



# Citrix Receiver para Windows 4.12

## Contents

<b>Novedades</b>	<b>3</b>
<b>Problemas resueltos</b>	<b>4</b>
<b>Problemas conocidos</b>	<b>7</b>
<b>Avisos de terceros</b>	<b>8</b>
<b>Requisitos del sistema y compatibilidad</b>	<b>8</b>
<b>Conexiones, certificados y autenticación</b>	<b>10</b>
<b>Instalar</b>	<b>13</b>
<b>Configurar e instalar mediante parámetros de línea de comandos</b>	<b>16</b>
<b>Implementar mediante System Center Configuration Manager 2012 R2</b>	<b>36</b>
<b>Implementar Citrix Receiver para Windows desde una pantalla de inicio de sesión de la Interfaz Web</b>	<b>40</b>
<b>Instalar y desinstalar manualmente Citrix Receiver para Windows</b>	<b>41</b>
<b>Implementar mediante Active Directory y scripts de inicio de ejemplo</b>	<b>43</b>
<b>Implementar Citrix Receiver para Windows desde Receiver para Web</b>	<b>46</b>
<b>Configurar</b>	<b>46</b>
<b>Configurar la entrega de aplicaciones</b>	<b>47</b>
<b>Configurar StoreFront</b>	<b>60</b>
<b>Configurar características y funciones</b>	<b>66</b>
<b>Configurar el transporte adaptable</b>	<b>67</b>
<b>Configurar la compatibilidad con USB</b>	<b>69</b>
<b>Configurar la redirección de dispositivos USB compuestos</b>	<b>76</b>
<b>Ocultar la hoja de Preferencias avanzadas</b>	<b>78</b>
<b>Configurar teclados Bloomberg</b>	<b>80</b>

<b>Configurar la redirección de contenido bidireccional</b>	<b>82</b>
<b>Proporcionar información de cuentas a los usuarios</b>	<b>84</b>
<b>Configurar Actualizaciones de Citrix Receiver</b>	<b>88</b>
<b>Configurar la plantilla administrativa de objeto de directiva de grupo</b>	<b>94</b>
<b>Optimizar el entorno</b>	<b>97</b>
<b>Respaldar la resolución de nombres DNS</b>	<b>97</b>
<b>Usar servidores proxy con XenDesktop</b>	<b>98</b>
<b>Asignar dispositivos cliente</b>	<b>98</b>
<b>Respaldar la configuración del espacio de trabajo</b>	<b>102</b>
<b>Reducir el tiempo de inicio de las aplicaciones</b>	<b>102</b>
<b>Mejorar la experiencia del usuario</b>	<b>105</b>
<b>Ajustar escala de DPI</b>	<b>114</b>
<b>Codificación de vídeo H.265</b>	<b>115</b>
<b>Iniciar vPrefer</b>	<b>117</b>
<b>Editores IME de cliente genérico</b>	<b>118</b>
<b>Barra de idioma y distribución del teclado</b>	<b>120</b>
<b>Autenticación</b>	<b>123</b>
<b>Configurar la autenticación PassThrough de dominio</b>	<b>123</b>
<b>Configurar la autenticación con tarjeta inteligente</b>	<b>127</b>
<b>Configurar la autenticación PassThrough de dominio con Kerberos</b>	<b>132</b>
<b>Habilitar la comprobación de la lista de revocación de certificados para mejorar la seguridad</b>	<b>135</b>
<b>Proteger comunicaciones</b>	<b>135</b>
<b>Aplicar relaciones de confianza</b>	<b>136</b>
<b>Configurar la autenticación con tarjeta inteligente para la Interfaz Web 5.4</b>	<b>137</b>

<b>Conectar a través de un servidor proxy</b>	<b>139</b>
<b>Conectar a través de un firewall</b>	<b>139</b>
<b>ICA File Signing para proteger ante el inicio de aplicaciones y escritorios desde servidores que no son de confianza</b>	<b>141</b>
<b>Configurar conjuntos de cifrado obsoletos</b>	<b>142</b>
<b>Configurar y habilitar TLS</b>	<b>143</b>
<b>Conectar con Secure Gateway</b>	<b>148</b>
<b>Nivel de elevación y wfcrun32.exe</b>	<b>149</b>
<b>Desktop Lock y Citrix Receiver para Windows</b>	<b>149</b>
<b>SDK y API</b>	<b>155</b>

## Novedades

January 7, 2019

### Novedades en la versión 4.12

#### Actualización con kit Crypto

Esta versión contiene dos cambios importantes para los protocolos de comunicación segura TLS/DTLS: respaldo para **DTLS 1.2** y obsolescencia de los conjuntos de cifrado TLS/DTLS, que no ofrecen confidencialidad directa.

DTLS 1.2 admite el protocolo de transporte UDP, lo que proporciona el equivalente de TLS 1.2 para el protocolo de transporte TCP. Las versiones anteriores de Receiver para Windows ya admitían TLS 1.2.

Los conjuntos de cifrado con el prefijo **TLS\_RSA\_** no ofrecen confidencialidad directa. Por lo general, estos conjuntos de cifrado se consideran obsoletos en el sector de las TIC. Sin embargo, por compatibilidad con versiones anteriores de XenApp y XenDesktop, Receiver para Windows aún puede utilizar estos conjuntos de cifrado.

Se ha creado una nueva plantilla administrativa de objeto de directiva de grupo para permitir el uso de los conjuntos de cifrado obsoletos. En Receiver para Windows 4.12, esta directiva está habilitada de forma predeterminada, pero no se aplica la obsolescencia de estos conjuntos de cifrado mediante los algoritmos AES o 3DES de forma predeterminada. Sin embargo, puede modificar y usar esta directiva para aplicar la obsolescencia más estrictamente.

A continuación, dispone de la lista de conjuntos de cifrado obsoletos:

1. TLS\_RSA\_AES256\_GCM\_SHA384
2. TLS\_RSA\_AES128\_GCM\_SHA256
3. TLS\_RSA\_AES256\_CBC\_SHA256
4. TLS\_RSA\_AES256\_CBC\_SHA
5. TLS\_RSA\_AES128\_CBC\_SHA
6. TLS\_RSA\_3DES\_CBC\_EDE\_SHA
7. TLS\_RSA\_WITH\_RC4\_128\_MD5
8. TLS\_RSA\_WITH\_RC4\_128\_SHA

#### Nota

Los últimos dos conjuntos de cifrado usan el algoritmo RC4, que está obsoleto porque esos conjuntos de cifrado no son seguros. El conjunto de cifrado **TLS\_RSA\_3DES\_CBC\_EDE\_SHA** tam-

bién se puede considerar obsoleto. Puede usar esta directiva para aplicar todos estos elementos obsoletos.

Para obtener información sobre la configuración de DTLS 1.2, consulte [Transporte adaptable](#) en la documentación de XenApp y XenDesktop.

Para obtener información sobre cómo configurar conjuntos de cifrado obsoletos, consulte [Configurar conjuntos de cifrado obsoletos](#).

## Notificación del icono de batería

Aparece una batería en el área de notificaciones del host de la sesión, donde se representa información sobre la batería del cliente.

Esta funcionalidad solo está disponible en VDA 7.18 o versiones posteriores.

## Tarjeta inteligente rápida

La tarjeta inteligente rápida mejora el rendimiento cuando se usan tarjetas inteligentes en redes WAN con latencia alta. La tarjeta inteligente rápida está habilitada de manera predeterminada en los hosts que ejecutan Windows Server 2012, Windows Server 2016 o Windows 10 (versión mínima). Para habilitar la tarjeta inteligente rápida en el lado del cliente, configure el parámetro **SmartCardCryptographicRedirection** en default.ica.

## Cámaras Web Plug and Play

Las aplicaciones detectan dinámicamente una cámara Web que se conecta al cliente o se elimina de este. No es necesario que los usuarios reinicien la aplicación para detectar esos cambios.

## Respaldo para Citrix Analytics

Citrix Receiver para Windows está equipado para transmitir registros de manera segura a Citrix Analytics. Los registros se analizan y almacenan en Citrix Analytics cuando está habilitado. Para obtener más información sobre Citrix Analytics, consulte la documentación de [Citrix Analytics](#).

## Problemas resueltos

February 20, 2019

## Citrix Receiver para Windows 4.12

Comparado con: Citrix Receiver para Windows 4.11

### Redirección de HDX MediaStream para Flash

- Con el parámetro “Redirección de HDX MediaStream para Flash” habilitado, el proceso Pseudo-Container2.exe puede cerrarse inesperadamente al desconectar la sesión. [#LC8802]

### Teclado

- Cuando se utilizan archivos APPSRV.INI o ICA descargados de StoreFront, puede que fallen los intentos de utilizar la distribución de teclado predeterminada del servidor o la que se prefiera.

A continuación, se ofrecen las limitaciones en este caso:

- Debe establecer la distribución del teclado manualmente en la sesión a través del panel de control durante la primera configuración, incluso aunque haya configurado previamente la distribución.
- En **Preferencias avanzadas**, debe establecer la sincronización de distribución de teclado a **No**. Si establece la distribución en **Sí**, se dirige el IME local. [#LC9593]

### Sesión/Conexión

- Cuando intenta iniciar un escritorio mediante Microsoft Internet Explorer 11, aparece este mensaje de error:  
“La conexión con <escritorio\_publicado> falló con el estado (Error de cliente desconocido 0)”.  
[#LC8841]
- Cuando se configura la agregación entre dos sitios en StoreFront, no se crea la sesión de preinicio. [#LC8847]
- En una sesión desde una unidad de cliente asignada, puede que algunos vídeos DVD no se reproduzcan. [#LC8912]
- En una situación de doble salto (con un VDA de escritorio en el primer salto y una aplicación que se inicia en el VDA en el segundo salto), al volver a conectarse al primer salto que ejecuta el VDA de escritorio, la pantalla puede parpadear durante unos segundos. [#LC9071]
- Al redirigir contenido bidireccional a un VDA, se abre una segunda dirección URL en un nuevo explorador Web cuando ya está abierto el explorador Web. [#LC9157]

- Cuando se inicia una aplicación, Citrix Receiver para Windows puede mostrar “Conectándose...” antes de que falle el inicio. Aparece este mensaje de error:  
“El recurso publicado no está disponible actualmente. Contacte con su administrador de sistemas para obtener ayuda”. [#LC9170]
- Cuando se inicia una sesión en el modo no integrado y de ventanas desde Citrix Receiver para Windows, puede que aparezca una pantalla gris. El problema ocurre cuando la resolución del archivo ICA es mayor que la resolución del dispositivo de punto final del cliente. [#LC9266]
- Los intentos de iniciar aplicaciones desde Citrix Receiver para Mac pueden fallar. El problema ocurre cuando no se puede obtener la licencia del cliente (LicenseRequestClientLicense). [#LC9286]
- Pueden fallar los intentos de iniciar escritorios mediante Citrix Receiver para Windows. El problema ocurre incluso después de aumentar el tiempo de inicio con el parámetro **LaunchTime-outMs** mediante StoreFront. [#LC9369]
- Si selecciona la función de borrado o eliminación del portapapeles en una aplicación publicada que se ejecuta en un VDA de servidor, el portapapeles del VDA se borra, pero el texto permanece en el portapapeles del dispositivo de punto final. [#LC9434]
- Después de actualizar Citrix Receiver para Windows a través de System Center Configuration Manager (SCCM), Receiver para Windows puede solicitar el reinicio del sistema. [#LC9706]
- Cuando se instala Citrix Receiver para Windows a través de System Center Configuration Manager (SCCM) o PSEXEC, puede que se dé una instalación sin supervisión de Receiver para Windows. [#RFWIN-8188]

### Tarjetas inteligentes

- Cuando intenta iniciar un escritorio publicado en modo de pantalla completa usando la autenticación con tarjeta inteligente, la solicitud de PIN puede no aparecer en Desktop Viewer. [#LC8579]

### Excepciones del sistema:

- El proceso wfica32 puede cerrarse de forma intermitente cuando se usa un dispositivo táctil para conectarse a un VDA. [#LC9228]
- El proceso wfica32.exe puede cerrarse de forma intermitente. [#LC9397]

### Experiencia de usuario:

- Cuando se inicia un escritorio publicado con la **Aceleración de hardware para gráficos** habilitada, puede que aparezca una vista previa en gris de Desktop Viewer en la barra de herramientas. [#LC8545]



- El escritorio puede desaparecer poco después de iniciarlo. El problema ocurre debido a paquetes TLS duplicados que se envían desde Citrix Receiver para Windows. [#LC8724]
- Los iconos del menú Inicio y la barra de tareas pueden parpadear cuando se actualizan las aplicaciones en Citrix Receiver para Windows. [#LC8890]
- Cuando se inicia un escritorio publicado con el códec de vídeo H.265, aparece un color verde en la pantalla de los escritorios publicados. [#LC9083]
- Las aplicaciones y los iconos pueden asociarse parcialmente a tipos de archivo cuando se usa Citrix Receiver para Windows con el sitio de servicios Citrix XenApp. [#LC9402]
- Elegir **No; usar la distribución de teclado del servidor** en la ficha de teclado de la página **Barra de idioma y teclado** podría no admitir dinámicamente la sincronización de la distribución del teclado. Elegir **Sí** admite dinámicamente la sincronización de la distribución del teclado. Sin embargo, la distribución del teclado se sincroniza durante la conexión inicial en ambos casos. [#RFWIN-7999]
- En una máquina de 64 bits, cuando inicia una instancia de 32 bits de una aplicación con una entrada de Registro %ProgramFiles%, la entrada se expande a C:\Archivos de programa, pero no a C:\Archivos de programa (X86)\. En consecuencia, la instancia de 32 bits del inicio de la aplicación recurre al inicio de una instancia de servidor, con lo que vPrefer falla para esa aplicación. [#RFWIN-8025]

## Otros

- Esta corrección soluciona problemas de rendimiento y ofrece mejoras de calidad para Enlightened Data Transport (EDT). [#LC9417]

**Nota:** Esta versión de Citrix Receiver para Windows también incluye todas las correcciones incluidas en las versiones [4.11](#), [4.10.1](#), [4.10](#), [4.9](#), [4.8](#), [4.7](#), [4.6](#), [4.5](#), [4.4](#).

## Problemas conocidos

January 7, 2019

### Problemas conocidos en Citrix Receiver para Windows 4.12

No se han observado nuevos problemas en esta versión.

Citrix Receiver para Windows 4.12 contiene algunos de los problemas conocidos que presentaban las versiones [4.5](#), [4.6](#), [4.7](#), [4.8](#), [4.9](#), [4.10](#) y [4.11](#).

## Avisos de terceros

October 5, 2018

Citrix Receiver para Windows puede incluir software de terceros con licencias definidas en los términos del siguiente documento:

[Citrix Receiver para Windows - Avisos legales de terceros](#)

## Requisitos del sistema y compatibilidad

March 18, 2019

### Requisitos

- Esta versión de Citrix Receiver para Windows requiere un mínimo de 500 MB de espacio libre en el disco y 1 GB de RAM.
- Requisitos mínimos de .NET Framework
  - Self-Service Plug-in requiere NET 3.5 Service Pack 1. Permite suscribirse e iniciar aplicaciones y escritorios desde la línea de comandos o la interfaz de usuario de Receiver. Para obtener más información, consulte [Configurar e instalar Receiver para Windows mediante parámetros de línea de comandos](#).
  - .NET 2.0 Service Pack 1.

### Matriz de compatibilidad

Citrix Receiver para Windows es compatible con los siguientes sistemas operativos Windows y exploradores Web. También es compatible con todas las versiones actualmente respaldadas de XenApp, XenDesktop y NetScaler Gateway, según se indican en la tabla [Citrix Product Lifecycle Matrix](#).

#### Nota

El plugin de análisis de punto final o EPA (End Point Analysis) de NetScaler Gateway no admite Citrix Receiver para Windows nativo.

---

Sistema operativo

Windows 10 (ediciones de 32 y 64 bits) \*

---

Sistema operativo

---

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

Windows 7, ediciones de 32 y 64 bits (incluida la Embedded Edition)

Windows Thin PC

Windows Server 2016

Windows Server 2012 R2, ediciones Standard y Datacenter

Windows Server 2008 R2, edición de 64 bits

Windows Server 2019

Windows 10 Enterprise 2016 LTSB 1607

---

\* Respaldar Windows 10 Versión 1607, 1703, 1709 y 1803.

Explorador Web

---

Explorador Web

---

Internet Explorer

La versión más reciente de Google Chrome (se necesita StoreFront)

La versión más reciente de Mozilla Firefox

Microsoft Edge

---

### Matriz de respaldo

---

Sistemas operativos respaldados en dispositivos táctiles	Sistemas operativos respaldados en agentes VDA
Windows 10	Windows 10
Windows 8	Windows 8
Windows 7	Windows 7
	Windows 2012 R2
	Windows Server 2016
	Windows 2008 R2

---

## Conexiones, certificados y autenticación

April 2, 2019

### Conexiones

- Tienda HTTP
- Tienda HTTPS
- NetScaler Gateway 10.5 y versiones posteriores
- Interfaz Web 5.4

### Certificados

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

### Certificados privados (autofirmados)

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

#### Nota

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

### Instalar certificados raíz

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

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

## Certificados comodín

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

Citrix Receiver para Windows respalda el uso de certificados comodín, aunque deben usarse solo de acuerdo con las directivas de seguridad de su organización. En la práctica, se puede considerar la posibilidad de usar alternativas a certificados comodines, como por ejemplo, un certificado que contenga la lista de nombres de servidor con la extensión de nombre de sujeto alternativo (Subject Alternative Name o SAN). Las entidades de certificación privadas o públicas emiten esos certificados.

## Certificados intermedios

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

## Autenticación

### Autenticar en StoreFront

	<b>Receiver para Web usando exploradores Web</b>	<b>Sitio de servicios StoreFront (nativo)</b>	<b>Sitio de XenApp y XenDesktop de StoreFront (nativo)</b>	<b>NetScaler a Receiver para Web (explorador)</b>	<b>NetScaler a sitio de servicios StoreFront (nativo)</b>
Anónimo	Sí	Sí			
Dominio	Sí	Sí	Sí	Sí*	Sí*
PassThrough de dominio	Sí	Sí	Sí		
Token de seguridad				Sí*	Sí*

Autenticación de dos factores (dominio con token de seguridad)			Sí*	Sí*
SMS			Sí*	Sí*
Tarjeta inteligente	Sí	Sí	Sí	Sí
Certificado de usuario			Sí (NetScaler Plug-in)	Sí (NetScaler Plug-in)

\* Con o sin el plugin de NetScaler instalado en el dispositivo.

#### Nota

Citrix Receiver para Windows admite la autenticación de dos factores (dominio y token de seguridad) a través de NetScaler Gateway en el servicio nativo de StoreFront.

### Autenticarse en la Interfaz Web

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

	Interfaz Web (exploradores Web)	Sitio de XenDesktop y XenApp de Interfaz Web	NetScaler a Interfaz Web (explorador Web)	NetScaler a sitio de XenApp y XenDesktop de Interfaz Web
Anónimo	Sí			
Dominio	Sí	Sí	Sí*	
PassThrough de dominio	Sí	Sí		
Token de seguridad			Sí*	

Autenticación de dos factores (dominio con token de seguridad)				Sí*
SMS				Sí*
Tarjeta inteligente	Sí	Sí		
Certificado de usuario				Sí (NetScaler Plug-in)

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

Para obtener información acerca de la autenticación, consulte [Configurar la Autenticación y autorización](#) en la documentación de NetScaler Gateway, y los temas de la sección [Administrar](#) en la documentación de StoreFront.

Para obtener más información acerca de los métodos de autenticación que admite la Interfaz Web, consulte la documentación de la Interfaz Web.

## Instalar

December 6, 2018

El paquete CitrixReceiver.exe puede instalarse siguiendo cualquiera de los siguientes métodos:

- Por un usuario, desde Citrix.com o desde un sitio de descarga
  - Un usuario nuevo que obtiene Citrix Receiver para Windows desde Citrix.com o desde un sitio de descarga puede configurar una cuenta mediante la introducción de una dirección de correo electrónico en lugar de una dirección URL de servidor. Citrix Receiver para Windows determina el servidor NetScaler Gateway o StoreFront asociado con esa dirección de correo electrónico y pide al usuario que inicie una sesión para continuar con la instalación. Esta característica se conoce como “detección de cuentas basada en correo electrónico”.  
Nota: Un usuario nuevo es aquel que no tiene Citrix Receiver para Windows instalado en el dispositivo.  
Nota: La detección de cuentas basada en correo electrónico para un usuario nuevo no se

aplica cuando Citrix Receiver para Windows se descarga desde una ubicación distinta a Citrix.com (como, por ejemplo, un sitio de Receiver para Web).

- Si el sitio requiere la configuración de Citrix Receiver para Windows, utilice un método de implementación alternativo.
- Automáticamente desde [Receiver para Web](#) o desde la [página de inicio de sesión de la Interfaz Web](#).
  - Un usuario nuevo puede configurar una cuenta introduciendo la dirección URL de un servidor, o descargando un archivo de aprovisionamiento (CR).
- Mediante una herramienta de distribución electrónica de software (ESD)
  - Un usuario nuevo debe introducir una dirección URL de servidor o abrir un archivo de aprovisionamiento para configurar una cuenta.

Citrix Receiver para Windows no requiere derechos de administrador para la instalación, a menos que vaya a usar la autenticación PassThrough.

## Verificar la integridad de Citrix Receiver para Windows

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

## Instalar con y sin privilegios de administrador

Existen las siguientes diferencias entre las instalaciones de Citrix Receiver para Windows realizadas por un administrador y las realizadas por un usuario (no administrador).

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

### Nota

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



## Actualizar manualmente a Citrix Receiver para Windows

Para implementaciones con StoreFront:

- Se recomienda que los usuarios de BYOD (Bring Your Own Device), es decir usuarios que traen sus propios dispositivos, configuren las últimas versiones de NetScaler Gateway y StoreFront según se describe en la documentación correspondiente en el [sitio de documentación de productos](#). Adjunte el archivo de aprovisionamiento creado por StoreFront en un mensaje de correo electrónico e informe a los usuarios de cómo realizar la actualización e indíqueles que abran el archivo de aprovisionamiento después de instalar Citrix Receiver para Windows.
- Como alternativa a proporcionar un archivo de aprovisionamiento, indique a los usuarios que introduzcan la URL de NetScaler Gateway. O, si configuró la detección de cuentas basada en correo electrónico según se describe en la documentación de StoreFront, indique a los usuarios que introduzcan su dirección de correo electrónico.
- Otro método consiste en configurar un sitio de Citrix Receiver para Web según se describe en la documentación de StoreFront, y completar la configuración que se describe en [Implementación de Citrix Receiver para Windows desde Receiver para Web](#). Informe a los usuarios sobre cómo actualizar Citrix Receiver para Windows, cómo acceder al sitio de Citrix Receiver para Web y cómo descargar el archivo de aprovisionamiento desde Citrix Receiver para Web (haciendo clic en el nombre de usuario y luego en Activar).

Para implementaciones con la Interfaz Web

- Actualice el sitio de la Interfaz Web con Citrix Receiver para Windows y complete la configuración que se describe en [Implementar Citrix Receiver para Windows desde una pantalla de inicio de sesión de la Interfaz Web](#). Indique a los usuarios cómo actualizar Citrix Receiver para Windows. Por ejemplo, puede crear un sitio de descargas donde los usuarios pueden obtener el instalador de Citrix Receiver con el nuevo nombre.

## Consideraciones sobre la actualización

Para obtener más información sobre qué hay que tener en cuenta antes de actualizar Citrix Receiver para Windows, consulte el artículo [CTX135933](#) de Knowledge Center.

## HDX RealTime Media Engine (RTME)

Ahora hay un instalador único que combina la versión más reciente de Citrix Receiver para Windows con el instalador de HDX RTME. Cuando se instala Citrix Receiver mediante el ejecutable (.exe), HDX RTME también se instala.

Si tiene instalado HDX RealTime Media Engine, al desinstalar y volver a instalar Citrix Receiver para Windows, asegúrese de usar el mismo modo que utilizó para instalar HDX RealTime Media Engine.

### Nota

La instalación de la versión más reciente de Citrix Receiver con el RTME integrado requiere privilegios administrativos en el host.

Tenga en cuenta los problemas siguientes de HDX RTME al instalar o actualizar Citrix Receiver para Windows:

- La versión más reciente de Citrix ReceiverPlusRTME contiene HDX RTME; no es necesario instalar nada más para instalar RTME.
- Se admite la actualización desde una versión de Citrix Receiver para Windows anterior a la versión empaquetada más reciente (Citrix Receiver con RTME). Las versiones anteriores de RTME instaladas se sobrescribirán con la versión más reciente; no se admite la actualización desde una versión de Citrix Receiver para Windows a la misma versión empaquetada más reciente (por ejemplo, no se puede actualizar desde Receiver 4.7 a la versión empaquetada de Receiver 4.7 con RTME).
- Si tiene una versión anterior de RTME, cuando instale la versión más reciente de Citrix Receiver para Windows, RTME se actualizará automáticamente en el dispositivo cliente.
- Si tiene una versión más reciente de RTME, el instalador la conservará.

### Importante

HDX RealTime Connector debe ser al menos de la versión mínima 2.0.0.417 para la compatibilidad con el nuevo paquete RTME. Es decir, RTME 2.0 no se puede usar con 1.8 RTME Connector.

## Configurar e instalar mediante parámetros de línea de comandos

April 2, 2019

Puede personalizar el instalador de Citrix Receiver para Windows mediante opciones en la línea de comandos. El paquete de instalación se descomprime automáticamente en el directorio temporal del usuario antes de iniciar el instalador. El requisito de espacio incluye espacio para archivos de programa, datos de usuarios y directorios temporales después de iniciar varias aplicaciones.

Para obtener más información acerca de los requisitos del sistema, consulte [Requisitos del sistema](#).

Para instalar Citrix Receiver para Windows desde la interfaz de comandos, use la siguiente sintaxis:

### **CitrixReceiver.exe [Opciones]**

### **Actualizaciones de Receiver**

Opción	/AutoUpdateCheck = auto/manual/disabled
<b>Descripción</b>	Indica que Citrix Receiver para Windows detecta si hay una actualización disponible. <b>Auto (Automático):</b> Se le notifica cuando hay una actualización disponible (predeterminado). <b>Manual:</b> No se le notifica cuando hay actualizaciones disponibles. Compruebe manualmente si hay actualizaciones. <b>Disabled (Inhabilitado):</b> Se inhabilita la actualización automática.
<b>Ejemplo de uso</b>	CitrixReceiver.exe /AutoUpdateCheck = auto ; CitrixReceiver.exe /AutoUpdateCheck = manual ; CitrixReceiver.exe /AutoUpdateCheck = disabled

Opción	/AutoUpdateStream= LTSR/Current
<b>Descripción</b>	Indica la versión de Citrix Receiver para Windows. <b>LTSR:</b> Indica que la versión es una versión Long Term Service Release. <b>Current (Reciente):</b> Indica que la versión es la versión más reciente de Citrix Receiver para Windows.
<b>Ejemplo de uso</b>	CitrixReceiver.exe /AutoUpdateStream= LTSR ; CitrixReceiver.exe /AutoUpdateStream= Current

Opción	/DeferUpdateCount
<b>Descripción</b>	Indica la versión de Citrix Receiver para Windows. <b>-1:</b> Indica que puede aplazar las notificaciones cualquier cantidad de veces (el valor predeterminado es -1). <b>0:</b> Indica que no se muestra la opción “Recordármelo más tarde”. <b>Cualquier otro número:</b> La opción “Recordármelo más tarde” se muestra esa cantidad de veces. Por ejemplo, si establece el valor en 10, la opción Recordármelo más tarde aparecerá 10 veces.
<b>Ejemplo de uso</b>	CitrixReceiver.exe /DeferUpdateCount=-1 ; CitrixReceiver.exe /DeferUpdateCount=-0; CitrixReceiver.exe /DeferUpdateCount= <i>cualquier otro número</i>

Opción	/AURolloutPriority
<b>Descripción</b>	Indica el período en que se puede organizar el despliegue de la actualización. <b>Fast (Rápido):</b> La implantación de la actualización tiene lugar al comienzo del período de entrega. <b>Medium (Medio):</b> La implantación de la actualización tiene lugar hacia la mitad del periodo de entrega. <b>Slow (Lento):</b> La implantación de la actualización tiene lugar al final del período de entrega.
<b>Ejemplo de uso</b>	CitrixReceiver.exe /AURolloutPriority=Fast; CitrixReceiver.exe /AURolloutPriority=Medium; CitrixReceiver.exe /AURolloutPriority=Slow

## Habilitar la redirección de contenido bidireccional

### Nota

De forma predeterminada, Citrix Receiver para Windows no instala los componentes de la redirección de contenido bidireccional si ya están instalados en el servidor. Si está usando XenDesk-

top como una máquina cliente, debe instalar Citrix Receiver para Windows utilizando el conmutador /FORCE\_LAA para instalar los componentes de la redirección de contenido bidireccional. La función, sin embargo, debe configurarse tanto en el cliente como en el servidor.

Opción	ALLOW_BIDIRCONTENTREDIRECTION=1
<b>Descripción</b>	Indica que la redirección de contenido bidireccional del cliente al host y del host al cliente está <b>Habilitada</b> .
<b>Ejemplo de uso</b>	CitrixReceiver.exe /ALLOW_BIDIRCONTENTREDIRECTION=1

### Ocultar opción de parámetros

Opción	/DisableSetting
<b>Descripción</b>	Impide que Opción de parámetros aparezca en el diálogo Preferencias avanzadas.
<b>Ejemplo de uso</b>	CitrixReceiver.exe /DisableSetting=3

Si quiere que Presentación de las aplicaciones y Opciones de reconexión aparezcan en Opción de parámetros	Escriba CitrixReceiver.exe /DisableSetting=0
Si quiere que Opción de parámetros no aparezca en el diálogo Preferencias avanzadas	Escriba CitrixReceiver.exe /DisableSetting=3
Si quiere que Opción de parámetros solo muestre Presentación de las aplicaciones	Escriba CitrixReceiver.exe /DisableSetting=2
Si quiere que Opción de parámetros solo muestre Opciones de reconexión	Escriba CitrixReceiver.exe /DisableSetting=1

### Habilitar el acceso a aplicaciones locales

Opción	FORCE_LAA=1
<b>Descripción</b>	De manera predeterminada, Citrix Receiver para Windows no instala los componentes de cliente de Acceso a aplicaciones locales, si los componentes ya están instalados en el servidor. Para forzar los componentes de Acceso a aplicaciones locales del lado del cliente en Citrix Receiver, utilice el conmutador de línea de comandos FORCE_LAA. Se requieren privilegios de administrador para realizar estos pasos. Para obtener más información sobre el Acceso a aplicaciones locales, consulte Acceso a aplicaciones locales en la documentación de XenApp y XenDesktop.
<b>Ejemplo de uso</b>	CitrixReceiver.exe /FORCE_LAA=1

### Mostrar información de uso

Opción	/? o /help
<b>Descripción</b>	Indica información de uso
<b>Ejemplo de uso</b>	CitrixReceiver.exe /?; CitrixReceiver.exe /help

### Omitir el reinicio durante las instalaciones con interfaz de usuario

Opción	/noreboot
<b>Descripción</b>	Omite el reinicio durante las instalaciones con interfaz de usuario. Esta opción no es necesaria para instalaciones silenciosas. Si elimina las solicitudes de reinicio, Citrix Receiver para Windows no reconocerá aquellos dispositivos USB que estén en estado suspendido cuando Citrix Receiver para Windows se instale; permanecerán sin reconocimiento hasta que se reinicie el dispositivo del usuario.

Opción	/noreboot
<b>Ejemplo de uso</b>	CitrixReceiver.exe /noreboot

### Instalación silenciosa

Opción	/silent
<b>Descripción</b>	Inhabilita los cuadros de diálogo de error y progreso para ejecutar una instalación completamente silenciosa.
<b>Ejemplo de uso</b>	CitrixReceiver.exe /silent

### Habilitar autenticación Single Sign-on

Opción	/includeSSON
<b>Descripción</b>	<p>Indica que Citrix Receiver para Windows se instalará con el componente de inicio de sesión único Single Sign-On. La opción relacionada, ENABLE_SSON, se habilita cuando /includeSSON figura en la línea de comandos. Si usa ADDLOCAL= para especificar características y quiere instalar Single Sign-On, también tiene que especificar el valor SSON. Para habilitar la autenticación PassThrough en un dispositivo de usuario, es necesario instalar Citrix Receiver para Windows con derechos de administrador local desde una línea de comandos que incluya la opción /includeSSON. Para obtener más información, consulte <a href="#">How to Manually Install and Configure Citrix Receiver for Pass-Through Authentication</a>. <b>Nota:</b> Las directivas Tarjeta inteligente, Kerberos y Nombre de usuario y contraseña locales son interdependientes. El orden de configuración es importante. Le recomendamos que inhabilite primero las directivas que no desee usar y, a continuación, habilite las directivas que necesite. Compruebe los resultados con atención.</p>
<b>Ejemplo de uso</b>	CitrixReceiver.exe /includeSSON

### Habilitar Single Sign-on cuando /includeSSON está especificado



Opción	ENABLE_SSON={Yes, No}
<b>Descripción</b>	Habilita el inicio de sesión único (Single Sign-on) cuando se especifica /includeSSON. El valor predeterminado es Yes. Esta propiedad es necesaria para los inicios de sesión Single Sign-on con tarjeta inteligente. Después de realizar una instalación con la autenticación Single Sign-On habilitada, los usuarios deberán cerrar y volver a iniciar sus sesiones en los dispositivos. Requiere derechos de administrador.
<b>Ejemplo de uso</b>	CitrixReceiver.exe ENABLE_SSON=Yes

### Seguimiento permanente

Opción	/EnableTracing={true, false}
<b>Descripción</b>	De manera predeterminada, esta función tiene el valor true. Use esta propiedad para habilitar o inhabilitar la función Seguimiento permanente (Always-on tracing). La función Seguimiento permanente ayuda a recopilar registros importantes en el momento de la conexión. Esos registros pueden resultar de utilidad en la resolución de problemas de conectividad intermitente. La directiva Seguimiento permanente sobrescribe este parámetro.
<b>Ejemplo de uso</b>	CitrixReceiver.exe /EnableTracing=true

### Uso del programa Customer Experience Improvement Program de Citrix (CEIP)

Opción	EnableCEIP={true, false }
<b>Descripción</b>	Cuando se participa en el programa CEIP de mejora de la experiencia del usuario (Customer Experience Improvement Program), se envían estadísticas e información de uso anónimos a Citrix para ayudar a Citrix a mejorar la calidad y el rendimiento de sus productos.
<b>Ejemplo de uso</b>	CitrixReceiver.exe EnableCEIP=true

### Especificar el directorio de instalación

Opción	INSTALLDIR= <i>Installation Directory</i>
<b>Descripción</b>	Especifica la ruta de instalación donde se instala la mayor parte del software de Citrix Receiver. El valor predeterminado es C:\Archivos de programa\Citrix\Receiver. Los siguientes componentes de Receiver se instalan en la ruta C:\Archivos de programa\Citrix: <b>Authentication Manager</b> , <b>Citrix Receiver</b> y <b>Self-Service plug-in</b> . Si usa esta opción y especifica un directorio de instalación, debe instalar RIInstaller.msi en el directorio \Receiver y los demás archivos .msi en el directorio de instalación.
<b>Ejemplo de uso</b>	CitrixReceiver.exe INSTALLDIR=c:\Citrix\Test

### Identificar un dispositivo de usuario

Opción	CLIENT_NAME= <i>ClientName</i>
<b>Descripción</b>	Especifica el nombre del cliente, donde ClientName identifica el dispositivo de usuario en el servidor. El valor predeterminado es %COMPUTERNAME%

Opción	CLIENT_NAME= <i>ClientName</i>
<b>Ejemplo de uso</b>	CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%

---

### Nombre de cliente dinámico

Opción	ENABLE_CLIENT_NAME=Yes, No
<b>Descripción</b>	La función de nombre de cliente dinámico 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. El valor predeterminado es Yes. Si quiere inhabilitar el respaldo para usar el nombre de cliente dinámico, defina esta propiedad con el valor “No” y especifique un valor para la propiedad CLIENT_NAME.
<b>Ejemplo de uso</b>	CitrixReceiver.exe ENABLE_DYNAMIC_CLIENT_NAME =Yes

---

### Instalar componentes especificados

Opción	ADDLOCAL=<característica... ,>
<b>Descripción</b>	<p>Instala uno o varios componentes especificados. Cuando quiera especificar varios parámetros, separe cada parámetro con una coma y no incluya espacios. Los nombres distinguen mayúsculas de minúsculas. Si no especifica este parámetro, todos los componentes se instalarán de forma predeterminada. Citrix recomienda usar el ejemplo de uso de ADDLOCAL que se muestra más abajo. Si el ejemplo de uso no se aplica como se describe aquí, puede tener resultados inesperados. Los componentes incluyen:</p> <p>ReceiverInside : instala la experiencia de la aplicación Citrix Workspace (componente necesario para el funcionamiento de la aplicación Workspace). ICA_Client: Instala la aplicación Citrix Workspace estándar (componente requerido para el funcionamiento de la aplicación Citrix Workspace). WebHelper: Instala el componente WebHelper. Este componente recupera el archivo ICA de StoreFront y lo transfiere a HDX Engine. Además, comprueba los parámetros del entorno y los comparte con StoreFront (similar a la detección de cliente ICO). [Optativo] SSON: Instala el inicio de sesión con Single Sign-on. Requiere derechos de administrador. AM: Instala Authentication Manager. SELFSERVICE: Instala Self-Service Plug-in. El valor AM debe especificarse en la línea de comandos, y .NET 3.5 Service Pack 1 tiene que estar instalado en el dispositivo del usuario. El Self-Service Plug-in no está disponible para dispositivos Windows Thin PC, que no admiten .NET 3.5. Para obtener información sobre la creación de scripts de Self-Service Plug-in (SSP) y ver una lista de los parámetros disponibles en Receiver para Windows 4.2 y versiones posteriores, consulte el artículo CTX200337 de Knowledge Center. El Self-Service Plug-in permite a los usuarios acceder a aplicaciones y escritorios virtuales desde la ventana de la aplicación Citrix Workspace o desde una línea de comandos,</p>

Opción	ADDLOCAL=<característica... ,>
<b>Ejemplo de uso</b>	CitrixReceiver.exe ADDLOCAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopView

### Configurar Citrix Receiver para Windows para agregar tiendas manualmente

Opción	ENABLE_CLIENT_NAME=Yes, No
<b>Descripción</b>	La función de nombre de cliente dinámico 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. El valor predeterminado es Yes. Si quiere inhabilitar el respaldo para usar el nombre de cliente dinámico, defina esta propiedad con el valor "No" y especifique un valor para la propiedad CLIENT_NAME.
<b>Ejemplo de uso</b>	CitrixReceiver.exe ENABLE_DYNAMIC_CLIENT_NAME =Yes

### Guardar las credenciales de las tiendas localmente usando el protocolo PNAgent

Opción	ALLOWSAVEPWD={N, S, A}
<b>Descripción</b>	<p>El valor predeterminado es el valor especificado desde el servidor PNAgent durante la ejecución. Especifica si los usuarios pueden guardar las credenciales para las tiendas localmente en sus equipos y se aplica solamente a tiendas que usan el protocolo PNAgent. El valor predeterminado es "S". A continuación, dispone de las demás opciones disponibles. <b>N:</b> Nunca se permite que los usuarios guarden sus contraseñas. <b>S:</b> Se permite que los usuarios guarden contraseñas tanto para tiendas seguras (HTTPS), tienda no seguras (HTTPS) como tiendas no seguras (HTTP). También puede controlar esta característica actualizando la clave de Registro HKLM\Software[Wow6432Node]\Citrix\Dazzle\AllowSavePwd</p> <p><b>Nota:</b> Si AllowSavePwd no funciona, debe agregarse manualmente la siguiente clave de Registro: <b>1 Clave</b> para SO cliente de 32 bits: HKLM\Software\Citrix\AuthManager <b>2 Clave</b> para SO cliente de 64 bits: HKLM\Software\wow6432node\Citrix\AuthManager</p> <p><b>3 Tipo:</b> REG_SZ <b>4 Valor:</b> never (no permitir nunca a los usuarios guardar sus contraseñas), secureonly (permitir a los usuarios guardar contraseñas solo para las tiendas seguras, es decir, configuradas con HTTPS) y always (permitir a los usuarios guardar sus contraseñas tanto para las tiendas seguras, es decir, HTTPS, como para las no seguras, es decir, HTTP).</p>
<b>Ejemplo de uso</b>	CitrixReceiver.exe ALLOWADDSTORE=N

## Seleccionar el certificado

Opción	AM_CERTIFICATESELECTIONMODE={Prompt, SmartCardDefault, LatestExpiry }
<b>Descripción</b>	Use esta opción para seleccionar un certificado. El valor predeterminado es “Prompt”, que pide al usuario que elija un certificado de la lista. Cambie esta propiedad para seleccionar la opción de certificado predeterminado (según lo indique el proveedor de la tarjeta inteligente) o la opción de certificado con la fecha de caducidad más lejana. Si no hay certificados de inicio de sesión válidos, se notifica de ello al usuario y se le da la opción de usar un método de inicio de sesión alternativo, si hay alguno disponible. También se puede controlar esta característica actualizando la clave de Registro HKCU o HKLM\Software[Wow6432Node]Citrix\AuthManager:CertificateSelectionMode={Prompt   SmartCardDefault   LatestExpiry }. Los valores definidos en HKCU tienen preferencia sobre los valores definidos en HKLM para facilitar al usuario la selección de certificado.
<b>Ejemplo de uso</b>	CitrixReceiver.exe AM_CERTIFICATESELECTIONMODE=Prompt

## Usar componentes del proveedor CSP para administrar la entrada del PIN de tarjeta inteligente

Opción	AM_SMARTCARDPINENTRY=CSP
<b>Descripción</b>	Usar los componentes del proveedor de servicios criptográficos (CSP) para administrar la entrada del PIN de la tarjeta inteligente. De manera predeterminada, los diálogos de PIN que se presentan a los usuarios provienen de Citrix Receiver en lugar de venir del proveedor CSP (Cryptographic Service Provider) de la tarjeta inteligente. Receiver pide a los usuarios que introduzcan un PIN cuando es necesario, y luego pasa el PIN al proveedor CSP de la tarjeta inteligente. Especifique esta propiedad para usar los componentes del proveedor CSP para gestionar la introducción del PIN, incluidas las solicitudes de PIN.
<b>Ejemplo de uso</b>	CitrixReceiver.exe AM_SMARTCARDPINENTRY=CSP

## Usar Kerberos

Opción	ENABLE_KERBEROS={Yes, No}
<b>Descripción</b>	El valor predeterminado es "No". Esta opción especifica si el motor HDX debe usar la autenticación Kerberos y se aplica solo cuando la autenticación Single Sign-On (PassThrough) está habilitada. Para obtener más información, consulte Configurar autenticación PassThrough de dominio con Kerberos.
<b>Ejemplo de uso</b>	CitrixReceiver.exe ENABLE_KERBEROS=No

## Mostrar iconos de FTA antiguos



Opción	LEGACYFTAICONS={False, True}
<b>Descripción</b>	Use esta opción para mostrar los iconos de asociación de tipos de archivos (FTA) antiguos. El valor predeterminado es "False". Especifique si se muestran los iconos de aplicación para aquellos documentos que tienen asociaciones de tipo de archivo con aplicaciones suscritas. Cuando el parámetro está configurado como False, Windows genera iconos para documentos que no tienen un icono específico asignado a ellos. Los iconos generados por Windows consisten en un icono de documento genérico superpuesto con un icono de la aplicación de tamaño más pequeño. Citrix recomienda habilitar esta opción si planea entregar aplicaciones de Microsoft Office a usuarios que ejecutan Windows 7.
<b>Ejemplo de uso</b>	CitrixReceiver.exe LEGACYFTAICONS=False

### Habilitar el preinicio de sesiones

Opción	ENABLEPRELAUNCH={False, True}
<b>Descripción</b>	El valor predeterminado es "False". Para obtener información acerca del preinicio de sesiones, consulte Reducir el tiempo de inicio de las aplicaciones.
<b>Ejemplo de uso</b>	CitrixReceiver.exe ENABLEPRELAUNCH=False

### Especificar el directorio para los accesos directos del menú Inicio

Opción	STARTMENUDIR={Nombre del directorio}
<b>Descripción</b>	<p>De forma predeterminada, las aplicaciones aparecen en Inicio &gt; Todos los programas.</p> <p>Puede especificar la ruta relativa de los accesos directos en la carpeta de programas. Por ejemplo, para colocar accesos directos en Inicio &gt; Todos los programas &gt; Receiver, especifique STARTMENUDIR=\Receiver. Puede cambiar o mover la carpeta en cualquier momento. También puede controlar esta característica con una clave de Registro. Cree la entrada REG_SZ para StartMenuDir y establézcala en el valor “\RelativePath”</p> <p>Location:  HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\Dazzle  HKEY_CURRENT_USER\Software\Citrix\Dazzle.</p> <p>Para aplicaciones publicadas a través de XenApp con el elemento Carpeta de aplicaciones del cliente (también llamado Carpeta de Program Neighborhood) especificado, se puede configurar para que esa carpeta se agregue a la ruta de accesos directos. Para ello, cree la entrada REG_SZ para UseCategoryAsStartMenuPath y otórguele el valor “true”. Use las mismas ubicaciones de Registro señaladas anteriormente. <b>Nota:</b> Windows 8 u 8.1 no permite crear carpetas anidadas dentro del menú Inicio. Las aplicaciones se mostrarán de forma individual o dentro de la carpeta raíz, no en las subcarpetas de categorías definidas. Ejemplos:</p> <p><b>1</b> Si la carpeta de aplicaciones del cliente es \office, UseCategoryAsStartMenuPath tiene el valor “true”, y no se especifica un directorio StartMenuDir, los accesos directos se colocan en Inicio &gt; Todos los programas &gt; Office. <b>2</b> Si la carpeta de aplicaciones del cliente es \office, UseCategoryAsStartMenuPath tiene el valor “true” y el directorio StartMenuDir es \Receiver, los accesos directos se colocan en Inicio &gt; Todos los programas &gt; Receiver &gt; Office. Los cambios que se hagan a estos parámetros no tienen impacto alguno en los accesos directos ya creados. Para mover accesos directos, es necesario desinstalar y</p>

Opción	STARTMENUMDIR={Nombre del directorio}
<b>Ejemplo de uso</b>	CitrixReceiver.exe STARTMENUMDIR=\Office

## Especificar el nombre de la tienda

Opción	STOREx="storename;http[s]://servername.domain/IISLocation/Off"; [descripción de la tienda] "[STOREy="-"]
<b>Descripción</b>	<p>Use esta opción para especificar el nombre de la tienda. Especifica hasta 10 tiendas para usar con Citrix Receiver. Valores: <b>x</b> e <b>y</b> (números enteros de <b>0 a 9</b>); <b>storename</b> (el valor predeterminado es la tienda). Este valor debe coincidir con el nombre configurado en el servidor StoreFront. <b>servername.domain:</b> El nombre de dominio completo del servidor que aloja la tienda. <b>IISLocation:</b> La ruta a la tienda en IIS. La URL de la tienda debe coincidir con la URL en los archivos de aprovisionamiento de StoreFront. Las direcciones URL de tienda tienen el formato "/Citrix/store/discovery".</p> <p>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 &lt;Address&gt;.</p> <p><b>On, Off:</b> El parámetro de configuración "Off" opcional permite entregar tiendas inhabilitadas, lo que ofrece a los usuarios la opción de acceso. Cuando el estado de la tienda no se especifica, el parámetro predeterminado es "On" (habilitado).</p> <p><b>storedescription:</b> Una descripción optativa de la tienda, por ejemplo "Tienda de aplicaciones de RRHH". <b>Nota:</b> En esta versión, es importante incluir "/discovery" en la URL de la tienda para que la autenticación PassThrough se realice correctamente.</p>

Opción	STOREx="storename;http[s]://servername.domain/IISLocation/Off] ; [descripción de la tienda] "[STOREy="-"]
<b>Ejemplo de uso</b>	CitrixReceiver.exe STORE0="Store; <a href="https://test.xx.com/Citrix/Store/Discovery">https://test.xx.com/Citrix/Store/Discovery</a> "

### Habilitar la redirección de URL en los dispositivos de los usuarios

Opción	ALLOW_CLIENTHOSTEDAPPSURL=1
<b>Descripción</b>	Habilita la característica de redirección de URL en los dispositivos de los usuarios. Requiere derechos de administrador. Requiere que Citrix Receiver se instale para Todos los usuarios. Para obtener información sobre la redirección de URL, consulte "Acceso a aplicaciones locales" y sus temas secundarios en la documentación de XenDesktop 7.
<b>Ejemplo de uso</b>	CitrixReceiver.exe ALLOW_CLIENTHOSTEDAPPSURL=1

### Habilitar el modo de autoservicio

Opción	SELSERVICEMODE={False, True}
<b>Descripción</b>	El valor predeterminado es True. Cuando el administrador establece la marca SelfServiceMode con el valor False, el usuario deja de tener acceso a la interfaz de usuario de autoservicio de Citrix Receiver. En vez de ello, el usuario puede acceder a las aplicaciones suscritas desde el menú Inicio y a través de accesos directos de escritorio, lo que se conoce como <b>modo de acceso directo solamente</b> .
<b>Ejemplo de uso</b>	CitrixReceiver.exe SELSERVICEMODE=False

### Especificar el directorio para los accesos directos de escritorio

Opción	DESKTOPDIR= <i>Directory Name</i>
<b>Descripción</b>	Coloca todos los accesos directos en una misma carpeta. Se respalda el uso de CategoryPath para los accesos directos de escritorio. <b>Nota:</b> Cuando se usa la opción DESKTOPDIR, configure la clave PutShortcutsOnDesktop con el valor True.
<b>Ejemplo de uso</b>	CitrixReceiver.exe DESKTOPDIR=\Office

### Actualizar desde una versión de Citrix Receiver no respaldada

#### Nota

Cuando se actualiza Citrix Receiver 13.x Enterprise o 12.x a Citrix Receiver para Windows 4.4 y versiones posteriores desde la interfaz gráfica de usuario, el instalador ejecuta la utilidad de limpieza de Receiver de forma predeterminada.

Sin embargo, la utilidad no se ejecuta de forma predeterminada cuando se actualiza desde la línea de comandos. Para actualizar desde la línea de comandos, ejecute el siguiente comando:

```
CitrixReceiver.exe /rcu /silent
```

Cuando se actualiza Citrix Receiver para Windows desde 13.x (no Enterprise) o 4.1 a la versión 4.2 o una versión posterior, el modificador de línea de comandos /rcu no es necesario y se ignora.

Opción	/rcu
<b>Descripción</b>	Permite actualizar una versión no respaldada a la versión más reciente de Citrix Receiver.
<b>Ejemplo de uso</b>	CitrixReceiver.exe /rcu

### Solucionar problemas de la instalación

Si existe un problema con la instalación, busque en el directorio %TEMP%/CTXReceiverInstallLogs del usuario para consultar los registros que tengan el prefijo CtxInstall- o TrolleyExpress- . Por ejemplo:

```
CtxInstall-ICAWebWrapper-20141114-134516.log
```

```
TrolleyExpress-20090807-123456.log
```

## Ejemplos de una instalación de línea de comandos

### Para especificar la URL de tienda de NetScaler Gateway:

CitrixReceiver.exe STORE0="<StoreFriendlyName>;[servidor de prueba](#) <StoreName>;<On/Off>;<StoreDescription>

**Nota:** La URL de tienda de NetScaler Gateway debe ser la primera entrada en la lista de direcciones URL configuradas de tienda.

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

Para especificar el inicio de sesión único (autenticación PassThrough) y agregar una tienda que apunte a una [dirección URL de servicios XenApp](#):

### Para iniciar una aplicación o un escritorio virtual desde la línea de comandos

Citrix Receiver para Windows crea una aplicación de código auxiliar (stub) para cada aplicación o escritorio suscrito. Es posible usar una aplicación de código auxiliar para iniciar una aplicación o un escritorio virtual desde la línea de comandos. Las aplicaciones de código auxiliar se encuentran en %appdata%\Citrix\SelfService. El nombre de archivo de una aplicación de código auxiliar es el nombre simplificado de la aplicación con los espacios eliminados. Por ejemplo, el nombre de archivo de la aplicación de código auxiliar para Internet Explorer es InternetExplorer.exe.

## Implementar mediante System Center Configuration Manager 2012 R2

February 20, 2019

Puede usar Microsoft System Center Configuration Manager (SCCM) para implementar Citrix Receiver para Windows.

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

Hay cuatro partes a completar en la implementación de Citrix Receiver para Windows usando SCCM:

1. [Agregar Citrix Receiver para Windows a la implementación SCCM](#)
2. [Agregar puntos de distribución](#)
3. [Implementar el software de Receiver en el Centro de software](#)
4. [Crear colecciones de dispositivos](#)

## Agregar Citrix Receiver para Windows a la implementación SCCM

1. Copie el Citrix Receiver descargado a una carpeta en el servidor de Configuration Manager y abra la consola de Configuration Manager.
2. Seleccione **Biblioteca de Software > Administración de aplicaciones**. Haga clic con el botón secundario en **Aplicación** y haga clic en **Crear aplicación**.  
Se abrirá el Asistente para crear aplicaciones.
3. En el panel **General**, haga clic en **Especificar manualmente la información de la aplicación** y, a continuación, haga clic en **Siguiente**.
4. En el panel **Información general**, especifique información acerca de la aplicación (por ejemplo, el nombre, el fabricante o la versión de software).
5. En el asistente “Catálogo de aplicaciones”, especifique información adicional, como el idioma, el nombre de la aplicación, 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 Citrix Receiver.  
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 Receiver) y haga clic en **Siguiente**.
9. En el panel **Contenido**:
  - a) Suministre la ruta donde se encuentra el archivo de programa de instalación de Citrix Receiver. Por ejemplo: Herramientas en el servidor SCCM.
  - b) Especifique el **programa de instalación** como uno de los siguientes:
    - CitrixReceiver.exe /silent para la instalación silenciosa predeterminada.
    - CitrixReceiver.exe /silent /includeSSON para habilitar el paso de credenciales de dominio (PassThrough).
    - CitrixReceiver.exe /silent SELFSERVICEMODE=false para instalar Receiver en el modo de no autoservicio.
  - c) Especifique **Programa de desinstalación** como CitrixReceiver.exe /uninstall (para habilitar la desinstalación a través de SCCM).
10. En el panel **Método de detección**, seleccione **Configurar reglas para detectar la presencia de este tipo de implementación** y haga clic en **Agregar cláusula**.  
Aparece el cuadro de diálogo Regla de actualización.

11. Establezca **Tipo de configuración** en **Sistema de archivos**.
12. En **Especificar el archivo o la carpeta para detectar esta aplicación**, establezca las siguientes opciones:
  - **Tipo:** En el menú desplegable, seleccione “Archivo”.
  - **Ruta-** %ProgramFiles (x86)%\Citrix\ICA Client\Receiver
  - **Nombre de archivo o carpeta:** Receiver.exe
  - **Propiedad:** En el menú desplegable, seleccione **Versión**.
  - **Operador:** En el menú desplegable, seleccione **Mayor o igual que**.
  - **Valor:** Escriba **4.3.0.65534**

**Nota:** Esta combinación de regla también es aplicable a actualizaciones de Citrix Receiver para Windows.

13. En el panel **Experiencia del usuario**, establezca:
  - **Comportamiento de instalación:** Instalar para el sistema.
  - **Requisito de inicio de sesión:** Tanto si un usuario inició sesión como si no.
  - **Visibilidad del programa de instalación:** Normal.

Haga clic en **Next**.

**Nota:** No especifique requisitos ni dependencias para este tipo de implementación.

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

Aparecerá un mensaje indicando que la conexión tuvo lugar.
15. En el panel **Finalización**, aparece listado un nuevo tipo de implementación (Implementación de Receiver) en “Tipos de implementación”.
16. Haga clic en **Siguiente** y **Cerrar**.

## **Agregar puntos de distribución**

1. Haga clic con el botón secundario en Receiver para Windows en 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 el software de Receiver en el Centro de software

1. Haga clic con el botón secundario en Receiver para Windows 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 **Next**.
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 indicando que la operación es correcta.

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

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

## Crear colecciones de dispositivos

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

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 de atributo** en función de los dispositivos que quiere filtrar y suministre el valor para el “Nombre del atributo” para seleccionar los dispositivos.
5. Haga clic en **Next**. En el panel “Seleccionar recursos”, seleccione los dispositivos que deben formar parte de la colección de dispositivos.  
En el panel “Finalización”, se muestra un mensaje indicando que la operación es correcta.
6. Haga clic en **Close**.
7. En el panel “Reglas de pertenencia”, aparecerá una nueva regla. Haga clic en **Next**.
8. En el panel “Finalización”, se muestra un mensaje indicando que la operación es correcta. Haga clic en **Cerrar** para completar el Asistente para crear recopilación de dispositivos.  
La nueva colección de dispositivos aparece en **Recopilaciones de dispositivos**. La nueva colección de dispositivos forma parte de las Recopilaciones de dispositivos al buscar en el Asistente para implementar software.

#### Nota

Cuando se establece el atributo **MSIRESTARTMANAGERCONTROL** en **Falso**, la implementación de Citrix Receiver para Windows con SCCM puede fallar.  
Según nuestros análisis, Citrix Receiver para Windows NO es la causa de este fallo. Además, la implementación puede ser correcta en el siguiente intento.

## Implementar Citrix Receiver para Windows desde una pantalla de inicio de sesión de la Interfaz Web

November 16, 2018

Esta función solo está disponible para versiones de XenDesktop y XenApp que respaldan la Interfaz Web.

Es posible implementar Citrix Receiver para Windows desde una página Web para que los usuarios lo tengan instalado antes de que intenten utilizar la Interfaz Web. La Interfaz Web ofrece un proceso de detección e instalación de clientes que detecta los clientes Citrix que pueden instalarse en el entorno de cada usuario y, posteriormente, guía a los usuarios a través del proceso de instalación.

Puede configurar el proceso de detección e instalación de clientes para que se ejecute automáticamente cuando los usuarios accedan a un sitio Web de XenApp. Si la Interfaz Web detecta que un

usuario no dispone de una versión compatible de Citrix Receiver para Windows, se solicita al usuario que descargue e instale Citrix Receiver para Windows.

La detección de cuentas basada en correo electrónico no se aplica cuando Citrix Receiver para Windows se implementa desde la Interfaz Web. Si la detección de cuentas basada en correo electrónico está configurada y un usuario nuevo instala Citrix Receiver para Windows desde Citrix.com, Citrix Receiver para Windows pide al usuario una dirección de correo electrónico o de servidor. Al introducir una dirección de correo electrónico, se recibe un mensaje de error similar al siguiente: **Su dirección de correo electrónico no puede usarse para agregar una cuenta.** Use la siguiente configuración para que solo se pida la dirección del servidor.

1. Descargue CitrixReceiver.exe en el equipo local.
2. Cambie el nombre de CitrixReceiver.exe por CitrixReceiverWeb.exe.
3. Especifique el nuevo nombre de archivo en el parámetro ClientIcaWin32, en los archivos de configuración de los sitios Web de XenApp.

Para utilizar el proceso de detección e instalación de clientes, los archivos de instalación de Citrix Receiver para Windows deben estar disponibles en el servidor de la Interfaz Web. De forma predeterminada, la Interfaz Web asume que los archivos de instalación de Citrix Receiver para Windows son los mismos que los archivos suministrados en los medios de instalación de XenApp o XenDesktop.

4. Agregue los sitios desde donde descargará el archivo CitrixReceiverWeb.exe a la zona de sitios de confianza.
5. Distribuya el ejecutable con el nuevo nombre usando su método de distribución habitual.

## Instalar y desinstalar manualmente Citrix Receiver para Windows

October 5, 2018

Citrix Receiver para Windows puede instalarse desde los medios de instalación, un recurso compartido de red, Windows Explorer o la línea de comandos ejecutando manualmente el paquete de instalación CitrixReceiver.exe. Para ver los parámetros de la línea de comandos y los requisitos de espacio, consulte [Configurar e instalar Receiver para Windows mediante parámetros de línea de comandos](#).

### Validar el espacio libre en disco

Citrix Receiver para Windows hace una comprobación para determinar si hay suficiente espacio en disco disponible para completar la instalación. La verificación se lleva a cabo tanto si se trata de una instalación nueva como si es una actualización.

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

Cuando se está actualizando Citrix Receiver para Windows, la instalación termina cuando no hay suficiente espacio en el disco y aparece el siguiente diálogo.

alt\_text

La siguiente tabla describe en el espacio mínimo necesario en el disco para instalar Citrix Receiver para Windows.

---

Tipo de instalación	**Espacio de disco requerido **
Instalación nueva	320 MB
Actualización de Citrix Receiver	206 MB

---

#### Nota

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

## Desinstalar Citrix Receiver para Windows

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

#### Nota

Recibirá un mensaje para desinstalar el paquete Citrix HDX RTME antes de continuar con la instalación de Citrix Receiver para Windows. Para obtener más información, consulte el artículo [CTX200340](#) de Knowledge Center.

## Para desinstalar Citrix Receiver para Windows mediante la interfaz de línea de comandos

También es posible desinstalar Citrix Receiver para Windows desde una línea de comandos con el comando siguiente:

CitrixReceiver.exe /uninstall

Las claves de Registro que crearon receiver.adm/receiver.adml o receiver.admx permanecen en el directorio Software\Policies\Citrix\ICA Client en HKEY\_LOCAL\_MACHINE y HKEY\_LOCAL\_USER después de la desinstalación.

Al reinstalar Citrix Receiver para Windows, estas directivas podrían aplicarse y podrían provocar un comportamiento inesperado. Para quitar estas personalizaciones, elimínelas manualmente.

Para una desinstalación silenciosa de Receiver para Windows, ejecute el siguiente modificador de línea de comandos:

```
CitrixReceiver.exe \silent \uninstall
```

## Implementar mediante Active Directory y scripts de inicio de ejemplo

November 16, 2018

Se pueden usar scripts de directiva de grupo de Active Directory para realizar una pre-implementación de Citrix Receiver en sistemas basados en la estructura de organización de Active Directory. Citrix recomienda usar los scripts en lugar de extraer los archivos MSI, dado que los scripts permiten la instalación, actualización y desinstalación desde una sola ubicación, consolidar las entradas de Citrix en Programas y características, y facilitar la detección de la versión de Citrix Receiver que se va a implementar. Use el parámetro Scripts en la Consola de administración de directivas de grupo (GPMC) que se encuentra en Configuración del equipo o Configuración de usuario. Para obtener información general acerca de los scripts de inicio, consulte la documentación de Microsoft.

Citrix incluye ejemplos de scripts de inicio por equipos para instalar y desinstalar CitrixReceiver.exe. Los scripts se encuentran en la página de [descarga](#) de Citrix Receiver para Windows.

- CheckAndDeployReceiverPerMachineStartupScript.bat
- CheckAndRemoveReceiverPerMachineStartupScript.bat

Cuando los scripts se ejecutan al inicio o cierre de una directiva de grupo de Active Directory, se pueden crear archivos de configuración personalizados en el perfil de usuario predeterminado (Default User) del sistema. Si no se eliminan, estos archivos de configuración pueden impedir que los usuarios accedan al directorio de registros de Receiver. Los scripts de ejemplo de Citrix incluyen funciones para eliminar correctamente dichos archivos de configuración.

### Para usar los scripts de inicio para distribuir Receiver con Active Directory

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

## Modificar los scripts de ejemplo

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

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

## Para agregar scripts de inicio de equipo

1. Abra la Consola de administración de directivas de grupo.
2. Seleccione Configuración del equipo > Directivas > Configuración de Windows > Scripts (inicio o apagado).
3. En el panel de la derecha de la Consola de administración de directivas de grupo, seleccione Inicio.
4. En el menú Propiedades, haga clic en Mostrar archivos, copie el script apropiado a la carpeta que se muestra y después cierre la ventana.
5. En el menú Propiedades, haga clic en Agregar y use la opción Examinar para buscar y agregar los scripts recientemente creados.

## Para distribuir Citrix Receiver para Windows por equipos

1. Mueva los dispositivos de usuario designados para recibir esta distribución a la unidad organizativa creada.
2. Reinicie el dispositivo de usuario e inicie una sesión como cualquier usuario.
3. Verifique que Programas y características (Agregar o quitar programas en versiones anteriores del sistema operativo) contiene el paquete recientemente instalado.

### **Para quitar Citrix Receiver para Windows por equipos**

1. Mueva los dispositivos de usuario designados para la eliminación a la unidad organizativa creada.
2. Reinicie el dispositivo de usuario e inicie una sesión como cualquier usuario.
3. Compruebe que Programas y características (Agregar o quitar programas en versiones anteriores del sistema operativo) haya quitado el paquete anteriormente instalado.

### **Usar los scripts de inicio de ejemplo por usuario**

Citrix recomienda usar scripts de inicio por equipo. En caso de implementaciones para Windows por usuario (en lugar de por máquina), se incluyen dos scripts de Citrix Receiver para Windows en los medios de instalación de XenDesktop y XenApp, en la carpeta Citrix Receiver for Windows and Plugins\Windows\Receiver\Startup\_Logon\_Scripts.

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

### **Para configurar scripts de inicio por usuario**

1. Abra la Consola de administración de directivas de grupo.
2. Seleccione Configuración de 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. En el menú Propiedades de inicio de sesión, haga clic en Mostrar archivos, copie el script apropiado a la carpeta que se muestra y después cierre la ventana.
5. En el menú Propiedades de inicio de sesión, haga clic en Agregar y use la opción Examinar para buscar y agregar los scripts recientemente creados.

### **Para implementar Citrix Receiver para Windows por usuarios**

1. Mueva los usuarios designados para recibir esta implementación a la unidad organizativa que ha creado.
2. Reinicie el dispositivo de usuario e inicie una sesión como el usuario especificado.
3. Verifique que Programas y características (Agregar o quitar programas en versiones anteriores del sistema operativo) contiene el paquete recientemente instalado.

### **Para quitar Citrix Receiver para Windows por usuarios**

1. Mueva los usuarios designados a la unidad organizativa creada.

2. Reinicie el dispositivo de usuario e inicie una sesión como el usuario especificado.
3. Compruebe que Programas y características (Agregar o quitar programas en versiones anteriores del sistema operativo) haya quitado el paquete anteriormente instalado.

## Implementar Citrix Receiver para Windows desde Receiver para Web

January 7, 2019

Puede implementar Citrix Receiver para Windows desde Citrix Receiver para Web si quiere que los usuarios lo tengan instalado antes de que intenten conectarse a una aplicación desde un explorador. Los sitios de Citrix Receiver para Web permiten a los usuarios acceder a almacenes o tiendas de StoreFront a través de una página Web. Si el sitio de Citrix Receiver para Web detecta que un usuario no dispone de una versión compatible de Citrix Receiver para Windows, se le solicita que descargue e instale Citrix Receiver para Windows.

Para obtener más información, consulte

[Sitios de Citrix Receiver para Web](#) en la documentación de StoreFront.

La detección de cuentas basada en correo electrónico no recibe respaldo cuando Citrix Receiver para Windows se implementa desde Citrix Receiver para Web. Si la detección de cuentas basada en correo electrónico está configurada y un usuario nuevo instala Citrix Receiver para Windows desde Citrix.com, Citrix Receiver para Windows pide al usuario una dirección de correo electrónico o de servidor. Al introducir una dirección de correo electrónico, se recibe un mensaje de error similar al siguiente: “Su dirección de correo electrónico no puede usarse para agregar una cuenta”.

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

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

## Configurar

January 7, 2019

Cuando se utiliza el software de Citrix Receiver para Windows, los siguientes pasos de configuración permiten a los usuarios acceder a sus aplicaciones y escritorios alojados:



- [Configurar la entrega de aplicaciones](#) y [Configurar el entorno de XenDesktop](#). Asegúrese de que el entorno de XenApp está configurado correctamente. Familiarícese con las opciones y ofrezca descripciones de las aplicaciones útiles para sus usuarios.
- [Configure el modo de autoservicio](#) agregando una cuenta de StoreFront a Citrix Receiver para Windows. Este modo permite a los usuarios suscribirse a aplicaciones desde la interfaz de usuario de Citrix Receiver para Windows.
- [Configurar mediante plantilla administrativa de objeto de directiva de grupo](#)
- [Proporcionar la información de cuentas a los usuarios](#). Proporcione a los usuarios la información que necesiten para configurar el acceso a las cuentas donde se alojan sus aplicaciones y escritorios virtuales. En algunos entornos, los usuarios deben configurar manualmente el acceso a las cuentas.

Para los usuarios que se conecten desde fuera de la red interna, configure la autenticación a través de NetScaler Gateway. Para obtener más información, consulte [Autenticar y autorizar](#) en la documentación de NetScaler Gateway.

## Configurar la entrega de aplicaciones

April 2, 2019

Cuando entregue aplicaciones con XenDesktop o XenApp, tenga en cuenta las siguientes opciones para mejorar la experiencia de los usuarios:

- **Modo de acceso Web.** Sin configuración, Citrix Receiver para Windows ofrece acceso basado en explorador Web a las aplicaciones y los escritorios. Puede abrir un explorador Web para ir a un sitio de Receiver para Web o sitio de Interfaz Web para seleccionar y usar las aplicaciones que desee. En este modo, no se colocan accesos directos en el escritorio del usuario.
- **Modo de autoservicio:** Cuando agrega una cuenta de StoreFront a Citrix Receiver para Windows o lo configura para que apunte a un sitio de StoreFront, puede definir un *modo de autoservicio*. Este modo permite a los usuarios suscribirse a las aplicaciones desde la interfaz de usuario de Citrix Receiver para Windows. Esta experiencia de usuario mejorada es similar al uso de un almacén o 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, Citrix Receiver para Windows le permite seleccionar las aplicaciones que quiera mostrar en su menú Inicio.

- **Modo de accesos directos solamente:** Como administrador de Citrix Receiver para Windows, puede configurar Citrix Receiver para Windows para que coloque automáticamente los accesos directos de aplicaciones y escritorios en el menú Inicio o en el escritorio, de una manera similar

al modo en que lo hace Citrix Receiver para Windows 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 acerca de la entrega de aplicaciones mediante XenApp y XenDesktop 7, consulte [Creación de una aplicación para un grupo de entrega](#).

#### **Nota**

Cuando actualiza o instala Citrix Receiver para Windows por primera vez, debe agregar los archivos de plantilla más recientes al GPO local.

## **Configurar una tienda de NetScaler Gateway**

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

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

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

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
2. En el nodo “Configuración del equipo”, vaya a **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > StoreFront**.
3. Seleccione “Lista de cuentas de StoreFront/URL de NetScaler Gateway”.
4. Modifique los parámetros.
  - Nombre de la tienda: El nombre de tienda que verá el usuario.
  - URL de la tienda: La dirección URL de la tienda.
  - #Nombre de la tienda: El nombre de la tienda detrás de NetScaler Gateway.
  - Habilitación de la tienda: El estado de la tienda (Habilitada o Inhabilitada).
  - Descripción de la tienda: Una descripción de la tienda.
5. Agregue o especifique la URL de NetScaler. Introduzca el nombre de la dirección URL separada por punto y coma:

**Ejemplo:** [HRStore](#) TiendaRRHH; name; Activado; Tienda para el personal de RRHH

Donde #Store name es el nombre de la tienda detrás de NetScaler Gateway y dtls.blrwinrx.com es la dirección URL de NetScaler.

Cuando inicie Citrix Receiver para Windows tras haber agregado el NetScaler Gateway utilizando el objeto de directiva de grupo, aparecerá el siguiente mensaje en el área de notificaciones.

## Limitaciones

1. La URL de NetScaler debe incluirse la primera, seguida de direcciones URL de StoreFront.
2. No se admiten varias URL de NetScaler.
3. Cualquier cambio en la URL de NetScaler requiere que Citrix Receiver para Windows se restablezca para que los cambios surtan efecto.
4. La URL de NetScaler Gateway configurada con este método no admite el sitio de servicios de PNA detrás de NetScaler Gateway.

## Configurar el modo de autoservicio

Simplemente agregando una cuenta de StoreFront a Citrix Receiver o configurando Citrix Receiver para que apunte a un sitio de StoreFront, puede configurar el *modo de autoservicio*, que permite a los usuarios suscribirse a las aplicaciones desde la interfaz de usuario de Receiver. Esta experiencia de usuario mejorada es similar al uso de un almacén o tienda de aplicaciones móviles.

### Nota

De forma predeterminada, Citrix Receiver para Windows permite a los usuarios seleccionar las aplicaciones que quieran mostrar en su menú Inicio.

En el modo de autoservicio, se pueden configurar parámetros de palabra clave para aplicaciones provisionadas 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 ser eliminada de Citrix Receiver para Windows), 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 una tienda a una aplicación, agregue la cadena **KEYWORDS:Auto** a la descripción. Cuando los usuarios inicien sesión en la tienda, la aplicación se suministrará automáticamente sin necesidad de 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 mediante su incorporación a la lista Destacados de Citrix Receiver, agregue la cadena **KEYWORDS:Featured** a la descripción de la aplicación.

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

### Nota

Debe realizar cambios en las directivas de grupo antes de configurar una tienda. En cualquier momento que desee personalizar las directivas de grupo, restablezca Citrix Receiver, configure la directiva de grupo y vuelva a configurar la tienda.

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de `gpedit.msc`.
2. En el nodo “Configuración del equipo”, vaya a Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > Autoservicio.
3. Seleccione la directiva **Administrar modo Self-Service**.
  - a) Habilítela para ver la interfaz de usuario que ofrece la directiva de autoservicio.
  - b) Inhabilítela si quiere suscribirse manualmente a las aplicaciones. Esta opción oculta la interfaz de usuario de autoservicio.
4. Haga clic en Aplicar y, a continuación, en Aceptar.
5. En el nodo “Configuración del equipo”, vaya a Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > Autoservicio.
6. Seleccione la directiva **Administrar accesos directos de aplicaciones**.
7. Seleccione las opciones según sea necesario.
8. Haga clic en Aplicar y, a continuación, en Aceptar.
9. Reinicie Citrix Receiver para Windows 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 la siguiente configuración al archivo `web.config` en **C:\inetpub\wwwroot\Citrix\Roaming** en la sección **<annotatedServices>**:

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

- Para usar la ruta de categoría en el menú Inicio, UseCategoryAsStartMenuPath. Parámetros: “true” o “false” (predeterminado: true).

**Nota**

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

- Para establecer un único directorio para todos los accesos directos en el menú Inicio, use StartMenuDir. Parámetro: Valor de cadena, correspondiente al nombre de la carpeta donde se van a incluir los accesos directos.
- Para volver a instalar aplicaciones modificadas, use AutoReinstallModifiedApps. Parámetros: “true” o “false” (predeterminado: true).
- Para mostrar un único directorio para todos los accesos directos en el escritorio, use DesktopDir. Parámetro: Valor de cadena, correspondiente al nombre de la carpeta donde se van a incluir los accesos directos.
- Para no crear una entrada en el panel ‘Agregar o quitar programas’ del cliente, use DontCreateAddRemoveEntry. Parámetros: “true” o “false” (predeterminado: false).
- Para quitar los accesos directos y el icono de Receiver de una aplicación que previamente estuvo disponible en la tienda 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 </account>, en la primera sección de propiedades:

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

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

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

**Nota**

Los elementos de propiedad agregados antes de la etiqueta <clear /> pueden invalidarlos. Si lo desea, 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. Asegúrese de que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los otros servidores de la implementación. Una vez completado, [propague los cambios de configuración al grupo de servidores](#), para que se actualicen los demás servidores de la implementación.

## Usar parámetros por aplicación en XenApp y XenDesktop 7.x para personalizar las ubicaciones de los accesos directos de las aplicaciones

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

Si quiere establecer la ubicación de los accesos directos de modo que cada usuario las encuentre en el mismo lugar, use los parámetros 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 para Windows con <b>PutShortcutsInStartMenu=false</b> y habilite los parámetros por aplicación. <b>Nota:</b> Este parámetro solo se aplica a sitios de Interfaz Web.
---	---

---

### Nota

The **PutShortcutsInStartMenu=false** setting applies to both XenApp 6.5 and XenDesktop 7.x.

## Configurar parámetros por aplicación en XenApp 6.5

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

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

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

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

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

1. En Citrix Studio, busque la pantalla **Parámetros de la aplicación**.
2. En la pantalla **Parámetros de la aplicación**, seleccione **Entrega**. En esta pantalla, puede especificar cómo se entregarán las aplicaciones a los usuarios.
3. Seleccione el icono adecuado para la aplicación. Haga clic en **Cambiar** para ir a la ubicación del icono pertinente.
4. En el campo de **Categoría de la aplicación**, de forma optativa, puede especificar la categoría de Receiver en la que aparece la aplicación. Por ejemplo, si está agregando accesos directos a aplicaciones de Microsoft Office, escriba **Microsoft Office**.
5. Marque la casilla **Agregar acceso directo al escritorio del usuario**.
6. Haga clic en **Aceptar**.

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

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

Esta funcionalidad requiere una serie de pasos a seguir:

1. Cree el código auxiliar de cada aplicación en la máquina cliente.
2. Copie el código auxiliar de las aplicaciones en una ubicación común, accesible desde un recurso compartido de red.

3. Si es necesario, prepare una lista blanca, o firme el código auxiliar con un certificado de empresa.
4. Agregue una clave del Registro para dejar que Receiver 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 HKCU\Software\Citrix\Dazzle /v ReuseStubs /t REG\_SZ /d "true".
2. Use regedit para agregar HKLM\Software\Citrix\Dazzle /v ReuseStubs /t REG\_SZ /d "true". HKCU tiene preferencia sobre HKLM.

Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

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

1. En una máquina cliente cree ejecutables de código auxiliar para todas las aplicaciones. Para lograr esto, agregue todas las aplicaciones a la máquina mediante Receiver. Receiver generará los archivos ejecutables.
2. Después, tome los archivos stub de los ejecutables que encontrará en %APPDATA%\Citrix\SelfService. Solamente necesita los archivos .exe.
3. Copie los archivos ejecutables a un recurso compartido de red.
4. Ahora, para cada máquina cliente que se va a bloquear, establezca las siguientes claves del Registro:
  - a) Reg add HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG\_SZ /d "\\ShareOne\ReceiverStu
  - b) Reg add HKLM\Software\Citrix\Dazzle /v
  - c) CopyStubsFromCommonStubDirectory /t REG\_SZ /d "true". También es posible configurar estos parámetros en HKCU, si lo prefiere. HKCU tiene preferencia sobre HKLM.
  - d) Salga de Receiver y reinicielo para probar la configuración.

## Ejemplo de casos de uso

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



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

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

---

Si quiere que el usuario elija las aplicaciones que desea tener en su menú Inicio...	Configure Citrix Receiver en el modo de autoservicio. En este modo, también deberá configurar los parámetros de palabra clave <i>auto</i> (aprovisionada automáticamente) y <i>mandatory</i> (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 Citrix Receiver sin opciones y, a continuación, use parámetros para cada una de las aplicaciones que quiera mostrar en el escritorio. Use aplicaciones aprovisionadas automáticamente ( <i>auto</i> ) y obligatorias ( <i>mandatory</i> ), 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 Citrix Receiver sin configuración alguna y vaya a Citrix Receiver para Web o a la Interfaz Web. También puede configurar Citrix Receiver para el acceso de autoservicio sin colocar accesos directos en ningún lugar.

---

Si quiere evitar que Citrix Receiver coloque accesos directos de aplicaciones en el menú Inicio automáticamente...	Configure Citrix Receiver con <code>PutShortcutsInStartMenu=False</code> . Citrix Receiver no colocará aplicaciones en el menú Inicio, incluso en el modo de autoservicio, a menos que usted los coloque mediante los parámetros de cada aplicación.
--	--

---

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

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

---

Si quiere que Citrix Receiver coloque todos los accesos directos de las aplicaciones en el menú Inicio automáticamente...

Configure Citrix Receiver con `SelfServiceMode=False`. Todas las aplicaciones disponibles aparecerán en el menú Inicio.

Si quiere que se coloquen accesos directos de todas las aplicaciones en el escritorio...

Configure Citrix Receiver con `PutShortcutsOnDesktop = true`. Todas las aplicaciones disponibles aparecerán en el escritorio.

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

Configure Citrix Receiver 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 Citrix Receiver 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 Citrix Receiver coloca en el menú Inicio aparezcan en su categoría (carpeta) asociada...	Configure Citrix Receiver con UseCategoryAsStartMenuPath=True.
Si quiere que las aplicaciones que Citrix Receiver coloca en el menú Inicio aparezcan en una carpeta específica...	Configure Citrix Receiver con StartMenuDir=el nombre de la carpeta del menú Inicio.

---

### Quitar aplicaciones al cerrar la sesión o al salir

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

---

---

Si quiere que Citrix Receiver quite todas las aplicaciones al cerrar sesión...	Configure Citrix Receiver con RemoveAppsOnLogoff=True.
Si quiere que Citrix Receiver quite las aplicaciones al salir...	Configure Citrix Receiver 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 Citrix Receiver, añada la cadena de texto KEYWORDS:prefer="patrón". Esta característica se conoce como Acceso a aplicaciones locales.

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

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

**Nota**

La palabra clave “prefer” se aplica cuando Citrix Receiver se suscribe a una aplicación. Si se añade 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 Citrix Receiver, añada la cadena KEYWORDS:prefer=”patrón”. Esta característica se conoce como Acceso a aplicaciones locales.

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

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

Nota: La palabra clave “prefer” se aplica cuando Citrix Receiver se suscribe a una aplicación. Si se añade 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 <b>Word</b> 2010	Sí

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

- 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 XenDesktop.

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 las “Recomendaciones adicionales” en la sección [Optimizar la experiencia de usuario](#) de la documentación de StoreFront.

## Configurar StoreFront

April 2, 2019

Citrix StoreFront autentica una conexión con XenDesktop, XenApp y VDI-in-a-Box, y enumera y agrupa los escritorios y las aplicaciones disponibles en unas tiendas (antes llamados almacenes), a las que los usuarios acceden mediante Citrix Receiver para Windows.

Además de la configuración resumida en esta sección, es necesario configurar NetScaler 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).

### Sugerencia

Cuando se selecciona la opción para mostrar todas las tiendas, es posible que vea la antigua interfaz de usuario de StoreFront.

### Para configurar StoreFront

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

**Nota:**

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

## Administrar la reconexión del control del área de trabajo

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

**Precaución**

Si modifica el Registro de forma incorrecta, pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente 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 host del servidor XenApp. El escritorio publicado puede cambiar el comportamiento de Citrix Receiver para Windows.

Los parámetros posibles para la clave WSCReconnectMode de Citrix Receiver para Windows:

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

## Inhabilitar el control del espacio de trabajo para Citrix Receiver para Windows

Para inhabilitar el control del espacio de trabajo para Citrix Receiver para Windows, cree la siguiente clave:

HKEY\_CURRENT\_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 bits)

HKEY\_CURRENT\_USER\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\_CURRENT\_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle (64 bits)

HKEY\_CURRENT\_USER\SOFTWARE\Citrix\Dazzle (32 bits)

Nombre: **WSCReconnectMode**

Tipo: REG\_SZ

Información del valor: 0

#### **Nota**

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

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

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

#### **Advertencia**

Si modifica el Registro de forma incorrecta, pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

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

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



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

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

### Trabajar con accesos directos

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

#### Nota

Windows 8 u 8.1 no permiten la creación de carpetas anidadas dentro del menú Inicio. Las aplicaciones se mostrarán de forma individual o bajo la carpeta raíz, pero no en las subcarpetas de categorías definidas con XenApp.

- Puede agregar una marca `[/DESKTOPDIR="Dir_name"]` durante la instalación para reunir todos los accesos directos en una misma carpeta. Se admite el uso de `CategoryPath` para los accesos

directos de escritorio.

- La reinstalación automática de aplicaciones modificadas es una funcionalidad que se puede habilitar mediante la clave de Registro `AutoReInstallModifiedApps`. Cuando `AutoReInstallModifiedApps` está habilitada, los cambios que se hagan en los atributos de aplicaciones y escritorios publicados en el servidor se reflejarán en la máquina cliente. Cuando `AutoReInstallModifiedApps` está inhabilitada, los atributos de las aplicaciones y escritorios no se actualizan y los accesos directos no vuelven a aparecer al actualizar, si han sido eliminados del cliente. De manera predeterminada, `AutoReInstallModifiedApps` está habilitada. Consulte [Uso de las claves del Registro para personalizar las ubicaciones de los accesos directos de las aplicaciones](#).

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

### Nota

De forma predeterminada, las claves del Registro usan un formato de cadena.

Debe realizar cambios en las claves de Registro para configurar una tienda. Siempre que usted o un usuario quieran personalizar las claves de Registro, deben restablecer Receiver, configurar las claves del Registro y luego reconfigurar la tienda.

Claves de Registro para máquinas de 32 bits

Claves de Registro para máquinas de 64 bits

## Configurar accesos directos y opciones de reconexión mediante la interfaz gráfica del usuario

### Nota

Los accesos directos solo se pueden configurar para las aplicaciones y los escritorios suscritos.

Puede ocultar total o parcialmente las opciones de la hoja de **Preferencias avanzadas**, disponible en el icono de Citrix Receiver en el área de notificación. Para obtener más información, consulte [Ocultar la hoja de Preferencias avanzadas](#).

1. Inicie una sesión en Citrix Receiver para Windows.
2. Haga clic con el botón secundario en el icono de Citrix Receiver para Windows situado en el área de notificaciones y, a continuación, haga clic en **Preferencias avanzadas**. Aparecerá la ventana Preferencias avanzadas.
3. Haga clic en **Opción de parámetros**.

### Nota

De forma predeterminada, está seleccionada la opción **Mostrar aplicaciones en el menú**

### Inicio.

4. Especifique el nombre de la carpeta. Con ello, todas las aplicaciones suscritas se moverán a la carpeta especificada en el menú Inicio. Las aplicaciones pueden agregarse tanto a una carpeta nueva como a una ya existente en el menú Inicio. Al habilitar esta característica, las aplicaciones recién agregadas y las existentes se agregan a la carpeta especificada.
5. Marque la casilla **Mostrar aplicaciones en el escritorio** en el panel **Opciones de escritorio**.
6. Especifique el nombre de la carpeta. Con ello, todas las aplicaciones suscritas se moverán a la carpeta especificada en el escritorio local.
7. Marque la casilla **Habilitar ruta diferente para el menú Inicio y el escritorio** en las opciones de **Categoría**. Con ello, se crea la carpeta de categorías y accesos directos para las aplicaciones como se define en el servidor de propiedades de las aplicaciones. Por ejemplo, aplicaciones de finanzas o del departamento de TI.

### Nota

De forma predeterminada, está seleccionada la opción **Categoría como ruta del menú Inicio**.

- i. Seleccione **Categoría como ruta del menú Inicio** para que las aplicaciones suscritas y su carpeta correspondiente de categorías aparezcan según se defina en el servidor de propiedades de las aplicaciones en el menú Inicio de Windows.
  - ii. Seleccione **Categoría como ruta del escritorio** para que las aplicaciones suscritas y su carpeta correspondiente de categorías aparezcan según se defina en el servidor de propiedades de las aplicaciones en el escritorio local.
8. Haga clic en **Aceptar**.

## Configurar opciones de reconexión mediante la interfaz gráfica de usuario

### Nota

Puede ocultar total o parcialmente las opciones de la hoja de Preferencias avanzadas, disponible en el icono de Citrix Receiver en el área de notificación. Para obtener más información, consulte [Ocultar la hoja de Preferencias avanzadas](#).

Después de iniciar sesión en el servidor, los usuarios pueden reconectarse a todos sus escritorios o aplicaciones en cualquier momento. De manera predeterminada, Opciones de reconexión abre las aplicaciones o los escritorios desconectados, además de los que estén ejecutándose en ese momento en otro dispositivo cliente. Puede configurar Opciones de reconexión para reconectar solo los escritorios o aplicaciones de los que se desconectó el usuario anteriormente.

1. Inicie una sesión en Citrix Receiver para Windows.

2. Haga clic con el botón secundario en el icono de Citrix Receiver para Windows situado en la bandeja del sistema y, a continuación, haga clic en **Preferencias avanzadas**. Aparecerá la ventana Preferencias avanzadas.
  3. Haga clic en **Opción de parámetros**.
  4. Haga clic en **Opciones de reconexión**.
  5. Seleccione **Habilitar para respaldo de control del espacio de trabajo** si quiere permitir que los usuarios se vuelvan a conectar a todos sus escritorios o aplicaciones en cualquier momento.
    - a) Seleccione **Reconectar con todas las sesiones activas y desconectadas** para permitir que los usuarios se vuelvan a conectar a las sesiones activas y desconectadas.
    - b) Seleccione **Reconectar solo con sesiones desconectadas** para permitir a los usuarios reconectarse solo a las sesiones desconectadas.
- Nota:
- El **Modo de reconexión admitido** adquiere el valor que esté definido en el objeto de directiva de grupo. Los usuarios pueden modificar esta opción desde **Plantillas administrativas > Componentes de Citrix > Citrix Receiver > Autoservicio > Controlar cuándo intenta Receiver reconectar con sesiones existentes**.
- Para modificar esta opción mediante el Registro, consulte el artículo [CTX136339](#) en Knowledge Center.
6. Haga clic en **Aceptar**.

## Configurar características y funciones

November 16, 2018

Una vez instalado Receiver para Windows, puede realizar los siguientes pasos de configuración para acceder a las aplicaciones y los escritorios alojados:

- Transporte adaptable: El transporte adaptable optimiza el transporte de datos mediante la aplicación de un nuevo protocolo de Citrix llamado Enlightened Data Transport (EDT), que se usa preferentemente en lugar de TCP, siempre que sea posible. Para obtener más información sobre cómo configurar el transporte adaptable, consulte [Configurar el transporte adaptable](#).
- Actualizaciones de Receiver: Ofrece actualizaciones automáticas de Receiver para Windows y del HDX Real Time Optimization Pack, sin necesidad de descargar las actualizaciones manualmente. Para obtener más información sobre la configuración de Actualizaciones de Receiver, consulte [Configurar Actualizaciones de Receiver](#).

- Redirección de contenido bidireccional: Permite habilitar o inhabilitar la redirección de direcciones URL entre el host y el cliente y viceversa. Para obtener información sobre cómo configurar la redirección de contenido bidireccional, consulte [Configurar la redirección de contenido bidireccional](#).
- Teclados Bloomberg: Pueden configurarse dispositivos USB especializados (por ejemplo, los teclados Bloomberg y Mouse 3D) para utilizar el respaldo de USB. Para obtener información sobre cómo configurar los teclados Bloomberg, consulte [Configurar teclados Bloomberg](#).
- Dispositivo USB compuesto: Un dispositivo USB compuesto realiza más de una función. Esto se logra mediante la exposición de cada una de esas funciones desde interfaces diferentes. Para obtener más información sobre cómo configurar el dispositivo USB compuesto, consulte [Configurar dispositivos USB compuestos](#).
- Respaldo para USB: Permite a los usuarios interactuar con una amplia variedad de dispositivos USB cuando se conectan a un escritorio virtual. Para obtener más información sobre cómo configurar el respaldo para USB, consulte [Configurar el respaldo para USB](#).

## Configurar el transporte adaptable

October 5, 2018

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

A partir de la versión 4.10, y con la fiabilidad de la sesión habilitada, EDT y TCP se intentan en paralelo durante la conexión inicial, la reconexión de fiabilidad de la sesión y la reconexión automática de clientes. Esta mejora reduce el tiempo de conexión cuando se prefiere EDT pero el transporte UDP subyacente necesario no está disponible y hay que recurrir a TCP.

De forma predeterminada, después de recurrir a TCP, el transporte adaptable sigue buscando EDT cada 5 minutos.

### Requisitos

- XenApp y XenDesktop 7.12 o una versión posterior (necesario para habilitar la función mediante Citrix Studio).
- StoreFront 3.8.
- Solo agentes VDA IPv4. No se admiten configuraciones de IPv6 ni mixtas (de IPv4 e IPv6).
- Agregue reglas de firewall para permitir el tráfico entrante en los puertos UDP 1494 y 2598 del VDA.

#### Nota

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

El transporte adaptable debe configurarse en el VDA aplicando la directiva antes de poder utilizarlo para la comunicación entre el VDA y Citrix Receiver.

De forma predeterminada, el transporte adaptable está permitido en Citrix Receiver para Windows. Sin embargo, también de forma predeterminada, el cliente intenta usar el transporte adaptable solo si el VDA está configurado como **Preferido** en la directiva de Citrix Studio y si se ha aplicado la configuración en el VDA.

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

Si quiere inhabilitar el transporte adaptable en un cliente específico, establezca las opciones de EDT como corresponda usando la plantilla administrativa del objeto de directiva de grupo de Citrix Receiver.

#### Para configurar el transporte adaptable con la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver

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

#### Nota

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

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
2. En el nodo "Configuración del equipo", vaya a **Plantillas administrativas > Citrix Receiver > Enrutamiento de red**.
3. Defina la directiva **Protocolo de transporte para Receiver** como **Habilitada**.
4. Seleccione el **protocolo de comunicación para Citrix Receiver** como convenga.
  - **Desactivado:** Se usará TCP para la transferencia de datos.
  - **Preferido:** Citrix Receiver intenta conectar con el servidor mediante el protocolo UDP en primer lugar y, si no puede, recurre a TCP como alternativa.
  - **Activado:** Citrix Receiver se conecta con el servidor solo mediante el protocolo UDP. Con esta opción, no existe la alternativa de recurrir a TCP.

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

6. Desde una línea de comandos, ejecute el comando `gpupdate /force`.

Además, para que tenga efecto la configuración de transporte adaptable, se requiere que el usuario agregue los archivos de plantilla de Citrix Receiver para Windows a la carpeta de definiciones de directivas. Para obtener información sobre cómo agregar los archivos de plantilla ADMX o ADML al objeto de directiva de grupo local, consulte [Configurar Citrix Receiver para Windows con la plantilla administrativa de objeto de directiva de grupo](#).

Para confirmar que la configuración de directiva surte efecto:

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

## Configurar la compatibilidad con USB

April 2, 2019

El respaldo USB permite interactuar con una amplia variedad de dispositivos USB cuando se está conectado con un escritorio virtual. 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. Los usuarios de Desktop Viewer pueden controlar si los dispositivos USB se encuentran disponibles en el escritorio virtual utilizando una preferencia de la barra de herramientas.

Las funciones isócronas de los dispositivos USB (como cámaras web, micrófonos, altavoces y auriculares) se admiten en entornos LAN típicos de baja latencia y alta velocidad. Esto permite a estos dispositivos interactuar con paquetes tales como Microsoft Office Communicator y Skype.

Los siguientes tipos de dispositivos reciben respaldo directamente en una sesión XenApp y XenDesktop, y por lo tanto no utilizan respaldo USB:

- Teclados
- Mouse
- Tarjetas inteligentes

### Nota

Los dispositivos USB especializados (por ejemplo, los teclados Bloomberg y mouse 3D) pueden configurarse para utilizar el respaldo USB. Para obtener información sobre cómo configurar los teclados Bloomberg, consulte

[Configuración de 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, ciertos tipos de dispositivos USB no reciben respaldo para comunicaciones remotas a través de XenDesktop y XenApp. 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 tienen respaldo predeterminado para ser utilizados en una sesión de XenDesktop:

- Dispositivos Bluetooth
- Tarjetas de interfaz de red integradas
- Concentradores 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 tienen respaldo predeterminado para ser utilizados en una sesión de XenApp:

- Dispositivos Bluetooth
- Tarjetas de interfaz de red integradas
- Concentradores USB
- Adaptadores gráficos USB
- Dispositivos de sonido
- Dispositivos de almacenamiento masivo

Para obtener instrucciones sobre cómo modificar la gama de dispositivos USB disponibles para los usuarios, consulte [Actualizar la lista de dispositivos USB disponibles para la comunicación remota](#).

Para obtener instrucciones sobre la redirección automática de dispositivos USB específicos, consulte el artículo [CTX123015](#) en Knowledge Center.

## **Funcionamiento del respaldo USB**

Cuando un usuario conecta un dispositivo USB, éste se comprueba con la directiva USB y, si se lo admite, se lo coloca en comunicación remota con el escritorio virtual. Si la directiva predeterminada rechaza el dispositivo, sólo estará disponible para el escritorio local.

Cuando un usuario conecta un dispositivo USB, se muestra una notificación para informar al usuario sobre el nuevo dispositivo. El usuario puede decidir qué dispositivos USB se comunican de forma remota con el escritorio virtual seleccionando los dispositivos de la lista cada vez que se conectan. También, el usuario puede configurar el respaldo 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 uso.



## Dispositivos de almacenamiento masivo

Solo para dispositivos de almacenamiento masivo, además del respaldo USB, el acceso remoto está disponible mediante la asignación de unidades del cliente, que configura a través de la siguiente directiva de Citrix Receiver: Comunicación remota de dispositivos cliente > Asignación de unidades de cliente. Cuando se aplica esta directiva, en el momento en que los usuarios inician sesión, las unidades del dispositivo del usuario se asignan automáticamente a las letras de las unidades del escritorio virtual. Las unidades se muestran como carpetas compartidas con letras de unidades asignadas.

Las principales diferencias entre los dos tipos de directivas de comunicación remota son las siguientes:

Función	Asignación de unidades del cliente	Compatibilidad con USB
Habilitada de forma predeterminada	Sí	No
Configuración para acceso de sólo 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 notificación

Si se habilitan las directivas de USB genérico y de asignación de unidades del cliente, y se inserta un dispositivo de almacenamiento masivo antes del inicio de una sesión, se lo redirigirá primero mediante la asignación de unidades del cliente antes de ser considerado para la redirección de USB genérico. Si se inserta después del inicio de una sesión, se redirigirá a través de la compatibilidad con USB antes de la asignación de unidades del cliente.

## Clases de dispositivos USB que se admiten de manera predeterminada

Las reglas de directivas USB predeterminadas admiten distintas clases de dispositivos USB:

A pesar de que se encuentran enumeradas en esta lista, algunas clases están solo disponibles de forma remota en las sesiones de XenDesktop y XenApp después de una configuración adicional. Estos parámetros no se pueden configurar.

- **Sonido (clase 01).** Incluye los dispositivos de entrada de sonido (micrófonos), los dispositivos de salida de sonido y los controladores MIDI. Los dispositivos de sonido modernos generalmente utilizan transferencias isócronas, que son compatibles con XenDesktop 4 o posterior.

El audio (clase 01) no es aplicable a XenApp, ya que estos dispositivos no están disponibles para la comunicación remota en XenApp mediante el respaldo 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”. Estos incluyen joystick con fuerza de respuesta, plataformas de movimiento y exoesqueletos con fuerza de respuesta.
- **Digitalización de imágenes fijas (clase 06).** Abarca los escáneres y las cámaras digitales. Las cámaras digitales suelen admitir la clase de digitalización de imagen fija que utiliza el protocolo de transferencia de imágenes (PTP) o el protocolo de transferencia multimedia (MTP) para transferir imágenes a un equipo u otro dispositivo periférico. Las cámaras también pueden aparecer como dispositivos de almacenamiento masivo y puede ser posible configurar una cámara para que utilice cualquiera de las clases mediante los menús de configuración que proporciona la cámara propiamente dicha.

#### Nota

Si una cámara aparece como un dispositivo de almacenamiento masivo, se utiliza la asignación de unidades del cliente y no se requiere respaldo 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 el respaldo 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 incluyen las unidades de disco duro con conexión USB, las unidades de CD/DVD y los lectores de tarjetas SD/MMC. Existe una amplia variedad de dispositivos con almacenamiento interno que también presentan una interfaz de almacenamiento masivo y que incluyen los reproductores multimedia, las cámaras digitales y los teléfonos celulares. El almacenamiento masivo (clase 08) no es aplicable a XenApp, ya que

estos dispositivos no están disponibles para la comunicación remota en XenApp mediante el respaldo 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 utiliza esta variante de SCSI

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

### Importante

Algunos virus se propagan en forma activa utilizando todos los tipos de almacenamiento masivo. Considere cuidadosamente si existe o no una necesidad comercial de permitir el uso de los dispositivos de almacenamiento masivo, ya sea a través de la asignación de unidades del cliente o mediante el respaldo USB.

- **Seguridad del contenido (clase 0d).** Los dispositivos para seguridad del contenido aplican la protección del contenido, generalmente para la administración de derechos digitales o para la gestión de licencias. Esta clase incluye las llaves.
- **Vídeo (clase 0e).** La clase vídeo abarca los dispositivos que se utilizan para controlar vídeos o material relacionado con vídeos, como las cámaras web, videograbadoras digitales, convertidores de vídeo analógico, algunos sintonizadores de televisión y algunas cámaras digitales que admiten la transmisión por secuencias de vídeo.

### Importante

La mayoría de los dispositivos de streaming por vídeo utilizan transferencias isócronas, que son compatibles con XenDesktop 4 o posterior. Algunos dispositivos de vídeo (por ejemplo, cámaras Web con detección de movimiento) requieren una configuración adicional. Para obtener instrucciones, consulte el artículo [CTX123015](#) de Knowledge Center.

- **Atención médica personal (clase 0f).** Estos dispositivos incluyen los dispositivos de atención médica personal como los sensores de presión arterial, los monitores de frecuencia cardíaca, podómetros, monitores de píldoras y espirómetros.
- **Específico del proveedor y de la aplicación (clases fe y ff).** Muchos dispositivos utilizan protocolos específicos del proveedor o protocolos no estandarizados por el consorcio USB, que generalmente se muestran como específicos del proveedor (clase ff).

## Clases de dispositivos USB que se rechazan de manera predeterminada

Las siguientes clases de dispositivo USB se rechazan por las reglas de directiva de USB predeterminadas:

- Comunicaciones y control CDC (clases 02 y 0a). La directiva USB predeterminada no permite estos dispositivos porque es posible que uno de ellos proporcione la conexión al propio escritorio virtual.
- Dispositivos de interfaz humana (HID) (clase 03). Incluye una amplia variedad de dispositivos de entrada y de salida. Los dispositivos de interfaz humana (HID, por su sigla en inglés) típicos son los teclados, los mouse, los dispositivos señaladores, las tabletas gráficas, los controladores de juegos, los botones y las funciones de control.

La subclase 01 se conoce como la clase de “interfaz de arranque” y se utiliza para los teclados y mouse.

La directiva USB predeterminada no permite teclados USB (clase 03, subclase 01, protocolo 1) ni mouse USB (clase 03, subclase 01, protocolo 2). Esto se debe a que la mayoría de los teclados y mouse se gestionan de manera apropiada sin respaldo USB y a que normalmente es necesario utilizar estos dispositivos de forma local y de forma remota cuando se conecta con un escritorio virtual.

- Concentradores USB (clase 09). Los concentradores USB permiten conectar dispositivos adicionales al equipo local. No es necesario acceder a estos dispositivos de forma remota.
- Tarjeta inteligente (clase 0b). Los lectores de tarjeta inteligente abarcan los lectores de tarjeta inteligente con contacto y sin contacto, y los tokens USB con un chip inteligente incluido que equivale a la tarjeta.

Se accede a los lectores de tarjeta inteligente utilizando la comunicación remota de la tarjeta inteligente y no se requiere respaldo USB.

- Controlador inalámbrico (clase e0). Es posible que algunos de estos dispositivos proporcionen acceso de red crítico o conecten periféricos importantes, tales como mouse o teclados Bluetooth.

La directiva USB predeterminada no permite estos dispositivos. No obstante, es posible que haya dispositivos concretos para los que sea apropiado dar acceso usando el respaldo USB.

- **Varios dispositivos de red (Clase ef, subclase 04)**. Es posible que algunos de estos dispositivos proporcionen acceso de red crítico. La directiva USB predeterminada no permite estos dispositivos. No obstante, es posible que haya dispositivos concretos para los que sea apropiado dar acceso usando el respaldo USB.

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

Puede actualizar el rango de dispositivos USB disponibles para la comunicación remota con los escritorios. Para ello, deberá modificar el archivo de plantilla de Citrix Receiver para Windows. Con ello, puede realizar cambios en el sitio de Citrix Receiver para Windows mediante la directiva de grupo. El archivo se localiza en la carpeta de instalación siguiente:

<unidad raíz>:\Archivos de programa\Citrix\ICA Client\Configuration\<idioma>

O bien, se puede editar el Registro en cada dispositivo de usuario, agregando la siguiente clave de Registro:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Name="DeviceRules"  
Value=

Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

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 las reglas y su sintaxis, consulte el artículo [CTX119722](#) de Knowledge Center.

## Configurar el sonido USB

### Nota

- Cuando actualiza o instala Citrix Receiver para Windows por primera vez, debe agregar los archivos de plantilla más recientes al GPO local. Para obtener más información sobre cómo agregar archivos de plantilla al GPO local, consulte [Configurar la plantilla administrativa de objeto de directiva de grupo](#). En caso de una actualización, la configuración existente se conserva al importar los archivos más recientes.
- Esta característica solo está disponible en el servidor XenApp.

## Para configurar dispositivos de audio USB por usuario

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.

2. En el nodo “Configuración del equipo”, vaya a **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > Experiencia de usuario**, y seleccione **Audio a través de redirección USB genérica**.
3. Modifique los parámetros.
4. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
5. Abra el símbolo del sistema en modo de administrador.
6. Ejecute el comando siguiente:  
`gpupdate /force.`

## Configurar la redirección de dispositivos USB compuestos

November 16, 2018

### Configurar la redirección de dispositivos USB compuestos usando la plantilla administrativa de objeto de directiva de grupo (GPO)

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de `gpedit.msc`.
2. En el nodo “Configuración del usuario”, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Receiver > Uso remoto de dispositivos cliente > Uso remoto de USB genérico**.
3. Seleccione la directiva **Dividir dispositivos**.
4. Seleccione **Habilitada**.
5. Haga clic en **Aplicar**.
6. Haga clic en **Aceptar** para guardar la directiva.

### Para permitir o rechazar el uso de una interfaz mediante la plantilla administrativa de objeto de directiva de grupo

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de `gpedit.msc`.
2. En el nodo “Configuración del usuario”, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Receiver > Uso remoto de dispositivos cliente > Uso remoto de USB genérico**.
3. Seleccione la directiva **Reglas de dispositivos USB**.
4. Seleccione **Habilitada**.
5. En el cuadro de texto **Reglas de dispositivos USB**, agregue el dispositivo USB que quiere permitir o denegar.

Por ejemplo, *ALLOW: vid=047F pid= C039 split=01 intf=00,03 // Se permiten las interfaces 00 y 03, y se restringen las demás.*

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

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

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

La siguiente tabla proporciona detalles sobre el comportamiento cuando se permite o se deniega una interfaz de USB.

#### Para permitir una interfaz:

Dividido	Interfaz	Acción
TRUE	Número válido 0 - n	Permitir la interfaz especificada
TRUE	Número no válido	Permitir todas las interfaces
FALSE	Cualquier valor	Permitir USB genérico del dispositivo principal
No especificado	Cualquier valor	Permitir USB genérico del dispositivo principal

Por ejemplo, *SplitDevices- true* indica que todos los dispositivos se dividen.

#### Para denegar una interfaz:

Dividido	Interfaz	Acción
TRUE	Número válido 0 - n	Denegar la interfaz especificada
TRUE	Número no válido	Denegar todas las interfaces
FALSE	Cualquier valor	Denegar USB genérico del dispositivo principal
No especificado	Cualquier valor	Denegar USB genérico del dispositivo principal

Por ejemplo, *SplitDevices- false* indica que los dispositivos no se dividen con el número de la interfaz especificado.

Ejemplo: Mis auriculares *\_<plantronics>*

## Número de interfaz

- Clase de interfaz de audio-0
- Clase de interfaz HID-3

Ejemplo de reglas que se usan para Mis auriculares\_ *plantronics*:

- ALLOW: vid=047F pid= C039 split=01 intf=00,03 //Se permiten las interfaces 00 y 03, y se restringen las demás
- DENY: vid=047F pid= C039 split=01 intf=00,03 // denegar 00 y 03

### Limitación:

Citrix recomienda que no dividida 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.

## Ocultar la hoja de Preferencias avanzadas

October 5, 2018

A partir de la versión 4.10, puede personalizar la disponibilidad y el contenido de la hoja **Preferencias avanzadas** que figura en el menú contextual del icono de Citrix Receiver en el 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
  - DPI alto
  - Información de asistencia
  - Accesos directos y reconexión

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

Puede ocultar la hoja “Preferencias avanzadas” utilizando la plantilla administrativa de objeto de directiva de grupo (GPO) de Citrix Receiver:



1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Receiver > 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 Citrix Receiver 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 de Preferencias avanzadas, utilizando la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver. Para ello:

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Receiver > Autoservicio > Opciones de Preferencias avanzadas**.
3. Seleccione la directiva para el parámetro que quiere ocultar.

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

- Configuration Checker
- Central de conexiones
- DPI alto
- Recopilación de datos
- Eliminar contraseñas guardadas
- Barra de idioma y teclado
- Accesos directos y reconexión
- Información de asistencia

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

Opciones	Acción
No configurado	Muestra el parámetro
Habilitada	Oculto el parámetro
Inhabilitada	Muestra el parámetro

## Ocultar la opción de Restablecer Receiver en la hoja de Preferencias avanzadas mediante el editor del Registro

Puede ocultar opción **Restablecer Receiver** en la hoja “Preferencias avanzadas” usando solamente el editor del Registro.

1. Abra el Editor del Registro.
2. Vaya a **HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Dazzle**
3. Cree una nueva clave de valor de cadena **EnableFactoryReset** y configúrela con cualquiera de las siguientes opciones:
  - a) True: Mostrará la opción de Restablecer Receiver en la hoja de Preferencias avanzadas
  - b) False: Ocultará la opción de Restablecer Receiver en la hoja de Preferencias avanzadas

## Ocultar la opción de Actualizaciones de Receiver en la hoja de Preferencias avanzadas

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

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Receiver > Actualizaciones de Receiver**.
3. Seleccione la directiva **Actualizaciones de Receiver**.
4. Seleccione **Inhabilitada** para ocultar los parámetros de “Actualizaciones de Receiver” en la hoja “Preferencias avanzadas”.

## Configurar teclados Bloomberg

October 5, 2018

Citrix Receiver para Windows respalda el uso de teclado Bloomberg en una sesión de XenApp y Xen-Desktop. Los componentes necesarios se instalan con el plug-in. Puede habilitar la función de teclado Bloomberg durante la instalación de Citrix Receiver para Windows o mediante el Registro.

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

## Para habilitar o inhabilitar el respaldo para teclado Bloomberg

### Precaución

Si se usa el Editor del Registro de forma incorrecta, se pueden generar problemas graves que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

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 **EnableBloombergHID** con el valor 1.
- Para inhabilitar esta función, establezca el valor en 0.

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

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

Si utiliza varias ventanas de Desktop Viewer, de manera predeterminada se atenúan los escritorios que no están activos. Si necesita ver varios escritorios de forma simultánea, esto puede hacer que la información que se incluye en ellos sea ilegible. Se puede desactivar el comportamiento predeterminado e impedir que la ventana de Desktop Viewer se atenúe editando el Registro.

Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

1. En el dispositivo de usuario, cree una entrada de Registro REG\_DWORD denominada DisabledDimming 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. Ya 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 con los parámetros de dispositivo o de usuario anteriores, puede definir una directiva local creando el mismo registro REG\_WORD en una de las siguientes claves:

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

El uso de estas claves es opcional porque los administradores de XenDesktop, en lugar de los usuarios o administradores de plug-ins, generalmente controlan los parámetros de la directiva mediante las directivas de grupo. Por lo tanto, antes de utilizar estas claves, compruebe si el administrador de XenDesktop ha establecido una directiva para esta función.

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

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

- a) HKEY\_CURRENT\_USER\Software\Policies\Citrix\...
- b) HKEY\_LOCAL\_MACHINE\Software\Policies\Citrix\...
- c) HKEY\_CURRENT\_USER\Software\Citrix\...
- d) HKEY\_LOCAL\_MACHINE\Software\Citrix\...

## Configurar la redirección de contenido bidireccional

April 2, 2019

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

1. Plantilla administrativa de objeto de directiva de grupo (GPO)
2. Registro

### Nota

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

### Para habilitar la redirección de contenido bidireccional usando la plantilla administrativa de GPO

Use la configuración de la plantilla administrativa de objeto de directiva de grupo para la primera instalación Citrix Receiver para Windows.

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.

2. En el nodo “Configuración del usuario”, vaya a **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > Experiencia de usuario**.
3. Seleccione la directiva Redirección de contenido bidireccional.
4. Modifique los parámetros.

#### Nota

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.

5. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
6. Desde una línea de comandos, ejecute el comando `gpupdate /force`.

### Para habilitar la redirección de contenido bidireccional mediante el Registro

Para habilitar la redirección de contenido bidireccional, ejecute el comando **redirector.exe /RegIE** desde la carpeta de instalación de Citrix Receiver para Windows (C:\Archivos de programa (x86)\Citrix\ICA Client).

### Limitación

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

#### Importante

- Asegúrese de que las reglas de redirección no resultan en un bucle. Por ejemplo, cuando las reglas del VDA se definen para que la URL [https://www.my\\_company.com](https://www.my_company.com) se redirija al cliente y también para que la misma URL se redirija al VDA, el resultado es un bucle.
- La función de redirección de URL solo admite direcciones URL explícitas (aquellas que aparecen en la barra de direcciones del explorador o las que se encuentran navegando dentro del explorador, según el explorador que se esté usando).
- Si hay dos aplicaciones con el mismo nombre simplificado que están configuradas para usar varias cuentas de StoreFront, el nombre simplificado de la cuenta principal de StoreFront se utiliza para lanzar la sesión de escritorio o de aplicación.
- Solo se abre una nueva ventana de explorador Web cuando la dirección URL se redirige al cliente. Cuando la dirección URL se redirige al VDA, si el explorador Web ya está abierto, la URL redirigida se abre en una nueva pestaña.
- Se da respaldo a enlaces incrustados en archivos como documentos, mensajes de correo electrónico y archivos PDF.

## Proporcionar información de cuentas a los usuarios

March 18, 2019

Proporcione a los usuarios la información de cuenta necesaria para que puedan acceder a sus escritorios y aplicaciones virtuales. Puede proporcionarles esta información de las siguientes formas:

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

### Importante

Citrix recomienda que reinicie Citrix Receiver para Windows después de la instalación. Esto es para garantizar que los usuarios pueden agregar cuentas y Citrix Receiver para Windows puede detectar los dispositivos USB que estaban suspendidos durante la instalación.

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

## Quitar el diálogo Agregar cuenta

El diálogo Agregar cuenta aparece cuando la tienda no está configurada. Los usuarios pueden utilizar esta ventana para configurar una cuenta de Citrix Receiver. Para ello, pueden escribir una dirección de correo electrónico o una URL de servidor.

Citrix Receiver para Windows determina el dispositivo NetScaler Gateway, el servidor StoreFront o el dispositivo virtual AppController asociado con la dirección de correo electrónico y pide al usuario que inicie sesión para la enumeración.

El diálogo Agregar cuenta se puede quitar de las siguientes formas:

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

Seleccione **No mostrar esta ventana automáticamente al iniciar la sesión** para evitar que la ventana Agregar cuenta aparezca como elemento emergente en el siguiente inicio de sesión. Este parámetro es específico para cada usuario y se restablece cuando se restablece Citrix Receiver para Windows.

### 2. Instalar desde la línea de comandos

Instale Citrix Receiver para Windows como administrador a partir de la interfaz de línea de comandos con el siguiente conmutador.

**CitrixReceiver.exe /ALLOWADDSTORE=N**

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

Aparecerá el siguiente mensaje si la tienda no está configurada.

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

#### Nota

Citrix recomienda que los usuarios quiten el cuadro de diálogo “Agregar cuenta” siguiendo los métodos del inicio de sesión del sistema o de la interfaz de línea de comandos.

- Cambiar el nombre del archivo de ejecución de Citrix:  
Cambie el nombre de **CitrixReceiver.exe** a **CitrixReceiverWeb.exe** para modificar el comportamiento del diálogo “Agregar cuenta”. Al cambiar el nombre del archivo, el diálogo “Agregar cuenta” no aparece en el menú Inicio.  
Consulte [Implementar Receiver para Windows desde Receiver para Web](#) para obtener más información relacionada con Citrix Receiver para Web.
- Objeto de directiva de grupo:  
Para ocultar el botón “Agregar cuenta” en el asistente de instalación de Citrix Receiver para Windows, inhabilite **EnableFTUpolicy** en el nodo Autoservicio del Editor de directivas de grupo como se muestra a continuación.  
Este es un parámetro por máquina; por tanto, el comportamiento se aplicará a todos los usuarios.  
Para cargar el archivo de plantilla, consulte [Configurar Receiver con la plantilla de objeto de directiva de grupo](#).

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

Cuando se configura Citrix Receiver para Windows 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 Citrix Receiver para Windows. Citrix Receiver para Windows determina el dispositivo NetScaler Gateway o el servidor StoreFront que está asociado con esa dirección de correo electrónico, en función de los registros de servicio (SRV) de sistema de nombres de dominio (DNS) y, posteriormente, solicita a los usuarios que inicien sesión para obtener acceso a sus aplicaciones y escritorios virtuales.

#### Nota

La detección de cuentas basada en correo electrónico no está respaldada en implementaciones con la Interfaz Web.

Para configurar NetScaler Gateway, consulte [Conectarse a StoreFront mediante la detección basada en correo electrónico](#) en la documentación de NetScaler Gateway.

## Proporcionar archivos de aprovisionamiento a los usuarios

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

Es posible utilizar StoreFront para crear archivos de aprovisionamiento que contengan los detalles de conexión de las cuentas. Estos archivos se ponen a disposición de los usuarios para que puedan configurar Citrix Receiver para Windows de forma automática. Después de instalar Citrix Receiver para Windows, los usuarios simplemente abren el archivo para configurar Citrix Receiver para Windows. Si se configuran sitios de Citrix Receiver para Web, los usuarios también pueden obtener los archivos de aprovisionamiento de Citrix Receiver para Windows desde esos sitios.

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

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

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

- Para las conexiones con una tienda o almacén de StoreFront, proporcione la dirección URL de ese servidor. Por ejemplo: <https://nombreservidor.empresa.com>.

Para implementaciones con Interfaz Web, proporcione la dirección URL del sitio de servicios XenApp.

- Para conexiones a través de NetScaler Gateway, primero determine si el usuario necesita ver todas las tiendas o almacenes configurados o solo la tienda que tiene habilitado el acceso remoto para un NetScaler Gateway concreto.
  - Para presentarles todas las tiendas configuradas, suministre a sus usuarios el nombre de dominio completo de NetScaler Gateway.
  - Para limitar el acceso a una tienda en concreto, suministre a sus usuarios el nombre de dominio completo de NetScaler Gateway y el nombre de la tienda, con el formato:


### **NetScalerGatewayFQDN?MyStoreName**

Por ejemplo, si tiene una tienda llamada “AplicacionesVentas” con acceso remoto habilitado para servidor1.com, y una tienda llamada “AplicacionesRRHH” con acceso remoto habilitado para servidor2.com, el usuario deberá introducir servidor1.com?AplicacionesVentas si quiere acceder AplicacionesVentas, o introducir servidor2.com?AplicacionesRRHH si quiere acceder a AplicacionesRRHH. Esta característica



requiere que el usuario cree una cuenta cuando usa el producto por primera vez, introduciendo una dirección URL, y no está disponible para la detección basada en correo electrónico.

Cuando un usuario introduce la información de una cuenta nueva, Citrix Receiver para Windows intenta verificar la conexión. Si se puede establecer la conexión, Citrix Receiver para Windows solicita al usuario que inicie sesión en la cuenta.

Para administrar cuentas, el usuario de Citrix Receiver debe abrir la página de inicio de Citrix Receiver para Windows, hacer clic en el  y luego hacer clic en **Cuentas**.

## Compartir automáticamente varias cuentas de tienda

### Advertencia

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

Si dispone de más de una cuenta de tienda, puede configurar Citrix Receiver para Windows para que se conecte automáticamente con todas las cuentas al establecer una sesión. Para ver automáticamente todas las cuentas al abrir Citrix Receiver para Windows:

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

Ubicación: HKLM\Software\Citrix\Dazzle

Nombre de la clave: CurrentAccount

Valor: AllAccount

Tipo: REG\_SZ

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

Ubicación: HKLM\Software\Wow6432Node\Citrix\Dazzle

Nombre de la clave: CurrentAccount

Valor: AllAccount

Tipo: REG\_SZ

## Configurar Actualizaciones de Citrix Receiver

February 20, 2019

Cuando configure la función Actualizaciones de Citrix Receiver en Citrix Receiver para Windows, siga los métodos siguientes en el orden de prioridad:

1. Plantilla administrativa de objeto de directiva de grupo (GPO)
2. Interfaz de línea de comandos
3. Preferencias avanzadas (por usuario)

### Nota

- Después de actualizar Citrix Receiver para Windows con la función Actualizaciones de Citrix Receiver, la ventana de inicio de sesión no aparece.
- Con esta versión, HDX RTME para Windows se incluye en las actualizaciones de Citrix Receiver. Se le notifica sobre la actualización de HDX RTME disponible tanto en las versiones LTSR como en las versiones Current Release de Citrix Receiver para Windows.

### Limitaciones:

1. Si ha configurado un proxy SSL interceptor de salida, debe agregar una excepción al servicio de firma de actualización automática de Receiver <https://citrixupdates.cloud.com> y la ubicación de descarga <https://downloadplugins.citrix.com>.
2. El sistema debe tener acceso a Internet.
3. Los usuarios de Receiver para Web no pueden descargar automáticamente la directiva de StoreFront.
4. De forma predeterminada, la función Actualizaciones de Citrix Receiver está inhabilitada en el VDA. Esto incluye máquinas de servidor multiusuario RDS, máquinas VDI y Remote PC.
5. La función Actualizaciones de Citrix Receiver está inhabilitada en máquinas donde esté instalado Desktop Lock.

### Configurar mediante la plantilla administrativa de objeto de directiva de grupo

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de `gpedit.msc`.
2. En el nodo “Configuración del equipo”, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Receiver > Actualizaciones de Receiver**.
3. Seleccione la directiva **Definir demora para comprobar actualizaciones**. Esta directiva permite organizar la implantación durante un periodo temporal.

4. Seleccione **Habilitada** y, en el menú desplegable **Demorar grupo**, seleccione alguna de las siguientes opciones:
  - **Fast (Rápido)**: La implantación de la actualización tiene lugar al comienzo del período de entrega.
  - **Medium (Medio)**: La implantación de la actualización tiene lugar hacia la mitad del período de entrega.
  - **Slow (Lento)**: La implantación de la actualización tiene lugar al final del período de entrega.

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

6. En la sección de plantillas de Actualizaciones de Receiver, seleccione la directiva **Actualizaciones de Receiver**.

#### Nota

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

7. Marque **Habilitada** y establezca los valores según sea necesario:
  - En la lista desplegable **Habilitar Actualización de Receiver**, seleccione una de las siguientes opciones:
    - **Auto**: Se le notificará cuando haya una actualización disponible (predeterminado).
    - **Manual**: No se le notificará cuando haya actualizaciones disponibles. Compruebe manualmente si hay actualizaciones.
  - Seleccione **SOLO LTSR** para obtener las actualizaciones para LTSR solamente.
  - En la lista desplegable **Auto-Update-DeferUpdate-Count**, seleccione un valor entre **-1** y **30**, donde
    - **-1**: Puede aplazar las notificaciones cualquier cantidad de veces (valor predeterminado = -1).
    - **0**: No se muestra la opción **Recordármelo más tarde**.
    - Cualquier otro número: La opción **Recordármelo más tarde** se muestra esa cantidad de veces. Por ejemplo, si establece el valor en 10, la opción **Recordármelo más tarde** aparecerá 10 veces.

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

## Configurar mediante la interfaz de línea de comandos

### Al instalar Citrix Receiver para Windows

Para configurar los parámetros de Actualizaciones de Citrix Receiver como administrador usando los parámetros de línea de comandos durante la instalación de Citrix Receiver:

- **/AutoUpdateCheck** = auto/manual/disabled
- **/AutoUpdateStream** = LTSR/Current. Donde, LTSR hace referencia a Long Term Service Release y Current hace referencia a la versión actual.
- **/DeferUpdateCount** = cualquier valor entre -1 y 30
- **/AURolloutPriority** = auto/fast/medium/slow

Por ejemplo `CitrixReceiver.exe /AutoUpdateCheck=auto /AutoUpdateStream=Current /DeferUpdateCount=-1 /AURolloutPriority=fast`

- Para configurar los parámetros de Actualizaciones de Citrix Receiver como usuario mediante los parámetros de línea de comandos durante la instalación de Citrix Receiver
  - **/AutoUpdateCheck=auto/manual**

Por ejemplo: `CitrixReceiver.exe /AutoUpdateCheck=auto`

Cuando se modifican los parámetros de Actualizaciones de Citrix Receiver usando la plantilla administrativa de objeto de directiva de grupo, se anulan los parámetros aplicados durante la instalación de Citrix Receiver para Windows para todos los usuarios.

## Después de instalar Citrix Receiver para Windows

Actualizaciones de Citrix Receiver se puede configurar después de instalar Citrix Receiver para Windows.

Para usar la línea de comandos:

Abra el símbolo del sistema de Windows y sitúese en el directorio donde se encuentra **CitrixReceiverUpdater.exe**. Por regla general, CitrixReceiverUpdater.exe se encuentra en `CitrixReceiverInstallLocal\Citrix\Ica Client\Receiver`.

También se puede establecer la directiva de línea de comandos de Actualizaciones de Citrix Receiver mediante este binario.

Por ejemplo: Los administradores pueden usar todas (las cuatro) opciones:

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

## Configurar mediante la interfaz gráfica de usuario

### Nota

Puede ocultar total o parcialmente las opciones de la hoja de Preferencias avanzadas, disponible en el icono de Citrix Receiver en el área de notificación. Para obtener más información, consulte [Ocultar la hoja de Preferencias avanzadas](#).

Un usuario individual puede anular la configuración de Actualizaciones de Citrix Receiver desde el 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 Citrix Receiver para Windows desde el área de notificaciones.
2. Seleccione **Preferencias avanzadas** y haga clic en **Actualizaciones de Receiver**.
3. Seleccione una de estas opciones:
  - Sí, notificarme
  - No, no notificarme
  - Usar parámetros especificados por el administrador
4. Haga clic en **Guardar**.

### Configurar Actualizaciones de Citrix Receiver usando StoreFront

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

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

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

```
1 <properties>
2 <clear />
3 </properties>
```

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

```
1 <account>
2
3     <clear />
4
5     <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="F84Store"
6
7         description="" published="true" updaterType="Citrix"
8             remoteAccessType="None">
9
10        <annotatedServices>
11
12        <clear />
```

```
12
13     <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
14
15         <metadata>
16
17             <plugins>
18
19                 <clear />
20
21             </plugins>
22
23             <trustSettings>
24
25                 <clear />
26
27             </trustSettings>
28
29             <properties>
30
31                 <property name="Auto-Update-Check" value="auto" />
32
33                 <property name="Auto-Update-DeferUpdate-Count" value="1"
34                     />
35
36                     <property name="Auto-Update-LTSR-Only" value="
37                         FALSE" />
38
39                 <property name="Auto-Update-Rollout-Priority" value="fast
40                     " />
41
42             </properties>
43
44         </metadata>
45
46     </annotatedServiceRecord>
47
48 </annotatedServices>
49
50 <metadata>
51
52     <plugins>
53
54         <clear />
55
56     </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>
```

### **auto-update-Check**

Este atributo indica que Citrix Receiver para Windows detecta cuándo hay una actualización disponible.

#### **Valores válidos:**

- Auto: Se le notificará cuando haya una actualización disponible (predeterminado).
- Manual: No se le notificará cuando haya actualizaciones disponibles. Compruebe manualmente si hay actualizaciones.
- Inhabilitada: La función Actualizaciones de Citrix Receiver está oculta y no se le notificará cuando haya una actualización disponible.

### **auto-update-LTSR-Only**

Este atributo indica que Citrix Receiver para Windows debe aceptar actualizaciones solo para LTSR.

#### **Valores válidos:**

- True: La función Actualizaciones de Citrix Receiver solo comprueba si hay actualizaciones LTSR de Citrix Receiver para Windows
- False: La función Actualizaciones de Citrix Receiver también comprueba si hay actualizaciones de Citrix Receiver para Windows que no solo sean de LTSR.

### **auto-update-DeferUpdate-Count**

Este atributo indica la cantidad de veces que se pueden aplazar las notificaciones. La opción **Recordármelo más tarde** se podrá mostrar tantas veces como indique este valor.

#### **Valores válidos:**

- -1: Puede aplazar las notificaciones cualquier cantidad de veces (valor predeterminado = -1).
- 0: No se muestra la opción “Recordármelo más tarde”.
- Cualquier otro número: La opción “Recordármelo más tarde” se muestra esa cantidad de veces. Por ejemplo, si establece el valor en 10, la opción Recordármelo más tarde aparecerá 10 veces.

### **auto-update-Rollout-Priority**

Este atributo indica el período que se puede configurar para la implantación.

#### **Valores válidos:**

- 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 periodo de entrega.
- Slow (Lento): La implantación de la actualización tiene lugar al final del período de entrega.

## **Configurar la plantilla administrativa de objeto de directiva de grupo**

April 2, 2019

Citrix recomienda usar el Editor de objetos de directiva de grupo (GPO) de Windows para configurar Citrix Receiver para Windows. Citrix Receiver para Windows incluye archivos de plantilla administrativa (receiver.adm o receiver.admx)\receiver.adml -dependiendo del sistema operativo) en el directorio de instalación.

#### **Nota**

- A partir de Citrix Receiver para Windows versión 4.6, el directorio de instalación incluye los archivos CitrixBase.admx y CitrixBase.adml.
- Citrix recomienda usar los archivos CitrixBase.admx y CitrixBase.adml para asegurarse de que las opciones se organizan y se muestran correctamente en el Editor de objetos de directiva de grupo.
- El archivo .adm solo se usa para plataformas Windows XP Embedded. Los archivos .adm/.adml se usan con Windows Vista/Windows Server 2008 y todas las versiones posteri-



ores de Windows.

- Si Citrix Receiver para Windows se instala con el VDA, los archivos admx/adml se encuentran en el directorio de instalación de Citrix Receiver para Windows. Por ejemplo: \Online Plugin\Configuration.
- Si Citrix Receiver para Windows se instala sin el VDA, los archivos admx/adml se suele encontrar en el directorio C:\Archivos de programa\Citrix\ICA Client\Configuration.

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

#### Nota

Citrix recomienda usar los archivos de plantilla de objetos de directiva de grupo proporcionados con la versión más reciente de Citrix Receiver para Windows.

Tipo de archivo	Ubicación del archivo
receiver.adm	\ICA Client\Configuration
receiver.admx	\ICA Client\Configuration
receiver.adml	\ICA Client\Configuration\[[MU]culture\]
CitrixBase.admx	\ICA Client\Configuration
CitrixBase.adml	\ICA Client\Configuration\[[MU]culture\]

#### Nota

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

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

#### Nota

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

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta **Plantillas administrativas**.
3. En el menú Acción, seleccione **Agregar o quitar plantillas**.
4. Seleccione Agregar y vaya a la ubicación del archivo de plantilla \ICA Client\Configuration\receiver.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.

El archivo de la plantilla de Citrix Receiver para Windows estará disponible en el objeto de directiva de grupo local, en **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver**.

Tras agregarse los archivos ADM de plantilla al GPO local, aparecerá el siguiente mensaje:

“The following entry in the strings section is too long and has been truncated:”

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

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

#### Nota

Puede utilizar archivos de plantilla ADMX o ADML para configurar los GPO locales y/o aquellos que utilizan dominios. Consulte el artículo de Microsoft MSDN acerca de la administración de archivos ADMX.

Después de instalar Citrix Receiver para Windows, copie los archivos de plantilla como se indica en la siguiente tabla:

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

### Nota

Los archivos de plantillas de Citrix Receiver para Windows están disponibles en el GPO local, en la carpeta Plantillas administrativas > Componentes de Citrix > Citrix Receiver solo cuando el usuario agrega los archivos CitrixBase.admx/CitrixBase.adml a la carpeta \policyDefinitions.

## Optimizar el entorno

October 5, 2018

Puede optimizar el entorno con las siguientes características:

- Respalda la configuración del espacio de trabajo
- Reducir el tiempo de inicio de las aplicaciones
- Asignar dispositivos del cliente
- Respalda la resolución de nombres DNS
- Usar servidores proxy en conexiones de XenDesktop

## Respalda la resolución de nombres DNS

October 5, 2018

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

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

Citrix Receiver para Windows que se conecta a aplicaciones publicadas a través de la Interfaz Web también usa Citrix XML Service. Para Citrix Receiver para Windows que se conecta a través de la Interfaz Web, el servidor Web resuelve el nombre DNS en nombre de Citrix Receiver para Windows.

La resolución de nombres DNS está inhabilitada de forma predeterminada en la comunidad de servidores y está habilitada de forma predeterminada en Citrix Receiver para Windows. Cuando la resolución de nombres DNS está inhabilitada en la comunidad, cualquier solicitud de Citrix Receiver para Windows de un nombre DNS devuelve una dirección IP. No es necesario desactivar la resolución de nombres DNS en Citrix Receiver para Windows.

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

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

### Precaución:

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

1. Agregue una clave de Registro **xmlAddressResolutionType** a HKEY\_LOCAL\_MACHINE\Software\Wow6432N 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.

## Usar servidores proxy con XenDesktop

February 20, 2019

Si no utiliza servidores proxy en su entorno, corrija los parámetros de proxy de Internet Explorer en los dispositivos de usuario que ejecutan Internet Explorer 7.0 con Windows XP. De manera predeterminada, esta configuración detecta automáticamente los parámetros de proxy. Si no se utilizan servidores proxy, los usuarios experimentarán demoras innecesarias durante el proceso de detección.

Para obtener instrucciones para modificar los parámetros de proxy, consulte la documentación de Internet Explorer. O bien, puede modificar los parámetros de proxy mediante la Interfaz Web. Para obtener más información, consulte la [documentación de la Interfaz Web](#).

## Asignar dispositivos cliente

January 7, 2019

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

- Tener acceso imperceptible a las unidades locales, impresoras y puertos COM.

- Cortar y pegar entre sesiones y el portapapeles de Windows local.
- Escuchar sonido (sonidos del sistema y archivos .wav) reproducido en la sesión.

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

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

### **Desactivar la asignación 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 mayor información sobre las opciones disponibles, consulte la documentación de Servicios de Terminal Server.

### **Redirigir carpetas del cliente**

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

Solo las carpetas especificadas por el usuario aparecerán como enlaces UNC dentro de las sesiones, en lugar de aparecer todo el sistema de archivos del dispositivo del usuario. Si se inhabilitan los enlaces UNC mediante el Registro, las carpetas del cliente aparecen como unidades asignadas dentro de la sesión. Para obtener más información sobre cómo configurar la redirección de carpetas del cliente para los dispositivos de usuario, consulte la documentación de XenDesktop 7.

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

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

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

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

---

Letra de unidad del cliente	El servidor accede a ella como:
A	A
N	N
C	V
D	S

---

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

---

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

---

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

Cuando un dispositivo cliente se conecta con un servidor, se restablecen las asignaciones del cliente

a menos que la asignación automática de dispositivos del cliente esté inhabilitada. La asignación de unidades del cliente está habilitada de forma predeterminada. Para cambiar esta configuración, use la herramienta de Configuración de Servicios de Escritorio remoto (Servicios de Terminal Server). Es también posible usar directivas para tener mayor control sobre cómo se aplica la asignación de dispositivos del cliente. Para obtener más información acerca de las directivas, consulte la documentación de XenDesktop o XenApp en la documentación del producto Citrix.

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

La redirección de dispositivos USB de HDX Plug-n-Play permite la redirección dinámica de varios dispositivos, incluyendo cámaras, escáneres, reproductores multimedia y dispositivos de punto de venta (POS) al servidor. Al mismo tiempo, se puede impedir la redirección de todos o algunos dispositivos. Edite 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 XenApp y XenDesktop.

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

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

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

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

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

**Importante:** La asignación de puertos COM no es compatible con TAPI.

1. En implementaciones de XenDesktop 7, habilite la configuración de directiva Redirección de puertos COM del cliente.
2. Inicie sesión en Citrix Receiver para Windows.
3. Escriba lo siguiente en una interfaz de comandos:

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

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

4. Para confirmar la operación, escriba:

```
net use
```

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

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

## Respaldo la configuración del espacio de trabajo

January 7, 2019

Citrix Receiver para Windows ofrece respaldo para la configuración de espacios de trabajo para suscriptores, que pueden estar usando uno o varios servicios disponibles en Citrix Cloud.

Un espacio de trabajo (Workspace) forma parte de una solución de espacio de trabajo digital que permite a los departamentos de TI entregar de manera segura un acceso a aplicaciones desde cualquier dispositivo.

Esta captura de pantalla es un ejemplo de un espacio de trabajo tal y como lo ven los suscriptores. El diseño de esta interfaz está evolucionando y es posible que no sea exactamente igual a la interfaz que estén usando actualmente sus suscriptores. Por ejemplo, puede figurar “StoreFront” en la parte superior de la página en lugar de “Workspace”.

Citrix Receiver para Windows y Receiver para Web respaldan actualmente la autenticación de Azure Active Directory.

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

## Reducir el tiempo de inicio de las aplicaciones

November 16, 2018



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

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

El inicio previo de sesiones está respaldado en implementaciones de StoreFront a partir de la versión StoreFront 2.0. En implementaciones con la Interfaz Web, asegúrese de usar la opción Guardar contraseña para evitar que aparezcan diálogos de inicio de sesión. El inicio previo de sesiones no está respaldado en implementaciones de XenDesktop 7.

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

Nota: Si la máquina cliente se ha configurado para dar respaldo a 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`.

Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Las ubicaciones en el Registro son:

`HKEY_LOCAL_MACHINE\Software\[Wow6432Node]\Citrix\Dazzle`

`HKEY_CURRENT_USER\Software\Citrix\Dazzle`

Existen dos tipos de inicio previo:

- **Inicio previo a petición.** El inicio previo se lleva a cabo inmediatamente después de que se autentican las credenciales del usuario, independientemente del tráfico de la red. Por lo general, se usa en periodos de tráfico normal. Un usuario puede provocar el preinicio reiniciando Citrix Receiver para Windows.

- **Inicio previo programado.** El inicio previo ocurre a una hora programada. El inicio previo programado ocurre solo cuando el dispositivo de usuario ya se está ejecutando y se ha autenticado. Si no se cumplen estas dos condiciones cuando llega la hora del inicio previo programado, no se inicia la sesión. La sesión se inicia en una ventana a la hora programada lo que permite distribuir la carga de red y del servidor. Por ejemplo, si el inicio previo se ha programado para la 13:45, la sesión en realidad se inicia entre la 13:15 y la 13:45. Esto se utiliza, por lo general, en periodos de mucho tráfico.

La configuración del inicio previo en el servidor XenApp consiste en crear, modificar o eliminar aplicaciones de inicio previo, así como actualizar las configuraciones de directivas de usuario que controlan el inicio previo de aplicaciones. Consulte “Para realizar el inicio previo de aplicaciones en los dispositivos de los usuarios” en la documentación de XenApp si quiere ver información sobre cómo configurar inicios previos de sesiones en el servidor XenApp.

No se admite usar el archivo receiver.admx para personalizar la función de preinicio. No obstante, se puede cambiar la configuración del preinicio modificando valores de Registro durante o después de la instalación de Citrix Receiver para Windows. Hay tres valores HKLM y dos valores HKCU:

- Los valores HKLM se escriben durante la instalación del cliente.
- Los valores HKCU permiten dar diferentes parámetros a los distintos usuarios de un mismo equipo. Los usuarios pueden cambiar los valores HKCU sin necesidad de permisos de administrador. Se pueden proporcionar scripts a los usuarios para lograr este resultado.

## Valores de Registro HKEY\_LOCAL\_MACHINE

Para Windows 7 y 8 de 64 bits: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

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

Nombre: UserOverride

Valores:

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

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

Nombre: State

Valores:

0: Inhabilita el inicio previo.

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

2: Habilita el inicio previo programado. (El preinicio ocurre a la hora configurada en Schedule.)

Nombre: Schedule

Valor:

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

HH:MM	M:T:W:TH:F:S:SU, donde HH y MM son 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 la 13:45, configure Schedule en Schedule=13:45	1:0:1:0:1:0:0 . La sesión en realidad se inicia entre la 1:15 p. m. y la 1:45 p. m.
-------	--	---

### 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.

## Mejorar la experiencia del usuario

May 23, 2019

Puede mejorar la experiencia del usuario en Citrix Receiver para Windows utilizando las siguientes características y funcionalidades:

- **Iniciar vPrefer**: Controla cómo se deben iniciar las aplicaciones publicadas en las sesiones de escritorio publicadas.
- **Codificación de vídeo H.265**: Ofrece una mejor compresión de datos (utiliza menos ancho de banda) sin sacrificar la calidad de la imagen o la calidad superior.
- **Ajuste de escala de DPI**: Permite que el sistema operativo controle la resolución de la sesión.
- **IME de cliente genérico**: Permite el respaldo a opciones y teclados virtuales para cambiar el IME.
- **Barra de idioma y distribución del teclado**: Permite usar diseños de teclado preferidos.

Además, puede utilizar las siguientes características que también ayudan a ofrecer una mejor experiencia de usuario.

## 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. Citrix Receiver para Windows versión 4.10 ahora respalda 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 XenApp y XenDesktop.

El VDA de Windows 10 detecta la presencia de un teclado o un mouse en un dispositivo cliente con función táctil cuando se conecta o se reconecta a una sesión. También detecta cuando se conecta o desconecta un teclado o mouse durante la sesión. Esta función está habilitada de forma predeterminada. Para inhabilitar la función, modifique la directiva **Cambiar modo tableta** usando Citrix Studio.

El modo tableta ofrece una interfaz de usuario que se adapta mejor a las pantallas táctiles:

- Botones ligeramente más grandes.
- La pantalla Inicio y todas las aplicaciones que inicie se abren en modo de pantalla completa.
- La barra de tareas contiene el botón Atrás.
- Los iconos desaparecen de la barra de tareas.

El modo escritorio ofrece la interfaz de usuario tradicional, donde se interactúa de la misma manera que con el PC con teclado y mouse.

Nota: Los Receivers para Web no respaldan el uso de las funciones de Windows Continuum.

Para obtener más información, consulte [notas de la versión 7.2 de XenServer](#).

## Mouse relativo

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

**Nota:** Esta característica solo se puede aplicar en una sesión de escritorio publicado.

## Para habilitar el respaldo del mouse relativo

1. Inicie una sesión en Citrix Receiver para Windows

2. Lance una sesión de escritorio publicado
3. En la barra de herramientas de Desktop Viewer, seleccione **Preferencias**.  
Aparecerá la ventana Preferencias de Citrix Receiver.
4. Seleccione “Conexiones”.
5. En los parámetros del mouse relativo, habilite **Usar mouse relativo**.
6. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

**NOTA:** Esta es una característica para cada sesión. No se conserva al volver a conectarse a una sesión desconectada. Los usuarios deben volver a habilitar la característica cada vez que se conecten o vuelvan a conectarse a los escritorios publicados.

## Decodificación por hardware

Cuando se usa Citrix Receiver para Windows (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 **DXVA** (DirectX Video Acceleration).

Para habilitar la decodificación por hardware con la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver:

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Receiver > Experiencia del usuario**.
3. Seleccione **Aceleración de hardware para gráficos**.
4. Seleccione **Habilitada** y haga clic en **Aplicar** y luego en **Aceptar**.

Para validar si la directiva se aplicó y la aceleración por hardware se está utilizando en una sesión ICA activa, busque las entradas de Registro siguientes:

Ruta del Registro: HKEY\_CURRENT\_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender

### Sugerencia

El valor de **Graphics\_GfxRender\_Decoder** y **Graphics\_GfxRender\_Renderer** debe ser 2. Si el valor es 1, esto significa que se está usando la decodificación por CPU.

Cuando use la función de decodificación por hardware, tenga en cuenta que existen las limitaciones siguientes:

- Si el cliente tiene dos unidades GPU y si uno de los monitores está activo en la segunda GPU, se usará la decodificación basada en CPU.

- Al conectar con un servidor XenApp 7.x que ejecuta Windows Server 2008 R2, Citrix recomienda no usar la decodificación por hardware en el dispositivo Windows del usuario. Si se habilita, pueden observarse problemas como un rendimiento lento al resaltar texto y un parpadeo de pantalla.

## Entrada de micrófono en el cliente

Citrix Receiver para Windows admite múltiples entradas de micrófono en el cliente. Los micrófonos instalados localmente se pueden usar para:

- Actividades en tiempo real, como llamadas desde sistemas de telefonía integrada en el equipo y conferencias web.
- Aplicaciones de grabación en el servidor, como programas de dictado.
- Grabaciones de vídeo y sonido.

Los usuarios de Citrix Receiver para Windows pueden seleccionar si quieren usar los micrófonos conectados a sus dispositivos cambiando un parámetro en la Central de conexiones. Los usuarios de XenDesktop también pueden usar las Preferencias de XenDesktop Viewer para inhabilitar sus micrófonos y cámaras Web.

## Admitir varios monitores

Puede usar un máximo de ocho monitores con Citrix Receiver 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.  
**XenDesktop.** 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 los monitores y haga clic en el botón **Maximizar**.
- En modo de ventanas, con una única imagen de monitor para la sesión; las aplicaciones no se muestran en monitores individuales.

**XenDesktop:** 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 XenDesktop usa el monitor principal en el dispositivo, éste 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 el respaldo de varios monitores, asegúrese de lo siguiente:

- El dispositivo de usuario está configurado para respaldar el uso de varios monitores.
- El sistema operativo del dispositivo de usuario debe ser capaz de detectar cada monitor. Para verificar que esta detección ocurre en el dispositivo de usuario en las plataformas Windows, confirme que cada monitor aparece por separado en la ficha Configuración del cuadro de diálogo Configuración de pantalla.
- Después de detectar los monitores:
  - **XenDesktop:** Configure el límite de memoria gráfica con la configuración “Límite de memoria de presentación” de las directivas de máquina de Citrix.
  - **XenApp:** Según la versión del servidor XenApp que tenga instalada:
    - \* Configure el límite de memoria de gráficos con la configuración de directiva de equipo de Citrix Límite de memoria de presentación.
    - \* En la consola de administración Citrix del servidor XenApp, seleccione la comunidad y, en el panel de tareas, seleccione Modificar las propiedades del servidor > Modificar todas las propiedades > Predeterminadas del servidor > HDX Broadcast > Presentación (o Modificar las propiedades del servidor > Modificar todas las propiedades > Predeterminadas del servidor > ICA > Presentación) y configure el parámetro Memoria máxima que se puede utilizar en cada uno de los gráficos de las sesiones.

Asegúrese de que el parámetro es lo suficientemente amplio (en kilobytes) para ofrecer suficiente memoria gráfica. Si este parámetro no es lo suficientemente grande, el recurso publicado se restringirá al subconjunto de monitores que cubra el tamaño especificado.

Para obtener información acerca del cálculo de los requisitos de memoria gráfica para XenApp y XenDesktop, consulte el artículo [CTX115637](#) en Knowledge Center.

## Anular parámetros de impresora en los dispositivos

Si en la configuración de directiva Valores predeterminados de optimización de impresión universal está habilitada la opción Permitir a los no administradores modificar estos parámetros, los usuarios pueden anular las opciones Compresión de imágenes y Almacenamiento en caché de imágenes y fuentes especificadas en esa configuración de directiva.

Para sobrescribir los parámetros de la impresora en el dispositivo de usuario

1. En el menú Imprimir de la aplicación del dispositivo de usuario, elija Propiedades.
2. En la ficha Parámetros del cliente, haga clic en Optimizaciones avanzadas y realice cambios a las opciones Compresión de imagen y Almacenamiento en caché de imágenes y fuentes.

## Control del teclado en pantalla

Para habilitar el acceso táctil a las aplicaciones y escritorios virtuales desde tabletas Windows, Citrix Receiver para Windows muestra automáticamente el teclado en pantalla al activar un campo de entrada de texto y cuando el dispositivo está en modo tienda o tableta.

En algunos dispositivos y en algunas circunstancias, Citrix Receiver para Windows no puede detectar el modo en que se encuentra un dispositivo, y es posible que el teclado en pantalla aparezca cuando no sea necesario.

Para impedir que aparezca el teclado en pantalla al usar un dispositivo convertible, cree un valor `REG_DWORD` `DisableKeyboardPopup` en `HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver` y establezca el valor en 1.

**Nota:** En una máquina x64, cree el valor en `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver`.

Las claves se pueden establecer en 3 modos diferentes, como se muestra a continuación:

- **Automatic:** `AlwaysKeyboardPopup = 0`; `DisableKeyboardPopup = 0`
- **Always popup** (teclado en pantalla): `AlwaysKeyboardPopup = 1`; `DisableKeyboardPopup = 0`
- **Never popup** (teclado en pantalla): `AlwaysKeyboardPopup = 0`; `DisableKeyboardPopup = 1`

## Teclas de acceso rápido

Se pueden configurar combinaciones de teclas para que Receiver las interprete como una funcionalidad especial. Cuando se habilita la directiva de teclas de acceso directo, se pueden especificar las teclas de acceso directo de Citrix, el comportamiento de las teclas de acceso directo de Windows y la disposición del teclado para las sesiones.

1. Como administrador, abra el Editor de directivas de grupo mediante la ejecución de `gpedit.msc` localmente desde el menú Inicio si va a aplicar directivas para un solo equipo, o bien, mediante la Consola de administración de directivas de grupo si va a aplicar directivas de dominio.

Nota: Si ya ha importado la plantilla de Citrix Receiver para Windows en el Editor de directivas de grupo, puede omitir los pasos de 2 a 5.

2. En el panel izquierdo del Editor de directivas de grupo, seleccione la carpeta Plantillas administrativas.
3. En el menú Acción, seleccione Agregar o quitar plantillas.
4. Seleccione Agregar y vaya a la carpeta Configuration de Receiver (normalmente `C:\Archivos de programa\Citrix\ICA Client\Configuration`) y seleccione el archivo de la plantilla de Citrix Receiver para Windows.



**Nota:** Seleccione el archivo de plantilla de Citrix Receiver para Windows (receiver.adm o receiver.admx/receiver.adml) en función de la versión del sistema operativo Windows.

5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. En el Editor de directivas de grupo, vaya a Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > Experiencia de usuario > Teclas de acceso rápido.
7. En el menú Acción, elija Propiedades, seleccione Habilitada y luego elija las opciones pertinentes.

## Disponibilidad de iconos de color de 32 bits en Citrix Receiver para Windows

Citrix Receiver para Windows admite iconos de color de alta densidad (de 32 bits) y selecciona automáticamente la profundidad de color de las aplicaciones que aparecen en el cuadro de diálogo Central de conexiones de Citrix, en el menú Inicio y en la barra de tareas para proporcionar una integración total de aplicaciones.

Precaución: Si modifica el Registro de forma incorrecta, podrían generarse problemas graves que pueden provocar la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Para establecer una profundidad preferida, se puede agregar la clave de Registro TWIDesiredIconColor a HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences y establecerla en el valor deseado. 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.

## Habilitar Desktop Viewer

Cada empresa tiene sus propias necesidades de negocio. Los requisitos para el acceso por parte de los usuarios a los escritorios virtuales pueden variar de usuario a usuario y a medida que evolucionan las necesidades de la empresa. La experiencia del usuario a la hora de conectarse a los escritorios virtuales, así como su interacción en la configuración de las conexiones depende de cómo se configure Citrix Receiver 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 y, desplazar y cambiar el tamaño de ese escritorio dentro del escritorio local. Los usuarios pueden definir preferencias y conectarse con más de un escritorio utilizando varias conexiones XenDesktop en el mismo dispositivo de usuario.

Nota: Los usuarios deben usar Citrix Receiver para Windows si quieren cambiar la resolución de pantalla en sus escritorios virtuales. No pueden cambiar la resolución de pantalla usando el Panel de control de Windows.

## **Entrada de teclado en sesiones de Desktop Viewer**

En las sesiones de Desktop Viewer, la combinación de la tecla con el logotipo de Windows+L se transfiere al equipo local.

Ctrl+Alt+Supr se transfiere al equipo local.

Las pulsaciones de teclas que activan Teclas especiales, Teclas de filtro y Teclas de alternancia (funciones de accesibilidad de Microsoft) siempre se transfieren al equipo local.

Como una función de accesibilidad de Desktop Viewer, al presionar Ctrl+Alt+Interrumpir se muestran los botones de la barra de herramientas de Desktop Viewer en una ventana emergente.

Ctrl+Esc se envía al escritorio virtual remoto.

Nota: De forma predeterminada, Alt+Tab transfiere el foco entre las ventanas de la sesión si Desktop Viewer está maximizado. Si Desktop Viewer se muestra en una ventana, Alt+Tab transfiere el foco entre las ventanas fuera de la sesión.

Las secuencias de teclas de acceso rápido son combinaciones de teclas diseñadas por Citrix. Por ejemplo, la secuencia Ctrl+F1 reproduce las teclas Ctrl+Alt+Supr, y Mayús+F2 cambia entre el modo de pantalla completa y de ventanas en las aplicaciones. No puede usar las secuencias de teclas de acceso rápido con escritorios virtuales que se muestran en Desktop Viewer (en sesiones de XenDesktop), pero puede usarlas con aplicaciones publicadas (en sesiones de XenApp).

## **Conectar con escritorios virtuales**

Los usuarios no pueden conectarse con el mismo escritorio virtual desde una sesión de escritorio. Si se intenta, se desconectará la sesión de escritorio existente. Por lo tanto, Citrix recomienda lo siguiente:

- Los administradores no deben configurar a los clientes de un escritorio para que se conecten con un sitio que publica el mismo escritorio.
- Los usuarios no deben buscar un sitio que aloje el mismo escritorio si el sitio se configura para reconectar a los usuarios automáticamente con las sesiones existentes.

- Los usuarios no deben buscar un sitio que aloje el mismo escritorio e intentar ejecutarlo.

Tenga en cuenta que un usuario que inicia una sesión localmente en un equipo que actúa como escritorio virtual bloquea las conexiones con ese escritorio.

Si los usuarios se conectan con aplicaciones virtuales (publicadas con XenApp) desde un escritorio virtual y la organización dispone de un administrador de XenApp independiente, Citrix sugiere aunar esfuerzos para definir la asignación de dispositivos para que los dispositivos de escritorio se asignen siempre dentro de las sesiones de aplicación y escritorio. Debido a que las unidades locales se muestran como unidades de red en las sesiones de escritorio, el administrador de XenApp necesita modificar la directiva de asignación de unidades para que incluya las unidades de red.

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

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

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

#### **Nota**

Puede ocultar total o parcialmente las opciones de la hoja de Preferencias avanzadas, disponible en el icono de Citrix Receiver en el área de notificación. Para obtener más información, consulte [Ocultar la hoja de Preferencias avanzadas](#).

El programa para la mejora de la experiencia del usuario de Citrix (Customer Experience Improvement Program o CEIP) recopila información anónima de uso y de configuración de Receiver para Windows y envía esos datos automáticamente a Citrix. Esos datos ayudan a Citrix a mejorar la calidad, la fiabilidad y el rendimiento de Receiver.

CEIP no recopila ninguna información que pueda identificar el entorno del cliente.

Sugerencia: Puede cambiar su participación en el programa CEIP usando la interfaz de Receiver. Tiene 7 días para inhabilitar CEIP a partir del momento de la instalación.

Para inhabilitar el programa CEIP, o para cancelar su participación:

1. Haga clic con el botón secundario en el icono de Citrix Receiver situado en el área de notificación.
2. Seleccione **Preferencias avanzadas**.  
Aparecerá la ventana 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**.

## Ajustar escala de DPI

October 5, 2018

Citrix Receiver para Windows permite que el sistema operativo controle la resolución de la sesión.

Puede aplicar DPI alto en una sesión, pero la función está inhabilitada de forma predeterminada. Esto significa que el ajuste de escala de la sesión sigue la resolución del sistema operativo.

Puede configurar la escala de DPI mediante las siguientes opciones:

1. Plantilla administrativa de objeto de directiva de grupo (configuración por equipo)
2. Preferencias avanzadas (configuración por usuario)

### Limitaciones

- Incluso con esta característica habilitada, se ha observado una leve falta de definición en Desktop Viewer.
- En una sesión, cuando cambian los parámetros de DPI y se vuelve a iniciar la sesión, es posible que el tamaño de la ventana de la sesión no sea el adecuado.  
Como solución alternativa, cambie el tamaño de la ventana de la sesión.

### Para configurar el ajuste de escala de DPI usando la plantilla administrativa de objeto de directiva de grupo (GPO) de Citrix Receiver

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de `gpedit.msc`.
2. En el nodo "Configuración del equipo", vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Receiver > DPI**.
3. Seleccione la directiva **DPI alto**.
4. Cambie la configuración según sea necesario.
5. Haga clic en Aplicar y, a continuación, en Aceptar.
6. Desde una línea de comandos, ejecute el comando `gpupdate /force`.

## Para configurar la escala de DPI mediante la interfaz gráfica de usuario

### Nota

Puede ocultar total o parcialmente las opciones de la hoja de Preferencias avanzadas, disponible en el icono de Citrix Receiver en el área de notificación. Para obtener más información, consulte [Ocultar la hoja de Preferencias avanzadas](#).

1. Haga clic con el botón secundario en Citrix Receiver para Windows desde el área de notificación.
2. Seleccione **Preferencias avanzadas** y haga clic en **Parámetros de DPI**.  
Aparecerá el cuadro de diálogo Parámetros de DPI.
3. Cambie la configuración según sea necesario.  
De forma predeterminada, está seleccionada la opción **Dejar que el sistema operativo ajuste la resolución**.
4. Haga clic en **Guardar**.

Reinicie la sesión de Citrix Receiver para Windows para que los cambios surtan efecto.

Para obtener más información sobre la solución de problemas de ajuste en la escala de DPI, consulte el artículo [CTX230017](#) de Knowledge Center.

## Codificación de vídeo H.265

November 16, 2018

Citrix Receiver para Windows respalda el uso del códec de vídeo H.265 para la aceleración de hardware de vídeos y gráficos remotos. Para utilizar esta función, es necesario que reciba respaldo y esté habilitado tanto en el VDA como en Citrix Receiver para Windows. Si la GPU en el punto final no admite la decodificación H.265 utilizando la interfaz DXVA, la configuración de directiva “Decodificación H265 para gráficos” se ignora y la sesión recurre al uso del códec de vídeo H.264.

### Requisitos previos

1. VDA 7.16 y versiones posteriores.
2. Habilite la directiva **Optimizar para cargas de trabajo de gráficos 3D** en el VDA.
3. Habilite la directiva **Usar codificación por hardware para códec de vídeo** en el VDA.

**Nota:** La codificación H.265 solo está respaldada en las GPU de NVIDIA.

Esta función está **Inhabilitada** de forma predeterminada en Citrix Receiver para Windows.

## Configurar Citrix Receiver para Windows para usar la codificación de vídeo H.265 mediante la plantilla administrativa de objeto de directiva de grupo (GPO) de Citrix

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Citrix Receiver > Experiencia del usuario**.
3. Seleccione la directiva **Decodificación H265 para gráficos**.
4. Seleccione **Habilitada**.
5. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.

## Configurar Citrix Receiver para Windows para usar 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 usando 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 usando 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.

Vuelva a iniciar la sesión para que los cambios surtan efecto.

#### Nota

- Si la directiva **Aceleración de hardware para gráficos** está inhabilitada en la plantilla administrativa de GPO de Citrix Receiver, las configuraciones de la directiva **Decodificación H265 para gráficos** se ignoran y esta característica no funciona.
- Ejecute la herramienta HDX Monitor 3.x para saber si el codificador de vídeo H.265 está habilitado dentro de las sesiones. Para obtener más información acerca de la herramienta HDX Monitor 3.x, consulte el artículo [CTX135817](#) de Knowledge Center.

## Iniciar vPrefer

January 7, 2019

### Configurar el inicio de vPrefer usando la plantilla de objeto de directiva de grupo

En las versiones anteriores, podía especificar que se iniciara preferentemente la instancia de una aplicación instalada en el VDA (denominada instancia local en este documento) antes que la aplicación publicada. Para ello, configuraba el atributo KEYWORDS: prefer = atributo “application” en Citrix Studio.

A partir de la versión 4.11, en una situación de doble salto (donde Citrix Receiver se ejecuta en el VDA que aloja su sesión), puede controlar si Receiver inicia la instancia local de una aplicación instalada en el VDA (si está disponible como aplicación local) en lugar de iniciar una instancia alojada de la aplicación.

vPrefer está disponible en StoreFront 3.14, XenApp 7.17 y versiones posteriores.

Cuando inicia la aplicación, Citrix Receiver para Windows lee los datos de los recursos presentes en el servidor StoreFront y aplica la configuración en función del indicador **vPrefer** en el momento de la enumeración. Citrix Receiver para Windows busca la ruta de instalación de la aplicación en el Registro de Windows en el VDA y, si está presente, inicia la instancia local de la aplicación. De lo contrario, se inicia una instancia alojada de la aplicación.

Si inicia una aplicación que no está instalada en el VDA, se iniciará la aplicación alojada. Para obtener más información sobre cómo se gestiona el inicio local en StoreFront, consulte [Controlar el inicio de aplicaciones locales en escritorios publicados](#) en la documentación de StoreFront.

Si no quiere que la instancia local de la aplicación se inicie en el VDA, establezca **LocalLaunchDisabled** en **True** usando PowerShell en el Delivery Controller.

Esta característica 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

Cuando actualiza o instala Citrix Receiver para Windows por primera vez, debe agregar los archivos de plantilla más recientes al GPO local. Para obtener más información sobre cómo agregar los archivos de plantilla al GPO local, consulte [Configurar la plantilla administrativa de objeto de directiva de grupo](#). En caso de una actualización, la configuración existente se conserva al importar los archivos más recientes.

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.

2. En el nodo “Configuración del equipo”, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Receiver > Autoservicio**.
3. Seleccione la directiva **vPrefer**.
4. Seleccione **Habilitada** y, en el menú desplegable **Permitir aplicaciones**, seleccione una de las siguientes opciones:
  - a) **Permitir todas las aplicaciones:** Esta opción inicia la instancia local de todas las aplicaciones presentes en el VDA. Citrix Receiver para Windows busca la aplicación instalada (incluidas las aplicaciones nativas de Windows, como el Bloc de notas, la Calculadora, el WordPad, el símbolo del sistema) e inicia la aplicación que haya en el VDA, en lugar de iniciar la aplicación alojada.
  - b) **Permitir aplicaciones instaladas:** Esta opción inicia la instancia local de las aplicaciones instaladas que haya presentes en el VDA. Si la aplicación no está instalada en el VDA, se inicia la aplicación alojada. De forma predeterminada, se selecciona la opción **Permitir aplicaciones instaladas** cuando se **habilita** la directiva **vPrefer**. Esta opción excluye las aplicaciones nativas del sistema operativo Windows, como el Bloc de notas, la Calculadora, etc.
  - c) **Permitir aplicaciones de red:** Esta opción inicia la instancia de una aplicación que esté publicada en una red compartida.
5. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
6. Vuelva a iniciar la sesión para que los cambios surtan efecto.

**Limitación:**

- Receiver para Web no admite esta característica.

Para obtener información adicional sobre la función vPrefer, consulte el artículo [CTX232210](#) de Knowledge Center.

## Editores IME de cliente genérico

February 20, 2019

### Configurar IME de cliente genérico usando 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 Citrix Receiver para Windows (C:\Archivos de programa (x86)\Citrix\ICA Client).

**Nota**

Puede usar el conmutador 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 Citrix Receiver para Windows (C:\Archivos de programa (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 ejecutando el comando **wfica32.exe /localgenericime:on**.

## Activar/desactivar

Citrix Receiver para Windows respalda la activación/desactivación de esta función. Ejecute **wfica32.exe /localgenericime:on** cuando quiera habilitarla o inhabilitarla. Sin embargo, los parámetros de sincronización de distribución de teclado tienen prioridad sobre este comando conmutador. Si la sincronización de la distribución de teclado está **desactivada**, la activación con el conmutador no habilita el IME de cliente genérico.

## Configurar el IME de cliente genérico usando la interfaz gráfica de usuario

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

La función de IME de cliente genérico se puede habilitar mediante la habilitación de la sincronización de la distribución de teclado. Para obtener más información, consulte [Sincronizar la distribución del teclado](#).

Citrix Receiver para Windows permite configurar diferentes opciones para usar el IME de cliente genérico. Se puede seleccionar alguna de estas opciones en función de los requisitos y el uso.

1. En una sesión activa de aplicación, haga clic con el botón secundario en el icono de Citrix Receiver 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:** Seleccione esta opción para inhabilitar el IME local. Esta opción significa que solo se pueden usar los idiomas configurados en el servidor.
2. **Definir IME local en modo de alto rendimiento:** Seleccione esta opción para usar 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:** Seleccione esta opción para usar el IME local con la mejor experiencia de usuario. Esta opción consume mucho ancho de banda. De forma predeterminada, se selecciona esta opción cuando se habilita el IME de cliente genérico.

El cambio de parámetro se aplica solo en la sesión actual.

## Habilitar la configuración de teclas de acceso rápido usando un editor del Registro

Cuando el IME de cliente genérico está habilitado, se puede usar **MAYÚS + F4** para seleccionar distintos modos de IME. Las diferentes opciones de modos IME aparecen en la esquina superior derecha de la sesión.

De forma predeterminada, la tecla de acceso rápido para el IME de cliente genérico está inhabilitada.

En el editor del Registro, vaya a HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys.

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

### Nota

La funcionalidad de la tecla de acceso rápido recibe respaldo tanto en sesiones de escritorio como en sesiones de aplicación.

## Limitaciones

- El IME de cliente genérico no respalda las aplicaciones UWP (Universal Windows Platform) tales como UI de búsqueda y el explorador Edge del sistema operativo Windows 10. Como solución temporal, use el editor IME del servidor en su lugar.
- El IME de cliente genérico no recibe respaldo en Internet Explorer 11 en **modo protegido**. Como solución temporal, puede inhabilitar el modo protegido en las **Opciones de Internet**. Para ello, haga clic en **Seguridad** y desmarque la casilla **Habilitar modo protegido**.

## Barra de idioma y distribución del teclado

October 5, 2018

### Distribución del teclado

#### Nota

Puede ocultar total o parcialmente las opciones de la hoja de Preferencias avanzadas, disponible en el icono de Citrix Receiver en el área de notificación. Para obtener más información, consulte [Ocultar la hoja de Preferencias avanzadas](#).

La sincronización de la distribución del teclado permite a los usuarios cambiar entre distintas distribuciones de teclado preferidas en el dispositivo cliente. Esta función está inhabilitada de forma predeterminada.

Para habilitar la sincronización de la distribución del teclado:

1. Desde el icono de Citrix Receiver para Windows en el área de notificaciones, seleccione **Preferencias avanzadas > Barra de idioma y teclado**. Aparecerá la ventana de la barra de idioma y teclado.
2. Haga clic en **Guardar**.

Para inhabilitar la función, seleccione **No**.

También puede habilitar o inhabilitar la sincronización de la distribución del teclado mediante la línea de comandos. Para ello, ejecute **wfica32:exe /localime:on** o **wfica32:exe /localime:off** desde la carpeta de instalación de Citrix Receiver para Windows (C:\Archivos de programa (x86)\Citrix\ICA Client).

**Nota:**

La opción de distribución de teclado local activa el IME (Input Method Editor) del cliente. Si los usuarios que trabajan en japonés, chino y coreano prefieren usar el editor IME del servidor, deben inhabilitar la opción de distribución de teclado local. Para ello, deben seleccionar la opción **No** o ejecutar **wfica32:exe/localime:off**. La sesión recurrirá a la distribución de teclado que suministre el servidor remoto cuando se conecten a la sesión siguiente.

En ocasiones, el cambio a la distribución de teclado del cliente no tiene efecto en una sesión activa. Para resolver este problema, cierre la sesión en Citrix Receiver para Windows y vuelva a iniciar sesión.

**Limitaciones:**

- Las aplicaciones remotas que se ejecutan con privilegios elevados (por ejemplo, al 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. Para solucionar este problema, cambie manualmente la distribución del teclado en el lado del servidor (VDA) o inhabilite el Control de cuentas de usuario (UAC).
- Si el usuario cambia la distribución de teclado en el cliente por una distribución que no recibe respaldo en el servidor, la característica de sincronización de la distribución del teclado se inhabilitará por razones de seguridad, ya que una distribución de teclado no reconocida se trata como una potencial amenaza de seguridad. Para restaurar la funcionalidad de la sincronización de distribución del teclado, el usuario debe cerrar la sesión y volver a iniciarla.
- Cuando RDP se distribuye como una aplicación y el usuario está trabajando en una sesión RDP, no es posible cambiar la distribución del teclado con los accesos directos Alt + Mayús. Para solucionar este problema, el usuario puede usar la barra de idioma en la sesión RDP para cambiar la distribución del teclado.

- Esta característica está inhabilitada en Windows Server 2016 debido a un problema de terceros que puede introducir un riesgo para el rendimiento. La característica se puede habilitar mediante un parámetro de Registro en el VDA: en HKLM\Software\Citrix\ICA\Icalme, agregue una nueva clave llamada DisableKeyboardSync y establezca el valor en 0.

## Barra de idioma

A partir de la versión 4.11, puede optar por mostrar u ocultar la barra de idioma remota en una sesión de aplicación utilizando la interfaz gráfica de usuario. La barra de idioma muestra el idioma de entrada preferido en una sesión. En versiones anteriores, solo podía cambiar esta configuración usando las claves de Registro en el VDA. A partir de Citrix Receiver para Windows 4.11, puede cambiar la configuración desde el cuadro de diálogo **Preferencias avanzadas** en Citrix Receiver para Windows. La barra de idioma aparece en una sesión de forma predeterminada.

### Nota

Esta característica está disponible en sesiones que se ejecutan en VDA 7.17 y versiones posteriores.

## Definir si mostrar u ocultar la barra de idioma remota

1. Haga clic con el botón secundario en Citrix Receiver para Windows en el área de notificaciones y seleccione **Preferencias avanzadas**.
2. Seleccione **Barra de idioma y teclado**.
3. Seleccione la ficha **Barra de idioma**.
4. Cambie la configuración según sea necesario.

### Nota

- Los cambios de configuración surten efecto de inmediato.
- 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\Local

3. Cree una nueva clave de valor DWORD, **ToggleOffLanguageBarFeature**, y establézcala en **1** para ocultar la opción de barra de idioma en la hoja “Preferencias avanzadas”.

## Autenticación

January 7, 2019

Para aumentar al máximo la seguridad del entorno, las conexiones entre Citrix Receiver para Windows y los recursos que publique deben ser seguras. Puede configurar diversos tipos de autenticación para el software de Citrix Receiver para Windows, incluidos: autenticación con tarjeta inteligente, comprobación de lista de revocaciones de certificados y autenticación PassThrough con Kerberos.

## Configurar la autenticación PassThrough de dominio

January 7, 2019

Single Sign-On permite autenticarse en un dominio y usar las aplicaciones y los escritorios entregados por ese dominio sin necesidad de volver a autenticarse para cada aplicación o escritorio.

Cuando inicia sesión en Citrix Receiver, las credenciales se transfieren a StoreFront, junto con las aplicaciones y los escritorios enumerados para usted, incluidos los parámetros del menú Inicio. Después de configurar el tipo de inicio de sesión Single Sign-On, puede iniciar sesión en Citrix Receiver e iniciar sesiones de XenApp o XenDesktop sin tener que escribir varias veces las credenciales.

Cuando hace clic en el icono de una aplicación, Citrix Receiver transfiere las credenciales de dominio al Delivery Controller y la aplicación seleccionada se abre.

Puede configurar Single Sign-On cuando instala Citrix Receiver mediante una de estas opciones:

- Interfaz de línea de comandos
- Interfaz gráfica de usuario

## Requisitos previos

1. Agregar el servidor StoreFront a la lista de sitios de confianza usando Internet Explorer. Para hacerlo:
  - a) Abra Internet Explorer.
  - b) Seleccione **Herramientas > Opciones de Internet > Seguridad > Internet local** y haga clic en **Sitios**. Aparecerá la ventana **Intranet local**.

- c) Seleccione **Avanzado**.
  - d) Agregue la URL del FQDN de StoreFront o de la Interfaz Web con los protocolos HTTP o HTTPS correspondientes.
  - e) Haga clic en “Aplicar” y, a continuación, en “Aceptar”.
2. Modifique los parámetros de **Autenticación de usuario** en Internet Explorer. Para hacerlo:
    - a) Abra Internet Explorer.
    - b) En la ficha **Opciones de Internet > Seguridad**, haga clic en **Sitios de confianza**.
    - c) Haga clic en **Nivel personalizado**. Aparecerá la ventana **Configuración de seguridad: zona de sitios de confianza**.
    - d) En el panel **Autenticación de usuario**, seleccione **Inicio de sesión automático con el nombre de usuario y contraseña actuales**.

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

Instale Citrix Receiver para Windows con el modificador de línea de comandos **/includeSSON**.

Reinicie Receiver para Windows para que los cambios surtan efecto.

#### Nota

Si Citrix Receiver se instala sin el componente Single Sign-On, no se admite actualizar a la versión más reciente de Citrix Receiver con el modificador de línea de comandos **/includesson**.

### Configurar Single Sign-On desde la interfaz gráfica de usuario

1. Busque el archivo de instalación de Citrix Receiver para Windows (CitrixReceiver.exe).
2. Haga doble clic en **CitrixReceiver.exe** para iniciar el instalador.
3. En el asistente de instalación **Habilitar Single Sign-On**, marque la casilla “Habilitar Single Sign-On” para instalar Citrix Receiver para Windows con la característica SSON habilitada; lo que equivale a instalar Citrix Receiver para Windows con la opción de línea de comandos **/includeSSON**.

La imagen siguiente ilustra cómo habilitar Single Sign-on:

### Configurar Single Sign-On en Receiver para Web

Puede configurar Single Sign-On en Receiver para Web usando la plantilla administrativa de objeto de directiva de grupo.

Nota: Cuando actualiza o instala Citrix Receiver para Windows por primera vez, debe agregar los archivos de plantilla más recientes al GPO local. Para obtener más información sobre cómo agregar archivos de plantilla al GPO local, consulte <https://docs.citrix.com/es-es/receiver/windows/current->

[release/configure/config-gpo-template.html](https://docs.citrix.com/en-us/release/configure/config-gpo-template.html). Cuando se actualiza el producto, los parámetros existentes se conservan al importar los archivos más recientes.

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
2. En el nodo **Configuración del equipo**, vaya a **Plantillas administrativas > Componentes de Citrix > Citrix Receiver > Autenticación de usuarios**.
3. Seleccione la directiva **Nombre de usuario y contraseña locales** y establézcala en **Habilitada**.
4. Haga clic en **Habilitar autenticación PassThrough**. Esta opción permite a Citrix Receiver usar las credenciales de inicio de sesión para la autenticación 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 para todas las conexiones.
6. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
7. Reinicie Citrix Receiver para Web para que los cambios surtan efecto.

Compruebe que Single Sign-On está habilitado. Para ello, inicie Citrix Receiver. Después de iniciar Receiver, inicie el Administrador de tareas y compruebe si el proceso ssonsvr.exe se está ejecutando.

## Configurar Single Sign-On en StoreFront y la Interfaz Web

### Configurar StoreFront

Para configurar SSON en StoreFront y la Interfaz Web, abra Citrix Studio en el servidor StoreFront y seleccione **Autenticación > Agregar o quitar métodos**. Seleccione **PassThrough de dominio**.

### Configurar la Interfaz Web

Para configurar SSON en la Interfaz Web, seleccione **Administración de la Interfaz Web de Citrix > Sitios de servicios XenApp > Métodos de autenticación** y habilite **Paso de credenciales**.

## Usar Configuration Checker para validar la configuración de Single Sign-On

Configuration Checker permite ejecutar pruebas para comprobar que Single Sign-On está configurado correctamente. Las pruebas se ejecutan en varios puntos de control de la configuración de Single Sign-On y muestran los resultados de la configuración.

1. Haga clic con el botón secundario en Citrix Receiver para Windows en el área de notificaciones y seleccione **Preferencias avanzadas**.
2. Haga clic en **Configuration Checker**.  
Aparecerá la ventana de Citrix Configuration Checker.

3. Seleccione **SSONChecker** desde el panel **Seleccionar**.
4. Haga clic en **Ejecutar**. Aparecerá la barra de progreso, que muestra el estado de la prueba.

La ventana de Configuration Checker consta de las siguientes columnas:

1. **Estado:** Muestra el resultado de una prueba en un punto de control concreto.
  - Una marca de verificación (✓) verde indica que el punto de control está configurado correctamente.
  - Una I azul indica información sobre el punto de control.
  - Una X roja indica que ese punto de control no está configurado correctamente.
2. **Proveedor:** Muestra el nombre del módulo en que se ejecuta la prueba. En este caso, Single Sign-On.
3. **Suite:** Indica la categoría de la prueba. Por ejemplo, Instalación.
4. **Prueba:** Indica el nombre de la prueba específica que se ejecuta.
5. **Detalles:** Ofrece información adicional acerca de la prueba, independientemente del resultado.

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

Se realizan las siguientes pruebas:

1. Instalado con Single Sign-On
2. Captura de credenciales de inicio de sesión
3. Registro de proveedores de red: El resultado de la prueba de registro de proveedor de red muestra una marca de verificación verde solo cuando "Citrix Single Sign-On" figura en primer lugar en la lista de proveedores de red. Si Citrix Single Sign-On aparece en algún otro lugar de la lista, el resultado de la prueba Registro de proveedores de red es una barra azul y se ofrece información adicional.
4. Proceso de Single Sign-On en ejecución
5. Directiva de grupo: De manera predeterminada, esta directiva está configurada en el cliente.
6. Parámetros de Internet para zonas de seguridad: Compruebe que ha agregado la URL de la tienda 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 de Preferencias avanzadas se vuelva a abrir para que los cambios surtan efecto y para mostrar el estado de la prueba.
7. Método de autenticación para la Interfaz Web o StoreFront.

#### Nota

- Si el usuario accede a Receiver para Web, los resultados de la prueba no se aplican. Si Citrix Receiver para Windows está configurado para varias tiendas, la prueba del método de autenticación se ejecuta en todas las tiendas configuradas.
- Puede guardar como informes los resultados de la prueba. El formato predeterminado del informe es TXT.



- Si el usuario accede a Receiver para Web, los resultados de la prueba no se aplican.
- Si Citrix Receiver para Windows está configurado para varias tiendas, la prueba del método de autenticación se ejecuta en todas las tiendas configuradas.
- Puede guardar como informes los resultados de la prueba. El formato predeterminado del informe es TXT.
- Si el usuario accede a Receiver para Web, los resultados de la prueba no se aplican.
- Si Citrix Receiver para Windows está configurado para varias tiendas, la prueba del método de autenticación se ejecuta en todas las tiendas configuradas.
- Puede guardar como informes los resultados de la prueba. El formato predeterminado del informe es TXT.
  - Si el usuario accede a Receiver para Web, los resultados de la prueba no se aplican.
  - Si Citrix Receiver para Windows está configurado para varias tiendas, la prueba del método de autenticación se ejecuta en todas las tiendas configuradas.
  - Puede guardar como informes los resultados de la prueba. El formato predeterminado del informe es TXT.

Para obtener información sobre cómo configurar la autenticación PassThrough de dominio, consulte el artículo [CTX133982](#) en Knowledge Center.

### Ocultar la opción Configuration Checker de la ventana Preferencias avanzadas

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
2. Vaya a **Componentes de Citrix > Citrix Receiver > Autoservicio > DisableConfigChecker**.
3. Haga clic en **Habilitada** para ocultar la opción “Configuration Checker” de la ventana “Preferencias avanzadas”.
4. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
5. Abra una ventana de símbolo del sistema.
6. Ejecute el comando gpupdate /force.

### Limitación

Configuration Checker no incluye el punto de control de la configuración “Confiar en las solicitudes enviadas a XML Service” en los servidores XenApp o XenDesktop.

### Configurar la autenticación con tarjeta inteligente

April 2, 2019

Citrix Receiver para Windows admite las siguientes características de autenticación con tarjeta inteligente. Para obtener información sobre la configuración de XenDesktop y StoreFront, consulte la documentación de esos componentes. En este tema, se describe la configuración de Citrix Receiver para Windows necesaria para usar tarjetas inteligentes.

- **Autenticación PassThrough (Single Sign-On):** La autenticación PassThrough captura las credenciales de la tarjeta inteligente cuando los usuarios inician una sesión en Citrix Receiver para Windows. Citrix Receiver para Windows usa las credenciales capturadas de la siguiente manera:
  - Los usuarios de dispositivos que pertenecen a un dominio que inician sesión en Citrix Receiver para Windows mediante una tarjeta inteligente pueden iniciar aplicaciones y escritorios virtuales sin necesidad de volver a autenticarse.
  - Los usuarios de dispositivos que no pertenecen a ningún dominio que inician una sesión en Citrix Receiver para Windows mediante una tarjeta inteligente deben introducir de nuevo sus credenciales para poder iniciar aplicaciones y escritorios virtuales.

La autenticación PassThrough requiere configuración de StoreFront y Citrix Receiver para Windows.

- **Autenticación bimodal:** La autenticación bimodal ofrece a los usuarios la opción de usar una tarjeta inteligente o introducir su nombre de usuario y contraseña. Esta función resulta útil cuando no se puede usar la tarjeta inteligente por alguna razón (por ejemplo, si el usuario la olvidó en casa o el certificado de inicio de sesión caducó). Para permitir esto, deben configurarse tiendas dedicadas para cada sitio, usando el método `DisableCtrlAltDel` con el valor `False` para permitir el uso de tarjetas inteligentes. La autenticación bimodal requiere una configuración de StoreFront. Si hay un dispositivo NetScaler Gateway en la implementación, también será necesario configurarlo.

Con la autenticación bimodal, administrador de StoreFront tiene ahora la oportunidad de ofrecer al usuario la posibilidad de autenticarse con nombre y contraseña o con tarjeta inteligente en una misma tienda, seleccionando estas opciones en la consola de StoreFront. Consulte la documentación de [StoreFront](#).

- **Varios certificados:** Puede haber varios certificados disponibles para una única tarjeta inteligente y si se utilizan varias tarjetas inteligentes. Cuando un usuario introduce una tarjeta inteligente en el lector de tarjetas, los certificados están disponibles para todas las aplicaciones que se ejecutan en el dispositivo del usuario, incluido Citrix Receiver para Windows. Para cambiar cómo se seleccionan los certificados, configure Citrix Receiver para Windows.
- **Autenticación por certificado del cliente:** La autenticación por certificado del cliente requiere la configuración de NetScaler Gateway y StoreFront.
  - Para acceder a los recursos de StoreFront a través de NetScaler Gateway, es posible que los usuarios tengan que volver a autenticarse después de extraer una tarjeta inteligente.

- Cuando la configuración SSL de NetScaler 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 adicional entre Receiver y el escritorio virtual del usuario. Las implementaciones que respaldan el doble salto se describen en la documentación de XenDesktop.
- **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 aplicación o escritorio virtual.

## Requisitos previos

Este tema presupone que el lector conoce los temas sobre tarjetas inteligentes en la documentación de XenDesktop y StoreFront.

## Limitaciones

- Los certificados deben guardarse en una tarjeta inteligente, no en el dispositivo del usuario.
- Citrix Receiver para Windows no guarda la elección de certificado del usuario, pero puede guardar el PIN si se configura así. El PIN solo se almacena en caché en la memoria no paginada durante la sesión del usuario. No se guarda en disco en ningún momento.
- Citrix Receiver para Windows no reconecta sesiones cuando se introduce una tarjeta inteligente.
- Cuando está configurado para la autenticación con tarjeta inteligente, Citrix Receiver para Windows no admite ni el Preinicio de sesiones ni Single Sign-On en redes privadas virtuales (VPN). Para usar túneles VPN con autenticación con tarjeta inteligente, los usuarios deben instalar el NetScaler Gateway Plug-in e iniciar una sesión a través de una página Web, usando sus tarjetas inteligentes y números PIN para autenticarse en cada paso. La autenticación PassThrough en StoreFront con NetScaler Gateway Plug-in no está disponible para los usuarios de tarjeta inteligente.
- Las comunicaciones de Citrix Receiver para Windows Updater con citrix.com y Merchandising Server no son compatibles con la autenticación con tarjeta inteligente en NetScaler Gateway.

### Advertencia

Parte de la configuración descrita en este tema incluye modificaciones del Registro. El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden hacer necesaria la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Edi-

tor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

## Para habilitar la autenticación Single Sign-on para tarjeta inteligente

Para configurar Citrix Receiver para Windows, incluya la siguiente opción de línea de comandos cuando lo instale:

- ENABLE\_SSON=Yes

Single Sign-on es otro término para el paso de credenciales/autenticación PassThrough. Habilitar este parámetro impide que Citrix Receiver para Windows Receiver muestre una segunda solicitud de PIN al usuario.

O, puede realizar la configuración a través de esta directiva y unos cambios en el Registro:

- Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > Autenticación de usuarios > Nombre de usuario y contraseña locales
- Defina SSONCheckEnabled como false en cualquiera de estas claves de Registro si el componente Single Sign-on no está instalado. La clave impide que Authentication Manager de Citrix Receiver para Windows busque el componente Single Sign-On, lo que permite que Citrix Receiver para Windows se autentique en StoreFront.

HKEY\_CURRENT\_USER\Software\Citrix\AuthManager\protocols\integratedwindows\

HKEY\_LOCAL\_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows\

De forma alternativa, es posible habilitar la autenticación con tarjeta inteligente en StoreFront en lugar de Kerberos. Para habilitar la autenticación con tarjeta inteligente en StoreFront en lugar de Kerberos, instale Citrix Receiver para Windows con las siguientes opciones de la línea de comandos. Esto requiere privilegios de administrador. La máquina no necesita estar unida a un dominio.

- /includeSSON instala Single Sign-On (autenticación PassThrough). Habilita el almacenamiento en caché de credenciales y el uso de la autenticación PassThrough de dominio.
- Si el usuario está iniciando una sesión en el punto final con otro método distinto de la tarjeta inteligente para la autenticación en Receiver (por ejemplo, con nombre de usuario y contraseña), la línea de comandos es:

```
1 /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
```

Lo que evita que se capturen credenciales al iniciar sesión al mismo tiempo que permite que Citrix Receiver para Windows almacene el PIN al iniciar sesión en Citrix Receiver para Windows.

- Vaya a Directiva > Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > Autenticación de usuarios > Nombre de usuario y contraseña locales.

Habilite la autenticación PassThrough. Dependiendo de la configuración y los parámetros de seguridad, puede que tenga que seleccionar 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 Citrix Receiver para Windows.

### **Para cambiar cómo se seleccionan los certificados**

De manera predeterminada, si hay varios certificados que son válidos, Citrix Receiver para Windows pide al usuario que elija uno de la lista. También puede configurar Citrix Receiver para Windows 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 periodo de validez del certificado.
- La clave pública Sujeto debe usar el algoritmo de RSA y tener una longitud de 1024, 2048 ó 4096 bits.
- El campo Uso de la clave debe contener Firma digital.
- El Nombre alternativo del sujeto debe contener el nombre principal del usuario (UPN).
- El campo Uso mejorado de claves debe contener Inicio de sesión de tarjeta inteligente y Autenticación del cliente o Todos los usos de la clave.
- Una de las entidades de certificación en la cadena de emisores del certificado debe coincidir con uno de los nombres distintivos (DN) enviado por el servidor durante el protocolo de enlace TLS.

Cambie el modo en que se seleccionan los certificados, usando alguno de estos métodos:

- En la línea de comandos de Citrix Receiver para Windows, especifique la opción `AM\_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }`.

La opción predeterminada es “Prompt” (Preguntar). Para SmartCardDefault (predeterminado de la tarjeta inteligente) o LatestExpiry (fecha de caducidad más lejana), si hay varios certificados que cumplen esos criterios, Citrix Receiver para Windows pide al usuario que elija uno.

- Agregue el siguiente valor a la clave de Registro HKCU o HKLM\Software\[Wow6432Node]Citrix\AuthManager\CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry } .

Los valores definidos en HKCU tienen preferencia sobre los valores definidos en HKLM para facilitar al usuario la selección de certificado.

## Para usar solicitudes de PIN del proveedor de servicios criptográficos (CSP)

De manera predeterminada, los diálogos de PIN que se presentan a los usuarios provienen de Citrix Receiver para Windows en lugar de venir del proveedor CSP (Cryptographic Service Provider) de la tarjeta inteligente. Citrix Receiver para Windows solicita a los usuarios que introduzcan un PIN cuando es necesario, y pasa ese PIN al proveedor CSP de la tarjeta inteligente. Si el sitio o la tarjeta inteligente tiene unos requisitos de seguridad más estrictos (por ejemplo, prohibir el almacenamiento del PIN en caché por proceso o por sesión), puede configurar Citrix Receiver para Windows 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 entrada de PIN usando alguno de estos métodos:

- En la línea de comandos de Citrix Receiver para Windows, especifique la opción AM\_SMARTCARDPINENTRY=CSP.
- Agregue el siguiente valor a la clave de Registro HKLM\Software\[Wow6432Node]Citrix\AuthManager: SmartCardPINEntry=CSP.

## Configurar la autenticación PassThrough de dominio con Kerberos

January 7, 2019

Lo descrito en este artículo se aplica solo a conexiones entre Citrix Receiver para Windows y StoreFront, XenDesktop o XenApp.

Citrix Receiver para Windows respalda Kerberos para la autenticación PassThrough de dominio en implementaciones que usan tarjetas inteligentes. Kerberos es uno de los métodos de autenticación incluidos en la autenticación de Windows integrada (IWA).

Cuando la autenticación Kerberos está habilitada, Kerberos se autentica sin contraseña de Citrix Receiver para Windows, y así impide ataques de tipo troyano que intentan acceder a las contraseñas del dispositivo de usuario. Los usuarios pueden iniciar una sesión en el dispositivo de usuario con cualquier método de autenticación; por ejemplo, un autenticador biométrico, tal como un lector de huellas digitales, y aún acceder a los recursos publicados sin necesidad de otra autenticación.

Citrix Receiver para Windows gestiona la autenticación PassThrough con Kerberos del siguiente modo cuando Citrix Receiver para Windows, StoreFront, XenDesktop y XenApp están configurados para usar la autenticación con tarjeta inteligente y el usuario inicia sesión con una tarjeta inteligente:

1. El servicio Single Sign-on de Citrix Receiver para Windows captura el PIN de la tarjeta inteligente.
2. Citrix Receiver para Windows usa la autenticación integrada de Windows (Kerberos) para autenticar al usuario en StoreFront. A continuación, StoreFront proporciona a Citrix Receiver para Windows información sobre las aplicaciones y los escritorios virtuales disponibles.  
Nota: No tiene que usar la autenticación Kerberos para este paso. Solo se necesita habilitar Kerberos en Citrix Receiver para Windows para evitar que se vuelva a pedir el PIN. Si no se usa la autenticación Kerberos, Citrix Receiver para Windows se autentica en StoreFront con las credenciales de la tarjeta inteligente.
3. El motor de HDX (antes conocido como cliente ICA) pasa el PIN de la tarjeta inteligente a XenDesktop o XenApp para iniciar la sesión Windows del usuario. A continuación, XenDesktop o XenApp entregan los recursos solicitados.

Para usar autenticación Kerberos con Citrix Receiver para Windows, compruebe que la configuración de Kerberos cumple lo siguiente.

- Kerberos solo funciona entre Citrix Receiver para Windows y servidores que pertenecen a los mismos dominios de Windows o a dominios que son de confianza. Los servidores también deben ser de confianza para la delegación, una opción que se configura a través de la herramienta de administración de usuarios y equipos de Active Directory.
- Kerberos debe estar habilitado en el dominio y en XenDesktop y XenApp. 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 autenticación Básica, para usar siempre la información de inicio de sesión especificada o para pedir siempre una contraseña.

El resto de este tema describe cómo configurar la autenticación PassThrough de dominio para los escenarios de uso más frecuentes. Si migra a StoreFront desde la Interfaz Web y previamente utilizó una solución de autenticación personalizada, póngase en contacto con un representante del servicio de asistencia de Citrix Support para obtener más información.

#### **Advertencia**

Parte de las configuraciones descritas en este tema contienen modificaciones del Registro. El uso incorrecto del Editor del Registro del sistema puede causar problemas graves que pueden hacer necesaria la reinstalación del sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Asegúrese de hacer una copia de seguridad del Registro antes de editarlo.

## Para configurar la autenticación PassThrough de dominio con Kerberos para usarla con tarjetas inteligentes

Si no está familiarizado con implementaciones de tarjeta inteligente en un entorno XenDesktop, le recomendamos que consulte la información sobre tarjetas inteligentes que figura en la sección [Proteger la implementación](#) de la documentación de XenDesktop antes de continuar.

Cuando instale Citrix Receiver 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 permite a Citrix Receiver para Windows autenticarse en StoreFront mediante IWA (Kerberos). El componente Single Sign-on guarda el PIN de la tarjeta inteligente, que luego es utilizado por el motor HDX cuando comunica de forma remota el hardware de tarjeta inteligente y las credenciales a XenDesktop. XenDesktop selecciona automáticamente un certificado desde la tarjeta inteligente y obtiene el PIN desde el motor HDX.

Hay una opción relacionada, ENABLE\_SSON, que está habilitada de manera predeterminada y debe dejarse así.

Si hay una directiva de seguridad que impide la habilitación de Single Sign-On en un dispositivo, configure Citrix Receiver para Windows con la directiva siguiente:

Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > Autenticación de usuarios > Nombre de usuario y contraseña locales

### Nota

En este caso, quiere permitir que el motor de HDX use la autenticación de tarjeta inteligente y no Kerberos, de modo que no use la opción ENABLE\_KERBEROS=Yes, ya que forzaría al motor de HDX a usar Kerberos.

Para aplicar la configuración, reinicie Citrix Receiver para Windows en el dispositivo de usuario.

Para configurar StoreFront:

- En el archivo default.ica ubicado en el servidor StoreFront, defina DisableCtrlAltDel con el valor false.

### Nota

Este paso no es necesario si todas las máquinas cliente ejecutan Citrix Receiver para Windows 4.2 o una versión posterior.

- Durante la configuración del servicio de autenticación en el servidor StoreFront, marque la casilla PassThrough de dominio. Este parámetro habilita la autenticación de Windows integrada (IWA). No es necesario marcar la casilla 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.

### **Acerca de la API de FastConnect y la autenticación básica HTTP**

La API de FastConnect usa el método de autenticación básica HTTP, que frecuentemente se confunde con métodos de autenticación asociados con el paso de credenciales de dominio (PassThrough), Kerberos y la autenticación integrada de Windows (IWA). Citrix recomienda inhabilitar IWA en StoreFront y en la directiva de grupo ICA.

## **Habilitar la comprobación de la lista de revocación de certificados para mejorar la seguridad**

October 5, 2018

Cuando está habilitada la comprobación de la lista de revocación de certificados (CRL), Citrix Receiver para Windows verifica si el certificado del servidor se ha revocado. Al obligar a Citrix Receiver para Windows a realizar esta verificación, se puede mejorar la autenticación criptográfica del servidor, así como la seguridad general de la conexión TLS entre un dispositivo de usuario y el servidor.

Se pueden habilitar varios niveles de verificación de revocación de certificados (CRL). Por ejemplo, se puede configurar Citrix Receiver para Windows de forma que verifique solo la lista local de certificados, o para que verifique las listas de certificados locales y de red. Además, se 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 va a realizar este cambio en un equipo local, salga de Citrix Receiver para Windows. Compruebe que todos los componentes de Citrix Receiver para Windows, incluida la **Central de conexiones**, estén cerrados.

Para obtener información sobre cómo configurar TLS, consulte [Configurar y habilitar TLS](#).

## **Proteger comunicaciones**

July 31, 2018

Para proteger la comunicación entre los sitios de XenDesktop o las comunidades de servidores XenApp y Citrix Receiver para Windows, se pueden integrar las conexiones de Citrix Receiver para Windows con la ayuda de tecnologías de seguridad como las siguientes:

- Citrix NetScaler Gateway. Para obtener más información, consulte los temas de esta sección además de la documentación de NetScaler Gateway y StoreFront.  
Nota: Citrix recomienda utilizar NetScaler Gateway para proteger las comunicaciones entre los servidores StoreFront y los dispositivos de los usuarios.
- Un firewall. Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino. Si utiliza Citrix Receiver para Windows a través de un firewall de red que asigna la dirección IP de red interna del servidor a una dirección de Internet externa (es decir, traducción de direcciones de red o NAT), configure la dirección externa.
- Configuración de confianza del servidor.
- Solamente para implementaciones de XenApp o la Interfaz Web; no se aplica a XenDesktop 7: un servidor proxy SOCKS o un servidor proxy seguro (también conocido como servidor proxy de seguridad o servidor proxy HTTPS). Se pueden utilizar servidores proxy para limitar el acceso hacia y desde la red, y para gestionar las conexiones entre Receiver y los servidores. Receiver respalda protocolos de proxy seguro y SOCKS.
- Para implementaciones de XenApp o Interfaz Web solamente; no se aplica a XenDesktop 7, XenDesktop 7.1, XenDesktop 7.5 o XenApp 7.5: Soluciones de Traspaso SSL con protocolos TLS (Transport Layer Security).
- Para XenApp 7.6 y XenDesktop 7.6, puede habilitar una conexión SSL directamente entre los usuarios y los VDA.

Citrix Receiver para Windows es compatible y funciona con entornos en los que se utilizan las plantillas de seguridad de escritorio de Microsoft Specialized Security - Limited Functionality (SSLF). Estas plantillas reciben respaldo en varias plataformas de Windows.

Consulte las guías de seguridad de Windows disponibles en <http://technet.microsoft.com> para obtener más información sobre las plantillas y su configuración.

## Aplicar relaciones de confianza

November 16, 2018

El parámetro “Servidor de confianza” identifica y aplica relaciones de confianza en las conexiones de Citrix Receiver para Windows.

Cuando se habilita la característica “Servidor de confianza”, Citrix Receiver para Windows especifica los requisitos y decide si la conexión con el servidor es de confianza o no. Por ejemplo, si Citrix Receiver para Windows se conecta a una dirección determinada (por ejemplo, [https://\\*.citrix.com](https://*.citrix.com)) a través de un tipo de conexión específico (por ejemplo, TLS), se redirige a una zona de confianza en el servidor.

Al habilitar esta característica, servidor conectado reside en la zona “Sitios de confianza” de Windows.

Para ver instrucciones detalladas sobre cómo agregar servidores a la zona “Sitios de confianza” de Windows, consulte la ayuda en línea de Internet Explorer.

Para habilitar la configuración de servidor de confianza mediante la plantilla administrativa de objeto de directiva de grupo

**Requisito previo:**

Debe salir de los componentes de Citrix Receiver para Windows, incluida la Central de conexiones.

1. Como administrador, abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
  - a) Para aplicar la directiva en un solo equipo, abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver desde el menú Inicio.
  - b) Si quiere aplicar la directiva en un dominio, abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver desde la Consola de administración de directivas de grupo.
2. Desde el nodo Configuración del equipo, vaya a **Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > Enrutamiento de red > Configuración de servidores de confianza**.
3. Marque **Habilitado** para obligar a que Citrix Receiver para Windows realice la identificación de la región.
4. Marque **Aplicar configuración de servidor de confianza**. Eso obliga al cliente a realizar la identificación mediante un servidor de confianza.
5. Desde la lista desplegable **Zona de Internet de Windows**, seleccione la dirección del servidor de cliente. Esta configuración solo se aplica a la zona “Sitios de confianza” de Windows.
6. En el campo **Dirección**, establezca la dirección del servidor de cliente en una zona “Sitios de confianza” que no sea Windows. Puede utilizar una lista separada por comas.
7. Haga clic en **Aceptar** y **Aplicar**.

## Configurar la autenticación con tarjeta inteligente para la Interfaz Web

### 5.4

October 5, 2018

Si se instala Citrix Receiver para Windows con un componente de Single Sign-On (SSON), la autenticación PassThrough se habilita de forma predeterminada incluso aunque la autenticación PassThrough de PIN para tarjeta inteligente no esté habilitada en el sitio PNAgent de XenApp; la configuración de PassThrough como método de autenticación ya no tiene efecto. En la pantalla siguiente, se muestra cómo habilitar la tarjeta inteligente como método de autenticación cuando Citrix Receiver para Windows está configurado correctamente con SSON.

Use la directiva de extracción de tarjetas inteligentes para controlar el comportamiento de extracción de tarjetas inteligentes cuando un usuario se autentica en el sitio PNAgent de la Interfaz Web de Citrix 5.4.

Si esta directiva está habilitada, la sesión del usuario se cierra en la sesión de XenApp si se extrae la tarjeta inteligente del dispositivo cliente. No obstante, la sesión de usuario de Citrix Receiver para Windows sigue abierta.

Para que esta directiva se aplique, la directiva de extracción de tarjetas inteligentes debe establecerse en el sitio de servicios XenApp de la Interfaz Web. Los parámetros se encuentran en la Interfaz Web 5.4, en **Sitio de servicios XenApp > PassThrough con tarjeta inteligente > Habilitar movilidad > Cerrar las sesiones al quitar la tarjeta inteligente**.

Cuando la directiva de extracción de tarjetas inteligentes está inhabilitada, la sesión de XenApp del usuario se desconecta si se extrae la tarjeta inteligente del dispositivo cliente. Extraer la tarjeta inteligente en el sitio de servicios XenApp de Interfaz Web no tiene ningún efecto.

**Nota:** Hay directivas distintas para clientes de 32 bits y 64 bits. Para dispositivos de 32 bits, el nombre de la directiva es **Directiva de extracción de tarjetas inteligentes (máquina de 32 bits)**, mientras que, para los dispositivos de 64 bits, el nombre de la directiva es **Directiva de extracción de tarjetas inteligentes (máquina de 64 bits)**.

## Cambios en la extracción y el respaldo a tarjetas inteligentes

Tenga en cuenta lo siguiente cuando se conecte a un sitio PNAgent de XenApp 6.5:

- A partir de Citrix Receiver para Windows 4.5, el inicio de sesión con tarjeta inteligente se admite para los inicios de sesión en el sitio PNAgent.
- La directiva de extracción de tarjetas inteligentes ha cambiado en el sitio PNAgent: Una sesión de XenApp se cierra cuando se extrae la tarjeta inteligente: si el sitio PNAgent está configurado con la tarjeta inteligente como método de autenticación, la directiva correspondiente debe configurarse explícitamente en Receiver para Windows para aplicar el cierre de la sesión de XenApp. Habilite la movilidad para la autenticación con tarjeta inteligente en el sitio PNAgent de XenApp y habilite la directiva de extracción de tarjetas inteligentes, la cual cierra la sesión de XenApp de la sesión de Receiver (la sesión del usuario sigue abierta en Receiver).

## Limitación

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

## Conectar a través de un servidor proxy

July 31, 2018

Se usan servidores proxy para limitar el acceso hacia y desde la red, así como para administrar las conexiones entre los servidores y Citrix Receiver para Windows. Citrix Receiver para Windows admite protocolos de proxy seguro y SOCKS.

En la comunicación con la comunidad de servidores, Receiver utiliza los parámetros de servidor proxy configurados de forma remota en el servidor que ejecuta Receiver para Web o la Interfaz Web. Para obtener más información sobre la configuración de servidores proxy, consulte la documentación de StoreFront o de la Interfaz Web.

En la comunicación con el servidor Web, Receiver utiliza los parámetros de servidor proxy configurados a través de la configuración de Internet del explorador Web predeterminado en el dispositivo de usuario. Se deben configurar los parámetros de Internet del explorador Web predeterminado en el dispositivo de usuario según corresponda.

Configure el proxy con el Editor del Registro para indicar a Citrix Receiver para Windows que acepte o descarte el servidor proxy durante las conexiones.

### Advertencia

Si edita el Registro de forma incorrecta, pueden producirse problemas graves, que pueden hacer que sea necesario instalar nuevamente el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse.

1. Vaya a HKLM\Software\Citrix\AuthManager\.
2. Defina **ProxyEnabled** (REG\_SZ).
  - a) True: Citrix Receiver para Windows acepta al servidor proxy durante las conexiones.
  - b) False: Citrix Receiver para Windows descarta al servidor proxy durante las conexiones.
3. Cierre el Editor del Registro.
4. Reinicie la sesión de Citrix Receiver para Windows para que los cambios surtan efecto.

## Conectar a través de un firewall

April 2, 2019

Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino. Si utiliza un firewall en la implementación, Citrix Receiver para Windows debe poder comunicarse a través de él con el servidor Web y el servidor Citrix.

## Puertos comunes de comunicación Citrix

Origen	Tipo	Puerto	Detalles
Citrix Receiver	TCP	80/443	Comunicación con StoreFront
ICA/HDX	TCP	1494	Acceso a aplicaciones y escritorios virtuales
ICA/HDX con fiabilidad de la sesión	TCP	2598	Acceso a aplicaciones y escritorios virtuales
ICA/HDX por SSL	TCP	443	Acceso a aplicaciones y escritorios virtuales
ICA/HDX de Receiver HTML5	TCP	8008	Acceso a aplicaciones y escritorios virtuales
Sonido ICA/HDX por UDP	TCP	16500 - 16509	Intervalo de puertos para sonido ICA/HDX
IMA	TCP	2512	Arquitectura IMA (Independent Management Architecture)
Consola de administración	TCP	2513	Consolas de administración Citrix y * Nota de servicios WCF: Para plataformas FMA 7.5 y posterior, no se utiliza el puerto 2513.
Solicitud de aplicación o escritorio	TCP	80/8080/443	Servicio XML
STA	TCP	80/8080/443	Secure Ticket Authority (incrustada en el servicio XML)

### Nota

En XenApp 6.5, XenApp Commands Remoting Service utiliza el puerto 2513 a través de WCF.

Si el firewall se ha configurado para la traducción de direcciones de red (NAT), es posible usar la In-

terfaz Web para definir las asignaciones desde las direcciones internas hacia las direcciones externas y los puertos. Por ejemplo, si el servidor XenApp o XenDesktop no se ha configurado con una dirección alternativa, es posible configurar la Interfaz Web para proporcionar una dirección alternativa a Receiver. A continuación, Citrix Receiver para Windows se conecta al servidor mediante la dirección externa y el número de puerto. Para obtener más información, consulte la documentación de [Interfaz Web](#).

## ICA File Signing para proteger ante el inicio de aplicaciones y escritorios desde servidores que no son de confianza

November 16, 2018

La función ICA File Signing (firma de archivos ICA) permite protegerse ante inicios no autorizados de escritorios y aplicaciones. Citrix Receiver para Windows verifica si el inicio de la aplicación o del escritorio fue generado desde una fuente de confianza (para ello, se basa en una directiva de administración), y protege al usuario frente a inicios originados en servidores que no sean de confianza. Puede configurar ICA File Signing utilizando la plantilla administrativa de objeto de directiva de grupo, StoreFront o Citrix Merchandising Server. La función ICA File Signing no está habilitada de forma predeterminada. Para obtener más información sobre cómo habilitar ICA File Signing para StoreFront, consulte la documentación de StoreFront.

Para la implementación de Interfaz Web, la Interfaz Web habilita y configura los inicios de escritorios y aplicaciones para incluir una firma durante el proceso de inicio mediante el servicio Citrix ICA File Signing. Este servicio permite firmar los archivos ICA con un certificado proveniente del almacén de certificados personal del equipo.

Citrix Merchandising Server con Citrix Receiver para Windows permite y configura la verificación de firmas para el inicio mediante el asistente de la consola de administración Citrix Merchandising Server Administrator Console > Deliveries para agregar sellos de certificados de confianza.

### Configurar ICA File Signing mediante plantilla administrativa de objeto de directiva de grupo

#### 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 Citrix Receiver mediante la ejecución de 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 blanca de sellos de certificados de confianza.
  - b) **Certificados de confianza**: Haga clic en “Mostrar” para eliminar el sello del certificado con firma existente en la lista blanca. 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 desplegable.
    - i. **Permitir inicios con firma solamente (más seguro)**: Permite los inicios de solamente escritorios o aplicaciones con firma desde servidores de confianza. Aparece una advertencia de seguridad en caso de una firma no válida. No puede iniciar la sesión debido a que no se autoriza.
    - ii. **Preguntar al usuario en inicios sin firma (menos seguro)**: Aparece un mensaje cuando se inicia una sesión sin firma o sin firma válida. Puede optar por continuar el inicio o cancelarlo (opción predeterminada).
4. Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.

### **Para seleccionar y distribuir un certificado de firma digital**

Cuando se seleccione un certificado de firma digital, Citrix recomienda elegir a partir de la lista siguiente, en el orden siguiente:

1. Adquiera un certificado con firma de código o un certificado con firma SSL a partir de una entidad de certificados (CA) pública.
2. Si su empresa dispone de una entidad de certificados privada, cree un certificado con firma de código o un certificado con firma SSL a través de la entidad de certificados privada.
3. Utilice un certificado SSL existente, como el certificado del servidor de la Interfaz Web.
4. Cree un certificado raíz nuevo y distribúyalo a los dispositivos de usuario mediante un objeto de directiva de grupo o una instalación manual.

### **Configurar conjuntos de cifrado obsoletos**

October 5, 2018

#### **Nota**

Cuando actualiza o instala Citrix Receiver para Windows por primera vez, debe agregar los archivos de plantilla más recientes al GPO local. Para obtener más información sobre cómo agregar los archivos de plantilla al GPO local, consulte [Configurar la plantilla administrativa](#)



de objeto de directiva de grupo. En caso de una actualización, la configuración existente se conserva si se importan los archivos más recientes.

1. Abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver; para ello, ejecute gpedit.msc.
2. En el nodo “Configuración del equipo”, vaya a **Plantillas administrativas > Componente de Citrix > Citrix Receiver > Enrutamiento de red**.
3. Seleccione la directiva **Conjuntos de cifrado obsoletos**.
4. Seleccione **Habilitada** y elija una de las siguientes opciones:
  - a) **\*TLS\_RSA:\*\*** De forma predeterminada, está seleccionado TLS\_RSA\_\*. Debe seleccionar esta opción para poder utilizar los dos conjuntos de cifrado restantes. Cuando selecciona esta opción, se incluyen estos conjuntos de cifrado:
    - i. TLS\_RSA\_AES256\_GCM\_SHA384
    - ii. TLS\_RSA\_AES128\_GCM\_SHA256
    - iii. TLS\_RSA\_AES256\_CBC\_SHA256
    - iv. TLS\_RSA\_AES256\_CBC\_SHA
    - v. TLS\_RSA\_AES128\_CBC\_SHA
    - vi. TLS\_RSA\_3DES\_CBC\_EDE\_SHA
  - b) **TLS\_RSA\_WITH\_RC4\_128\_MD5:** Seleccione esta opción para utilizar el conjunto de cifrado RC4-MD5.
  - c) **TLS\_RSA\_WITH\_RC4\_128\_SHA:** Seleccione esta opción para utilizar el conjunto de cifrado RC4\_128\_SHA.
5. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
6. Ejecute gpupdate /force para que los cambios surtan efecto.

La tabla siguiente muestra los conjuntos de cifrado en cada grupo:

## Configurar y habilitar TLS

February 20, 2019

Este tema se aplica a XenApp y XenDesktop 7.6 y versiones posteriores.

Para usar el cifrado TLS para todas las comunicaciones de Citrix Receiver para Windows, configure el dispositivo de usuario, Citrix Receiver para Windows y, si usa la Interfaz Web, el servidor que ejecuta la Interfaz Web. Para obtener información sobre cómo proteger la Interfaz Web, consulte la sección [Seguridad](#) en la documentación de la Interfaz Web.

## Requisitos previos

Los dispositivos de los usuarios deben cumplir los requisitos especificados en los [Requisitos del sistema].(/es-es/receiver/windows/current-release/system-requirements.html)

Use esta directiva para configurar las opciones de TLS que garantizan que Citrix Receiver para Windows identifique de forma segura el servidor al que se está conectando y pueda cifrar todas las comunicaciones con el servidor.

Puede usar estas opciones para:

- Exigir el uso de TLS. Citrix recomienda usar TLS para todas las conexiones a través de redes que no son de confianza, como Internet.
- Exigir el uso de la criptografía aprobada por FIPS (Federal Information Processing Standards) para cumplir las recomendaciones de NIST SP 800-52. Estas opciones están inhabilitadas de forma predeterminada.
- Exigir el uso de una versión específica de TLS y de conjuntos de cifrado TLS específicos. Citrix respalda los protocolos TLS 1.0, TLS 1.1 y TLS 1.2 entre Citrix Receiver para Windows y XenApp o XenDesktop.
- 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.

## Configurar respaldo a TLS mediante plantilla administrativa de objeto de directiva de grupo

1. Como administrador, abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
  - Para aplicar la directiva en un solo equipo, abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver desde el menú Inicio.
  - Si quiere aplicar la directiva en un dominio, abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver usando la Consola de administración de directivas de grupo.
2. En el nodo “Configuración del equipo”, vaya a **Plantillas administrativas > Citrix Receiver > Enrutamiento 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. Establezca las siguientes opciones:

**Nota:** Citrix recomienda TLS para las conexiones seguras.

4. Seleccione **Requerir TLS para todas las conexiones** si quiere obligar a Citrix Receiver para Windows a usar TLS en todas las conexiones con aplicaciones y escritorios publicados.
5. En la lista desplegable **Modo de conformidad para la seguridad**, seleccione la opción correspondiente:

- **Ninguno:** No se impone ningún modo de conformidad.
- **SP800-52:** Seleccione **SP800-52** para la conformidad con NIST SP 800-52. Seleccione esta opción solo si los servidores o la puertas de enlace también cumplen las recomendaciones de NIST SP 800-52.

**Nota:**

Si selecciona SP 800-52, se usará automáticamente la criptografía aprobada por FIPS, incluso aunque no esté seleccionada la opción **Habilitar FIPS**. También debe habilitar la opción de seguridad de Windows **Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash**. De lo contrario Citrix Receiver para Windows puede fallar al intentar conectar con aplicaciones y escritorios publicados.

Si selecciona SP800-52, también debe seleccionar la directiva **Comprobación de revocación de certificados** con el valor **Comprobar con acceso completo** o con el valor **Requerir comprobación con acceso completo y lista de revocación de certificados**.

Si selecciona SP 800-52, Citrix Receiver para Windows verifica si el certificado de servidor cumple las recomendaciones de NIST SP 800-52. Si el certificado de servidor no las cumple, Citrix Receiver para Windows no se podrá conectar.

6. **Habilitar FIPS:** Seleccione esta opción para exigir el uso de la criptografía aprobada por FIPS. También debe habilitar la opción de seguridad de Windows **Criptografía de sistema: usar algoritmos que cumplan FIPS para cifrado, firma y operaciones hash** en la directiva de grupo del sistema operativo. De lo contrario Citrix Receiver para Windows puede fallar al intentar conectar con aplicaciones y escritorios publicados.
7. En la lista desplegable **Servidores TLS permitidos**, seleccione el número de puerto. Puede asegurarse de que Citrix Receiver se conecte solo a los servidores especificados, mediante una lista separada por comas. 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 Receiver no reconoce ni confía en el emisor de un certificado, se rechaza la conexión.
8. En la lista desplegable **Versión de TLS**, seleccione cualquiera de las siguientes opciones:
  - **TLS 1.0, TLS 1.1 o TLS 1.2:** Este es el parámetro predeterminado. Esta opción solo se recomienda si es un requisito del negocio usar TLS 1.0 para la compatibilidad.

- **TLS 1.1 o TLS 1.2:** Use esta opción para que las conexiones ICA usen TLS 1.1 o TLS 1.2.
  - **TLS 1.2:** Esta opción se recomienda si TLS 1.2 es un requisito del negocio.
9. **Conjunto de cifrado TLS:** Para exigir el uso de conjuntos de cifrado TLS específicos, seleccione Gubernamental (GOV), Comercial (COM) o Todos (ALL). Para determinadas configuraciones de NetScaler Gateway, es posible que tenga que seleccionar COM. Citrix Receiver para Windows respalda el uso de claves RSA de 1024, 2048 y 3072 bits. También se respaldan certificados raíz con claves RSA de 4096 bits.

Nota: Citrix no recomienda el uso de claves RSA de 1024 bits.

Consulte la siguiente tabla que enumera todos los conjuntos de cifrado respaldados.

- **Cualquiera:** Cuando tiene el valor “Cualquiera”, la directiva no está configurada y se permite cualquiera de los siguientes conjuntos de cifrado:
    - TLS\_RSA\_WITH\_RC4\_128\_MD5
    - TLS\_RSA\_WITH\_RC4\_128\_SHA
    - TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
    - TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
    - TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
    - TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
    - TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
  - **Comercial:** Cuando tiene el valor “Comercial”, se permiten solo los conjuntos de cifrado siguientes:
    - TLS\_RSA\_WITH\_RC4\_128\_MD5
    - TLS\_RSA\_WITH\_RC4\_128\_SHA
    - TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
    - TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
  - **Gubernamental:** Cuando tiene el valor “Gubernamental”, se permiten solo los conjuntos de cifrado siguientes:
    - TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
    - TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
    - TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
    - TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
10. En la lista desplegable **Directiva de comprobación de revocación de certificados**, seleccione alguna de las siguientes opciones:

- **Comprobar sin acceso a red:** Se lleva a cabo una comprobación de la lista de revocación de certificados. Solo se usan almacenes locales de listas de revocación de certificados. Se ignoran todos los puntos de distribución. No es obligatorio encontrar una lista de revocación de certificados para la verificación del certificado del servidor presentado por el servidor de Traspaso SSL/Secure Gateway de destino.
  - **Comprobar con acceso completo:** Se lleva a cabo una comprobación de la lista de revocación de certificados. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Si se encuentra información de revocación de un certificado, se rechaza la conexión. No es obligatorio encontrar una lista de revocación de certificados para la verificación del certificado del servidor presentado por el servidor de destino.
  - **Requerir comprobación con acceso completo y lista de revocación de certificados:** Se hace una comprobación de listas de revocación de certificados, con exclusión de la entidad de certificación (CA) raíz. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Si se encuentra información de revocación de un certificado, se rechaza la conexión. Para la verificación, es necesario encontrar todas las listas de revocación de certificados requeridas.
  - **Requerir comprobación con acceso completo y todas las listas de revocación de certificados:** Se hace una comprobación de listas de revocación de certificados, incluida la entidad de certificación (CA) raíz. Se utilizan los almacenes locales de listas de revocación de certificados y todos los puntos de distribución. Si se encuentra información de revocación de un certificado, se rechaza la conexión. Para la verificación, es necesario encontrar todas las listas de revocación de certificados requeridas.
  - **No comprobar:** No se comprueban listas de revocación de certificados.
11. Puede restringir Citrix Receiver para Windows 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**, Citrix Receiver para Windows solamente acepta certificados de servidor que contienen ese OID de extensión de directiva.
12. En la lista desplegable **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".

13. Use el parámetro **Certificado del cliente** para especificar la huella digital del certificado de identificación y evitar tener que preguntar al usuario innecesariamente.
14. Haga clic en **Aplicar** y **Aceptar** para guardar la directiva.

La tabla siguiente muestra los conjuntos de cifrado en cada grupo:

## Conectar con Secure Gateway

July 31, 2018

Este tema solo se aplica a entornos donde se usa la Interfaz Web.

Es posible usar Secure Gateway en modo Normal o en modo Relay (Traspaso) para proporcionar un canal de comunicaciones seguro entre Citrix Receiver para Windows y el servidor. No es necesario configurar Citrix Receiver para Windows si se utiliza Secure Gateway en modo Normal y los usuarios se conectan a través de la Interfaz Web.

Citrix Receiver para Windows usa parámetros que se configuran de forma remota en el servidor que ejecuta la Interfaz Web para conectarse a los servidores que ejecutan Secure Gateway. Consulte los temas de la Interfaz Web para obtener información sobre la configuración de los parámetros del servidor proxy para Citrix Receiver para Windows.

Para obtener más información sobre la configuración de servidores proxy, consulte la documentación de la Interfaz Web.

Si se instala Secure Gateway Proxy en un servidor de una red segura, se puede utilizar Secure Gateway Proxy en modo de traspaso (Relay).

Si se utiliza el **modo Relay**, el servidor Secure Gateway funciona como un proxy y es necesario configurar Citrix Receiver para Windows para que use lo siguiente:

- El nombre de dominio completo (FQDN) del servidor Secure Gateway.
- El número de puerto del servidor Secure Gateway. Tenga en cuenta que el modo Relay no recibe respaldo en la versión 2.0 de Secure Gateway.

El nombre de dominio completo (FQDN) debe tener los siguientes tres componentes, consecutivamente:

- Nombre de host
- Dominio intermedio
- Dominio superior

Por ejemplo: `mi_equipo.mi_empresa.com` es un nombre de dominio completo porque contiene el nombre de host (`mi_equipo`), un dominio intermedio (`mi_empresa`) y un dominio superior (`com`). Por

lo general, la combinación de nombre de dominio intermedio y dominio superior (mi\_empresa.com) se conoce como nombre de dominio.

## Nivel de elevación y wfcrun32.exe

July 31, 2018

Cuando se habilita el control de cuentas de usuario (UAC) en los dispositivos que ejecutan Windows 10, Windows 8 o Windows 7, solo los procesos que se encuentren en el mismo nivel de integridad o elevación que wfcrun32.exe pueden iniciar las aplicaciones virtuales.

### Ejemplo 1:

Cuando wfcrun32.exe se ejecuta como un usuario normal (no elevado), los procesos como Receiver deben ejecutarse como usuario normal para poder iniciar aplicaciones a través de wfcrun32.exe.

### Ejemplo 2:

Cuando wfcrun32.exe se ejecuta en modo elevado, otros procesos como Receiver, la Central de conexiones y aplicaciones de terceros que usan el objeto Cliente ICA y que se están ejecutando en modo no elevado no se pueden comunicar con wfcrun32.exe.

## Desktop Lock y Citrix Receiver para Windows

April 2, 2019

Puede usar Desktop Lock de Citrix Receiver para Windows cuando los usuarios no necesite interactuar con el escritorio local. Puede seguir usando Desktop Viewer (si está habilitado), pero solo verá el conjunto de opciones que sean estrictamente necesarias en la barra de herramientas: Ctrl+Alt+Supr, Preferencias, Dispositivos y Desconectar.

Desktop Lock de Citrix Receiver para Windows funciona en máquinas unidas a dominios que están habilitadas para el inicio de sesión SSON (Single Sign-On) y configuradas con una tienda; también se puede usar en máquinas que no pertenecen a ningún dominio y no tienen SSON habilitado. No respalda sitios de PNA. Las versiones anteriores de Desktop Lock no reciben respaldo después de actualizar a Citrix Receiver para Windows 4.2 o una versión posterior.

Debe instalar Citrix Receiver para Windows con la opción /includeSSON. Debe configurar la tienda y Single Sign-on, ya sea usando el archivo adm/admx o con opciones de línea de comandos. Para obtener más información, consulte [Instalar y configurar Citrix Receiver mediante la línea de comandos](#).

A continuación, instale Desktop Lock de Citrix Receiver para Windows como administrador con el archivo CitrixReceiverDesktopLock.MSI disponible en la página de [Descargas de Citrix](#).

## Requisitos del sistema para Citrix Receiver Desktop Lock

- Microsoft Visual C++ 2005 Service Pack 1 Redistributable Package. Para obtener más información, consulte la página de [descargas de Microsoft](#).
- Se respalda en Windows 7 (incluida Embedded Edition), Windows 7 Thin PC, Windows 8, Windows 8.1 y Windows 10 (incluida la actualización Anniversary Update).
- Se conecta a StoreFront solo a través de protocolos nativos.
- Puntos finales pertenecientes y no pertenecientes a dominios.
- Los dispositivos de usuario deben estar conectados a una red de área local (LAN) o a una red de área extensa (WAN).

## Acceso a aplicaciones locales

### Importante

Si se habilita el Acceso a aplicaciones locales se puede permitir el acceso al escritorio local, a menos que se haya aplicado un bloqueo completo mediante una plantilla de objeto de directiva de grupo o una directiva similar. Consulte [Configurar el acceso a aplicaciones locales y la redirección de URL](#) en la documentación de XenApp y XenDesktop para obtener más información.

## Funcionamiento de Desktop Lock de Citrix Receiver para Windows

- Puede usar Desktop Lock de Citrix Receiver para Windows con las siguientes funcionalidades de Citrix Receiver para Windows:
  - 3Dpro, Flash, USB, HDX Insight, plug-in de Microsoft Lync 2013 y acceso a aplicaciones locales
  - Solo autenticación de dominio, autenticación de dos factores o autenticación con tarjeta inteligente.
- Al desconectar la sesión de Desktop Lock de Citrix Receiver para Windows, 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 Citrix Receiver para Windows 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. Para obtener más información, consulte [Pasar teclas de acceso directo de Windows a la sesión remota](#).
- Ctrl+F1 activa Ctrl+Alt+Supr cuando se inhabilita la conexión o Desktop Viewer para conexiones de escritorio.

## Para instalar Desktop Lock de Citrix Receiver para Windows

Con este procedimiento, se instala Citrix Receiver para Windows de forma que los escritorios virtuales aparezcan mediante Desktop Lock de Citrix Receiver para Windows. Para las implementaciones que utilizan tarjetas inteligentes, consulte

[Para configurar tarjetas inteligentes y usarlas con dispositivos que ejecutan Receiver Desktop Lock](#).

1. Inicie sesión con una cuenta de administrador local.
2. En el símbolo del sistema, ejecute el siguiente comando (ubicado en la carpeta Citrix Receiver para Windows de los medios de instalación, Receiver y Plug-ins > Windows).

Por ejemplo:

```
1 CitrixReceiver.exe
2   /includeSSON
3 STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/
   discovery;on;Desktop Store"
```

Para obtener detalles sobre los comandos, consulte la documentación de instalación de Citrix Receiver para Windows en [Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos](#).

3. En la misma carpeta de los medios de instalación, haga doble clic en CitrixReceiverDesktopLock.msi. Se abrirá 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 Receiver Desktop Lock.

Para poder administrar el dispositivo de usuario una vez finalizada la instalación, la cuenta que se utilizó para instalar CitrixReceiverDesktopLock.msi se excluye del shell sustituto. Si, más adelante, esa cuenta se elimina, no podrá iniciar sesión ni administrar el dispositivo.

Para ejecutar una **instalación silenciosa** de Receiver Desktop Lock, use la siguiente línea de comandos: `msiexec /i CitrixReceiverDesktopLock.msi /qn`

## **Para configurar Desktop Lock de Citrix Receiver para Windows**

Otorgue acceso solamente a un escritorio virtual de Desktop Lock de Citrix Receiver para Windows por usuario.

Mediante directivas de Active Directory, impida que los usuarios pongan a hibernar los escritorios virtuales.

Para configurar Desktop Lock de Citrix Receiver para Windows, use la misma cuenta de administrador que utilizó para instalarlo.

- Compruebe que los archivos receiver.admx (o receiver.adml) y receiver\_usb.admx (.adml) se han cargado en las Directivas de grupo (las directivas aparecen en: Configuración del equipo o Configuración de usuario > Plantillas administrativas > Plantillas administrativas clásicas (ADMX) > Componentes de Citrix). Los archivos .admX están ubicados en %Program-Files%\Citrix\ICA Client\Configuration\.
- Preferencias de USB. Cuando un usuario conecta un dispositivo USB, ese dispositivo se comunica automáticamente de forma remota con el escritorio virtual, por lo que no se requiere ninguna interacción por parte del usuario. El escritorio virtual es el que controla el dispositivo USB y lo muestra en la interfaz de usuario.
  - Habilite la regla de directivas USB.
  - En Citrix Receiver > 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 Citrix Receiver > Uso remoto de dispositivos cliente, habilite y configure la directiva Asignación de unidades del cliente.
- Micrófono. En Citrix Receiver > Uso remoto de dispositivos cliente, habilite y configure la directiva Micrófono del cliente.

## **Para configurar tarjetas inteligentes y usarlas con dispositivos que ejecutan Desktop Lock de Citrix Receiver para Windows**

1. Configure StoreFront.
  - a) Configure XML Service para usar resolución de direcciones DNS para dar respaldo a 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 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 Receiver > 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 Citrix Receiver para Windows.
  - a) Agregue la dirección URL de Delivery Controller en la lista de Sitios de confianza de Internet Explorer en Windows.
  - b) Agregue la URL del primer grupo de entrega a la lista de sitios de confianza de Internet Explorer en el formato escritorio://nombre-de-grupo-de-entrega.
  - c) Permita a Internet Explorer que utilice el inicio de sesión automático en caso de sitios de confianza.

Cuando Desktop Lock de Citrix Receiver para Windows se instala en el dispositivo de usuario, se aplica una directiva de extracción de tarjetas inteligentes coherente. Por ejemplo, si la directiva de extracción de tarjetas inteligentes de Windows se establece en Forzar cierre de sesión para el escritorio, el usuario debe cerrar la sesión del dispositivo de usuario también, independientemente de cuál sea la directiva de extracción de tarjeta inteligente configurada en el equipo. Esto garantiza que el dispositivo de usuario no quede en un estado inconsistente. Esto se aplica solo a los dispositivos de usuario con Desktop Lock de Citrix Receiver para Windows.

### **Para quitar Desktop Lock de Citrix Receiver para Windows**

Quite los dos componentes de la siguiente lista.

1. Inicie sesión con la misma cuenta de administrador local que usó para instalar y configurar Desktop Lock de Citrix Receiver para Windows.
2. Con la función de Windows para quitar o cambiar programas:
  - Quite Desktop Lock de Citrix Receiver para Windows.
  - Quite Citrix Receiver 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+ImprPant: Toma una captura de pantalla y la guarda en Imágenes.
- Win+Tab: Abre una lista de cambio de ventana.
- Win+T: Vista previa de ventanas abiertas en la barra de tareas.

## SDK y API

October 5, 2018

### Citrix Common Connection Manager SDK

Common Connection Manager (CCM) SDK proporciona un conjunto de interfaces API nativas que le permiten interactuar y realizar operaciones básicas mediante programación. Este SDK no requiere una descarga por separado porque forma parte del paquete de instalación de Citrix Receiver para Windows.

Nota: Algunas de las API que están relacionadas con el lanzamiento de sesiones requieren que el archivo ICA inicie el proceso de lanzamiento para las sesiones de XenApp o XenDesktop.

Las capacidades del CCM SDK incluyen:

- Lanzamiento de sesiones
  - Permite iniciar aplicaciones y escritorios, mediante el archivo ICA generado.
- Desconexión de sesiones
  - Similar a la operación de desconexión mediante la Central de conexiones de Receiver. 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 de Receiver. Se pueden cerrar todas las sesiones o la sesión de un usuario concreto.
- Información de la sesión
  - Proporciona diferentes métodos para obtener información relacionada con la conexión de las sesiones iniciadas. Esto incluye sesiones de escritorio, sesiones de aplicación y sesiones de aplicación integrada

Para obtener más información acerca del SDK, consulte la guía [Programmers guide to Citrix CCM SDK](#).

## Citrix Virtual Channel SDK

El Citrix Virtual Channel Software Development Kit (SDK) ofrece respaldo para la escritura de aplicaciones del lado del servidor y controladores del lado del cliente para canales virtuales adicionales que usan el protocolo ICA. Las aplicaciones de canal virtual del lado del servidor se encuentran en servidores XenApp o XenDesktop. Esta versión del SDK ofrece respaldo para la escritura de canales virtuales nuevos en Receiver para Windows. Si desea 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. El respaldo para canales virtuales proporcionado por VD-API está diseñado para hacer más sencilla la creación de sus propios canales virtuales.
- La API de Windows Monitoring, que mejora la experiencia visual y el respaldo para aplicaciones de terceros integradas con ICA.
- Código fuente operacional de ejemplos de programas de canales virtuales, que demuestran varias técnicas de programación.
- El Virtual Channel SDK requiere el SDK de WF-API para escribir la parte del lado del servidor del canal virtual.

Para obtener más información sobre el SDK, consulte [Citrix Virtual Channel SDK para Citrix Receiver para Windows](#).

## Fast Connect 3 Credential Insertion API

La Fast Connect 3 Credential Insertion API ofrece una interfaz para suministrar credenciales de usuario a la función de inicio de sesión único o Single Sign-on (SSO) de Citrix Receiver para Windows 4.2 y versiones posteriores. Con esta API, los socios de Citrix pueden ofrecer productos de autenticación y SSO que usen StoreFront o la Interfaz Web para iniciar sesiones de usuarios en aplicaciones o escritorios virtuales y luego desconectar a los usuarios de esas sesiones.

Para obtener más información sobre la API de Fast Connect, consulte [Fast Connect 3 Credential Insertion API for Citrix Receiver for Windows](#).





### **Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2019 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).