Citrix Receiver para Windows 4.9 LTSR

Contents

Novedades en la versión 4.9 LTSR

April 16, 2019

Importantes actualizaciones sobre Citrix Receiver

Elementos retirados de la versión TLS de Citrix Cloud

Para mejorar la seguridad de las conexiones a Citrix Cloud, Citrix bloqueará toda comunicación a través de Transport Layer Security (TLS) 1.0 y 1.1 a partir del 15 de marzo de 2019. Sin embargo, estos elementos retirados no afectan a los usuarios de clientes que sigan LTSR de Citrix Receiver para Windows 4.9. Para obtener más información, consulte Elementos retirados de la versión TLS de Citrix Cloud.

Cumulative Update 6 está ya disponible

Cumulative Update 6 (CU6) para Citrix Receiver para Windows 4.9 LTSR se publicó el 19 de marzo de 2019. Con diez correcciones para problemas notificados por nuestros clientes, CU6 sigue mejorando la estabilidad y la sencillez de uso en esta versión LTSR. Citrix Receiver para Windows 4.9 CU6 también contiene las más de 12 correcciones de CU4, 20 correcciones de cada CU5, 18 correcciones de CU2 y más de 15 correcciones presentes en CU1. CU6 está disponible para la descarga desde la página de descargar de Citrix.

Tamaño reducido del instalador

Con esta versión, el tamaño del instalador de Citrix Receiver para Windows se ha reducido a 39,9 MB. Lo que se traduce en una reducción del 15 % en el tamaño con respecto a las versiones anteriores.

Nueva baliza externa para cuentas de StoreFront

En una cuenta de StoreFront, se utiliza “ping.citrix.com” en sustitución de la baliza externa “www.citrix.com”.

A partir de Citrix Receiver para Windows 4.9, no se requiere ningún cambio de configuración por parte del usuario.

Si utiliza una versión anterior de Citrix Receiver para Windows, Citrix recomienda que reemplace la baliza externa “www.citrix.com” por “ping.citrix.com”.

Para obtener más información acerca de la baliza externa, consulte el artículo CTX218708 de Knowledge Center.

Para obtener información sobre la configuración de las balizas externas en StoreFront, consulte Configurar balizas.

> **Nota**
>
> Ignore este contenido si la cuenta de StoreFront no se ha configurado con www.citrix.com como baliza externa.

Problemas resueltos

May 23, 2019

Citrix Receiver para Windows 4.9 LTSR CU6 Hotfix 1 (4.9.6001)

Comparado con: Citrix Receiver para Windows 4.9 LTSR CU6

Problemas de seguridad

- Esta corrección soluciona una problema de seguridad. Para obtener más información, consulte el artículo CTX251986 de Knowledge Center. [LD1518]

Citrix Receiver para Windows 4.9 LTSR CU6

Comparado con: Citrix Receiver para Windows 4.9 LTSR CU5

Redirección de HDX MediaStream para Windows Media

- Podría fallar la obtención de contenido del lado del cliente con la Redirección de Windows Media El problema se produce cuando reproduce archivos multimedia que contienen secuencias de script, que se archivan desde una transmisión web en directo. [LC7948]

Instalación, desinstalación y actualización

- Después de actualizar Citrix Receiver para Windows a la versión 4.9 LTSR, puede que se preserve la clave de Registro que se requiere para los canales virtuales personalizados. [LD0633]

Teclado

- Cuando el **IME local** o la función de **sincronización de la distribución del teclado local** están habilitados, si presiona una combinación de teclas que incluya Ctrl y Mayús derecha, es posible que la tecla Mayús se quede atascada. [LD0585]
- Si selecciona la opción **Sí, prefiero utilizar la distribución del teclado local en vez de la distribución de teclado que ofrece el servidor remoto**, es posible que el último carácter de entrada no se gestione correctamente. El problema se produce cuando cambia de coreano a inglés haciendo clic en la tecla Alt derecha. Tenga en cuenta que después de aplicar esta corrección, el problema podría persistir cuando se utiliza el ratón. [LD0825]

Sesión/Conexión

- Es posible que la redirección de host a cliente no funcione al utilizar algunas aplicaciones de terceros. El problema se produce cuando estas aplicaciones utilizan una dirección URL web especial que contiene direcciones HTTPS y HTTP. [LD0484]
- Si la persistencia de aplicaciones está configurada, es posible que las aplicaciones publicadas no puedan abrir un archivo existente después de que se desconecte la sesión. [LD0742]
- Tiene el tema básico de Windows 7 e inhabilita la aceleración de hardware (modo GDI) en el dispositivo de usuario. Al cambiar entre las aplicaciones integradas locales y publicadas, es posible que experimente problemas de visualización. [LD0853]
- Cuando utiliza las unidades de procesamiento de gráficos NVIDIA en el agente VDA y optimiza el NVENC más reciente en la GPU, puede haber daños en la decodificación DXVA h.264.

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

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\GfxRender

  Nombre: MaxNumRefFrames

  Tipo: DWORD

  Valor: Entre 2 y 8 [LD0943]

Experiencia de usuario

- Al maximizar una ventana no integrada de una aplicación, la ventana de la aplicación está dañada. [LD0755]
- Al iniciar un escritorio publicado con Windows 7, es posible que haya un retraso al mover el cursor dentro de la sesión de Citrix Receiver para Windows. [LD0923]

Citrix Receiver para Windows 4.9 LTSR CU5

Comparado con: Citrix Receiver para Windows 4.9 LTSR CU4

Redirección de contenido

- Cuando cancela la ventana del programa predeterminado mientras inicia la extensión habilitada “Asociación de tipos de archivo” por primera vez, puede aparecer este mensaje de error en los inicios posteriores de esta extensión:

  Windows no tiene acceso al archivo, ruta o dispositivo especificado. Puede que no tenga los permisos apropiados para tener acceso al elemento. [LD0026]

Teclado

- Al usar un lector de códigos de barras, pueden perderse algunos datos si se envía una gran cantidad de datos. [LD0243]

Sesión/Conexión

- Después de actualizar la versión de Citrix Receiver para Windows a la versión 4.9.1000, el CD-Viewer puede mostrar una pantalla gris al cerrar la sesión. [LC9290]
- Pueden fallar los intentos de iniciar una aplicación, aparece este mensaje de error:

  No se puede iniciar la aplicación. Póngase en contacto con el servicio de asistencia y proporcione la siguiente información: No se puede abrir Citrix Receiver.

  - Para habilitar la corrección, el administrador debe establecer la siguiente clave de Registro:

    HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine

    Nombre: EngineTimeout

    Tipo: DWORD

    Valor: Más de 20 segundos
  - Para habilitar la corrección, el usuario debe establecer la siguiente clave de Registro:

    HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine

    Nombre: EngineTimeout

    Tipo: DWORD

    Valor: Más de 20 segundos (por ejemplo, EngineTimeout=20) [LC9771]

- Inicie varias aplicaciones dentro de un escritorio compartido alojado. Si cambia entre los clientes o realiza una operación de desconexión o reconexión, puede aparecer este mensaje de error:

  Citrix HDX Engine has stopped working.
  Exception caused the program to stop working correctly. Cierre el programa. [LC9772]

- Las aplicaciones que se inician a través de Citrix Receiver para Windows podrían reflejarse en un monitor secundario. [LC9893]
- Cuando se minimiza la aplicación integrada, aparece como una versión en miniatura de la aplicación. En vez de ello, debe aparecer como una ventana minimizada o debe aparecer en la barra de tareas. [LD0034]
- La instancia publicada de algunas aplicaciones de terceros podría abrirse como una aplicación transparente al usar las tarjetas gráficas NVIDIA con GPU. [LD0175]
- Los accesos directos de aplicaciones locales que se crean desde el icono del Panel de control no se pueden empezar con **KEYWORDS:Prefer**, configurado desde Citrix Studio. [LD0288]
- Cuando intenta agregar una segunda tienda mediante la plantilla administrativa del objeto de directiva de grupo (GPO), podrían faltar las balizas y demás información en esa segunda tienda. [LD0413]

Excepciones del sistema

- Con la directiva "Redirección de contenido bidireccional" habilitada, el proceso Redirector.exe puede cerrarse inesperadamente si intenta abrir una página web en el explorador web local. Como resultado, la redirección de contenido bidireccional no funciona y aparece este mensaje de error:

  "Citrix FTA, URL Redirector stopped working" (La asociación de tipos de archivo de Citrix y el redirector de URL han dejado de funcionar). [LD0420]

- El proceso wfica32.exe puede cerrarse inesperadamente. El problema se produce cuando los parámetros del proxy están configurados y se intenta iniciar una sesión nueva en Citrix Receiver para Web. [LD0548]

Interfaz de usuario

- Los clics del mouse podrían no generar respuestas en la sesión remota. Este problema puede darse al abrir la ventana **Preferencias** desde la barra de herramientas de Desktop Viewer y establecer el parámetro **MouseTimer** en cualquier valor que no sea el predeterminado. [LD0260]

- Al seleccionar la opción **Restablecer Receiver**, Citrix Receiver para Windows puede solicitar que instale .NET Framework 3.5 en Microsoft Windows 10. [LD0690]

Citrix Receiver para Windows 4.9 LTSR CU4

Comparado con: Citrix Receiver para Windows 4.9 LTSR CU3

Problemas en el dispositivo cliente

- Al utilizar la directiva **Presentación automática del teclado** habilitada, puede que la ventana emergente de teclado automático no funcione en una sesión. [LC9925]

Redirección de HDX MediaStream para Windows Media

- Las secuencias de multidifusión redirigidas que contienen scripts incrustados pueden no recuperar el contenido del cliente. Aparece una pantalla en negro en lugar del vídeo. [LC9775]

Teclado

- Antes de que se introdujera esta corrección, el teclado Starboard modelo 4 de Bloomberg solo admitía el modo PC. Con esta corrección, el teclado Starboard modelo 4 de Bloomberg admite los modos PC y KVM. [LC9984]

Inicio de sesión/Autenticación

- Cuando se usa Citrix Receiver para Windows para agregar una cuenta, al escribir la URL de la tienda podría aparecer este mensaje de error: **No se pudo establecer contacto con el servicio de autenticación**. El problema ocurre cuando una URL de StoreFront comienza con la cadena de texto `citrix.com`. [LC9631]

Sesión/Conexión

- Con KEYWORDS:Prefer configurado desde Citrix Studio, el modificador de la línea de comandos o el argumento que se menciona en el acceso directo de la aplicación que hay en el dispositivo del usuario local podrían no respetarse. [LD0060]
- Esta corrección realiza los siguientes cambios:
  - Cuando se personaliza edtMSS y OutBufLength, edtMSS anula OutBufLength.

  - Cambia los nombres de los parámetros de udt* a edt* en All_regions.ini, defaulit.ica y el Registro.

Nota:
Después de una actualización como administrador, la clave de registro del usuario y las entradas no se renombran de udt* a edt* bajo la clave de Registro HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT. Además, el valor del parámetro no se conserva. [LD0098]

- Es posible que las tiendas agregadas a través del objeto de directiva de grupo (GPO) no se eliminen incluso cuando actualice o elimine la tienda en el GPO. [LD0147]

Excepciones del sistema

- Citrix Receiver para Windows podría cerrarse inesperadamente al iniciar sesión en una tienda. [LC8271]
- Citrix Receiver para Windows se cierra inesperadamente y aparece este mensaje de error: **Citrix HDX Engine ha dejado de funcionar**.

  El problema ocurre cuando hay una captura en el módulo de gráficos. [LC9466]
- El proceso wfica32.exe puede cerrarse inesperadamente al cerrar sesión en el sistema. [LC9892]

TWAIN

- Es posible que Citrix Receiver para Windows 4.7 o versiones posteriores no redirija los escáneres. El problema ocurre cuando los controladores TWAIN 2.0 no están presentes en el dispositivo del usuario. [LC8215]

Experiencia de usuario

- Cuando se establece una conexión VPN utilizando determinadas aplicaciones de terceros, Citrix Receiver para Windows puede permanecer inutilizable durante aproximadamente 15 minutos. [LC9302]
- Cuando se conecta a un Linux VDA 7.17 o versiones posteriores desde Citrix Receiver para Windows, Citrix HDX Engine puede consumir mucha GPU. [LC9506]
- Cuando utiliza el Editor de métodos de entrada (IME) en japonés y escribe texto en una aplicación que está en modo integrado, puede que el texto no se vea. El problema ocurre cuando el tamaño de fuente del texto es pequeño.

  Para habilitar la corrección, establezca las siguientes claves de Registro:

- *En sistemas de 32 bits*:

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client

  Nombre: DisableD3DRenderWidthHeightCheck

  Tipo: REG_DWORD

  Valor: 1
- *En sistemas de 64 bits*:

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow 6432Node\Citrix\ICA Client

  Nombre: DisableD3DRenderWidthHeightCheck

  Tipo: REG_DWORD

  Valor: 1 [LC9882]

Interfaz de usuario

- **Configuration Checker**, que valida la configuración del inicio Single Sign-On, puede quedarse bloqueado verificando el proceso de validación y no completarlo. [LC9625]

Citrix Receiver para Windows 4.9 LTSR CU3

Comparado con: Citrix Receiver para Windows 4.9 LTSR CU2

Problemas en el dispositivo cliente

- En una sesión desde una unidad de cliente asignada, puede que algunos vídeos DVD no se reproduzcan. [LC8912]

Redirección de contenido

- 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]
- 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]

Instalación, desinstalación y actualización

- Después de actualizar Citrix Receiver para Windows a través de System Center Configuration Manager (SCCM), Receiver para Windows puede solicitar un reinicio del sistema. [LC9706]

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 redirige el IME local. [LC9593]

Inicio de sesión/Autenticación

- Después de reiniciarse el proceso AuthManSvr.exe, no se puede cerrar la sesión en Citrix Receiver para Windows. [LC7981]

Impresión

- Cuando intenta imprimir documentos grandes usando el escritor de PDF como la preferencia de impresión, la impresora puede dejar de responder o puede aparecer este mensaje de error:

  "El visor emf ha dejado de funcionar". [LC8882]

Sesión/Conexión

- 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]
- Cuando intenta iniciar un escritorio mediante Microsoft Internet Explorer 11, aparece este mensaje de error:

  "Se ha producido un error en la conexión con con el estado (Error de cliente desconocido)" [LC8841]
- Cuando se configura la agregación entre dos sitios en StoreFront, no se crea la sesión de preinicio. [LC8847]
- 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]

- Puede agotarse el tiempo de espera al intentar iniciar escritorios mediante Citrix Receiver para Windows después de un periodo breve, y esos intentos pueden fallar. El problema ocurre incluso después de aumentar el tiempo de espera para el inicio mediante el parámetro **LaunchTimeoutMs** de StoreFront. [LC9369]
- Después de cambiar la baliza interna en StoreFront, puede que las aplicaciones no se inicien desde Citrix Receiver para Windows hasta que reinicie Citrix Receiver. [LC9442]
- Al cambiar entre varias aplicaciones publicadas mediante las claves Win+TAB o ALT+TAB, pueden aumentar los objetos GDI en el cliente hasta que las aplicaciones dejen de responder y muestren píxeles en negro. [LC9655]

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

- Puede que la ventana de Citrix Receiver para Windows aparezca automáticamente, incluso aunque no se abra la aplicación. El problema ocurre cuando el administrador quita o inhabilita cualquier aplicación publicada que hubiera en Citrix Studio. [LC8176]
- Los iconos del menú Inicio y la barra de tareas pueden parpadear cuando se actualizan las aplicaciones en Citrix Receiver para Windows. [LC8890]
- El cursor del mouse no aparece o aparece pequeño dentro de la sesión de Citrix Receiver para Windows. Puede ocurrir cuando se usan varios monitores con DPI diferentes en dispositivos de punto final que se ejecutan en Microsoft Windows 10. [LC8915]
- El cursor del mouse puede aparecer más pequeño de lo normal dentro de la sesión de Citrix Receiver para Windows. Este problema puede ocurrir cuando se usa una alta resolución de pantalla en los dispositivos de punto final que ejecutan Microsoft Windows 10 versión 1607 y versiones posteriores.

  A continuación, se ofrecen las limitaciones en este caso:

  - El puntero empequeñece cuando se hace clic con el botón secundario en el modo integrado inverso. Vuelve a su tamaño habitual cuando se deja de hacer clic.
  - El puntero se agranda levemente en casos de baja resolución cuando se ejecuta en un VDA para SO de escritorio o servidor anterior a Windows 10 versión 1607 y Windows Server 2016.
  - En un entorno de varios monitores, cuando los PPP de los monitores son diferentes, el puntero del mouse no cambia correctamente de tamaño. El problema ocurre cuando la ventana se mueve por los monitores, y se puede corregir cambiando el tamaño de la ventana de la aplicación.
  - El puntero del mouse sigue apareciendo pequeño en Desktop Viewer en escritorios iniciados. [LC9221]
- Esta corrección soluciona problemas de rendimiento y ofrece mejoras de calidad para Enlightened Data Transport (EDT). [LC9417]

Citrix Receiver para Windows 4.9 LTSR CU2

Comparado con: Citrix Receiver para Windows 4.9 LTSR CU1

Problemas en el dispositivo cliente

- Durante una llamada VoIP, si el usuario 1 inicia una aplicación de grabación de sonido publicada y comienza a grabar, el audio del micrófono del usuario 1 ya no se escucha dentro de la llamada. El usuario 1 puede oír al usuario 2. [LC8713]

Redirección de HDX MediaStream para Flash

- Con el parámetro “Redirección de HDX MediaStream para Flash” habilitado, el proceso PseudoContainer2.exe puede cerrarse inesperadamente al desconectar la sesión. [LC8802]

Redirección de HDX MediaStream para Windows Media

- No se oye la alerta de notificación cuando se envían mensajes usando ciertas aplicaciones de terceros. Esta solución mejora el respaldo para los sonidos que se reproducen durante un espacio corto de tiempo. [LC8468]

Aplicaciones locales HDX integradas

- No se inician las aplicaciones cuando se utiliza la función Acceso a aplicaciones locales **KEYWORDS:prefer=*pattern*** con cualquier aplicación de 64 bits que deba configurarse durante el inicio. [LC8580]

Instalación, desinstalación y actualización

- Después de actualizar Citrix Receiver para Windows, puede que se eliminen algunas claves de Registro que se requieren para canales virtuales personalizados. [LC8414]
- Después de la instalación de la actualización automática de Citrix Receiver para Windows, puede que no se conserve el modificador de línea de comandos **Auto-update**. Como resultado, la configuración de actualización automática se establece en la opción predeterminada. [LC9103]

Sesión/Conexión

- Es posible que fallen los intentos de lanzar sesiones, con el siguiente mensaje de error:

  "El archivo ICA contiene un parámetro sin firma no válido".

  Antes de actualizar o reemplazar el nuevo archivo ADMX, establezca la directiva de firma de archivos ICA "Habilitar ICA File Signing" como "No configurada".

  Nota: La corrección LC5338 funciona en StoreFront 3.0.4000, StoreFront 3.9 y versiones posteriores. [LC5338]
- Cuando inicia el proceso selfservice.exe desde Citrix Receiver para Windows en el primer salto del VDA para SO de servidor, desconectar el primer salto puede provocar que algunas aplicaciones de terceros o el Programador de tareas de Windows ejecute "SelfService.exe –disconnectapps" para desconectar el segundo salto al desconectar el primer salto. Cuando vuelve a conectarse al primer salto, se ejecuta "SelfService.exe –reconnectapps" para volver a conectarse al segundo salto. En este caso, Citrix Receiver para Windows aparece en primer plano (en lugar de aparecer en segundo plano), mientras que las aplicaciones reconectadas aparecen en segundo plano. [LC8224]

Excepciones del sistema

- El proceso wfica32 puede cerrarse intermitentemente cuando se utiliza el canal virtual de Citrix Mobile Receiver. [LC8526]
- Las sesiones de usuario pueden cerrarse inesperadamente al usar la autenticación biométrica del teclado de Bloomberg. [LC8766]
- Las sesiones de usuario pueden cerrarse inesperadamente cuando utiliza un dispositivo de escáner de huellas dactilares Bloomberg dentro de la sesión redirigida a través de la redirección USB. [LC8928]

Experiencia de usuario

- Al usar la función de frase personalizada en la barra de idioma del Editor de métodos de entrada (IME), algunos caracteres pueden desaparecer aleatoriamente en una sesión de usuario. [LC6155]
- Se eliminan los accesos directos de las aplicaciones de streaming que se hayan creado manualmente en los escritorios y la barra de tareas. [LC7500]
- Cuando inicia Citrix Receiver para Windows, el menú Inicio y los accesos directos de escritorio pueden parpadear si las aplicaciones suscritas contienen iconos con bpp = 4 en la ventana de autoservicio de Citrix Receiver. [LC8480]
- Cuando determinadas aplicaciones de terceros intentan enviar una gran cantidad de caracteres a una sesión con aplicaciones HDX integradas habilitadas, pueden enviarse solo algunos caracteres a la aplicación, en lugar de enviarse todos. [LC8560]
- Cuando se inicia un escritorio publicado en el modo de pantalla completa desde una máquina cliente con Windows 7, reproducir un vídeo Flash redirigido puede hacer que las aplicaciones configuradas con **Siempre visible** aparezcan sobre la ventana del visor de escritorio. De forma predeterminada, la corrección está inhabilitada.

  Para habilitar la corrección, establezca las siguientes claves de Registro:

  - *En sistemas de 32 bits*:

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XenDesktop\DesktopViewer

    Nombre: PreventAlwaysOnTopWindowPopover

    Tipo: DWORD

    Valor: 2. Para inhabilitar la corrección, elimine la clave de Registro o establezca su valor en 0.

  - *En sistemas de 64 bits*:

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\XenDesktop\DesktopViewer

    Nombre: PreventAlwaysOnTopWindowPopover

    Tipo: DWORD

    Valor: 2. Para inhabilitar la corrección, elimine la clave de Registro o establezca su valor en 0. [LC8616]
- Cuando actualiza aplicaciones en Citrix Receiver para Windows, los iconos de las aplicaciones de Microsoft Outlook que se anclaron manualmente a la barra de tareas podrían desaparecer. [LC8785]

Interfaz de usuario

- Puede que las aplicaciones no aparezcan en el menú Inicio si cambia la **Opción de parámetros** en Citrix Receiver para Windows y configura StoreFront con la configuración **Inhabilitar suscripciones de usuarios (tienda obligatoria)** para la tienda. [LC8648]

Citrix Receiver para Windows 4.9 LTSR CU1

Comparado con: Citrix Receiver para Windows 4.9 LTSR

Problemas en el dispositivo cliente

- No se pueden usar dispositivos tales como teclados, punteros o monitores conectados a una estación de acoplamiento o un concentrador USB. El problema ocurre cuando la sesión del usuario está en modo de pantalla completa o si la ventana de la sesión tiene el foco, y si usted conecta la estación de acoplamiento o el concentrador a una máquina cliente después de haber iniciado la sesión de usuario. [LC8295]

Redirección de contenido

- La asociación de tipos de archivo puede no funcionar si se inicia sesión en Citrix Receiver para Windows mediante un perfil móvil. [LC8042]

HDX RealTime

- Cuando hay varias cámaras Web del mismo modelo instaladas en el VDA para SO de escritorio, puede que la sesión solo reconozca y asigne la última cámara Web que se instaló. Con esta corrección, se pueden utilizar varias cámaras Web del mismo modelo en cualquier aplicación de videoconferencia dentro de una sesión.

  > **Nota:**
  >
  > – Con la corrección LC5008 instalada, es posible que no pueda cambiar de cámara Web desde la ficha “Preferencias”.
  > – Para habilitar esta corrección, debe instalar una revisión hotfix de servidor y de cliente que incluya la corrección LC5008. [LC5008]

Sesión/Conexión

- Al intentar iniciar Microsoft Internet Explorer como un usuario distinto del usuario conectado actualmente a la sesión mediante el comando "Ejecutar como" y con el proceso Redirector.exe ejecutándose en el sistema, es posible que se abra el explorador Web, pero el contenido no se carga hasta pasados aproximadamente entre 20 y 30 segundos. [LC5227]
- Es posible que no se pueda iniciar un escritorio usando Mozilla Firefox. El problema ocurre cuando Desktop Viewer no elimina el archivo ICA creado previamente en el directorio temporal de Internet Explorer. Resulta en un error de "Acceso denegado" que impide la copia del archivo ICA cuando se lanza una nueva sesión. [LC7883]
- Cuando se lanza una aplicación desde el menú Inicio o con el acceso directo del escritorio, es posible que la aplicación se abra, pero puede aparecer un mensaje de error similar al siguiente:

  "No se encuentra el archivo. Compruebe que se proporcionaron la ruta de acceso y el nombre de archivo correctos". [LC8253]
- Con Citrix Receiver para Windows 4.8 instalado, algunas funciones de un portal Web de empleado pueden no funcionar correctamente. No obstante, cuando el control ActiveX del cliente ICA de Citrix está inhabilitado en Microsoft Internet Explorer, el sitio Web funciona correctamente. [LC8428]

Excepciones del sistema

- Citrix Receiver para Windows puede cerrarse de forma inesperada con el siguiente mensaje de error:

  "Citrix HDX Engine ha dejado de funcionar". [LC8040]
- Citrix Receiver para Windows 4.8 podría experimentar una excepción irrecuperable y mostrar una pantalla azul. El problema ocurre cuando se reinicia el sistema usando algunos modelos de teclado multifunción y ese teclado se conecta y desconecta varias veces del sistema. [LC8182]
- Después de quitar los auriculares de un dispositivo de usuario mientras se reproduce un archivo de audio, la sesión puede dejar de responder hasta que se desconecte y se vuelva a conectar a la sesión. [LC8243]
- Cuando se usa el acceso directo de teclado "Alt + Entrar" en una aplicación integrada publicada, el proceso wfica32.exe puede cerrarse inesperadamente. [LC8317]
- En un caso de doble salto, el proceso wfica32.exe puede cerrarse inesperadamente cuando una sesión se cambia de un cliente a otro. [LC8354]

Experiencia de usuario

- Cuando se graba sonido con calidad de audio Alta, la calidad de la grabación de sonido puede ser deficiente. [LC8241]
- Cuando se restaura una ventana integrada desde la pantalla completa a su tamaño original, en un entorno de monitores múltiples, y luego se la arrastra de vuelta a través de los monitores para ver toda la aplicación, la ventana puede recortarse de forma incorrecta. Como resultado, solo se ve la ventana parcialmente. El problema ocurre con las ventanas integradas que son más anchas que el monitor y, por lo tanto, quedan parcialmente fuera de la pantalla. [LC8325]
- Cuando configura las opciones de acceso directo en el archivo web.config de Store, podrían desaparecer los accesos directos a aplicaciones publicadas en el menú Inicio y el escritorio.

  Nota: Esta corrección ofrece una solución completa para la corrección LC7577. [LC8391]
- Cuando inicia sesión en el modo integrado mientras utiliza Epic Hyperspace, la aplicación podría no permitir que otras aplicaciones que se ejecutan localmente en un punto final aparezcan en primer plano. La aplicación Epic Hyperspace podría conservar el foco hasta que se minimiza. [LC8462]
- Cuando se conecta a un escritorio publicado, pueden aparecer áreas en blanco en el escritorio que cambian al cambiar el tamaño de la ventana. Este error se produce cuando se usa el modo de gráficos antiguo. [LC8518]

Citrix Receiver para Windows 4.9 LTSR

Comparado con: Citrix Receiver para Windows 4.8

HDX 3D Pro

- Con HDX 3D Pro habilitado en un VDA, usar determinadas aplicaciones de terceros puede causar la desconexión del VDA.

  Para habilitar la corrección, establezca las siguientes claves de Registro:

  - *En Windows de 32 bits:*

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

    Client\Engine\Configuration\Advanced\Modules\Thinwire3.0

    Nombre: Tw2IgnoreValidationErrors

    Tipo: REG_SZ

    Valor: TRUE

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

Client\Engine\Configuration\Advanced\Modules\Thinwire3.0

Nombre: Tw2IgnoreExecutionErrors

Tipo: REG_SZ

Valor: TRUE

- *En Windows de 64 bits*

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced

  Nombre: Tw2IgnoreValidationErrors

  Tipo: REG_SZ

  Valor: TRUE

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced

  Nombre: Tw2IgnoreExecutionErrors

  Tipo: REG_SZ

  Valor: TRUE [LC7655]

Administración de sitio/servidor

- Cuando caduca una contraseña de usuario, no se puede interactuar con el formulario de entrada "Cambiar contraseña". El problema se produce cuando la nueva contraseña no cumple el requisito. [LC7943]

Sesión/Conexión

- Cuando se asigna un grupo de escritorios a una dirección IP de cliente externo siguiendo el procedimiento descrito en el artículo CTX128232 de Knowledge Center, el escritorio publicado puede no iniciarse cuando se acceda a él a través de NetScaler Gateway. Puede aparecer el siguiente mensaje de error:

  "No se puede iniciar la aplicación". [LC5932]

- Citrix Receiver para Windows puede no conectarse a StoreFront cuando se conecta a través de la VPN SSL de Juniper. El problema se produce cuando falla la resolución DNS para la dirección URL de StoreFront. [LC6711]

- Citrix Receiver para Windows puede cerrarse inesperadamente cuando se desconecta de un VDA que utiliza una cámara Web integrada. El problema se produce cuando se desconecta del VDA mientras se ejecuta la cámara Web. [LC6815]

- Con Desktop Lock habilitado, la sesión de usuario puede desconectarse automáticamente cuando caduca la sesión de StoreFront. [LC6984]
- Cuando se utiliza el software Epic Hyperspace para el dictado médico, la grabadora del dictado podría dejar de responder en el dispositivo del usuario durante la grabación. [LC7435]
- La sesión de cliente no se inicia cuando se utiliza la API de objetos de cliente de Citrix ICA a través de NetScaler y se configura la "Confianza selectiva de cliente" en el "Objeto de directiva de grupo". [LC7575]
- La asociación de tipo de archivos no abre el documento asociado si el valor del Registro "DisableStubCreation" se ha establecido en "true" en la clave del Registro HKEY_LOCAL_MACHINE\SOFTWARE\Ci (en Windows de 32 bits) y HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle (en Windows de 64 bits). El problema se produce cuando falta el parámetro "%1" en la extensión del nombre del archivo pertinente en la clave del Registro HKEY_CURRENT_USER\SOFTWARE\Classes\Dazzle.**. [LC7619]
- Con el acceso a aplicaciones locales habilitado, puede que el tamaño y la posición de las sesiones del VDA para SO de escritorio iniciadas en el modo de pantalla completa no sean correctos. [LC7646]
- Cuando se agrega una tienda desde los parámetros de directivas de grupo o desde la línea de comandos y se configura la opción de reconectar durante el inicio de sesión de Windows, Citrix Receiver para Windows no se reconecta automáticamente durante el inicio de sesión de Windows. [LC7679]
- Después de reanudar la actividad desde el modo de suspensión, la función Reconexión automática de clientes falla, por lo que las sesiones no se reconectan. [LC7705]
- Con el acceso a aplicaciones locales habilitado, el proceso wfcrun32.exe podría cerrarse inesperadamente. [LC7946]

Tarjetas inteligentes

- Con la configuración de seguridad local "Bloquear estación de trabajo", ubicada en la directiva "Inicio de sesión interactivo: Comportamiento de extracción de tarjetas inteligentes" se establece en una sesión de usuario, la sesión puede no bloquearse cuando quita el lector de tarjetas inteligentes de esa sesión. [LC7571]
- Cuando se llama a la API SCardListReaderGroup en una sesión de usuario desde el servidor, Citrix Receiver para Windows podría no ejecutar la API que se llama en el lado del cliente. [LC7699]

Experiencia de usuario

- En una sesión de usuario, la acción de tocar dos veces en la pantalla táctil de un dispositivo puede no funcionar para algunas aplicaciones. [LC6698]
- Al hacer clic en los iconos de la barra de tareas para cambiar el foco entre las ventanas de una aplicación de terceros en una sesión integrada, la ventana de la aplicación correspondiente de terceros puede no aparecer en primer plano. [LC6709]
- Cuando cambia la resolución del dispositivo de usuario mientras uno de los botones del mouse está presionado, las aplicaciones integradas pueden no recibir el cambio de estado del mouse cuando deja de presionarse el botón. Como resultado, se pierde la acción del mouse. [LC7419]
- Cuando configura las opciones de acceso directo en el archivo web.config de Store, podrían desaparecer los accesos directos a aplicaciones publicadas en el menú Inicio y el escritorio. [LC7577]
- Cuando inicia sesión en el modo integrado mientras utiliza Epic Hyperspace, la aplicación podría no permitir que otras aplicaciones que se ejecutan localmente en un punto final aparezcan en primer plano. La aplicación Epic Hyperspace podría conservar el foco hasta que se minimiza. [LC7906]

Nota: Esta versión de Citrix Receiver para Windows también contiene todas las soluciones que se incluyeron en las versiones 4.8, 4.7, 4.6, 4.5, 4.4, 4.3, 4.2, 4.1, y 4.0.

Problemas conocidos

April 2, 2019

Problemas conocidos en Citrix Receiver para Windows 4.9 LTSR CU6

No se han observado nuevos problemas en esta versión.

Problemas conocidos en Citrix Receiver para Windows 4.9 LTSR CU5

No se han observado nuevos problemas en esta versión.

Problemas conocidos en Citrix Receiver para Windows 4.9 LTSR CU4

No se han observado nuevos problemas en esta versión.

Problemas conocidos en Citrix Receiver para Windows 4.9 LTSR CU3

No se han observado nuevos problemas en esta versión.

Problemas conocidos en Citrix Receiver para Windows 4.9 LTSR CU2

No se han observado nuevos problemas en esta versión.

Problemas conocidos en Citrix Receiver para Windows 4.9 LTSR CU1

Citrix Receiver para Windows 4.9 contiene algunos de los problemas conocidos que presentaban las versiones 4.5, 4.6, 4.7 y 4.8, además del siguiente problema conocido:

- Con Framehawk habilitado, el proceso wfica32.exe puede cerrarse inesperadamente cuando se intenta iniciar y cerrar sesión continuamente. [LCMRFWIN-704]

Problemas conocidos en Citrix Receiver para Windows 4.9

- Cuando inicia una sesión de escritorio en el modo de ventana en Surface Pro, la opción Desktop Viewer puede dejar de responder cuando cambia entre el modo tableta y el modo escritorio. [RFWIN-5837]

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 (descarga en PDF)

Requisitos del sistema y compatibilidad

February 1, 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
  - El Self-Service Plug-in necesita .NET 3.5 Service Pack 1; este plug-in permite a los usuarios suscribirse a escritorios y aplicaciones, e iniciarlos desde la interfaz de usuario de Receiver o desde la línea de comandos. Para obtener más información, consulte Configurar e instalar Receiver para Windows mediante parámetros de línea de comandos.
  - Se necesitan .NET 2.0 Service Pack 1 y Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package.

Matriz de compatibilidad

Citrix Receiver para Windows versión 4.9 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	Explorador Web
Windows 10 [1]	Internet Explorer
Windows 8.1, ediciones de 32 y 64 bits (y Embedded)	La versión más reciente de Google Chrome (se necesita StoreFront)
Windows 7, ediciones de 32 y 64 bits (incluida la Embedded Edition)	La versión más reciente de Mozilla Firefox
Windows Thin PC	Microsoft Edge
Windows Server 2016	
Windows Server 2012 R2, ediciones Standard y Datacenter	
Windows Server 2012, ediciones Standard y Datacenter	
Windows Server 2008 R2, edición de 64 bits	

[1] Admite las actualizaciones de Windows 10 Anniversary Update, Creators Update, Falls Creators Update, la actualización de abril 2018 (versión 1803) y la actualización de octubre 2018 (versión 1809).

> **Nota**
>
> - La actualización de octubre 2018 (versión 1809) solo se admite en Receiver para Windows 4.9 CU5 y versiones posteriores.
> - La actualización de abril 2018 solo se respalda en Receiver para Windows 4.9 CU3 y versiones posteriores.
> - La actualización Falls Creators solo se respalda en Receiver para Windows 4.9 CU1 y versiones posteriores. Receiver para Windows 4.9 no la respalda.

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 Server 2008 R2

Conexiones, certificados y autenticación

April 2, 2019

Conexiones

1. Tienda HTTP
2. Tienda HTTPS
3. NetScaler Gateway 10.5 y versiones posteriores
4. Interfaz Web 5.4

Citrix Receiver para Windows se puede conectar al VDA o se puede establecer una sesión ICA en máquinas que pertenezcan a un dominio de Windows, dispositivos administrados (locales y remotos, con o sin VPN) y en máquinas que no pertenezcan a dominios.

Certificados

1. Privados (autofirmados)
2. Raíz
3. Carácter comodín
4. Intermedios

Certificados privados (autofirmados)

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

> **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). Estos certificados pueden ser emitidos por entidades de certificación (CA) tanto privadas como públicas.

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

	Receiver para Web usando exploradores Web	Sitio de servicios StoreFront (nativo)	Sitio de servicios XenApp de StoreFront (nativo)	NetScaler a Receiver para Web (explorador)	NetScaler a sitio de servicios StoreFront (nativo)
Anónimo	Sí	Sí			
Dominio	Sí	Sí	Sí	Sí*	Sí*
PassThrough de dominio	Sí	Sí	Sí		
Token de seguridad				Sí*	Sí*
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 plug-in de NetScaler instalado en el dispositivo.

> **Nota**
>
> Citrix Receiver para Windows 4.8 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 servicios XenApp de Interfaz Web	NetScaler a Interfaz Web (explorador Web)	NetScaler a sitio de servicios XenApp de Interfaz Web
Anónimo	Sí			
Dominio	Sí	Sí	Sí*	
PassThrough de dominio	Sí	Sí		
Token de seguridad			Sí*	
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 docu-

mentación 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 con 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.
  - 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 autenticación PassThrough.

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**
>
> El HDX RealTime Connector en los servidores XenApp/XenDesktop debe tener la versión 2.0.0.417 como mínimo para la compatibilidad con el nuevo paquete RTME; es decir, RTME 2.0 no se puede usar con el 1.8 RTME Connector.

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

Se puede usar Citrix Receiver para Windows 4.x para actualizar Citrix Receiver para Windows 3.x así como Citrix Online plug-in 12.x.

Si Citrix Receiver para Windows 3.x se instaló por máquina, no se admite la actualización por usuario (realizada por un usuario sin privilegios administrativos).

Si Citrix Receiver para Windows 3.x se instaló por usuario, no se admite la actualización por máquina.

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.

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

Después de desinstalar Citrix Receiver para Windows, las claves de Registro personalizadas de Citrix Receiver para Windows creadas por receiver.adm, receiver.adml o receiver.admx permanecen en el directorio Software\Policies\Citrix\ICA Client en HKEY_LOCAL_MACHINE y HKEY_LOCAL_USER.

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

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 sobre los requisitos de espacio, consulte Requisitos del sistema.

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

CitrixReceiver.exe [Opciones]

Actualización automática

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

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

Opción	/DeferUpdateCount
Descripción	Indica cuántas veces se puede mostrar la opción Recordármelo más tarde. Indica que puede aplazar la actualización esa cantidad de veces. **-1:** Indica que puede aplazar las notificaciones cualquier cantidad de veces (el valor predeterminado es -1). **0:** Indica que no se muestra la opción “Recordármelo más tarde”. **Cualquier otro número:** Indica que 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.
Ejemplo de uso	CitrixReceiver.exe /DeferUpdateCount=-1; CitrixReceiver.exe /DeferUpdateCount=-0; CitrixReceiver.exe /DeferUpdateCount=

Opción	/AURolloutPriority
Descripción	Indica el período en que se puede organizar la implantación de la actualización. **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.
Ejemplo de uso	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 XenDesktop 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
Descripción	Indica que la redirección de contenido bidireccional del cliente al host y del host al cliente está Habilitada.
Ejemplo de uso	CitrixReceiver.exe /ALLOW_BIDIRCONTENTREDIRECTION=1

Habilitar el acceso a aplicaciones locales

Opción	FORCE_LAA=1
Descripción	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.
Ejemplo de uso	CitrixReceiver.exe /FORCE_LAA =1

Mostrar información de uso

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

Omitir el reinicio durante las instalaciones con interfaz de usuario

Opción	/noreboot
Descripción	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
Ejemplo de uso	CitrixReceiver.exe /noreboot

Instalación silenciosa

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

Habilitar autenticación Single Sign-on

Opción	/includeSSON
Descripción	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 Cómo instalar y configurar manualmente Citrix Receiver para la autenticación PassThrough. **Nota:** 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.
Ejemplo de uso	CitrixReceiver.exe /includeSSON

Habilitar Single Sign-on cuando /includeSSON está especificado

Opción	ENABLE_SSON={Yes | No}
Descripción	Habilita el inicio de sesión único (Single Sign-on) cuando se especifica /includeSSON. El valor predeterminado es Yes. Habilita el inicio de sesión único (Single Sign-On) cuando /includeSSON también está especificado. Esta propiedad es necesaria para los inicios de sesión Single Sign-on con tarjeta inteligente. Tenga en cuenta que, 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.
Ejemplo de uso	CitrixReceiver.exe ENABLE_SSON=Yes

Seguimiento permanente

Opción	/EnableTracing={true | false}
Descripción	De manera predeterminada, esta función tiene el valor true. Use esta propiedad para habilitar o inhabilitar explícitamente 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.
Ejemplo de uso	CitrixReceiver.exe /EnableTracing=true

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

Opción	EnableCEIP={true | false}
Descripción	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.
Ejemplo de uso	CitrixReceiver.exe EnableCEIP=true

Especificar el directorio de instalación

Opción	INSTALLDIR=
Descripción	Especifica la ruta de instalación, donde "Directorio de instalación" es la ubicación donde se instalará la mayor parte del software de 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: Authentication Manager, Citrix Receiver, Self-service Plug-in. Si se usa esta opción y se especifica un Directorio de instalación, debe instalar RIInstaller.msi en el directorio Directorio de instalación\Receiver y los demás archivos .msi en el Directorio de instalación.
Ejemplo de uso	CitrixReceiver.exe INSTALLDIR=c:\Citrix\Test

Identificar un dispositivo de usuario

Opción	CLIENT_NAME=<ClientName>
Descripción	Especifica el nombre del cliente, donde ClientName identifica el dispositivo de usuario en el servidor. El valor predeterminado es %COMPUTERNAME%
Ejemplo de uso	CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%.

Nombre de cliente dinámico

Opción	ENABLE_CLIENT_NAME= Yes | No
Descripción	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.
Ejemplo de uso	CitrixReceiver.exe ENABLE_DYNAMIC_CLIENT_NAME =Yes

Instalar componentes especificados

Opción	ADDLOCAL=<característica… ,>
Descripción	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. Los componentes son: ReceiverInside (instala la experiencia de Citrix Receiver) e ICA_Client (instala Citrix Receiver estándar). Ambos componentes son necesarios para el funcionamiento de Receiver. 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 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 respaldan .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 Receiver o desde una línea de comandos, según se describe más adelante en esta sección, en “Para iniciar una aplicación o un escritorio virtual desde la línea de comandos”. USB: Instala el respaldo para USB. Requiere derechos de administrador. DesktopViewer: Instala Desktop Viewer. Flash: Instala el componente HDX MediaStream para Flash. Vd3d: Habilita la interfaz de Windows Aero (para los sistemas operativos que lo

Opción	ADDLOCAL=<característica… ,>
Ejemplo de uso	CitrixReceiver.exe ADDLO- CAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopView

Configurar Citrix Receiver para Windows para agregar tiendas manualmente

Opción	ALLOWADDSTORE={N | S | A}
Descripción	Especifica si los usuarios pueden agregar o quitar tiendas que no han sido configuradas a través de entregas de Merchandising Server; los usuarios pueden habilitar o inhabilitar tiendas configuradas a través de entregas de Merchandising Server, pero no pueden quitar dichas tiendas ni cambiar el nombre de las URL. El valor predeterminado es “S”. Las opciones disponibles son: “N”, que no permite nunca que los usuarios agreguen o quiten su propia tienda; “S”, que permite que los usuarios agreguen o quiten solamente tiendas seguras (configuradas con HTTPS) y “A”, que permite que los usuarios agreguen o quiten tanto tiendas seguras (HTTPS) como no seguras (HTTP). No se aplica si Citrix Receiver se instaló mediante una instalación por usuario. También puede controlar esta característica actualizando la clave de Registro HKLM\Software[Wow6432Node]Citrix\Dazzle\AllowAddStore. **Nota:** De forma predeterminada, únicamente se permiten tiendas seguras (HTTPS) y se recomienda utilizar éstas para entornos de producción. Para entornos de pruebas, puede usar conexiones a tiendas HTTP mediante la siguiente configuración: Establezca HKLM\Software[Wow6432Node]Citrix\Dazzle\AllowAddStore en “A” para permitir que los usuarios agreguen tiendas no seguras. Estabezca HKLM\Software[Wow6432Node]Citrix\Dazzle\AllowSavePwd en “A” para permitir que los usuarios guarden contraseñas de tiendas no seguras. Para permitir agregar una tienda configurada en StoreFront con un Tipo de transporte de HTTP, agregue a HKLM\Software[Wow6432Node]Citrix\AuthManager el valor ConnectionSecurityMode (tipo REG_SZ) y establézcalo en “Any”. Salga de Citrix Receiver y reinícielo.

Opción	ALLOWADDSTORE={N | S | A}
Ejemplo de uso	CitrixReceiver.exe ALLOWADDSTORE=N

Guardar las credenciales de las tiendas localmente usando el protocolo PNAgent

Opción	ALLOWSAVEPWD={N | S | A}
Descripción	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”. Las opciones son: “N”, que nunca permite que los usuarios guarden sus contraseñas; “S”, que permite a los usuarios guardar contraseñas solo para tiendas seguras (configuradas con HTTPS); “A”, que permite a los usuarios guardar contraseñas para tiendas seguras (HTTPS), tiendas no seguras (HTTPS) y tiendas no seguras (HTTP). También se puede controlar esta característica actualizando la clave de Registro HKLM\Software[Wow6432Node]\Citrix\Dazzle\AllowSavePwd **Nota:** La siguiente clave de registro se debe agregar manualmente si AllowSavePwd no funciona: Clave para el SO cliente de 32 bits: HKLM\Software\Citrix\AuthManager. •Clave para el SO cliente de 64 bits: HKLM\Software\wow6432node\Citrix\AuthManager •Tipo: REG_SZ •Valor: never - No permitir nunca a los usuarios guardar sus contraseñas. secureonly - Permitir a los usuarios guardar contraseñas solo para las tiendas seguras (configuradas con HTTPS). always - Permitir a los usuarios guardar sus contraseñas tanto para las tiendas seguras (HTTPS) como para las no seguras (HTTP).
Ejemplo de uso	CitrixReceiver.exe ALLOWSAVEPWD=N

Seleccionar el certificado

Opción	AM_CERTIFICATESELECTIONMODE={Prompt |SmartCardDefault | LatestExpiry}
Descripción	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 esto al usuario y se le da la opción de usar un método de inicio de sesión alternativo, si hay alguno disponible. 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 esto al usuario y se le da la opción de usar un método de inicio de sesión alternativo, si hay alguno disponible. También puede controlar esta característica actualizando la clave de Registro HKCU o HKLM\Software[Wow6432Node]Citrix\AuthManager:Certificat Prompt | SmartCardDefault | LatestExpiry }. Los valores definidos en HKCU tienen preferencia sobre los valores definidos en HKLM para facilitar al usuario la selección de certificado.
Ejemplo de uso	CitrixReceiver.exe AM_CERTIFICATESELECTIONMODE=Prompt

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

Opción	AM_SMARTCARDPINENTRY=CSP
Descripción	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.
Ejemplo de uso	CitrixReceiver.exe AM_SMARTCARDPINENTRY=CSP

Usar Kerberos

Opción	ENABLE_KERBEROS={Yes | No}
Descripción	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 la autenticación PassThrough de dominio con Kerberos.
Ejemplo de uso	CitrixReceiver.exe ENABLE_KERBEROS=No

Mostrar iconos de FTA antiguos

Opción	LEGACYFTAICONS={False | True}
Descripción	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.
Ejemplo de uso	CitrixReceiver.exe LEGACYFTAICONS=False

Habilitar el preinicio de sesiones

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

Especificar el directorio para los accesos directos del menú Inicio

Opción	STARTMENUDIR={Nombre del directorio}
Descripción	De forma predeterminada, las aplicaciones aparecen en Inicio > Todos los programas. Se puede especificar una ruta relativa bajo la carpeta de programas para contener los accesos directos a las aplicaciones suscritas. Por ejemplo, para colocar accesos directos en Inicio > Todos los programas > Receiver, especifique STARTMENUDIR=\Receiver. Los usuarios pueden cambiar el nombre de la carpeta o mover la carpeta cuando lo deseen. También se puede controlar esta característica mediante una clave de Registro. Para ello, cree la entrada REG_SZ para StartMenuDir y otórguele el valor “\RelativePath”. Ubicación: HKLM\Software[Wow6432Node]Citrix\Dazzle; HKCU\Software\Citrix\Dazzle. 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 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. **Nota**: Windows 8/8.1 no permite 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. Ejemplos: •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 > Todos los programas > Office. •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 > Todos los programas > Receiver > Office. Los cambios que se hagan a estos parámetros no tienen impacto alguno en los accesos directos ya creados. Para mover accesos directos, es

Opción	STARTMENUDIR={Nombre del directorio}
Ejemplo de uso	CitrixReceiver.exe STARTMENUDIR=\Office

Especificar el nombre de la tienda

Opción	STOREx="storename;http[s]://servername.domain/IISLocatio | Off] ; [storedescription]" [STOREy="…"]
Descripción	Use esta opción para especificar el nombre de la tienda. Especifica hasta 10 tiendas para usar con Citrix Receiver. Valores: x e y (números enteros de 0 a 9); storename (el valor predeterminado es la tienda). Este valor debe coincidir con el nombre configurado en el servidor StoreFront. servername.domain: El nombre de dominio completo del servidor que aloja la tienda. IISLocation: 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". Para obtener la dirección URL, exporte un archivo de aprovisionamiento desde StoreFront, ábralo en el bloc de notas y copie la URL desde el elemento <Address>. •On | Off: El parámetro de configuración Off opcional permite distribuir 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). storedescription: Una descripción optativa de la tienda, por ejemplo "Tienda de aplicaciones de RRHH". **Nota:** En esta versión, es importante incluir "/discovery" en la URL de la tienda para que la autenticación PassThrough se realice correctamente.
Ejemplo de uso	CitrixReceiver.exe STORE0="Store;`https://test.xx.com/Citrix/Store/Discovery`

Habilitar la redirección de URL en los dispositivos de los usuarios

Opción	ALLOW_CLIENTHOSTEDAPPSURL=1
Descripción	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.
Ejemplo de uso	CitrixReceiver.exe ALLOW_CLIENTHOSTEDAPPSURL=1

Especificar el directorio para los accesos directos de escritorio

Opción	DESKTOPDIR=<Nombre del directorio>
Descripción	Coloca todos los accesos directos en una misma carpeta. Se admite el uso de CategoryPath para los accesos directos de escritorio. **Nota:** Cuando se usa la opción DESKTOPDIR, configure la clave PutShortcutsOnDesktop con el valor True.
Ejemplo de uso	CitrixReceiver.exe DESKTOPDIR=\Office

Actualizar desde una versión de Citrix Receiver no respaldada

Opción	/rcu
Descripción	Permite actualizar una versión no respaldada a la versión más reciente de Citrix Receiver.
Ejemplo de uso	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 instalar todos los componentes de manera silenciosa y especificar dos tiendas de aplicaciones:

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

Para especificar la autenticación con Single Sign-On (autenticación PassThrough o paso de credenciales) y agregar una tienda que haga referencia a una URL de servicios XenApp:

CitrixReceiver.exe /INCLUDESSON /STORE0="PNAgent;https://testserver.net/Citrix/PNAgent/config.xml;on;My PNAgent Site"

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 Active Directory y scripts de inicio de ejemplo

October 5, 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 implementar 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. No obstante, en el caso de que necesite implementar Citrix Receiver para Windows por usuario en lugar de por equipo, hay dos scripts de Citrix Receiver incluidos en los medios de instalación de XenDesktop y XenApp en la carpeta Citrix Receiver and Plug-ins\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, 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.

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 nombres de los archivos de instalación de Citrix Receiver para Windows son los mismos que los de 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.

Implementar mediante System Center Configuration Manager 2012 R2

January 7, 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 **Siguiente**.

    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 **Siguiente**.

    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 **Siguiente**.

4. En el panel **Programación**, especifique la programación para implementar el software en los dispositivos de destino.
5. En el panel **Experiencia del usuario**, establezca el comportamiento de las **Notificaciones de usuario**; seleccione **Confirmar cambios dentro de la fecha límite o en una ventana de mantenimiento (reinicio necesario)** y haga clic en **Siguiente** para completar el asistente para implementar software. En el panel "Finalización", se muestra un mensaje 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 **Siguiente**.
4. En el panel "Reglas de pertenencia", haga clic en **Agregar regla** para filtrar los dispositivos. Aparecerá el Asistente para crear reglas de pertenencia directa.
   - En el panel "Buscar recursos", seleccione el **Nombre 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 **Siguiente**. En el panel "Seleccionar recursos", seleccione los dispositivos que deben formar parte de la colección de dispositivos. En el panel "Finalización", se muestra un mensaje indicando que la operación es correcta.
6. Haga clic en **Cerrar**.
7. En el panel "Reglas de pertenencia", aparecerá una nueva regla. Haga clic en **Siguiente**.
8. En el panel "Finalización", se muestra un mensaje 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.

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.

Si tiene usuarios que se conectan desde fuera de la red interna (por ejemplo, usuarios que se conectan desde Internet o desde ubicaciones remotas), 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 aparecerán en el 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: Indique descripciones claras para las aplicaciones de los grupos de entrega. Los usuarios de Citrix Receiver para Windows verán esas descripciones cuando usen el acceso Web o el modo de autoservicio.

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. Como administrador, abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
    - Si desea aplicar la directiva en un solo equipo, ábrala desde el menú Inicio.
    - Si desea aplicar la directiva en un dominio, ábrala usando la Consola de administración de directivas de grupo.
2. En el nodo "Configuración del equipo", vaya a "Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > StoreFront", y seleccione "Lista de cuentas de StoreFront/URL de NetScaler Gateway".
3. 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.
4. Agregue o especifique la URL de NetScaler. Introduzca el nombre de la dirección URL separada por punto y coma:

> **Ejemplo:**
>
> `HRStore; https://dtls.blrwinrx.com\##Store name;On; Store for HR staff`
> Donde #Store name es el nombre de la tienda detrás de NetScaler Gateway y dtls.blrwinrx.com es la dirección URL de NetScaler.
>
> Cuando Citrix Receiver para Windows se inicie después de agregar el NetScaler Gateway mediante 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 aprovisionadas automáticamente, destacadas y obligatorias.

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

- Para hacer obligatoria una aplicación concreta (de forma que no pueda 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.

Como administrador, puede configurar los accesos directos mediante directivas de grupo.

1. Abra el Editor de directivas de grupo local ejecutando el comando 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.
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, vaya a la carpeta Configuration de Receiver y seleccione receiver.admx (o receiver.adml).

5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para volver 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 > Autoservicio.
7. Seleccione Administrar modo Self-Service para habilitar o inhabilitar la interfaz de usuario de autoservicio de Receiver.
8. Elija “Administrar accesos directos de aplicaciones” para habilitar o inhabilitar:
    - Accesos directos en el escritorio
    - Accesos directos en el menú Inicio
    - Directorio en el escritorio
    - Directorio en el menú Inicio
    - Ruta de categoría para accesos directos
    - Quitar aplicaciones al cerrar la sesión
    - Quitar aplicaciones al salir
9. Elija “Permitir a los usuarios agregar o quitar cuentas” para dar a los usuarios privilegios para agregar o quitar más de una cuenta.

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).

NOTE: 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 Receiver con **PutShortcutsInStartMenu=false** y habilite los parámetros por aplicación. **Nota:** Este parámetro solo se aplica a sitios de Interfaz Web.

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

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 fun-

cionalidad 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\ReceiverStub
    b) Reg add HKLM\Software\Citrix\Dazzle /v
    c) opyStubsFromCommonStubDirectory /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 reinícielo 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 *auto* (aprovisionada automáticamente) y *mandatory* (obligatoria) para las aplicaciones, según sea necesario.
Si quiere que el usuario elija las aplicaciones que quiera colocar en su menú Inicio, pero también quiere colocar accesos directos específicos en el escritorio…	Configure 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 (*auto*) y obligatorias (*mandatory*), según sea necesario.

Menú Inicio sin accesos directos de aplicaciones

Si el usuario utiliza un equipo doméstico que usa toda la familia, es posible que no sea necesario o conveniente colocar accesos directos. En tales casos, lo más sencillo es usar el acceso por explorador Web; instale 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 PutShortcutsInStartMenu=False. 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. **Nota:** Este parámetro solo se aplica a sitios de Interfaz Web.

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**. **Note:** 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.
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 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 Word 2010	Sí
"Microsoft Word"	\Microsoft Office\Microsoft Word 2010	Sí
Consola	\McAfee\VirusScan Console	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

*KEYWORDS:prefer=	Acceso directo en Programas	¿Coincide?
“\Programs\Microsoft Word 2010”	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 Optimizar la experiencia de usuario en la documentación de StoreFront.

Configurar el entorno de XenDesktop

November 16, 2018

Una vez instalado el software de Citrix Receiver para Windows, los usuarios pueden realizar los siguientes pasos de configuración para acceder a sus aplicaciones y 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.

- Actualización automática - La actualización automática ofrece actualizaciones automáticas para Citrix Receiver para Windows y para HDX RealTime Optimization Pack, sin necesidad de descargar las actualizaciones manualmente. Para obtener más información sobre la configuración de la actualización automática, consulte Configurar la actualización automática.
- 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 tiene la capacidad de realizar 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

November 16, 2018

> **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 (optativo)

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. Como administrador, abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
   - Si desea aplicar la directiva en un solo equipo, ábrala desde el menú Inicio.
   - Si desea aplicar la directiva en un dominio, ábrala usando la Consola de administración de directivas de grupo.

   Para obtener información sobre cómo importar la plantilla administrativa de Citrix Receiver para Windows en el Editor de directivas de grupo, consulte Configurar Citrix Receiver para Windows con la plantilla de objeto de directiva de grupo.
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 alterativa 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 actualización automática

April 2, 2019

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

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

Configurar mediante la 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.
   - Si desea 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 desea 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** > **Componentes de Citrix** > **Citrix Receiver** > **Actualización automática**.

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 periodo 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 Actualización automática, seleccione la directiva **Habilitar o inhabilitar actualización automática**.
7. Marque **Habilitada** y establezca los valores según sea necesario:
    - En la lista desplegable **Habilitar directiva de actualización automática**, 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 la actualización automática 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 la actualización automática como usuario usando los parámetros de línea de comandos durante la instalación de Citrix Receiver:
  - **/AutoUpdateCheck=**auto/manua**l**

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

Cuando se modifican los parámetros de actualización automática 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

La actualización automática 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 lo general, CitrixReceiverUpdater.exe se encuentra en *Ubicación de la instalación de Citrix Receiver*\Citrix\Ica Client\Receiver.

También se puede establecer la directiva de línea de comandos de la actualización automática mediante este binario.

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

- CitrixReceiverUpdater.exe */AutoUpdateCheck=auto /AutoUpdateStream= STSR /DeferUpdateCount=-1 / AURolloutPriority= fast*

Configurar mediante la interfaz gráfica de usuario

Un usuario individual puede anular la configuración de actualización automática usando 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 notificación.
2. Seleccione **Preferencias avanzadas** y haga clic en **Actualización automática**.

   Aparecerá el cuadro de diálogo de Actualización automática.

3. Seleccione una de estas opciones:
    - Sí, notificarme
    - No, no notificarme
    - Usar parámetros especificados por el administrador
4. Haga clic en **Guardar**.

Configurar la actualización automática 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:

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

   ```
   <account>
   <clear />
       <account id=”d1197d2c-ac82-4f13-9346-2ee14d4b0202” name=”F84Store”
        description=”” published=”true” updaterType=”Citrix” remoteAccessType=”None”>
        <annotatedServices>
         <clear />
         <annotatedServiceRecord serviceRef=”1__Citrix_F84Store”>
          <metadata>
           <plugins>
            <clear />
           </plugins>
           <trustSettings>
            <clear />
   ```



```
    </trustSettings>
    <properties>
     <property name=”Auto-Update-Check” value=”auto” />
     <property name=”Auto-Update-DeferUpdate-Count” value=”1” />
          <property name=”Auto-Update-LTSR-Only” value=”FALSE” />
     <property name=”Auto-Update-Rollout-Priority” value=”fast” />
         </properties>
   </metadata>
  </annotatedServiceRecord>
 </annotatedServices>
 <metadata>
  <plugins>
    <clear />
  </plugins>
  <trustSettings>
    <clear />
  </trustSettings>
  <properties>
    <clear />
  </properties>
 </metadata>
</account>
```

auto-update-Check

Esto indica que Citrix Receiver para Windows detecta cuando 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.
- Disabled: La actualización automática está inhabilitada.

auto-update-LTSR-Only

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

Valores válidos:

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

auto-update-DeferUpdate-Count

Esto 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:

Esto 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.

Limitaciones:

1. El sistema debe tener acceso a Internet.
2. Los usuarios de Receiver para Web no pueden descargar automáticamente la directiva de StoreFront.
3. 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).
4. De forma predeterminada, la actualización automática está inhabilitada en el VDA. Esto incluye máquinas de servidor multiusuario RDS, máquinas VDI y Remote PC.

5. La actualización automática está inhabilitada en las máquinas donde está instalado Desktop Lock.

Configurar la redirección de contenido bidireccional

January 7, 2019

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

1. Plantilla administrativa de objeto de directiva de grupo
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 objeto de directiva de grupo

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

1. Como administrador, abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
    - Si desea aplicar la directiva en un solo equipo, ábrala desde el menú Inicio.
    - Si desea aplicar la directiva en un dominio, ábrala usando la Consola de administración de directivas de grupo.
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 separadas 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).

Limitaciones:

- 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` 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.

Configurar teclados Bloomberg

January 7, 2019

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

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

Para habilitar o inhabilitar el respaldo para teclados Bloomberg:

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. 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 la entrada 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. Para ello, debe modificar 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 DisableDimming en una de las siguientes claves, dependiendo de si quiere impedir la atenuación solo para el usuario actual del dispositivo, o para el dispositivo propiamente dicho. 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 dispositivos USB compuestos

January 7, 2019

Configurar la redirección de dispositivos USB compuestos usando la 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**.
   a) Si desea 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 desea 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 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. Como administrador, abra la plantilla administrativa de objeto de directiva de grupo de Citrix Receiver mediante la ejecución de gpedit.msc.
    a) Si desea 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 desea 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 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

Dividido	Interfaz	Acción
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

Limitaciones:

Citrix recomienda que no dividida interfaces para una cámara Web. Como solución alternativa, se puede redirigir el dispositivo como dispositivo único mediante la redirección de USB genérico. Para obtener un mejor rendimiento, use el canal virtual optimizado.

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 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:** Tenga en cuenta que, 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 escaneado 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 escaneado) requiere configuración adicional. Para obtener instrucciones, consulte el artículo CTX123015 de Knowledge Center.

- **Almacenamiento masivo (clase 08)**. Los dispositivos de almacenamiento masivo más comunes son las unidades flash USB. Otros 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: Se sabe que 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, conversores de vídeo analógico, algunos sintonizadores de televisión y algunas cámaras digitales que admiten la transmisión por secuencias de vídeo.

> **Nota:** 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 por usuario

Citrix recomienda usar el archivo de plantilla de objeto de directiva de grupo (GPO) receiver.admx o receiver.adml para configurar 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 el archivo de plantilla receiver.admx 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.

Nota: Esta característica solo está disponible en el servidor XenApp.

Para configurar dispositivos de sonido USB por usuario

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 Receiver en el Editor de directivas de grupo, puede omitir los pasos del 2 al 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 (en máquinas de 32 bits, C:\Archivos de programa\Citrix\ICA Client\Configuration; en máquinas de 64 bits, C:\Archivos de programa (x86)\Citrix\ICA Client\Configuration) y seleccione receiver.admx.
5. Seleccione **Abrir** para agregar la plantilla y luego, haga clic en **Cerrar** para regresar al Editor de directivas de grupo.

6. 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**.
7. Modifique los parámetros.
8. Haga clic en **Aplicar** y, a continuación, en **Aceptar**.
9. Abra el símbolo del sistema en modo de administrador.
10. Ejecute el siguiente comando
    gpupdate /force

Nota: Los cambios en la directiva requieren que el servidor XenApp se reinicie para que surtan efecto.

Configurar StoreFront

April 2, 2019

Citrix StoreFront autentica a los usuarios en XenDesktop, XenApp y VDI-in-a-Box, y enumera y agrupa los escritorios y las aplicaciones disponibles en almacenes o tiendas, 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**
>
> Citrix Receiver para Windows en ocasiones muestra la interfaz de usuario de StoreFront antigua en lugar de la actualizada después de mostrar la opción para ver todos los almacenes o tiendas.

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, 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. 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 cunado 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 desparezca 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 8/8.1 no permite 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 escrito-

rios 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.

Puede usar parámetros del Registro para personalizar los accesos directos. Puede establecer las claves del Registro en las siguientes ubicaciones. Cuando son aplicables, se aplican en el orden de preferencia listado.

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.

> **Nota:**
>
> 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

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
RemoveAppsOnLogoff	Falso	HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle; HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
RemoveAppsOnExit	Falso	HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle; HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
PutShortcutsOnDesktop	Falso	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM \SOFTWARE\Citrix\Dazzle
PutShortcutsInStartMenu	Verdadero	HKCU\Software\Citrix\Receiver\SR\Store+Sto HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle
SelfServiceMode	Verdadero	HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle
UseCategoryAsStartMenuPath	Verdadero	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM \SOFTWARE\Citrix\Dazzle

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
StartMenuDir	"" (vacío)	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM \SOFTWARE\Citrix\Dazzle
DesktopDir	"" (vacío)	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle
AutoReinstallModifiedApps	Verdadero	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle
HideEditStoresDialog	Verdadero en SelfServiceMode y Falso en NonSelfServiceMode	HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle; HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
WSCSupported	Verdadero	HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID +\Properties; HKLM\SOFTWARE\Policies\Citrix\Dazzle;HKL

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
WSCReconnectAll	Verdadero	HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectMode	3	HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID +\Properties; HKLM\SOFTWARE\Policies\Citrix\Dazzl; HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectModeUser	El Registro no se crea durante la instalación.	HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID+\Properties; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE \Citrix\Dazzle

Claves de Registro para máquinas de 64 bits

Nombre en el Registro	**Valor predeterminado**	**Ubicaciones por orden de preferencia**
RemoveAppsOnLogoff	Falso	HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Daz HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
RemoveAppsOnExit	Falso	HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Daz HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
PutShortcutsOnDesktop	Falso	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
PutShortcutsInStartMenu	Verdadero	HKCU\Software\Citrix\Receiver\SR\Store+Sto HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
SelfServiceMode	Verdadero	HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
UseCategoryAsStartMenuPath	Verdadero	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
StartMenuDir	”” (vacío)	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
DesktopDir	"" (vacío)	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
AutoReinstallModifiedApps	Verdadero	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
HideEditStoresDialog	Verdadero en SelfServiceMode y Falso en NonSelfServiceMode	HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
WSCSupported	Verdadero	HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID +\Properties; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
WSCReconnectAll	Verdadero	HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz

Nombre en el Registro	Valor predeterminado	Ubicaciones por orden de preferencia
WSCReconnectMode	3	HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID +\Properties; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
WSCReconnectModeUser	El Registro no se crea durante la instalación.	HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID+\Properties; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz

Configurar la presentación de las aplicaciones mediante la interfaz gráfica de usuario

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

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".

a) 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.
b) 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

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**.

Ocultar la Opción de parámetros mediante la interfaz de línea de comandos

Opción	/DisableSetting
Descripción	Impide que Opción de parámetros aparezca en el diálogo Preferencias avanzadas.
Ejemplo de uso	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

Configurar la plantilla administrativa de objeto de directiva de grupo

April 2, 2019

Citrix recomienda usar el Editor de objetos de directiva de grupo 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 .admx/.adml se usan con Windows Vista/Windows Server 2008 y todas las versiones posteriores 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\\\[MUIculture\]
CitrixBase.admx	\ICA Client\Configuration
CitrixBase.adml	\ICA Client\Configuration\\\[MUIculture\]

Nota:

- Si no se agrega CitrixBase.admx\adml al GPO local, se puede perder la directiva Habilitar ICA File Signing.
- Al actualizar 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. 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 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**.

Una vez que los archivos .adm de plantilla han sido agregados al GPO local, aparecerá el siguiente mensaje:
"The following entry in the [strings] section is too long and has been truncated:
(La siguiente entrada en la sección [strings] es demasiado larga y se ha truncado: 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 objetos de directiva de grupo locales y/o aquellos que utilizan dominios. Consulte el artículo de Microsoft MSDN acerca de la administración de archivos ADMX.

1. Después de instalar Citrix Receiver para Windows, copie los archivos de plantilla.

   ADMX:

   De: \ICA Client\Configuration\receiver.admx

   A: %systemroot%\policyDefinitions

   De: \ICA Client\Configuration\receiver.admx

   A: %systemroot%\policyDefinitions

   ADML:

   De: \ICA Client\Configuration\\[MUIculture]receiver.adml

   A: %systemroot%\policyDefinitions\[MUIculture]

   De: \ICA Client\Configuration\\[MUIculture]\CitrixBase.adml

   A: %systemroot%\policyDefinitions\[MUIculture]

Nota:
Los archivos de plantillas de Citrix Receiver para Windows están disponibles en la carpeta “Plantillas administrativas > Componentes de Citrix > Citrix Receiver” solo cuando el usuario agrega CitrixBase.admx o CitrixBase.adml a la carpeta \policyDefinitions.

Proporcionar información de cuentas a los usuarios

April 2, 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 la 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 cuadro de diálogo Agregar cuenta

El cuadro de 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 por 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 Implementación de Receiver para Windows desde Receiver para Web para obtener más información acerca de 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 Configuración de 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 direcciones de 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 tiendas 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://servername.company.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, y hacer clic en , 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 la actualización automática

February 20, 2019

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

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

Configurar mediante la 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.
    - Si desea 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 desea 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** > **Componentes de Citrix** > **Citrix Receiver** > **Actualización automática**.
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 periodo 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 Actualización automática, seleccione la directiva **Habilitar o inhabilitar actualización automática**.
7. Marque **Habilitada** y establezca los valores según sea necesario:

- En la lista desplegable **Habilitar directiva de actualización automática**, 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 la actualización automática 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 la actualización automática como usuario usando 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 actualización automática 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

La actualización automática 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 lo general, CitrixReceiverUpdater.exe se encuentra en *Ubicación de la instalación de Citrix Receiver*\Citrix\Ica Client\Receiver.

También se puede establecer la directiva de línea de comandos de la actualización automática mediante este binario.

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

- CitrixReceiverUpdater.exe */AutoUpdateCheck=auto /AutoUpdateStream= STSR /DeferUpdateCount=-1 / AURolloutPriority= fast*

Configurar mediante la interfaz gráfica de usuario

Un usuario individual puede anular la configuración de actualización automática usando 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 notificación.
2. Seleccione **Preferencias avanzadas** y haga clic en **Actualización automática**.

   Aparecerá el cuadro de diálogo de Actualización automática.
3. Seleccione una de estas opciones:
   - Sí, notificarme
   - No, no notificarme
   - Usar parámetros especificados por el administrador
4. Haga clic en **Guardar**.

Configurar la actualización automática 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:

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

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

```
<account>

    <clear />

    <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="F84Store"

      description="" published="true" updaterType="Citrix"
          remoteAccessType="None">

      <annotatedServices>

        <clear />

        <annotatedServiceRecord serviceRef="1__Citrix_F84Store">

          <metadata>

            <plugins>

              <clear />

            </plugins>

            <trustSettings>

              <clear />

            </trustSettings>

            <properties>

              <property name="Auto-Update-Check" value="auto" />

              <property name="Auto-Update-DeferUpdate-Count" value="1"
                  />

                    <property name="Auto-Update-LTSR-Only" value="
                        FALSE" />
```



```
36
37                <property name="Auto-Update-Rollout-Priority" value="fast
                     " />
38
39                    </properties>
40
41            </metadata>
42
43          </annotatedServiceRecord>
44
45        </annotatedServices>
46
47        <metadata>
48
49          <plugins>
50
51            <clear />
52
53          </plugins>
54
55          <trustSettings>
56
57            <clear />
58
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
```

auto-update-Check

Esto indica que Citrix Receiver para Windows detecta cuando 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.
- Disabled: La actualización automática está inhabilitada.

auto-update-LTSR-Only

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

Valores válidos:

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

auto-update-DeferUpdate-Count

Esto 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:

Esto 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.

Limitaciones:

1. El sistema debe tener acceso a Internet.
2. Los usuarios de Receiver para Web no pueden descargar automáticamente la directiva de StoreFront.

3. 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`.
4. De forma predeterminada, la actualización automática está inhabilitada en el VDA. Esto incluye máquinas de servidor multiusuario RDS, máquinas VDI y Remote PC.
5. La actualización automática está inhabilitada en las máquinas donde está instalado Desktop Lock.

Optimizar el entorno

November 16, 2018

Puede optimizar el entorno:

- Reducir el tiempo de inicio de las aplicaciones
- Facilitar la conexión de los dispositivos con los recursos publicados
- Respaldar la resolución de nombres DNS
- Usar servidores proxy en conexiones de XenDesktop
- Habilitar acceso a aplicaciones anónimas
- Comprobar la configuración de Single Sign-On

Reducir el tiempo de inicio de las aplicaciones

July 31, 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 para el usuario.

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 con-

traseña 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\Ci
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.

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, las impresoras y los 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

Letra de unidad del cliente	El servidor accede a ella como:
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

Actualizado: 27-01-2015

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.

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, también puede modificar los parámetros de proxy mediante la Interfaz Web. Para obtener más información, consulte la documentación de la Interfaz Web.

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

November 16, 2018

A partir de la versión 4.5 de Citrix Receiver para Windows, Configuration Checker permite a los usuarios llevar a cabo 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. Inicie una sesión en Citrix Receiver para Windows.
2. Haga clic con el botón secundario en Citrix Receiver para Windows en el área de notificaciones y seleccione **Preferencias avanzadas**. Aparecerá la ventana Preferencias avanzadas.
3. Seleccione **Configuration Checker**. Aparecerá la ventana de Citrix Configuration Checker.
4. Seleccione **SSONChecker** desde el panel **Seleccionar**.
5. 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 con varias tiendas, la prueba del método de autenticación se ejecuta en todas las tiendas configuradas.

Nota: Los resultados de las pruebas se pueden guardar como informes; el formato predeterminado para los informes es TXT.

Ocultar la opción Configuration Checker de la ventana Preferencias avanzadas:

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.
2. En el Editor de directivas de grupo, vaya a **Componentes de Citrix** > **Citrix Receiver** > **Self Service** > **DisableConfigChecker**.
3. Seleccione **Habilitada**.
   Se oculta 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.

Para que los cambios tengan efecto, cierre y vuelva a abrir el cuadro de diálogo Preferencias avanzadas.

Limitaciones:

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.

Mejorar la experiencia del usuario

April 2, 2019

Es posible mejorar la experiencia del usuario con las siguientes características:

Configurar editores IME de cliente genéricos

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 Sincronización de la distribución de 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:

1. 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.
2. E IME de cliente genérico no recibe respaldo en Internet Explorer versión 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**.

Distribución del teclado

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. En el icono de Citrix Receiver para Windows en el área de notificación, seleccione **Preferencias avanzadas** > **Distribución del teclado local** > **Sí**.
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: El uso de 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, pueden seleccionar la opción **No**, o ejecutar **wfica32:exe/localime:off**. La sesión recurrirá a la distribución de teclado que suministre el servidor remoto cuando se conecten a la sesión siguiente.

En ocasiones, el cambio a la distribución de teclado del cliente no tiene efecto en una sesión activa. Para resolver este problema, cierre la sesión en 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\IcaIme, agregue una nueva clave llamada DisableKeyboardSync y establezca el valor en 0.

> **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.

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 que funciona por 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 obtener más información, consulte Improved User Experience: Hardware Decoding for Citrix Windows Receiver..

> **Nota**
>
> Esta característica no está habilitada de forma predeterminada en las GPU incrustadas.

Para habilitar la decodificación por hardware:

1. Copie “receiver.adml” desde “root\Citrix\ICA Client\Configuration\en” en “C:\Windows\PolicyDefinitions\en US”.
2. Copie “receiver.admx” desde “root\Citrix\ICA Client\Configuration” en “C:\Windows\PolicyDefinitions\”.
3. Vaya al **Editor de directivas de grupo local**.
4. En Configuración del equipo -> Plantillas administrativas -> Citrix Receiver -> Experiencia de usuario, abra **Aceleración de hardware para gráficos**.
5. Seleccione **Habilitada** y haga clic 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: HKCU\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 característica 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 funcionalidad 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 cunado el usuario inicia una sesión. Para cambiar el tiempo de espera, cree el valor REG_DWORD llamado 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 desparezca más pronto.

> **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. Si utiliza el Editor del Registro, será bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Proteger conexiones

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.

La autenticación mediante Desafío/Respuesta de Windows NT (NTLM) recibe respaldo de manera predeterminada en los equipos Windows.

Configurar la autenticación PassThrough de dominio

April 2, 2019

Para obtener más información sobre cómo configurar la autenticación PassThrough de dominio, consulte el artículo CTX133982 en Knowledge Center.

Instalar Citrix Receiver para Windows con Single Sign-On

Hay dos maneras de habilitar la autenticación PassThrough de dominio (SSON) cuando se instala Citrix Receiver para Windows:

- mediante la línea de comandos
- mediante la interfaz gráfica de usuario

Habilitar PassThrough de dominio mediante la interfaz de línea de comandos

Para habilitar el paso de credenciales de dominio PassThrough (SSON) usando la interfaz de línea de comandos:

1. Instale Citrix Receiver 4.x con la opción **/includeSSON**.
    - Instale una o varias tiendas de StoreFront (puede completar este paso más adelante); la instalación de tiendas de StoreFront no es un requisito obligatorio para configurar la autenticación PassThrough de dominio.
    - Para verificar que la autenticación PassThrough está habilitada, inicie Citrix Receiver y compruebe que el proceso ssonsvr.exe se está ejecutando en el Administrador de tareas después de reiniciar el dispositivo de punto final donde está instalado Citrix Receiver.

> **Nota**
>
> Para obtener información sobre la sintaxis para agregar una o más tiendas StoreFront, consulte Configuración e instalación de Receiver para Windows mediante parámetros de línea de comandos.

Habilitar PassThrough de dominio mediante la interfaz gráfica

Para habilitar el paso de credenciales PassThrough de dominio usando la interfaz gráfica:

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:

> **Nota**
>
> El asistente de instalación Habilitar Single Sign-On solo está disponible en instalaciones nuevas en máquinas unidas a dominios.

Para verificar que la autenticación PassThrough está habilitada, inicie Citrix Receiver para Windows y compruebe que el proceso **ssonsvr.exe** se está ejecutando en el Administrador de tareas después de reiniciar el dispositivo de punto final donde está instalado Citrix Receiver para Windows.

Configuraciones de directiva de grupo para SSON

Use la información en esta sección para configurar parámetros de directiva de grupo para la autenticación con SSON.

> **Nota**
>
> El valor predeterminado de la configuración del objeto de directiva de grupo relacionado con SSON es **Habilitar autenticación PassThrough**.

Configurar SSON mediante plantilla administrativa de objeto de directiva de grupo

1. Abra **gpedit.msc**, haga clic con el botón secundario en **Configuración del equipo > Plantillas administrativas > Componentes de Citrix > Citrix Receiver > Autenticación de usuarios**.
2. Habilite las siguientes configuraciones de GPO de equipo local (en la máquina local del usuario y/o en la imagen maestra del VDA de escritorio):
   - Elija el mombre de usuario y contraseña locales.
   - Seleccione **Habilitada**.
   - Seleccione **Habilitar autenticación PassThrough**.
3. Reinicie el dispositivo de punto final (dispositivo donde está instalado Citrix Receiver para Windows) o la imagen maestra del VDA de escritorio.

Usar un archivo ADM para la directiva de grupo de SSON

Use el procedimiento siguiente para configurar parámetros de directiva de grupo usando el archivo ADM:

1. Abra el editor de directivas de grupo local seleccionando **Configuración del equipo > Haga clic con el botón secundario en Plantillas administrativas > Elija Agregar o quitar plantillas**.
2. Haga clic en **Agregar** para agregar una plantilla ADM.
3. Después de agregar la plantilla **receiver.adm**, expanda **Configuración del equipo > Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > Autenticación de usuarios**.
4. Abra Internet Explorer en la máquina local y/o en la imagen maestra del VDA de escritorio.
5. En **Opciones de Internet > Seguridad > Sitios de confianza**, agregue a la lista el nombre de dominio completo (FQDN) de los servidores StoreFront, sin la ruta de la tienda. Por ejemplo: `https://storefront.example.com`

   Nota: También puede agregar el servidor StoreFront a los Sitios de confianza usando un GPO de Microsoft. El GPO se llama **Lista de asignación de sitio a zona** y la encontrará en **Configuración del equipo > Plantillas administrativas > Componentes de Windows > Internet Explorer > Panel de control de Internet > Página Seguridad**.
6. Cierre la sesión y vuelva a iniciarla en el dispositivo de punto final de Citrix Receiver.

Cuando se abre Citrix Receiver, si el usuario actual tiene una sesión iniciada en el dominio, sus credenciales de usuario se transferirán a StoreFront, junto con las aplicaciones y escritorios enumerados dentro de Citrix Receiver, incluidos los parámetros del menú Inicio del usuario. Cuando el usuario hace clic en un icono, Citrix Receiver transfiere las credenciales de dominio del usuario al Delivery Controller y la aplicación o el escritorio seleccionados se abren.

Habilitar Delivery Controller para que confíe en XML

Con el procedimiento siguiente, puede configurar SSON en StoreFront y la Interfaz Web:

1. Inicie una sesión en el (o los) Delivery Controller como administrador.
2. Abra Windows PowerShell (con privilegios administrativos). Mediante PowerShell puede emitir comandos para hacer que Delivery Controller confíe en las solicitudes XML enviadas desde StoreFront.
3. Si aún no están cargados, cargue los cmdlets de Citrix. Para ello, escriba **Add-PSSnapin Citrix** y presione **Entrar**.
4. Presione Entrar.
5. Escriba **Add-PSSnapin citrix.broker.admin.v2** y presione **Entrar**.
6. Escriba S**et-BrokerSite -TrustRequestsSentToTheXmlServicePort $True**, y presione **Entrar**.
7. Cierre PowerShell.

Configurar SSON 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**.

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 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 con 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.

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 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 Editor 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, consulteConfigurar 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. .
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\AuthManage `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=C
- Agregue el siguiente valor a la clave de Registro HKLM\Software\[Wow6432Node]\Citrix\AuthManager: SmartCardPINEntry=CSP.

Habilitar la comprobación de la lista de revocación de certificados para mejorar la seguridad

July 31, 2018

Cuando está habilitada la comprobación de la lista de revocación de certificados (CRL), Citrix Receiver verifica si el certificado del servidor se ha revocado. Al obligar a Citrix Receiver a realizar esta verificación, se puede mejorar la autenticación criptográfica del servidor, así como la seguridad general de las conexiones TLS entre los dispositivos 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 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 si se está ejecutando. Compruebe que todos los componentes de Citrix Receiver, incluida la Central de conexiones, estén cerrados.

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, vaya a la carpeta Configuration de Receiver (normalmente en C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione el archivo de 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. Desde el Editor de directivas de grupo, expanda Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver > Enrutamiento de red > TLS/SSL data encryption and server identification.
7. En el menú Acción, elija Propiedades y seleccione Habilitada.
8. En el menú desplegable Verificación CRL, elija una de las opciones.
   - Inhabilitada. No se lleva a cabo la verificación de revocación.
   - Verificar solo listas de revocación de certificados almacenadas localmente. CRL que se instalaron o descargaron anteriormente y que se utilizan en la validación del certificado. Si se revoca el certificado, la conexión falla.
   - Requiere CRL para la conexión. Se verifican las listas CRL locales y de los emisores de certificados pertinentes en la red. Si se revoca el certificado o no se encuentra, la conexión falla.
   - Obtenga los CRL de la red. Se verifican los CRL de los emisores de certificados pertinentes. Si se revoca el certificado, la conexión falla.
     Si no establece la verificación CRL, se establecerá de forma predeterminada en “Verificar solo listas de revocación de certificados almacenadas localmente”.

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 la documentación de Microsoft para obtener más información sobre las plantillas y su configuración.

Configurar y habilitar TLS

April 2, 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 las comunicaciones con StoreFront, consulte los temas de la sección Proteger en la documentación de StoreFront. Para obtener más información, consulte la documentación de la Interfaz Web.

Requisitos previos:

Los dispositivos de los usuarios deben cumplir los requisitos especificados en los Requisitos del sistema.

Use esta directiva para configurar las opciones de TLS que garantizan que 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.

Para configurar TLS mediante la 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 el parámetro **Directiva de comprobación de revocación de certificados** con el valor **Comprobar con acceso completo** o con el valor **Requerir comprobación con acceso completo y lista de revocación de certificados**.

     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 **Permitir servidores TLS**, 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:

Conjunto de cifrado TLS	**GOB**	**COM**	**TODO**	**GOB**	**COM**	**TODO**	**GOB**	**COM**	**TODO**
Habilitar FIPS	No	No	No	Sí	Sí	Sí	Sí	Sí	Sí
Modo de conformidad SP 800-52 de seguridad	No	No	No	No	No	No	Sí	Sí	Sí
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384			X			X			
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X			
TLS_RSA_WITH_AES_256_GCM_SHA384						X	X		X
TLS_RSA_WITH_AES_256_CBC_SHA256	X	X	X	X	X	X	X	X	X
TLS_RSA_WITH_AES_256_CBC_SHA						X			

TLS_RSA	X		X	X		X	X		X			
TLS_RSA_WITH_AES	X	_128_CBC	X	_SHA		X	X		X	X		
TLS_RSA		X	X									
TLS_RSA_WITH_RC4		_128_MD5										
TLS_RSA	X		X	X		X	X		X			

Configurar la autenticación con tarjeta inteligente para la Interfaz Web 5.4

November 16, 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.

Consulte How to Manually Install and Configure Citrix Receiver for Pass-Through Authentication para obtener más información.

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).

Problema conocido

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

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.

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

Origen	Tipo	Puerto	Detalles
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 Interfaz 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.

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: Indica que Citrix Receiver para Windows acepta al servidor proxy durante las conexiones.
    b) False: Indica que 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.

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 (como `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**.

Nivel de elevación y wfcrun32.exe

January 7, 2019

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.

ICA File Signing para proteger ante el inicio de aplicaciones y escritorios desde servidores que no son de confianza

October 5, 2018

Este tema solo es aplicable a implementaciones con Interfaz Web que usan Plantillas administrativas.

La función ICA File Signing (firma de archivos ICA) permite proteger a los usuarios ante inicios de escritorios y aplicaciones no autorizados. 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 son de confianza. Esta directiva de seguridad de Citrix Receiver para Windows para la verificación de firmas de inicio de aplicaciones o escritorios se puede configurar mediante objetos 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.

En los entornos con 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 del almacén de certificados personal del equipo.

Citrix Merchandising Server con Citrix Receiver para Windows permite configurar e iniciar la verificación de firmas mediante el asistente de la consola de administración Citrix Merchandising Server Administrator Console > Deliveries para agregar sellos de certificados de confianza.

Para usar objetos de directiva de grupo para habilitar y configurar la verificación de firmas de inicio de aplicaciones o escritorios, siga este procedimiento:

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 importó la plantilla ica-file-signing.adm al Editor de directivas de grupo, puede omitir los pasos 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 de configuración de Citrix Receiver para Windows (normalmente C:\Archivos de programa\Citrix\ICA Client\Configuration) y seleccione ica-file-signing.adm.
5. Seleccione Abrir para agregar la plantilla y luego, haga clic en Cerrar para regresar al Editor de directivas de grupo.
6. Desde el Editor de directivas de grupo, vaya a Plantillas administrativas > Plantillas administrativas clásicas (ADM) > Componentes de Citrix > Citrix Receiver y vaya a Habilitar ICA File Signing.
7. Si elige Habilitada, podrá agregar sellos de certificados con firma a la lista blanca de certificados de confianza, o bien quitar los sellos de certificados con firma de la lista blanca haciendo clic en Mostrar y luego use la ventana Mostrar contenido. Puede copiar y pegar los sellos de certificados con firma desde las propiedades de los certificados. Use el menú desplegable Directiva para seleccionar Permitir inicios con firma solamente (más seguro) o Preguntar al usuario en inicios sin firma (menos seguro).

Opción	Descripción
Permitir inicios con firma solamente (más seguro)	Permite inicios de escritorios o aplicaciones con firma solamente desde servidores de confianza. Si un inicio de escritorio o aplicación no dispone de una firma válida, se mostrará al usuario un mensaje de advertencia de seguridad en Citrix Receiver para Windows. El usuario no podrá continuar y se bloqueará el inicio no autorizado.
Preguntar al usuario en inicios sin firma (menos seguro)	Pregunta al usuario cada vez que se realizan intentos de inicio de aplicación o escritorio sin firma o con una firma no válida. El usuario tiene la opción de continuar el inicio de la aplicación o cancelar el inicio (valor predeterminado).

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.

¿Qué es Citrix Receiver?

July 31, 2018

Citrix Receiver brinda acceso a aplicaciones y escritorios virtuales desde cualquier dispositivo, lo que facilita el trabajo desde cualquier ubicación. Receiver es seguro, fácil de usar y consistente en todos los dispositivos.

Nota: Es posible que el administrador no le haya dado acceso a todas las funciones que se describen en estos temas.

Agregar cuentas o cambiar de servidor

July 31, 2018

Si su servicio de asistencia le solicita que agregue una cuenta o utilice otro servidor NetScaler Gateway, siga estos pasos:

Para agregar una cuenta de Citrix Receiver para Windows

1. En la página principal de Citrix Receiver para Windows, haga clic en la flecha hacia abajo y, a continuación, haga clic en **Cuentas**.
2. En la ventana Agregar cuenta, haga clic **Agregar** e introduzca la información que le haya proporcionado el servicio de asistencia técnica.

Para usar otro servidor NetScaler Gateway

Es posible que la empresa utilice un servidor NetScaler Gateway para verificar la identidad de los usuarios.

1. Haga clic con el botón secundario en el icono de Citrix Receiver para Windows y, a continuación, haga clic en **Acerca de**.
2. En el menú **NetScaler Gateway**, elija un servidor.

Cambiar la apariencia y el funcionamiento de los escritorios

January 7, 2019

El escritorio virtual se muestra dentro de una ventana. Use los botones de la barra de herramientas de la ventana para mover el escritorio, cambiar su tamaño y controlar el acceso a los archivos y dispositivos. Hay un pequeño botón de control de la barra de herramientas en la parte superior de la ventana, o de la pantalla (si la ventana está maximizada). La barra de herramientas se muestra al hacer clic en el control.

Para mover la barra de herramientas a otra posición en la pantalla

Puede mover la barra de herramientas a una posición conveniente que no oculte los controles ni el contenido de otras ventanas.

- Haga clic en el control de la barra de herramientas que aparece en la parte superior de la pantalla o ventana y desplácelo hacia la derecha o hacia la izquierda.

Para controlar cómo se accede a los archivos locales

Puede que el escritorio virtual necesite acceder a los archivos del equipo local. El usuario puede controlar este acceso.

- En la barra de herramientas, haga clic en **Preferencias** > **Acceso a archivos**, seleccione y acepte una de las opciones siguientes:

Opción	Descripción
Lectura y escritura	Permite que los archivos locales puedan leerse y sobrescribirse desde el escritorio virtual.

Opción	Descripción
Solo lectura	Permite que los archivos locales puedan leerse pero no sobrescribirse desde el escritorio virtual.
Sin acceso	No permite el acceso a los archivos locales desde el escritorio virtual.
Preguntar siempre	Pregunta al usuario cada vez que el escritorio virtual necesita acceder a los archivos locales.

Para configurar un micrófono o una cámara Web

Siga este procedimiento si desea cambiar la forma en la que su escritorio virtual accede a un micrófono o cámara Web locales.

- En la barra de herramientas, haga clic en **Preferencias** > **Conexiones** y seleccione una de las opciones siguientes:

Opción	Descripción
Conectar automáticamente	Permite el uso del micrófono o la cámara Web en el escritorio virtual.
No conectar	No permite el uso del micrófono o la cámara Web en el escritorio virtual.
Preguntar	Pregunta al usuario cada vez que el escritorio virtual necesita acceder al micrófono o a la cámara Web.

1. En **Parámetros globales**, seleccione su **Cámara Web preferida**.
2. Haga clic en Aceptar.

Limitación:

- El cuadro de diálogo “Cámara Web preferida” se muestra en la Central de conexiones de Citrix, incluso cuando la directiva de redirección de Windows Media está **inhabilitada** en Desktop Delivery Controller.

Mostrar los dispositivos en Desktop Viewer

January 7, 2019

Citrix Receiver para Windows detecta los dispositivos que están conectados al equipo y le permite elegir cuáles de ellos quiere usar con las aplicaciones y los escritorios alojados en servidores.

Puede usar los parámetros de **Preferencias > Conexiones** para personalizar si quiere o no que los dispositivos, tales como micrófonos y cámaras Web, se conecten con la sesión virtual.

- Los dispositivos conectados a la máquina local aparecen en la lista Dispositivo en Preferencias > Dispositivos.
- Si ha conectado un dispositivo, pero no lo ve en la lista de dispositivos, haga clic en “Actualizar”.
- Una vez conectados, los dispositivos aparecen como **Optimizado**, **Restringido por directiva** o **Genérico**.

Dispositivo	Descripción
Optimizado	El dispositivo tiene un canal virtual de Citrix y está disponible automáticamente tanto en la sesión remota como en la máquina local al mismo tiempo. La columna Conexión actual para los dispositivos optimizados muestra que el dispositivo está conectado tanto a la Máquina local como a la Sesión remota. La casilla Redirigir está marcada y no se puede modificar. Se puede cambiar entre Optimizado y Genérico usando el botón Cambiar a en la columna Canal virtual. Por ejemplo, seleccione Cambiar a genérico si el canal virtual no respalda la funcionalidad completa del dispositivo.
Genérico	El dispositivo no tiene un canal virtual de Citrix y no se puede usar en la máquina local y en la sesión remota al mismo tiempo. Marque la casilla Redirigir para cambiar la disponibilidad del dispositivo entre la sesión remota y la máquina local. Puede ver el estado actual de la conexión en la columna Conexión actual.

Dispositivo	Descripción
Restringido por directiva	El administrador ha definido una directiva que restringe el uso de este tipo de dispositivo. Por ejemplo, los punteros y teclados USB están normalmente restringidos por directiva de manera predeterminada porque su comportamiento se controla automáticamente en la sesión remota sin respaldo USB. Otros dispositivos, como los dispositivos de red, pueden estar restringidos por motivos de seguridad. La columna Conexión actual para los dispositivos restringidos por directiva muestra solo Máquina local. En un dispositivo Restringido por directiva no se puede marcar la casilla Redirigir.

Administrar contraseñas

July 31, 2018

Citrix Single Sign-on administra la información necesaria para iniciar sesiones en programas o sitios Web protegidos por contraseña. La información del usuario se guarda en un servidor con el que se puede contactar desde cualquier equipo en la empresa que ejecute Single Sign-on. Eso significa que puede acceder a sus propios programas, configuraciones y trabajar desde muchos lugares dentro de las instalaciones.

Además de automatizar el proceso de inicio de sesión, Single Sign-on le ahorra tiempo porque elimina llamadas al servicio de asistencia técnica de la empresa para restablecer contraseñas o desbloquear cuentas. Single Sign-on puede incluso generar contraseñas nuevas y muy seguras por usted.

Depende de cómo la empresa lo configure, Single Sign-on se inicia cuando se inicia una sesión en el equipo o cuando se inicia por primera vez un programa o sitio Web protegido por contraseña. En ese momento, Single Sign-on se conecta con el servidor donde se encuentra guardada la información del usuario y confirma su identidad. A partir de ese momento, se podrá iniciar la sesión del usuario en cualquier programa o sitio Web para el que se tenga almacenada la información de inicio de sesión correspondiente. También se le puede pedir al usuario que agregue información de inicio de sesión cuando inicie programas o sitios Web para los cuales aún no tiene información almacenada.

Dependiendo de cómo la empresa lo haya configurado, se puede iniciar Single Sign-on desde el menú **Inicio** del sistema:

- En el menú **Inicio**, haga clic en **Todos los programas > Citrix > Citrix Single Sign-on**.

Single Sign-on sólo se cierra cuando se sale de Citrix Receiver para Windows, pero es posible ponerlo en pausa sin necesidad de cerrarlo.

Importante: Single Sign-on es un programa muy flexible que las empresas pueden configurar para ajustarse a sus necesidades específicas. No todas las funciones que se describen aquí estarán disponibles para todos los usuarios. La disponibilidad de las funciones es discreción de la empresa. En algunos casos, tareas enteras, tales como revelar las contraseñas, no estarán disponibles. En otros casos, algunos pasos descritos para una tarea pueden ser un poco diferentes. Se ha hecho lo posible por identificar estas variaciones, pero es posible que descubra otras. Si esto ocurriera, póngase en contacto con la documentación de Citrix.

Usar el autoservicio de cuentas

July 31, 2018

Si está disponible en la empresa, la función de Autoservicio de cuentas de Single Sign-on le permitirá:

- Desbloquear su cuenta de Windows si recibe un mensaje indicando que está bloqueada
- Restablecer la contraseña de su cuenta de Windows si se le olvida y no puede iniciar una sesión en el equipo.

El botón de Autoservicio de cuentas está disponible en la pantalla **Cambiar usuario** (en Windows Vista, Windows 7, Windows Server 2008 o Windows Server 2008 R2) o los cuadros de diálogo **Iniciar sesión en Windows** y **Desbloquear equipo** (en otros sistemas operativos Windows respaldados). Cuando hace clic en ese botón se inicia el Asistente de autoservicio de la cuenta.

Con el Autoservicio de cuentas puede solucionar estos problemas usted mismo sin tener que llamar al servicio de asistencia técnica de la empresa.

Importante: Cuando utilice el Autoservicio de cuentas, se le pedirá que confirme su identidad volviendo a contestar a las preguntas de seguridad de Single Sign-on. Si no conoce las respuestas a las preguntas de seguridad, póngase en contacto con el servicio de asistencia técnica de su empresa para que desbloqueen su cuenta o restablezcan su contraseña de Windows.

Para desbloquear una cuenta (de Windows Vista/Windows 7/Windows Server 2008/Windows Server 2008 R2)

1. Cuando se le pida, presione CTRL+ALT+SUPR.

2. Lleve a cabo una de las siguientes acciones:
   - En la pantalla de bienvenida, haga clic en **Cambiar usuario**.
     Aparece la pantalla Cambiar usuario.
   - En la pantalla de bienvenida, haga clic en **Otras credenciales**.
     Aparece la pantalla Cambiar usuario.
3. Haga clic en **Autoservicio de cuentas**. Aparece la pantalla del autoservicio de cuentas.
4. Haga clic en **Haga clic aquí para restablecer su contraseña o desbloquear su cuenta**, que se encuentra debajo del título Autoservicio de cuentas para iniciar el asistente de autoservicio de cuentas.
5. En la página **Éste es el asistente del autoservicio de cuentas**, haga clic en **Desbloquear mi cuenta** y luego haga clic en **Siguiente**.
6. En la página **Identifique su cuenta**, asegúrese de que el nombre de usuario y el dominio que aparecen son los correctos y haga clic en **Siguiente**. Aparecerá la página **Desbloquear cuenta**.
7. En la página **Desbloquear cuenta**, haga clic en **Siguiente** para ver la primera pregunta de seguridad.
8. En la casilla **Respuesta**, escriba la respuesta a la primera pregunta de seguridad y haga clic en **Siguiente**. Si hay preguntas de seguridad adicionales, aparecerá la siguiente pregunta.
9. Repita el paso 8 hasta que aparezca la página **Desbloquear cuenta**.
10. En la página **Desbloquear cuenta**, haga clic en **Siguiente**.
11. En la página **La cuenta se desbloqueó**, haga clic en **Finalizar**.

Para restablecer la contraseña de una cuenta de Windows (Windows Vista/Windows 7/Windows Server 2008/Windows Server 2008 R2)

1. Cuando se le pida, presione CTRL+ALT+SUPR.
2. Lleve a cabo una de las siguientes acciones:
   - En la pantalla de bienvenida, haga clic en **Cambiar usuario**.
     Aparece la pantalla Cambiar usuario.
   - En la pantalla de bienvenida, haga clic en **Otras credenciales**.
     Aparece la pantalla Cambiar usuario.
3. Haga clic en **Autoservicio de cuentas**. Aparece la pantalla del autoservicio de cuentas.
4. Haga clic en **Haga clic aquí para restablecer su contraseña o desbloquear su cuenta**, que se encuentra debajo del título Autoservicio de cuentas para iniciar el asistente de autoservicio de cuentas.
5. En la página **Éste es el asistente del autoservicio de cuentas**, haga clic en **Restablecer mi contraseña** y luego haga clic en **Siguiente**.
6. En la página **Identifique su cuenta**, asegúrese de que el nombre de usuario y el dominio que aparecen son los correctos y haga clic en **Siguiente**. Aparecerá la página **Restablecer contraseña**.

7. En la página **Restablecer contraseña**, haga clic en **Siguiente** para ver la primera pregunta de seguridad.
8. En la casilla **Respuesta**, escriba la respuesta a la primera pregunta de seguridad y haga clic en **Siguiente**.
9. Repita el paso 8 hasta que aparezca la página **Escriba una nueva contraseña**.
10. En la página **Escriba una nueva contraseña**, escriba y confirme su nueva contraseña y haga clic en **Siguiente**.
11. En la página **La contraseña se cambió correctamente**, haga clic en **Finalizar** para volver a la pantalla del autoservicio de cuentas donde podrá seleccionar su cuenta e iniciar la sesión.

Para desbloquear una cuenta (diferente de Windows Vista/Windows 7/Windows Server 2008/Windows Server 2008 R2)

1. Lleve a cabo una de las siguientes acciones:
   - En el cuadro de diálogo **Bienvenido a Windows**, presione CTRL+ALT+SUPR y, si hace falta, haga clic en **Opciones**.
   - En el cuadro de diálogo **Equipo bloqueado**, presione CTRL+ALT+SUPR y haga clic en **Opciones**.
2. Haga clic en **Autoservicio de cuentas** para iniciar el asistente de autoservicio de cuentas.
3. En la página **Éste es el asistente del autoservicio de cuentas**, haga clic en **Desbloquear mi cuenta** y luego haga clic en **Siguiente**.
4. En la página **Identifique su cuenta**, asegúrese de que el nombre de usuario y el dominio que aparecen son los correctos y haga clic en **Siguiente**. Aparecerá la página **Desbloquear cuenta**.
5. En la página **Desbloquear cuenta**, haga clic en **Siguiente** para ver la primera pregunta de seguridad.
6. En la casilla **Respuesta**, escriba la respuesta a la primera pregunta de seguridad y haga clic en **Siguiente**. Si hay preguntas de seguridad adicionales, aparecerá la siguiente pregunta.
7. Repita el paso 6 hasta que aparezca la página **Desbloquear cuenta**.
8. En la página **Desbloquear cuenta**, haga clic en **Siguiente**.
9. En la página **La cuenta se desbloqueó**, haga clic en **Finalizar**.

Para restablecer la contraseña de una cuenta de Windows (diferente de Windows Vista/Windows 7/Windows Server 2008/Windows Server 2008 R2)

1. Lleve a cabo una de las siguientes acciones:
   - En el cuadro de diálogo **Bienvenido a Windows**, presione CTRL+ALT+SUPR y, si hace falta, haga clic en **Opciones**.
   - En el cuadro de diálogo **Equipo bloqueado**, presione CTRL+ALT+SUPR y haga clic en **Opciones**.

2. Haga clic en **Autoservicio de cuentas** para iniciar el asistente de autoservicio de cuentas.
3. En la página **Éste es el asistente del autoservicio de cuentas**, haga clic en **Restablecer mi contraseña** y luego haga clic en **Siguiente**.
4. En la página **Identifique su cuenta**, asegúrese de que el nombre de usuario y el dominio que aparecen son los correctos y haga clic en **Siguiente**. Aparecerá la página **Restablecer contraseña**.
5. En la página **Restablecer contraseña**, haga clic en **Siguiente** para ver la primera pregunta de seguridad.
6. En la casilla **Respuesta**, escriba la respuesta a la primera pregunta de seguridad y haga clic en **Siguiente**.
7. Repita el paso 6 hasta que aparezca la página **Escriba una nueva contraseña**.
8. En la página **Escriba una nueva contraseña**, escriba y confirme su nueva contraseña y haga clic en **Siguiente**.
9. En la página **La contraseña se cambió correctamente**, haga clic en **Finalizar**.

Preguntas y problemas comunes

January 7, 2019

La siguiente es una lista de preguntas y problemas que puede encontrarse al trabajar con Single Sign-on.

Recibí un mensaje de error indicando que mi contraseña va a caducar

Una de la mejores formas de mantener la información segura es cambiando la contraseña periódicamente. En función de los parámetros que haya establecido su empresa, Single Sign-on le enviará un mensaje cuando sus contraseñas no hayan cambiado por mucho tiempo.

Continuará recibiendo estos mensajes hasta que cambie la contraseña.

No quiero ejecutar Single Sign-on ahora

Algunas veces no va a querer ejecutar Single Sign-on. Por ejemplo, si necesita trabajar en una página de inicio de sesión no deseará que Single Sign-on inicie una sesión en el programa.

En estos casos, use la función Pausa de Single Sign-on. La función Pausa detiene el inicio de sesión automático, pero mantiene Single Sign-on abierto y disponible.

El programa rechaza mi nueva contraseña

Cambió la contraseña para un programa en particular a través del asistente de cambio de contraseña, pero cuando trata de iniciar una sesión en el programa, éste rechaza la nueva contraseña.

Es muy posible que la nueva contraseña fuera almacenada por Single Sign-on, pero no fuera aceptada por el programa. Como resultado, Single Sign-on está enviando una contraseña incorrecta.

Si la empresa la ha habilitado, use la función Recuperar contraseña anterior para solucionar este problema.

Nota: Si esta función no está disponible, póngase en contacto con el servicio de asistencia técnica de su empresa.

Para restaurar una contraseña anterior del programa

1. En el área de notificación de Microsoft Windows, normalmente en la parte derecha de la barra de tareas, haga clic con el botón secundario en el icono de Citrix Receiver y luego haga clic en **Contraseñas > Administrar contraseñas**.
2. En la ventana Administrar contraseñas, seleccione el programa o sitio Web que desee y haga clic en **Modificar**.

   Nota: En este punto, es posible que su empresa haya activado un proceso de verificación de identidad. Si es así, introduzca su nombre de usuario y contraseña de Windows cuando lo pida el sistema. (Si inicia la sesión con una tarjeta inteligente u otro método de autenticación, úselo para verificar su identidad cuando lo pida el sistema.)

   Aparece un cuadro de diálogo que contiene las propiedades para el programa seleccionado.
3. Haga clic en **Recuperar contraseña anterior** y luego haga clic en **Sí** para confirmar la acción.

No puedo acceder a mis datos de usuario

Cuando inicia una sesión en su equipo, Single Sign-on se conecta con el servidor donde la empresa almacena la información de Single Sign-on relativa a los usuarios. Si la conexión se establece con éxito y se confirma su identidad, Single Sign-on se inicia.

Si por alguna razón, la conexión o la identificación no tienen éxito, Single Sign-on no se iniciará y muy probablemente reciba un mensaje de error indicando que no se puede acceder a sus datos de usuario. Si esto ocurre póngase en contacto con el servicio de asistencia técnica de la empresa.

Mi explorador Web no funciona con Single Sign-on

Single Sign-on sólo proporciona respaldo para su utilización con Microsoft Internet Explorer. El uso de otros exploradores Web podrá dar resultados no esperados.

Después de cerrar una sesión, Single Sign-on vuelve a iniciarla

En algunas instancias, cuando se cierra la sesión de un programa o sitio Web protegido por contraseña, el programa puede volver a la pantalla de inicio de sesión. Si esto sucede, en función de cómo la empresa haya configurado Single Sign-on, puede que éste reaccione a la página de inicio reiniciando la sesión en el programa.

Si esto sucede, tiene las siguientes opciones:

- Si la empresa la ha habilitado, use la función Pausa de Single Sign-on antes de cerrar la sesión
- Si la función Pausa no está disponible, cierre la sesión en el programa y rápidamente cierre la ventana del mismo antes de que Single Sign-on pueda volver a iniciar una sesión

Nota: Explique la situación al servicio de asistencia técnica de la empresa y sugiera que el administrador de Single Sign-on active el parámetro de detección avanzada de definición de aplicaciones denominado **Procesar solamente el primer inicio de sesión de esta aplicación**.

¿Debo hacer algo especial antes de trabajar sin conexión a la red?

Si la empresa instaló Single Sign-on en el equipo local en lugar de ejecutarlo desde un servidor en la red de la empresa, actualice la licencia antes de trabajar sin conexión a la red. Esto asegura que tendrá el tiempo total permitido para la licencia hasta que pueda volver a conectarse a la red de la empresa.

Para actualizar la licencia de Single Sign-on

1. En el área de notificación de Microsoft Windows, normalmente en la parte derecha de la barra de tareas, haga clic con el botón secundario en el icono de Citrix Receiver y luego haga clic en **Contraseñas > Administrar contraseñas**.

   Nota: En este punto, es posible que su empresa haya activado un proceso de verificación de identidad. Si es así, introduzca su nombre de usuario y contraseña de Windows cuando lo pida el sistema. (Si inicia la sesión con una tarjeta inteligente u otro método de autenticación, úselo para verificar su identidad cuando lo pida el sistema.)

2. Haga clic en **Acerca**.

   Aparecerá la ventana **Acerca de Citrix Single Sign-On**.

3. Haga clic en **Actualizar la licencia**.
4. Haga clic en **Aceptar**.

   La ventana **Acerca de Citrix Single Sign-On** se cerrará.

¿Por qué Single Sign-on bloquea mi estación de trabajo?

Single Sign-on bloquea la estación de trabajo cada vez que se quiere realizar una tarea que requiere un nivel de seguridad extra. Estas tareas pueden incluir cambiar o revelar una contraseña.

Una vez bloqueada la estación de trabajo, usted debe verificar su identidad ante Single Sign-on suministrando la contraseña de la cuenta. En algunos casos, se le puede pedir que responda a unas preguntas de seguridad. Mediante dicha verificación, Single Sign-on evita que otras personas puedan acceder a información confidencial.

Aunque esto parezca una molestia, se hace para proteger al usuario, sus datos y a la empresa.

Cambiar la contraseña automáticamente

July 31, 2018

El asistente de cambio de contraseña de Single Sign-on automatiza el proceso de cambio de contraseñas en programas identificados. Según cómo haya configurado Single Sign-on su empresa, puede que le esté permitido crear su propia contraseña, o que tenga que dejar que Single Sign-on cree una automáticamente.

Nota: Puesto que las contraseñas generadas por el Asistente de cambio de contraseña consisten en un grupo al azar de letras, números y otros caracteres, el nivel de seguridad es muy alto. Como Single Sign-on administra las contraseñas y no es necesario que las recuerde, tenga presente esta función.

Dependiendo de cómo lo haya configurado la empresa, el asistente de cambio de contraseña se inicia de alguna de estas dos maneras:

- Cuando el programa indica que la contraseña debe cambiarse
- Cuando usted inicia el proceso de cambio de la contraseña del programa

En algunos casos, puede que Single Sign-on no detecte el proceso de cambio de contraseña y por tanto no dé inicio al asistente de cambio de contraseña. En estos casos, debe cambiar la contraseña manualmente tanto en el sitio Web o programa como en Single Sign-on, para asegurarse de que ambas contraseñas sean iguales.

Elegir cómo crear una nueva contraseña

Si la empresa ofrece esta opción, la página **Elija cómo crear la nueva contraseña** del Asistente de cambio de contraseña le permite seleccionar la forma en que se creará su nueva contraseña. Las opciones son:

- **Elegir una contraseña generada por el sistema**

  Si selecciona esta opción y hace clic en **Siguiente**, el Asistente de cambio de contraseña creará una contraseña de alta seguridad. Esta contraseña no se revela durante este proceso, porque se guarda directamente en Single Sign-on y usted no necesita conocerla. Sin embargo, si la empresa configura Single Sign-on para que se pueda ver la contraseña, puede hacerlo al cerrar el asistente, si lo desea.

  Nota: Puesto que las contraseñas generadas por el Asistente de cambio de contraseña consisten en un grupo al azar de letras, números y otros caracteres, el nivel de seguridad es muy alto. Como Single Sign-on administra las contraseñas y no es necesario que las recuerde, tenga presente esta función.

- **Crear la contraseña**

  Si selecciona esta opción y hace clic en **Siguiente**, el Asistente de cambio de contraseña le permite crear y enviar su propia contraseña. Dicha contraseña debe seguir las directivas establecidas por la empresa en cuanto a la longitud, complejidad y otros factores que pueden afectar a la seguridad.

Esperar la confirmación

La página **Esperando la confirmación** del asistente de cambio de contraseña aparece cuando el asistente determina si se cambió la contraseña o si el cambió falló.

Si usted decide que el cambio de contraseña ha tenido éxito antes de que el asistente de cambio de contraseña cierre la página **Esperando la confirmación**, haga clic en **Omitir** para ir a la página **Confirmar el cambio de contraseña**.

Confirmar el cambio de contraseña

La página **Confirmar el cambio de contraseña** del Asistente de cambio de contraseña puede aparecer si la empresa la activó. Si aparece, le va a preguntar que determine si la contraseña se cambió o no. Hay tres opciones disponibles:

Sí:

La ausencia de la página para volver a configurar la contraseña o un mensaje notificando que se cambió indican que el cambio de la contraseña tuvo éxito.

Seleccione **Lo hizo** y haga clic en **Siguiente** para indicarle al Asistente de cambio de contraseña que el cambio se completó con éxito. El asistente termina el proceso.

No:

La presencia de la página para volver a configurar la contraseña o un mensaje notificando que el cambio falló indican que el cambio de la contraseña no se realizó.

Seleccione **No lo hizo** y haga clic en **Siguiente** para indicarle al Asistente de cambio de contraseña que el programa no ha aceptado la nueva contraseña. El asistente se cierra sin cambiar la contraseña.

No lo sé:

Si selecciona **No lo sé** y hace clic en **Siguiente**, pasará a una página que describe cómo determinar si la contraseña se cambió.

Hay otra forma de determinar si el asistente tuvo éxito, si creó su propia contraseña: ponga Single Sign-on en pausa e inicie una sesión en el programa con la nueva contraseña.

Nota: Puede ser que necesite mover la ventana del Asistente de cambio de contraseña para ver si la ventana de volver a configurar la contraseña del programa aún se encuentra abierta o si el programa le proporcionó alguna respuesta relacionada con la contraseña.

Confirmar que la contraseña no cambió

Si el Asistente de cambio de contraseña detecta que la contraseña no cambió o si elige **No lo hizo** en la página **Confirmar el cambio de contraseña** aparecerá la página **La contraseña no se cambió**.

La página **La contraseña no se cambió** ofrece dos opciones:

- Intentar con otra contraseña.

  Use esta opción solamente si el formulario de cambio de contraseña se encuentra aún abierto. Si se usa después de cerrarse el formulario, las contraseñas en su programa y en Single Sign-on podrían no coincidir.

  Seleccionando **Intentar con otra contraseña** y haciendo clic en **Siguiente** se puede intentar enviar otra contraseña al programa. Dependiendo de cómo esté configurado el asistente de cambio de contraseña, puede darse alguna de las siguientes situaciones:

  - Aparece la página **Elija cómo crear la nueva contraseña**. Puede seleccionar entre contraseñas generadas por el sistema o crear una propia.
  - Aparece la página **Crear la contraseña**.
  - Se crea y envía una contraseña generada por el sistema. El asistente de cambio de contraseña busca luego confirmación del cambio de contraseña.

- Salir del asistente sin hacer nada más.

Seleccionando **Salir del asistente sin hacer nada más** se pone fin a los intentos de cambiar la contraseña del programa. Puede, sin embargo, reiniciar el asistente de cambio de contraseña e intentarlo de nuevo en otro momento.

Salir del asistente sin hacer nada más

La página **La contraseña no se cambió** aparece si el Asistente de cambio de contraseña detecta que la contraseña no cambió, o si se elige **No lo hizo** en la página **Confirmar el cambio de contraseña**.

Si el Asistente de cambio de contraseña falló, haga lo siguiente para cambiar la contraseña:

- Haga clic en **Finalizar** en la página **La contraseña no se cambió** para cerrar el asistente y luego reinicie el asistente para intentarlo de nuevo.
- Cambie la contraseña manualmente en el programa y en Single Sign-on
- Póngase en contacto con el servicio de asistencia técnica de la empresa

Salir del asistente después de cambiar la contraseña

La página **La contraseña se cambió correctamente** aparece cuando el Asistente de cambio de contraseña detecta que la contraseña cambió, o si se elige **Lo hizo** en la página **Confirmar el cambio de contraseña**.

En este momento, el programa acepta la nueva contraseña y Single Sign-on la guarda.

Determinar si el programa aceptó la nueva contraseña

Si selecciona **No sé si lo hizo** y hace clic en **Siguiente** en la página **Confirmar el cambio de la contraseña** verá una página que describe cómo determinar si la contraseña cambió o no.

Otra forma de determinar si el asistente tuvo éxito es poner Single Sign-on en pausa y luego iniciar una sesión en el programa con la nueva contraseña.

Haciendo clic en **Siguiente** en esta página se hace que vuelva a aparecer la página **Confirmar el cambio de contraseña**.

Crear la contraseña

La página para **Crear la contraseña** del Asistente de cambio de contraseña aparece si seleccionó **Crear la contraseña** en la página **Elija cómo crear la nueva contraseña**. Esta página no aparece si la empresa no le proporciona la opción de crear sus propias contraseñas.

Para evitar el envío de una contraseña mal escrita, debe escribirla en las casillas **Nueva contraseña** y **Confirmar la contraseña**. El asistente de cambio de contraseña le indicará si las contraseñas no son iguales. Si las contraseñas son iguales, el botón **Siguiente** se verá disponible.

El asistente de cambio de contraseña requiere que siga todas las directivas establecidas por la empresa para las contraseñas. Los siguientes son algunos ejemplos de directivas establecidas por la empresa:

- Las contraseñas anteriores no se pueden volver a usar
- Las contraseñas deben contener una mezcla de números y letras
- Las contraseñas no pueden incluir ciertos caracteres
- Las contraseñas deben ser de cierta longitud

Almacenar nombres de usuarios y contraseñas

January 7, 2019

Si la empresa habilitó esta función, Single Sign-on detecta automáticamente cuando se abre un programa o un sitio Web que está protegido por contraseña. Si ya guardó su nombre de usuario, contraseña y otros datos de inicio de sesión para ese programa o sitio Web en Single Sign-on, Single Sign-on iniciará la sesión automáticamente por usted.

Según las funciones que haya habilitado su empresa, existen varias maneras de guardar la información de inicio de sesión en Single Sign-on cuando se abre un sitio Web o un programa protegidos por contraseña cuya información de inicio de sesión todavía no se ha almacenado en Single Sign-On:

- Si Single Sign-on detecta que se ha abierto un sitio Web o programa protegido por contraseña, aparecerá automáticamente un cuadro de diálogo preguntando si desea guardar la información de inicio de sesión
- Si Single Sign-on no detecta el programa, puede agregar la información de inicio de sesión manualmente

Single Sign-on almacena información de inicio de sesión de:

- **Programas basados en Windows**. Estos son programas que generalmente se abren desde el menú Inicio o desde el escritorio. Por ejemplo, Lotus Notes.
- **Sitios o programas basados en Web**. Estos son programas o sitios con los que se interactúa por medio de un explorador Web. Por ejemplo, tiendas de Internet y programas de aprendizaje basados en Web.

  ** Importante:** Microsoft Internet Explorer (de 32 bits) es el único explorador Web respaldado por Single Sign-on.

- **Aplicaciones de emulador de terminal.** Estos son programas de texto normalmente asociados con un emulador de terminal. Las ventanas de estos programas a menudo tienen un fondo de color oscuro, tal como verde y texto en un tono más claro del mismo color.

Nota: La información de inicio de sesión requerida puede variar de un programa a otro. En la mayoría de los casos, se debe proporcionar el nombre del usuario o ID y la contraseña. Si se le solicita información que no conoce, póngase en contacto con el servicio de asistencia técnica de la empresa.

Para almacenar la información de inicio de sesión automáticamente

1. Abra un sitio Web o inicie un programa que estén protegidos con contraseña. Aparecerá la página de inicio de sesión del sitio Web o el cuadro de diálogo de inicio de sesión del programa.
2. En el cuadro de diálogo que aparece preguntando si desea que Single Sign-on recuerde su contraseña para el sitio Web, haga clic en **Recordar**.
3. Si está almacenando información de inicio de sesión para un sitio Web o para un programa basado en Web, pueden aparecer unos rectángulos en la ventana de inicio de sesión del sitio Web, rodeando los cuadros y botones utilizados para enviar dicha información. En el cuadro de diálogo que aparece preguntando si se han seleccionado los cuadros y botones correctos, haga clic en **Sí**.
4. En el cuadro de diálogo **Nuevo inicio de sesión**, escriba la información de inicio de sesión y haga clic en **Finalizar**. El cuadro de diálogo **Nuevo inicio de sesión** se cerrará, la información de inicio de sesión se almacenará en Single Sign-on y se iniciará la sesión en el programa seleccionado.

Para almacenar la información de inicio de sesión manualmente

1. Abra un sitio Web o inicie un programa que estén protegidos con contraseña. Aparecerá la página de inicio de sesión del sitio Web o el cuadro de diálogo de inicio de sesión del programa.
2. Si no ve un cuadro de diálogo en que se le pregunta si quiere que Single Sign-On recuerde la contraseña para el programa o sitio Web, solicite a Single Sign-On que le deje almacenar la información de inicio de sesión manualmente: En el área de notificación de Microsoft Windows, situada normalmente a la derecha en la barra de herramientas, haga clic con el botón secundario en el icono de Citrix Receiver y seleccione **Contraseñas > Enviar contraseña**.

   Nota: En este punto, es posible que su empresa haya activado un proceso de verificación de identidad. Si es así, introduzca su nombre de usuario y contraseña de Windows cuando lo pida el sistema. (Si inicia la sesión con una tarjeta inteligente u otro método de autenticación, úselo para verificar su identidad cuando lo pida el sistema.)
3. En el cuadro de diálogo que aparece preguntando si desea que Single Sign-on recuerde su contraseña para el sitio Web, haga clic en **Recordar**.

4. Si está almacenando información de inicio de sesión para un sitio Web o para un programa basado en Web, pueden aparecer unos rectángulos en la ventana de inicio de sesión del sitio Web, rodeando los cuadros y botones utilizados para enviar dicha información. En el cuadro de diálogo que aparece preguntando si se han seleccionado los cuadros y botones correctos, haga clic en **Sí**.
5. En el cuadro de diálogo **Nuevo inicio de sesión**, escriba la información de inicio de sesión y haga clic en **Finalizar**. El cuadro de diálogo **Nuevo inicio de sesión** se cerrará, la información de inicio de sesión se almacenará en Single Sign-on y se iniciará la sesión en el programa seleccionado.

Almacenar varios nombres de usuario y contraseñas para un mismo programa

Hay casos en que se dispone de más de una cuenta para un solo programa o sitio Web. Por ejemplo:

- Cuando se tiene acceso a una cuenta de correo electrónico general para el departamento denominada “Solicitudes de acceso” y a otra cuenta propia personal
- Cuando se es responsable de la adquisición de materiales para dos proyectos y se tienen cuentas separadas para cada proyecto en el sitio Web del proveedor

Si la empresa habilitó la función de varias cuentas de Single Sign-on, se pueden guardar dos o más grupos de información de cuentas para un mismo programa o sitio Web. Después de guardar la información de las distintas cuentas, Single Sign-on usa el Selector de inicio de sesión para permitirle elegir el grupo de información de inicio de sesión que desea usar para iniciar una sesión.

Para agregar contraseñas adicionales de programas y sitios Web que ya existen en Single Sign-on

1. En el área de notificación de Microsoft Windows, normalmente en la parte derecha de la barra de tareas, haga clic con el botón secundario en el icono de Citrix Receiver y luego haga clic en **Contraseñas > Administrar contraseñas**.
2. En la ventana Administrar contraseñas, seleccione el programa o sitio Web al que desea agregar una cuenta de inicio de sesión adicional.
3. Haga clic en **Copiar**.

   Nota: En este punto, es posible que su empresa haya activado un proceso de verificación de identidad. Si es así, introduzca su nombre de usuario y contraseña de Windows cuando lo pida el sistema. (Si inicia la sesión con una tarjeta inteligente u otro método de autenticación, úselo para verificar su identidad cuando lo pida el sistema.)

   En la lista aparecerá una nueva entrada correspondiente al programa o página Web.

4. Seleccione la nueva entada y haga clic en **Modificar**. Aparece un cuadro de diálogo que contiene la información de inicio de sesión para el programa o el sitio Web.
5. Cambie la información de inicio de sesión si es necesario.
6. En el cuadro **Nombre de la aplicación**, modifique el nombre del programa o del sitio Web para que lo pueda diferenciar de la otra instancia.
7. Haga clic en **Aceptar**.

Iniciar sesión cuando se tienen varias cuentas

Si tiene varias cuentas para un programa o sitio Web, Single Sign-on abrirá el Selector de inicio de sesión para permitirle elegir con qué cuenta desea iniciar la sesión.

Para iniciar una sesión en programas o sitios Web para los que se tengan varias cuentas almacenadas en Single Sign-on:

1. Inicie el programa o sitio Web. Aparece el **Selector de inicio de sesión** junto con la página de inicio de sesión del programa.
2. En el **Selector de inicio de sesión**, haga clic en la cuenta de inicio de sesión adecuada y luego haga clic en **Aceptar**. El **Selector de inicio de sesión** se cierra y Single Sign-on inicia la sesión en el programa o sitio Web.

Registrar las respuestas a las preguntas de seguridad

July 31, 2018

1. En la página **Sistema de registro de preguntas de seguridad**, haga clic en **Siguiente** para ver la primera pregunta.
2. En la casilla **Respuesta**, escriba la respuesta a la primera pregunta. Dependiendo de la configuración de su empresa, la respuesta puede aparecer como puntos mientras la escribe. Si eso sucede, deberá volver a escribir la respuesta en la casilla **Confirmar la respuesta**.

   Nota: En las respuestas a las preguntas de seguridad, se distingue entre mayúsculas y minúsculas. Si usa una mayúscula para registrar sus respuestas, deberá usar la misma mayúscula para verificar su identidad. Del mismo modo, si usa un punto en las respuestas durante el proceso de registro (por ejemplo, si pone a “P. Marco” como su profesor preferido), tiene que usar también el punto cuando verifique su identidad.
3. Haga clic en **Siguiente**. Si hay preguntas de seguridad adicionales, aparecerá la siguiente pregunta.

4. Repita los pasos 2 y 3 hasta que aparezca la página **Envíe sus respuestas**.
5. En la página **Envíe sus respuestas**, haga clic en **Siguiente**.
6. En la página que indica que **Las preguntas de seguridad se registraron correctamente**, haga clic en **Finalizar**. Las respuestas a las preguntas de seguridad han quedado almacenadas.

Quitar nombres de usuarios y contraseñas

January 7, 2019

En este tema se describe cómo quitar las contraseñas que Single Sign-on guardó. Receiver también puede guardar las contraseñas si se seleccionó **Recordar mi contraseña** al iniciar sesión. Para eliminar la contraseña desde Receiver, haga clic con el botón secundario en el icono de Receiver, haga clic en **Acerca de**, expanda **Avanzado** y haga clic en **Eliminar contraseñas**.

Puede haber ocasiones en que desee quitar la información de cuentas de inicio de sesión de Single Sign-on. Por ejemplo:

- Tiene almacenadas varias cuentas para un programa o sitio Web pero ya no necesita tenerlas todas
- Tiene información guardada para programas o sitios Web que ya no usa

Importante: Si elimina la información de inicio de sesión que aún está usando, Single Sign-on no podrá iniciar la sesión automáticamente en el programa o sitio Web y volverá a pedir el almacenamiento de dicha información la próxima vez que inicie ese programa.

1. En el área de notificación de Microsoft Windows, normalmente en la parte derecha de la barra de tareas, haga clic con el botón secundario en el icono de Citrix Receiver y luego haga clic en **Contraseñas > Administrar contraseñas**.
2. En la ventana Administrar contraseñas, seleccione el programa o sitio Web que desee y haga clic en **Quitar**.

   Nota: En este punto, es posible que su empresa haya activado un proceso de verificación de identidad. Si es así, introduzca su nombre de usuario y contraseña de Windows cuando lo pida el sistema. (Si inicia la sesión con una tarjeta inteligente u otro método de autenticación, úselo para verificar su identidad cuando lo pida el sistema.)

   Aparecerá un cuadro de diálogo que le pedirá que confirme que desea eliminar la información de inicio de sesión para el programa seleccionado.
3. Haga clic en **Sí**. La información de inicio de sesión para ese programa o sitio Web se eliminará de Single Sign-on y ya no estará en la lista de la ventana Administrar Contraseñas.

Nota: Si vuelve al programa o al sitio web, se le preguntará si quiere guardar la información de inicio de sesión.

Revelar su contraseña

July 31, 2018

Si su empresa ha configurado esta función como disponible, Single Sign-on le permite ver sus contraseñas.

Nota: Es posible que su empresa haya definido que ciertas contraseñas no puedan revelarse.

Precaución: No deje que otras personas lleguen a conocer sus contraseñas. Si lo hace, pondrá en riesgo sus cuentas y los sistemas de su empresa.

1. En el área de notificación de Microsoft Windows, normalmente en la parte derecha de la barra de tareas, haga clic con el botón secundario en el icono de Citrix Receiver y luego haga clic en **Contraseñas > Administrar contraseñas**.
2. En la ventana Administrar contraseñas, seleccione el programa o sitio Web que desee y haga clic en **Mostrar contraseña**.

   Nota: En este punto, es posible que su empresa haya activado un proceso de verificación de identidad. Si es así, introduzca su nombre de usuario y contraseña de Windows cuando lo pida el sistema. (Si inicia la sesión con una tarjeta inteligente u otro método de autenticación, úselo para verificar su identidad cuando lo pida el sistema.)

   Aparece un nuevo cuadro de diálogo que contiene la contraseña para el programa seleccionado.
3. Haga clic en **Aceptar** para cerrar el cuadro de diálogo de contraseñas.

Configurar Citrix Single Sign-on para el primer uso

July 31, 2018

Depende de cómo la empresa lo configure, Citrix Single Sign-on se inicia automáticamente cuando se inicia una sesión en el equipo o cuando se inicia por primera vez un programa o sitio Web protegido por contraseña.

Si la empresa configuró Single Sign-on para obtener datos la primera vez que se ejecuta, es posible que el usuario tenga que responder a preguntas de seguridad, tales como “¿Quién era su profesor favorito?”. Las respuestas a estas preguntas le ayudarán a verificar su identidad cuando sea necesario.

Usar aplicaciones sin estar conectado a Internet

July 31, 2018

Para abrir una aplicación por primera vez, es necesario estar conectado a Internet. Citrix Receiver para Windows instala algunas aplicaciones en el dispositivo que se pueden ejecutar sin estar conectado a Internet. Esta instalación puede tardar varios minutos.

Nota: El acceso sin conexión no se encuentra disponible para todos los usuarios o aplicaciones. El administrador determina la cantidad de tiempo que se puede usar una aplicación sin conexión antes de que se requiera una conexión a Internet.

Buscar escritorios y aplicaciones

July 31, 2018

Tanto las aplicaciones como los escritorios virtuales están disponibles en la página de inicio de Citrix Receiver para Windows en todos los dispositivos.

Para comenzar, haga clic con el botón secundario en el icono de Citrix Receiver para Windows y, a continuación, haga clic en **Abrir**.

Los escritorios y las aplicaciones también se pueden encontrar en una o varias de estas ubicaciones:

- Menú Inicio de Windows: Las aplicaciones y los escritorios agregados desde Citrix Receiver para Windows también se agregan al menú Inicio de Windows en la carpeta Todos los programas.
- Escritorio: es posible que el administrador proporcione accesos directos en el escritorio del equipo. El acceso directo puede estar ubicado dentro de una carpeta en el escritorio.
- Página web: es posible que el administrador proporcione enlaces a aplicaciones y escritorios en una página web. Abra un explorador Web, Internet Explorer, Firefox o Google Chrome, e introduzca la dirección URL que le proporcionó el administrador.

Administrar sesiones

July 31, 2018

La opción Central de conexiones de Citrix muestra todas las conexiones activas establecidas desde Receiver.

Para abrir la opción Central de conexiones:

- Haga clic con el botón secundario en el icono de Receiver y después haga clic en **Central de conexiones**.

Para cerrar una aplicación virtual que no responde

Seleccione la aplicación en Central de conexiones y haga clic en **Finalizar**.

Para cerrar todas las aplicaciones virtuales activas de una sola vez

Seleccione el servidor en Central de conexiones y haga clic en **Cerrar sesión**.

Para cambiar cómo se ven las aplicaciones y los escritorios

Se puede cambiar entre los modos integrado y pantalla completa.

- **Modo de ventanas integradas**. Los escritorios y las aplicaciones no se colocan dentro de una ventana de sesión. Cada escritorio y aplicación aparece en su propia ventana de tamaño variable, como si estuvieran físicamente instalados en el dispositivo del usuario. Los usuarios pueden alternar entre las aplicaciones y el escritorio local.
- **Modo de pantalla completa**. Las aplicaciones se colocan en una ventana de escritorio.

Para pasar al modo de pantalla completa: seleccione el servidor en Central de conexiones, haga clic en **Pantalla completa** y seleccione **Aceptar**.

Para volver al modo de ventanas integradas: presione Mayús + F2.

Actualizar o eliminar aplicaciones

July 31, 2018

Cuando el usuario cierra sesión o sale de Citrix Receiver para Windows, las aplicaciones se desconectan. Vuelva a conectarse a la sesión, ya sea mediante la opción **Actualizar aplicaciones** del menú desplegable o haciendo clic en el icono de la aplicación.

Cuando el modo de autoservicio está inhabilitado, para actualizar las aplicaciones cuando se accede a ellas exclusivamente desde los accesos directos del menú Inicio o del escritorio, haga clic con el botón secundario en Citrix Receiver para Windows en el área de notificaciones y, a continuación, haga clic en **Actualizar**.

Seleccione **Actualizar aplicaciones** para obtener las aplicaciones y los escritorios publicados más recientes de StoreFront.

Para eliminar una aplicación de la vista Aplicaciones, haga clic con el botón secundario en la aplicación y seleccione **Quitar aplicación**.

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:


```
CitrixReceiver.exe
      /includeSSON
STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/
   discovery;on;Desktop Store"
```

Para obtener más información acerca de 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 %ProgramFiles%\Citrix\ICA Client\Configuration.
- Preferencias de USB. Cuando un usuario conecta un dispositivo USB, ese dispositivo se comunica automáticamente de forma remota con el escritorio virtual, 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

July 31, 2018

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 (VDAPI) se usa con las funciones de canal virtual en el SDK de WFAPI (Citrix Server API SDK) para crear nuevos canales virtuales. El respaldo para canales virtuales proporcionado por VDAPI 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 WFAPI 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