilita los tonos de llamada secundarios.

### Requisitos previos:

Actualice Microsoft Teams a la versión más reciente.

#### Nota:

La función anterior solo está disponible después de la implantación de la actualización correspondiente de Microsoft Teams. Consulte la actualización de la documentación y el anuncio en [CTX253754](#).

**Citrix Enterprise Browser** Esta versión incluye la versión 112.1.1.24 de Citrix Enterprise Browser, basada en la versión 112 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de [Citrix Enterprise Browser](#).

**Acceso directo de Citrix Enterprise Browser** A partir de la versión 2307 de la aplicación Citrix Workspace para Windows, los administradores pueden configurar y controlar la presencia del acceso directo de Citrix Enterprise Browser en el menú **Inicio**.

#### Nota:

De forma predeterminada, este parámetro está habilitado para almacenes de Workspace.

**Configuración** Un administrador de TI puede configurar la presencia del acceso directo de Citrix Enterprise Browser de una de estas maneras:

- Objeto de directiva de grupo (GPO)
- Global App Configuration Service (GACS)
- web.config.file.

**Notas:**

- Todos los métodos de configuración tienen la misma prioridad. Al habilitar uno, se habilita el acceso directo.
- Si no ha configurado el acceso directo, pero tiene al menos un almacén de Workspace, el acceso directo se habilita automáticamente.
- Para los usuarios finales, el acceso directo de Citrix Enterprise Browser aparece si el usuario lo convierte en una aplicación favorita, independientemente de la configuración.
- Para inhabilitar esta función en almacenes de Workspace, los administradores deben aplicar uno de estos parámetros:
  - set the **CEBShortcutEnabled** attribute to **false** in the **web.config** file.
  - disable the **Enable Citrix Enterprise Browser shortcut** property in GPO and GACS.

Mediante un objeto de directiva de grupo

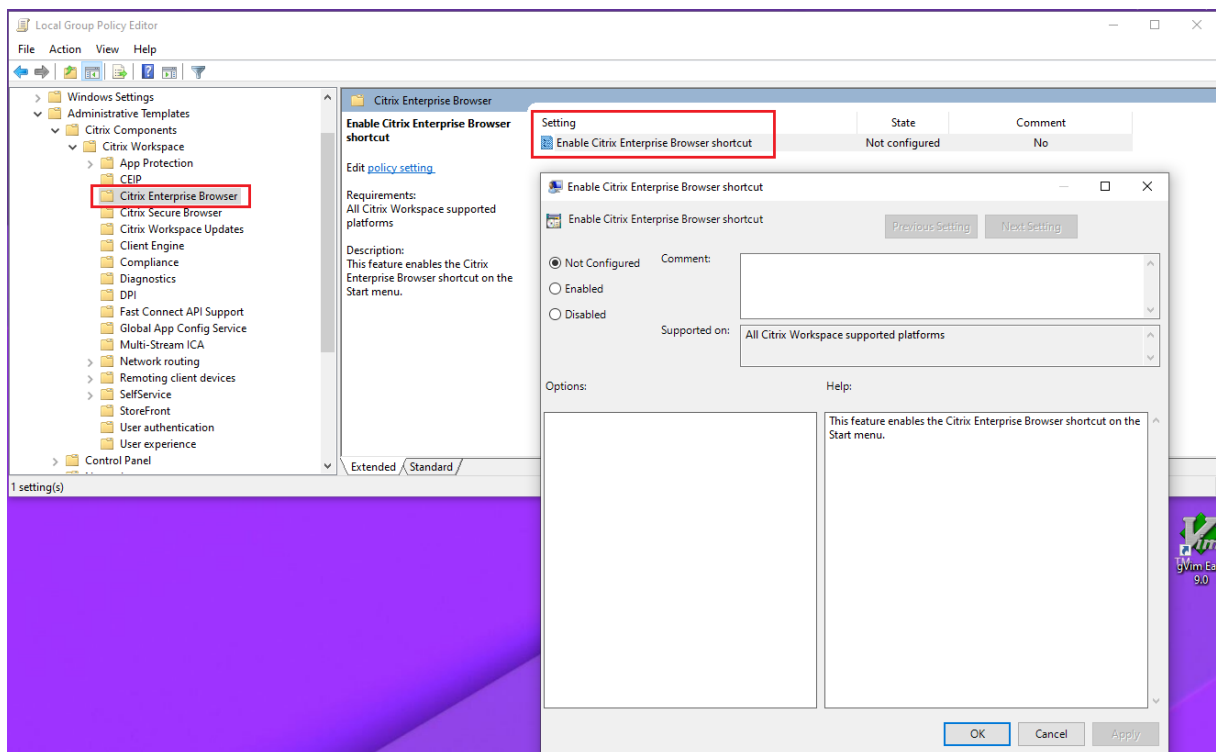
Los administradores pueden usar la propiedad **Habilitar acceso directo de Citrix Enterprise Browser** para controlar la visualización del acceso directo de Citrix Enterprise Browser en el menú Inicio.

**Nota:**

La configuración mediante GPO se aplica a Workspace y StoreFront.

Para habilitar el acceso directo de Citrix Enterprise Browser, 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 > Citrix Enterprise Browser**.
3. Seleccione la opción **Habilitar acceso directo de Citrix Enterprise Browser**.



Para obtener más información sobre cómo usar el GPO, consulte la página [Plantilla administrativa de objeto de directiva de grupo](#).

Global App Configuration Service (GACS)

Vaya a **Configuración de Workspace > Configuración de aplicaciones > Citrix Enterprise Browser** y habilite la opción **Habilitar acceso directo de Citrix Enterprise Browser**.

Para obtener más información sobre cómo utilizar la interfaz de usuario de GACS, consulte el artículo [Interfaz de usuario](#) de la documentación de Citrix Enterprise Browser.

### Nota:

Esta forma de configuración se aplica a Workspace y StoreFront.

### Archivo web.config:

Habilite el atributo **CEBShortcutEnabled** en las propiedades.

```
1 <properties>
2
3     <property name="CEBShortcutEnabled" value="True" />
4
5 </properties>
6 <!--NeedCopy-->
```

**Nota:**

La configuración mediante `web.config` se aplica en StoreFront.

**Mediante web.config:**

Para habilitar el acceso directo de Citrix Enterprise Browser, haga lo siguiente:

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">`
3. Antes de la etiqueta `</account>`, vaya a las propiedades de esa cuenta de usuario y agregue lo siguiente:

```

1 <properties>
2
3     <property name="CEBShortcutEnabled" value="True" />
4
5 </properties>
6 <!--NeedCopy-->
    
```

He aquí un ejemplo de archivo `web.config`:

```

1 <account>
2
3     <clear />
4
5     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="
6         F84Store"
7         description="" published="true" updaterType="Citrix"
8         remoteAccessType="None">
9         <annotatedServices>
10        <clear />
11        <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
12            <metadata>
13                <plugins>
14                    <clear />
15                </plugins>
16                <trustSettings>
17                    <clear />
18                </trustSettings>
19                <properties>
20                    <property name="CEBShortcutEnabled" value="True
21                        " />
22                </properties>
23            </metadata>
24        </annotatedServiceRecord>
    
```

```
23 </annotatedServices>
24 <metadata>
25     <plugins>
26         <clear />
27     </plugins>
28     <trustSettings>
29         <clear />
30     </trustSettings>
31     <properties>
32         <clear />
33     </properties>
34 </metadata>
35 </account>
36
37 <!--NeedCopy-->
```

## 2305.1

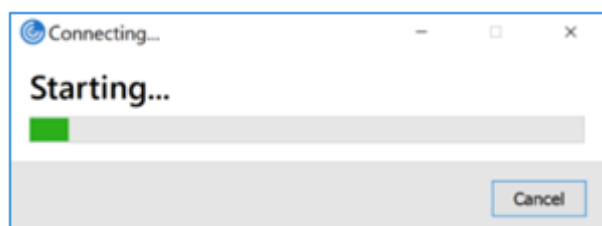
### Novedades

#### Experiencia mejorada al iniciar aplicaciones y escritorios virtuales

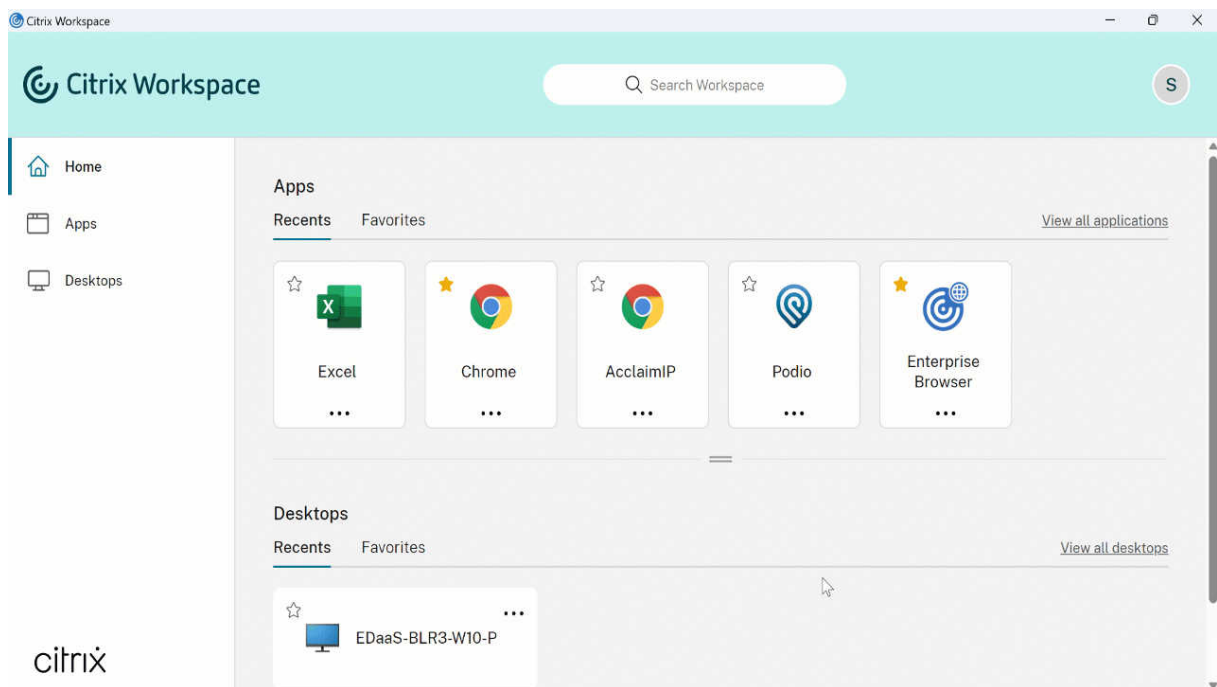
##### Nota:

Esta función está disponible de forma general para los almacenes de la nube y se encuentra en versión Technical Preview para los almacenes locales.

Antes, el cuadro de diálogo de progreso del inicio no era intuitivo para los usuarios. Les hacía creer que el proceso de inicio no respondía, y estos cerraban el cuadro de diálogo, ya que los mensajes de notificación eran estáticos.



La experiencia mejorada al iniciar aplicaciones y escritorios es más informativa, moderna e intuitiva en la aplicación Citrix Workspace para Windows. Esta funcionalidad ayuda a mantener a los usuarios informados con datos relevantes y oportunos sobre el estado del inicio. La notificación aparece en la esquina inferior derecha de la pantalla.



Los usuarios pueden ver notificaciones útiles sobre el progreso del inicio en lugar de un icono giratorio solamente. Si hay un inicio en curso y el usuario intenta cerrar el explorador, aparece un mensaje de advertencia.

A partir de la aplicación Citrix Workspace para Windows 2305.1, esta función está habilitada de forma predeterminada en sesiones de la nube.

Puede habilitar esta función mediante la clave del Registro de la sesión de StoreFront (local). Para obtener más información, consulte [Experiencia mejorada al iniciar aplicaciones y escritorios virtuales](#).

**Seguimiento del estado de los comandos de Storebrowse** Puede realizar un seguimiento del estado de ejecución de comandos de Storebrowse en un archivo. Para realizar un seguimiento del estado de operación correcta, proporcione un nombre de archivo único con el comando `-f launch`. Este comando genera un archivo con el nombre proporcionado. El estado de operación fallida está presente en el archivo `ica.error`, que se crea automáticamente.

**Nota:**

Asegúrese de agregar una `.ica` extensión al nombre del archivo con el comando `-f launch`. De lo contrario, el archivo no se generará.

Los archivos para realizar un seguimiento tanto de las operaciones correctas como de las erróneas están presentes en `%LOCALAPPDATA%\citrix\selfservice\cache`, y puede supervisarlos según sea necesario.

Esta mejora está habilitada de forma predeterminada.

A continuación, se muestra un ejemplo de cómo utilizar el comando de inicio con la opción `-f`:

```
1 -launch -f <uniqueFileName.ica> "launchcommandline"
2 For example:
3 SelfService.exe storebrowse -launch -f uniqueFileName.ica -s store0-5
   c3ec017 -CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-
   e33d0695df39.Notepad -ica "https://cwawiniwstest.cloudburrito.com/
   Citrix/Store/resources/v2/
   YTLh0GUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkJzJm5Lk5vdGVwYWQ-/launch/
   ica" -cmdline
4
5 <!--NeedCopy-->
```

**Compatibilidad con métodos de autenticación modernos para almacenes de StoreFront** La aplicación Citrix Workspace 2305.1 para Windows admite métodos de autenticación modernos para los almacenes de StoreFront. Puede autenticarse en los almacenes de Citrix StoreFront de cualquiera de las siguientes formas:

- Con claves de seguridad de Windows Hello y FIDO2. Para obtener más información, consulte [Otras formas de autenticarse](#).
- Single Sign-On (SSO) en los almacenes de Citrix StoreFront desde máquinas unidas a Azure Active Directory (AAD) con AAD como proveedor de identidades. Para obtener más información, consulte [Otras formas de autenticarse](#).
- Los administradores de Workspace pueden configurar y aplicar directivas de acceso condicional de Azure Active Directory para usuarios que se autentican en los almacenes de Citrix StoreFront. Para obtener más información, consulte [Compatibilidad con el acceso condicional con Azure AD](#).

Para habilitar esta funcionalidad, debe utilizar Microsoft Edge WebView2 como explorador subyacente para la autenticación directa de StoreFront y la puerta de enlace.

**Nota:**

Asegúrese de que la versión de Microsoft Edge WebView2 Runtime sea 102 o una posterior.

Puede habilitar métodos de autenticación modernos para los almacenes de StoreFront mediante Global App Config Service y una plantilla de objetos de directiva de grupo (GPO). Para obtener más información, consulte la sección [Compatibilidad con métodos de autenticación modernos para almacenes de StoreFront](#).

**Compatibilidad con más de 200 grupos en Azure AD** Con esta versión, un usuario de Azure AD que forme parte de más de 200 grupos puede ver las aplicaciones y escritorios que tiene asignados. Anteriormente, el mismo usuario no podía ver estas aplicaciones y escritorios.

**Nota:**

Para habilitar esta función, los usuarios deben cerrar sesión en la aplicación Citrix Workspace e iniciarla de nuevo.

## App Protection

**Mejora en la protección contra el registro de tecleo** Con esta mejora, se habilita la protección contra el registro de tecleo en las pantallas de autenticación y del plug-in de autoservicio (SSP) si se cumple uno de estos criterios:

- Habilitó App Protection mediante una de estas opciones:
  - Marcar la casilla **Iniciar App Protection** durante la instalación.
  - Inicie el componente App Protection mediante el parámetro `startappprotection` de línea de comandos.
- Si no marcó la casilla **Iniciar App Protection** ni utilizó el parámetro `startappprotection` de la línea de comandos durante la instalación, la protección contra el registro de tecleo se habilitará tras iniciar el primer recurso protegido.

**Nota:**

Global App Configuration Service (GACS) y los objetos de directiva de grupo (GPO) supeditan el comportamiento anterior. Por ejemplo, si inhabilitó GACS o la directiva de GPO para estas pantallas, la protección contra el registro de tecleo no estará habilitada en las pantallas de autenticación y SSP.

**Actualización importante sobre los nombres de los archivos** En una versión futura de la aplicación Citrix Workspace para Windows, se actualizarán estos nombres de archivo:

- EntryProtect.dll
- entryprotect.sys
- epclient32.dll
- epclient64.dll
- epinject.sys
- epusbfilter.sys
- entryprotectdrv
- epinject6

Estos archivos se instalan en `%ProgramFiles(x86)%\Citrix\ICA Client\`.

Si ha agregado alguno de estos nombres de archivo a la lista de archivos permitidos de su entorno, actualice la lista de archivos permitidos cuando se anuncien los nuevos nombres de archivo.



**Citrix Enterprise Browser** Esta versión incluye la versión 105.1.1.27 de Citrix Enterprise Browser, basada en la versión 105 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de [Citrix Enterprise Browser](#).

**Compatibilidad con extensiones de explorador** Es posible agregar de forma segura a Citrix Enterprise Browser las extensiones que proporcione su administrador. Un administrador puede implementar, administrar y controlar las extensiones. Los usuarios finales pueden ver y utilizar la extensión de `citrixbrowser://extensions` según sea necesario. Para obtener más información y parámetros, consulte [Global App Configuration Service](#).

Para obtener más información sobre la configuración, consulte [Compatibilidad con extensiones de explorador](#).

**Modificación en la implementación de directivas de SPA en aplicaciones web y SaaS internas** Esta función mejora la implementación de directivas de seguridad en aplicaciones web y SaaS. Ahora, cuando una página web y los iframes de la página web tienen directivas diferentes, tenemos una implementación de directivas más estricta, en la que se aplica una unión de todas las directivas en toda la página web, incluidos los iframes. Sin embargo, la marca de agua solo se aplica a la página web.

**Usar Global App Config Service para administrar Citrix Enterprise Browser** El administrador puede usar Global App Configuration Service (GACS) para Citrix Workspace para entregar los parámetros de Citrix Enterprise Browser a través de un servicio administrado de forma centralizada.

Global App Configuration Service se ha diseñado para que los administradores puedan configurar Citrix Workspace y administrar los parámetros de la aplicación Citrix Workspace con facilidad. Esta función permite a los administradores usar Global App Configuration Service para aplicar diversos parámetros o directivas del sistema al explorador Citrix Enterprise Browser de un almacén en particular. El administrador ahora puede configurar y administrar los siguientes parámetros de Citrix Enterprise Browser mediante las API o la interfaz de usuario de administración de GACS:

- “Enable CEB for all apps”: Convierte a Citrix Enterprise Browser en el explorador predeterminado para abrir aplicaciones web y SaaS desde la aplicación Citrix Workspace.
- “Enable save passwords”: Permite o deniega a los usuarios finales la posibilidad de guardar contraseñas.
- “Enable incognito mode”: Habilita o inhabilita el modo incógnito.
- “Managed Bookmarks”: Permite a un administrador enviar marcadores a Citrix Enterprise Browser.
- “Enable developer tools”: Habilita o inhabilita las herramientas para desarrolladores en Enterprise Browser.

- “Delete browsing data on exit”: Permite al administrador configurar qué datos de Citrix Enterprise Browser se eliminarán al salir.
- “Extension Install Force list”: Permite al administrador instalar extensiones en Citrix Enterprise Browser.
- “Extension Install Allow list”: Permite al administrador configurar una lista de extensiones permitidas que los usuarios pueden agregar a Citrix Enterprise Browser. Esta lista usa Chrome Web Store.

Para obtener más información, consulte [Usar Global App Configuration Service para administrar Citrix Enterprise Browser](#).

**Notas:**

- El par de nombre y valor distingue entre mayúsculas y minúsculas.
- Todos los parámetros del explorador en [Global App Configuration Service](#) se encuentran en estas categorías:

```
1 {
2
3     "category": "browser",
4     "userOverride": false,
5     "assignedTo": [
6         "AllUsersNoAuthentication"
7     ]
8 }
9
10
11 <!--NeedCopy-->
```

- El administrador también puede aplicar los parámetros a dispositivos no administrados. Para obtener más información, consulte la documentación de [Global App Configuration Service](#).

### Interfaz de usuario

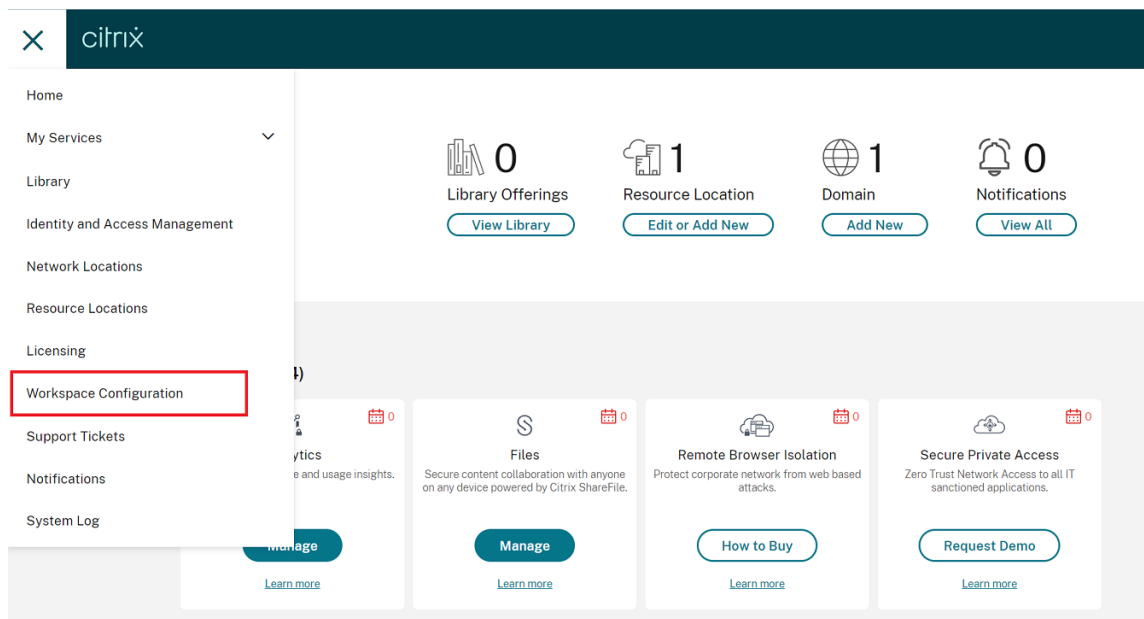
Para configurar Citrix Enterprise Browser a través de la interfaz de usuario de administración de Global App Configuration Service, haga lo siguiente:

1. Inicie sesión en [citrix.cloud.com](https://citrix.cloud.com) con sus credenciales.

**Nota:**

Consulte el artículo [Registrarse en Citrix Cloud](#) para obtener instrucciones detalladas para crear una cuenta de Citrix Cloud.

2. Tras la autenticación, haga clic en el menú situado en la esquina superior izquierda y seleccione **Configuración de Workspace**.



Aparecerá la pantalla **Configuración de Workspace**.

3. Haga clic en **Configuración de aplicaciones > Citrix Enterprise Browser**.

Ahora puede configurar, modificar y publicar los parámetros de las funciones de Citrix Enterprise Browser.

Para obtener más información, consulte [Usar Global App Configuration Service para administrar Citrix Enterprise Browser](#).

## 2303

### Novedades

**Configurar la ruta para el almacenamiento de datos temporales del explorador web superpuesto de la redirección de contenido del explorador web** A partir de la versión 2303 de la aplicación Citrix Workspace, se le solicita que configure la ruta de almacenamiento de datos temporales para el explorador web basado en el Chromium Embedded Framework (CEF).

Para obtener más información, consulte [Configurar la ruta para el almacenamiento de datos temporales del explorador web superpuesto de la redirección de contenido del explorador web](#).

**Compatibilidad con métodos de autenticación modernos para almacenes de StoreFront** La aplicación Citrix Workspace 2303 para Windows admite métodos de autenticación modernos para los almacenes de StoreFront. Puede autenticarse en los almacenes de Citrix StoreFront de cualquiera de las siguientes formas:

- Con claves de seguridad de Windows Hello y FIDO2. Para obtener más información, consulte [Otras formas de autenticarse](#).
- Single Sign-On (SSO) en los almacenes de Citrix StoreFront desde máquinas unidas a Azure Active Directory (AAD) con AAD como proveedor de identidades. Para obtener más información, consulte [Otras formas de autenticarse](#).
- Los administradores de Workspace pueden configurar y aplicar directivas de acceso condicional de Azure Active Directory para usuarios que se autentican en los almacenes de Citrix StoreFront. Para obtener más información, consulte [Compatibilidad con el acceso condicional con Azure AD](#).

Para habilitar esta funcionalidad, debe utilizar Microsoft Edge WebView2 como explorador subyacente para la autenticación directa de StoreFront y la puerta de enlace.

**Nota:**

La versión de Microsoft Edge WebView2 Runtime debe ser 102 o posterior.

Puede habilitar métodos de autenticación modernos para los almacenes de StoreFront con la plantilla de objeto de directiva de grupo. Para obtener más información, consulte la sección [Compatibilidad con métodos de autenticación modernos para almacenes de StoreFront](#).

**Experiencia mejorada para llamadas de videoconferencia en Microsoft Teams optimizado** A partir de esta versión, la función de transmisión simultánea está habilitada de forma predeterminada para las llamadas de videoconferencia en Microsoft Teams optimizado. Con esta compatibilidad, la calidad y la experiencia de las videoconferencias en diferentes dispositivos de punto final mejoran al adaptarse a la resolución adecuada para ofrecer la mejor experiencia en llamadas a todos los usuarios.

Con esta experiencia mejorada, es posible que cada usuario cuente con varias transmisiones de vídeo en diferentes resoluciones (por ejemplo, 720p, 360p...) en función de varios factores, como la capacidad del dispositivo de punto final, las condiciones de la red y más. El dispositivo de punto final receptor solicita entonces la resolución de máxima calidad que pueda gestionar, lo que ofrece a todos los usuarios una experiencia de vídeo óptima.

**Nota:**

Esta función está disponible solamente después de la implantación de una actualización de Microsoft Teams. Para obtener información sobre ETA, vaya a <https://www.microsoft.com/> y busque la hoja de ruta de Microsoft 365. Cuando Microsoft implante la actualización, consulte [CTX253754](#) para obtener información sobre la actualización de la documentación y el anuncio.

**Mejora de App Protection: Antiinyección de DLL** Como parte de App Protection, ahora contamos con una mejora de seguridad que ayuda a proteger la aplicación Citrix Workspace de determinadas

bibliotecas de enlace dinámico (DLL) no autorizadas o de módulos que no son de confianza. Si se inyectan estos módulos que no son de confianza, la aplicación Citrix Workspace detecta estas intervenciones e impide que los módulos se carguen.

La antiinyección de DLL se puede habilitar para estos componentes:

- Citrix Auth Manager
- Interfaz de usuario de la aplicación Citrix Workspace
- Citrix Virtual Apps and Desktops

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

**Aviso:**

Esta característica funciona mediante el filtrado del acceso a las funciones necesarias del sistema operativo subyacente (llamadas a API específicas necesarias para cargar las DLL). De este modo, puede proporcionar protección incluso contra ciertas herramientas de piratas informáticos personalizadas y diseñadas específicamente. Sin embargo, a medida que los sistemas operativos evolucionan, pueden surgir nuevas formas de cargar archivos DLL. Si bien seguimos identificándolas y abordándolas, no podemos garantizar una protección completa en configuraciones e implementaciones específicas.

**Citrix Enterprise Browser** Esta versión incluye la versión 109.1.1.29 de Citrix Enterprise Browser, basada en la versión 109 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de [Citrix Enterprise Browser](#).

**Compatibilidad de Secure Private Access con StoreFront** Ahora, como administrador, puede configurar aplicaciones web y SaaS en StoreFront mediante una solución de Secure Private Access. Una vez que el administrador haya configurado la aplicación, los usuarios finales pueden abrir las aplicaciones web y SaaS mediante Citrix Enterprise Browser con una seguridad reforzada.

Para obtener más información, consulte [Secure Private Access for on-premises](#) en la documentación de Citrix Secure Private Access.

## 2302

### Novedades

**Experiencia mejorada al reconectar aplicaciones y escritorios virtuales** Esta versión ofrece una experiencia de usuario mejorada al reconectarse a aplicaciones y escritorios virtuales de los que se había desconectado.

Cuando la aplicación Citrix Workspace intenta actualizar la aplicación Citrix Workspace desconectada o iniciar nuevas aplicaciones o escritorios virtuales como parte de la funcionalidad de control del espacio de trabajo, aparece el siguiente mensaje:

## Restore session?

You have one or more apps/desktops running from the previous session in Citrix Workspace app. Would you like to restore them?

Remember my preference



Este mensaje solo aparece cuando la opción para **mostrar la solicitud de reconexión para volver a conectar las sesiones** se establece en “true” en Global App Configuration Service.

Haga clic en **Restaurar** para volver a conectarse y abrir las aplicaciones y escritorios virtuales nuevos y desconectados. Si solo quiere iniciar las aplicaciones y escritorios recién seleccionados, haga clic en **Cancelar**.

También puede seleccionar la opción **Recordar mi preferencia** para aplicar la preferencia seleccionada al siguiente inicio de sesión.

El mensaje **¿Restaurar sesión?** anterior aparecerá solo si:

- el usuario intenta iniciar una aplicación perteneciente a un almacén del espacio de trabajo;
- las directivas administrativas o los parámetros de configuración de la aplicación no están configurados para la funcionalidad de control del espacio de trabajo;
- Las opciones de reconexión de control del espacio de trabajo están configuradas de forma pre-determinada en el cliente.

### Nota:

Los parámetros de reconexión de **Opciones de reconexión** tienen prioridad sobre las preferencias establecidas en el cuadro de diálogo. Para obtener más información, consulte [Configurar opciones de reconexión mediante el cuadro de diálogo Preferencias avanzadas](#).

**Administración de aplicaciones cliente para el plug-in de Zoom** Ahora puede administrar el plug-in de Zoom mediante la función Administración de aplicaciones cliente.

Para obtener más información, consulte [Administración de aplicaciones cliente para el plug-in de Zoom](#).

**Se ha actualizado el modo de selección de dispositivos de audio para Microsoft Teams optimizado** A partir de esta versión, al cambiar los dispositivos de audio predeterminados en la configuración de sonido del dispositivo de punto final, Microsoft Teams optimizado en la imagen de disco virtual (VDI) de Citrix VDI cambia la selección actual de dispositivos de audio para que coincida con los valores predeterminados del dispositivo de punto final.

Sin embargo, si selecciona un dispositivo de forma explícita en Microsoft Teams, su selección tendrá prioridad y no seguirá los valores predeterminados del dispositivo de punto final. Su selección se mantendrá hasta que borre la memoria caché de Microsoft Teams.

**Mejora en App Protection** A partir de esta versión, la aplicación Citrix Workspace para Windows permite configurar App Protection para la autenticación y para Self-Service plug-in mediante Global App Configuration Service. Anteriormente, solo se podían configurar estos componentes mediante el objeto de directiva de grupo.

Si habilita las funciones de protección contra registro de tecleo y contra la captura de pantalla mediante Global App Configuration Service, se aplicarán tanto a la autenticación como a Self-service Plug-in.

**Nota:**

Las configuraciones de Global App Configuration Service no afectan a las aplicaciones virtuales, los escritorios virtuales, las aplicaciones web y las aplicaciones SaaS. Estos recursos se siguen controlando mediante el Delivery Controller y Citrix Secure Private Access. Para obtener información, consulte la sección [Configurar](#) de la documentación de App Protection.

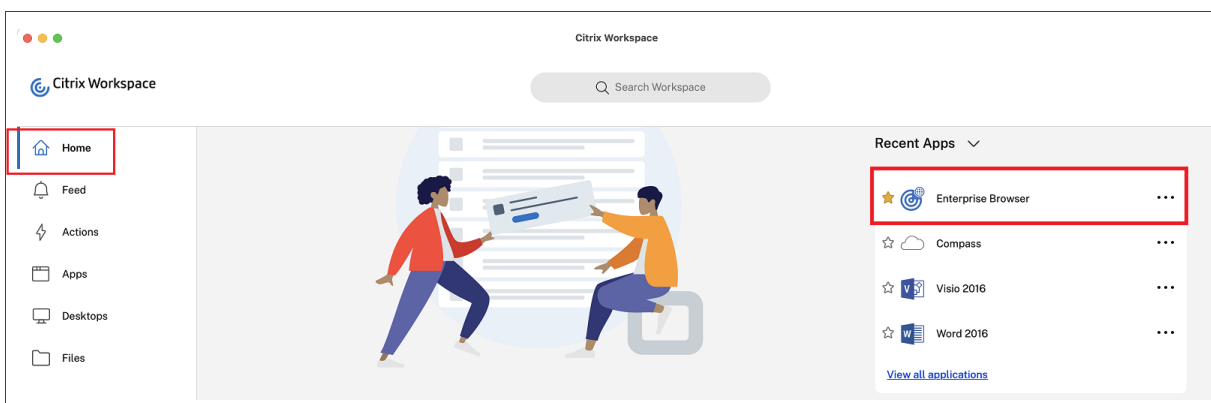
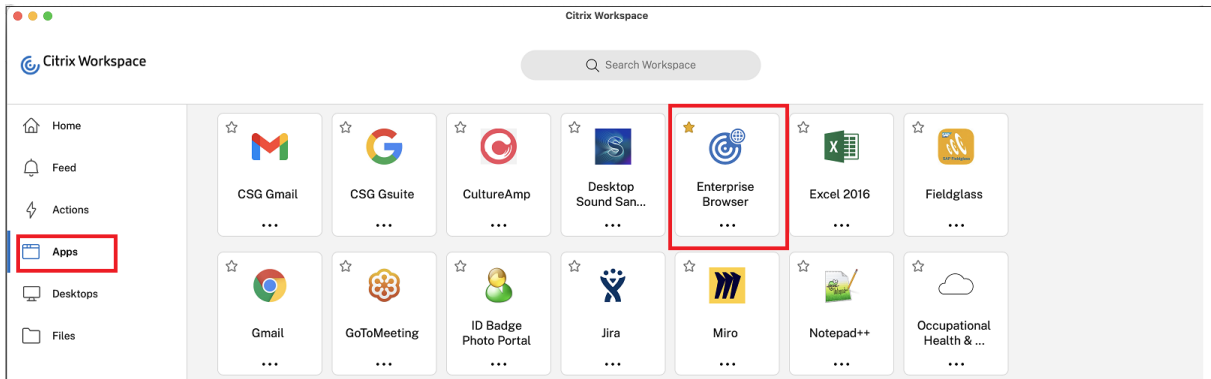
Para obtener más información, consulte la sección [Mejora en App Protection](#).

**Citrix Enterprise Browser** Esta versión incluye la versión 108.1.1.97 de Citrix Enterprise Browser, basada en la versión 108 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de [Citrix Enterprise Browser](#).

**Abrir todas las aplicaciones web y SaaS a través de Citrix Enterprise Browser** En esta versión de Enterprise Browser (en la aplicación Citrix Workspace para Windows), todas las aplicaciones web internas y las aplicaciones SaaS externas disponibles en la aplicación Citrix Workspace se abren en Citrix Enterprise Browser.

**Opción para iniciar Citrix Enterprise Browser desde la aplicación Citrix Workspace** Anteriormente, Citrix Enterprise Browser solo se podía abrir desde la aplicación Citrix Workspace después de abrir una aplicación web o SaaS.

A partir de esta versión, Enterprise Browser se puede abrir directamente desde la aplicación Citrix Workspace sin necesidad de abrir una aplicación web o SaaS. Esta función proporciona un acceso sencillo a Citrix Enterprise Browser y no requiere ninguna configuración por parte de los administradores. Esta función está disponible de forma predeterminada.



**Nota:**

El usuario final debe tener asignado un derecho de uso con relación a, al menos, una aplicación web o SaaS a través de Secure Private Access.

**2212**

**Novedades**

**Nota:**

A partir de esta versión, asegúrese de que la versión de Microsoft Edge WebView2 Runtime sea 102 o una posterior. Para obtener más información, consulte [Requisitos del sistema y compatibilidad](#).



**Administración de aplicaciones cliente** La aplicación Citrix Workspace 2212 para Windows ahora ofrece funcionalidad de administración de aplicaciones cliente, lo que la convierte en la única aplicación cliente necesaria en el dispositivo de punto final para instalar y administrar agentes, como el agente de Secure Access y el plug-in End Point Analysis (EPA).

Con esta capacidad, los administradores pueden implementar y administrar fácilmente los agentes necesarios desde una única consola de administración.

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

**Control de versiones con actualización automática** Ahora, los administradores pueden administrar la versión de las actualizaciones automáticas de los dispositivos de la organización.

Los administradores pueden controlar la versión estableciéndola en la propiedad `maximumAllowedVersion` de Global App Config Service.

Ejemplo de archivo JSON en Global App Config Service:

```
1 {
2
3   "category": "AutoUpdate",
4   "userOverride": false,
5   "assignedTo": [
6     "AllUsersNoAuthentication"
7   ],
8   "settings": [
9     {
10
11       "name": "Auto Update plugins settings",
12       "value": [
13         {
14
15           "pluginSettings": {
16
17             "upgradeToLatest": false,
18             "deploymentMode": "InstallAndUpdate",
19             "stream": "Current",
20             "maximumAllowedVersion": "23.03.0.49",
21             "minimumAllowedVersion": "0.0.0.0",
22             "delayGroup": "Fast"
23           }
24         },
25         {
26           "pluginName": "WorkspaceApp",
27           "pluginId": "1CDF566D-B2C7-47CA-802F-6283C862E1D6"
28         }
29       ]
30     }
31   ]
32 }
33 }
```

```
34  
35  
36 <!--NeedCopy-->
```

Cuando se establece la versión, la aplicación Citrix Workspace del dispositivo del usuario se actualiza automáticamente con la versión especificada en la propiedad `maximumAllowedVersion`.

**Notas:**

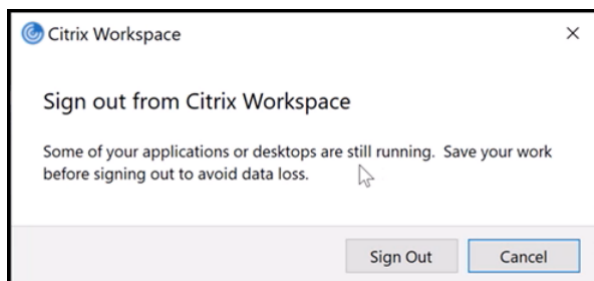
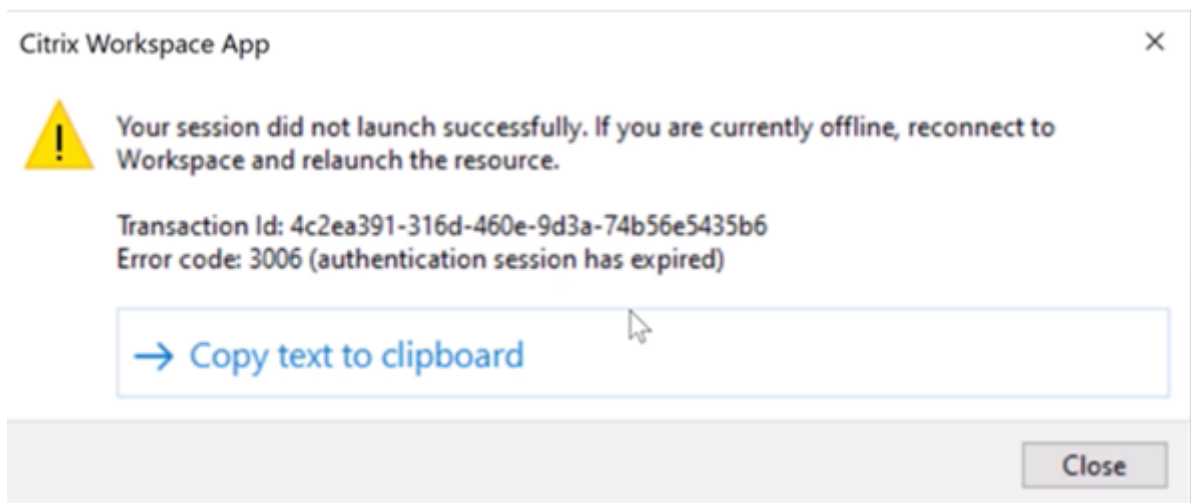
- Actualmente, todos los parámetros mencionados en el archivo JSON anterior son obligatorios. Debe proporcionar valores para los parámetros `upgradeToLatest` y `maximumAllowedVersion` en función de los requisitos de su organización. Sin embargo, para el resto de parámetros, puede utilizar valores similares a los del archivo JSON de ejemplo.
- Para efectuar el control de versiones de las actualizaciones automáticas, el parámetro `upgradeToLatest` de Global App Config Service debe estar establecido en `false`. Si tiene el valor `true`, `maximumAllowedVersion` se ignora.
- No modifique `pluginId`, ya que es el ID asignado a la aplicación Citrix Workspace.
- Si el administrador no ha configurado la versión en Global App Config Service, la aplicación Citrix Workspace se actualiza a la versión disponible más reciente de forma predeterminada.

**Forzar solicitud de inicio de sesión para el proveedor de identidades federadas** La aplicación Citrix Workspace ahora respeta la configuración sobre sesiones de proveedores de identidades federadas. Para obtener más información, consulte el artículo [CTX253779](#) de Knowledge Center.

Ya no es necesario usar la directiva Almacenar tokens de autenticación para forzar la solicitud de inicio de sesión.

**Mejora de la experiencia de reconexión tras la caducidad del archivo de concesión de conexiones** Anteriormente, el usuario final no recibía ninguna notificación cuando el archivo de concesión de conexiones y el token de autenticación caducaban.

A partir de esta versión, aparece un mensaje de error y un cuadro de diálogo de consentimiento. El cuadro de diálogo de consentimiento solo aparece cuando hay recursos ejecutándose en la sesión. Si no hay recursos en ejecución, solo aparece un cuadro de diálogo de error. Se cierra la sesión sin que aparezca el cuadro de diálogo de consentimiento.



Puede hacer clic en **Cerrar sesión** para cerrar la sesión actual de la aplicación Citrix Workspace o en **Cancelar** para continuar con la sesión.

**Nota:**

Guarde sus datos antes de hacer clic en **Cerrar sesión**.

**Compatibilidad con la instalación predeterminada de App Protection** El componente App Protection ahora se instala de forma predeterminada durante la instalación de la aplicación Citrix Workspace.

La casilla de verificación **Habilitar App Protection** que se muestra durante la instalación se sustituye por Iniciar App Protection después de la instalación.



Al seleccionar esta casilla de verificación, App Protection se inicia inmediatamente después de la instalación.

**Nota:**

Si no se habilita esta casilla de verificación, App Protection se inicia automáticamente al iniciar por primera vez un recurso o componente protegido en el caso de los clientes que tienen asignado el derecho de uso del componente App Protection.

También puede iniciar el componente App Protection mediante el parámetro `/startappprotection` de línea de comandos. No obstante, el modificador `/includeappprotection` anterior se ha retirado.

**Nota:**

Anteriormente, las funcionalidades de protección contra la captura de teclado y contra las capturas de pantalla se aplicaban de forma predeterminada para la autenticación de Citrix y las pantallas de la aplicación Citrix Workspace. Sin embargo, a partir de 2212, estas capacidades están inhabilitadas de forma predeterminada y deben configurarse mediante el objeto de directiva de grupo. Para obtener información sobre la configuración del objeto de directiva de grupo, consulte [Mejora de la configuración de App Protection](#).

**Mejora de App Protection: Detección y notificación de capturas de pantalla** A partir de esta versión, podrá ver una notificación cuando haya un posible intento de captura de pantalla con relación a cualquier recurso protegido. Para obtener información sobre los recursos protegidos con App Protection, consulte [¿Qué protege App Protection?](#)

La notificación aparece cuando hay:

- Un intento de hacer una captura de pantalla o grabar un vídeo a través de una herramienta para captura de pantallas.
- Un intento de hacer una captura de pantalla con la tecla Imprimir pantalla.

**Nota:**

La notificación aparece solo una vez por instancia en ejecución de la herramienta de captura de pantallas. La notificación vuelve a aparecer si reinicia la herramienta e intenta capturar una pantalla.

**Optimización de Desktop Viewer** Esta versión optimiza la experiencia con Desktop Viewer al reducir el tiempo de inicio en 5 segundos. La barra de herramientas de **Desktop Viewer** se abre rápidamente y puede mostrar la pantalla de inicio de sesión predeterminada de Windows. Los administradores pueden ocultarla configurando la siguiente clave de Registro para introducir cierto retraso en milisegundos:

- Ubicación: HKEY\_CURRENT\_USER\SOFTWARE\Citrix\XenDesktop\DesktopViewer
- Nombre: ExtendConnectScreenMS
- Tipo: DWORD
- Valor: 00000000 (retraso en milisegundos)

**Nota:**

La configuración del Registro es opcional.

### Citrix Enterprise Browser

**Nota:**

A partir de la versión 2210 de la aplicación Citrix Workspace para Windows, la función **Abrir todas las aplicaciones web y SaaS a través de Citrix Enterprise Browser** está inhabilitada.

Esta versión incluye la versión 107.1.1.13 de Citrix Enterprise Browser, basada en la versión 107 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de [Citrix Enterprise Browser](#).

- **Configurar Citrix Enterprise Browser como explorador de trabajo**

Ahora puede configurar Citrix Enterprise Browser como explorador de trabajo para abrir todos los enlaces de trabajo. Puede seleccionar un explorador alternativo para abrir los enlaces que no sean de trabajo.

Un enlace de trabajo es un enlace asociado a las aplicaciones web o SaaS configuradas por el administrador para el usuario final. Cuando un usuario hace clic en cualquier enlace de una aplicación nativa, si se trata de un enlace de trabajo, se abre a través de Citrix Enterprise Browser. De lo contrario, se abre a través del explorador alternativo que seleccione el usuario final.

Para obtener más información, consulte [Configurar Citrix Enterprise Browser como explorador de trabajo](#).

## 2210.5

### **Novedades**

En esta versión se han resuelto problemas para mejorar la estabilidad, la seguridad y el rendimiento general.

**Mejora de la actualización automática** Ahora, la aplicación Citrix Workspace admite la actualización automática cuando están habilitadas la detección del protocolo de detección automática de proxies web (WPAD) y la configuración automática de proxy (PAC).

**Citrix Enterprise Browser** Esta versión incluye la versión 105.2.1.40 de Citrix Enterprise Browser, basada en la versión 105 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de [Citrix Enterprise Browser](#).

## 2210

### **Novedades**

**Desenfoco de fondo para la redirección de cámaras web** Ahora, la aplicación Citrix Workspace para Windows admite el desenfoco de fondo para la redirección de cámaras web. Para habilitar esta función, seleccione la casilla **Preferencias > Conexiones > Habilitar desenfoco de fondo**.

**Mejoras en App Protection para aplicaciones web y SaaS en Windows 11** Esta mejora de App Protection optimiza la experiencia y las prestaciones de seguridad para los usuarios de aplicaciones web y SaaS en Windows 11. Esta mejora está disponible a través de Citrix Enterprise Browser para clientes de Secure Private Access.

**Limitar resoluciones de vídeo** Los administradores que tienen usuarios en dispositivos de punto final clientes de bajo rendimiento pueden optar por limitar las resoluciones de vídeos entrantes o salientes para reducir el impacto de la codificación y la decodificación de vídeo en dichos dispositivos. A partir de la aplicación Citrix Workspace 2010 para Windows, puede limitar estas resoluciones mediante las opciones de configuración del cliente.

**Nota:**

Los usuarios con resoluciones restringidas afectan a la calidad general del vídeo de las conferencias, ya que el servidor de Microsoft Teams se verá obligado a utilizar la resolución con el mínimo común denominador para todos los participantes de la conferencia.

Las restricciones de llamadas están inhabilitadas de forma predeterminada en el cliente con la aplicación Citrix Workspace 2210. Para habilitarlas, los administradores deben definir estas configuraciones en el lado del cliente en HKEY\_CURRENT\_USER\SOFTWARE\Citrix\HDXMediaStream:

Nombre	Tipo	Obligatorio	Valores aceptados
EnableSimulcast	Entero	SÍ	1-3 (configúrelo en 1)
MaxOutgoingResolution	Entero	SÍ	180, 240, 360, 540, 720, 1080 (resoluciones compatibles con Microsoft Teams)
MaxIncomingResolution	Entero	SÍ	180, 240, 360, 540, 720, 1080 (resoluciones compatibles con Microsoft Teams)
MaxIncomingStreams	Entero	SÍ	1-8
MaxSimulcastLayers	Entero	SÍ	1-3 (configúrelo en 1)
MaxVideoFrameRate	Entero	NO	1-30
MaxScreenShareFrameRate	Entero	NO	1-15

Todas las claves son DWORD.

**Citrix Enterprise Browser** Esta versión incluye la versión 105.1.1.27 de Citrix Enterprise Browser, basada en la versión 105 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de [Citrix Enterprise Browser](#).

**Cambio de nombre de Citrix Workspace Browser** Citrix Workspace Browser se llama ahora Citrix Enterprise Browser. El esquema personalizado ahora ha cambiado de “citrixworkspace://” a “citrixbrowser://”.

La implementación de esta transición en nuestros productos y en su documentación es un proceso continuo. Agradecemos su comprensión durante esta transición.

- La interfaz de usuario del producto, el contenido del producto y las imágenes e instrucciones de la documentación del producto se actualizarán en las próximas semanas.
- Es posible que algunos elementos (como los comandos y los MSI conserven los nombres anteriores para que los scripts existentes de cliente sigan funcionando).
- Asimismo, la documentación de producto y otros recursos relacionados (como vídeos y entradas de blog) que se incluyan como enlaces en la documentación de este producto pueden contener todavía los nombres anteriores.

**Abrir todas las aplicaciones web y SaaS a través de Citrix Enterprise Browser** A partir de esta versión, todas las aplicaciones web internas y las aplicaciones SaaS externas disponibles en la aplicación Citrix Workspace se abren en Citrix Enterprise Browser.

**Nota:**

A partir de la versión 2210 de la aplicación Citrix Workspace para Windows, la función **Abrir todas las aplicaciones web y SaaS a través de Citrix Enterprise Browser** está inhabilitada.

**Función de actualización automática de la aplicación Citrix Workspace en VDA** Ahora puede habilitar la función de actualización automática en el VDA mediante la creación de este valor del Registro:

En una máquina de 32 bits:

- Clave del Registro: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\AutoUpdate
- Valor del Registro: AllowAutoUpdateOnVDA
- Tipo de Registro: REG\_SZ
- Datos del Registro: True

En una máquina de 64 bits:

- Clave del Registro: HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\AutoUpdate
- Valor del Registro: AllowAutoUpdateOnVDA
- Tipo de Registro: REG\_SZ
- Datos del Registro: True



**Citrix Enterprise Browser (anteriormente, Citrix Workspace Browser)** Esta versión incluye la versión 103.2.1.10 de Citrix Enterprise Browser, basada en la versión 103 de Chromium. Para obtener más información sobre Citrix Enterprise Browser, consulte la documentación de [Citrix Enterprise Browser](#).

- **Perfiles de Citrix Enterprise Browser**

Los perfiles le ayudan a mantener información personal, como el historial, los marcadores, las contraseñas y otros parámetros, por separado para cada una de sus cuentas de Citrix Workspace. En función de su almacén de Workspace, se crea un perfil que le permite disfrutar de una experiencia de navegación única y personalizada.

**Nota:**

Después de actualizar la versión a 103.2.1.10 e iniciar sesión en el dispositivo por primera vez, solo se quitarán las contraseñas guardadas anteriormente. Al iniciar sesión en el dispositivo en un almacén diferente por primera vez, se pierden todos los datos guardados anteriormente.

## 2207

### Novedades

**Efectos y desenfoco de fondo para la optimización de Microsoft Teams con HDX** Ahora, la aplicación Citrix Workspace para Windows admite efectos y el desenfoco de fondo en la optimización de Microsoft Teams con HDX.

Puede difuminar o reemplazar el fondo por una imagen personalizada y evitar distracciones inesperadas al ayudar a que la conversación se centre en la silueta (cuerpo y rostro). La función se puede utilizar con llamadas de conferencia o entre dos usuarios.

**Nota:**

Ahora, esta función está integrada en los botones y la interfaz de usuario de Microsoft Teams. La compatibilidad con varias ventanas es un requisito previo que necesita una actualización de VDA a la versión 2112 o a una posterior. Para obtener más información, consulte [Reuniones y chat en modo multiventana](#).

### Limitaciones:

- No se admite el reemplazo de fondo definido por el administrador y el usuario.
- El efecto de fondo no persiste entre sesiones. Cuando cierra y reinicia Microsoft Teams o el VDA se conecta de nuevo, el efecto de fondo se restablece y se desactiva.

- Cuando la sesión ICA se conecta de nuevo, el efecto está desactivado. Sin embargo, la interfaz de usuario de Microsoft Teams muestra que el efecto anterior sigue activado con una marca de verificación. Citrix y Microsoft están trabajando juntos para resolver este problema.
- El dispositivo debe estar conectado a Internet mientras se reemplaza la imagen de fondo.

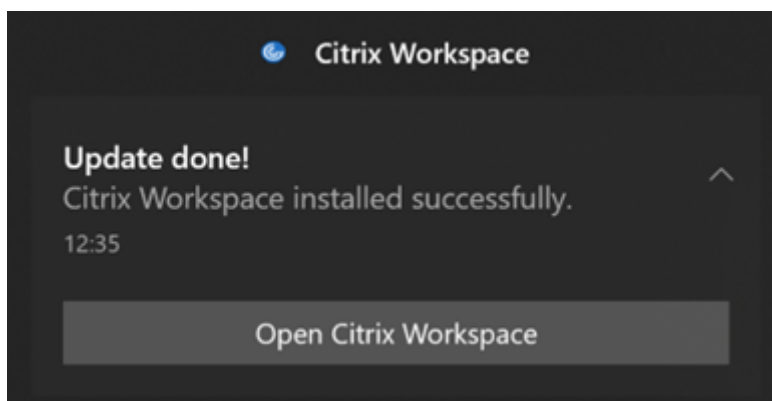
**Nota:**

Esta función estará disponible solamente después de la implantación de una futura actualización de Microsoft Teams. Cuando Microsoft implante la actualización, puede consultar el artículo [CTX253754](#) de Knowledge Center y el [Plan de desarrollo público de Microsoft 365](#) para obtener información sobre el anuncio y la actualización de la documentación.

**Experiencia de actualización automática mejorada** La función de actualización automática actualiza automáticamente la aplicación Citrix Workspace a la versión más reciente sin necesidad de la intervención del usuario.

La aplicación Citrix Workspace comprueba periódicamente y descarga la versión más reciente disponible de la aplicación. La aplicación Citrix Workspace determina el mejor momento para la instalación en función de la actividad del usuario para no provocar ninguna interrupción.

Cuando se complete la instalación, aparecerá esta notificación:



Si la aplicación Citrix Workspace no encuentra el momento adecuado para instalar las actualizaciones en segundo plano, aparece una notificación.

**Citrix Enterprise Browser** Esta versión incluye la versión 102.1.1.14 de Citrix Enterprise Browser, basada en la versión 102 de Chromium.

**Nota sobre la actualización de la aplicación Citrix Workspace** Al actualizar la aplicación Citrix Workspace para Windows de la versión anterior a la versión 2207, se le pide al usuario que inicie sesión. El inicio de sesión solo se solicita para el almacén del espacio de trabajo.

## 2206

### Novedades

**Rendimiento gráfico mejorado** La aplicación Citrix Workspace 2206 presenta importantes mejoras de rendimiento para las GPU integradas de Intel:

- Se ha reducido el consumo de GPU para los gráficos, lo que mejora el rendimiento general.

Se han solucionado estos problemas:

- Un nivel bajo de fotogramas por segundo después de reproducir un vídeo en la GPU de Intel de 10.<sup>a</sup> generación o una posterior.
- Diferencia de brillo en la opción gradual sin pérdida o para las regiones que cambian activamente en las GPU de Intel y AMD.

**Habilitar la correspondencia de PPP** A partir de la aplicación Citrix Workspace 2206 para Windows, la correspondencia de PPP está habilitada de forma predeterminada. Esto significa que la aplicación Citrix Workspace intenta corresponder automáticamente la resolución de la pantalla y los parámetros del escalado de PPP del cliente Windows local con la sesión de Citrix. Como parte de este cambio, la opción de PPP elevados disponible en Preferencias avanzadas de la aplicación Citrix Workspace ya no está disponible. Para obtener más información, consulte el artículo [CTX460068](#) de Knowledge Center.

**Citrix Enterprise Browser** Esta versión incluye la versión 101.1.1.12 de Citrix Enterprise Browser, basada en la versión 101 de Chromium. Para ver las funciones o correcciones de errores de Citrix Enterprise Browser, consulte [Novedades](#) en la documentación de Citrix Enterprise Browser.

## 2205

### Novedades

**Nota:**

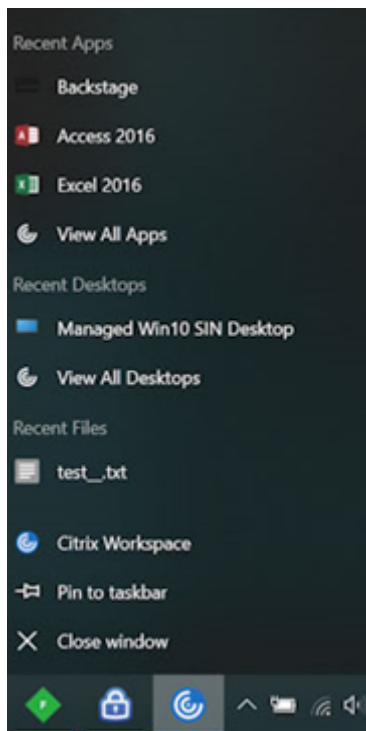
A partir de esta versión, asegúrese de que la versión de Microsoft Edge WebView2 Runtime sea 99 o una posterior. Para obtener más información, consulte [Requisitos del sistema y compatibilidad](#).

**Cambio en Citrix Casting** Antes, Citrix Casting estaba habilitado de forma predeterminada durante la instalación de la aplicación Citrix Workspace. A partir de esta versión, Citrix Casting solo se habilita si ejecuta el instalador de la aplicación Citrix Workspace con el comando

`/IncludeCitrixCasting` durante la instalación.

Al actualizar la aplicación Citrix Workspace, Citrix Casting se actualiza automáticamente. Para obtener más información sobre Citrix Casting, consulte [Citrix Casting](#).

**Acceso rápido a recursos** A partir de esta versión, puede obtener acceso rápido a aplicaciones y escritorios que haya utilizado recientemente. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace de la barra de tareas para ver y abrir los recursos utilizados recientemente en el menú emergente.



**Cerrar sesión en el almacén web personalizado al salir de la aplicación Citrix Workspace**

Cuando el atributo `signoutCustomWebstoreOnExit` tiene el valor `True`, al cerrar la aplicación Citrix Workspace se cierra la sesión en los almacenes web personalizados. Puede configurar el atributo `signoutCustomWebstoreOnExit` en **Global App Configuration Service**.

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

**Función para abrir la aplicación Citrix Workspace en modo maximizado**

A partir de esta versión, puede optar por abrir la aplicación Citrix Workspace en modo maximizado. En lugar de maximizar la aplicación Citrix Workspace de forma manual cada vez, puede establecer la propiedad `maximise workspace window` en Global App Configuration Service para permitir que la aplicación Citrix Workspace se abra en modo maximizado de forma predeterminada.

Para obtener más información sobre Global App Configuration Service, consulte [Getting Started](#).

**Función Storebrowse para Workspace** Ahora, la aplicación Citrix Workspace para Windows permite usar Storebrowse para el autoservicio, lo que permite a los usuarios de Storebrowse acceder a las funciones de Cloud y Workspace.

**Nota:**

- Esta función garantiza compatibilidad con Storebrowse solamente con Single Sign-On.
- Los requisitos previos mencionados en [Requisitos y compatibilidad del sistema](#) deben estar disponibles para usar esta función.

Para obtener más información, consulte [Storebrowse para Workspace](#).

### **Citrix Enterprise Browser**

- Esta versión incluye la versión 99.1.1.8 de Citrix Enterprise Browser, basada en la versión 99 de Chromium. Para ver las funciones o correcciones de errores de Citrix Enterprise Browser, consulte [Novedades](#) en la documentación de Citrix Enterprise Browser.
- Ahora, la aplicación Citrix Workspace le avisa sobre el cierre de ventanas activas del explorador web al hacer una de estas acciones en la aplicación Citrix Workspace:
  - Cerrar la sesión de un almacén
  - Cambiar a otro almacén
  - Agregar un nuevo almacén
  - Eliminar el almacén actual

## **2204.1**

### **Novedades**

**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.

**Citrix Enterprise Browser** Esta versión incluye la versión 98.1.2.20 de Citrix Enterprise Browser, basada en la versión 98 de Chromium. Para ver las funciones o correcciones de errores de Citrix Enterprise Browser, consulte [Novedades](#) en la documentación de Citrix Enterprise Browser.

### **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.

## Documentación antigua

Para ver las versiones de productos que han alcanzado el fin de su vida (EOL), consulte [Documentación antigua](#).

## Avisos legales de terceros

Es posible que la aplicación Citrix Workspace 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)

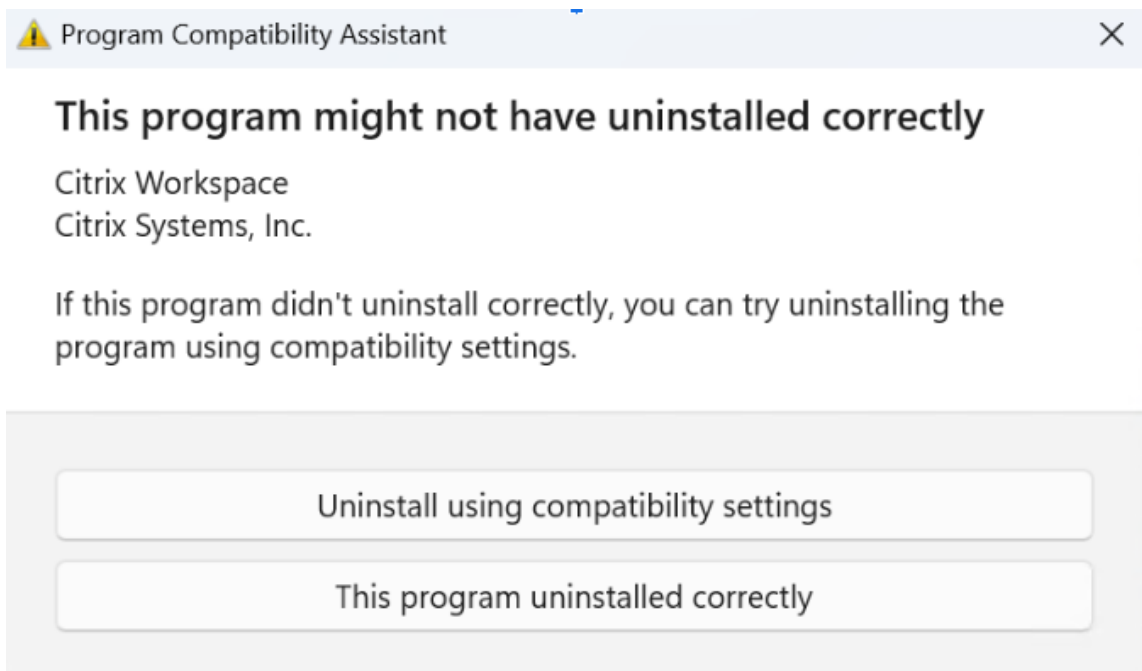
## Problemas resueltos

June 14, 2024

### Problemas resueltos en la versión 2402 LTSR

- Es posible que observe que no hay un enfoque automático dentro del escritorio virtual que se abre en modo de pantalla completa. Debe hacer clic dentro de la sesión para recuperar el enfoque. [RFWIN-32051]
- Al volver a conectar las aplicaciones publicadas, se abre una instancia adicional de una aplicación publicada. [CVADHELP-24485]
- Es posible que las claves de controlador virtual personalizadas no se conserven al desinstalar la aplicación Citrix Workspace para Windows. [CVADHELP-24513]
- Es posible que el panel táctil y el teclado virtual de Windows Surface no sean compatibles en la pantalla de inicio de sesión de la aplicación Citrix Workspace. Este problema se produce al iniciar sesión en una sesión que se publica desde Windows VDA en modo de pantalla completa. Como solución alternativa, abra la sesión en modo Ventana y, a continuación, inicie sesión en la aplicación Citrix Workspace. [RFWIN-32050]
- Se observan dos instancias de una aplicación publicada, por ejemplo, la aplicación 1, después de desconectar la aplicación 1 e iniciar otra aplicación desde el mismo VDA. [RFWIN-32517]
- Para la versión **Windows 10 32bits x86**, la casilla de verificación **Habilitar desenfoco de fondo** se ha quitado, pues el efecto de desenfoco de fondo no es compatible con esta versión. [HDX-60308]

- Es posible que el panel táctil y el teclado virtual de Windows Surface no sean compatibles en la pantalla de inicio de sesión de la aplicación Citrix Workspace. Este problema se produce al iniciar sesión en una sesión que se publica desde Windows VDA en modo de pantalla completa. [RFIN-32050]
- El audio puede estar dañado si se está reproduciendo más de un flujo al mismo tiempo en la misma página. [HDX-50486]
- Es posible que observe artefactos visuales al intentar dividir la pantalla o ajustar el monitor principal en la ficha **Diseño del monitor** de la pantalla **Preferencias**. [HDX-59798]
- El Reproductor de Windows Media (WMP) muestra una pantalla negra con la función Rave habilitada en un monitor cuando el monitor principal no es el que está más a la izquierda (cuando hay varias GPU involucradas). Para resolver este problema, el generador predeterminado se cambió de **VMR9** a **EVR**.  
Si quiere inhabilitar **EVR**, cree una DWORD AllowEvrH264=0 bajo `Computer\HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream`. [HDX-60494]
- Cuando comparte una pantalla e incluye el sonido de un equipo, si hay varios dispositivos de salida de audio reproduciendo sonido, uno o más receptores podrían notar anomalías en el sonido. [HDX-48213]
- BCR puede reproducir varios flujos de audio al mismo tiempo en lugar de un flujo activo. [HDX-61600]
- Si usa monitores externos y después cambia a un solo monitor (por ejemplo, un portátil), es posible que el tamaño de las opciones del menú de la aplicación Citrix Workspace, el texto de la interfaz de usuario y los cuadros de diálogo se vean más pequeños que el tamaño normal de la pantalla. [HDX-47575]
- Al actualizar a la versión 2402 de la aplicación Citrix Workspace, el comando `InstallEmbeddedBrowser=N` no se ejecuta si Citrix Enterprise Browser ya está instalado. [RFIN-33169]
- Si usa audio mono para los flujos de audio estéreo, es posible que solo escuche un canal de audio en un auricular en lugar de recibir ambos canales en ambos oídos. [HDX-56344]
- Al desinstalar la versión preliminar de la aplicación Citrix Workspace 2402 LTSR para Windows desde **Panel de control > Programas > Programas y funciones**, se muestra la siguiente ventana emergente:



Este problema se produce de forma intermitente en las máquinas con Windows 11. Además, este problema no se produce con ningún otro método de desinstalación, incluida la desinstalación desde **Inicio > Aplicaciones > Aplicaciones y funciones**. La desinstalación se completa correctamente aunque se muestre el mensaje de error anterior. [RFWIN-32669]

- De forma predeterminada, el proceso de inicio de la aplicación Citrix Workspace puede ejecutarse en las sesiones de aplicaciones publicadas. Si quiere ejecutar el proceso de inicio en una sesión de aplicación publicada, configure la clave de registro `RunCWAInPublishedAppSession` o escriba `DWORD` en `HKLM/Software/Wow6432Node/Citrix/ICA Client`. [CVADHELP-24070]
- No está disponible el uso compartido de pantalla desde el chat en Microsoft Teams. [HDX-62146]
- El instalador de la aplicación Citrix Workspace deja de responder durante una instalación nueva si se especifican caracteres Unicode en la línea de comandos durante la instalación. [RFWIN-32987]

## Problemas conocidos

June 14, 2024



## Problemas conocidos en la versión 2402 LTSR

- Si tiene instalada una versión anterior a la 2.9.700 de Real-Time Media Engine (RTME) en el dispositivo de punto final, es posible que no pueda abrir las aplicaciones o los escritorios publicados. Este problema se produce en la aplicación Citrix Workspace para Windows 2403 y en la aplicación Citrix Workspace para Windows 2402 LTSR. Como solución temporal, puede hacer una de las siguientes acciones:
  - Si usa Skype empresarial con el plug-in RTME, actualice RTME a la versión 2.9.700 o posterior.
  - Si no usa Skype Empresarial, desinstale HDX Real Time Pack mediante el asistente de desinstalación (agregar o quitar programas) en Windows.

Para obtener más información, consulte el artículo [CTX676765](#) de Knowledge Center. [HDX-63684]

- En un caso de doble salto, es posible que la tecla **ALT +TAB** no funcione en los clientes de macOS. [CVADHELP-23085]
- BCR MSI independiente no es compatible actualmente con una instalación que no sea de administrador. [HDX-62636]
- Si la máquina del usuario final tiene varias versiones de .Net instaladas y .Net se actualiza para la versión que no utiliza la aplicación Citrix Workspace, la aplicación se reinicia. [RFWIN-32377]

## Requisitos del sistema y compatibilidad

June 17, 2024

### Requisitos

#### Requisitos de hardware

- Mínimo 2 GB de RAM.
- 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	1 GB

---

Tipo de instalación	Espacio de disco requerido
Actualizaciones	1 GB

---

**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 `\Citrix\Logs\CTXWorkspaceInstallLogs-*`.

### Requisitos de software

- Versión 119 de Microsoft Edge WebView2 Runtime o una posterior
- .NET Framework 4.8 y .NET Desktop Runtime 6.0.20 o posterior
- La versión más reciente de Microsoft Visual C++ Redistributable

**Nota:**

Para gestionar los parches de seguridad de Microsoft u otros componentes dependientes de terceros (por ejemplo, .NET Core, .NET Framework, VC redistributable, Edge webview), puede utilizar uno de estos métodos:

- Habilitar la actualización automática de Windows en las máquinas cliente
- Los administradores de TI administrarán la implementación de parches mediante herramientas como SCCM

### Requisitos de Microsoft Edge WebView2

- 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](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
- Conexión a Internet
- El dispositivo debe tener acceso a estas URL:

**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

### Requisitos previos

- .NET Framework 4.8 y versión x86 de .NET Desktop Runtime 6.0.20 o posterior. Debe instalar la versión x86 incluso en un sistema x64.
- En caso de instalar .NET como parte de la instalación de la aplicación Citrix Workspace, asegúrese de tener conexión a Internet.
- Privilegios de administrador

**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 cuando ni .NET Framework 4.8 ni .NET Desktop Runtime 6.0.20 o posterior no están presentes en el sistema.

## Métodos de instalación

---

Versión de .NET

¿Cómo realizar la implementación?

---

La aplicación Citrix Workspace 1904 o posterior requiere .NET Framework 4.8. Junto con .NET Framework 4.8, la aplicación Citrix Workspace 2309 o versiones posteriores requieren la versión x86 de .NET Desktop Runtime 6.0.20 o posterior tanto para sistemas x86 como para sistemas x64.

Método 1: La aplicación Citrix Workspace instala .NET Framework 4.8 y la versión más reciente de .NET Desktop Runtime 6.0 durante la instalación de la aplicación. Esta instalación es una instalación en línea y requiere conectividad a Internet. El dispositivo debe tener acceso a la URL de dominio

[downloadplugins.citrix.com](https://downloadplugins.citrix.com).

Método 2: En el caso de los dispositivos que no tienen conexión a Internet, los administradores tienen la opción de descargar un instalador sin conexión para la aplicación Citrix Workspace, disponible en la página [Descargas](#). Además, el administrador puede instalar estos requisitos mediante un método de implementación, como, por ejemplo, SCCM.

Método 3: Los administradores pueden instalar [.NET Framework 4.8](#) y [.NET Desktop Runtime 6.0.20](#) desde el sitio de Microsoft por separado antes de instalar la aplicación Citrix Workspace. Se recomienda descargar la versión más reciente de .NET Desktop Runtime 6.0 (6.0.20 o una posterior).

---

**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.

## Requisitos de conectividad

**Administrar marcas de función** Si se produce un problema con la aplicación Citrix Workspace en producción, use marcas de función y un servicio de terceros llamado LaunchDarkly para inhabilitar dinámicamente las funciones afectadas en la aplicación Citrix Workspace incluso después de que se haya publicado la función.

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 direccionalidad.

Puede permitir el tráfico a estas URL:

- [events.launchdarkly.com](#)
- [stream.launchdarkly.com](#)
- [clientstream.launchdarkly.com](#)
- [Firehose.launchdarkly.com](#)
- [mobile.launchdarkly.com](#)

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 **Inhabilitar el envío de datos a terceros** y actívelo.
4. Haga clic en **Aplicar** y **Aceptar**.

## Puertos

Para obtener información sobre los puertos necesarios, consulte [Puertos de comunicación comunes de Citrix](#).

## 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](#).

### Nota:

- El plug-in del análisis de punto final (EPA) de Citrix Gateway está disponible en Citrix Workspace. En la aplicación nativa de Citrix Workspace, solo se ofrece al utilizar la autenticación nFactor. Para obtener más información, consulte [Configure pre-auth and post-auth EPA scan as a factor in nFactor authentication](#) en la documentación de Citrix ADC.
- La instalación de la aplicación Citrix Workspace en Windows solo se admite cuando los clientes cuentan con asistencia y mantenimiento generales o ampliados de Microsoft.
- La aplicación Citrix Workspace para Windows solamente se admite en modo de emulación en el sistema operativo Windows ARM64.
- 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.

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

---

## 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](#).

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

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	2206 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	Versión 2311 y posteriores
22H2	22621	2209 y versiones posteriores
21H2	22000	2109.1 y versiones posteriores

## Instalación y desinstalación

June 14, 2024

Puede descargar la aplicación Citrix Workspace desde la [página de descargas](#) de Citrix o desde la página de descargas de su empresa (si está disponible).

Puede instalar el paquete de la siguiente manera:

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

**Nota:**

Compruebe que instaló todos los requisitos del sistema necesarios, tal y como se menciona en la sección [Requisitos del sistema](#).

### 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](#), [Single Sign-On](#), [App Protection](#), el [plug-in VDI de Microsoft Teams](#) 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	Para 64 bits: C:\Archivos de programa (x86)\Citrix\ICA Client, y para 32 bits: C:\Archivos de programa\Citrix\ICA Client	Instalación por sistema
Usuario	%USERPROFILE%\AppData\Local\Citrix\ICA Client	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.

## Comando para borrar e instalar la aplicación Citrix Workspace

Use el comando `/CleanInstall` para borrar rastros que hayan quedado, como archivos y valores del Registro, de una desinstalación anterior y, a continuación, instale de nuevo la nueva versión de la aplicación Citrix Workspace.

Por ejemplo:

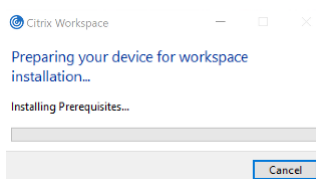
```
1 CitrixWorkspaceApp.exe /CleanInstall
2 <!--NeedCopy-->
```

## Instalación por la interfaz de usuario

Para instalar la aplicación Citrix Workspace para Windows, ejecute manualmente el paquete del instalador **CitrixWorkspaceApp.exe**.

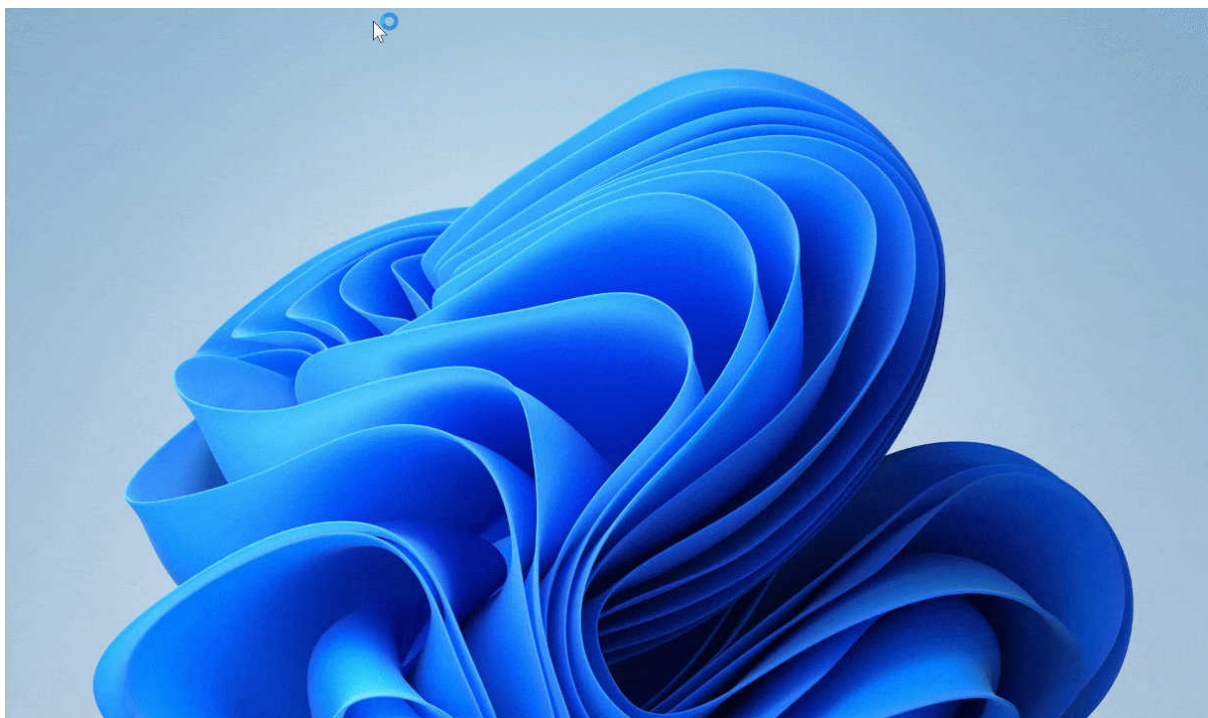
1. Abra el archivo `CitrixWorkspaceApp.exe`.

El sistema verifica los requisitos previos necesarios para la aplicación Citrix Workspace y, si es necesario, la instala automáticamente.



Tras instalar los requisitos previos, aparece la pantalla **Le damos la bienvenida al instalador de Citrix Workspace**.

2. Haga clic en **Continuar**. Aparece la página **Contrato de licencia de Citrix**.
3. Lea y acepte el contrato de licencia de Citrix y continúe con la instalación. La instalación de la aplicación Citrix Workspace continúa y se completa correctamente.
4. Al realizar la instalación con privilegios de administrador, si es necesario habilitar la función de App Protection, marque la casilla **Iniciar App Protection tras la instalación**. La instalación de la aplicación Citrix Workspace continúa y se completa correctamente.



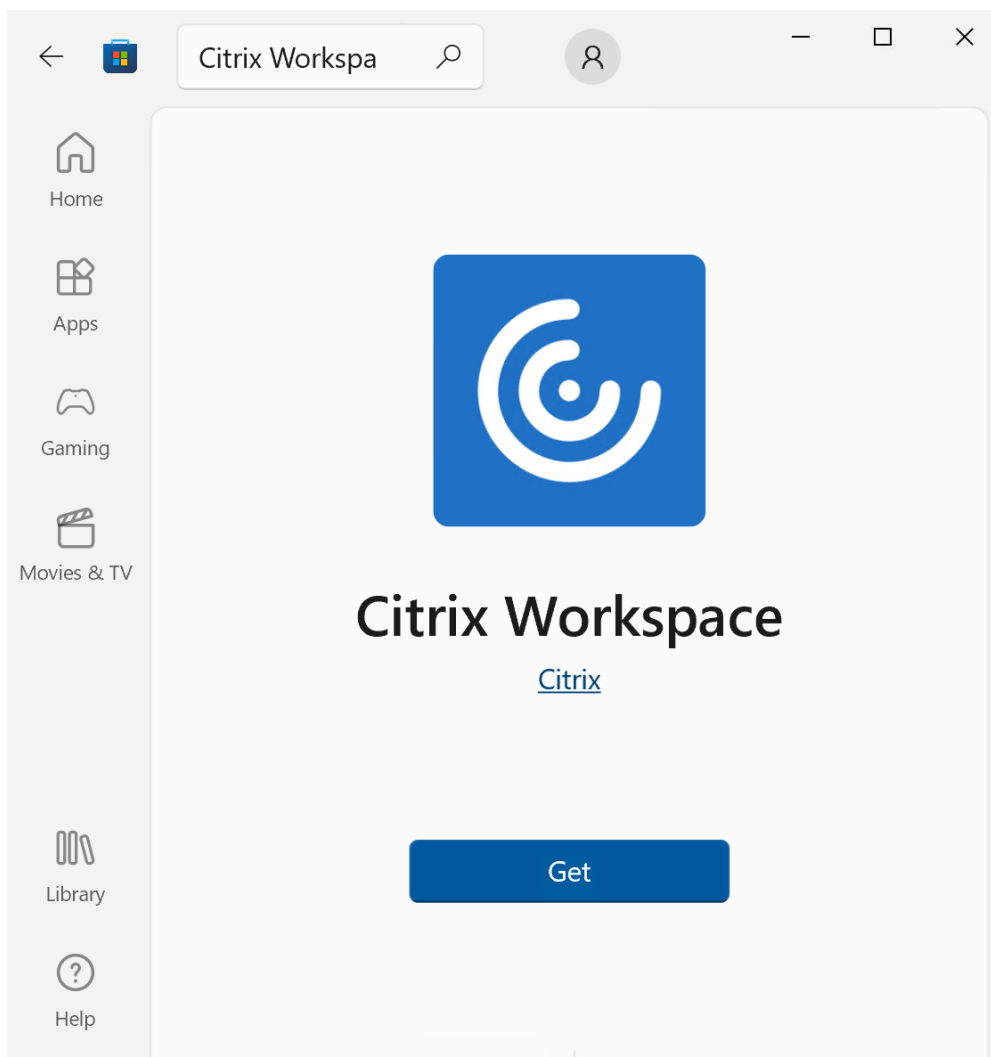
### **Importante:**

El TrolleyExpress se sustituye por CWAInstaller-`<date and timestamp>`. Por ejemplo, el registro se graba en `C:\Program Files (x86)\Citrix\Logs\CTXWorkspaceInstallLogs-20231225-093441`.

## **Mediante la Tienda Windows**

1. Vaya a Microsoft Store.

## 2. Busque Citrix Workspace.



1. Haga clic en **Get**. La aplicación Citrix Workspace se instala.

### Instalación mediante la 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`]

### Listado de parámetros de la línea de comandos

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

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

### Parámetros comunes

---

Comando	Descripción
<code>? O bien, help</code>	Enumera todos los comandos y propiedades de instalación.
<code>/silent</code>	Inhabilita los cuadros de diálogo y solicitudes de instalación durante la instalación.
<code>noreboot</code>	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.
<code>/forceinstall</code>	Este modificador es efectivo al limpiar cualquier configuración existente o entradas de la aplicación Citrix Workspace que hubiera en el sistema. Utilice este modificador cuando actualice una versión no compatible de la aplicación Citrix Workspace y cuando la instalación o la actualización no se realicen correctamente.

---

**Nota:**

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

## Actualizar parámetros automáticamente

### Detectar actualizaciones disponibles

- Comando: `AutoUpdateCheck`
- Descripción: Este comando indica que la aplicación Citrix Workspace detecta cuándo hay una actualización disponible.

Los valores posibles son los siguientes:

Valores del comando	Descripción	Ejemplo
<code>AutoUpdateCheck</code>		
Automático (predeterminado)	Recibirá una notificación cuando haya una actualización disponible.	<code>CitrixWorkspaceApp.exe AutoUpdateCheck=auto.</code>
Manual	No recibirá una notificación cuando haya actualizaciones disponibles. Compruebe manualmente si hay actualizaciones.	<code>CitrixWorkspaceApp.exe AutoUpdateCheck&gt;manual</code>
Inhabilitado	Inhabilita las actualizaciones automáticas.	<code>CitrixWorkspaceApp.exe AutoUpdateCheck=disabled.</code>

**Nota:**

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

### Seleccionar la versión que actualizar

- Comando `AutoUpdateStream`
- Descripción: Si habilitó la actualización automática, puede elegir la versión que quiere actualizar. Consulte [Hitos del ciclo de vida](#) para obtener más información.

Los valores posibles son los siguientes:

Valor del comando	Descripción	Ejemplo
AutoUpdateStream		
LTSR	Actualizaciones automáticas solamente para actualizaciones acumulativas de Long Term Service Release.	<code>CitrixWorkspaceApp.exe AutoUpdateStream=LTSR.</code>
Actual	Actualizaciones automáticas para la versión más reciente de la aplicación Citrix Workspace.	<code>CitrixWorkspaceApp.exe AutoUpdateStream=Current</code>

### Aplazar las notificaciones de las actualizaciones

- Comando: [DeferUpdateCount](#)
- Descripción: Indica las veces que puede aplazar las notificaciones cuando haya una actualización disponible. Para obtener más información, consulte [Actualizaciones de Citrix Workspace](#).

Los valores posibles son los siguientes:

Valor del comando	Descripción	Ejemplo
DeferUpdateCount		
-1(predeterminado)	Permite aplazar notificaciones tantas veces como quiera	<code>CitrixWorkspaceApp.exe DeferUpdateCount=-1</code>
0	Indica que recibirá (solo) una notificación por cada actualización disponible. No le recuerda de nuevo la actualización.	<code>CitrixWorkspaceApp.exe DeferUpdateCount=0</code>
Cualquier otro número “n”	<ul style="list-style-type: none"> <li>• Permite aplazar la notificación “n”veces. La opción <b>Recordármelo más tarde</b> se podrá mostrar tantas veces como indique el valor “n”</li> </ul>	<code>CitrixWorkspaceApp.exe DeferUpdateCount=&lt;n&gt;</code>

**Nota:**

A partir de la versión 2207 de la aplicación Citrix Workspace para Windows, se ha mejorado la función de actualización automática y el parámetro `DeferUpdatCount` no se aplica.

**Definir la prioridad de la implantación**

- Comando: `AURolloutPriority`
- Descripción: 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.

Los valores posibles son los siguientes:

---

Valor del comando	Descripción	Ejemplo
<code>AURolloutPriority</code>		
Automático (predeterminado)	Recibe las actualizaciones durante el período de entrega configurado por Citrix.	<code>CitrixWorkspaceApp.exe AURolloutPriority=Auto</code>
Rápido	Recibe las actualizaciones al comienzo del período de entrega.	<code>CitrixWorkspaceApp.exe AURolloutPriority=Fast</code>
Medio	Recibe las actualizaciones a mitad del período de entrega.	<code>CitrixWorkspaceApp.exe AURolloutPriority=Medium</code>
Lento	Recibe las actualizaciones al final del período de entrega.	<code>CitrixWorkspaceApp.exe AURolloutPriority=Slow</code>

---

**Parámetros de configuración de almacenes**

**Configurar almacén**

- Comando: `ALLOWADDSTORE`
- Descripción: Permite configurar los almacenes (HTTP o HTTPS) en función del parámetro especificado.

Los valores posibles son los siguientes:

Valor del comando	Descripción	Ejemplo
ALLOWADDSTORE		
S (predeterminado)	Permite agregar o quitar solamente almacenes seguros (configurados con HTTPS).	<code>CitrixWorkspaceApp.exe ALLOWADDSTORE=S</code>
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.	<code>CitrixWorkspaceApp.exe ALLOWADDSTORE=A</code>
N	No permite nunca que los usuarios agreguen o quiten su propio almacén.	<code>CitrixWorkspaceApp.exe ALLOWADDSTORE=N</code>

### Guardar las credenciales del almacén de forma local

- Comando: `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.

Los valores posibles son los siguientes:

Valor del comando	Descripción	Ejemplo
ALLOWSAVEPWD		
• S (predeterminado)	Permite guardar contraseñas solamente para almacenes seguros (configurados con HTTPS).	<code>CitrixWorkspaceApp.exe ALLOWSAVEPWD=S</code>
N	No permite guardar contraseñas.	<code>CitrixWorkspaceApp.exe ALLOWSAVEPWD=N</code>
A	Permite que los usuarios guarden contraseñas tanto para almacenes seguros (HTTPS) como no seguros (HTTP).	<code>CitrixWorkspaceApp.exe ALLOWSAVEPWD=A</code>



## Ejemplos de configuración de almacén con la instalación mediante la línea de comandos

### Para especificar la URL de almacén de StoreFront:

```
1 CitrixWorkspaceApp.exe /silent
2 STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;HR
  App Store
3
4 <!--NeedCopy-->
```

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

```
1 CitrixWorkspaceApp.exe STORE0= HRStore;https://ag.mycompany.com#
  Storename;On;Store
2 <!--NeedCopy-->
```

Donde, **Storename** indica el nombre del almacén que debe configurarse.

#### Nota:

- En una configuración con varios almacenes, solo se permite la configuración de una URL de almacén de Citrix Gateway, que debe estar en primer lugar en la lista (parámetro STORE0).
- La URL de almacén de Citrix Gateway configurada con este método no admite los sitios de servicios de PNA que utilicen Citrix Gateway.
- El parámetro "Discovery" no es necesario cuando se especifica una URL de almacén de Citrix Gateway.

### Para configurar varios almacenes:

```
1 CitrixWorkspaceApp.exe STORE0= NetScaler Store;https://ag.mycompany.
  com#Storename;On;NetScaler Store
2 STORE1="StoreFront Store;https://testserver.net/Citrix/MyBackupStore/
  discovery;on; StoreFrontStore
3 <!--NeedCopy-->
```

#### 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.

## Parámetros de instalación

### Iniciar App Protection

- Comando: `startAppProtection`

- Descripción: Inicia el componente App Protection y proporciona una seguridad mejorada porque restringe la posibilidad de que los clientes corran peligro por parte de malware que registra las pulsaciones de teclas y captura pantallas.
- Ejemplo: `CitrixWorkspaceApp.exe startAppProtection`

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

**Nota:**

El modificador `startAppProtection` reemplaza al modificador `includeAppProtection`. El modificador `includeAppProtection` ha sido retirado. Para obtener más información, consulte [Elementos retirados](#).

### Excluir los binarios de Citrix Enterprise Browser

- Comando: `InstallEmbeddedBrowser`
- Descripción: Excluye los binarios de Citrix Enterprise Browser.
- Ejemplo: Ejecute el modificador `InstallEmbeddedBrowser=N` para excluir la función del explorador integrado.

Puede excluir los binarios de Citrix Enterprise Browser solo en los siguientes casos:

- Instalación nueva
- Actualice una versión que no incluya los binarios de Citrix Enterprise Browser.

Si la versión de la aplicación Citrix Workspace incluye los binarios del Citrix Enterprise Browser y usted va a actualizar a la versión 2002, los binarios de Citrix Enterprise Browser se actualizan automáticamente durante la actualización.

### Especificar el directorio de instalación personalizado

- Comando: `INSTALLDIR`
- Descripción: Especifica el directorio de instalación personalizado para la instalación de la aplicación Citrix Workspace. La ruta predeterminada es `C:\Program Files\Citrix`.
- Ejemplo: `CitrixWorkspaceApp.exe INSTALLDIR=C:\custom path\Citrix`.

**Nota:**

La carpeta **Archivos de programa** está protegida por el sistema operativo. Si quiere utilizar una carpeta personalizada que no sea Archivos de programa, asegúrese de que la carpeta tenga los permisos correctos y que esté protegida.

### Instalar al menos uno de los componentes específicos

- Comando: `ADDLOCAL`

- Descripción: Utilice la clave `ADDLOCAL` para instalar uno o varios componentes específicos de la aplicación Citrix Workspace. Con esta clave, si instala algún componente específico, la aplicación Citrix Workspace instala todos los componentes obligatorios de forma predeterminada.

**Nota:**

Le recomendamos que utilice la clave `ADDLOCAL` solo si quiere instalar alguno de los componentes específicos de la aplicación Citrix Workspace. De forma predeterminada, si no se especifica ningún parámetro `ADDLOCAL`, se instalan todos los componentes compatibles durante la instalación de la aplicación Citrix Workspace.

En la siguiente tabla se enumeran los componentes compatibles con la clave `ADDLOCAL`:

Clave <code>ADDLOCAL</code>	Nombre del componente	Descripción
<code>ReceiverInside</code>	Receiver	Proporciona los servicios del SDK de Workspace al plug-in de autoservicio.
<code>ICA_Client</code>	Motor HDX	Este componente gestiona el proceso de inicio de sesión o archivo ICA.
<code>BCR_Client</code>	Cliente BCR	Plug-in para gestionar la redirección de contenido del explorador.
<code>USB</code>	Cliente USB	Plug-in para realizar la redirección USB.
<code>DesktopViewer</code>	Cliente Desktop Viewer	Marco de interfaz de usuario para escritorio virtual.
<code>AM</code>	AuthManager	Administrador de autenticación: Autoriza al usuario a acceder a la aplicación Citrix Workspace.
<code>SSON</code>	SSON	Componente Single Sign-On: Admite Single Sign-On (SSO).
<code>SELSERVICE</code>	Autoservicio	Plug-in para inicio nativo de Citrix Workspace.
<code>WebHelper</code>	Web Helper	Ayudante para conectar el explorador con la aplicación de espacio de trabajo nativa.

Clave ADDLOCAL	Nombre del componente	Descripción
<code>CitrixEnterpriseBrowser</code>	Explorador web	Explorador nativo que permite a los usuarios abrir aplicaciones web o SaaS desde la aplicación Citrix Workspace de forma segura.
<code>EPAClient</code>	Cliente EPA	Plug-in para realizar escaneos de Endpoint Analysis.

Por ejemplo, con el siguiente comando, puede instalar los componentes mencionados en el comando:

```
1 CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,BCR_Client,
   USB,DesktopViewer,AM,SSON,SelfService,WebHelper,
   CitrixEnterpriseBrowser
2 <!--NeedCopy-->
```

**Nota:**

La función App Protection se instala de forma predeterminada. Como resultado, `AppProtection` ya no es una opción válida para ADDLOCAL.

## Instalar Citrix Casting

**Importante:**

En la versión 2402 y posteriores de la aplicación Citrix Workspace LTSR, Citrix Casting no se puede instalar, ni siquiera con el comando `IncludeCitrixCasting`. Para usar esta función, debe usar una versión anterior de la aplicación Citrix Workspace. Para obtener más información, consulte la página [Elementos retirados](#).

- Comando: `IncludeCitrixCasting`
- Descripción: Instala Citrix Casting durante la instalación.

Para obtener más información sobre Citrix Casting, consulte [Citrix Casting](#).

## Parámetros de funciones HDX

### Configurar la redirección bidireccional de contenido

- Comando: `ALLOW_BIDIRCONTENTREDIRECTION`
- Descripción: 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.

Los valores posibles son los siguientes:

Valor del comando ALLOW_BIDIRCONTENTREDIRECTION	Descripción	Ejemplo
0 (predeterminado)	Indica que la redirección bidireccional de contenido está inhabilitada.	<code>CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=0</code>
1	Indica que la redirección bidireccional de contenido está habilitada.	<code>CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=1</code>

### Configurar el acceso a aplicaciones locales

- Comando: [FORCE\\_LAA](#)
- Descripción: 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. Para obtener más información, consulte la sección [Acceso a aplicaciones locales](#) en la documentación de Citrix Virtual Apps and Desktops.

Los valores posibles son los siguientes:

Valor del comando FORCE_LAA	Descripción	Ejemplo
0 (predeterminado)	Indica que el componente de acceso a aplicaciones locales no está instalado.	<code>CitrixWorkspaceApp.exe FORCE_LAA =0</code>
1	Indica que el componente de acceso a aplicaciones locales del cliente está instalado.	<code>CitrixWorkspaceApp.exe FORCE_LAA =1</code>

### Configurar la función de redirección de URL en el dispositivo del usuario

- Comando: [ALLOW\\_CLIENTHOSTEDAPPSURL](#)
- Descripción: Habilita la función de redirección de URL en el dispositivo del usuario. Para obtener más información, consulte la sección [Acceso a aplicaciones locales](#) en la documentación de Citrix Virtual Apps and Desktops.

Los valores posibles son los siguientes:

Valor del comando ALLOW_CLIENTHOSTEDAPPSURL	Descripción	Ejemplo
0 (predeterminado)	Inhabilita la función de redirección de URL en el dispositivo del usuario.	<code>CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=0</code>
1	Habilita la función de redirección de URL en los dispositivos de usuario.	<code>CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=1</code>

### Mostrar iconos para documentos o archivos

- Comando: `LEGACYFTAICONS`
- Descripción: Especifica si quiere mostrar iconos de documentos o archivos que tienen asociaciones de tipo de archivo con aplicaciones suscritas.

Los valores posibles son los siguientes:

Valor del comando LEGACYFTAICONS	Descripción	Ejemplo
False (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.	<code>CitrixWorkspaceApp.exe LEGACYFTAICONS=False</code>

Valor del comando

LEGACYFTAICONS	Descripción	Ejemplo
True	No muestra iconos de documentos o archivos que tienen asociaciones de tipo de archivo con aplicaciones suscritas.	<code>CitrixWorkspaceApp.exe LEGACYFTAICONS=True</code>

**Parámetros de preferencias e interfaz de usuario**

**Especificar el directorio para los accesos directos en el menú Inicio y en el escritorio**

Valor del comando	Descripción	Nombre del directorio	Ejemplo
<code>CitrixWorkspaceApp.exe STARTMENUDIR</code>	Especifica el directorio para los accesos directos en el menú Inicio.	De forma predeterminada, las aplicaciones aparecen en <b>Inicio &gt; Todos los programas</b> . Puede especificar la ruta relativa de los accesos directos en la carpeta <code>Programs</code> .	Para colocar accesos directos en <b>Inicio &gt; Todos los programas &gt; Workspace</b> , especifique <code>STARTMENUDIR=Workspace</code> .
<code>CitrixWorkspaceApp.exe DESKTOPDIR</code>	Especifica el directorio para los accesos directos del escritorio.	Puede especificar la ruta relativa de los accesos directos.	Para colocar accesos directos en <b>Inicio &gt; Todos los programas &gt; Workspace</b> , especifique <code>DESKTOPDIR=Workspace</code> .

**Nota:**

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

**Controlar el acceso al autoservicio**

- Comando: `SELSERVICEMODE`

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

Los valores posibles son los siguientes:

Valor del comando	Descripción	Ejemplo
SELFSEVICEMODE		
True	Indica que el usuario tiene acceso a la interfaz de usuario de autoservicio.	<code>CitrixWorkspaceApp.exe SELFSEVICEMODE=True</code>
False	Indica que el usuario no tiene acceso a la interfaz de usuario de autoservicio.	<code>CitrixWorkspaceApp.exe SELFSEVICEMODE=False</code>

### Controlar el preinicio de sesiones

- Comando: [ENABLEPRELAUNCH](#)
- Descripción: Controla el preinicio de sesiones. Para obtener más información, consulte [Tiempo de inicio de aplicaciones](#).

Los valores posibles son los siguientes:

Valor del comando	Descripción	Ejemplo
ENABLEPRELAUNCH		
True	Indica que el preinicio de sesiones está habilitado.	<code>CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True</code>
False	Indica que el preinicio de sesiones está inhabilitado.	<code>CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False</code>

### Ocultar accesos directos y la opción de reconexión

- Comando: [DisableSetting](#)
- Descripción: Oculta la opción **Accesos directos y reconexión** para que no se muestre en la hoja **Preferencias avanzadas**. Para obtener más información, consulte [Ocultar parámetros concretos de la hoja de Preferencias avanzadas](#).

Los valores posibles son los siguientes:



Valor del comando	Descripción	Ejemplo
DisableSetting		
0 (predeterminado)	Muestra tanto la opción de <b>Accesos directos</b> como la de <b>Reconexión</b> en la hoja Preferencias avanzadas.	<code>CitrixWorkspaceApp.exe DisableSetting=0</code>
1	Muestra solo la opción <b>Reconexión</b> en la hoja Preferencias avanzadas.	<code>CitrixWorkspaceApp.exe DisableSetting=1</code>
2	Muestra solo la opción <b>Accesos directos</b> en la hoja Preferencias avanzadas.	<code>CitrixWorkspaceApp.exe DisableSetting=2</code>
3	Oculto tanto la opción de <b>Accesos directos</b> y la de <b>Reconexión</b> en la hoja Preferencias avanzadas.	<code>CitrixWorkspaceApp.exe DisableSetting=3</code>

### Habilitar el programa Customer Experience Improvement Program

- Comando: [EnableCEIP](#)
- Descripción: Indica su participación en el programa CEIP de mejora de la experiencia del cliente. Para obtener más información, consulte [CEIP](#).

Los valores posibles son los siguientes:

Valor del comando EnableCEIP	Descripción	Ejemplo
True (predeterminado)	Participa en el programa Citrix Customer Improvement Program (CEIP).	<code>CitrixWorkspaceApp.exe EnableCEIP=True</code>
False	Rechazar la participación en el programa Customer Experience Improvement Program de Citrix.	<code>CitrixWorkspaceApp.exe EnableCEIP=False</code>

### Habilitar el seguimiento permanente

- Comando: [EnableTracing](#)
- Descripción: Controla la función de **Seguimiento permanente (Always-on tracing)**.

Los valores posibles son los siguientes:

Valor del comando	Descripción	Ejemplo
EnableTracing		
True (predeterminado)	Habilita la función de <b>Seguimiento permanente (Always-on tracing)</b> .	<code>CitrixWorkspaceApp.exe EnableTracing=true</code>
False	Inhabilita la función de <b>Seguimiento permanente (Always-on tracing)</b> .	<code>CitrixWorkspaceApp.exe EnableTracing=false</code>

### Especificar el nombre utilizado para identificar el dispositivo del usuario

- Comando: `CLIENT_NAME`
- Descripción: 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%`.
- Ejemplo: `CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%`.

### Configurar el nombre del cliente igual que el nombre del equipo

- Comando: `ENABLE_DYNAMIC_CLIENT_NAME`
- Descripción: 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.

Los valores posibles son los siguientes:

Valor del comando EN-ABLE_DYNAMIC_CLIENT_NAME	Descripción	Ejemplo
Sí (predeterminado)	Permite que el nombre del cliente sea el mismo que el nombre del equipo.	<code>CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=Yes</code>
No	No permite que el nombre del cliente sea el mismo que el nombre del equipo. Especifique un valor para la propiedad <code>CLIENT_NAME</code> .	<code>CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No</code>

## Parámetros de autenticación

### Incluir Single Sign-On

- Comando: `/includeSSON`
- Descripción: 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.
- Ejemplo: `CitrixWorkspaceApp.exe /includeSSON`

#### Nota:

El comando `includeSSON` solo admite la instalación nueva de la aplicación Citrix Workspace.

### Habilitar Single Sign-On

- Comando: `ENABLE_SSON`
- Descripción: Habilita Single Sign-On cuando se instala la aplicación Citrix Workspace con el comando `/includeSSON`. Para obtener más información, consulte [Autenticación PassThrough de dominio](#).

Los valores posibles son los siguientes:

Valor del comando	Descripción	Ejemplo
<code>ENABLE_SSON</code>		
Sí (predeterminado)	Indica que Single Sign-On está habilitado.	<code>CitrixWorkspaceApp.exe ENABLE_SSON=Yes</code>
No	Indica que Single Sign-On está inhabilitado.	<code>CitrixWorkspaceApp.exe ENABLE_SSON=No</code>

## Desinstalar la aplicación Citrix Workspace

### Desinstalación mediante un desinstalador basado en Windows

Puede desinstalar la aplicación Citrix Workspace para Windows desde el **Panel de control**. Para obtener más información, consulte la sección [Desinstalar la aplicación Citrix Workspace para 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.

## Desinstalar mediante la interfaz de línea de comandos

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

```
1 CitrixWorkspaceApp.exe /uninstall
2 <!--NeedCopy-->
```

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

```
1 CitrixWorkspaceApp.exe /silent /uninstall
2 <!--NeedCopy-->
```

### 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.

## Solución de problemas

### Códigos de error

- Para ver los códigos de error relacionados con el instalador, consulte [MsiExec.exe y mensajes de error de InstMsi.exe](#).
- Para ver los códigos de error relacionados con el sistema, consulte [Códigos de error del sistema](#).

### Ubicación de los registros del instalador

De forma predeterminada, los registros del instalador se encuentran en esta ubicación:

	Carpeta de registros de instalación	Tipo de instalación
Administrador	Para 64 bits: C:\Archivos de programa (x86)\Citrix\Logs, y para 32 bits: C:\Archivos de programa\Citrix\ICA Client	Instalación por sistema
Usuario	%USERPROFILE%\AppData\Local\Citrix\Logs	Instalación por usuario

**Nota:**

El `TrolleyExpress` se sustituye por `CWAInstaller-<date and timestamp>`. Por ejemplo, el registro se graba en `C:\Program Files (x86)\Citrix\Logs\CTXWorkspaceInstallLogs-20231225-093441`.

## Solución de problemas

### Códigos de error

- Para ver los códigos de error relacionados con el instalador, consulte [MsiExec.exe y mensajes de error de InstMsi.exe](#).
- Para ver los códigos de error relacionados con el sistema, consulte [Códigos de error del sistema](#).

### Ubicación de los registros del instalador

De forma predeterminada, los registros del instalador se encuentran en esta ubicación:

	Carpeta de registros de instalación	Tipo de instalación
Administrador	Para 64 bits: C:\Archivos de programa (x86)\Citrix\Logs, y para 32 bits: C:\Archivos de programa\Citrix\ICA Client	Instalación por sistema
Usuario	%USERPROFILE%\AppData\Local\Citrix\Logs	Instalación por usuario

## 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:

```
1 "C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe  
  " -cleanUser  
2 <!--NeedCopy-->
```

Para el restablecimiento silencioso, use este comando:

```
1 "C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe  
  " /silent -cleanUser  
2 <!--NeedCopy-->
```

**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.

## Implementación

June 14, 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.

Para obtener información sobre cómo crear una unidad organizativa en Azure Active Directory, consulte [Cree una unidad organizativa \(OU\) en un dominio administrado de Azure Active Directory Domain Services](#).

## 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	CheckAndDeployWorkspacePerMachineStartUpScript.bat	CheckAndRemoveWorkspacePerMachineStartUpScript.bat
Por usuario	CheckAndDeployWorkspacePerUserLoginScript.bat	CheckAndRemoveWorkspacePerUserLoginScript.bat

---

#### 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 el número de versión actual de la aplicación Citrix Workspace.

**Nota:**

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

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

- **Comportamiento de instalación:** Instalar para el sistema.
  - **Requisito de inicio de sesión:** Si un usuario inició sesión.
  - **Visibilidad del programa de instalación:** Normal
- Haga clic en **Siguiente**.

**Nota:**

No especifique requisitos ni dependencias para este tipo de implementación.

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

Aparecerá un mensaje indicando que la conexión tuvo lugar.

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

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

### Agregar puntos de distribución

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

Aparecerá el asistente para distribuir contenido.

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

Aparecerá el cuadro de diálogo para agregar puntos de distribución.

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

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

4. Haga clic en **Cerrar**.

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

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

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

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

En los dispositivos de punto final, la aplicación Citrix Workspace está visible en el Centro de software, en **Software disponible**. La instalación se activa automáticamente en función de la programación 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 seleccionar la 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.

## Configuración del almacén

June 14, 2024

### Almacén

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

Un **almacén** reúne las aplicaciones y los escritorios disponibles para un usuario en un mismo lugar. Un usuario puede tener varios almacenes y cambiar de uno a otro según sea necesario. Un administrador entrega la URL del almacén que tiene recursos y ajustes preconfigurados. Puede acceder a estos almacenes a través de la aplicación Citrix Workspace.

## Tipos de almacenes

Puede agregar los siguientes tipos de almacenes en la aplicación Citrix Workspace: Workspace, StoreFront, almacén de Citrix Gateway y almacén web personalizado.

### Workspace

Citrix Workspace es un almacén de aplicaciones de empresa basado en la nube que proporciona acceso seguro y unificado a aplicaciones, escritorios y contenido (recursos) desde cualquier lugar y en cualquier dispositivo. Estos recursos pueden ser Citrix DaaS, aplicaciones de contenido, aplicaciones locales y móviles, aplicaciones web y SaaS y aplicaciones para explorador web. Para obtener más información, consulte [Descripción general de Citrix Workspace](#).

### StoreFront

StoreFront es un intuitivo almacén de aplicaciones de empresa local que combina aplicaciones y escritorios de los sitios de Citrix Virtual Apps and Desktops en un solo almacén.

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

### Almacén de Citrix Gateway

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.

### 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](#).

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**.



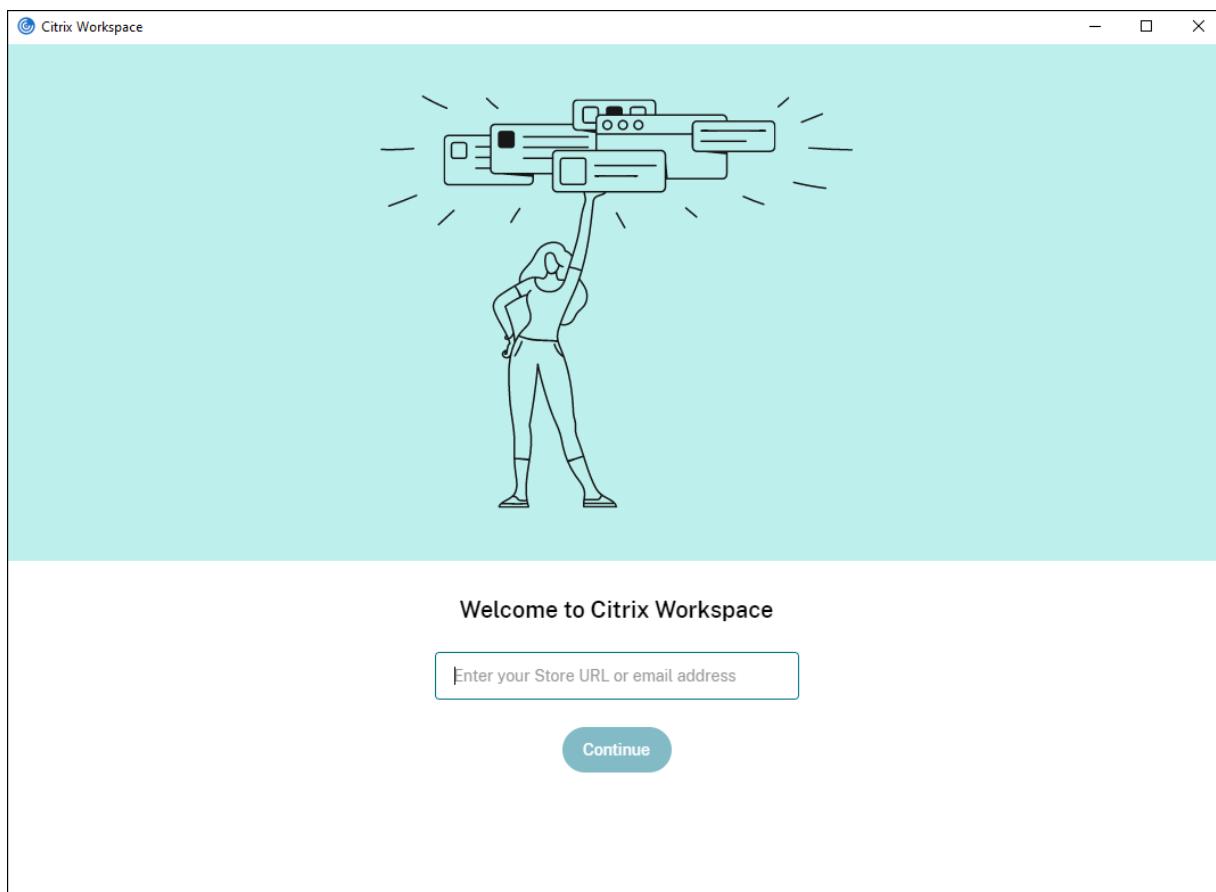
## Agregar URL de almacén a la aplicación Citrix Workspace

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

- Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente
- Configurar la detección de cuentas basada en direcciones de correo electrónico
- Agregar almacén a través de la CLI
- Archivo de aprovisionamiento
- Usar la plantilla administrativa de objeto de directiva de grupo

## 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, distribuya 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:

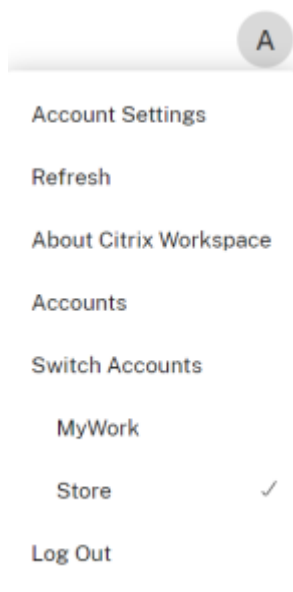
**CitrixGatewayFQDN?MyStoreName:**

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.



En las máquinas cliente configuradas para la autenticación de proxy, si las credenciales de proxy no se almacenan en el **Administrador de credenciales de Windows**, aparece un mensaje de autenticación en el que se le pide que introduzca las credenciales del proxy. A continuación, la aplicación Citrix Workspace guarda las credenciales del servidor proxy en el **Administrador de credenciales de Windows**. Esto simplifica la experiencia de inicio de sesión porque no necesita guardar manualmente las credenciales en el **Administrador de credenciales de Windows** antes de acceder a la aplicación Citrix Workspace.

### 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 configurar la detección de cuentas basada en correo electrónico para los almacenes de Citrix Workspace, consulte la sección [Getting started](#) en la documentación de Global App Configuration Service.

Para configurar la detección de cuentas basada en correo electrónico para los almacenes de Citrix StoreFront o Citrix Gateway, consulte [Configuring email-based account discovery](#).

## Agregar almacén a través de la CLI

Instale la aplicación Citrix Workspace para Windows como administrador desde la interfaz de línea de comandos.

Para obtener más información, consulte [Lista de parámetros de la línea de comandos](#).

## 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.

**Usar la plantilla administrativa de objeto de directiva de grupo** Para agregar o especificar un Citrix StoreFront o 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. Seleccione la opción **Habilitado** y haga clic en **Mostrar**. Si habilita esta configuración de directiva, puede introducir una lista de cuentas de StoreFront y una URL de NetScaler Gateway.
5. Introduzca la URL en el campo **Valor**.
6. Especifique la URL del almacén que se utiliza con la aplicación Citrix Workspace:

```
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, como “Almacén de aplicaciones de RR. HH.”

7. Agregue o especifique la URL de Citrix Gateway. Introduzca el nombre de la dirección URL separada por punto y coma:

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

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

**Nota:**

- La URL del almacén de Citrix Gateway debe ser la primera de la lista (parámetro STORE0).
- En una configuración con varios almacenes, solo se permite la configuración de una URL de almacén de Citrix Gateway.
- La URL de almacén de Citrix Gateway configurada con este método no admite los sitios de servicios de PNA que utilicen Citrix Gateway.
- El parámetro `/Discovery` no es necesario cuando se especifica una URL de almacén 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:**

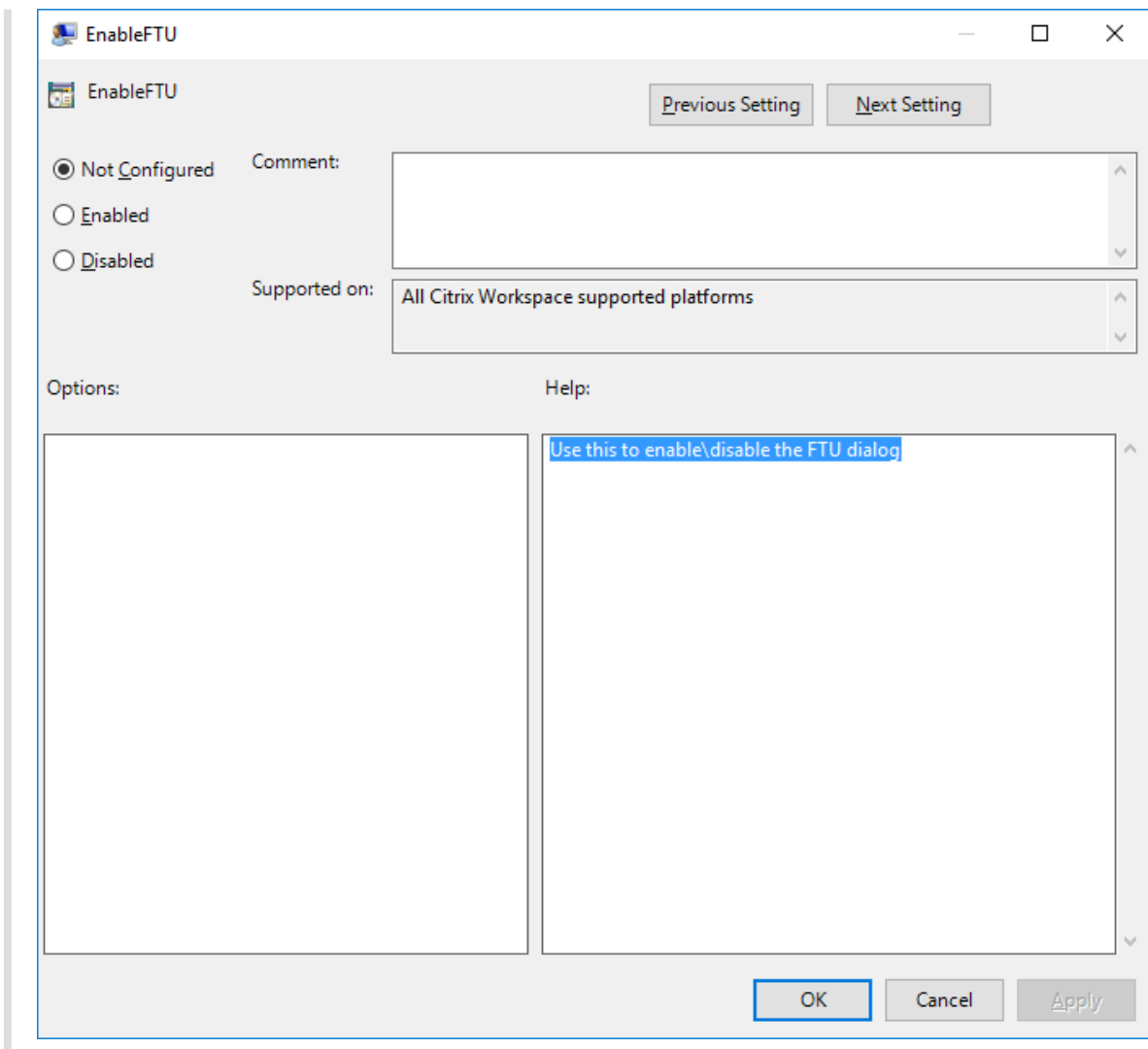
- La URL de Citrix Gateway debe incluirse en primer lugar, seguida de direcciones URL de StoreFront.
- No está disponible la opción de usar varias direcciones URL de Citrix Gateway.

**Nota:**

Los usuarios también pueden acceder al almacén desde un explorador web. Los usuarios pueden iniciar sesión en Citrix Store desde un explorador web e iniciar una aplicación virtual o un escritorio desde la Web. El inicio de aplicaciones o escritorios virtuales aprovecha las capacidades de la aplicación Citrix Workspace instalada de forma nativa.

En este caso, puede ser conveniente ocultar la solicitud **Agregar cuenta** a los usuarios. Esto se puede hacer mediante la siguiente configuración:

- **Cambiar el nombre del archivo de ejecución de Citrix:** Cambie el nombre de **Citrix-WorkspaceApp.exe** a **CitrixWorkspaceAppWeb.exe** para modificar el comportamiento del cuadro de diálogo **Agregar cuenta**. Al cambiar el nombre del archivo, el diálogo **Agregar cuenta** no aparece en el menú **Inicio**.
- **Plantilla administrativa de GPO:** Para ocultar la opción **Agregar cuenta** en el asistente de instalación de la aplicación Citrix Workspace, inhabilite **EnableFTUpolicy** en el nodo Autoservicio de la plantilla administrativa de GPO, como se muestra a continuación. Como este es un parámetro por máquina, el comportamiento se aplica a todos los usuarios.



## 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 modificarlo.

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

## Conectar

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

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

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

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



## Migración de URL de StoreFront a Workspace

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 la configuración 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
3   "serviceURL": {
4
5     "url": "https://storefront.acme.com:443",
6     "migrationUrl": [
7       {
8
9         "url": "https://sampleworkspace.cloud.com:443",
10        "storeFrontValidUntil": "2023-05-01"
11      }
12    ]
13  ]
14 }
15 ,
16 "settings": {
17
18   "name": "Productivity Apps",
19   "description": "Provides access StoreFront to Workspace Migration"
20 ,
```

```
20 "useForAppConfig": true,  
21 "appSettings": {  
22  
23   "windows": [  
24     {  
25  
26       "category": "root",  
27       "userOverride": false,  
28       "assignmentPriority": 0,  
29       "assignedTo": [  
30         "AllUsersNoAuthentication"  
31       ],  
32       "settings": [  
33         {  
34  
35           "name": "Hide advanced preferences",  
36           "value": false  
37         }  
38  
39       ]  
40     }  
41  
42   ]  
43 }  
44  
45 }  
46  
47 }  
48  
49  
50 <!--NeedCopy-->
```

**Nota:**

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

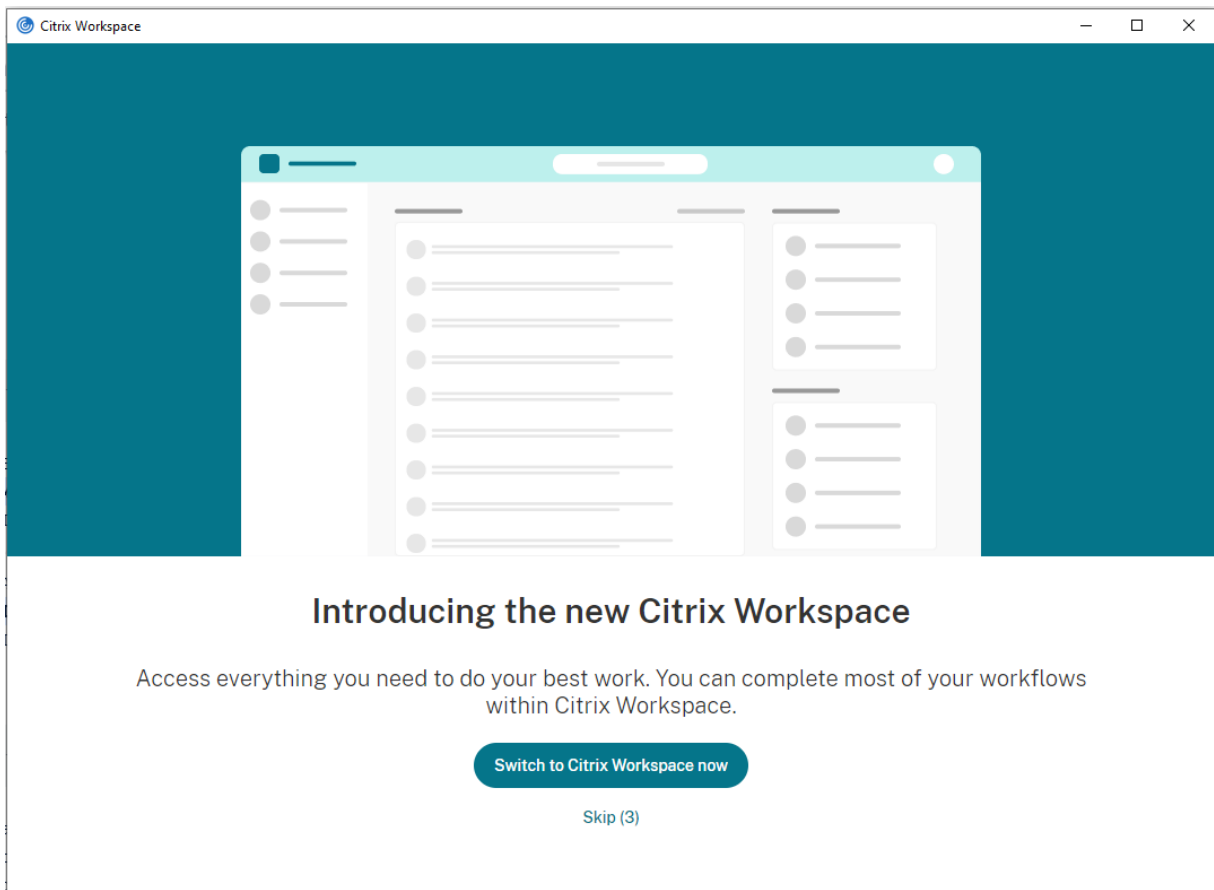
Si piensa modificar la configuración de la carga útil existente, utilice **PUT** y compruebe que tiene una carga útil que consta de todos los parámetros compatibles.

3. Especifique la URL de StoreFront `storefront.com` como el valor de **URL** en la sección **serviceURL**.
4. Configure la URL del espacio de trabajo `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.

Después de enviar los parámetros del servicio de configuración de la aplicación, aparece 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.

### **Función de detección de aplicaciones locales dentro de la aplicación Citrix Workspace**

A partir de la versión 2112.1, los administradores pueden configurar la detección y la enumeración de aplicaciones instaladas localmente dentro de la aplicación Citrix Workspace. Puede configurar esta función mediante Global App Configuration Service. Para obtener más información sobre cómo configurar esta función, consulte [Global App Configuration Service](#).

Esta función es ideal para dispositivos en modo quiosco y para aquellas aplicaciones que no se pueden virtualizar dentro de Citrix Workspace.

## Administración de actualizaciones y plug-ins

April 22, 2024

En esta sección se describe lo siguiente:

- [Actualizaciones](#)
- [Administración de plug-ins](#)

## Actualización

June 14, 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 para Windows 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 inhabilitadas en el VDA. Esto incluye máquinas de servidor multiusuario RDS, máquinas 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. Aparece una notificación cuando hay actualizaciones disponibles de HDX RTME tanto en la versión LTSR como en la versión Current Release 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.
- También puede realizar la actualización automática cuando están habilitadas la detección del protocolo de detección automática de proxies web (WPAD) y la configuración automática de proxy (PAC). Esto no se admite cuando el proxy requiere credenciales para la autenticación.
- Si se agrega un conjunto de cifrado que no sea EDCHE, la aplicación Citrix Workspace no puede contactar con el servidor de actualización automática de Citrix, y aparece este error durante la actualización automática:

### **No se puede conectar con el servidor**

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

Puede comprobar la versión actual de la aplicación Citrix Workspace instalada en su dispositivo a través de **Preferencias avanzadas** o consultar el registro **DisplayVersion** desde la ubicación `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\`

`CurrentVersion\Uninstall\CitrixOnlinePluginPackWeb.`

Para ver la versión en **Preferencias avanzadas**:

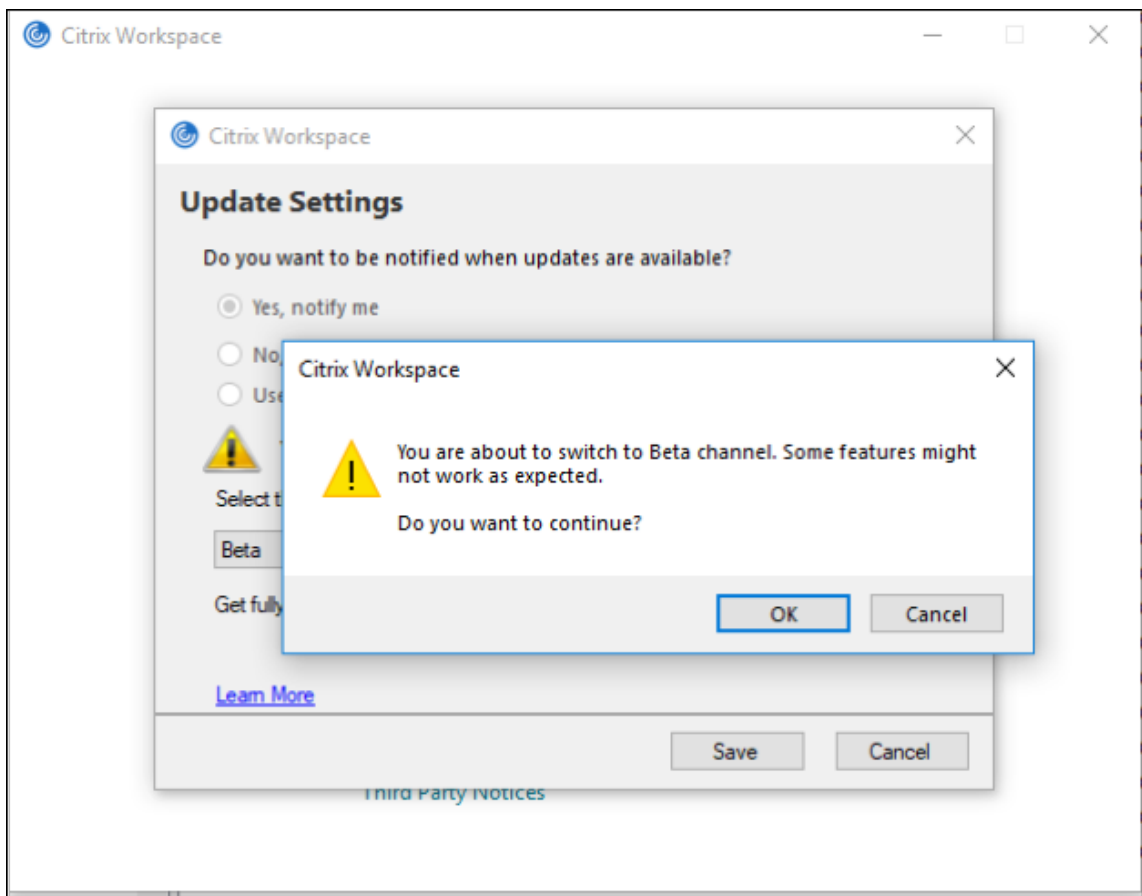
1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace situado en el área de notificaciones.
2. Seleccione **Preferencias avanzadas**.

La versión de la aplicación Citrix Workspace aparece en la sección **Acerca de**.

### **Instalar el programa Beta de la aplicación Citrix Workspace**

Recibirá una notificación de actualización cuando la Citrix Workspace se haya configurado para obtener actualizaciones automáticas. Para instalar la compilación Beta en el sistema, siga estos pasos:

1. Abra la aplicación Citrix Workspace desde el área de notificaciones.
2. Vaya a **Preferencias avanzadas > Actualizaciones de Citrix Workspace**.
3. Seleccione **Beta** en la lista desplegable cuando la compilación Beta esté disponible y haga clic en **Guardar**.  
Aparecerá una ventana de notificación.



4. Haga clic en **Aceptar** para actualizar su versión a la versión Beta.

Para cambiar de una compilación Beta a una compilación pública, siga estos pasos:

1. Abra la aplicación Citrix Workspace desde el área de notificaciones.
2. Vaya a **Preferencias avanzadas > Actualizaciones de Citrix Workspace**.
3. En la pantalla **Parámetros de actualización**, seleccione **Público** en la lista desplegable “Canal de actualización” y haga clic en **Guardar**.

**Nota:**

- Si hay nuevas actualizaciones disponibles, aparece una notificación de actualización automática.
- Las compilaciones beta están disponibles para que los clientes las prueben en sus entornos de producción limitados o en entornos que no son de producción y para compartir comentarios. Citrix no acepta casos de asistencia de compilaciones beta, pero agradece [comentarios](#) para mejorarlas. Citrix puede o no actuar a partir de los comentarios en función de su gravedad e importancia. No es aconsejable implementar compilaciones beta en entornos de producción.

## **Función de actualización automática de la aplicación Citrix Workspace en VDA**

A partir de la versión 2209 de la aplicación Citrix Workspace para Windows, puede habilitar la función de actualización automática en VDA. Para habilitar esta función, debe crear el siguiente valor de Registro:

En una máquina de 32 bits:

- Clave del Registro: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\AutoUpdate
- Valor del Registro: AllowAutoUpdateOnVDA
- Tipo de Registro: REG\_SZ
- Datos del Registro: True

En una máquina de 64 bits:

- Clave del Registro: HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\AutoUpdate
- Valor del Registro: AllowAutoUpdateOnVDA
- Tipo de Registro: REG\_SZ
- Datos del Registro: True

## **Control de versiones con actualización automática**

Ahora, los administradores pueden administrar la versión de las actualizaciones automáticas de los dispositivos de la organización.

Los administradores pueden controlar la versión estableciéndola en la propiedad `maximumAllowedVersion` de Global App Config Service.

Ejemplo de archivo JSON en Global App Config Service:

```
1 {
2
3   "category": "AutoUpdate",
4   "userOverride": false,
5   "assignedTo": [
6     "AllUsersNoAuthentication"
7   ],
8   "settings": [
9     {
10
11       "name": "Auto Update plugins settings",
12       "value": [
13         {
14
15           "pluginSettings": {
16
17             "upgradeToLatest": false,
18             "deploymentMode": "InstallAndUpdate",
```



```
19     "stream": "Current",
20     "maximumAllowedVersion": "23.03.0.49",
21     "minimumAllowedVersion": "0.0.0.0",
22     "delayGroup": "Fast"
23   }
24   ,
25     "pluginName": "WorkspaceApp",
26     "pluginId": "1CDF566D-B2C7-47CA-802F-6283C862E1D6"
27   }
28
29   ]
30 }
31
32 ]
33 }
34
35
36 <!--NeedCopy-->
```

Cuando se establece la versión, la aplicación Citrix Workspace del dispositivo del usuario se actualiza automáticamente con la versión especificada en la propiedad `maximumAllowedVersion`.

#### Notas:

- Actualmente, todos los parámetros mencionados en el archivo JSON anterior son obligatorios. Debe proporcionar valores para los parámetros `upgradeToLatest` y `maximumAllowedVersion` en función de los requisitos de su organización. Sin embargo, para el resto de parámetros, puede utilizar valores similares a los del archivo JSON de ejemplo.
- Para efectuar el control de versiones de las actualizaciones automáticas, el parámetro `upgradeToLatest` de Global App Config Service debe estar establecido en `false`. Si tiene el valor `true`, `maximumAllowedVersion` se ignorará.
- No modifique `pluginId`, ya que está asignado a la aplicación Citrix Workspace.
- Si el administrador no ha configurado la versión en Global App Config Service, la aplicación Citrix Workspace se actualiza a la versión disponible más reciente de forma predeterminada.

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

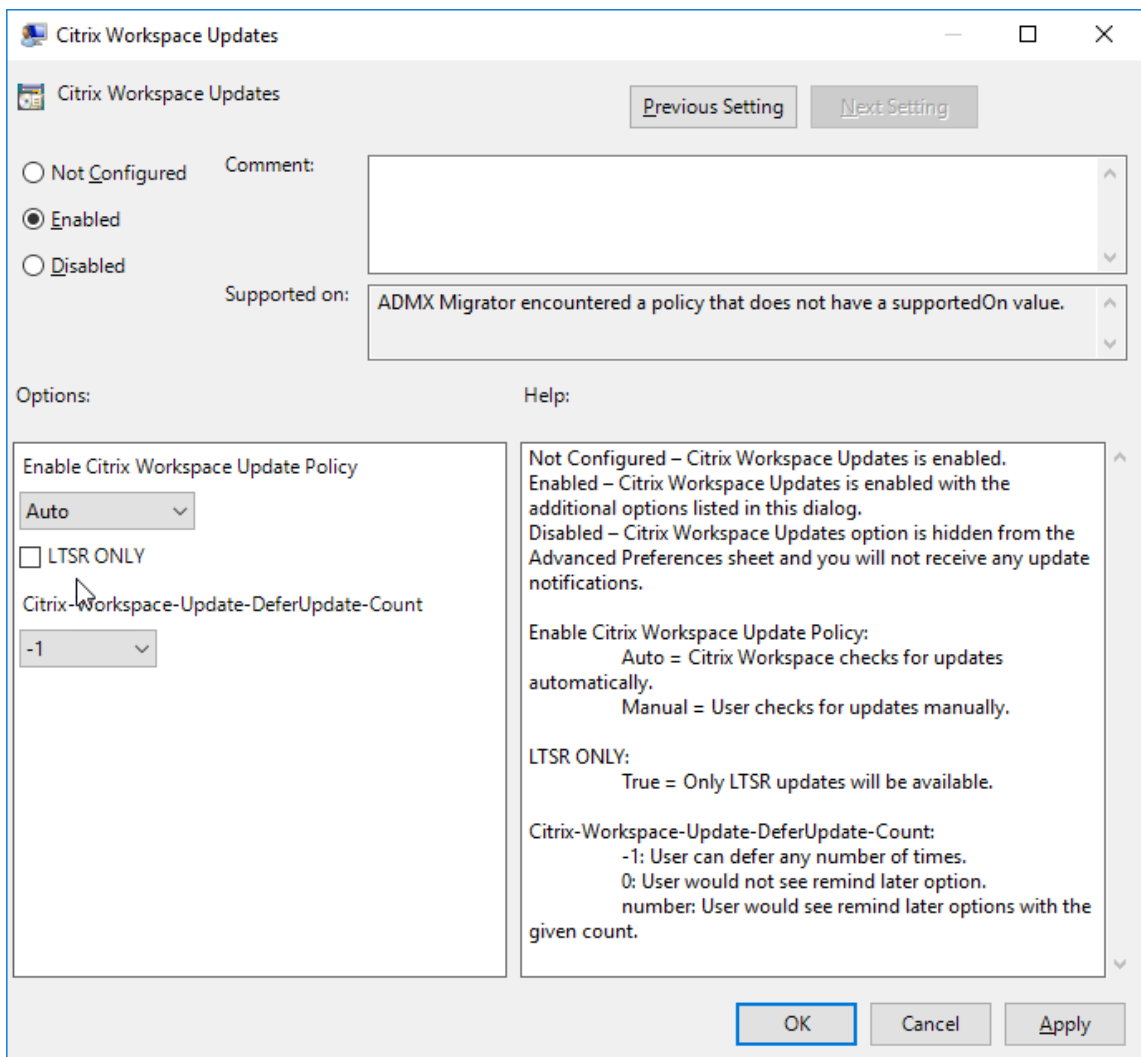
Puede configurar Actualizaciones de Citrix Workspace con estos métodos:

1. Plantilla administrativa de objetos de directiva de grupo (GPO)
2. Global App Configuration Service (GACS)
3. Interfaz de línea de comandos
4. Interfaz gráfica (GUI)

5. 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.**



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:**

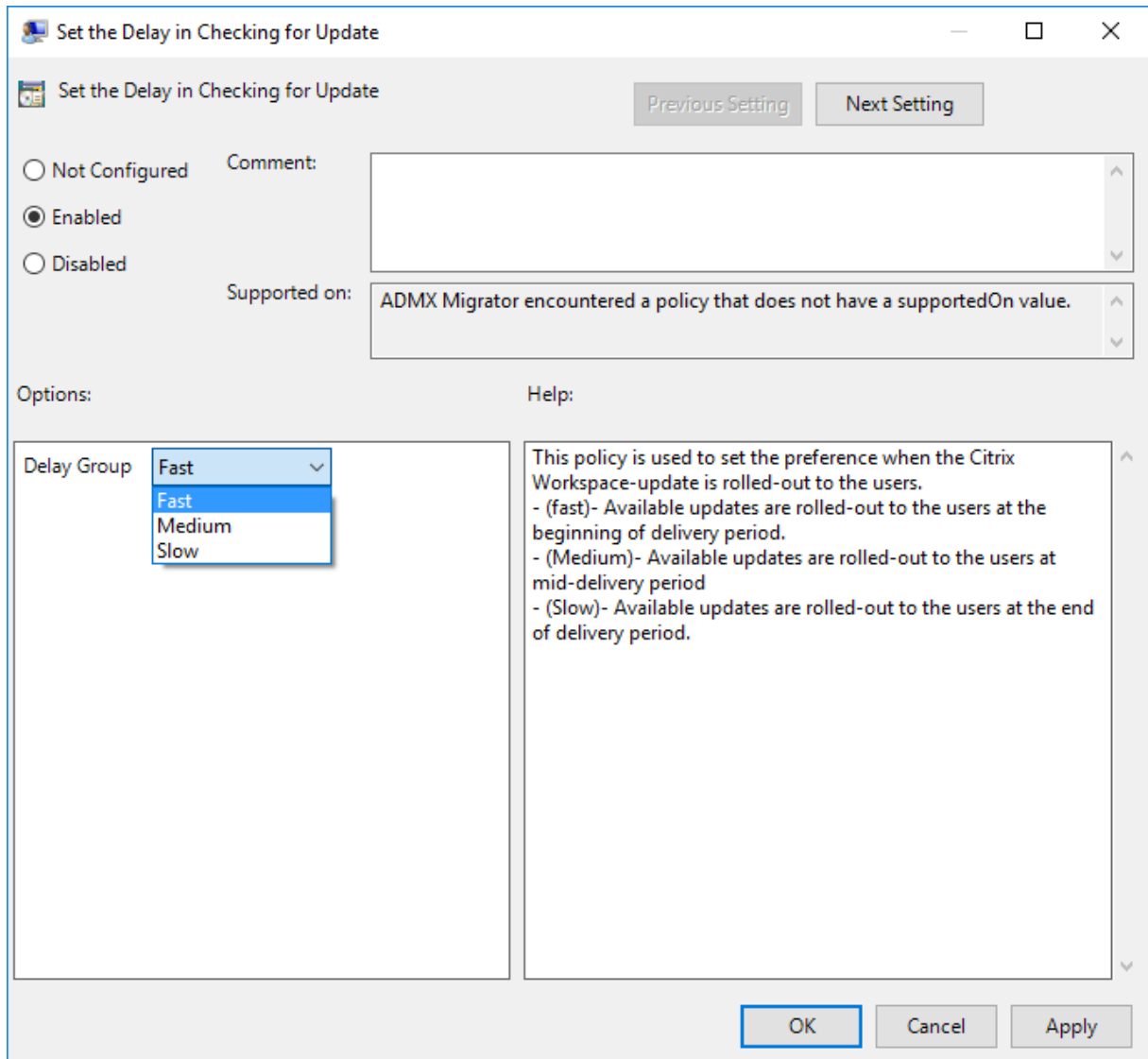
- Auto: Se le notificará cuando haya una actualización disponible (predeterminado). Esto solo se aplica a las versiones anteriores a la aplicación Citrix Workspace 2207. A partir de la versión 2207, la actualización de la aplicación Citrix Workspace es automática y no se le notificará cuando haya una actualización disponible.
  - 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, no 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**.

**Nota:**

A partir de la versión 2207 de la aplicación Citrix Workspace para Windows, se ha mejorado la función de actualización automática y no se requiere el campo **Citrix-Workspace-Update-DeferUpdate-Count**.

**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 Actualizaciones de Citrix Workspace mediante la interfaz de línea de comandos

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

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

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

Actualizaciones de Citrix Workspace se puede configurar después de instalar la aplicación Citrix Workspace para Windows. 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

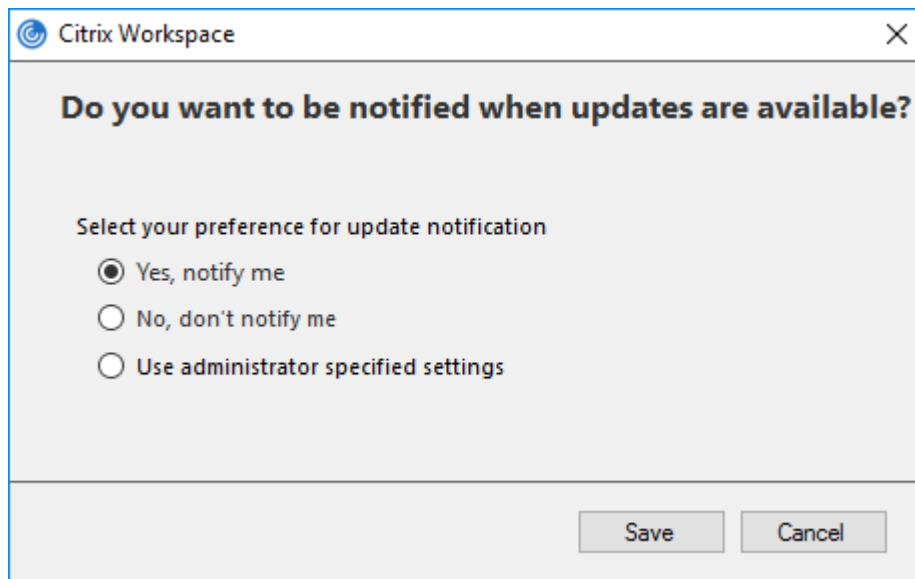
Un usuario individual puede supeditar el parámetro **Actualizaciones de Citrix Workspace** desde el cuadro de diálogo **Preferencias avanzadas**. Se trata de una configuración específica de usuario y los parámetros se aplican solamente al usuario actual.

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 una de estas opciones de preferencias de notificación:

- **Sí, notificarme:** Se le notificará cuando haya una actualización disponible para la aplicación Citrix Workspace.
- **No, no notificarme:** No se le notificará cuando haya una actualización disponible para la aplicación Citrix Workspace. Compruebe si hay actualizaciones manualmente.
- **Usar parámetros especificados por el administrador:** Usa los parámetros configurados en el servidor de StoreFront.



4. Haga clic en **Guardar**.

**Nota:**

- Las opciones **Sí, notificarme** y **No, no notificarme** solo se aplican a versiones anteriores a la aplicación Citrix Workspace 2207. A partir de la versión 2207, la actualización de la aplicación Citrix Workspace es automática y no se le notificará cuando haya una actualización disponible. Si selecciona la opción **No, no notificarme**, compruebe si hay actualizaciones manualmente.
- 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 Actualizaciones de Citrix Workspace mediante StoreFront

1. Utilice un editor de texto para abrir el archivo `web.config`, que normalmente se encuentra en `C:\inetpub\wwwroot\Citrix\Roaming directory`.

- 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-->

```

- 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"
8             remoteAccessType="None">
9
10        <annotatedServices>
11
12            <clear />
13
14            <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
15
16                <metadata>
17
18                    <plugins>
19
20                        <clear />
21
22                    </plugins>
23
24                    <trustSettings>
25
26                        <clear />
27
28                    </trustSettings>
29
30                    <properties>
31
32                        <property name="Auto-Update-Check" value="auto" />
33
34                        <property name="Auto-Update-DeferUpdate-Count" value
35                            ="1" />
36
37                            <property name="Auto-Update-LTSR-Only" value
38                                ="FALSE" />

```

```

37         <property name="Auto-Update-Rollout-Priority" value=
           "fast" />
38
39         </properties>
40
41     </metadata>
42
43 </annotatedServiceRecord>
44
45 </annotatedServices>
46
47 <metadata>
48
49     <plugins>
50
51         <clear />
52
53     </plugins>
54
55     <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 (predeterminado): Comprueba y realiza las actualizaciones automáticamente
  - Manual: Las actualizaciones solo se obtienen cuando el usuario realiza una solicitud de comprobación desde el menú de la bandeja del sistema de la aplicación Citrix Workspace,
  - Disabled: No se realizan comprobaciones de actualizaciones.
- **Auto-update-LTSR-Only:** Indica que la actualización es solamente para LTSR.
  - True: El programa de actualización ignora las actualizaciones que no estén marcadas como válidas para LTSR. Solo se tienen en cuenta las actualizaciones LTSR.



- False (predeterminado) : El programa de actualización solo considera las actualizaciones por stream actuales.
- **Auto-Update-Rollout-Priority:** Indica el período de entrega en el que puede recibir la actualización.
  - Fast: Las actualizaciones se envían a los usuarios hacia el comienzo del período de entrega.
  - Medium: Las actualizaciones se implementan hacia la mitad del período de entrega.
  - Slow: Las actualizaciones se implementan al final del período de entrega.
- **Auto-update-DeferUpdate-Count:** Indica el número de veces que puede aplazar las notificaciones relativas a las actualizaciones.

**Nota:**

Esta configuración solo es aplicable a las actualizaciones interactivas y no cuando la función de actualización automática silenciosa está habilitada, ya que el usuario no tiene una opción para aplazar las actualizaciones.

- -1: El usuario puede posponer la actualización cuantas veces quiera.
- 0: El usuario no puede ver la opción de recordatorio.
- número: El usuario puede ver las opciones de recordatorio la cantidad de veces especificada.

## Administración de plug-ins

June 14, 2024

La aplicación Citrix Workspace para Windows ofrece funcionalidad de administración de plug-ins, lo que la convierte en la única aplicación cliente necesaria en el dispositivo de punto final para instalar y administrar agentes, como el agente de Secure Access y el plug-in End Point Analysis (EPA).

Con esta capacidad, los administradores pueden implementar y administrar fácilmente los agentes necesarios desde una única consola de administración.

La administración de plug-ins incluye estos pasos:

- Los administradores deben especificar los agentes necesarios en los dispositivos de los usuarios finales en Global App Configuration Service. Los administradores pueden especificar el agente de Secure Access y el agente de Endpoint Analysis (EPA).
- La aplicación Citrix Workspace obtiene la lista de agentes de Global App Configuration Service.

- Según la lista obtenida de Global App Configuration Service, la aplicación Citrix Workspace descarga los paquetes de agente a través del servicio de actualización automática. Si el agente no se ha instalado anteriormente en el dispositivo de punto final, la aplicación Citrix Workspace desencadena la instalación del agente. Si el agente ya está instalado, la aplicación Citrix Workspace desencadena una actualización del agente (si la versión del agente descargado es posterior a la versión instalada).

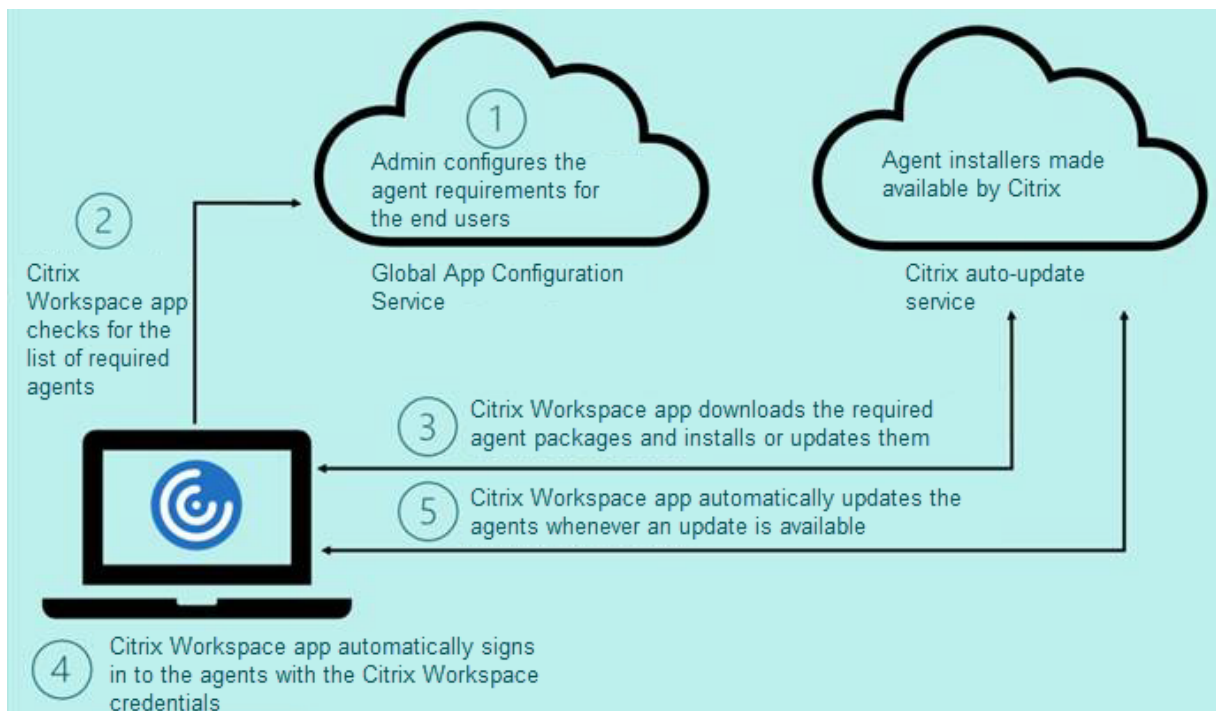
La aplicación Citrix Workspace garantiza la actualización automática de los agentes siempre que haya una actualización disponible en el futuro.

La aplicación Citrix Workspace inicia sesión automáticamente en los agentes con las credenciales de Citrix Workspace.

**Notas:**

- Si los plug-ins de EPA y ZTNA no existen, se descargan y se instalan al agregar el almacén o la cuenta por primera vez.
- Si el almacén o la cuenta y los plug-ins ya existen y el instalador contiene una versión posterior, los plug-ins se actualizan durante el ciclo de actualización automática.

El siguiente diagrama ilustra el flujo de trabajo:



**Importante:**

Se requiere Global App Configuration Service para habilitar la función de administración de plug-ins.

- Para los almacenes de la nube, se puede acceder a la interfaz de usuario de Global App Configuration Service en la sección **Configuración de Workspace** del portal de administración de Citrix Cloud. Para obtener más información, consulte [Configurar la aplicación Citrix Workspace](#).
- Para incorporar almacenes locales o si los clientes necesitan configurar la detección por correo electrónico para los almacenes de la nube, consulte la documentación de [Global App Configuration Service](#).

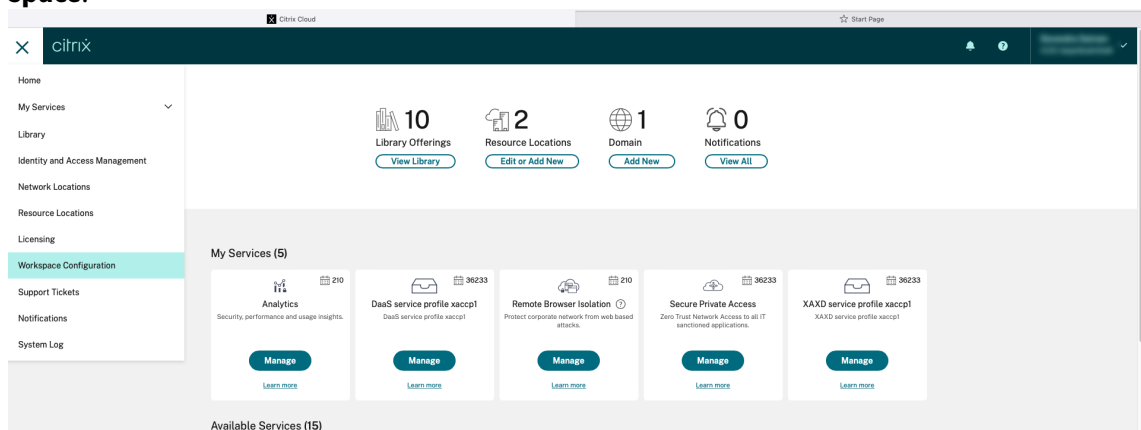
Puede habilitar la función de administración de plug-ins con estos métodos:

- Usar la interfaz de usuario de Global App Configuration Service: Use este método para implementar la versión más reciente del cliente.
- Usar la API de Global App Configuration Service: Use este método para personalizar la instalación mediante parámetros con el fin de controlar la versión, los modos de implementación, los intervalos de actualización automática...

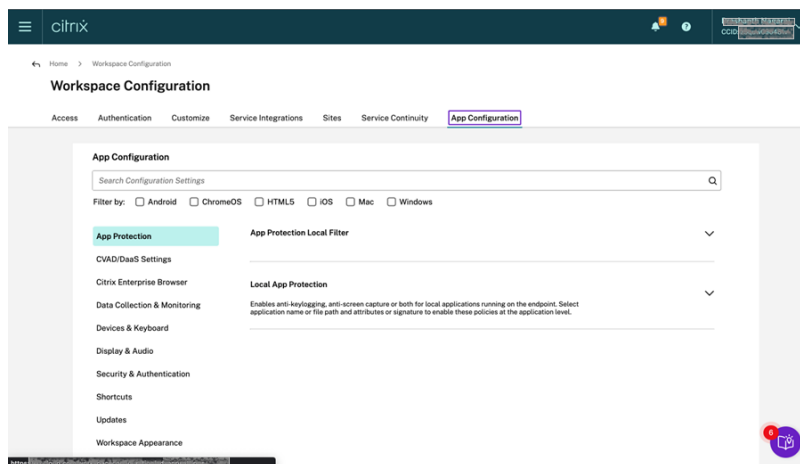
### Habilitar la administración de plug-ins mediante la interfaz de usuario de Global App Configuration Service

Este método solo se aplica a los almacenes de la nube. Los administradores pueden implementar agentes (EPA/Secure Access, Zoom o WebEx) mediante la interfaz de usuario.

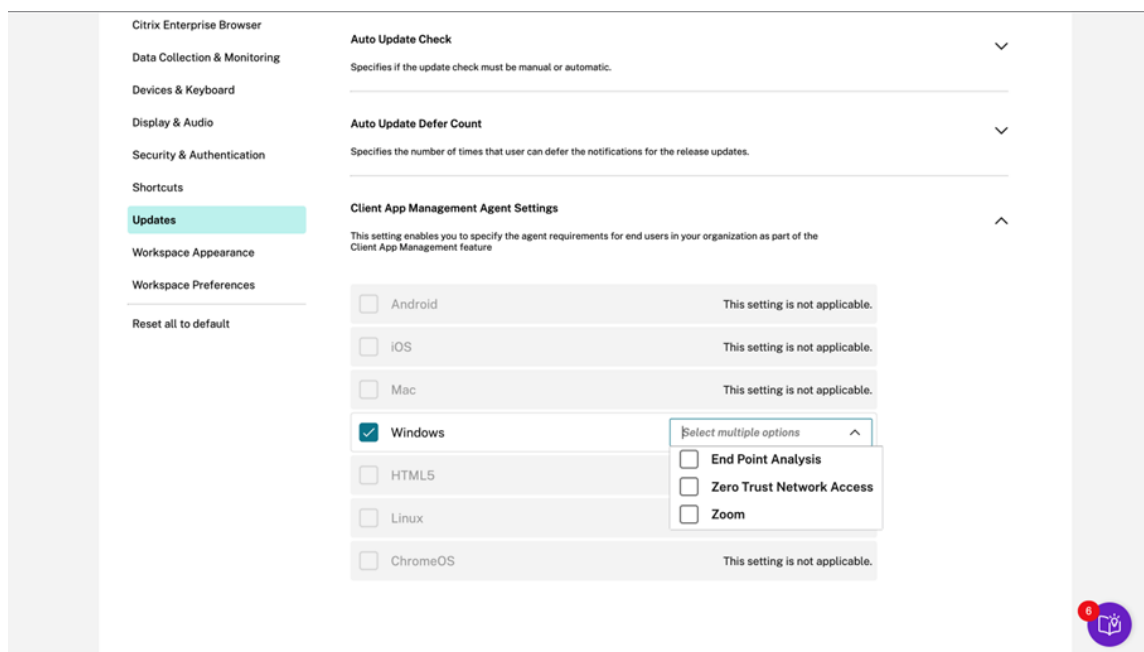
1. Inicie sesión en [Citrix Cloud](#).
2. En el menú de la parte superior izquierda de la pantalla, seleccione **Configuración de Workspace**.



Aparecerá la página **Configuración de Workspace**.



3. Haga clic en la ficha **Configuración de aplicaciones**.
4. Haga clic en **Actualizaciones**.
5. Asegúrese de que la casilla **Windows** esté marcada.
6. Seleccione los agentes necesarios junto a **Windows** en la lista desplegable de **Parámetros del agente de administración de aplicaciones cliente**.



### Habilitar la administración de plug-ins mediante la API de Global App Configuration Service

1. Configure e incorpore los parámetros a Global App Configuration Service mediante la API. Para obtener más información, consulte [Map service URLs and configure settings](#).

2. Se deben incorporar estos parámetros de Global App Configuration para que el almacén o la cuenta puedan incorporar EPA y los clientes ZTNA/Secure Access Client:

```
1 {
2
3   "serviceURL":
4   {
5
6     "url": "https://storefront.acme.com:443"
7   }
8 ,
9   "settings":
10  {
11
12    "description": "Install and update plugins",
13    "name": "Install and update plugins",
14    "useForAppConfig": true,
15    "appSettings":
16    {
17
18      "windows":
19      [
20        {
21
22          "assignedTo":
23          [
24            "AllUsersNoAuthentication"
25          ],
26          "category": "AutoUpdate",
27          "settings":
28          [
29            {
30
31              "name": "Auto Update plugins settings",
32              "value":
33              [
34                {
35
36                  "pluginId": "8A8AF6C0-11F6-4343-
37                    BA2D-A85A766170D4",
38                  "pluginName": "Citrix EPA Client",
39                  "pluginSettings":
40                  {
41
42                    "delayGroup": "Fast",
43                    "deploymentMode": "
44                    InstallAndUpdate",
45                    "detectRule": "UpgradeCode:{
46                    37A181F7-870E-4BDF-B0EA-E3B4766119FE }
47                    ",
48                    "isBlocking": true,
49                    "isFTU": true,
50                    "maximumAllowedVersion": "
```

```

49         "23.8.1.24",
50         "minimumAllowedVersion": "
51           0.0.0.0",
52         "stream": "Current",
53         "upgradeToLatest": true
54       }
55     },
56     {
57       "pluginId": "9A8AF6C0-11F6-4343-
58         BA2D-A85A766170D5",
59       "pluginName": "Citrix Secure Access
60         Client",
61       "pluginSettings":
62       {
63         "delayGroup": "Fast",
64         "deploymentMode": "
65           InstallAndUpdate",
66         "detectRule": "UpgradeCode:{
67           F0ED53AB-11BE-4E9C-87E5-CD4A81DA2A4D }
68         ",
69         "isBlocking": false,
70         "isFTU": true,
71         "maximumAllowedVersion": "
72           21.8.0.0",
73         "minimumAllowedVersion": "
74           0.0.0.0",
75         "stream": "Current",
76         "upgradeToLatest": true
77       }
78     },
79     {
80       "pluginId": "C03BAE37-F3AC-4D63-8
81         BC1-3C9CD2BC9E8D",
82       "pluginName": "WebEx VDI
83         AutoUpgrade Plugin",
84       "pluginSettings":
85       {
86         "delayGroup": "Fast",
87         "deploymentMode": "
88           InstallAndUpdate",
89         "detectRule": "UpgradeCode:{
90           AA2AACDC-D30B-433F-A602-3E25975010A6 }
91         ",
92         "isBlocking": false,
93         "isFTU": false,

```

```

92         "maximumAllowedVersion": "
93             3.1.0.24263",
94         "minimumAllowedVersion": "0.0.0
95             ",
96         "stream": "Current",
97         "upgradeToLatest": true
98     }
99
100     ],
101     "userOverride": false
102 }
103 ],
104 "userOverride": false
105 }
106
107 ]
108 }
109
110 }
111
112 }
113
114
115 <!--NeedCopy-->

```

Esta tabla muestra el esquema, los valores y la descripción de los parámetros de la administración de plug-ins.

Parámetro del esquema	Valor	Descripción
isBlocking	True o False	Quando el parámetro isBlocking se establece en true, el plug-in se considera obligatorio y la página de inicio de sesión solo aparece cuando está instalado el plug-in requerido. Citrix recomienda configurar EPA como plug-in obligatorio.
pluginName		Nombre descriptivo del plug-in. pluginName se puede modificar.
pluginId		ID del plug-in y no debe modificarse.

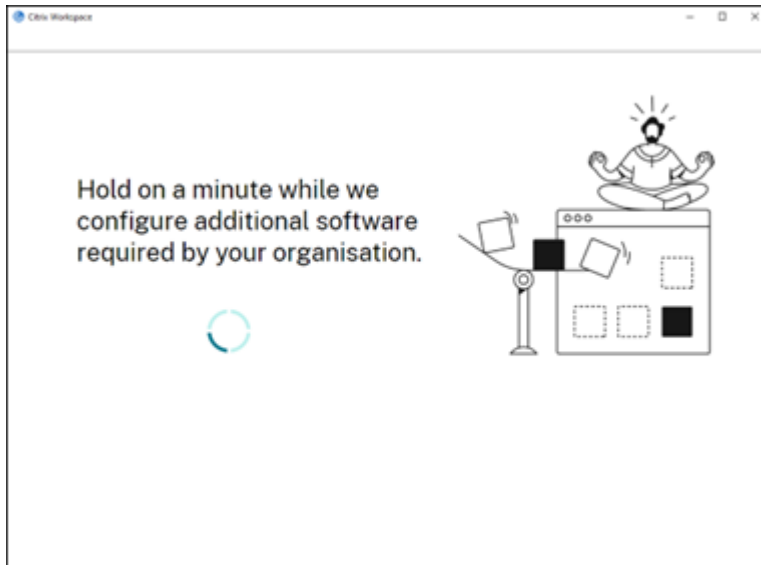
Parámetro del esquema	Valor	Descripción
delayGroup	Rápido, medio, lento	Intervalo de actualización automática en el que deben actualizarse los plug-ins.
deploymentMode	InstallAndUpdate/Update	InstallAndUpdate: el plug-in puede instalarse desde cero y actualizarse con la nueva versión. Actualización: solo se debe permitir la actualización, no una nueva instalación.
Ninguno		No es necesario realizar ninguna acción con relación a este plug-in.
detectRule	El valor no se debe modificar.	Comprueba si el plug-in ya está instalado o no.
maximumAllowedVersion		Versión máxima permitida del plug-in.
minimumAllowedVersion		Versión mínima permitida del plug-in.
upgradeToLatest	True o False	Debe configurarse en false para admitir maximumAllowedVersion y minimumAllowedVersion. True: Durante la actualización se tiene en cuenta la versión más reciente del plug-in.
Flujo	Actual	Debe configurarse en Current para recibir, instalar o actualizar automáticamente los plug-ins

### Flujo de trabajo de los usuarios

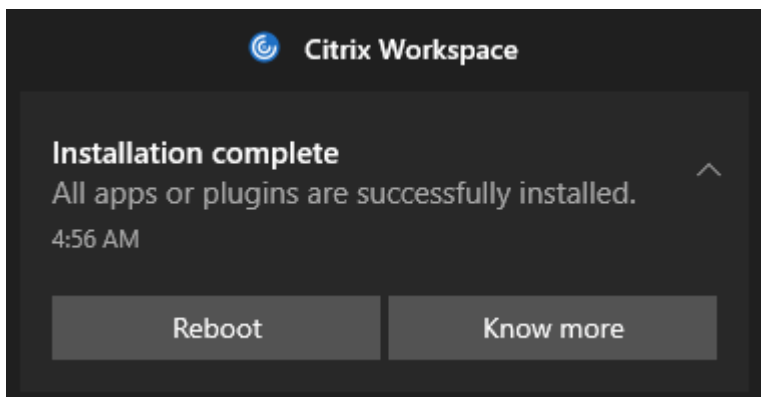
1. Descargar e instalar la aplicación Citrix Workspace para Windows.
2. Haga clic en **Agregar cuenta** al terminar la instalación.
3. Agregue el almacén/cuenta donde están incorporados los ajustes de configuración de la aplicación.



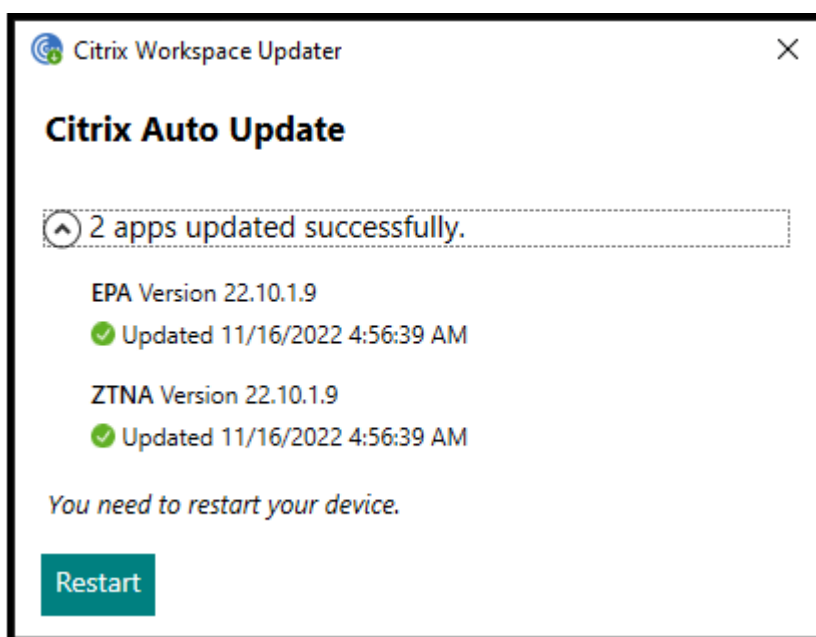
Al instalar los plug-ins obligatorios, aparece el siguiente mensaje:



4. Cuando se complete la instalación, aparecerá esta notificación:



5. Haga clic en **Know More** para saber qué plug-ins hay instalados.



## Administración de plug-ins para el plug-in de Zoom

La descarga, la instalación y la actualización automática del plug-in Zoom también se admiten y se gestionan de la misma manera que los plug-ins de EPA y ZTNA.

Para usar esta funcionalidad, se deben incorporar los siguientes ajustes de Global App Configuration para el almacén o cuenta:

```

1  {
2
3    "serviceURL":
4    {
5
6      "url": "https://storefront.acme.com:443"
7    }
8  ,
9    "settings":
10   {
11
12     "description": "Install and update plugins",
13     "name": "Install and update plugins",
14     "useForAppConfig": true,
15     "appSettings":
16     {
17
18       "windows":
19       [
20         {
21
22           "assignedTo":
23           [

```

```

24         "AllUsersNoAuthentication"
25     ],
26     "category": "AutoUpdate",
27     "settings":
28     [
29         {
30
31             "name": "Auto Update plugins settings",
32             "value":
33             [
34                 {
35
36                     "pluginId": "1A4BB471-022C-4C87-
37                         BDCD-0B64FB42869C",
38                     "pluginName": "Zoom VDI AutoUpgrade
39                         Plugin",
40                     "pluginSettings":
41                     {
42
43                         "delayGroup": "Fast",
44                         "deploymentMode": "
45                         InstallAndUpdate",
46                         "detectRule": "UpgradeCode:{
47                         34225638-14F3-4059-BE34-175AC9B35435 }
48                         ",
49                         "isBlocking": false,
50                         "isFTU": false,
51                         "maximumAllowedVersion": "
52                         5.11.2872",
53                         "minimumAllowedVersion": "0.0.0
54                         ",
55                         "stream": "Current",
56                         "upgradeToLatest": true
57                     }
58                 }
59             ]
60         },
61     ],
62     "userOverride": false
63 }
64 ]
65 }
66 }
67 }
68 }
69 }
70 }
71 <!--NeedCopy-->

```

## Experiencia en la aplicación

April 22, 2024

En esta sección se describe lo siguiente:

- [Entrega de aplicaciones](#)
- [Experiencia mejorada al iniciar aplicaciones y escritorios virtuales](#)
- [Preferencias de la aplicación](#)
- [Aplicaciones SaaS](#)
- [Recopilación y supervisión de datos](#)

## Entrega de aplicaciones

June 14, 2024

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, así, 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 de las aplicaciones de los grupos de entrega:

- Para hacer obligatoria una aplicación concreta (de forma que no pueda quitarse de la aplicación Citrix Workspace), agregue la cadena KEYWORDS: Mandatory a la descripción de la aplicación. Los usuarios no tienen la opción Quitar para cancelar la suscripción a las aplicaciones obligatorias.
- Para suscribir automáticamente a todos los usuarios de un almacén a una aplicación, agregue la cadena KEYWORDS: Auto a la descripción. Cuando los usuarios inicien sesión en el almacén, la aplicación se aprovisionará automáticamente sin que los usuarios tengan que suscribirse de forma manual a la aplicación.
- Para anunciar aplicaciones a los usuarios o facilitar la búsqueda de las aplicaciones más utilizadas incorporándolas a la lista Destacados de Citrix Workspace, agregue la cadena KEYWORDS: Featured a la descripción de cada aplicación.

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

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.

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

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

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

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

#### Nota:

Windows 8, Windows 8.1 y Windows 10 no permiten la creación de carpetas anidadas dentro del menú Inicio. 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 y Citrix DaaS.

- 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

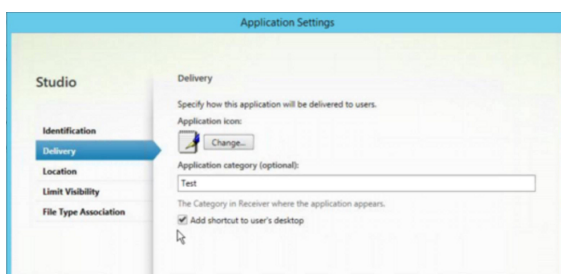
La aplicación Citrix Workspace puede configurarse para que coloque automáticamente los accesos directos de los escritorios y las aplicaciones directamente en el menú Inicio o en el escritorio. Sin

embargo, esta configuración es similar a la de las versiones anteriores de Workspace para Windows. Dicho esto, la versión 4.2.100 incorporó la capacidad de controlar la ubicación del acceso directo a la aplicación mediante los 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 fuera 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 quiera tener en su menú Inicio.

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

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

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

---

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

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

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

Configure la aplicación Citrix Workspace con `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 `UseCategoryAsStartMenuPath=True`.

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 `StartMenuDir=el nombre de la carpeta del menú Inicio`.

---

## 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 `RemoveAppsOnLogoff=True`.

Si quiere que la aplicación Citrix Workspace quite las aplicaciones al salir.

Configure la aplicación Citrix Workspace con `RemoveAppsOnExit=True`.

---

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

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

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

- prefer=”NombreDeAplicación”

El patrón del nombre de la aplicación hará coincidir cualquier aplicación que contenga dicho nombre en el nombre del archivo de acceso directo. El nombre de aplicación puede ser una

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

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

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

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

## 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, entre otras.
  - **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:**

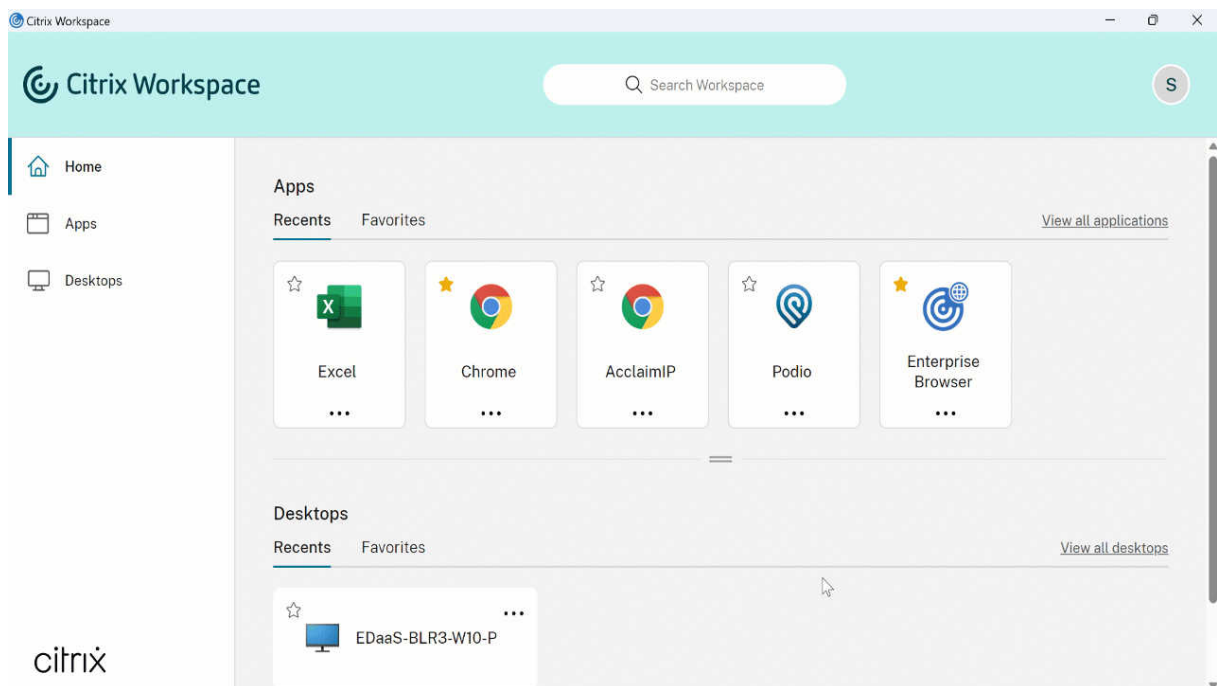
- Workspace para Web no admite esta función.



## Experiencia mejorada al iniciar aplicaciones y escritorios virtuales

June 14, 2024

Esta función está habilitada de forma predeterminada para los almacenes locales y la nube. La experiencia mejorada al iniciar aplicaciones y escritorios es más informativa, moderna e intuitiva en la aplicación Citrix Workspace para Windows. Esto ayuda a mantener a los usuarios informados con datos relevantes y oportunos sobre el estado del inicio. La notificación aparece en la esquina inferior derecha de la pantalla.



Los usuarios pueden ver notificaciones útiles sobre el progreso del inicio en lugar de un icono giratorio solamente. Si hay un inicio en curso y el usuario intenta cerrar el explorador, aparece un mensaje de advertencia.

## Preferencias de la aplicación

June 14, 2024

### Hoja de Preferencias avanzadas

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 parámetros siguientes:
  - Recopilación de datos
  - Central de conexiones
  - Configuration Checker
  - Barra de idioma y teclado
  - PPP elevados
  - Información de asistencia
  - Accesos directos y reconexión
  - Citrix Casting

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

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

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

#### Nota:

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

### Ocultar 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.

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

Opciones	Acción
No configurado	Muestra el parámetro
Habilitado	Ocultar 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**.

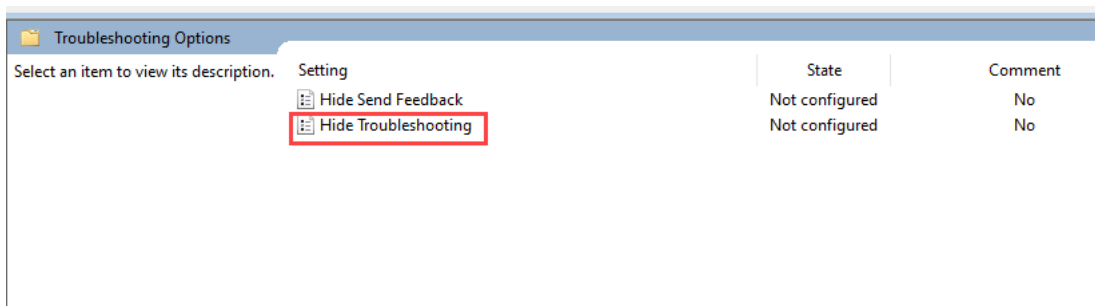
**Ocultar la opción de solución de problemas para los usuarios finales**

Los administradores pueden ocultar las opciones de solución de problemas para sus usuarios finales mediante el editor de GPO. Una vez habilitado este parámetro, se oculta la opción de solución de problemas que antes estaba visible para los usuarios finales en la bandeja del sistema.

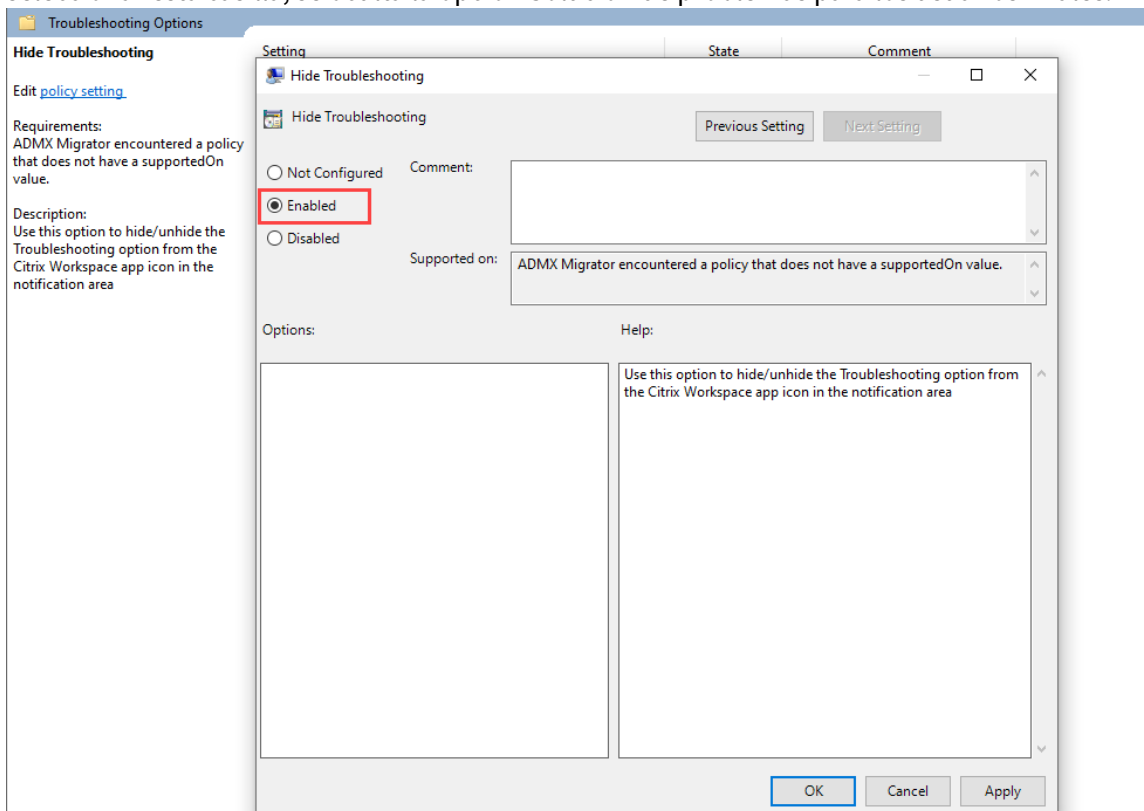
1. En el editor de GPO, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Autoservicio**.
2. Seleccione la carpeta **Opciones de solución de problemas**.

Setting	State	Comment
Advance Preferences Options		
<b>Troubleshooting Options</b>		
Allow users to Add/Remove Account	Not configured	No
Manage App Protection	Not configured	No
Manage App shortcut	Disabled	No
Enable Default FTA	Not configured	No
Enable FTA	Not configured	No
EnableFTU	Not configured	No
Enable application PreLaunch	Not configured	No
Quick Desktop Launch Support	Not configured	No
Silent authentication for Citrix Workspace	Not configured	No
Local app discovery	Not configured	No
Local Application Protection	Not configured	No
Allow/Prevent users to publish safe content	Not configured	No
Allow/Prevent users to publish unsafe content	Not configured	No
Control when Citrix Workspace attempts to reconnect to exi...	Not configured	No
Manage SelfServiceMode	Not configured	No
Store authentication tokens	Not configured	No
vPrefer	Not configured	No

3. Seleccione el parámetro **Ocultar solución de problemas**.



4. En el cuadro de diálogo Ocultar solución de problemas, seleccione la casilla **Habilitado**. Al seleccionar esta casilla, se oculta la opción Solución de problemas para los usuarios finales.



5. Haga clic en **Aceptar** para guardar los parámetros.

## 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.
- Ejecute el comando `/IncludeCitrixCasting` durante la instalación para habilitar Citrix Casting.

**Configurar el inicio de Citrix Casting**

**Nota:**

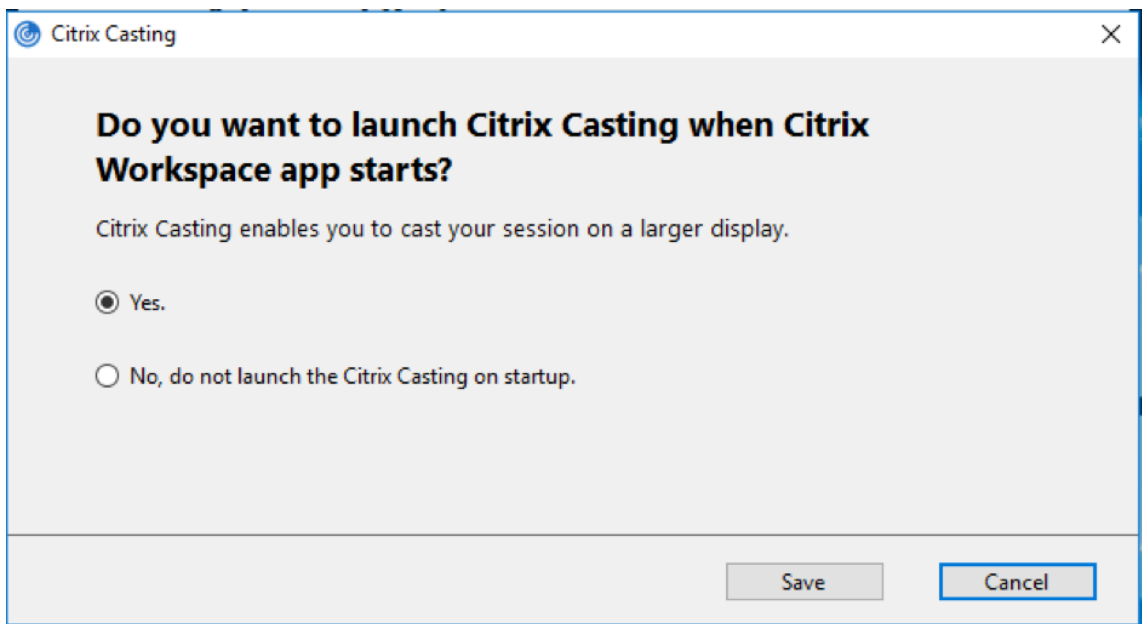
Puede ocultar toda o parte de la hoja Preferencias avanzadas. Para obtener más información, consulte [Hoja de Preferencias avanzadas](#).

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:

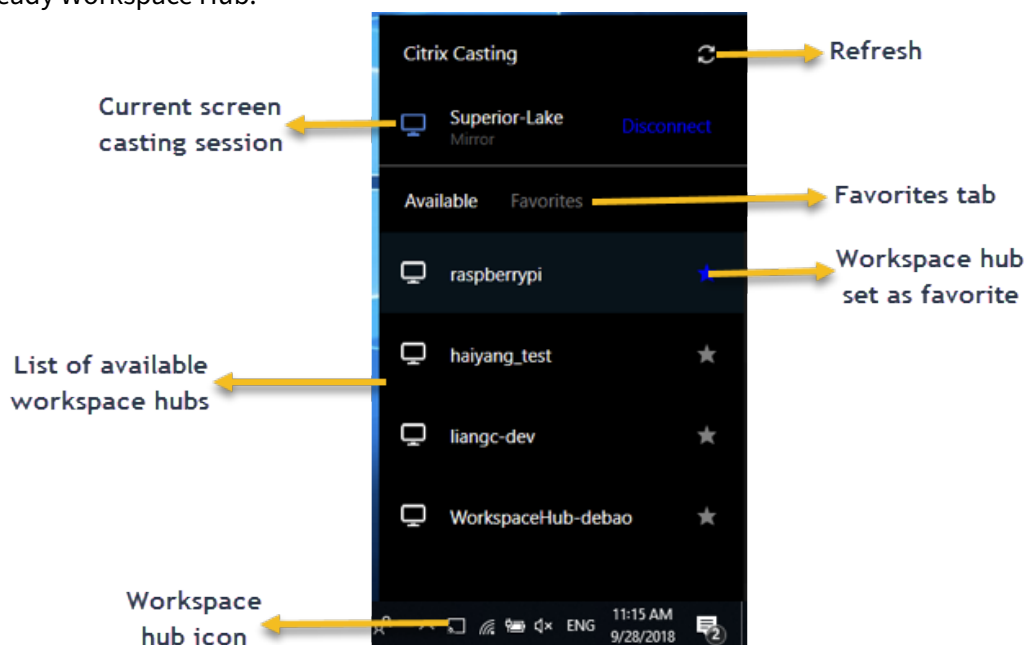
- **Mirror** (reflejar) para duplicar la pantalla principal y proyectarla en el dispositivo Workspace Hub conectado.
- **Extend** (extender) para usar la pantalla del dispositivo Workspace Hub como pantalla secundaria.

**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` 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

- Citrix Casting no funciona a menos que el dispositivo esté conectado a la misma red que Citrix Ready Workspace Hub.
- Si hay problemas de red, es posible que haya demoras en la pantalla del dispositivo Workspace Hub.
- Cuando selecciona **Extender**, la pantalla principal donde esté iniciada la aplicación Citrix Ready Workspace parpadea varias veces.
- En el modo **Extender**, no se puede configurar la pantalla secundaria como pantalla principal.
- 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.
- 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.
- No se admiten las sesiones de proyección en varias pantallas.
- La resolución de pantalla máxima admitida por Citrix Casting es 1920 x 1440.
- 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.
- Esta función no se ofrece en la aplicación Citrix Workspace para la Tienda Windows.
- 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.

## Aplicaciones SaaS

June 14, 2024

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:**

- 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.
- Es posible que los vídeos incrustados en una aplicación no funcionen.
- No puede abrir aplicaciones SaaS con comandos de Storebrowse.

Para obtener más información sobre cómo configurar espacios de trabajo, consulte [Configurar el espacio de trabajo](#) en Citrix Cloud.

## **Recopilación y supervisión de datos**

June 14, 2024

### **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](#).

## Mejora en Citrix Analytics Service

Con esta versión, la aplicación Citrix Workspace está destinada a transmitir de forma segura la dirección IP pública del salto de red más reciente a Citrix Analytics Service. Estos datos se recopilan por inicio de sesión. Ayuda a Citrix Analytics Service a analizar si los problemas de rendimiento deficiente están vinculados a áreas geográficas específicas.

De forma predeterminada, los registros de direcciones IP se envían a Citrix Analytics Service. Sin embargo, puede inhabilitar esta opción en la aplicación Citrix Workspace mediante el Editor del Registro.

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

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

### Nota:

- Las transmisiones de direcciones IP se producen en el mejor de los casos. Aunque la aplicación Citrix Workspace transmite todas las direcciones IP en las que se inicia, es posible que algunas de las direcciones no sean exactas.
- En entornos de clientes cerrados, donde los dispositivos de punto final operan dentro de una intranet, compruebe que la URL `https://locus.analytics.cloud.com/api/locateip` se halla en la lista de permitidos del dispositivo de punto final en cuestión.

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

Para obtener más información sobre cómo utiliza esta información Performance Analytics, consulte [Self-Service Search for Performance](#).

## 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.	Estos datos ayudan a Citrix a mejorar la calidad, la funcionalidad y el rendimiento de la aplicación Citrix Workspace, asignar adecuadamente los recursos para el desarrollo de productos, mantener los niveles de servicio y administrar la inversión en personal e infraestructura.

### Datos recopilados

Como se indicó anteriormente, Citrix recopila datos de uso y configuración de la aplicación Citrix Workspace para mejorar la calidad, la funcionalidad y el rendimiento de la aplicación Workspace, y para poder asignar adecuadamente los recursos para el desarrollo de productos, así como para mantener los niveles de servicio y administrar la inversión en personal e infraestructura. Los datos se utilizan y analizan únicamente de forma agregada. No se singulariza a ningún usuario o máquina ni se hacen análisis de usuarios finales específicos en función de los datos del CEIP.

Elementos concretos de datos CEIP recopilados por Google Analytics y Citrix 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

Modelo/propiedades del dispositivo	Estado de inicio de las sesiones de Citrix Virtual Apps and Desktops	Nombre de escritorio/aplicación virtual	Estado de la actualización automática
Detalles de la concesión de conexiones	Uso de la función de migración de direcciones URL de StoreFront a Workspace	Uso de Citrix Enterprise Browser	Canal de actualización automática
Detalles del tiempo de espera por inactividad	Versión de Citrix Enterprise Browser		

### Preferencias para la recopilación de datos

A partir de la versión 2205, tanto los usuarios como los administradores pueden dejar de enviar datos de CEIP (excepto los dos elementos de datos que se pueden bloquear como se especifica en la Nota a continuación) siguiendo estos pasos.

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace situado en el área de notificaciones.
2. Seleccione **Preferencias avanzadas**.  
Se mostrará el cuadro de diálogo **Preferencias avanzadas**.
3. Seleccione **Recopilación de datos**.
4. Seleccione **No, gracias** para inhabilitar CEIP o dejar de participar en el programa.
5. Haga clic en **Guardar**.

También puede ir a la siguiente entrada del Registro como administrador 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`, también podrá dejar de enviar los dos últimos elementos de datos de CEIP, es decir, la versión

de la aplicación Citrix Workspace y del sistema operativo, si va a la siguiente entrada del Registro y define el valor:

**Ruta:** HKEY\_LOCAL\_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP

**Clave:** DisableHeartbeat

**Valor:** True

### 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](#).

## Seguridad y autenticación

April 22, 2024

En esta sección se describe lo siguiente:

- [Seguridad](#)
- [Proteger comunicaciones](#)
- [Autenticación](#)
  - [Tabla de acceso de PassThrough de dominio](#)
  - [PassThrough de dominio a Citrix Workspace con Citrix Gateway local como proveedor de identidades](#)
  - [PassThrough de dominio a Citrix Workspace con Azure Active Directory como proveedor de identidades](#)
  - [PassThrough de dominio a Citrix Workspace con Okta como proveedor de identidades](#)

## Seguridad

June 14, 2024

## App Protection

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. Para obtener más información, consulte [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.

Para configurar App Protection en la aplicación Citrix Workspace para Windows, consulte la sección Aplicación Citrix Workspace para Windows del artículo [Configuración](#).

### Nota:

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

## Seguridad de archivos ICA mejorada

Esta función proporciona una mayor seguridad al gestionar archivos ICA durante el inicio de sesiones de aplicaciones y escritorios virtuales.

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:**

Puede usar Global App Config Service desde la aplicación Citrix Workspace 2106.

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.

## 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).

## Proteger comunicaciones

June 14, 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 1.3 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 use posteriormente la interfaz de usuario de autoservicio, para introducir la URL haga clic 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:**

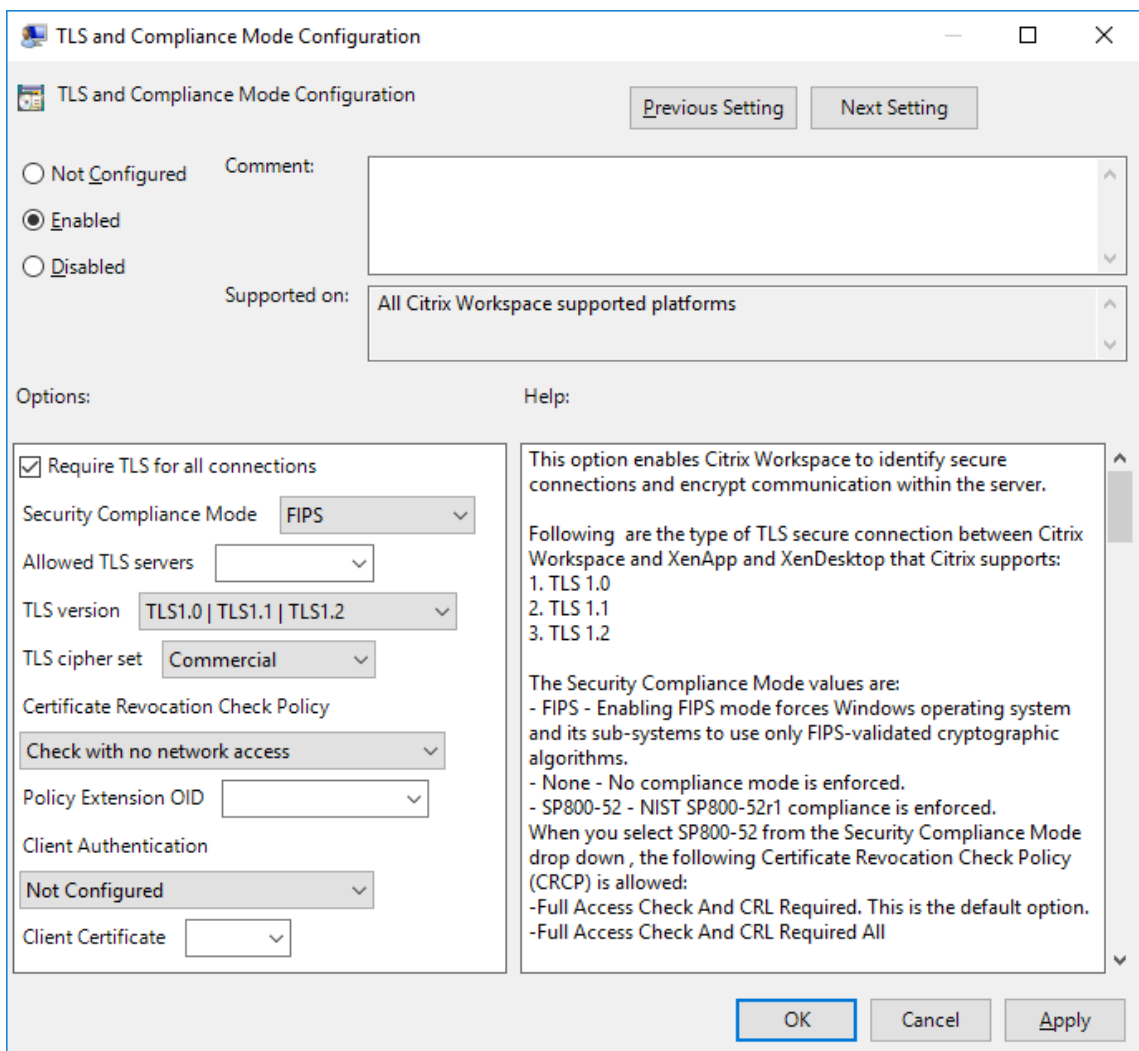
Estos conjuntos de cifrado se han retirado para mejorar la seguridad:

- 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

### Aplicar conexiones de servidor de confianza

La directiva de configuración “Servidor de confianza” identifica y aplica relaciones de confianza en las conexiones de la aplicación Citrix Workspace.

Con esta directiva, los administradores pueden controlar cómo el cliente identifica la aplicación o el escritorio publicados a los que se conecta. El cliente determina un nivel de confianza, denominado región de confianza, con una conexión. La región de confianza, a su vez, determina cómo se configura el cliente para la conexión.

Al habilitar esta directiva, se evitan conexiones a los servidores que no se encuentran en las regiones de confianza.

De manera predeterminada, la identificación de la región se basa en la dirección del servidor con el que se conecta el cliente. Para ser miembro de la región de confianza, el servidor debe ser miembro de la **zona de Sitios de confianza** de Windows. Esto se puede configurar con el parámetro **Zona de Internet de Windows**.



También se puede confiar específicamente en la dirección del servidor mediante el parámetro **Address**. La dirección del servidor debe ser una lista de servidores separados por comas que admitan el uso de comodines. Por ejemplo, `cps*.citrix.com`.

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**.

Cuando esta directiva está habilitada y el servidor no está en la región de confianza, se impide la conexión y se muestra un mensaje de error.

El servidor identificado debe agregarse a la **zona de Sitios de confianza** de Windows para que la conexión se realice correctamente. Por ejemplo, agregue el servidor como “`http://`” o “`https://`” para las conexiones SSL.

#### **Nota:**

Para las conexiones SSL, el nombre común del certificado debe ser de confianza. Para las conexiones que no son SSL, es necesario que todos los servidores contactados sean de confianza individualmente.

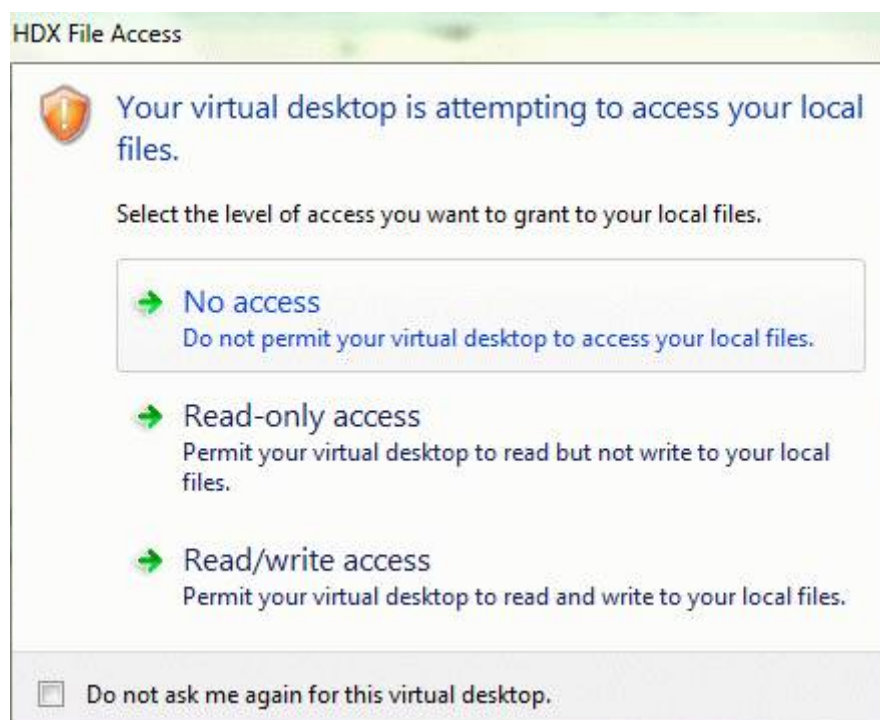
Además, debe asegurarse de que el FQDN interno de StoreFront se agregue a la zona de Intranet local o a las zonas de Sitios de confianza. Para obtener información, consulte **Modificar los parámetros de Internet Explorer** en la sección [Autenticación](#).

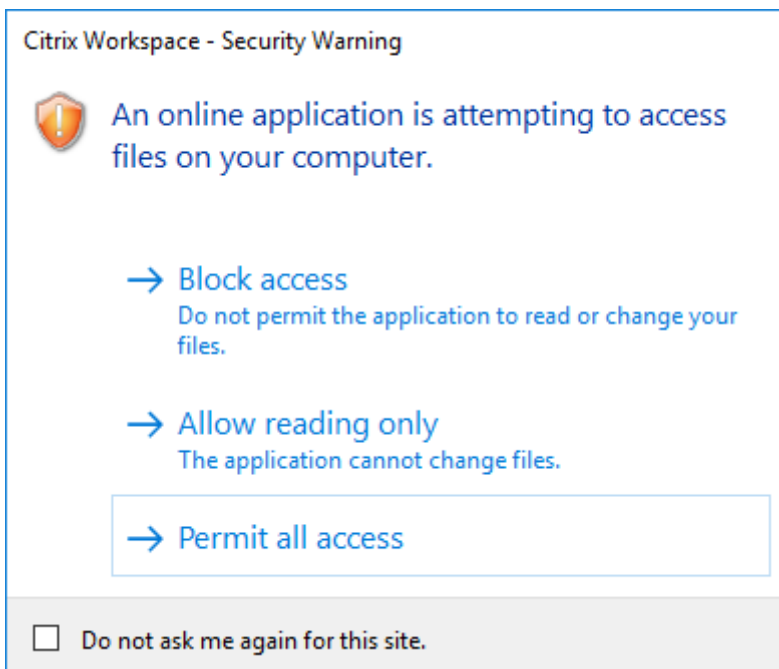
#### **Confianza selectiva de clientes**

Además de permitir o impedir conexiones a los servidores, el cliente también utiliza las regiones para identificar el acceso SSO a archivos, micrófonos o cámaras web.

Regiones	Recursos	Nivel de acceso
Internet	Archivo, micrófono, web	Solicitar acceso al usuario, no se permite SSO
Intranet	Micrófono, web	Solicitar acceso al usuario, se permite SSO
Sitios restringidos	Todo	Es posible que no se impida el acceso ni la conexión
De confianza	Micrófono, web	Lectura o escritura, se permite SSO

Cuando el usuario ha seleccionado el valor predeterminado para una región, es posible que aparezca este cuadro de diálogo:





Los administradores pueden modificar este comportamiento predeterminado al crear y configurar las claves del Registro de la **confianza selectiva de cliente** mediante la directiva de grupo o en el Registro. Para obtener más información sobre cómo configurar las claves del Registro de la confianza selectiva de cliente, consulte el artículo [CTX133565](#) de Knowledge Center.

## 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 es-

critorio 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 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"
```

## Conexiones y certificados

### 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](#).

### **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](#).

## **Función para mitigar los ataques de tipo “Man in the middle”**

La aplicación Citrix Workspace para Windows le ayuda a reducir el riesgo de ataques de tipo “Man in the middle” mediante la función **Asignación de certificados de empresa** de Microsoft Windows. Un ataque de tipo “Man in the middle” es un tipo de ciberataque en el que el atacante intercepta y retransmite mensajes en secreto entre dos partes que creen que se están comunicando directamente entre sí.

Antes, al contactar con el servidor del almacén, no había forma de comprobar si la respuesta recibida provenía del servidor con el que intentaba contactar. Con la función **Asignación de certificados de empresa** de Microsoft Windows, puede comprobar la validez y la integridad del servidor mediante la asignación de su certificado.

La aplicación Citrix Workspace para Windows está preconfigurada para saber qué certificado de servidor debe esperar para un dominio o sitio en particular mediante las reglas de asignación de certificados. Si el certificado del servidor no coincide con el certificado de servidor preconfigurado, la aplicación Citrix Workspace para Windows bloquea la sesión.

Para obtener información sobre cómo implementar la función **Asignación de certificados de empresa**, consulte la [documentación de Microsoft](#).

### **Nota:**

Debe conocer la caducidad del certificado y actualizar correctamente las directivas de grupo y las listas de certificados de confianza. De lo contrario, es posible que no pueda iniciar la sesión aunque no haya ningún ataque.

## **Autenticación**

June 14, 2024

Puede configurar diversos tipos de autenticación para la aplicación Citrix Workspace: autenticación con tarjeta inteligente, autenticación PassThrough de dominio (Single Sign-On o SSON) y autenticación PassThrough con Kerberos.

## Autenticación PassThrough de dominio (Single Sign-On)

La autenticación PassThrough de dominio (Single Sign-On o SSON) permite autenticarse en un dominio y usar Citrix Virtual Apps and Desktops y Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) sin necesidad de autenticarse de nuevo.

### Nota:

Si inhabilita la directiva **Habilitar notificaciones de MPR para el sistema** en la plantilla de objetos de directiva de grupo, Windows 11 no admite la función de autenticación de PassThrough de dominio (Single Sign-On).

Esta función está disponible a partir de la versión 2012 y posteriores de la aplicación Citrix Workspace para Windows.

Cuando está habilitada, la autenticación PassThrough de dominio (Single Sign-On) almacena en caché las credenciales para que pueda conectarse a otras aplicaciones de Citrix sin tener que iniciar sesión cada vez. Para mitigar el riesgo de robo de credenciales, asegúrese de que solo se ejecute en su dispositivo software que cumpla con las directivas corporativas.

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 línea de comandos
- Interfaz gráfica (GUI)

### Nota:

Es posible que los términos PassThrough de dominio, Single Sign-On y SSON se usen indistintamente en este documento.

## 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. Sin embargo, debe asegurarse de haber habilitado la autenticación básica y la autenticación de factor único (nFactor con 1 factor) en Citrix Gateway.

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 **Habilitada**.
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

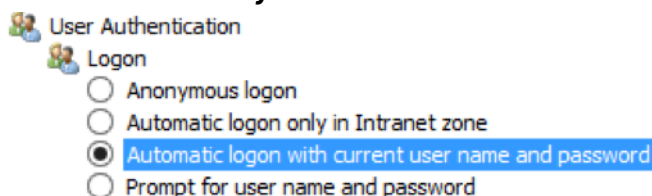
En Citrix Virtual Apps and Desktops y Citrix DaaS, ejecute el siguiente comando de PowerShell como administrador en el Delivery Controller:

```
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 de usuarios** en **Internet Explorer**. Para modificarlos:
  - a) Inicie **Opciones de Internet** desde el Panel de control.
  - b) Haga clic en la ficha **Seguridad > Intranet local**.

- c) Haga clic en **Nivel personalizado**. Aparece la ventana **Configuración de seguridad: Zona de intranet local**.
- 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.

### 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

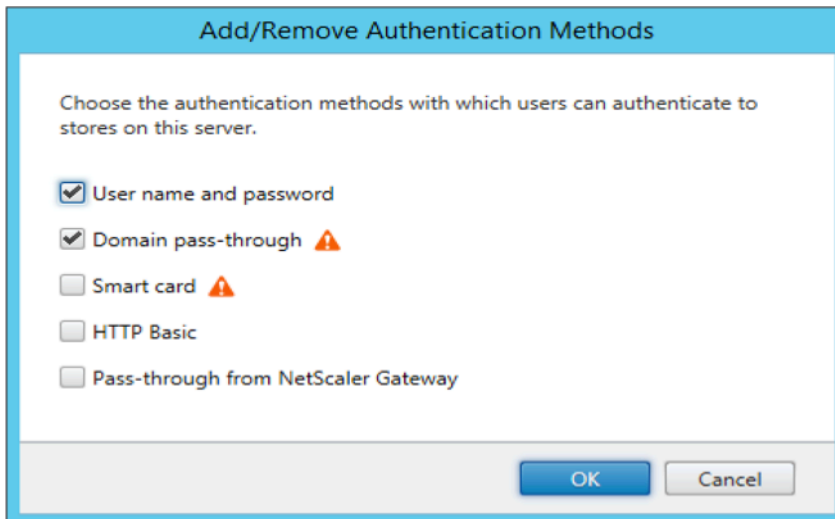
Complete los pasos siguientes para configurar la aplicación Citrix Workspace para la autenticación PassThrough mediante la directiva de grupo de Active Directory. En este caso, puede obtener la autenticación Single Sign-On sin utilizar las herramientas de implementación del software de empresa, como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

Puede configurar este parámetro mediante Global App Configuration Service mediante uno de estos métodos:

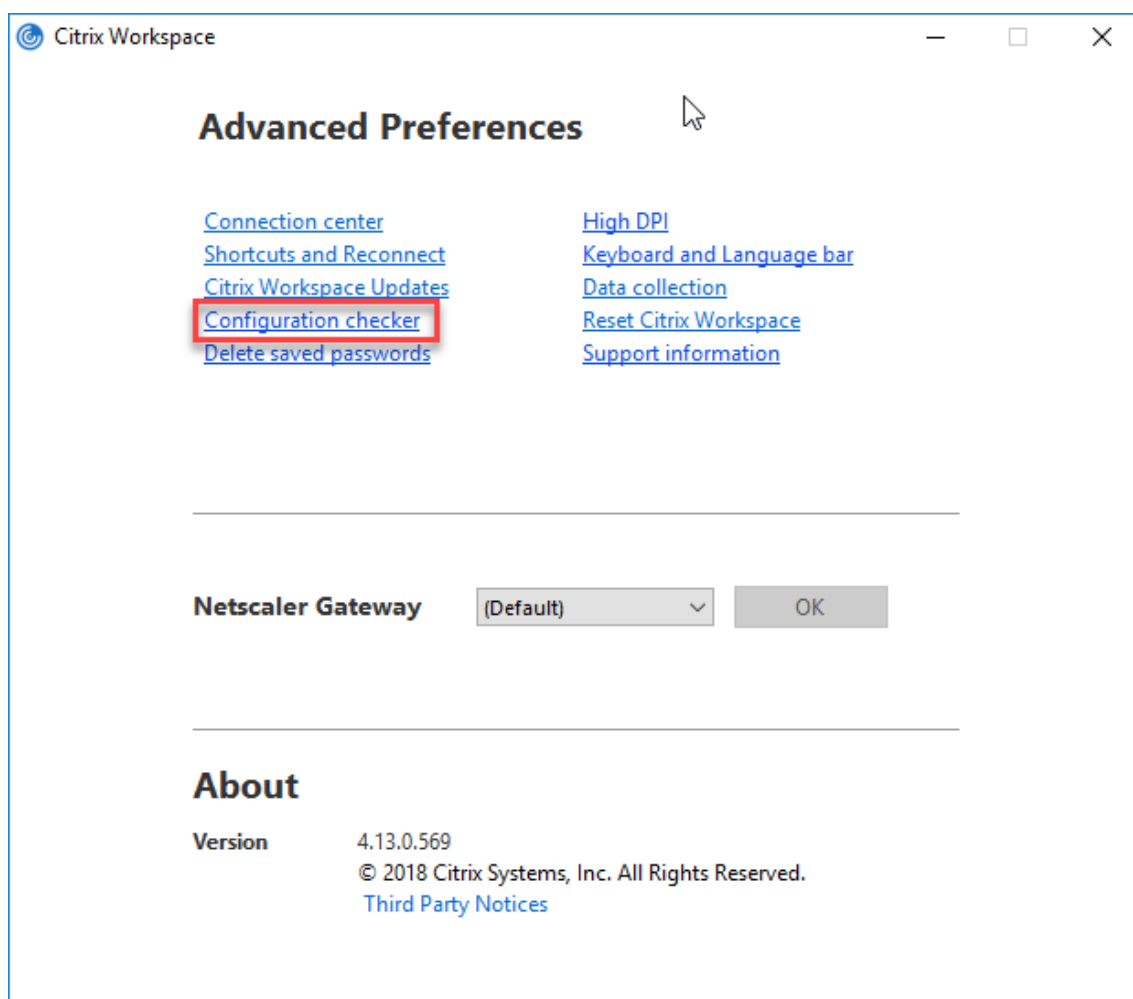
- **Interfaz de usuario (IU) de Global App Configuration Service:** Para la configuración mediante la interfaz de usuario, consulte [Configurar la aplicación Citrix Workspace](#).
- **API:** Para configurar parámetros mediante las API, consulte la documentación para [desarrolladores de Citrix](#).

### 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**.  
Se mostrará 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 (Single Sign-On) 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 (Single Sign-On o SSON) 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 (Single Sign-On) 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:

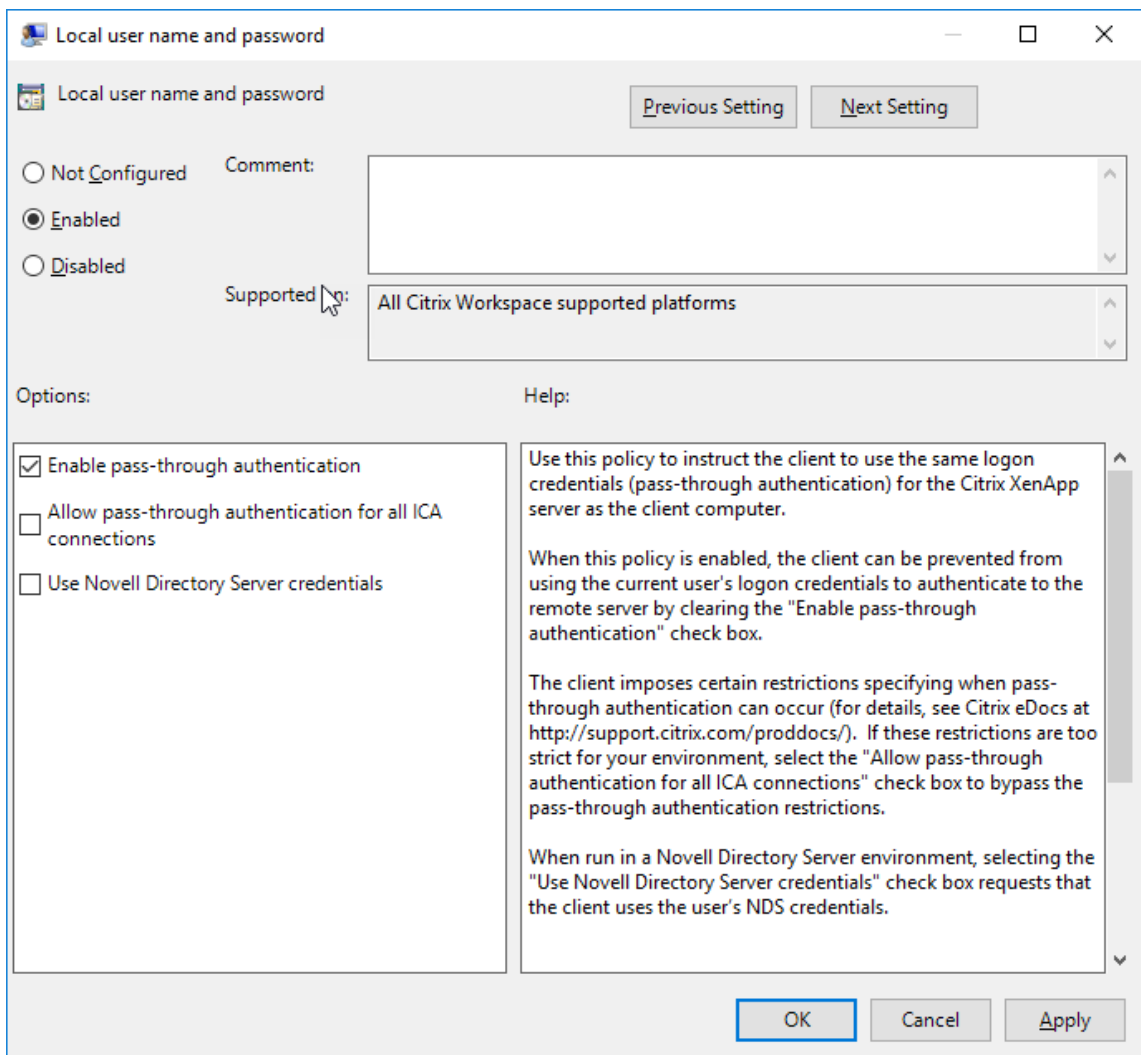
- `/includeSSON`

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 99 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).

## **Compatibilidad con métodos de autenticación modernos para almacenes de StoreFront**

Puede habilitar la compatibilidad con métodos de autenticación modernos para los almacenes de StoreFront mediante la plantilla de objetos de directiva de grupo (GPO). Puede habilitar esta función mediante Global App Configuration Service.

Puede autenticarse en los almacenes de Citrix StoreFront de cualquiera de las siguientes formas:

- Con claves de seguridad de Windows Hello y FIDO2. Para obtener más información, consulte [Otras formas de autenticarse](#).
- Single Sign-On (SSO) en los almacenes de Citrix StoreFront desde máquinas unidas a Azure Active Directory (AAD) con AAD como proveedor de identidades. Para obtener más información, consulte [Otras formas de autenticarse](#).
- Los administradores de Workspace pueden configurar y aplicar directivas de acceso condicional de Azure Active Directory para usuarios que se autentican en los almacenes de Citrix StoreFront. Para obtener más información, consulte [Compatibilidad con el acceso condicional con Azure AD](#).

Para habilitar esta funcionalidad, debe utilizar Microsoft Edge WebView2 como explorador subyacente para la autenticación directa de StoreFront y la puerta de enlace.

**Nota:**

La versión de Microsoft Edge WebView2 Runtime debe ser 102 o posterior.

Puede habilitar métodos de autenticación modernos para los almacenes de StoreFront mediante Global App Config Service y una plantilla de objetos de directiva de grupo (GPO).

### **Mediante Global App Config Service**

Para habilitar esta funcionalidad:

1. En el menú de **Citrix Cloud**, seleccione **Configuración de Workspace** y, luego, **Configuración de aplicaciones**.
2. Haga clic en **Seguridad y autenticación**.
3. Asegúrese de que la casilla **Windows** esté marcada.
4. Seleccione **Habilitado** junto a **Windows** en la lista desplegable **Autenticación de Microsoft Edge WebView para StoreFront**.

**Microsoft Edge WebView For StoreFront Authentication**

This policy allows to control the WebView where the StoreFront authentication related web content is loaded. Microsoft Edge WebView2 provides support for modern authentication methods for StoreFront authentication.

<input type="checkbox"/>	Android	This setting is not applicable.
<input type="checkbox"/>	iOS	This setting is not applicable.
<input type="checkbox"/>	Mac	This setting is not applicable.
<input checked="" type="checkbox"/>	Windows	Enabled
<input type="checkbox"/>	HTML5	This setting is not applicable.
<input type="checkbox"/>	Linux	This setting is not applicable.

**Nota:**

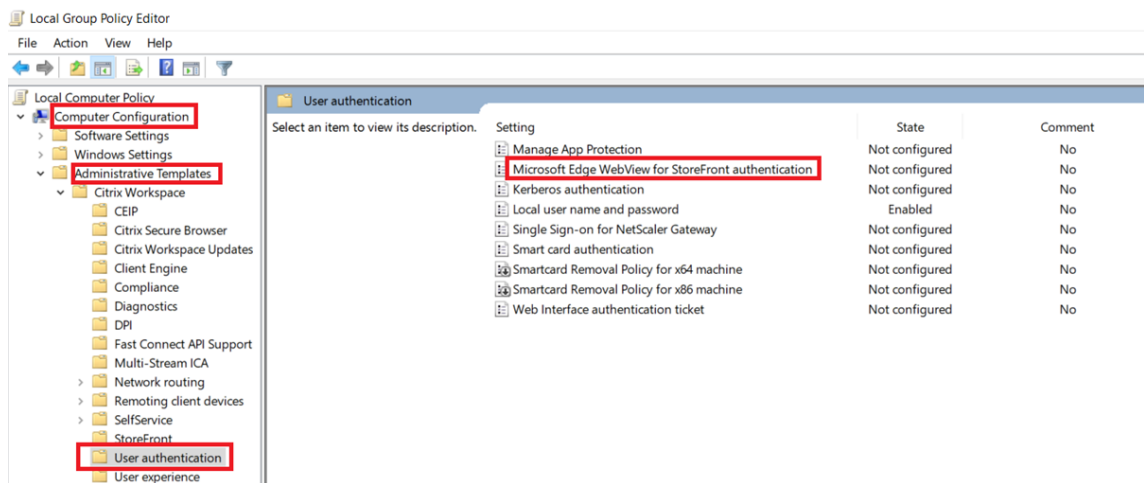
Si selecciona **Inhabilitado** junto a **Windows** en la lista desplegable **Autenticación de Microsoft Edge WebView para StoreFront**, se utiliza Internet Explorer WebView en la aplicación Citrix Workspace. Como resultado, no se admitirán métodos de autenticación modernos para los almacenes de Citrix Storefront.

**Mediante un GPO**

Para habilitar esta funcionalidad:

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 > Autenticación de usuarios**.
3. Haga clic en la directiva de **autenticación de Microsoft Edge WebView para StoreFront** y configúrela en **Habilitada**.





4. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

Cuando esta directiva está inhabilitada, la aplicación Citrix Workspace utiliza Internet Explorer Web-View. Como resultado, no se admiten los métodos de autenticación modernos para los almacenes de Citrix StoreFront.

## Otras formas de autenticarse

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 99 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 (Single Sign-On o SSON).

2. 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).

3. 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 compo-  
nente 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_CERTIFICATESELECT={ 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 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[WFClient]
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 o SSON) esté configurada para Citrix Workspace en dispositivos unidos a un dominio. Esta función está disponible a partir de la versión 2012 y posteriores de la aplicación Citrix Workspace para Windows.

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. 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**.
3. Haga clic en la directiva **Autenticación silenciosa para Citrix Workspace** y **habilítela**.
4. Haga clic en **Aplicar** y **Aceptar**.

### **Impedir que la aplicación Citrix Workspace para Windows almacene en caché contraseñas y nombres de usuario**

De manera predeterminada, la aplicación Citrix Workspace para Windows rellena el formulario automáticamente con el último nombre de usuario que se utilizó. Para que el campo de nombre de usuario no se rellene automáticamente, modifique el Registro en el dispositivo del usuario:

1. Cree un valor REG\_SZ HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\AuthManager\RememberUsername.
2. Establezca su valor en “false”.

Para inhabilitar la casilla **Recordar mi contraseña** e impedir el inicio de sesión automático, cree la siguiente clave de Registro en el equipo cliente en el que esté instalada la aplicación Citrix Workspace para Windows:

- Ruta: HKEY\_LOCAL\_MACHINE\Software\wow6432node\Citrix\AuthManager
- Tipo: REG\_SZ
- Nombre: SavePasswordMode
- Valor: Never

#### **Nota:**

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

Para evitar el almacenamiento en caché de las credenciales de los almacenes de StoreFront, consulte [Impedir que la aplicación Citrix Workspace para Windows almacene en caché contraseñas y nombres de usuario](#) en la documentación de StoreFront.

### **Compatibilidad con más de 200 grupos en Azure AD**

Con esta versión, un usuario de Azure AD que forme parte de más de 200 grupos puede ver las aplicaciones y escritorios que tiene asignados. Anteriormente, el mismo usuario no podía ver estas aplicaciones y escritorios.



**Nota:**

Para habilitar esta función, los usuarios deben cerrar sesión en la aplicación Citrix Workspace e iniciarla de nuevo.

### **Compatibilidad con la autenticación de proxy**

Antes, en máquinas cliente configuradas con autenticación de proxy, si las credenciales del proxy no existían en el **Administrador de credenciales de Windows**, no se le permitía autenticarse en la aplicación Citrix Workspace.

A partir de la versión 2102 y posteriores de la aplicación Citrix Workspace para Windows, en las máquinas cliente configuradas para la autenticación de proxy, si las credenciales de proxy no se almacenan en el **Administrador de credenciales de Windows**, aparece un mensaje de autenticación en el que se le pide que introduzca las credenciales del proxy. A continuación, la aplicación Citrix Workspace guarda las credenciales del servidor proxy en el **Administrador de credenciales de Windows**. Esto simplifica la experiencia de inicio de sesión porque no necesita guardar manualmente las credenciales en el Administrador de credenciales de Windows antes de acceder a la aplicación Citrix Workspace.

### **User-Agent**

La aplicación Citrix Workspace envía un agente de usuario en las solicitudes de red que puede utilizarse para configurar las directivas de autenticación, incluida la redirección de la autenticación a otros proveedores de identidades (IDP).

**Nota:**

Los números de versión que se mencionan como parte de usuario-agente en esta tabla son ejemplos, y esta se actualiza automáticamente en función de las versiones que utilice.

Esta tabla describe el caso, la descripción y el usuario-agente correspondiente para cada caso:

Caso	Descripción	User-Agent
<b>Solicitudes HTTP normales</b>	En general, una solicitud de red realizada por la aplicación Citrix Workspace contiene un usuario-agente. Por ejemplo, solicitudes de red como <code>GET /Citrix/Roaming/Accounts</code> o <code>GET /AGServices/discover</code>	<code>CitrixReceiver/23.5.0.63 Windows/10.0 (22H2 Build 19045.2965) SelfService/23.5.0.63 (Release)X1Class CWACapable</code>
<b>Almacén de la nube</b>	Cuando un usuario se autentica en un almacén de la nube de la aplicación Citrix Workspace, las solicitudes de red se realizan con un usuario-agente específico. Por ejemplo, solicitudes de red con ruta <code>/core/connect/authorize</code> .	<code>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50 CWA/23.5.0.63 Windows/10.0 (22H2 Build 19045.2965)</code>
<b>Almacén local con autenticación avanzada de Gateway mediante Edge WebView</b>	Cuando un usuario se autentica en el dispositivo Gateway configurado con autenticación avanzada en la aplicación Citrix Workspace mediante Edge WebView, las solicitudes de red se realizan con un usuario-agente específico. Por ejemplo, las solicitudes de red que incluyen <code>GET /nf/auth/doWebview.do</code> y <code>GET /logon/LogonPoint/tmindex.html</code> .	<code>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.54 CWAWEBVIEW/23.2.0.2111 Windows/10.0 (22H2 Build 19045.2364)</code>

Caso	Descripción	User-Agent
<b>Almacén local con autenticación avanzada de Gateway mediante IE WebView</b>	Cuando un usuario se autentica en el dispositivo Gateway configurado con autenticación avanzada en la aplicación Citrix Workspace mediante Internet Explorer WebView, las solicitudes de red se realizan con un usuario-agente específico. Por ejemplo, las solicitudes de red que incluyen <code>GET /nf/auth/doWebview.do</code> y <code>GET /logon/LogonPoint/tmindex.html</code> .	<code>Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko, CWAWEVIEW/23.5.0.43</code>
<b>Almacén web personalizado</b>	Cuando un usuario agrega un almacén web personalizado a la aplicación Citrix Workspace, la aplicación envía un usuario-agente.	<code>Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50 CWA/23.5.0.63 Windows/10.0 (22H2 Build 19045.2965)</code>

## Tabla de acceso de PassThrough de dominio

June 14, 2024

Si utiliza Citrix Workspace y quiere usar PassThrough de dominio, las tablas de las subsecciones describen los diferentes casos y si puede usar o no PassThrough de dominio para cada caso.

Los diferentes elementos de los encabezados de las tablas y la información adicional sobre los elementos de los encabezados son los siguientes:

- Dispositivo de punto final unido a: Indica el directorio al que se une el dispositivo de punto final.

El directorio proporciona control de acceso a recursos locales. Puede ser Active Directory (AD) local, Azure Active Directory (AAD) o híbrido.

- Proveedor de identidades (IdP): Entidad utilizada para proporcionar servicios de autenticación a Citrix Workspace. Le permite conectarse a los recursos.
- Servicio de autenticación federada (FAS): Para obtener más información, consulte [Habilitar Single Sign-On para espacios de trabajo con Citrix Federated Authentication Service](#).
- Virtual Delivery Agent (VDA): Para obtener más información, consulte [Instalar VDA](#).
- VDA unido a: Indica el directorio al que está unido el dispositivo VDA. Para obtener más información, consulte [Administración de acceso e identidad](#).
- Single Sign-On (SSO) en Citrix Workspace/VDA: El valor Sí o No indica si se admite PassThrough de dominio a Citrix Workspace o VDA.
- Aplicación Citrix Workspace: Para aplicar Single Sign-On, consulte [Configurar Single Sign-On durante una instalación nueva en Autenticación de PassThrough de dominio](#).

**Nota:**

Es posible que necesite la versión más reciente de la aplicación Citrix Workspace para poder usar PassThrough de dominio en algunos de estos casos.

### PassThrough de dominio para Citrix Workspace

---

Dispositivo de punto final unido a	IdP	VDA unido a	SSO en Citrix Workspace	SSO en VDA	Documentación
AD	Dispositivo Citrix Gateway local	AD	Sí	Aplicación Citrix Workspace/FAS	<a href="#">PassThrough de dominio a Citrix Workspace con Citrix Gateway local como proveedor de identidades</a> .

Dispositivo de punto final unido a	IdP	VDA unido a	SSO en Citrix Workspace	SSO en VDA	Documentación
AD	Autenticación adaptable	AD	Sí	Aplicación Citrix Workspace/FAS	Para configurar la autenticación adaptable, consulte <a href="#">Servicio de autenticación adaptable</a> y siga las instrucciones de <a href="#">PassThrough de dominio a Citrix Workspace</a> mediante <a href="#">Citrix Gateway local</a> como proveedor de identidades.
AD	Citrix Gateway federado en otro IdP (AAD/Okta)	AD	Sí	Aplicación Citrix Workspace/FAS	Configure el IdP mediante <a href="#">Configure SAML Single Sign-On</a> y consulte la documentación del IdP utilizado para configurar <a href="#">PassThrough de dominio</a> .

Dispositivo de punto final unido a	IdP	VDA unido a	SSO en Citrix Workspace	SSO en VDA	Documentación
AD	Okta	AD	Sí	Aplicación Citrix Workspace/FAS	<a href="#">PassThrough de dominio a Citrix Workspace con Okta como proveedor de identidades.</a>
Unido a AD/híbrido	AAD (AD con AAD Connect)	AD	Sí	Aplicación Citrix Workspace/FAS **	<a href="#">PassThrough de dominio a Citrix Workspace con Azure Active Directory como proveedor de identidades.</a>
AD	Un proveedor de identidades basado en SAML (por ejemplo: ADFS)	AD	Sí	Aplicación Citrix Workspace/FAS	Consulte <a href="#">Conectar SAML como proveedor de identidades con Citrix Cloud</a> y consulte la documentación del proveedor de identidades utilizado para configurar PassThrough de dominio.

Dispositivo de punto final unido a	IdP	VDA unido a	SSO en Citrix Workspace	SSO en VDA	Documentación
AD	AD	AD	No	No compatible	NA
AD	AD+OTP	AD	No	No compatible	NA
AD	AAD	AAD	No	No compatible	NA
AAD	AAD sin AD local	AD	Sí	FAS	Citrix Workspace usa Microsoft Edge WebView, que permite SSO en Workspace. SSO en VDA se puede usar a través de FAS. Para obtener más información, consulte <a href="#">Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.</a>

Dispositivo de punto final unido a	IdP	VDA unido a	SSO en Citrix Workspace	SSO en VDA	Documentación
AAD	AAD	AAD	Sí	El usuario debe introducir las credenciales.	Citrix Workspace usa Microsoft Edge WebView, que permite SSO en Workspace. No se admite SSO en VDA.
No unido a ningún dominio	IdP que admite la autenticación sin contraseña: Enlace	AD	No	FAS	Citrix Workspace usa Microsoft Edge WebView, que permite SSO en Workspace. SSO en VDA se puede usar a través de FAS. Para obtener más información, consulte <a href="#">Otras maneras de autenticarse en Citrix Workspace</a> .

**Notas:**

- El cliente debe poder contactarse en AD para que Kerberos funcione.
- \*\*Citrix Single Sign-On (SSONSVR.exe) solo funciona con el nombre de usuario o la contraseña en el cliente. Si el usuario usa Windows Hello para iniciar sesión, se necesita FAS.
- Es posible que la autenticación no sea completamente silenciosa en la nube si se habilita LLT o si se configura la directiva de aceptación de usuarios finales.



- Se recomienda configurar FAS, ya que se aplica a plataformas que no son Windows.

### PassThrough de dominio para StoreFront

Dispositivo de punto final unido a	IdP	VDA unido a	SSO en Citrix Workspace	SSO en VDA	Documentación
AD	StoreFront	AD	Sí	Aplicación Citrix Workspace	<a href="#">Autenticación PassThrough de dominio</a>
Unido a AD/híbrido/Windows Hello para empresas	StoreFront	AD	Sí(1)	Aplicación Citrix Workspace/FAS(2)	<a href="#">Autenticación de PassThrough de dominio y Habilitar Single Sign-On para espacios de trabajo con Citrix Federated Authentication Service</a>
AD	Citrix Gateway: Autenticación avanzada	AD	Sí	Aplicación Citrix Workspace(3)	
AD	Citrix Gateway: Autenticación básica	AD	Sí	Aplicación Citrix Workspace(4)	<a href="#">Autenticación PassThrough de dominio.</a>

#### Notas:

1. 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_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\`

`protocols\integratedwindows\`

The key prevents the Citrix Workspace app authentication manager from checking for the single sign-on component and allows Citrix Workspace app to authenticate to StoreFront.

2. Si usa Windows Hello para iniciar sesión, se necesitan FAS y la configuración del Registro para habilitar SSO.
3. Necesita que el cliente pueda contactarse en AD, ya que utiliza Kerberos.
4. Funciona incluso si el cliente no puede contactarse en AD. No se usa Kerberos.

## PassThrough de dominio a Citrix Workspace con Citrix Gateway local como proveedor de identidades

June 14, 2024

### Importante:

Este artículo ayuda a configurar la autenticación PassThrough de dominio. Si ya ha configurado Gateway local como proveedor de identidades, vaya a la sección [Configurar PassThrough de dominio como método de autenticación en Citrix Gateway](#).

Citrix Cloud admite el uso de dispositivos Citrix Gateway locales como proveedores de identidades para autenticar a los suscriptores que inician sesión en sus espacios de trabajo.

Con la autenticación de Citrix Gateway, puede:

- Siga autenticando a los usuarios a través de su dispositivo Citrix Gateway existente para que puedan acceder a los recursos de la implementación local de Virtual Apps and Desktops a través de Citrix Workspace.
- Utilice las funciones de autenticación, autorización y auditoría de Citrix Gateway con Citrix Workspace.
- Proporcione a los usuarios acceso a los recursos que necesitan a través de Citrix Workspace con funciones como la autenticación PassThrough, las tarjetas inteligentes, los tokens seguros, las directivas de acceso condicional, la federación y muchas otras.

La autenticación de Citrix Gateway se puede utilizar con las siguientes versiones de producto:

- Citrix Gateway 13.1.4.43 Advanced Edition o posterior

### Requisitos previos:

- Cloud Connectors: Necesita al menos dos (2) servidores donde instalar el software Citrix Cloud Connector.

- Active Directory y asegúrese de que el dominio esté registrado.
- Requisitos de Citrix Gateway
  - Use directivas avanzadas en la puerta de enlace local porque las directivas clásicas han dejado de utilizarse.
  - Cuando configure Gateway para autenticar suscriptores en Citrix Workspace, la puerta de enlace actúa como un proveedor de OpenID Connect. Los mensajes entre Citrix Cloud y Gateway se ajustan al protocolo OIDC, que implica la firma digital de tokens. Por lo tanto, debe configurar un certificado para firmar estos tokens.
  - Sincronización del reloj: Citrix Gateway debe sincronizarse con la hora NTP.

Para obtener más información, consulte [Requisitos previos](#) en la documentación de Citrix Cloud.

Antes de crear la directiva de IdP de OAuth, debe configurar Citrix Workspace o Cloud para que usen Gateway como opción de autenticación en el IdP (proveedor de identidades). Para obtener más información sobre cómo configurarlo, consulte [Conectar un dispositivo Citrix Gateway local como proveedor de identidades con Citrix Cloud](#). Cuando completa la configuración, se generan el ID de cliente, el secreto y la URL de redireccionamiento necesarios para crear la directiva de IdP de OAuth.

PassThrough de dominio para Workspace para web está habilitado si utiliza Internet Explorer, Microsoft Edge, Mozilla Firefox y Google Chrome. PassThrough de dominio solo se habilita cuando el cliente se detecta correctamente.

**Nota:**

Si un usuario prefiere el cliente HTML5 o el administrador lo exige, el método de autenticación PassThrough de dominio no está habilitado.

Al iniciar la URL de StoreFront en un explorador, se muestra el aviso **Detectar Receiver**.

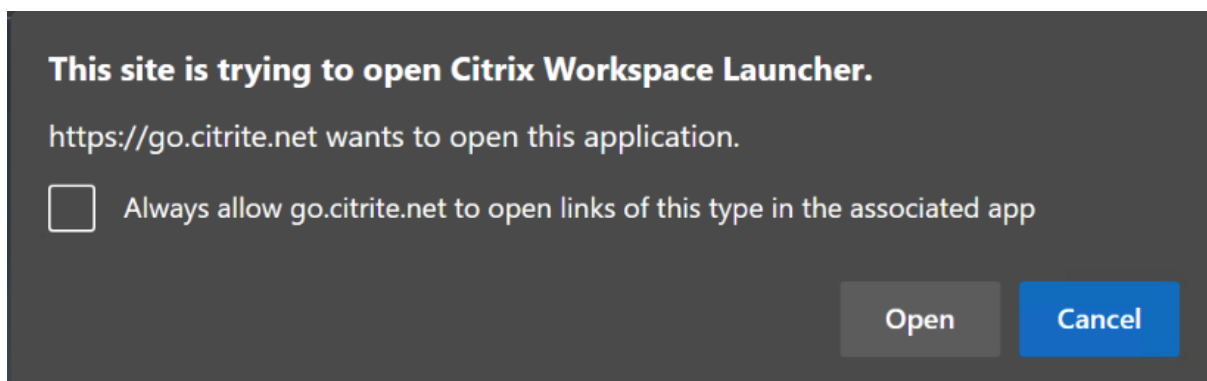
Si los dispositivos están administrados, configure la directiva de grupo para inhabilitar este aviso, en lugar de inhabilitar la detección de clientes. Para obtener más información, consulte:

- [URLAllowlist](#) en la documentación de Microsoft.
- [URLAllowlist](#) en la documentación de Google Chrome.

**Nota:**

El controlador de protocolo utilizado por la aplicación Citrix Workspace es **receiver**. Configúrelo como una de las URL permitidas.

Los usuarios también pueden seleccionar la casilla de verificación, como se muestra en el siguiente aviso de ejemplo, para una URL de StoreFront en la solicitud de detección del cliente. Al seleccionar esta casilla de verificación, se evita también el aviso en inicios posteriores.



En los siguientes pasos se explica cómo configurar Citrix Gateway como IdP.

### Crear una directiva de IdP de OAuth en el dispositivo Citrix Gateway local

La creación de una directiva de autenticación de IdP de OAuth implica las siguientes tareas:

1. Crea un perfil de IdP de OAuth.
2. Agregar una directiva de IdP de OAuth.
3. Enlazar la directiva de IdP de OAuth a un servidor virtual.
4. Enlazar el certificado globalmente.

### Crear un perfil de IdP de OAuth

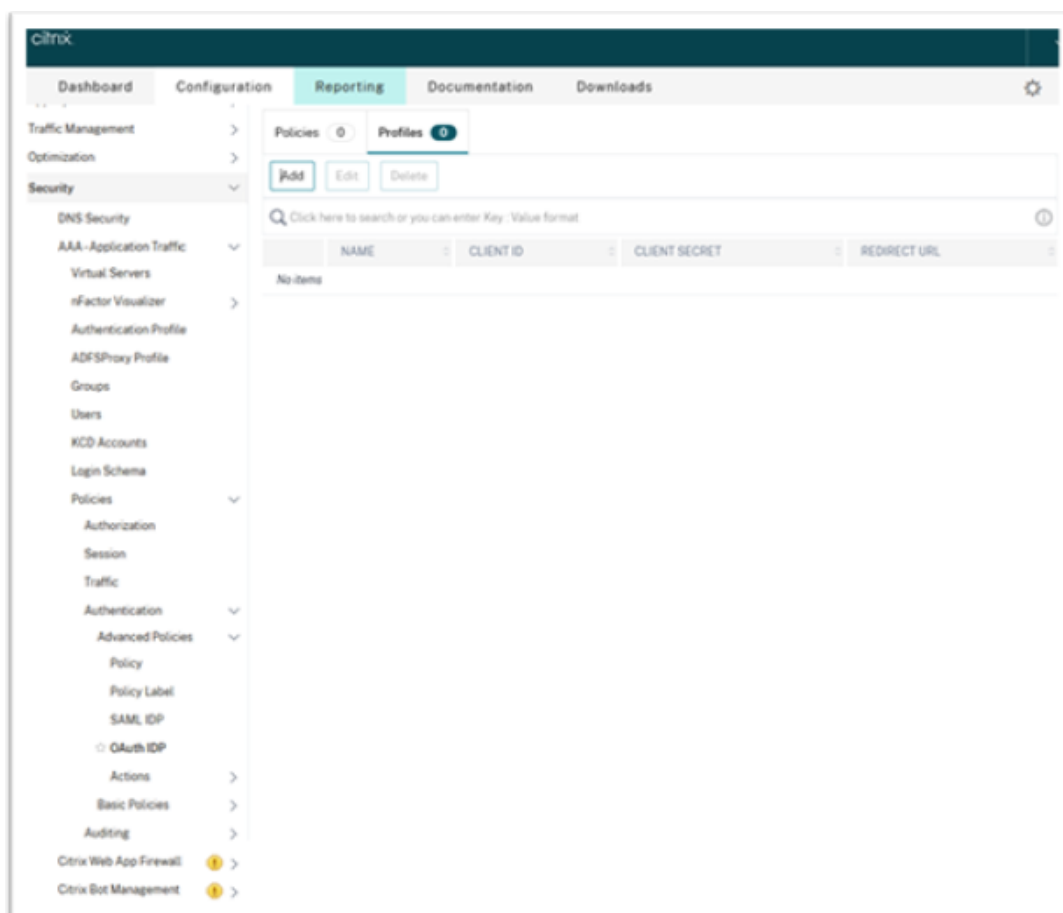
1. Para crear un perfil de IdP de OAuth a través de la CLI, escriba lo siguiente en el símbolo del sistema:

```
1 add authentication OAuthIdPProfile <name> [-clientID <string>][-  
clientSecret ][-redirectURL <URL>][-issuer <string>][-audience  
<string>][-skewTime <mins>] [-defaultAuthenticationGroup <  
string>]  
2  
3 add authentication OAuthIdPPolicy <name> -rule <expression> [-  
action <string> [-undefAction <string>] [-comment <string>][-  
logAction <string>]  
4  
5 add authentication ldapAction <name> -serverIP <IP> -ldapBase "dc=  
aaa,dc=local"  
6  
7 ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password  
> -ldapLoginName sAMAccountName  
8  
9 add authentication policy <name> -rule <expression> -action <  
string>  
10  
11 bind authentication vserver auth_vs -policy <ldap_policy_name> -  
priority <integer> -gotoPriorityExpression NEXT
```

```
12
13 bind authentication vserver auth_vs -policy <OAuthIdPPolicyName> -
    priority <integer> -gotoPriorityExpression END
14
15 bind vpn global -certkey <>
16
17 <!--NeedCopy-->
```

2. Para crear un perfil de IdP de OAuth a través de la GUI:

- a) Inicie sesión en el portal de administración local de Citrix Gateway y vaya a **Security > AAA –Application Traffic > Policies > Authentication > Advanced Policies > OAuth IDP**.



- b) En la página **OAuth IDP**, haga clic en la ficha **Profiles** y, a continuación, en **Add**.

- c) Configure el perfil de IdP de OAuth.

**Nota:**

- Copie y pegue los valores de ID de cliente, secreto y URL de redireccionamiento desde la ficha **Citrix Cloud > Identity and Access Management > Identity and Access Management** para establecer la conexión con Citrix Cloud.

- Introduzca la URL de Gateway correctamente en el campo **Issuer Name**. Por ejemplo, <https://GatewayFQDN.com>.
- Copie y pegue también el ID de cliente en el campo **Audience**.
- **Send Password**: Habilite esta opción para admitir Single Sign-On. De forma predeterminada, esta opción está inhabilitada.

d) En la pantalla **Create Authentication OAuth IdP Profile**, defina los valores para los siguientes parámetros y haga clic en **Create**.

- **Name**: Nombre del perfil de autenticación. Debe empezar por una letra, un número o un guion bajo (\_). El nombre solo debe tener letras, números y guiones (-), punto (.), libra (#), espacio (), arroba (@), igual (=), dos puntos (:) y guiones bajos. No puede cambiar el nombre una vez creado el perfil.
- **Client ID**: Cadena única que identifica al proveedor de servicios. El servidor de autorización infiere la configuración del cliente mediante este ID. Longitud máxima: 127.
- **Client Secret**: Cadena secreta establecida por el usuario y el servidor de autorización. Longitud máxima: 239.
- **Redirect URL**: Dispositivo de punto final del proveedor de servicios al que se debe enviar el código/token.
- **Issuer Name**: Identidad del servidor cuyos tokens se van a aceptar. Longitud máxima: 127. Ejemplo: <https://GatewayFQDN.com>.
- **Audience**: Destinatario al que se dirige el token enviado por el IdP. El destinatario verifica este token.
- **Skew Time**: Esta opción especifica el sesgo de reloj (en minutos) que Citrix ADC permite para un token entrante. Por ejemplo, si skewTime es 10, el token es válido desde (hora actual - 10) minutos hasta (hora actual + 10) minutos, es decir, 20 minutos en total. Valor predeterminado: 5
- **Default Authentication Group**: Un grupo que se agrega a la lista de grupos internos de la sesión cuando el IdP elige este perfil y que se puede usar en el flujo nFactor. Se puede usar en la expresión (AAA.USER.IS\_MEMBER\_OF("xxx")) para que las directivas de autenticación identifiquen el flujo nFactor relacionado con el usuario de confianza. Longitud máxima: 63

Se agrega un grupo a la sesión de este perfil para simplificar la evaluación de las directivas y ayudar a personalizarlas. Este es el grupo predeterminado que se elige cuando la autenticación tiene éxito además de los grupos extraídos. Longitud máxima: 63.

The screenshot shows the Citrix console interface for creating an OAuth IDP profile. The navigation bar includes Dashboard, Configuration, Reporting, Documentation, and Downloads. The main heading is 'Create Authentication OAuth IDP Profile'. The form contains the following fields and options:

- Name\*: gatewayIDP
- Client ID\*: cclientid
- Client Secret\*: cclientsecret
- Redirect URL\*: https://redirecturl
- Issuer Name: (empty)
- Audience: cclientid
- Skew Time (mins): 5
- Default Authentication Group: testGroup
- Relying Party Metadata URL: (empty)
- Refresh Interval: 50
- Encrypt Token
- Signature Service: (empty)
- Attributes: (empty)
- Send Password

At the bottom, there are 'Create' and 'Close' buttons.

### Agregar una directiva de IdP de OAuth

1. En la página OAuth IdP , haga clic en **Policies** y, a continuación, en **Add**.
2. En la pantalla **Create Authentication OAuth IdP Policy**, defina los valores de los siguientes parámetros y haga clic en **Create**.
  - **Name**: El nombre de la directiva de autenticación.
  - **Action**: Nombre del perfil creado anteriormente.
  - **Log Action**: Nombre de la acción del registro de mensajes que se utilizará cuando una solicitud coincida con esta directiva. No es un campo obligatorio.
  - **Undefined-Result Action**: Acción que realizar si el resultado de la evaluación de directivas es indefinido (UNDEF). No es un campo obligatorio.
  - **Expression**: Expresión sintáctica predeterminada que la directiva utiliza para responder a una solicitud específica. Por ejemplo, true.
  - **Comments**: Cualquier comentario sobre la directiva.

The screenshot shows the 'Create Authentication OAuth IDP Policy' form in the Citrix Gateway administration console. The form has the following fields and controls:

- Name\***: A text input field containing 'gatewayIDP\_pol'.
- Action\***: A dropdown menu with 'gatewayIDP' selected, accompanied by 'Add' and 'Edit' buttons.
- Log Action**: A dropdown menu with an empty selection, accompanied by 'Add' and 'Edit' buttons.
- Undefined Result Action**: A dropdown menu with an empty selection.
- Expression\***: A section containing three 'Select' dropdown menus, a text area with 'true', and an 'Evaluate' button.
- Comments**: A large text area for additional notes.
- Buttons**: 'Create' and 'Close' buttons at the bottom of the form.

**Nota:**

Cuando sendPassword se establece en ON (tiene el valor OFF de forma predeterminada), las credenciales del usuario se cifran y se transmiten a través de un canal seguro a Citrix Cloud. La transmisión de las credenciales de usuario a través de un canal seguro le permite habilitar Single Sign-On en Citrix Virtual Apps and Desktops al iniciarse.

**Enlazar la directiva de OAuthIDP y la directiva de LDAP al servidor de autenticación virtual**

Ahora debe enlazar la directiva de IdP de OAuth al servidor de autenticación virtual en Citrix Gateway local.

1. Inicie sesión en el portal de administración local de Citrix Gateway y vaya a **Configuration > Security > AAA-Application Traffic > Policies > Authentication > Advanced Policies > Actions > LDAP**.
2. En la pantalla **LDAP Actions**, haga clic en **Add**.
3. En la pantalla c, defina los valores de los siguientes parámetros y haga clic en **Create**.
  - **Name**: El nombre de la acción LDAP.
  - **ServerName/ServerIP**: Proporcione el FQDN o la IP del servidor LDAP.
  - Elija valores apropiados para **Security Type**, **Port**, **Server Type** y **Time-Out**.
  - Asegúrese de que la opción **Authentication** esté marcada.



- **Base DN:** Base desde la que se inicia la búsqueda LDAP. Por ejemplo `dc=aaa,dc=local`.
  - **Administrator Bind DN:** Nombre de usuario del enlace al servidor LDAP. Por ejemplo, `admin@aaa.local`.
  - **Administrator Password/Confirm Password:** Contraseña para enlazar LDAP.
  - Haga clic en **Test Connection** para probar la configuración.
  - **Server Logon Name Attribute:** Elija «sAMAccountName».
  - Otros campos no son obligatorios y, por lo tanto, se pueden configurar según sea necesario.
4. Vaya a **Configuration > Security > AAA-Application Traffic > Policies > Authentication > Advanced Policies > Policy**.
  5. En la pantalla **Authentication Policies**, haga clic en **Add**.
  6. En la página **Create Authentication Policy**, defina los valores de los siguientes parámetros y haga clic en **Create**.
    - **Name:** Nombre de la directiva de autenticación de LDAP.
    - **Action Type:** Elija LDAP.
    - **Action:** Elija la acción LDAP.
    - **Expression:** Expresión sintáctica predeterminada que la directiva utiliza para responder a una solicitud específica. Por ejemplo, `true**`.

### Enlazar el certificado globalmente a la VPN

Para enlazar el certificado de forma global a la VPN, se requiere acceso de CLI al dispositivo Citrix Gateway local. Con Putty (o similar), inicie sesión en el dispositivo Citrix Gateway local mediante SSH.

1. Inicie una utilidad de línea de comandos, como Putty.
2. Inicie sesión en Citrix Gateway local mediante SSH.
3. Escriba este comando:

```
show vpn global
```

**Nota:**

No se debe enlazar ningún certificado.

Mostrar VPN global/en-us/citrix-workspace-app-for-windows/media/show-vpn-global.png

4. Para mostrar los certificados en el dispositivo Citrix Gateway local, escriba el siguiente comando:

```
show ssl certkey
```

5. Seleccione el certificado apropiado y escriba el siguiente comando para enlazar el certificado de forma global a la VPN:

```
bind vpn global -certkey cert_key_name
```

donde cert\_key\_name es el nombre del certificado.

6. Escriba el siguiente comando para comprobar si el certificado está enlazado globalmente a la VPN:

```
show vpn global
```

Mostrar VPN global/en-us/citrix-workspace-app-for-windows/media/show-vpn-global-1.png

## Configurar PassThrough de dominio como método de autenticación en Citrix Gateway

Cuando termine de configurar Citrix Gateway como IdP, siga estos pasos para configurar PassThrough de dominio como método de autenticación en Citrix Gateway.

Cuando se establece PassThrough de dominio como método de autenticación, el cliente utiliza tíquets de Kerberos, en lugar de credenciales, para autenticarse.

Citrix Gateway admite tanto suplantación como delegación limitada de Kerberos (KCD). Sin embargo, en este artículo se describe la autenticación KCD. Para obtener más información, consulte el artículo [CTX236593](#) de Knowledge Center.

La configuración de PassThrough de dominio incluye los siguientes pasos:

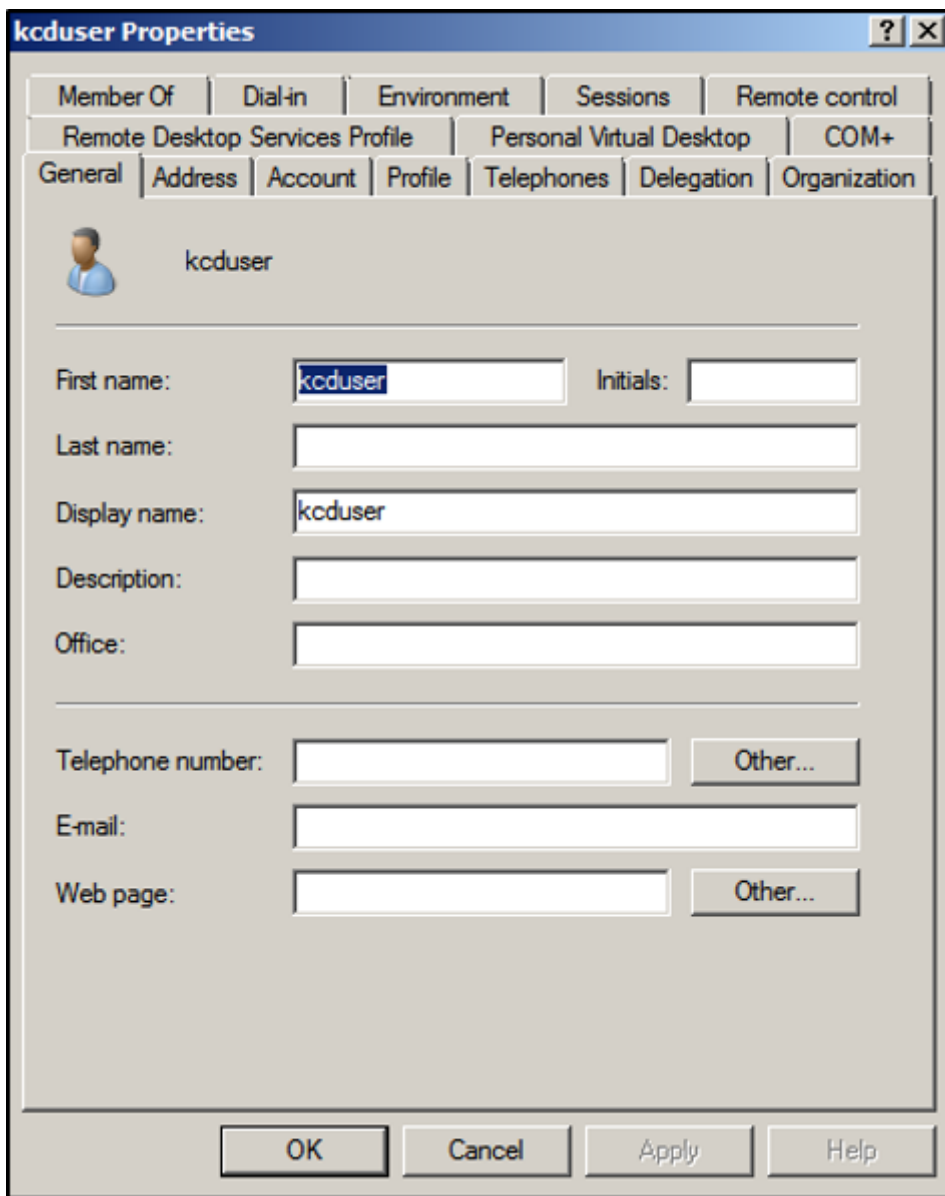
1. Configuración de delegación limitada de Kerberos
2. Configuración del cliente

### Configuración de delegación limitada de Kerberos

1. Crear un usuario de KCD en Active Directory

Kerberos funciona con un sistema de concesión de tíquets para autenticar a los usuarios en los recursos, e implica un cliente, un servidor y un centro de distribución de claves (KDC).

Para que Kerberos funcione, el cliente debe solicitar un tíquet al KDC. El cliente primero debe autenticarse en el KDC con su nombre de usuario, contraseña y dominio antes de solicitar un tíquet, denominado solicitud AS.



2. Asocie al nuevo usuario con el nombre de principal de servicio (SPN).

El cliente utiliza el SPN de Gateway para autenticarse.

- Nombre principal de servicio (SPN): Un nombre principal de servicio (SPN) es un identificador único de una instancia de servicio. La autenticación Kerberos usa SPN para asociar una instancia de servicio a una cuenta de inicio de sesión de servicio. Esta función permite que una aplicación cliente solicite la autenticación de servicio de una cuenta, incluso si el cliente no tiene el nombre de la cuenta.

SetSPN es la aplicación utilizada para administrar los SPN en un dispositivo Windows. Con SetSPN, se pueden ver, modificar y eliminar registros de SPN.

- a) En el servidor de Active Directory, abra un símbolo del sistema.

b) En el símbolo del sistema, introduzca el siguiente comando:

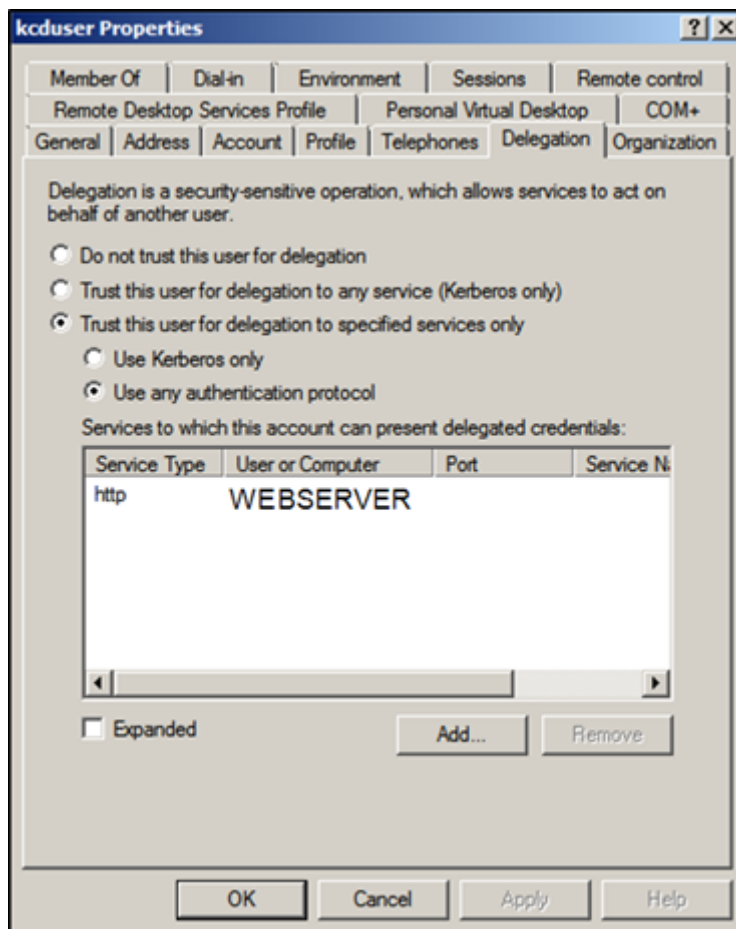
```
setspn -A http/<LB fqdn> <domain\Kerberos user>
```

c) Para confirmar los SPN del usuario de Kerberos, ejecute el siguiente comando:

```
setspn -l <Kerberos user>
```

La ficha Delegación aparece después de ejecutar el comando `setspn`.

d) Seleccione las opciones **Confiar en este usuario para la delegación solo a los servicios especificados** y **Usar cualquier protocolo de autenticación**. Agregue el servidor web y seleccione el servicio HTTP.

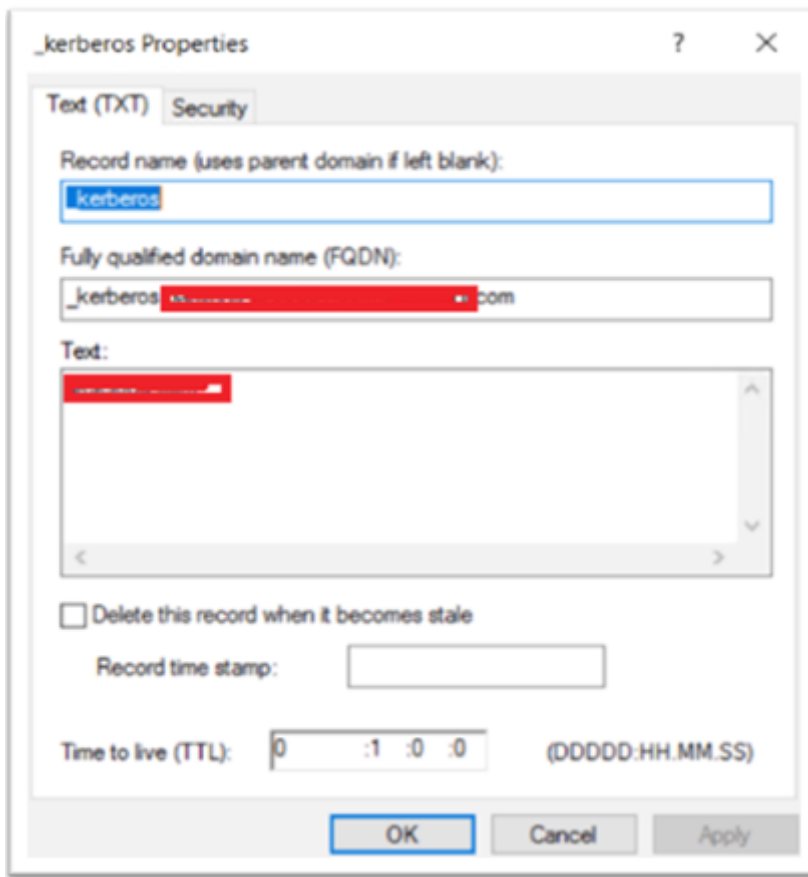


3. Cree un registro DNS para que el cliente encuentre el SPN de Gateway:

Agregue un registro TXT de DNS en Active Directory.

**Nota:**

El nombre debe comenzar por `_Kerberos`, los datos deben ser el nombre de dominio. El FQDN debe mostrar Kerberos..



El cliente unido al dominio de Windows usa `_kerberos.fqdn` para solicitar tíquets. Por ejemplo, si el cliente está unido a `citrite.net`, el sistema operativo puede obtener tíquets para cualquier sitio web con `*.citrite.net`. Sin embargo, si el dominio de Gateway es externo, como `gateway.citrix.com`, el sistema operativo cliente no puede obtener el tíquet de Kerberos.

Por lo tanto, debe crear un registro TXT de DNS que ayude al cliente a buscar `_kerberos.gateway.citrix.com` y obtener el tíquet de Kerberos para la autenticación.

#### 4. Configure Kerberos como factor de autenticación.

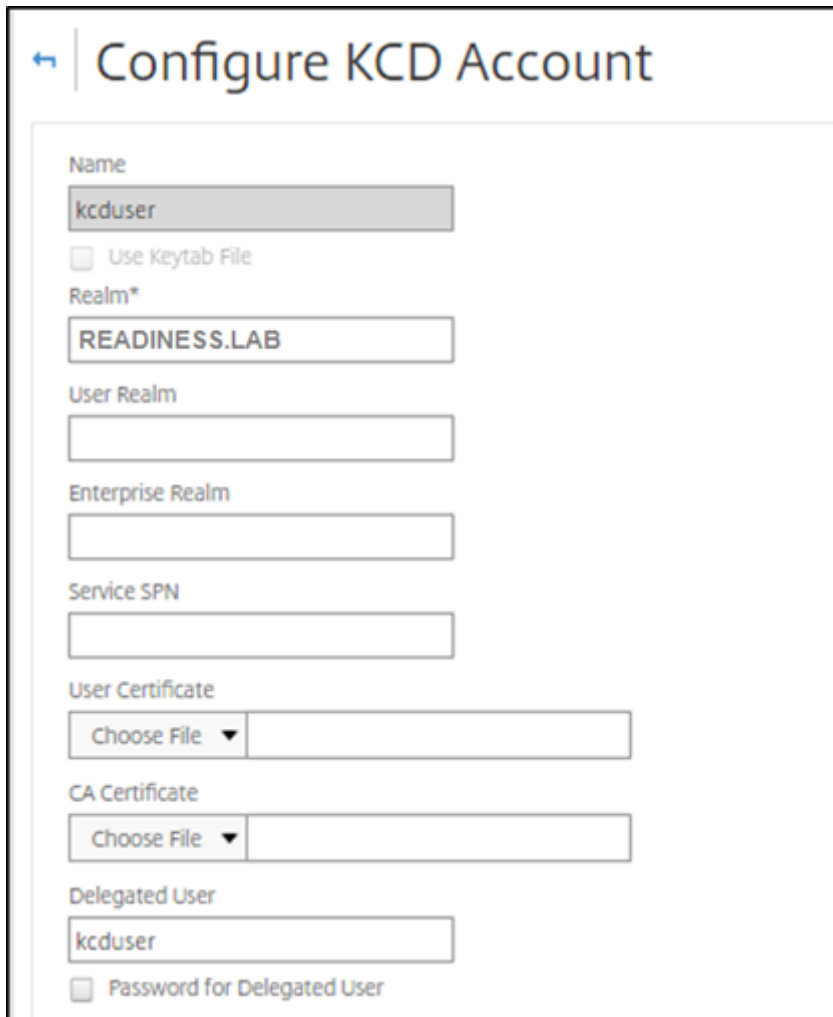
- a) Cree una cuenta de KCD para el usuario de NetScaler. Aquí hemos optado por hacerlo manualmente, pero puede crear un archivo `keytab`.

##### Nota:

Si utiliza dominios alternativos (dominio interno y dominio externo), debe configurar el nombre SPN del servicio en `HTTP/PublicFQDN.com@InternalDomain.ext`.

- **Realm:** Territorio Kerberos. Por lo general, el sufijo del dominio interno.
- **User Realm:** Es el sufijo del dominio interno del usuario.

- **Enterprise Realm:** Solo se debe dar en ciertas implementaciones de KDC en las que KDC espera un nombre de usuario empresarial, en lugar de un nombre principal.
- **Delegated User:** Es la cuenta de usuario de NetScaler para KCD que creó en AD en los pasos anteriores. Asegúrese de que la contraseña es correcta.



The screenshot shows a web form titled "Configure KCD Account" with a back arrow icon. The form contains the following fields and options:

- Name:** Text input field containing "kcduser".
- Use Keytab File
- Realm\*:** Text input field containing "READINESS.LAB".
- User Realm:** Empty text input field.
- Enterprise Realm:** Empty text input field.
- Service SPN:** Empty text input field.
- User Certificate:** "Choose File" dropdown menu and an empty text input field.
- CA Certificate:** "Choose File" dropdown menu and an empty text input field.
- Delegated User:** Text input field containing "kcduser".
- Password for Delegated User

- b) Asegúrese de que el perfil de sesión utiliza la cuenta de KCD correcta. Enlace la directiva de sesión al servidor virtual de autenticación, autorización y auditoría.

← | **Configure Session Profile**

Name  
mysso

Unchecked Override Global check box indicates that the value is inherited from Global Session Parameters.

	Override Global
Session Time-out (mins) 10	<input checked="" type="checkbox"/>
Default Authorization Action* ALLOW	<input checked="" type="checkbox"/>
Single Sign-on to Web Applications* ON	<input checked="" type="checkbox"/>
Credential Index* PRIMARY	<input checked="" type="checkbox"/>
Single Sign-on Domain readiness	<input checked="" type="checkbox"/>
HTTPOnly Cookie* YES	<input type="checkbox"/>
Enable Persistent Cookie* OFF	<input type="checkbox"/>
Persistent Cookie Validity	<input type="checkbox"/>
KCD Account kcduser	<input checked="" type="checkbox"/>
Home Page	<input type="checkbox"/>

- c) Enlace la directiva de autenticación al servidor virtual de autenticación, autorización y auditoría. Estas directivas utilizan métodos de autenticación, autorización y auditoría que no obtienen una contraseña del cliente, de ahí la necesidad de usar KCD. Sin embargo, deben obtener el nombre de usuario y la información de dominio, en formato UPN.

**Nota:**

Puede usar el análisis de EPA o dirección IP para diferenciar los dispositivos unidos a

un dominio y los que no están unidos a un dominio y usar Kerberos o LDAP normal como factor de autenticación.

## Configurar el cliente

Para que Single Sign-On funcione correctamente en el VDA, haga lo siguiente.

### Requisitos previos:

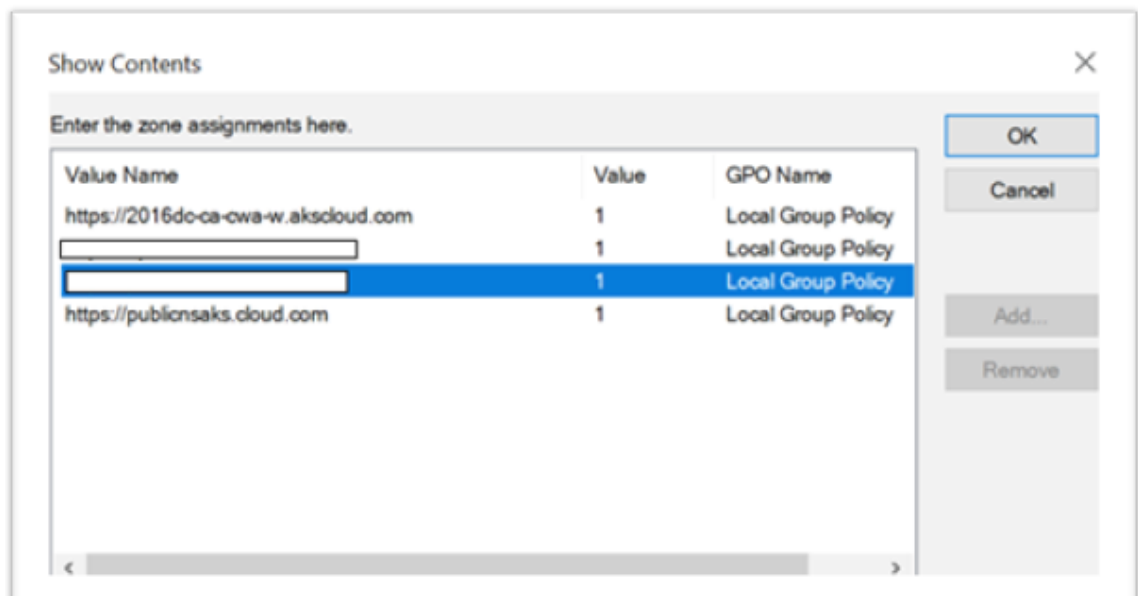
- Máquina unida a un dominio
- Citrix Workspace 2112.1 o posterior con Single Sign-On habilitado
- URL de confianza necesarias que comprueban si las conexiones son seguras
- Validar Kerberos desde el cliente y AD. El sistema operativo del cliente debe tener conectividad con AD para obtener los tiquets de Kerberos.

A continuación, se presentan algunas de las URL de confianza en el explorador.

- FQDN o URL de Gateway
- FQDN de AD
- URL del espacio de trabajo para Single Sign-On con inicios desde un explorador.

1. Si utiliza Internet Explorer, Microsoft Edge o Google Chrome, haga lo siguiente:

- a) Inicie el explorador.
- b) Abra el Editor de directivas de grupo local en el cliente.



- a) Vaya a la página **Configuración del equipo > Componente de Windows > Internet Explorer > Panel de control de Internet > Seguridad**.



- b) Abra Lista de asignación de sitio a zona y agregue todas las URL enumeradas con el valor uno (1).
  - c) (Opcional) Ejecute `Gpupdate` para aplicar directivas.
2. Si utiliza el explorador Mozilla Firefox, haga lo siguiente:
- a) Abra el explorador.
  - b) Escriba `about:config` en la barra de búsqueda.
  - c) Acepte el riesgo y continúe.
  - d) En el campo de búsqueda, escriba **negotiate**.
  - e) En la lista de datos completados, verifique si **network.negotiate-auth.trusted-uris** está configurado en el valor de dominio.



De esta forma, se completa la configuración en el lado del cliente.

3. Inicie sesión con la aplicación Citrix Workspace o con el explorador web en Workspace.

Esto no debe solicitar el nombre de usuario ni la contraseña en un dispositivo unido a un dominio.

## Solución de problemas de Kerberos

### Nota:

Para ejecutar este paso de verificación, debe ser administrador de dominio.

En el símbolo del sistema o en Windows PowerShell, ejecute el siguiente comando para comprobar la validación del tíquet de Kerberos para el usuario de SPN:

```
KLIST get host/FQDN of AD
```

## PassThrough de dominio a Citrix Workspace con Azure Active Directory como proveedor de identidades

June 14, 2024

Se puede implementar Single Sign-On (SSO) en Citrix Workspace con Azure Active Directory (AAD) como proveedor de identidades con dispositivos de punto final/VM unidos a un dominio, híbridos o inscritos en AAD.

Con esta configuración, también puede usar Windows Hello para SSO en Citrix Workspace mediante dispositivos de punto final inscritos en AAD.

- Puede autenticarse en la aplicación Citrix Workspace con Windows Hello.
- Autenticación basada en FIDO2 con la aplicación Citrix Workspace.
- Single Sign-On en la aplicación Citrix Workspace desde máquinas unidas a Microsoft AAD (AAD como IdP) y acceso condicional con AAD.

Para el inicio de sesión único (SSO) en aplicaciones y escritorios virtuales, puede implementar FAS o configurar la aplicación Citrix Workspace de la siguiente manera.

**Nota:**

SSO en los recursos de Citrix Workspace solo funciona con Windows Hello. Sin embargo, se le pedirá el nombre de usuario y la contraseña al acceder a sus aplicaciones y escritorios virtuales publicados. Para resolver este aviso, puede implementar FAS y SSO en escritorios y aplicaciones virtuales.

**Requisitos previos:**

1. Conecte Azure Active Directory a Citrix Cloud. Para obtener más información, consulte [Conectar Azure Active Directory a Citrix Cloud](#) en la documentación de Citrix Cloud.
2. Active la autenticación de Azure AD para acceder al espacio de trabajo Para obtener más información, consulte [Habilitar la autenticación de Azure AD para espacios de trabajo](#) en la documentación de Citrix Cloud.

Para implementar SSO en Citrix Workspace:

1. Configure la aplicación Citrix Workspace con includeSSON.
2. Inhabilite el atributo `prompt=login` en Citrix Cloud.
3. Configure PassThrough de Azure Active Directory con Azure Active Directory Connect.

**Configurar la aplicación Citrix Workspace para que admita SSO****Requisitos previos:**

- Citrix Workspace 2109 o una versión posterior.

**Nota:**

Si usa FAS para SSO, no es necesaria la configuración de Citrix Workspace.

1. Instale la aplicación Citrix Workspace desde la línea de comandos de administración con la opción `includeSSON`:

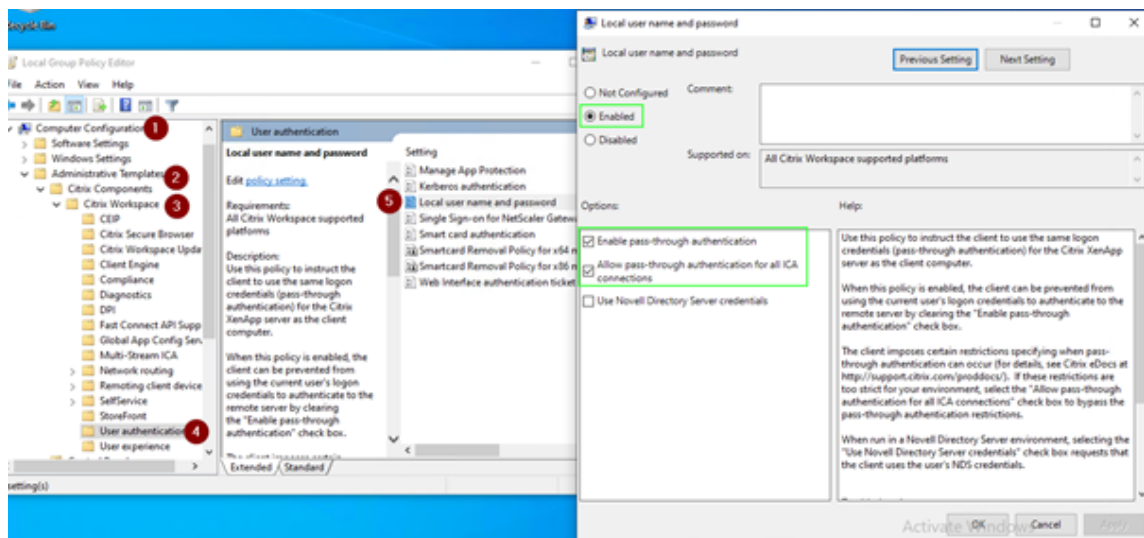
```
CitrixWorkspaceApp.exe /includeSSON
```

2. Cierre sesión en el cliente de Windows e inicie sesión para iniciar el servidor SSO.
3. Haga clic en **Configuración del equipo > Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Autenticación de usuarios** para cambiar el GPO de Citrix Workspace y permitir **el nombre de usuario y la contraseña actuales**.

**Nota:**

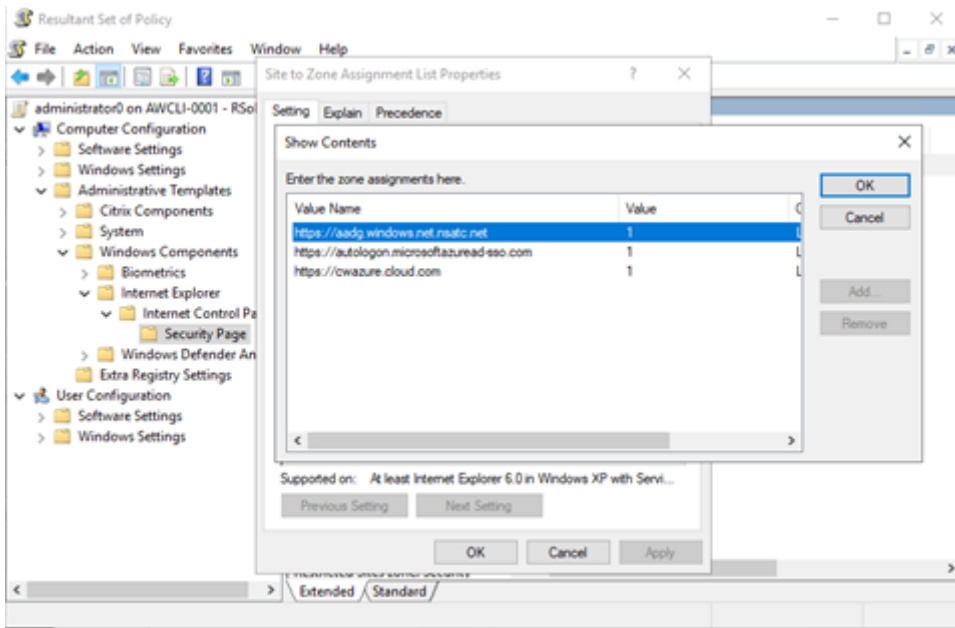
Estas directivas se pueden enviar al dispositivo cliente a través de Active Directory. Este paso solo es necesario para acceder a Citrix Workspace desde el explorador web.

4. Habilite la configuración como se indica en la captura de pantalla.



5. Agregue los siguientes sitios de confianza a través del GPO:

- <https://aadg.windows.net.nsatc.net>
- <https://autologon.microsoftazuread-ss0.com>
- <https://xxxtenantxxx.cloud.com>: URL del espacio de trabajo



**Nota:**

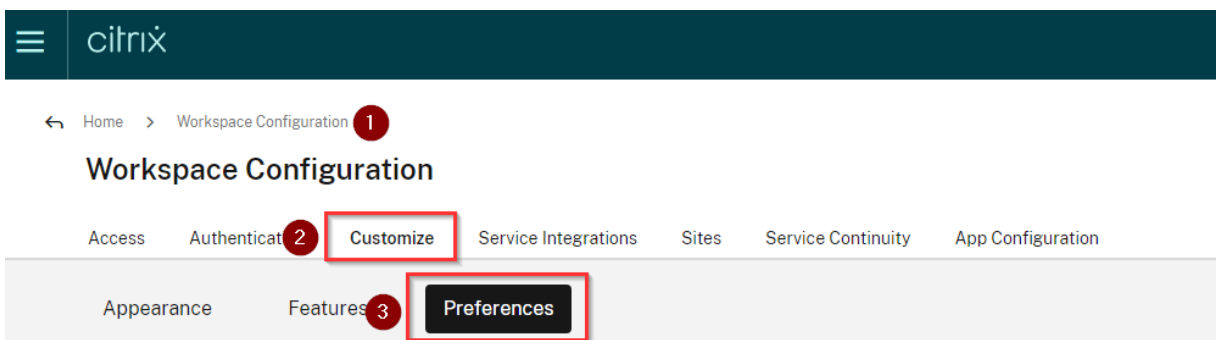
Cuando el registro **AllowSSOForEdgeWebview** de `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` se establece en false, se inhabilita Single Sign-On para AAD.

### Inhabilitar el parámetro `prompt=login` en Citrix Cloud

De forma predeterminada, `prompt=login` está habilitado para Citrix Workspace, lo que fuerza la autenticación incluso si el usuario optó por **mantener abierta la sesión** o si el dispositivo está unido a Azure AD.

Puede inhabilitar `prompt=login` en su cuenta de Citrix Cloud. Vaya a `Workspace Configuration\Customize\Preferences-Federated Identity Provider Sessions` e inhabilita la opción.

Para obtener más información, consulte el artículo [CTX253779](#) de Knowledge Center.



### Workspace Sessions

#### Federated Identity Provider Sessions



When Workspace is configured to use a federated identity provider, the authentication session and its lifetime are controlled by the identity provider. When enabled, Workspace forces a login prompt with the identity provider when a new Workspace session is needed. When disabled, a subscriber will not be prompted to authenticate with the identity provider if accessing Workspace with a valid session, achieving single sign-on.

#### Nota:

En los dispositivos unidos a AAD o a AAD híbrido, si se utiliza AAD como IdP para Workspace, la aplicación Citrix Workspace no solicita las credenciales. Los usuarios pueden iniciar sesión automáticamente con una cuenta profesional o educativa.

Para permitir que los usuarios inicien sesión con una cuenta diferente, establezca el siguiente registro en false.

Cree y agregue una cadena de Registro REG\_SZ con el nombre **AllowSSOForEdgeWebview** en `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` o `Computer\HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle` y establezca su valor en False. Como alternativa, si los usuarios cierran sesión en la aplicación Citrix Workspace, podrán iniciar sesión con una cuenta diferente la próxima vez.

## Configurar PassThrough de Azure Active Directory con Azure Active Directory Connect

- Si va a instalar Azure Active Directory Connect por primera vez, en la página **User sign-in**, seleccione **Pass-through Authentication** como método de inicio de sesión. Para obtener más información, consulte [Azure Active Directory Pass-Through Authentication: Quickstart](#) en la documentación de Microsoft.
- Si ya tiene Microsoft Azure Active Directory Connect:
  1. Seleccione la tarea **Change user sign-in** y haga clic en **Next**.
  2. Seleccione **Pass-through Authentication** como método de inicio de sesión.

#### Nota:

Puede omitir este paso si el dispositivo cliente está unido a Azure AD o tiene una unión híbrida. Si el dispositivo está unido a AD, la autenticación PassThrough de dominio funciona mediante la autenticación Kerberos.

## PassThrough de dominio a Citrix Workspace con Okta como proveedor de identidades

June 14, 2024

Puede implementar Single Sign-On en Citrix Workspace con Okta como proveedor de identidades (IdP).

### Requisitos previos:

- Citrix Cloud
  - Cloud Connectors

#### Nota:

Si es la primera vez que usa Citrix Cloud, defina una ubicación de recursos y configure los conectores. Se recomienda tener al menos dos Cloud Connectors implementados en entornos de producción. Para obtener información sobre la instalación de Citrix Cloud Connectors, consulte [Instalar Cloud Connector](#).

- Citrix Workspace
- Servicio de autenticación federada (opcional). Para obtener más información, consulte [Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix](#).
- Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)
- VDA unido al dominio de AD o dispositivos físicos unidos a AD
- Arrendatario de Okta
  - Agente de IWA para Okta (autenticación integrada de Windows)
  - Okta Verify (Okta Verify se puede descargar de la tienda de aplicaciones) (opcional)
- Active Directory

### 1. Implemente el agente de AD para Okta:

- a) En el portal de administración de Okta, haga clic en **Directory > Directory Integrations**.
- b) Haga clic en **Add Directory > Add Active Directory**.
- c) Revise los requisitos de instalación siguiendo el flujo de trabajo, que cubre los requisitos de instalación y arquitectura del agente.
- d) Haga clic en el botón **Set Up Active Directory** y, a continuación, en **Download Agent**.
- e) Instale el agente de AD para Okta en un servidor Windows. Para ello, siga las instrucciones que se indican en [Install the Okta Active Directory agent](#).

**Nota:**

Antes de instalar el agente, asegúrese de que se cumplen los requisitos previos mencionados en [Active Directory integration prerequisites](#).

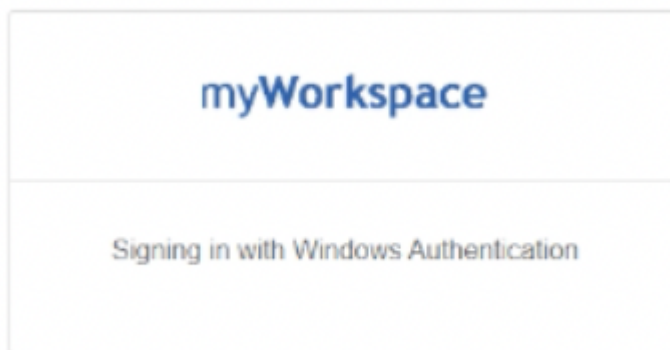
2. Configure la autenticación integrada de Windows (IWA):

- a) En el portal de administración de Okta, haga clic en **Security** y, a continuación, en **Delegated Authentication**
- b) En la página que se carga, desplácese a la sección **On-prem Desktop SSO** y haga clic en **Download Agent**.
- c) Configure las **reglas de redirección** para IWA. Para obtener más información, consulte [Configure Identity Provider routing rules](#).

3. Inicie el portal de clientes de Okta.

**Nota:**

- Cuando se instala el agente de IWA para Okta y el estado es habilitado, puede iniciar sesión desde un dispositivo unido a un dominio de Windows. Esta configuración además omite el inicio de sesión y lo dirige a la página de inicio de sesión de IWA y transmite las credenciales de usuario.



- Para obtener más información sobre cómo solucionar cualquier problema, consulte [Install and configure the Okta IWA Web agent for Desktop single sign-on](#).

4. Inicie sesión en Citrix Cloud, en <https://citrix.cloud.com>, y habilite Okta como proveedor de identidades. Para obtener información, consulte [Tech Insight: Authentication - Okta](#) en la documentación de Citrix Tech Zone.

**Nota:**

Puede iniciar sesión desde la aplicación Citrix Workspace o el explorador; ambos ofrecen la modalidad PassThrough que se indica en la documentación de Tech Zone.

5. Para el inicio de sesión único (SSO) en aplicaciones y escritorios virtuales, puede implementar FAS o configurar la aplicación Citrix Workspace.

**Nota:**

Sin FAS, se le pedirán el nombre de usuario y la contraseña de AD. Para obtener más información, consulte [Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix](#).

Si no usa FAS, [configure la aplicación Citrix Workspace para que admita SSO](#).

## PassThrough de dominio mejorado para Single Sign-On (SSO mejorado)

June 14, 2024

Antes, la aplicación Citrix Workspace para Windows solo permitía la autenticación SSON o la autenticación PassThrough de dominio para Single Sign-On en entornos de Citrix Virtual Apps and Desktops mediante credenciales de usuario. Esta autenticación permite al usuario autenticarse en el dominio de su dispositivo y usar sus aplicaciones y escritorios virtuales sin tener que autenticarse de nuevo.

Este enfoque para el PassThrough de dominio con credenciales de usuario tiene estas limitaciones:

- No permite la autenticación sin contraseña con métodos de autenticación modernos como Windows Hello o FIDO2. Se requiere un componente adicional denominado Servicio de autenticación federada (FAS) para Single Sign-On (SSO).
- La instalación o actualización de la aplicación Citrix Workspace con SSON habilitado requiere reiniciar el dispositivo.
- Requiere que las notificaciones del enrutador de varios proveedores (MPR) estén habilitadas en máquinas con Windows 11.
- Debe estar en la parte superior de la lista de proveedores de red.

Con esta versión, la aplicación Citrix Workspace ofrece un PassThrough de dominio mejorado, que es un nuevo método de SSO. Aprovecha la autenticación de Kerberos en lugar de las credenciales de usuario y ayuda a superar las limitaciones mencionadas anteriormente. Ahora, los usuarios pueden iniciar sesión en Citrix Virtual Apps and Desktops y en StoreFront mediante la autenticación de Windows integrada.

**Nota:**

Esta función no se ofrece en Windows 10 de 32 bits ni en Windows Server 2016.

### Requisitos del sistema

- Aplicación Citrix Workspace 2309 o una versión posterior
- Citrix Virtual Apps and Desktops 2308 o una versión posterior



## Versiones de SO de VDA compatibles

- Para SO multisesión:
  - Windows Server 2019
  - Windows Server 2022
- Para SO de sesión única:
  - Windows 10, versión 22H2
  - Windows 11, versión 22H2

## Requisitos previos

- El cliente o el dispositivo de punto final deben estar conectados al dominio.
- Requiere una línea de visión directa de Active Directory.

## Parámetros de StoreFront y DDC

Configure un entorno de PassThrough de dominio mediante estos parámetros:

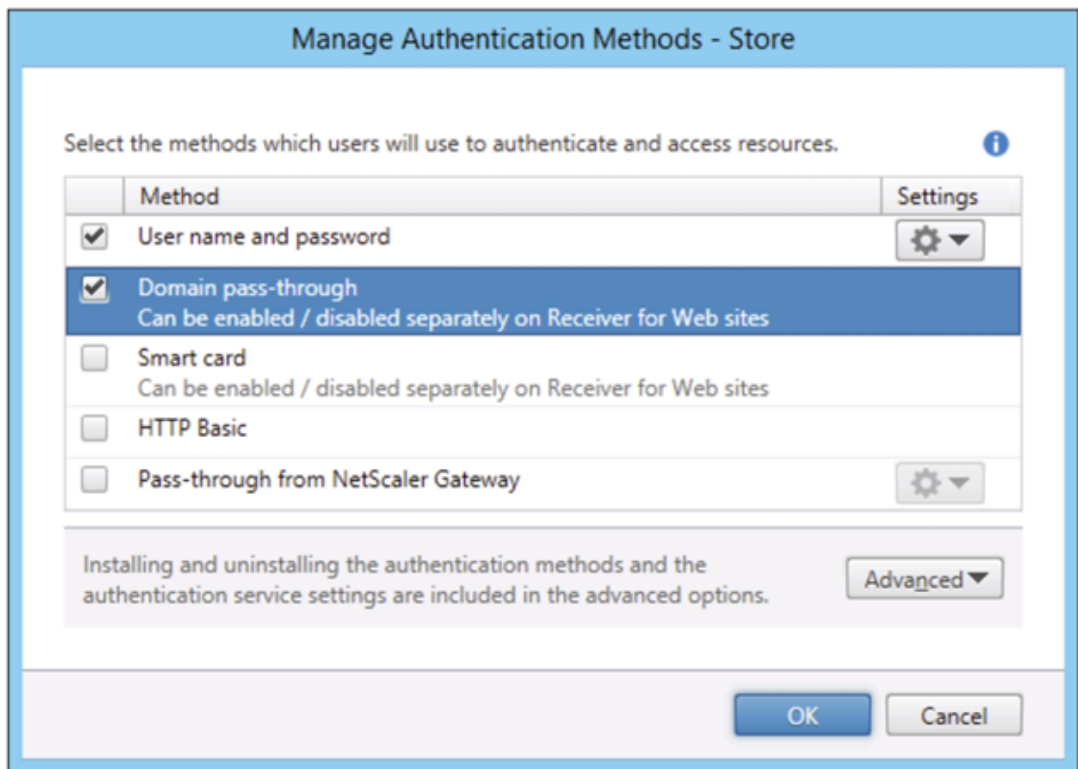
### Nota:

Puede omitir este paso si ya configuró el PassThrough de dominio en su entorno.

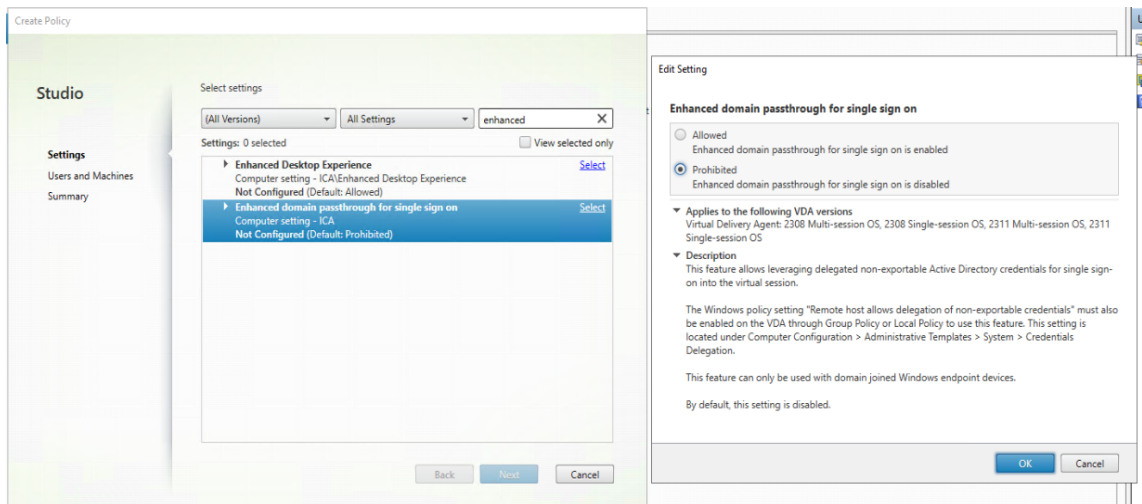
1. Cuando la aplicación Citrix Workspace está configurada en StoreFront:
  - a) Abra **StoreFront Studio**.
  - b) Vaya a **Almacén > Administrar métodos de autenticación**.
  - c) Habilite **PassThrough de dominio**.

O bien:

1. Al usar la aplicación Citrix Workspace desde el explorador web:
  - a) Abra StoreFront.
  - b) Abra **Almacenes > Sitios de Receiver para Web > Administrar métodos de autenticación**.
  - c) Habilite **PassThrough de dominio**.



2. Habilite la directiva **PassThrough de dominio mejorado para Single Sign-On** en DDC.

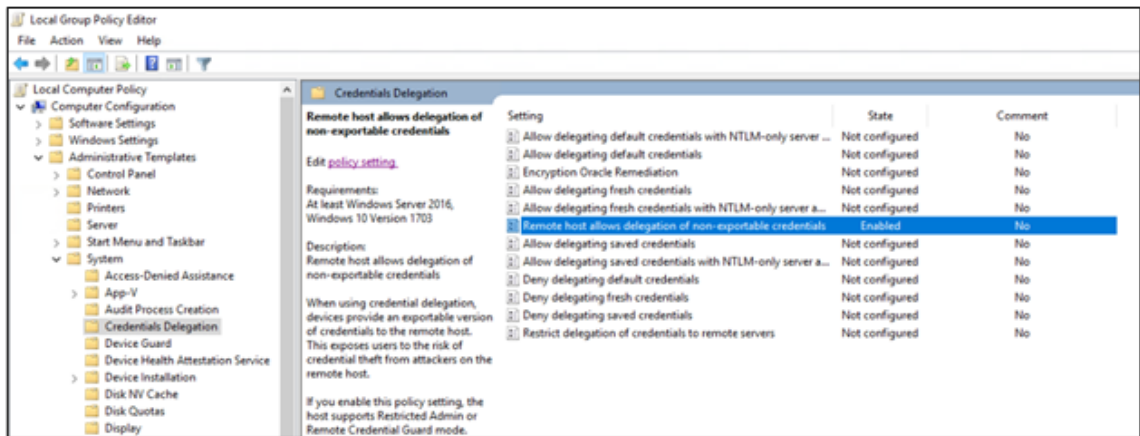


3. Haga clic en **Aceptar**.

## Parámetros de VDA

1. Vaya a **Configuración del equipo\Plantillas administrativas\Sistema\Delegación de credenciales** en el VDA.

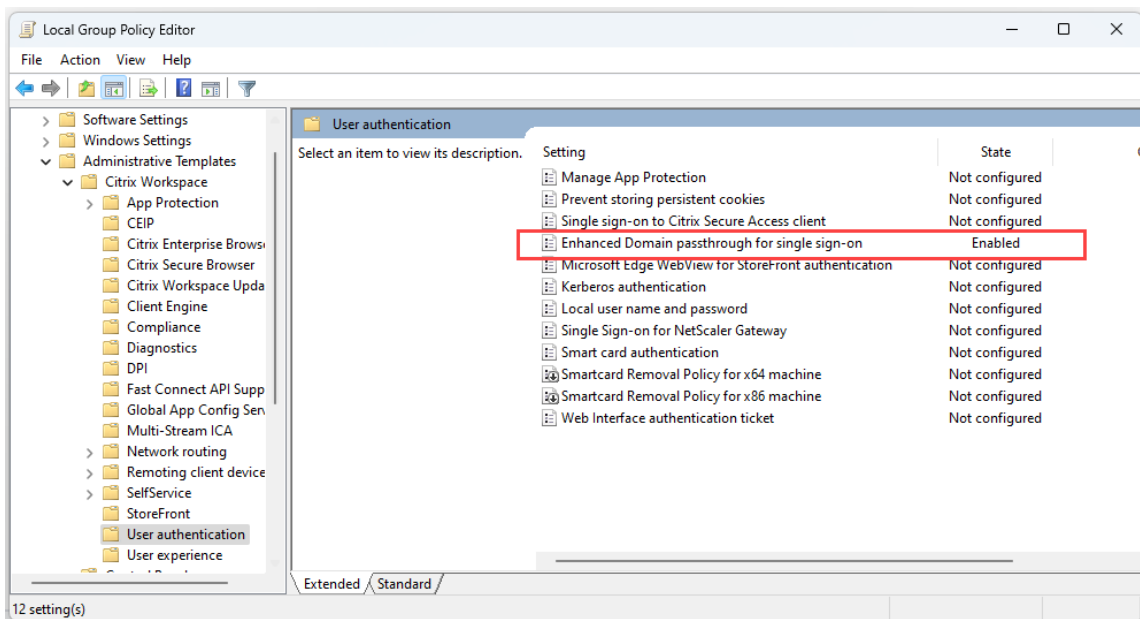
2. Habilita la directiva de Windows **El host remoto permite la delegación de credenciales no exportables** en el VDA.

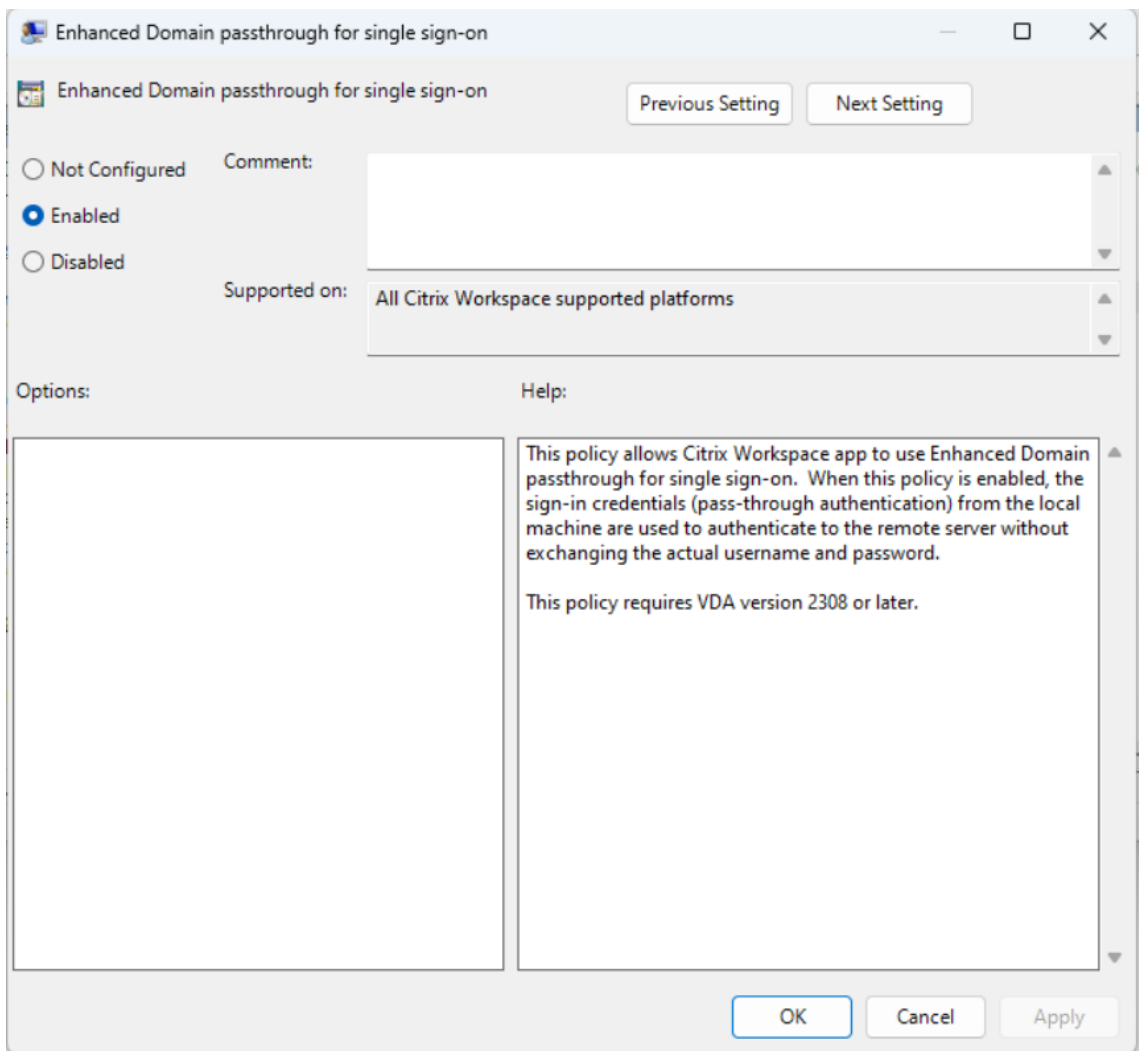


3. Reinicie la máquina VDA.

## Parámetros del cliente

1. Asegúrese de que la máquina cliente esté unida a un dominio.
2. Asegúrese de que la máquina cliente sea de 64 bits.
3. Abra el **Editor de directivas de grupo**.
4. Vaya a **Configuración del equipo\Plantillas administrativas\Componentes de Citrix\Citrix Workspace\Autenticación de usuarios**.
5. Configure la directiva de grupo **PassThrough de dominio mejorado para Single Sign-On**.





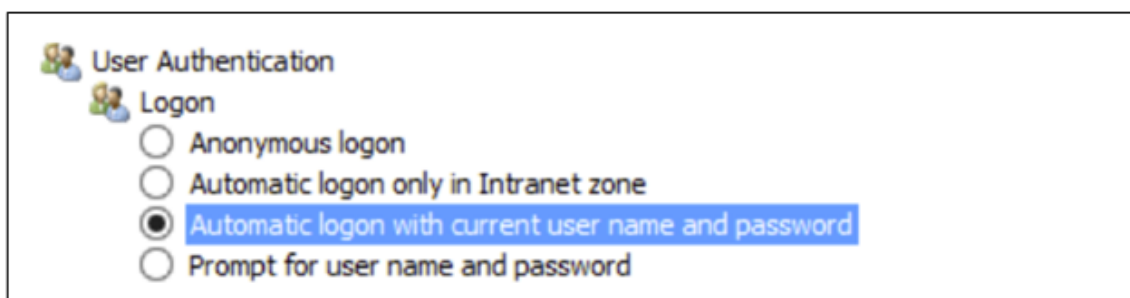
6. Modifique los parámetros de **Opciones de Internet** en el cliente.

**Nota:**

Puede omitir este paso si ya configuró el PassThrough de dominio en su entorno.

1. Agregue el servidor de StoreFront a la lista de sitios de confianza mediante **Opciones de Internet**. Para agregarlo:
  - a) Abra **Opciones de Internet** desde **Panel de control > Red e Internet**.
  - b) Haga clic en **Seguridad > Internet local** y, a continuación, haga clic en **Sitios**. Aparecerá la ventana **Intranet local**.
  - c) Haga clic en la ficha **Avanzado**.
  - d) Agregue la URL del FQDN de StoreFront con los protocolos HTTP o HTTPS correspondientes.
  - e) Haga clic en **Cerrar** y en **Aceptar**.
2. Modifique los parámetros de Autenticación de usuarios en Internet Explorer. Para modificarlos:

- a) Abra **Opciones de Internet** desde **Panel de control > Red e Internet**.
- b) Haga clic en la ficha **Seguridad > Intranet local**.
- c) Haga clic en **Nivel personalizado**. Aparece la ventana **Configuración de seguridad: Zona de intranet local**.
- d) En el panel **Autenticación del usuario**, seleccione **Inicio de sesión automático con el nombre de usuario y contraseña actuales**.



3. Haga clic en **Aceptar**.

## HDX

April 22, 2024

En esta sección se describe lo siguiente:

- [Gráficos y pantalla](#)
- [Microsoft Teams optimizado](#)
- [Transporte HDX](#)
- [Redirección de contenido del explorador web](#)
- [Redirección bidireccional de contenido](#)
- [Referencia para parámetros ICA](#)

## Gráficos y pantalla

June 17, 2024

### 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.

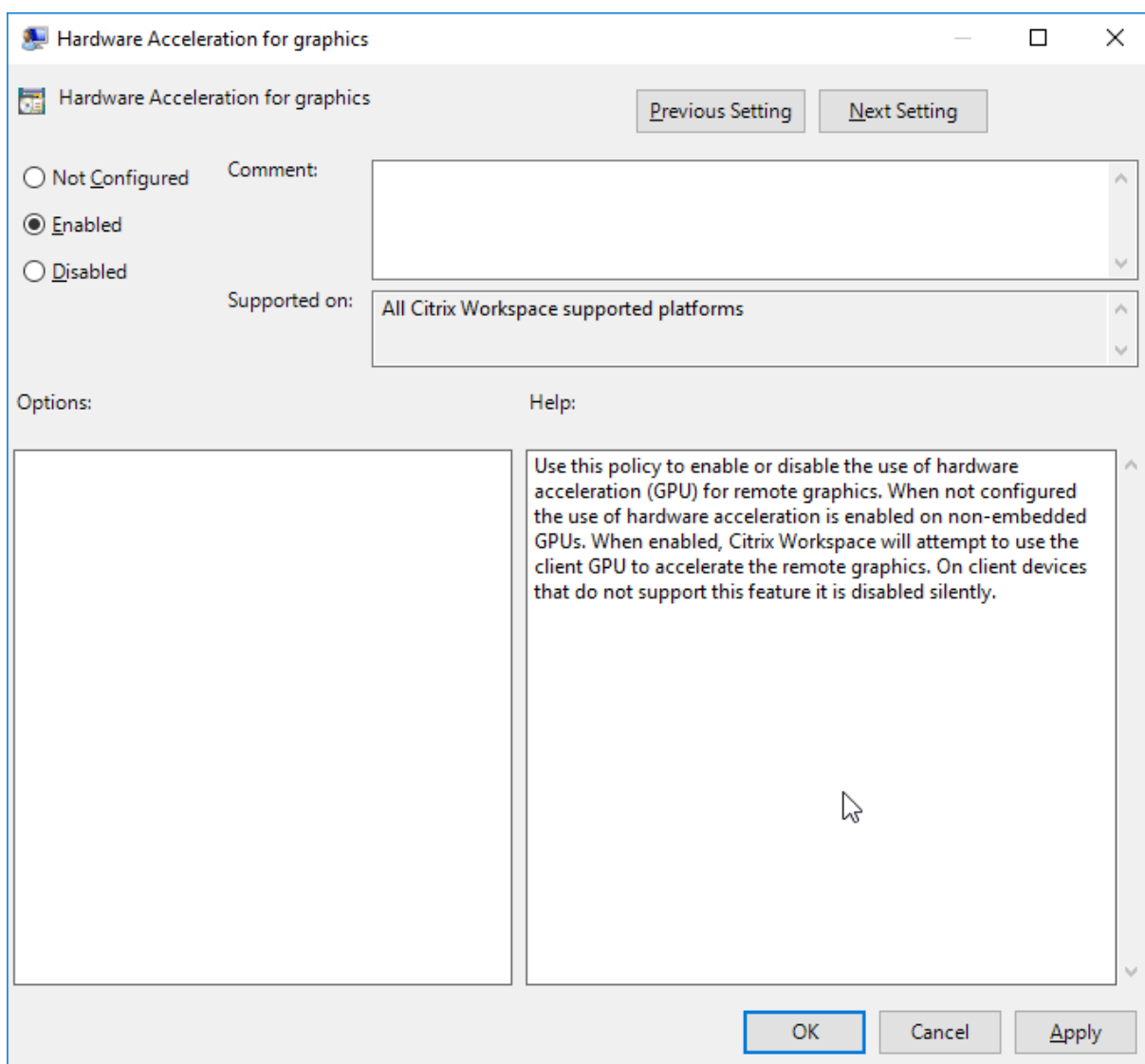
Para calcular los requisitos de memoria gráfica para Citrix Virtual Apps and Desktops y Citrix DaaS, consulte el artículo [CTX115637](#) en Knowledge Center.

#### **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.

## 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 **Distribución del monitor** en Desktop Viewer. Allí, puede dibujar líneas horizontales o verticales para separar la pantalla en monitores virtuales. La pantalla se divide en función de porcentajes especificados en la resolución del monitor cliente.

Puede establecer los PPP en los monitores virtuales que se utilizarán para el escalado de PPP o la correspondencia de PPP. Después de aplicar una distribución de monitores virtuales, cambie el tamaño o vuelva a conectarse a la sesión.

Esta configuración se aplica solo a las sesiones de escritorio de un solo monitor y en pantalla completa, 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

## Escalado de PPP

La aplicación Citrix Workspace cuenta con reconocimiento de PPP y permite la correspondencia de resoluciones de pantalla y el escalado de PPP en el cliente Windows con la sesión de aplicaciones y

escritorios virtuales.

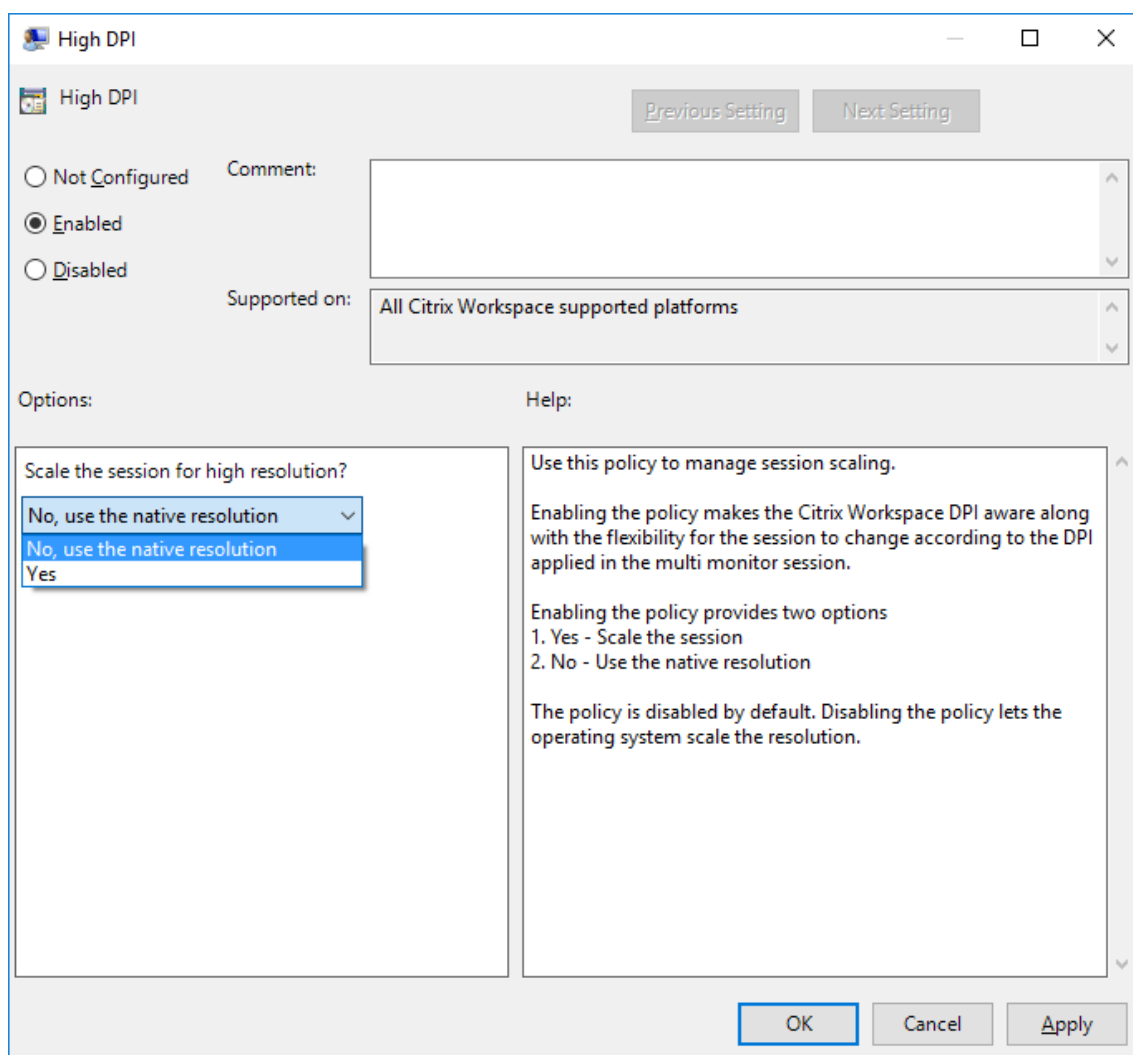
El escalado de PPP se usa principalmente con monitores de gran tamaño y alta resolución para mostrar aplicaciones, texto, imágenes y otros elementos gráficos en un tamaño que se pueda ver cómodamente.

Esta función está habilitada de forma predeterminada y es el parámetro recomendado para todos los casos de uso. Sin embargo, los administradores pueden seguir configurando el escalado de PPP mediante la plantilla administrativa de objeto de directiva de grupo, o GPO, (configuración por máquina), si es necesario.

Para configurar el ajuste de escala de PPP mediante la plantilla administrativa de GPO:

**Para configurar el ajuste de escala de PPP mediante la plantilla administrativa de GPO:**

1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > PPP**.
3. Seleccione la directiva **PPP elevados**.



4. Seleccione una de estas opciones:
  - a) Sí: Se aplican PPP elevados en una sesión.
  - b) No, usar la resolución nativa: El sistema operativo se encarga de configurar la resolución.
5. Haga clic en **Aplicar** y **Aceptar**.
6. Desde la línea de comandos, ejecute el comando `gpupdate /force` para aplicar los cambios.

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

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 **PPP elevado**.
3. Seleccione una de estas opciones:
  - a) **Sí**: Se aplican PPP elevados en una sesión.

- b) **No, usar la resolución nativa:** La aplicación Citrix Workspace detecta los PPP en el VDA y los aplica.
  - c) De forma predeterminada está seleccionada la opción **Dejar que el sistema operativo ajuste la resolución**. Permite a Windows encargarse del escalado de PPP. Esta opción también significa que se inhabilita la directiva PPP elevados.
4. Haga clic en **Guardar**.
  5. Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

NOTA:

**Consideraciones adicionales:**

- La correspondencia de PPP requiere la versión 1912 LTSR de Citrix Virtual Apps and Desktops o una posterior.
- En la mayoría de los casos, se recomienda el parámetro **No, usar la resolución nativa** (correspondencia de PPP).
- El parámetro predeterminado **Dejar que el sistema operativo ajuste la resolución** inhabilita el reconocimiento de PPP en la aplicación Citrix Workspace. Es posible que este modo produzca gráficos borrosos cuando la escala de PPP del cliente Windows se establece en un valor distinto al 100 %. Este modo no admite varios monitores con diferentes escalas de PPP.
- La opción **Sí** hace que la aplicación Citrix Workspace amplíe la escala de la ventana de la sesión para que coincida con la escala de PPP configurada en el cliente Windows. Se trata de una función antigua que se recomienda solo para conexiones a entornos antiguos de XenApp y XenDesktop cuando se requieren escalas de PPP superiores al 100 % en el cliente. Es posible que este modo produzca gráficos borrosos.

Para obtener información sobre la solución de problemas de escalado de PPP, consulte el artículo [CTX230017](#) de Knowledge Center.

### Selección automática del códec de vídeo

La aplicación Citrix Workspace para Windows ahora detecta automáticamente el mejor códec de vídeo que se puede usar. Durante la instalación de la aplicación Citrix Workspace para Windows, se evalúan las capacidades de decodificación del dispositivo de punto final. En función de esta información, la aplicación Citrix Workspace para Windows selecciona el mejor códec para usar con el VDA cuando se inicia la sesión. Este es el orden en el que se evalúan los códecs de vídeo:

1. AV1
2. H.265
3. H.264

Esta función está disponible cuando la directiva **Usar códec de vídeo para compresión** está establecida en una de las siguientes opciones:

- **Usar si se prefiere**
- **Para la pantalla entera**
- **Para áreas en cambio constante**

Para obtener más información sobre la directiva **Usar códec de vídeo para la compresión**, consulte [Usar códec de vídeo para la compresión](#).

La selección automática solo se aplica a las variantes YUV 4:2:0 de estos códecs. YUV 4:2:0 utiliza menos ancho de banda, lo que puede afectar la calidad. Si la configuración de la directiva de **Calidad visual** está establecida en **Gradual sin pérdida** o **Siempre sin pérdida** y si la directiva **Permitir sin pérdida visual** está establecida en **habilitada**, la selección automática del códec de vídeo está inhabilitada y, en su lugar, se utiliza YUV 4:4:4 H.264 o H.265.

Para obtener más información sobre estas directivas, consulte lo siguiente:

- [Calidad visual](#)
- [Permitir compresión sin pérdida visual](#)

**Nota:**

El YUV 4:2:0 es un submuestreo de croma y es una técnica de compresión de color que reduce el consumo total de ancho de banda.

Al conectarse a un recurso, la aplicación Citrix Workspace prueba la capacidad del dispositivo de punto final para decodificar H.265 y AV1 y guardar las capacidades en el registro. Después, la aplicación Citrix Workspace selecciona automáticamente el mejor códec de vídeo para usar y negocia este códec con el VDA. Si tanto el VDA como el cliente pueden usar H.265 y AV1, se selecciona AV1 como códec de vídeo. Si el AV1 no está disponible en el VDA ni en el cliente, se selecciona H.265. Si H.265 tampoco está disponible en ninguno de los dos, la sesión usa H.264 como códec de vídeo.

Esta función está habilitada de manera predeterminada.

Para inhabilitar la selección automática del códec de vídeo, configure **DisableDecoderCaps** de la siguiente manera:

1. Abra el Editor del Registro con `regedit` en el comando Ejecutar.
2. Vaya a `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Policies\Citrix\ICA Client\Graphics Engine`.

O bien:

Vaya a `HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Graphics Engine`

3. Cree una clave DWORD con el nombre **DisableDecoderCaps** y establezca el valor de la clave en 1.

Si el valor de **DisableDecoderCaps** se establece en 1 en HKEY\_LOCAL\_MACHINE o HKEY\_CURRENT\_USER, no se utiliza la selección automática del códec de vídeo.

## 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.

GPU de cliente que ofrece compatibilidad con la decodificación H.265:

- GPU de la generación NVIDIA Pascal o posterior
- GPU Intel de 6.ª generación o posterior
- AMD de la Generación GCN3 o posterior

### Nota:

Esta función tiene más requisitos de VDA, como los siguientes:

- GPU de la generación NVIDIA Maxwell o posterior
- GPU Intel de 6.ª generación o posterior
- GPU de la generación AMD Raven o posterior

Esta función se habilita automáticamente con la introducción de la función **Selección automática del códec de vídeo**.

Este comportamiento se puede cambiar controlando explícitamente la decodificación H.265 con la clave de registro del lado del cliente **EnableH265**.

### 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 con [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 la 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 con `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.
4. Inicie la sesión de nuevo para que los cambios surtan efecto.

La presencia del **EnableH265** inhabilita la detección automática. Si se establece **EnableH265** en 0, se inhabilita la decodificación H.265. Por lo tanto, la sesión no usa el códec de vídeo H.265, aunque esté configurado en el VDA.

Si se establece **EnableH265** en 1, la aplicación Citrix Workspace para Windows intenta utilizar la decodificación H.265. Si la decodificación H.265 falla, el cliente y el servidor vuelven a la codificación H.264.

El uso de H.265 también se puede habilitar configurando la aplicación Citrix Workspace para que utilice la codificación de vídeo H.265 mediante la plantilla administrativa de objetos de directiva de grupo (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 > > Experiencia del usuario**.
3. Seleccione la directiva Decodificación H265 para gráficos.
4. Seleccione **Habilitada**.
5. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
6. 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, la configuración de directiva Decodificación H.265 para gráficos se ignora. En ese caso, la función no se aplica y utiliza de nuevo el códec de vídeo H.264.
- El indicador de estado de gráficos y el monitor Citrix HDX se pueden utilizar para validar el uso del códec de vídeo.

## AV1

La aplicación Citrix Workspace es compatible con el uso del códec de vídeo AV1 para la aceleración de hardware de vídeos y gráficos remotos. El códec de vídeo AV1 debe ser compatible y estar habilitado tanto en el VDA como en la aplicación Citrix Workspace.

### Los requisitos previos para el AV1 son los siguientes:

- VDA 2308 o posterior.
- Aplicación Citrix Workspace para Windows 2305 o posterior
- Habilite la directiva **Usar codificación por hardware para códec de vídeo** en el VDA (de manera predeterminada).
- La aplicación Citrix Workspace para Windows tiene los siguientes requisitos de hardware de cliente para AV1:
  - NVIDIA Ampere o posterior
  - Intel 11.<sup>a</sup> generación/Arc o más reciente
  - AMD Radeon RX 6000/Radeon Pro serie W6000 (RDNA2) o posterior

#### Nota:

AV1 tiene más requisitos de VDA, como los siguientes:

- GPU NVIDIA de la generación Lovelace o posterior (por ejemplo, L4/L40)
- GPU de la generación Intel Arc o posterior

Esta función se habilita automáticamente con la introducción de la función **Selección automática del códec de vídeo**.

Este comportamiento se puede cambiar controlando explícitamente la decodificación de AV1 con la clave de Registro **EnableAV1** del lado del cliente.

### Configuración de la codificación de vídeo AV1 mediante el Editor de Registro:

Habilitar la codificación de vídeo AV1 en una red no unida a un dominio en un sistema operativo de 32 bits:

1. Abra el Editor del Registro con `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 **EnableAV1** y establezca el valor de la clave en 1.
4. Inicie la sesión de nuevo para que los cambios surtan efecto.

Habilitar la codificación de vídeo AV1 en una red no unida a un dominio en un sistema operativo de 64 bits:

1. Abra el Editor del Registro con `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 **EnableAV1** y establezca el valor de la clave en 1.
4. Inicie la sesión de nuevo para que los cambios surtan efecto.

La presencia del **EnableAv1** inhabilita la detección automática. Si se establece **EnableAV1** en 0, se inhabilita la decodificación AV1 y, por lo tanto, la sesión no utiliza el códec de vídeo AV1.

Al establecer **EnableAV1** en 1, la aplicación Citrix Workspace para Windows intenta utilizar la decodificación AV1. Si se produce un error en la decodificación del AV1, el cliente y el servidor vuelven a la codificación H.264.

**Nota:**

Si la directiva Aceleración de hardware para gráficos está inhabilitada en la plantilla administrativa de GPO de la aplicación Citrix Workspace, la configuración de directiva Decodificación AV1 para gráficos se ignora. En ese caso, la función no se aplica y utiliza de nuevo el códec de vídeo H.264.

El indicador de estado de gráficos y el monitor Citrix HDX se pueden utilizar para validar el uso del códec de vídeo.

## Microsoft Teams optimizado

June 14, 2024

### Instalar el plug-in VDI de Microsoft Teams

Puede instalar el plug-in VDI de Microsoft Teams durante la instalación de la aplicación Citrix Workspace mediante una de las siguientes opciones.

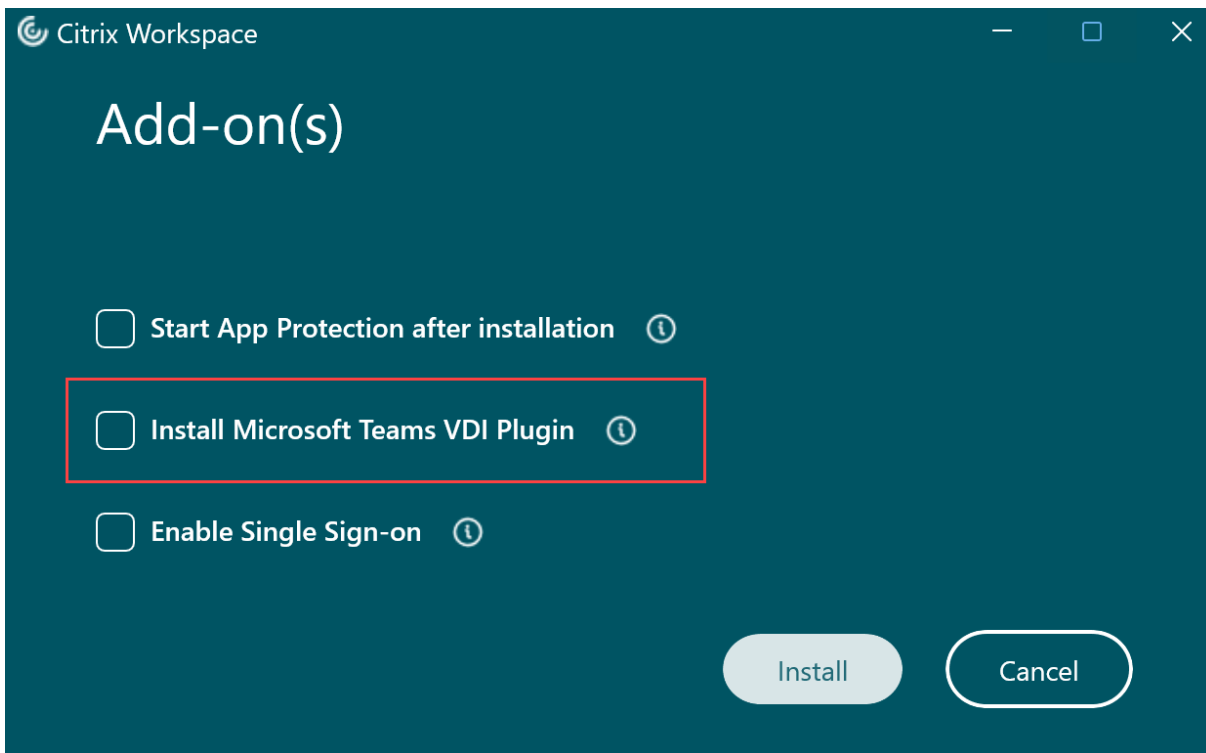
**Nota:**

Para conocer la compatibilidad de las versiones con VDI y los detalles de configuración, consulte [Microsoft Teams 2.1 compatible con VDI/DaaS](#) y [Nuevos requisitos para VDI de Teams](#).

### Uso de la interfaz de usuario

1. En la página de **complementos**, seleccione la casilla **Instalar el plug-in VDI de Microsoft Teams** y después haga clic en **Instalar**.

2. Acepte el acuerdo de usuario que aparece y continúe con la instalación de la aplicación Citrix Workspace.



### Uso de la línea de comandos

Utilice el modificador de línea de comandos `/installMSTeamsPlugin`.

Por ejemplo: `CitrixWorkspaceApp.exe /installMSTeamsPlugin`

### Se agregó una función para reproducir tonos cortos en Microsoft Teams optimizado

Antes, con la función de tono de llamada secundario habilitada, los tonos cortos, como los pitidos o las notificaciones, se reproducían una y otra vez. Por ejemplo, se repetía el tono que se escuchaba cuando se unían invitados a las reuniones de Microsoft Teams. La única alternativa era cerrar y reiniciar Microsoft Teams. Este problema provocaba una mala experiencia para el usuario final.

La aplicación Citrix Workspace permite reproducir los tonos cortos como quiera. Esta función también habilita los tonos de llamada secundarios.

#### Requisitos previos:

Actualice Microsoft Teams a la versión más reciente.

## **Experiencia mejorada para llamadas de videoconferencia en Microsoft Teams optimizado**

De forma predeterminada, la función de transmisión simultánea está habilitada para las llamadas de videoconferencia en Microsoft Teams optimizado. Con esta compatibilidad, la calidad y la experiencia de las videoconferencias en diferentes dispositivos de punto final mejoran al adaptarse a la resolución adecuada para ofrecer la mejor experiencia en llamadas a todos los usuarios.

Con esta experiencia mejorada, es posible que cada usuario cuente con varias transmisiones de vídeo en diferentes resoluciones (por ejemplo, 720p, 360p...) en función de varios factores, como la capacidad del dispositivo de punto final, las condiciones de la red y más. El dispositivo de punto final receptor solicita entonces la resolución de máxima calidad que pueda gestionar, lo que ofrece a todos los usuarios una experiencia de vídeo óptima.

## **Efectos y desenfoque de fondo para la optimización de Microsoft Teams con HDX**

Ahora, la aplicación Citrix Workspace para Windows admite efectos y el desenfoque de fondo en la optimización de Microsoft Teams con HDX.

Puede difuminar o reemplazar el fondo por una imagen personalizada y evitar distracciones inesperadas al ayudar a que la conversación se centre en la silueta (cuerpo y rostro). La función se puede utilizar con llamadas de conferencia o entre dos usuarios.

Puede seleccionar las siguientes opciones para el desenfoque y los efectos del fondo:

- Sin efectos de fondo
- Seleccione el desenfoque de fondo
- Seleccione la imagen de fondo

### **Nota:**

Ahora, esta función está integrada en los botones y la interfaz de usuario de Microsoft Teams. La compatibilidad con varias ventanas es un requisito previo que necesita una actualización de VDA a la versión 2112 o a una posterior. Para obtener más información, consulte Reuniones y chat en modo multiventana.

### **Limitaciones:**

- No está disponible la función de reemplazo de fondo definido por el usuario.
- El efecto de fondo no persiste entre sesiones. Cuando cierra y reinicia Microsoft Teams o el VDA se conecta de nuevo, el efecto de fondo se restablece y se desactiva.
- Cuando la sesión ICA se conecta de nuevo, el efecto está desactivado. Sin embargo, la interfaz de usuario de Microsoft Teams muestra que el efecto anterior sigue activado con una marca de verificación. Citrix y Microsoft están trabajando juntos para resolver este problema.

- El dispositivo debe estar conectado a Internet mientras se reemplaza la imagen de fondo.

**Nota:**

Esta función estará disponible solamente después de la implantación de una futura actualización de Microsoft Teams. Cuando Microsoft implante la actualización, puede consultar [CTX253754](#) y el [Plan de desarrollo público de Microsoft 365](#) para obtener información sobre el anuncio y la actualización de la documentación.

## 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

- La versión de WebRTC que se utiliza para Microsoft Teams optimizado se ha actualizado a la versión M98.
- **Se ha actualizado el modo de seleccionar dispositivos de audio para Microsoft Teams optimizado:** Al cambiar los dispositivos de audio predeterminados en la configuración de sonido del dispositivo de punto final, Microsoft Teams optimizado en la imagen de disco virtual (VDI) de Citrix VDI cambia la selección actual de dispositivos de audio para que coincida con los valores predeterminados del dispositivo de punto final.

1 However, **if** you make an explicit device selection in Microsoft Teams, your selection takes precedence and does not follow the endpoint defaults. Your selection is persistent until you clear the Microsoft Teams cache.

Para obtener información sobre las funciones que formaban parte de las versiones que llegaron al fin de vida, consulte la [documentación antigua](#).

## Transporte HDX

June 14, 2024

### 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.

Así, se obtiene 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 Enlightened Data Transport (EDT) como protocolo de transporte para conexiones ICA. Para obtener más información, consulte la sección [Transporte adaptable](#) en la documentación de Citrix Virtual Apps and Desktops.

### Modo tolerante a pérdidas para audio

La aplicación Citrix Workspace usa la redirección del modo tolerante a pérdidas para audio. Esta función mejora la experiencia del usuario para la transmisión en tiempo real cuando los usuarios se conectan a través de redes con alta latencia y pérdida de paquetes.

Debe usar la versión del VDA 2311 o posterior. De forma predeterminada, esta función está habilitada en la aplicación Citrix Workspace para Windows. Sin embargo, está inhabilitada en el VDA.

Para habilitar el modo tolerante a pérdidas para audio, configure el siguiente valor de registro y reinicie la máquina.

**Para VDA multisesión:**

- Clave: HKEY\_LOCAL\_MACHINE\SOFTWARE\WOW6432Node\Citrix\Audio
- Nombre del valor: EdtUnreliableAllowed
- Tipo de valor: DWORD
- Información del valor: 1

**Para VDA de estaciones de trabajo:**

- Clave: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Audio
- Nombre del valor: EdtUnreliableAllowed
- Tipo de valor: DWORD
- Información del valor: 1

## Redirección de contenido del explorador web

June 14, 2024

Redirigir el contenido del explorador web impide que las páginas web incluidas en la lista de permitidos se generen en el lado del agente VDA. Esta función utiliza la aplicación Citrix Workspace para crear una instancia de motor de generación correspondiente en el lado del cliente, que obtiene el contenido HTTP y HTTPS a partir de la URL.

La redirección de contenido del explorador es compatible con el explorador Google Chrome. La redirección de contenido del explorador web redirige el contenido de un explorador web a un dispositivo cliente, y crea un explorador web correspondiente incrustado en la aplicación Citrix Workspace. Esta función reduce el uso de red, el procesamiento de páginas y los gráficos que aparecen en el dispositivo de punto final. Por tanto, mejora la experiencia del usuario cuando este navega por páginas web con contenido sofisticado, especialmente aquellas páginas web que contienen vídeos HTML5 o WebRTC.

- Las cookies persisten en todas las sesiones: al salir de un explorador y al volver a iniciarlo, no se le pedirá que vuelva a introducir sus credenciales.
- Los exploradores ahora respetan el idioma establecido en el sistema local.

Para obtener más información, consulte [Redirección de contenido del explorador web](#).

**Importante:**

- La redirección de contenido del explorador se puede habilitar para 2402 LTSR mediante la línea de comandos
- Está habilitada de forma predeterminada para todas las versiones actuales de la aplicación Citrix Workspace para Windows.
- La redirección de contenido del explorador no se admite en las versiones LTSR 1912 y 2203.1 de la aplicación Citrix Workspace.

Para habilitar la redirección de contenido del explorador en el VDA, asegúrese de que estén habilitadas las siguientes directivas en Citrix Web Studio:

- [Redirección de contenido del explorador web](#)
- [Configuración de lista ACL para redirección de contenido del explorador web](#)
- [Sitios de autenticación para la Redirección de contenido del explorador web](#)

### **Configurar la ruta para el almacenamiento de datos temporales del explorador web superpuesto de la redirección de contenido del explorador web**

Puede configurar la ruta de almacenamiento temporal de datos para el explorador basado en Chromium Embedded Framework (CEF). Puede configurar la ruta en el VDA o el cliente de esta manera:

**En VDA:**

1. Abra el Editor del Registro con `regedit` en el comando Ejecutar.
2. Vaya a la ruta del Registro `HKEY_LOCAL_MACHINE\Software\Citrix\DXMediaStream\ClientConfigurations\WindowsCef`.
3. Cree la entrada de cadena **BcrProfilePath** y establezca como valor la carpeta para los archivos bcrTmp basados en CEF. Por ejemplo:

```
"BcrProfilePath"="C:\\tmp\\AlternateBcrProfilePath"
```

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

**En el cliente:**

1. Abra el Editor del Registro con `regedit` en el comando Ejecutar.
2. Vaya a la ruta del Registro `HKEY_CURRENT_USER\Software\Citrix\HdxMediaStream`.
3. Cree un valor del Registro con estos atributos:
  - Nombre de la clave del Registro: `BcrProfilePath`

- Valor del Registro: Cadena <folder for CEF based BCRtmp files>

4. Reinicie la aplicación Citrix Workspace para que los cambios surtan efecto.

**Nota:**

La versión de Chromium Embedded Framework (CEF) se actualizó a la 117. Esta nueva versión ayuda a resolver vulnerabilidades de seguridad.

**Limitaciones:**

La redirección de contenido del explorador tiene las siguientes limitaciones:

- No es compatible con aplicaciones web que requieran ventanas emergentes o persistencia de cookies de sesión.
- Microsoft Internet Explorer no es compatible.
- Las aplicaciones que dependen del servicio de autenticación de Google (por ejemplo, Google Meet) están bloqueadas actualmente.
- El plug-in de extensión no está publicado oficialmente en Microsoft Edge en la actualidad. Sin embargo, hay una solución alternativa.
- La directiva de redirección de vídeo HTML5 debe estar inhabilitada cuando se utilice la redirección de contenido del explorador.
- A veces, las sesiones se pueden desconectar debido a redes poco fiables, una latencia en la red muy variable o limitaciones en el alcance de los dispositivos inalámbricos. La redirección de contenido del explorador no cuenta con un mecanismo de reserva o generación de informes suficiente para estos casos.
- Los archivos descargados a través de la superposición se almacenan localmente (en la máquina cliente del usuario final).

**Mejora del rendimiento de BCR**

Antes, BCR utilizaba la caché de espacio en disco del lado del cliente y la información almacenada en caché no se eliminaba durante una actualización de versión. Este parámetro tuvo como resultado un mayor uso del espacio en disco a lo largo del tiempo y un comportamiento incoherente al redireccionar una página mediante BCR.

Para resolver este problema, BCR usa una caché en memoria. Esta mejora ayuda a mejorar el rendimiento del BCR.

Esta función está inhabilitada de forma predeterminada. Puede habilitar esta función en el VDA o en el cliente de esta manera:

**En VDA:**

1. Abra el Editor del Registro con [regedit](#) en el comando Ejecutar.



2. Vaya a la ruta del Registro `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HDXMediaStream\ClientConfigurations\WindowsCef`.
3. Cree una clave `DWORD` con el nombre `BCRStoreCEFCacheInMemory` y establezca el valor de la clave en 1.

Si el valor de `BCRStoreCEFCacheInMemory` se establece en 0, BCR utiliza el espacio en disco del cliente.

#### **En el cliente:**

1. Abra el Editor del Registro con `regedit` en el comando Ejecutar.
2. Vaya a la ruta del Registro `HKEY_CURRENT_USER\Software\Citrix\HDXMediaStream`.
3. Cree una clave `DWORD` con el nombre `BCRStoreCEFCacheInMemory` y establezca el valor de la clave en 1.

Si el valor de `BCRStoreCEFCacheInMemory` se establece en 0, BCR utiliza el espacio en disco del cliente.

#### **Nota:**

- Si `BCRStoreCEFCacheInMemory` se establece tanto en el cliente como en el VDA, los parámetros del cliente tiene prioridad.
- Si tanto `BCRStoreCEFCacheInMemory` como `BCRProfilePath` ya están establecidos, la configuración de `BCRProfilePath` tiene prioridad y se hace caso omiso de la configuración de `BCRStoreCEFCacheInMemory`.

#### **Limitación:**

El límite de tamaño de la caché en memoria está establecido en 10 MB.

## **Redirección bidireccional de contenido**

June 14, 2024

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

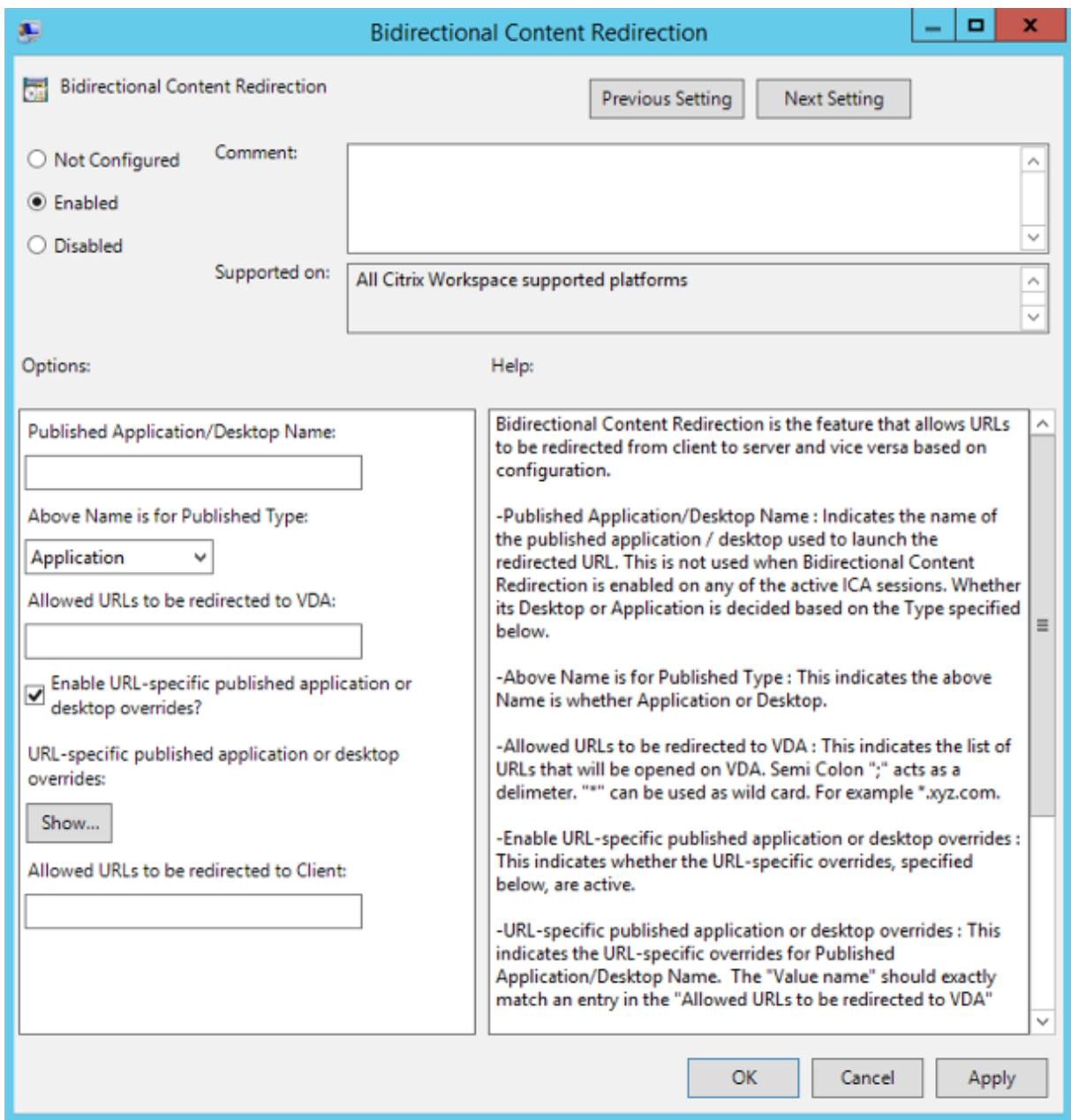
**Nota:**

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

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

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

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



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

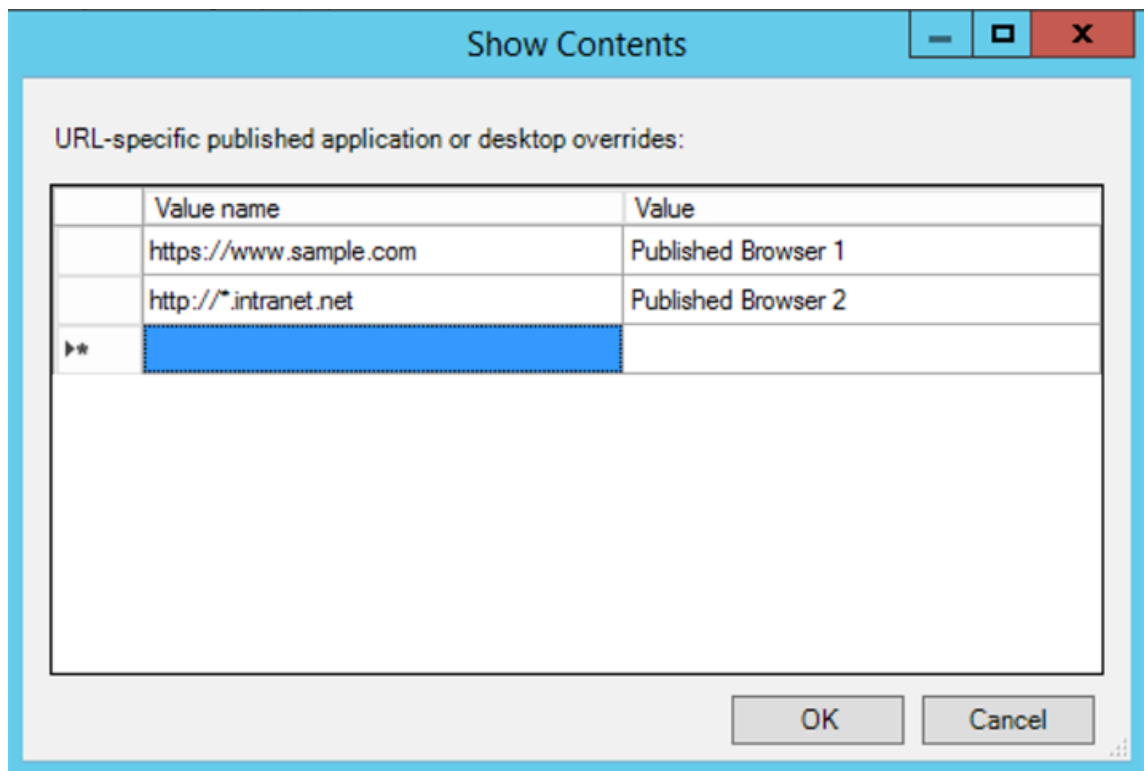
**Nota:**

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` en el cliente de la aplicación Citrix Workspace y 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.
- En Internet Explorer, haga clic en **Configuración > Opciones de Internet > Avanzado** y marque la casilla **Habilitar extensiones de explorador de terceros** en la sección **Exploración**.

**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, ignórela:

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

**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\...

## Referencia para parámetros ICA

June 14, 2024

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 \(descarga en PDF\)](#)

## Dispositivos

April 22, 2024

En esta sección se describe lo siguiente:

- [Puntero](#)
- [Teclado](#)
- [Impresión](#)
- [USB](#)
- [Asignación de unidades de cliente](#)
- [Micrófono](#)

## Puntero

June 14, 2024

### 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.

## Teclado

June 14, 2024

### Accesos directos de teclado

Se pueden configurar combinaciones de teclas para que la aplicación Citrix Workspace las interprete como una funcionalidad especial. Cuando se habilita la directiva Accesos directos de teclado, 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.

### 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 las aplicaciones suscritas desde el menú Inicio o mediante accesos directos del escritorio, conocido 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 apare-

cer 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 10 no permite la creación de carpetas anidadas dentro del menú Inicio. Las aplicaciones pueden mostrarse en la carpeta raíz, pero no dentro de subcarpetas de categorías 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. Cuando la clave `AutoReInstallModifiedApps` está inhabilitada, los atributos de las aplicaciones y el escritorio no se actualizan. Además, los accesos directos no se restauran al actualizar si se eliminan en el 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

### 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.

### 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
4 - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

## 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.

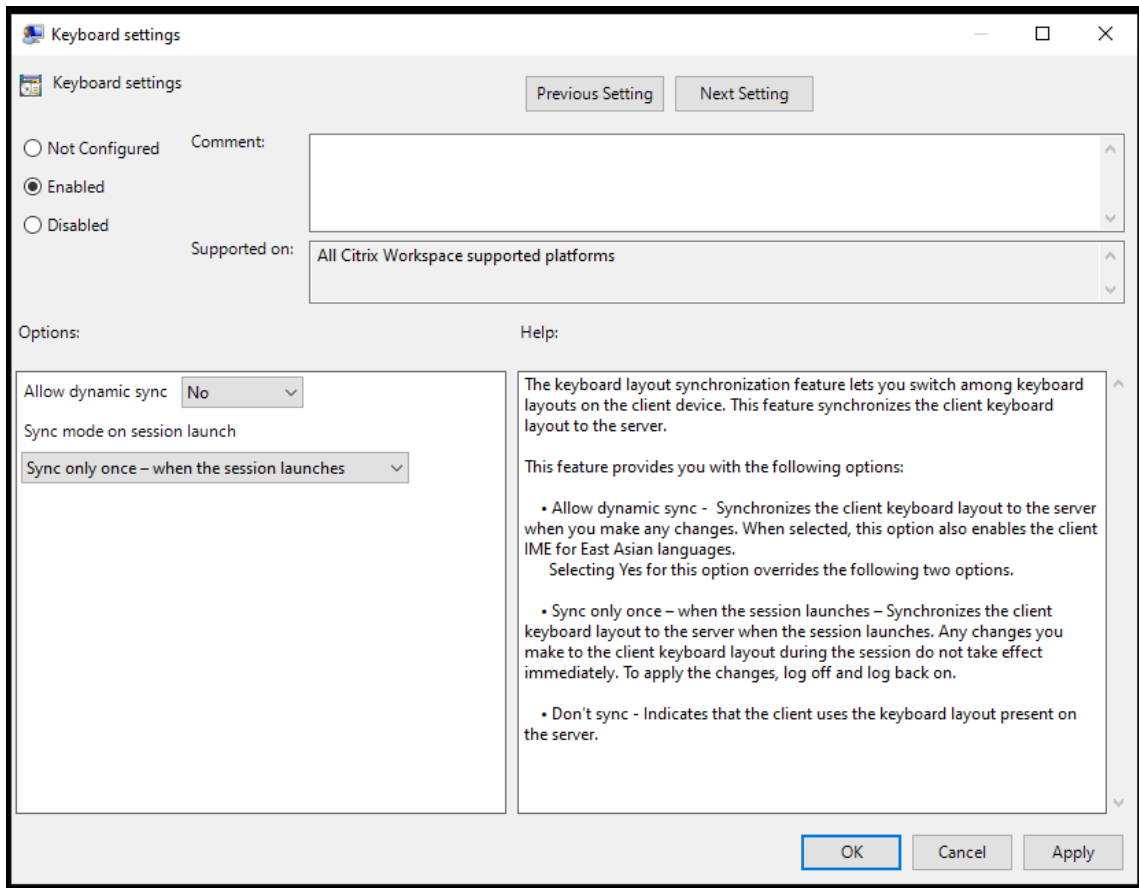
### Para configurar la sincronización de la distribución del teclado mediante la plantilla administrativa de GPO:

**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.

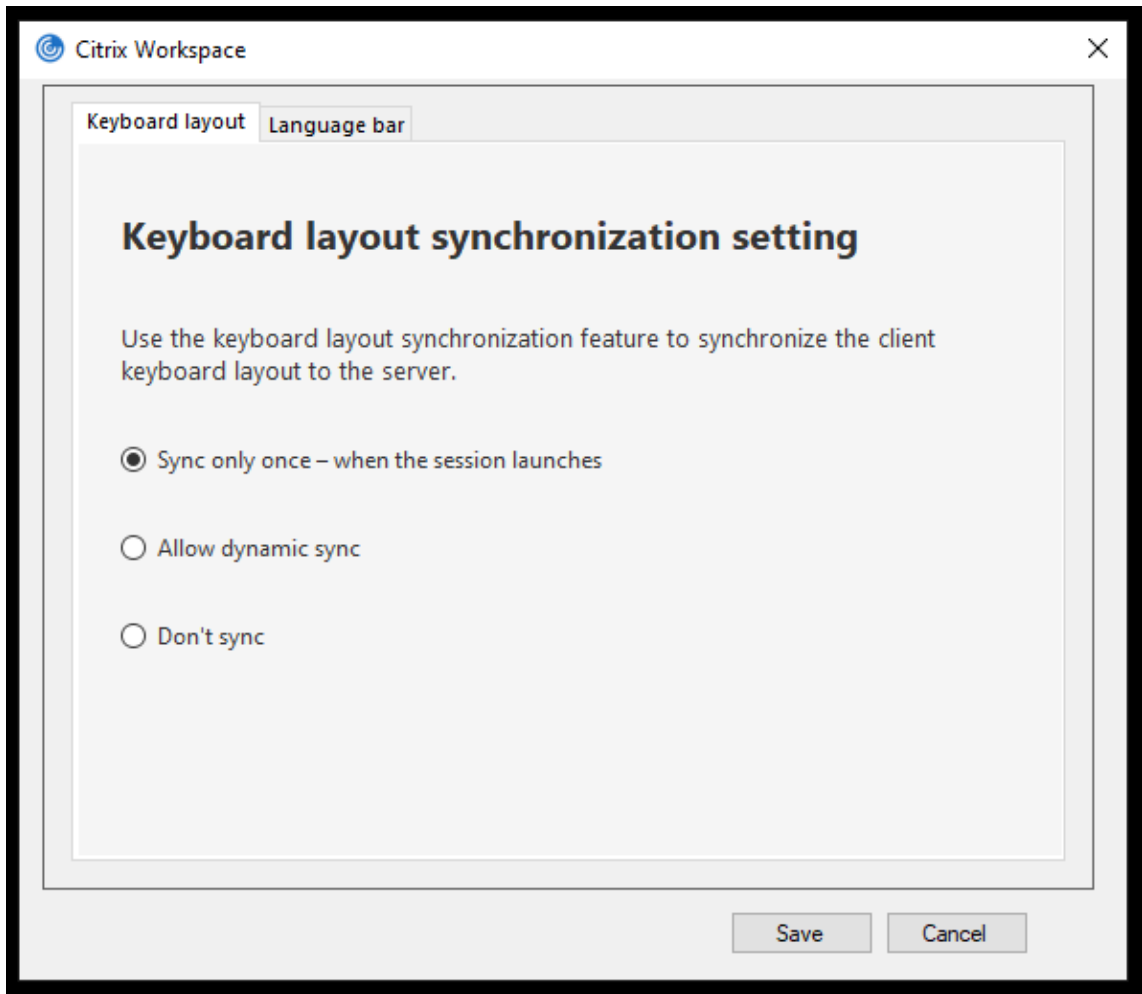
- **Modo de sincronización al iniciar la sesión:** En el menú desplegable, seleccione una de estas opciones:
  - **Sincronizar solo una vez: cuando se inicia la sesión:** Sincroniza la distribución del teclado del cliente con la del servidor cuando se inicia la sesión. Los cambios que haga en la distribución 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 de la distribución del teclado mediante la interfaz de línea de comandos** Se presentan estos comandos para configurar la sincronización de la distribución del teclado mediante la interfaz de línea de comandos:

---

Comandos	Descripción
<code>wfica32.exe /kbsyncmode:once</code>	Establece el modo de sincronización del teclado en “Sincronizar solo una vez”.
<code>wfica32.exe /kbsyncmode:dynamic</code>	Establece el modo de sincronización del teclado en “Sincronización dinámica”.
<code>wfica32.exe /kbsyncmode:no</code>	Establece el modo de sincronización del teclado en “No sincronizar”.

---

Ejecute los comandos anteriores 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:\Archivos de programa (x86)\Citrix\ICA Client`.

### Configurar la sincronización del teclado en Windows VDA

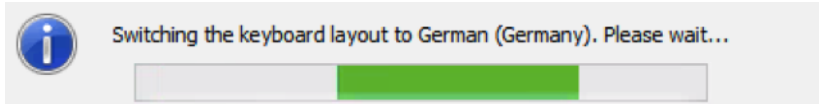
**Nota:**

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:

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Citrix\LanguageBar"-v "SyncKeyboardLayout"-d "0x00000001"
```

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 la distribución del teclado en el cliente se cambia por una distribución no admitida 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:

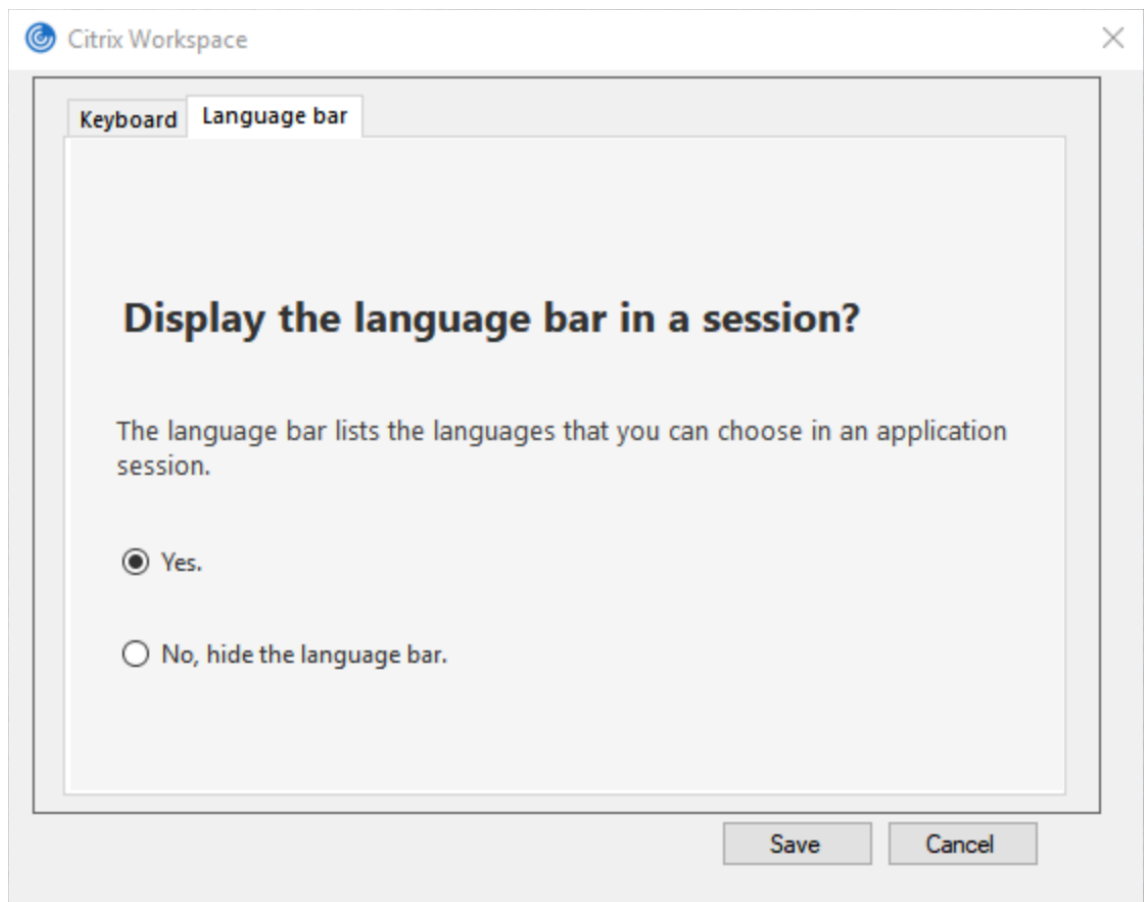
- Sí: indica que se muestra la barra de idioma en una sesión de aplicación.
- No, ocultar la barra de idioma: Indica que la barra de idioma se oculta en la sesión de una aplicación.

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: indica que se muestra la barra de idiomas 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”.

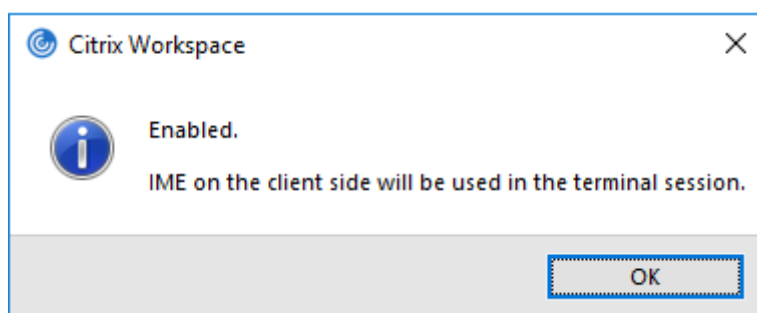
**Editores IME de cliente genérico**

**Nota:**

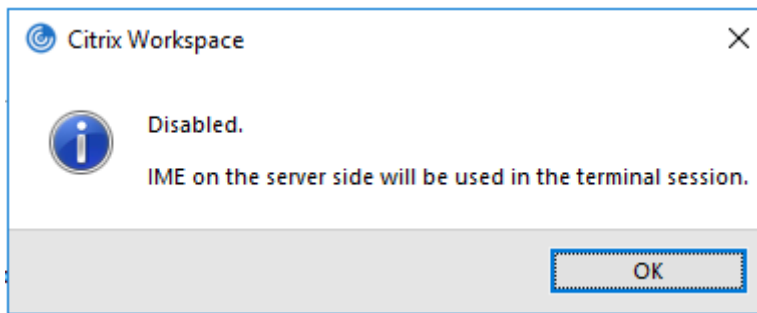
Si utiliza un sistema operativo Windows 10, versión 2004, es posible que tenga problemas técnicos al usar la función IME en una sesión. Esos problemas son el resultado de una limitación de terceros. Para obtener más información, consulte el [artículo de asistencia de Microsoft](#).

**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`.



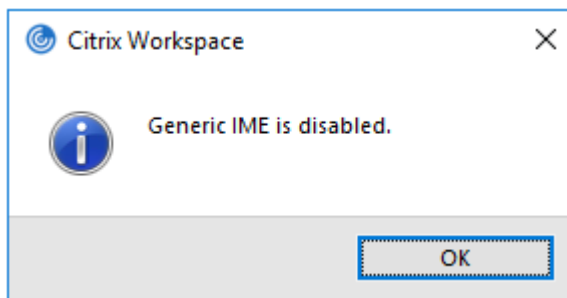
- Para inhabilitar el IME de cliente genérico, ejecute el comando `wfica32.exe /localime:off` desde la carpeta de instalación de la aplicación Citrix Workspace `C:\Program Files (x86)\Citrix\ICA Client`.



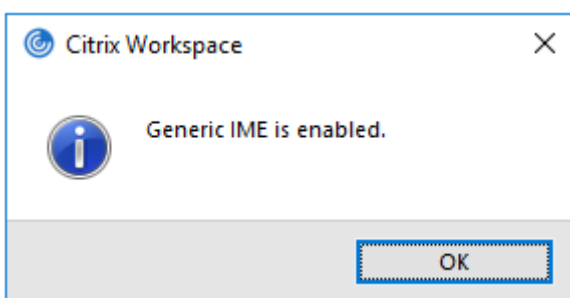
**Nota:**

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 de teclado.



Si ha inhabilitado el IME de cliente genérico desde la interfaz de línea de comandos, puede habilitar la función de nuevo mediante el comando `wfica32.exe /localgenericime:on`.



**Activar/desactivar:**

La aplicación Citrix Workspace admite la activación o desactivación de esta función. Ejecute `wfica32.exe /localgenericime:on` para habilitarla o inhabilitarla. Sin embargo, los parámetros de sincronización de distribución de teclado tienen prioridad sobre este comando modificador. Si el parámetro de sincronización de la distribución del teclado se ha establecido en **Desactivada**, activar la alternancia no habilita el IME de cliente genérico.



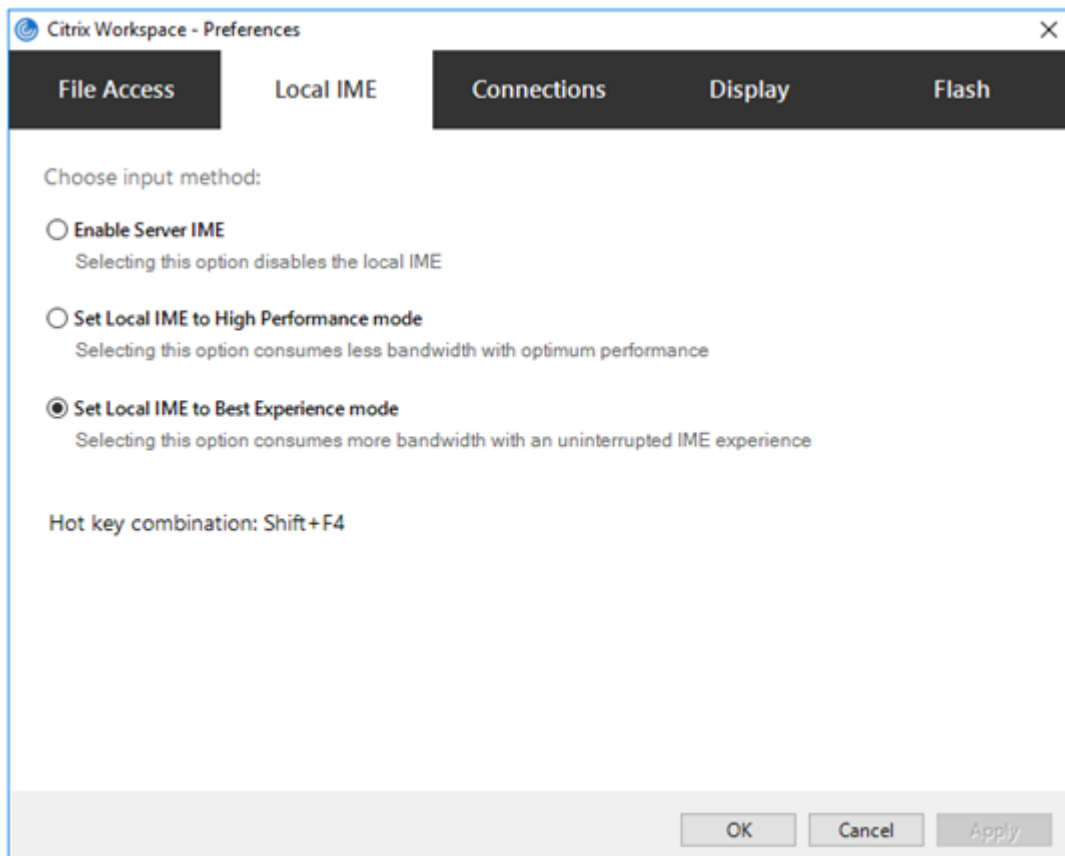
### Configurar el IME de cliente genérico mediante la interfaz gráfica de usuario:

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 **Mayús+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 acceso directo.



#### **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**.

## Sincronice varios teclados al inicio de la sesión

Antes, solo el teclado activo del cliente se sincronizaba con el VDA una vez iniciada la sesión en modo de pantalla completa. En este caso, si configuró **Sincronizar solo una vez - cuando se inicia la sesión** en la aplicación Citrix Workspace y tuvo que cambiar a un teclado diferente, debe instalar manualmente el teclado en el escritorio remoto. Del mismo modo, si configuró **Permitir sincronización dinámica** en la aplicación Citrix Workspace, debe pasar al modo de ventana, cambiar el teclado del cliente y, a continuación, volver al modo de pantalla completa.

Todos los teclados disponibles en el cliente se sincronizan con el VDA una vez que se inicia la sesión en modo de pantalla completa. Puede seleccionar el teclado necesario de la lista de teclados instalados o disponibles en el cliente una vez que se inicie la sesión en modo de pantalla completa.

La función **Sincronizar varios teclados al iniciar la sesión** está habilitada de forma predeterminada en el VDA y está inhabilitada de forma predeterminada en la aplicación Citrix Workspace.

### Requisitos previos

#### En la aplicación Citrix Workspace para Windows:

Habilite el parámetro de distribución del teclado **Sincronización solo una vez, cuando se inicie la sesión**. Para obtener más información, consulte la documentación sobre la [Distribución del teclado](#).

#### En VDA:

Habilite las siguientes directivas de VDA:

- Asignación de distribución de teclado Unicode. Para obtener más información, consulte [Habilitar la asignación de distribución de teclado Unicode](#) o [Editor de métodos de entrada \(IME\) y teclado](#)
- Sincronización de la distribución del teclado del cliente y mejora de IME. Para obtener más información, consulte [Editor de métodos de entrada \(IME\) y teclado](#)

#### Configuración de la aplicación Citrix Workspace:

Esta función solo se aplica a los escritorios virtuales. Esta función está inhabilitada de forma predeterminada. Para habilitar esta función, lleve a cabo lo siguiente:

1. Vaya a la sección [Virtual Channels\Keyboard] del archivo **All\_Regions.ini**.
2. Agregue una clave de Registro booleana `SyncKbdLayoutList to HKEY_CURRENT_USER\SOFTWARE\Citrix\Ica Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard`.
3. Establezca el valor en 1.

### Configuración de VDA:

La función **Sincronizar varios teclados al inicio de la sesión** está habilitada de forma predeterminada en el VDA.

Para inhabilitar esta función, actualice el registro del VDA de la siguiente manera:

1. Abra el Editor del Registro y vaya a `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`.
2. Cree la entrada DWORD `DisableKbdLayoutList` y establezca su valor en 0. Al establecer el valor en 1, se inhabilita la función **Sincronizar varios teclados al inicio de la sesión**.
3. Inicie la sesión de nuevo para que los cambios surtan efecto.

## Impresión

June 14, 2024

### 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\LOCAL_MACHINE\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

## 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:

- Citrix Virtual Apps and Desktops 7 1808 o una versión más reciente.
- Debe haber instalado al menos un visor de PDF en el equipo.

### Para habilitar la impresión de documentos PDF:

1. En el Delivery Controller, use Citrix Studio para seleccionar el nodo **Directiva** en el panel de la izquierda. Puede crear una directiva o modificar una existente.
2. Establezca la directiva **Crear automáticamente la impresora universal de PDF** en Habilitada.

Reinicie la sesión de la aplicación Citrix Workspace para que los cambios surtan efecto.

### Limitación:

- El explorador Microsoft Edge no admite la visualización ni la impresión de documentos PDF.

## Modo de tableta expandida en Windows 10 cuando se usa Windows Continuum

Windows Continuum es una función de Windows 10 que se adapta al uso que se le da al dispositivo cliente. La aplicación Citrix Workspace para Windows 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.

## USB

June 14, 2024

### 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.

### **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 las aplicaciones virtuales, ya que estos dispositivos no están disponibles para la comunicación remota en aplicaciones virtuales 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 transfer-



encia 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 las aplicaciones virtuales, ya que estos dispositivos no están disponibles para la comunicación remota en aplicaciones virtuales 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, conversores 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 Citrix Workspace para Windows mediante la directiva 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.

### **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 una experiencia con HDX optimizado, al tiempo que permite el reenvío y la disposición de los dispositivos necesarios a 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)

---

Parámetro de filtro	Descripción
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 la interfaz de administración, 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.

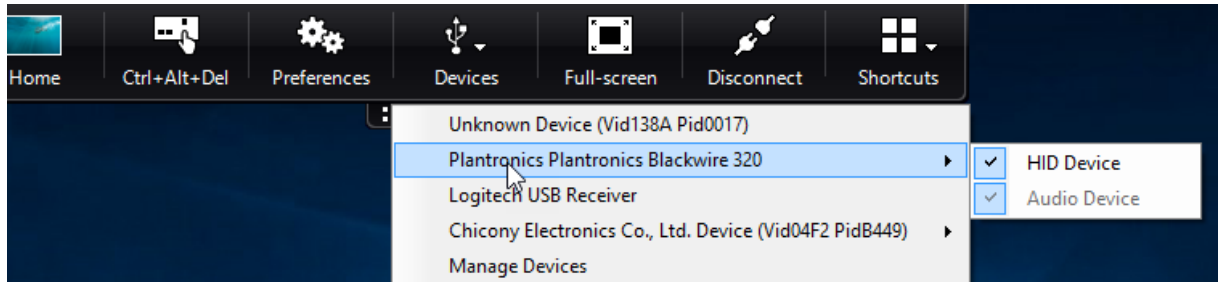
Para habilitar la directiva de reglas de dispositivo para la aplicación Citrix Workspace para Windows:

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:

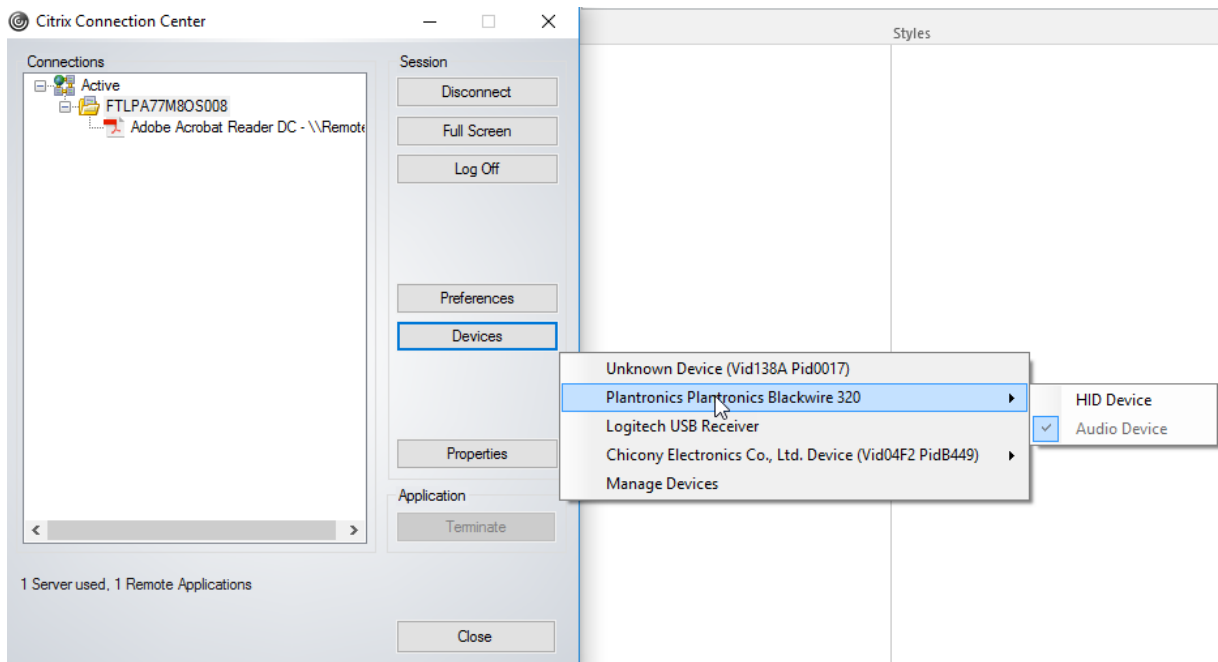
En una sesión de escritorio, los dispositivos USB divididos se muestran en Desktop Viewer, en **Dispositivos**. Además, los dispositivos USB divididos se pueden ver también en **Preferencias > Dispositivos**.



#### 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.

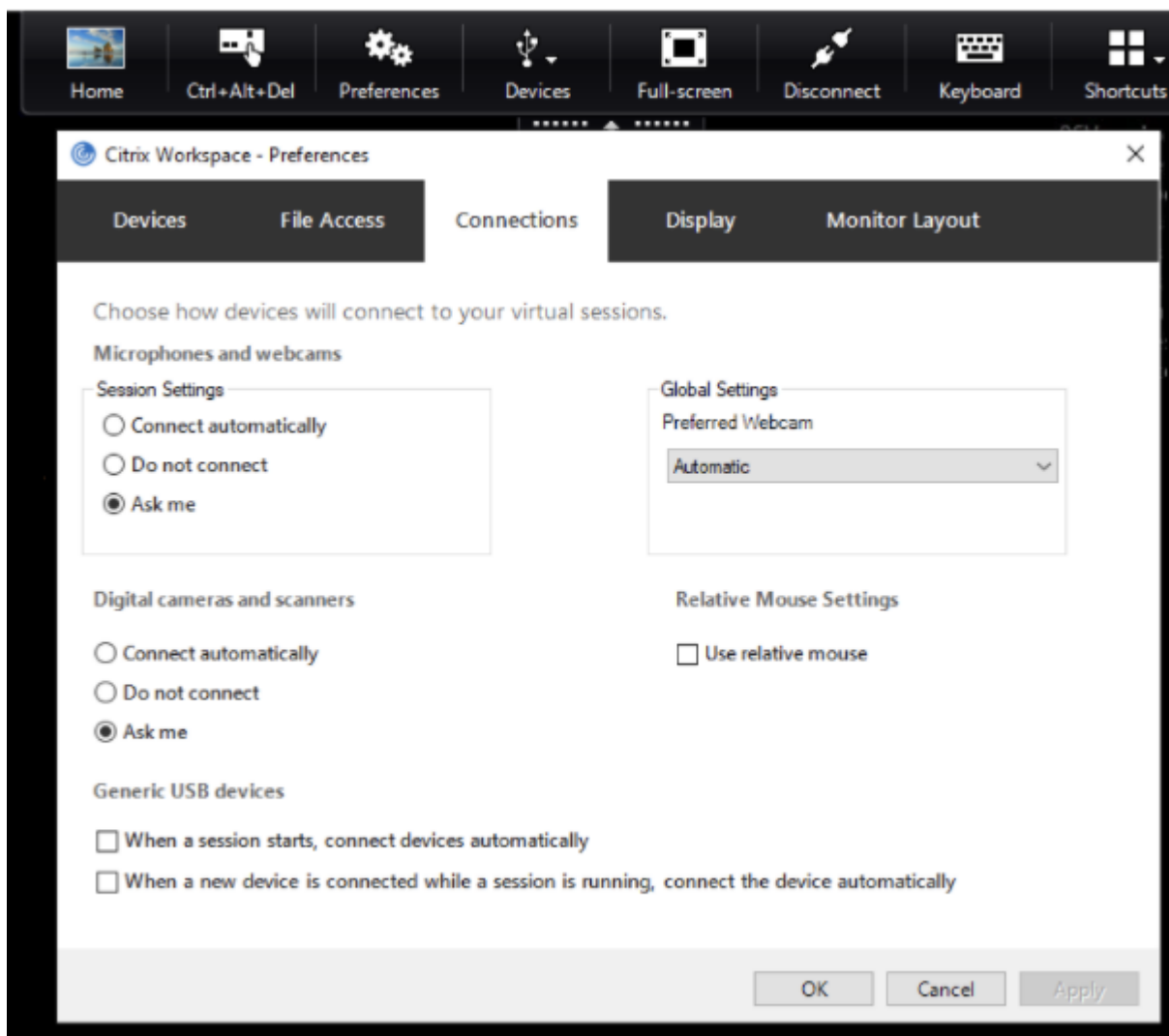
1. Abra la plantilla administrativa de GPO de la aplicación Citrix Workspace; para ello, ejecute gpedit.msc.
2. En el nodo **Configuración del usuario**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Workspace > Uso remoto de dispositivos cliente > Uso remoto de USB genérico**.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

Si no, un administrador puede supeditar las preferencias de usuario mediante la implementación de 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.
- A veces, es posible que los dispositivos compuestos USB no se dividan automáticamente aunque se haya establecido una regla de redireccionamiento de dispositivos correcta para dividir el dispositivo. Este problema se produce porque el dispositivo está en modo de bajo consumo. En estos casos, es posible que el dispositivo secundario que entra en el modo de bajo consumo no esté presente en la lista de dispositivos. Puede utilizar una de las siguientes soluciones temporales para solucionar este problema:
  - Desconecte la sesión, inserte el dispositivo USB y vuelva a conectarse a la sesión.
  - Desenchufe el dispositivo USB y vuelva a conectarlo. Esta acción hace que el dispositivo salga del modo de bajo consumo. [HDX-34143]

**Teclados Bloomberg**

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

Los teclados Bloomberg ofrecen otra funcionalidad en comparación con 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:**

A partir de la versión 2109 de la aplicación Citrix Workspace para Windows, 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.

#### **Nota:**

Con la introducción de la versión 2 de las reglas de redirección de dispositivos en Studio, en Citrix Virtual Apps and Desktops, no es necesario configurar el teclado Bloomberg 5 mediante directivas de grupo del lado del cliente en la aplicación Citrix Workspace para Windows. Para obtener más detalles, consulte [Reglas de redirección de dispositivos USB del cliente \(versión 2\)](#) en la documentación de Citrix Virtual Apps and Desktops.

Para las versiones anteriores a la versión 2212 de la aplicación Citrix Workspace para Windows, en este ejemplo se muestra cómo utilizar 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:**

Las líneas nuevas o el punto y coma se pueden utilizar para separar reglas, lo que 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, a continuación, 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 la siguiente clave en el Registro:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
2. Lleve a cabo una de las siguientes acciones:
  - Para habilitar esta función, configure una entrada de tipo DWORD y el nombre **Enable-BloombergHID** con el valor 1.
  - Para inhabilitar esta función, establezca el valor en 0.

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. De todos modos, puede 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 tal caso, 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 aparece y no se puede usar en 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.

**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.

## 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:`

## 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

Función	Asignación de unidades del cliente	Compatibilidad con USB
Configuración para acceso de solo lectura	Sí	No
Dispositivo para quitar con seguridad durante una sesión	No	Sí, si un usuario hace clic en Quitar hardware con seguridad en el área de notificaciones

Si 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.

## Asignación de unidades de cliente

June 14, 2024

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

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.

## Micrófono

June 14, 2024

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 y Citrix DaaS para inhabilitar sus micrófonos y cámaras web.

## Directiva de grupo

June 14, 2024

### 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 de usuario

Puede utilizar los archivos de plantilla `receiver.admx` o `receiver.adml` con directivas de dominio y de equipos locales. Para las directivas de dominio, importe el archivo de plantilla mediante la Consola de administración de directivas de grupo. 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 utilizan con la versión de Windows mencionada en la [Tabla de compatibilidad](#).

Si la aplicación Citrix Workspace se instala con el VDA, los archivos ADMX/ADML suelen encontrarse en el directorio `<installation directory>\Online Plugin\Configuration`.

Si la aplicación Citrix Workspace se instala sin el VDA, los archivos ADMX/ADML suelen encontrarse en el siguiente directorio.

- Para 64 bits: `C:\Program Files (x86)\Citrix\ICA Client\Configuration directory`
- Para 32 bits: `C:\Program Files\Citrix\ICA Client\Configuration directory`

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

Tipo de archivo	Ubicación de archivos
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]



Tipo de archivo	Copiar de	Copiar a
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**.

## Experiencia en las sesiones

June 14, 2024

### 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: Habilita el preinicio a petición (el preinicio comienza después de autenticar las credenciales del usuario).

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

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.

## 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.

## 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)

## Experiencia mejorada al reconectar aplicaciones y escritorios virtuales

La versión 2302 de Citrix Workspace ofrece una experiencia de usuario mejorada al volver a conectarse a las aplicaciones y escritorios virtuales de los que se había desconectado.

Cuando la aplicación Citrix Workspace intenta actualizar la aplicación Citrix Workspace desconectada o iniciar nuevas aplicaciones o escritorios virtuales como parte de la funcionalidad de control del espacio de trabajo, aparece el siguiente mensaje:

### Restore session?

You have one or more apps/desktops running from the previous session in Citrix Workspace app. Would you like to restore them?

Remember my preference



Este mensaje solo aparece cuando la opción para **mostrar la solicitud de reconexión para volver a conectar las sesiones** se establece en “true” en Global App Configuration Service.

Haga clic en **Restaurar** para volver a conectarse y abrir las aplicaciones y escritorios virtuales nuevos y desconectados. Si solo quiere iniciar las aplicaciones y escritorios recién seleccionados, haga clic en **Cancelar**.

También puede seleccionar la opción **Recordar mi preferencia** para aplicar la preferencia seleccionada al siguiente inicio de sesión.

El mensaje **¿Restaurar sesión?** anterior aparecerá solo si:

- el usuario intenta iniciar una aplicación perteneciente a un almacén del espacio de trabajo;
- las directivas administrativas o los parámetros de configuración de la aplicación no están configurados para la funcionalidad de control del espacio de trabajo;

- Las opciones de reconexión de control del espacio de trabajo están configuradas de forma predeterminada en el cliente.

**Nota:**

La configuración de reconexión de **Opciones de reconexión** tiene prioridad sobre las preferencias establecidas en el cuadro de diálogo. Para obtener más información, consulte [Configurar opciones de reconexión mediante el cuadro de diálogo Preferencias avanzadas](#).

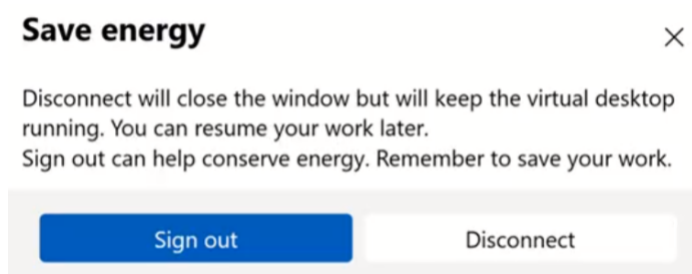
## Iniciativa de sostenibilidad de la aplicación Citrix Workspace

### Para inicio nativo

Cuando esta función está habilitada, se muestra un mensaje para cerrar sesión en la sesión de escritorio cuando un usuario cierra un escritorio virtual. Es posible que esta función ayude a ahorrar energía si hay directivas de sistema operativo Windows que se usen para apagar máquinas virtuales cuando estas no tengan usuarios conectados.

Para habilitar esta función, lleve a cabo lo siguiente:

1. Vaya a Citrix Studio.
2. Haga clic en **Grupos de entrega**, en el panel de navegación de la izquierda.
3. Seleccione el VDA requerido en la sección **Grupo de entrega**.
4. Haga clic en el icono **Modificar**. Aparece la página **Modificar grupo de entrega**.
5. Haga clic en **Escritorios**, en el panel de navegación de la izquierda.
6. Seleccione el VDA requerido donde debe agregar las palabras clave.
7. Haga clic en **Edit**. Aparece la página **Modificar escritorio**.
8. Defina la palabra clave `LogoffOnClose` como **true** en el campo **Descripción**.
9. Haga clic en **Aceptar**. Al cerrar el escritorio virtual, aparece este cuadro de diálogo:



**Personalizar el texto en la pantalla de ahorro de energía** También puede personalizar el texto en la pantalla **Ahorra energía**.

1. Siga los pasos 1-8 de la sección anterior.
2. Defina la palabra clave `PromptMessage` con el texto necesario en el campo **Descripción**.

**Ejemplo:**

```
1 KEYWORDS:LogoffOnClose=true PromptMessage="Do you want to Log off?"  
  "  
2 <!--NeedCopy-->
```

**Edit Desktop**

Display name:

Description:  
  
The name and description are shown in Citrix Workspace app.

Restrict launches to machines with tag:

Allow everyone with access to this delivery group to use a desktop

Restrict desktop use:  

Allow list ?

You have not yet added any users or groups.

Enable desktop  
Clear this check box to disable delivery of this desktop.

Session roaming  
When enabled, if the user launches this desktop and then moves to another device, the same session is used, and applications are available on both devices. When disabled, the session no longer roams between devices.

Las palabras clave se asignan de forma predeterminada a los nuevos equipos de escritorio asignados al grupo. Para los equipos de escritorio existentes, debe ejecutar los siguientes coman-



dos de PowerShell para que se apliquen los cambios:

```
1 $dg = Get-BrokerDesktopGroup -Name '<group name>' -Property 'Name'  
   , 'UId'  
2  
3 $apr = @( Get-BrokerAssignmentPolicyRule -DesktopGroupUId $dg.UId  
   -Property 'Description' )  
4  
5 Get-BrokerMachine -DesktopGroupUId $dg.UId -IsAssigned $true | Set  
   -BrokerMachine -Description $apr[0].Description  
6 <!--NeedCopy-->
```

Con este script de PowerShell, es posible tener varias reglas de directiva de asignación para un único grupo de entrega. Con Citrix Studio, también puede configurar varias reglas de directiva de asignación, cada una con un valor de descripción único y un posible conjunto de palabras clave diferentes.

3. Haga clic en **Aceptar**. Al cerrar el escritorio virtual, aparece este cuadro de diálogo.



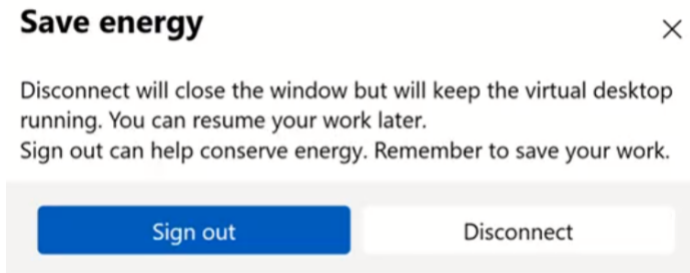
### Para inicio de nube híbrida

Desde la versión 2402 de la aplicación Citrix Workspace, esta función está disponible para inicios híbridos en la nube. Una vez que esta función está habilitada, se muestra un mensaje para cerrar sesión en la sesión de escritorio cuando un usuario cierra un escritorio virtual. Esta función ayuda a ahorrar energía si hay directivas de sistema operativo Windows que se usen para apagar máquinas virtuales cuando estas no tengan usuarios conectados.

Para habilitar esta función, lleve a cabo lo siguiente:

1. Vaya a Citrix Studio.
2. Haga clic en **Grupos de entrega**, en el panel de navegación de la izquierda.
3. Seleccione el VDA requerido en la sección **Grupo de entrega**.
4. Haga clic en el icono **Modificar**. Aparece la página **Modificar grupo de entrega**.
5. Haga clic en **Escritorios**, en el panel de navegación de la izquierda.
6. Seleccione el VDA requerido donde debe agregar las palabras clave.
7. Haga clic en **Edit**. Aparece la página **Modificar escritorio**.
8. Defina la palabra clave `ICA-LogOffOnClose` como **true** en el campo **Descripción**.

9. Haga clic en **Aceptar**. Al cerrar el escritorio virtual, aparece este cuadro de diálogo:



**Personalizar el texto de la pantalla de ahorro de energía** También puede personalizar el texto que se muestra en la pantalla de **ahorro de energía**.

1. Siga los pasos 1-8 de la sección anterior.
2. Defina la palabra clave `ICA-PromptMessage` con el texto necesario en el campo **Descripción**.

**Nota:**

La cantidad máxima de caracteres permitida en el campo Descripción es de 200.

**Ejemplo:**

```
1 KEYWORDS:ICA-LogOffOnClose=true ICA-PromptMessage="Do you want to  
Log off?"  
2 <!--NeedCopy-->
```

## Edit Desktop

Display name:

Description:  
  
The name and description are shown in Citrix Workspace app.

Restrict launches to machines with tag:

Allow everyone with access to this delivery group to use a desktop

Restrict desktop use:

Allow list <span>?</span> ↓
CWAWINAD\Domain Users
TestVeda(CWAWINAD\TestVeda)

**Enable desktop**  
Clear this check box to disable delivery of this desktop.

**Session roaming**  
When enabled, if the user launches this desktop and then moves to another device, the same session is used, and applications are available on both devices. When disabled, the session no longer roams between devices.

Las palabras clave se asignan de forma predeterminada a los nuevos equipos de escritorio asignados al grupo. Para los equipos de escritorio existentes, debe ejecutar los siguientes comandos de PowerShell para que se apliquen los cambios:

```
1 $dg = Get-BrokerDesktopGroup -Name '<group name>' -Property 'Name'  
    , 'Uid'  
2  
3 $apr = @( Get-BrokerAssignmentPolicyRule -DesktopGroupUid $dg.Uid  
    -Property 'Description' )  
4  
5 Get-BrokerMachine -DesktopGroupUid $dg.Uid -IsAssigned $true | Set  
    -BrokerMachine -Description $apr[0].Description  
6 <!--NeedCopy-->
```

Con este script de PowerShell, es posible tener varias reglas de directiva de asignación para un único grupo de entrega. Con Citrix Studio, también puede configurar varias reglas de directiva de asignación, cada una con un valor de descripción único y un posible conjunto de palabras clave diferentes.

3. Haga clic en **Aceptar**. Al cerrar el escritorio virtual, aparece este cuadro de diálogo.



## Desktop Lock de la aplicación Citrix Workspace

June 14, 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.

**Nota:**

Al utilizar la aplicación Citrix Workspace para Windows con Desktop Lock, el usuario inicia sesión en el primer escritorio que está ordenado alfabéticamente con el nombre de todos los escritorios disponibles para el usuario. Actualmente, no existe la opción de elegir de forma selectiva en qué escritorio debe iniciar sesión el usuario. Además, esta función solo es compatible con escritorios y no con aplicaciones.

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 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.
- Se crea un perfil de usuario local en el dispositivo final cuando el usuario inicia sesión en el sistema. El perfil se conserva en el dispositivo final incluso cuando el usuario cierra sesión y se basa en las configuraciones de la administración de perfiles.

**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/
4 <!--NeedCopy--> discovery;on;Desktop Store"
```

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 detal-

lada 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.

## Quitar 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 14, 2024

### 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.

La versión más reciente de la [Declaración de identidad de certificado para Citrix Workspace para Windows](#) es la versión **2212**.

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:

- Inicio 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.

La versión más reciente de [Virtual Channel SDK para Windows](#) es la versión **2302**.

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.

La versión más reciente de la [API de Fast Connect para Citrix Workspace para Windows](#) es la versión **2212**.

Para obtener más información, consulte la documentación [Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows](#).

## Scripts para implementar Citrix Workspace para Windows

Estos son scripts de ejemplo para implementar y configurar la aplicación Citrix Workspace.

La versión más reciente de los [scripts para implementar Citrix Workspace para Windows](#) es la versión **2212**.

## Storebrowse

June 14, 2024

### Nota:

Este artículo solo se aplica a las implementaciones locales de Citrix Workspace. Para las implementaciones de la nube, consulte la documentación de [Storebrowse para Workspace](#).

**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 Server 2022

Windows Server 2016

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](#).
- **HTTP básica:** Este método lo utilizan portales web e integraciones de clientes de terceros, donde se usa una interfaz de usuario externa para capturar un nombre de usuario y una contraseña aptos para el dominio. StoreFront utiliza la función de autenticación básica de IIS para transportar las credenciales al servidor de StoreFront. A continuación, StoreFront utiliza los [Servicios de dominio](#) o la [autenticación de XML Broker Service](#) para validar las credenciales y obtener la información del grupo. Para obtener información sobre cómo habilitar la autenticación HTTP básica, consulte [HTTP básica](#) en la documentación sobre [Administrar métodos de autenticación](#).
- **Directivas avanzadas de NetScaler para Storebrowse:** la aplicación Citrix Workspace para Windows admite directivas avanzadas en NetScaler Gateway con Storebrowse. El protocolo de autenticación admitido es la autenticación LDAP.

### Nota:

El protocolo de autenticación nFactor no es compatible con Storebrowse en Windows.

La utilidad **Storebrowse** permite la autenticación de todas 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**. Este método es aplicable cuando el usuario proporciona las credenciales mediante los comandos de **Storebrowse**.
- Utilice el [Authmanager](#) que se incluye en la aplicación Citrix Workspace para Windows. Puede utilizar este método cuando utilice la autenticación PassThrough de dominio. Para obtener más información, consulte la documentación de [Autenticación PassThrough de dominio](#).

## Iniciar una aplicación o un escritorio publicado

Ahora puede iniciar un recurso directamente desde el almacén, sin tener que usar ningún archivo ICA.

### Nota:

No puede abrir aplicaciones SaaS ni [contenido publicado](#) mediante comandos de Storebrowse.

## Uso de comandos

En la siguiente sección se ofrece información detallada sobre los comandos que se pueden usar desde la utilidad **Storebrowse**.

### Agregar un almacén

`-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>
```



## Ayuda

/?

### Descripción:

Ofrece información detallada sobre el uso de la utilidad **Storebrowse**.

### Enumerar almacenes

(-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
```

### Enumerar

(-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>
```

### Inicio rápido

-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>
```

## Inicio

-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>
```

## Inicio de sesiones

-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>
```

### Carpeta de archivos

`-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 }
```

### Autenticación del seguimiento

`-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 }
```

## Eliminar un almacén

`-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
```

## Seguimiento del estado de los comandos de Storebrowse

Puede realizar un seguimiento del estado de ejecución de comandos de Storebrowse en un archivo. Para realizar un seguimiento del estado de operación correcta, proporcione un nombre de archivo único con el comando `-f launch`. Este comando genera un archivo con el nombre proporcionado. El estado de operación fallida está presente en el archivo `ica.error`, que se crea automáticamente.

### Nota:

Asegúrese de agregar una `.ica` extensión al nombre del archivo con el comando `-f launch`. De lo contrario, el archivo no se generará.

Los archivos para realizar un seguimiento tanto de las operaciones correctas como de las erróneas están presentes en `%LOCALAPPDATA%\citrix\selfservice\cache`, y puede supervisarlos según sea necesario.

Esta mejora está habilitada de forma predeterminada.

A continuación, se muestra un ejemplo de cómo utilizar el comando de inicio con la opción `-f`:

```
1 -launch -f <uniqueFileName.ica> "launchcommandline"
2 For example:
3 SelfService.exe storebrowse -launch -f uniqueFileName.ica -s store0-5
   c3ec017 -CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-
   e33d0695df39.Notepad -ica "https://cwawiniwstest.cloudburrito.com/
   Citrix/Store/resources/v2/
   YTLh0GUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkbZjM5Lk5vdGVwYWQ-/launch/
   ica" -cmdline
4
5 <!--NeedCopy-->
```

## **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.
- Esta función es compatible a partir de la versión 2107.

## Storebrowse para Workspace

June 17, 2024

La aplicación Citrix Workspace para Windows permite usar **Storebrowse** en la implementación local y de autoservicio de la aplicación Citrix Workspace. También permite a los usuarios de **Storebrowse** acceder a las funciones de Cloud y Workspace.

**Nota:**

- Este artículo solo se aplica a las implementaciones de la nube de Citrix Workspace. Para las implementaciones locales, consulte la documentación de [Storebrowse](#).
- Esta función garantiza compatibilidad con **Storebrowse** solamente con Single Sign-On.
- Los requisitos previos mencionados en [Requisitos y compatibilidad del sistema](#) deben estar disponibles para usar esta función.
- No puede abrir aplicaciones SaaS ni [contenido publicado](#) mediante comandos de Storebrowse.

### Uso de comandos

En la siguiente sección se ofrece información detallada sobre los comandos que se pueden usar desde la utilidad **Storebrowse**.

**Nota:**

- Esta función también admite otros comandos del plug-in de autoservicio, como se menciona en [CTX200337](#).
  - Puede ejecutar estos comandos en el símbolo del sistema.
- **-a "discoveryurl":** Agrega un almacén a través de la línea de comandos. Este comando no muestra el mensaje de autenticación cuando SSO está habilitado. Por ejemplo, los dominios de AAD se unen a dispositivos donde la autenticación se realiza a través de la vista web. En los demás dispositivos, aparece el mensaje de autenticación.
    - Ejemplo:`SelfService.exe storebrowse -a "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`
  - **-d "discoveryurl":** Elimina el almacén.
    - Ejemplo:`SelfService.exe storebrowse -d "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`
  - **-e "discoveryurl":** Exporta los detalles del recurso en formato JSON. Este comando almacena el archivo resource.json en la ubicación predeterminada `%LOCALAPPDATA%\citrix\selfservice`. La aplicación Citrix Workspace debe estar activa para ejecutar este comando y el usuario debe haber iniciado sesión.
    - Ejemplo:`SelfService.exe storebrowse -e "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`
- También puede especificar su propia ruta si no quiere almacenar el archivo resource.json en la ubicación predeterminada.
- Ejemplo: `.\SelfService.exe storebrowse -e "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"C:\Users\. Esto almacena el archivo resource.json en C:\Users\.`
- **-q "FriendlyName""discoveryurl":** Utilice este comando para ejecutar rápidamente el recurso especificado.
    - Ejemplo:`SelfService.exe storebrowse -q "Excel 2016""https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`
  - **-launch "launchcommandline":** Inicio de recursos mediante "launchcommandline" desde resource.json.



**Nota:**

- Copie la línea "launchcommandline" de resource.json.
- Quite / de la línea "launchcommandline" especificada en el archivo resource.json antes de ejecutar el comando.

- Ejemplo:`SelfService.exe storebrowse -launch -s store0-5c3ec017-CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-e33d0695df39 .Notepad -ica "https://cwawiniwstest.cloudburrito.com/Citrix/Store/resources/v2/YTlh0GUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkJm5Lk5-/launch/ica"-cmdline`

Después de ejecutar `-launch "launchcommandline"`, el archivo ICA se almacenará en el directorio `%LOCALAPPDATA%\citrix\selfservice\cache`. Haga doble clic en el archivo ICA para iniciar el recurso.

- `-liststore`: Enumera los almacenes que se agregan dentro de SSP. Es una lista de almacenes que incluye storeID y la URL de detección de cada almacén.
  - Ejemplo:`SelfService.exe storebrowse -liststore`

**Nota:**

La aplicación Citrix Workspace debe estar activa para ejecutar el comando `-liststore`.

El comando `Selfservice.exe storebrowse -liststore` almacena el archivo `store-details.json` en `AppData\Local\Citrix\SelfService`.

## Solucionar problemas técnicos

June 14, 2024

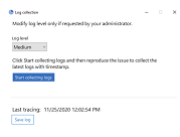
### Recopilación de registros

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. Esta función está disponible a partir de la versión 2012 y posteriores de la aplicación Citrix Workspace para Windows.

Puede recopilar registros mediante la interfaz gráfica de usuario.

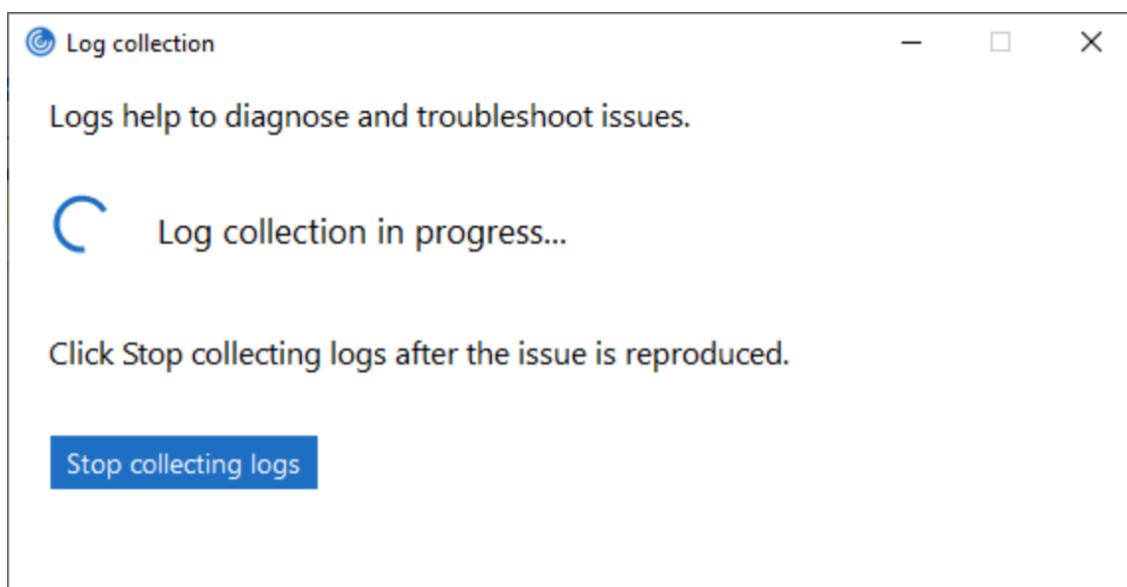
### Recopilación de registros:

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.

## Datos recopilados a través de registros

### Hardware

- Información de monitores adjuntos

- Información de memoria
- Adaptadores de red
- Procesador
- Información de diagnóstico de DirectX

### **Software**

- Versión de la aplicación Citrix Workspace
- Información del sistema operativo (versión, Service Pack y arquitectura)
- Versión de Internet Explorer
- Explorador web predeterminado
- Versión de Flash ActiveX
- Versión de Flash NPAPI

### **Registro**

- HKEY\_LOCAL\_MACHINE\Software\Citrix\AuthManager
- HKEY\_LOCAL\_MACHINE\Software\Citrix\CitrixCAB
- HKEY\_LOCAL\_MACHINE\Software\Citrix\Dazzle
- HKEY\_LOCAL\_MACHINE\Software\Citrix\ICA Client
- HKEY\_LOCAL\_MACHINE\Software\Citrix\Install
- HKEY\_LOCAL\_MACHINE\Software\Citrix\InstallDetect
- HKEY\_LOCAL\_MACHINE\Software\Citrix\PluginPackages
- HKEY\_LOCAL\_MACHINE\Software\Citrix\Receiver
- HKEY\_LOCAL\_MACHINE\Software\Citrix\ReceiverInside
- HKEY\_LOCAL\_MACHINE\Software\Citrix\XenDesktop
- HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains
- HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\NetworkProvider\Order
- HKEY\_CURRENT\_USER\Software\Citrix\AuthManager
- HKEY\_CURRENT\_USER\Software\Citrix\CitrixCAB
- HKEY\_CURRENT\_USER\Software\Citrix\Dazzle
- HKEY\_CURRENT\_USER\Software\Citrix\ICA Client
- HKEY\_CURRENT\_USER\Software\Citrix\Install
- HKEY\_CURRENT\_USER\Software\Citrix\InstallDetect
- HKEY\_CURRENT\_USER\Software\Citrix\PluginPackages
- HKEY\_CURRENT\_USER\Software\Citrix\Receiver
- HKEY\_CURRENT\_USER\Software\Citrix\ReceiverInside
- HKEY\_CURRENT\_USER\Software\Citrix\XenDesktop

- HKEY\_CURRENT\_USER\Software\Policies\Citrix
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\VisualEffects
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
- HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains

### **Registros de eventos**

- Registro de eventos de aplicación
- Registro de eventos del sistema

### **Seguimiento**

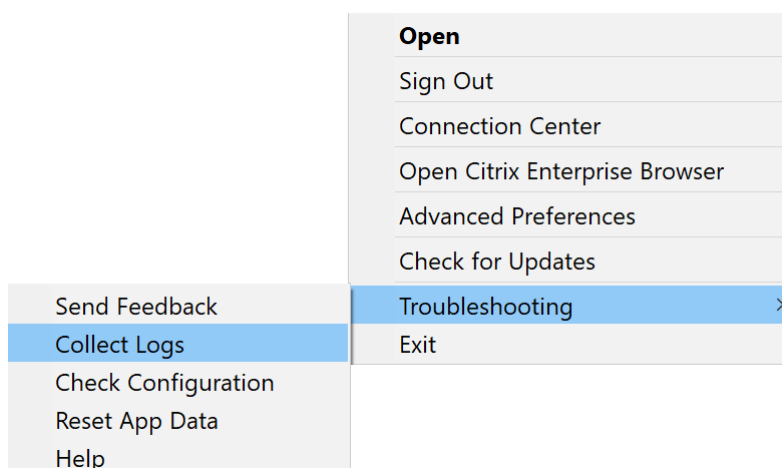
- HDX
- Shell de Receiver, Auth Manager y Self-service Plug-in
- Instalar registros
- Registros Always-On

### **Incorporación de la opción Solución de problemas en la bandeja del sistema de la aplicación Citrix Workspace**

Presentamos la opción **Solución de problemas** para mejorar la experiencia del usuario y proceder fácilmente a la solución de problemas. Puede hacer clic con el botón secundario en el icono de la aplicación Citrix Workspace de la bandeja del sistema que se encuentra en la esquina inferior derecha de la pantalla y, a continuación, seleccionar **Solución de problemas** para acceder a ella.

Las opciones disponibles en Solución de problemas son:

- Enviar comentarios
- Recopilar registros
- Comprobar configuración
- Restablecer datos de la aplicación
- Ayuda



### Enviar comentarios sobre la aplicación Citrix Workspace

La opción **Enviar comentarios** le permite informar a Citrix de cualquier problema que pueda surgir al usar la aplicación Citrix Workspace. También puede enviar sugerencias para ayudarnos a mejorar su experiencia en la aplicación Citrix Workspace.

Para enviar comentarios, siga estos pasos:

1. Haga clic con el botón secundario en el icono de la aplicación Citrix Workspace, en el área de notificaciones, y seleccione **Solución de problemas > Enviar comentarios**. Aparecerá la pantalla **Enviar comentarios**.

Send Feedback

**Title\***

Example: Unable to launch desktop/application

**Tell us more\***

Include details such as:

- What results you expected
- What results you got
- Steps to recreate the issue

**i** The log file and attachment file size must not exceed 20 MB

**Logs**

We recommend you to click "Capture my issue" to capture detailed logs.

Capture my issue

**Attachments**

For example, screenshots or screen recordings of the issue.

Choose file No file chosen

Your feedback will be used to improve Citrix Workspace app. [Learn more](#)

Send Cancel

2. Indique el **título** del problema.
3. Agregue los detalles del problema en el campo **Cuéntenos más**.
4. Haga clic en **Capturar mi problema**. Aparecerá la pantalla **Recopilación de registros**.

Log collection

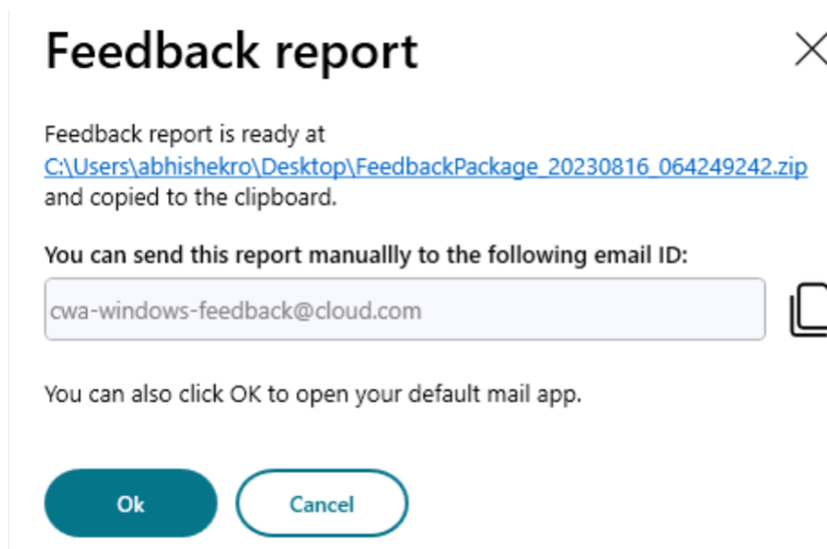
Log level

Medium

Click "Start collecting logs" and then reproduce the issue to collect the latest logs or click "Collect existing logs" if you are not able to reproduce the issue.

Start collecting logs Collect Existing Logs

- a) Haga clic en **Comenzar a recopilar registros** y reproduzca el problema para recopilar los registros más recientes.
  - b) Haga clic en **Dejar de recopilar registros** una vez reproducido el problema.  
O bien:  
Haga clic en **Recopilar registros existentes** si no puede reproducir el problema.
  - c) Haga clic en **Dejar de recopilar registros** una vez reproducido el problema.
5. Asegúrese de que los archivos de registros se muestren junto a **Capturar mi problema**.
  6. Haga clic en **Elegir archivo** y agregue los archivos adjuntos que describan sus problemas, como capturas de pantalla o grabaciones de pantalla. El tamaño máximo permitido para todos los archivos adjuntos, incluido el archivo de registros, es de 20 MB.
  7. Haga clic en **Enviar**. Aparecerá la pantalla **Informe de comentarios**.



El archivo ZIP contiene los archivos de registros, la descripción del problema como archivos de prueba y los archivos adjuntos.

8. Puede enviar el informe de comentarios a Citrix de estas maneras:
  - Haga clic en **Aceptar** para usar la aplicación de correo predeterminada de su sistema.

O bien:

- Envíe el informe manualmente al ID de la dirección de correo electrónico proporcionada.

**Nota:**

Asegúrese de que el archivo ZIP esté adjunto en el correo electrónico.

## Elementos retirados

June 14, 2024

Los anuncios de este artículo le avisan con antelación de las plataformas, los productos Citrix y las funciones que se están retirando progresivamente. Con estos anuncios, puede tomar decisiones comerciales oportunas.

Citrix analiza el uso que hacen los clientes de una función que está por retirar y los comentarios que tengan sobre la eliminación de la función para determinar cuándo retirarla. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas.

Los elementos retirados no se quitan inmediatamente. Citrix sigue dándoles asistencia en esta versión, pero en el futuro se retirarán.

### Tabla de elementos retirados

Elemento	Retirada anunciada en	Eliminado en	Alternativa
Servicios XenApp (también conocidos como PNAgent)	2402	2402	En la aplicación Workspace, conéctese a los almacenes con la URL de almacén en lugar de la URL de los servicios XenApp
Redirección de contenido del explorador basada en Internet Explorer	2311.1	2311.1	Redirección de contenido del explorador basada en Google Chrome
Compatibilidad con el formato SDP de WebRTC (Plan B)	2309		Actualice la aplicación Citrix Workspace a una versión compatible.



Elemento	Retirada anunciada en	Eliminado en	Alternativa
Compatibilidad con el modo de ventana única en la optimización de Microsoft Teams	2309		Actualice la aplicación Citrix Workspace a una versión que admita el modo multiventana. Para obtener más información, consulte <a href="#">Tabla de funciones y compatibilidad de versiones</a> .
Modificador / <code>includeappprotection</code>	2212	2212	Use / <code>startappprotection</code> para iniciar el componente App Protection
Compatibilidad con direcciones URL personalizadas a través de redirecciones 301	2210		Migración de URL de StoreFront a Workspace
Compatibilidad con Windows 8.1 y Windows Server 2012 R2	2204.1	2204.1	Utilice el sistema operativo compatible tal y como se indica en la sección <a href="#">Requisitos del sistema</a> .
Citrix Casting se instala de forma predeterminada con la aplicación Citrix Workspace	2112.1	2205	Citrix Casting se puede instalar a la carta con la aplicación Citrix Workspace. <b>Nota:</b> Citrix Casting no se instala de forma predeterminada durante la aplicación Citrix Workspace.
La opción <b>Todas las cuentas</b> en el menú para almacenes de Workspace (nube) solamente.	2112.1	2202	

Elemento	Retirada anunciada en	Eliminado en	Alternativa
La opción <b>Recordar mi contraseña</b> en la pantalla de inicio de sesión en los almacenes (en la nube) de la aplicación Workspace.	2008	2008	
Citrix Receiver para UWP (Plataforma universal de Windows)	2006	2102	
La opción para agregar o quitar la descripción de almacenes en el cuadro de diálogo <b>Agregar o quitar cuentas</b> . Se ha retirado la columna <b>Descripción</b> .	2006.1		Puede agregar o quitar detalles de la cuenta de almacén sin agregar ninguna descripción.
La opción para habilitar o inhabilitar almacenes en el cuadro de diálogo <b>Agregar o quitar cuentas</b>	2006.1		
Compatibilidad con Windows 7	2002	2006.1	Utilice el sistema operativo compatible tal y como se indica en la sección <a href="#">Requisitos del sistema</a> . <b>NOTA</b> Windows 7 es compatible con la versión 2002. Use el modificador <code>/forceinstall</code> en lugar de <code>/rcu</code> .
Modificador de instalador <code>/rcu</code>	1909		

---

Elemento	Retirada anunciada en	Eliminado en	Alternativa
Instalación bajo demanda de Citrix Casting con la aplicación Citrix Workspace	2112.1	2402	Usar una versión anterior de la aplicación Citrix Workspace

---



© 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).