

Acerca de Citrix Receiver para Chrome 2.3

Feb 08, 2017

Citrix Receiver para Chrome es una aplicación empaquetada nativa de Chrome que permite a los usuarios acceder a escritorios virtuales y aplicaciones alojadas desde dispositivos Chrome. Los recursos entregados por XenApp y XenDesktop se combinan en una tienda o almacén de StoreFront que se pone a disposición de los usuarios mediante un sitio de Citrix Receiver para Web.

Con la aplicación Citrix Receiver para Chrome instalada, los usuarios pueden acceder a escritorios y aplicaciones desde sus exploradores Web y no se necesita ninguna configuración ni implementación adicional en StoreFront.

Novedades en la versión 2.3

Respaldo para varios monitores

Con esta versión, Citrix Receiver para Chrome da respaldo al uso de varios monitores para la presentación de aplicaciones y escritorios remotos en una sesión de cliente. Se pueden usar hasta dos monitores en el modo de escritorio unificado. Cada monitor en una configuración de varios monitores tiene su propia resolución, configurada por el fabricante. Cuando se usan monitores con dos resoluciones distintas, Chrome OS estira la resolución del monitor secundario para ajustarse a la altura de la pantalla de Chromebook.

Para obtener más información, consulte [Configuración de la presentación con varios monitores](#).

Respaldo para el uso selectivo de H.264 en Thinwire

Citrix Receiver para Chrome ahora da respaldo a las capacidades de Selective H.264 en Thinwire, lo que mejora la experiencia del usuario al usar contenido transitorio. Por ejemplo, vídeo.

Esta funcionalidad está solo disponible en VDA 7.11 o versiones posteriores.

Para obtener más información sobre Selective H.264, consulte [Configuración de Selective H.264](#).

Mejoras en el comportamiento del almacenamiento en caché del contenido de vídeo en Thinwire

Ahora, Thinwire puede omitir el almacenamiento en caché del contenido de vídeo generado por el servidor al mismo tiempo que conserva en caché mapas de bits de otras ventanas abiertas con datos de texto (por ejemplo, Excel, el Explorador de Windows, fondo de escritorio), lo que reduce en un 5% el consumo del ancho de banda. Esta mejora está disponible en XenApp y XenDesktop 7.11 o versiones posteriores.

Para obtener más información sobre cómo configurar Thinwire, consulte la documentación de [XenApp y XenDesktop](#).

HDX SDK para Chrome (API experimental)

Con esta versión, Citrix Receiver para Chrome ofrece una API que permite que una aplicación Chrome de terceros lance las sesiones de XenApp y XenDesktop.

Nota: Esta funcionalidad se ha verificado solo con el lanzamiento de una sola aplicación o escritorio.

Para obtener más información, consulte [HDX SDK para Chrome](#).

Novedades en la versión 2.2

Configuración de la fiabilidad de la sesión

Citrix Receiver para Chrome permite ahora que los administradores configuren las siguientes directivas usando Citrix Studio:

1. Tiempo de espera de fiabilidad de la sesión
2. Nivel de transparencia de la interfaz de usuario durante la reconexión

Para obtener más información, consulte [Configuración de la fiabilidad de la sesión](#).

Mejoras de zona horaria

Con esta versión, Citrix Receiver para Chrome cuenta con respaldo extendido para inglés e idiomas nativos en la redirección de zona horaria del cliente.

Novedades en la versión 2.1

Configuración mejorada

Citrix Receiver para Chrome ofrece funcionalidad adicional que le permite tener un mayor control de la configuración y nuevas formas de configurar Receiver. Con esta versión, se puede configurar Receiver usando lo siguiente:

- Directiva de administración de Google
- Web.config en StoreFront
- default.ica
- configuration.js

Con estos métodos, se pueden configurar los parámetros de sesión siguientes:

- Ocultar o mostrar la barra de herramientas
- Habilitar o inhabilitar NACL
- Sonido
- Gráficos
- Transferencia de archivos

Para obtener más información, consulte [Configuración de Citrix Receiver](#).

Sugerencia

El archivo configuration.js se encuentra en la carpeta raíz de ChromeApp. Se necesitan credenciales de nivel de administrador para editar este archivo. Después de editarlo, vuelva a empaquetar la aplicación para hacer modificaciones adicionales en los elementos de la barra de herramientas.

Nota

Citrix recomienda hacer una copia de seguridad del archivo configuration.js antes de hacer cambios en él.

Autenticación con tarjeta inteligente.

Citrix Receiver para Chrome permite ahora a los usuarios autenticarse con tarjeta inteligente. Usando esta función, los administradores pueden iniciar sesiones en Citrix Receiver mediante una tarjeta inteligente y pueden también firmar mensajes de correo electrónico o acceder a sitios Web en una sesión ICA usando las credenciales de su tarjeta inteligente.

Para obtener más información, consulte [Configuración de Citrix Receiver](#).

Redirección de puertos serie

Citrix Receiver para Chrome permite a los usuarios redirigir dispositivos de puerto serie/COM a aplicaciones y escritorios virtuales de XenApp y XenDesktop. Con esta funcionalidad, los usuarios pueden ver y acceder a dispositivos basados en puertos serie/COM en una sesión de Receiver activa.

Para obtener más información, consulte [Configuración de Citrix Receiver](#).

Nota

De manera predeterminada, Citrix Receiver para Chrome asigna COM5 como puerto COM serie preferido para la redirección.

Single Sign-on (SSON)

Citrix Receiver para Chrome ahora respalda la funcionalidad de inicio de sesión Single Sign-on (SSON) en dispositivos Chromebook así como en el back-end de Citrix XenApp/XenDesktop usando autenticación federada.

Con esta funcionalidad, los usuarios no necesitan volver a introducir sus contraseñas en un entorno Citrix. SSON funciona configurando el Single Sign-on de SAML en dispositivos Chrome y sesiones de Receiver usando cookies de SAML para iniciar sesión en NetScaler Gateway.

Para obtener más información, consulte [Configuración de Citrix Receiver](#).

Más dispositivos USB

Esta versión respalda una gama más amplia de periféricos USB. Con esta funcionalidad adicional, un administrador puede crear una directiva de Google para identificar el PID/VID del dispositivo para habilitar su uso en Citrix Receiver. Este respaldo se extiende a nuevos dispositivos USB, incluido el mouse 3D Space, dispositivos compuestos adicionales y el teclado Bloomberg.

Botón para recargar la URL de la tienda

Se ha agregado un botón nuevo para cargar la tienda. Al hacer clic en el botón, las cookies de la tienda se borran y la página de la tienda vuelve a cargarse.

ID exclusivo

Citrix Receiver para Chrome genera un nombre exclusivo usando el ID de API de Directory de los dispositivos inscritos a través de Google Chrome Management. El nombre generado tiene el formato CRxxxxxxxxxxxxxxxx.

Novedades en la versión 2.0

Barra de herramientas rediseñada

Citrix Receiver para Chrome ofrece una barra de herramientas rediseñada para mejorar la experiencia del usuario en esta versión. Esta mejora ofrece nuevas opciones accesibles desde la barra de herramientas para facilitar tareas comunes.

Para obtener más información, consulte [Barra de herramientas rediseñada](#).

Central de conexiones

Citrix Receiver para Chrome 2.0 presenta la Central de conexiones. Esta funcionalidad facilita la administración de aplicaciones cuando se usan sesiones integradas, presentando una barra de tareas que enumera todas las aplicaciones que están abiertas.

Para obtener más información, consulte [Central de conexiones](#).

Ventanas integradas

Citrix Receiver para Chrome mejora la experiencia del usuario permitiendo la integración de varias aplicaciones alojadas en ventanas distintas dentro de una sesión activa. Con esta funcionalidad, Citrix Receiver permite abrir aplicaciones en una interfaz de usuario independiente comparado con abrir todas las aplicaciones de una sesión en una misma ventana.

Novedades en la versión 1.9

Respaldo de portapapeles mejorado

Citrix Receiver para HTML5 ahora da respaldo al formato HTML además de texto simple entre un cliente y una sesión. Esto es útil para aplicaciones Office y exploradores Web. El respaldo mejorado para el portapapeles solo está disponible en exploradores Chrome y Safari.

Para obtener más información, consulte [Respaldo de portapapeles mejorado](#).

Respaldo para la codificación de hardware de cámaras Web

Citrix Receiver para Chrome ofrece una mejora para la redirección de cámaras Web en esta versión. La codificación por hardware H.264 para cámaras Web ayuda a reducir la carga de CPU e incrementa la eficiencia de la batería de los dispositivos Chromebook. Estos dispositivos tienen codificadores para H.264, que aprovechan la funcionalidad de Intel en la API de PPB_VideoEncoder.

Problemas resueltos

Problemas resueltos en Citrix Receiver para Chrome 2.3

Comparado con: Citrix Receiver para Chrome 2.2

Citrix Receiver para Chrome 2.3 contiene todas las correcciones incluidas en las versiones 2.2, 2.1, 1.9, 1.8, 1.7, 1.6, 1.5 y 1.4, además de la siguiente corrección nueva:

- Al abrir una aplicación publicada desde un VDA que se ejecuta en Linux, se puede congelar la sesión.

[#662083]

Problemas resueltos en Citrix Receiver para Chrome 2.1

Comparado con: Citrix Receiver para Chrome 2.0

Citrix Receiver para Chrome 2.2 contiene todas las correcciones incluidas en las versiones 2.1, 1.9, 1.8, 1.7, 1.6, 1.5 y 1.4, además de las siguientes correcciones nuevas:

- La sesión no se podía lanzar desde RDP o escenarios de doble salto de Citrix ICA.

[#653980]

- No se podía conectar con versiones antiguas de StoreFront o NetScaler Gateway; la sesión se abría en un explorador Web en lugar de abrirse en Citrix Receiver.

[#653981]

- Las teclas CTRL y MAYÚS no funcionaban al seleccionar archivos o texto.

[#654185]

Problemas conocidos

Problemas conocidos en Citrix Receiver para Chrome 2.3

- Cuando el modo de gráficos antiguo está habilitado en XenDesktop 7.12 en un VDA que se ejecuta en Windows Server 2016, la sesión ICA ignora la profundidad de color preferida y la sesión se termina.

[RFHTMCRM-965]

- En una configuración multimonitor, la sesión puede dejar de responder si se arrastra la barra de herramientas de la sesión al segundo monitor.

[RFHTMCRM-1113]

- Cuando el modo de gráficos antiguo está habilitado en XenDesktop 7.12 en un VDA que se ejecuta en Windows Server 2016 y se cambia de tamaño la ventana de la sesión, puede aparecer una notificación para indicar que se está ajustando la resolución de pantalla:

("Adjusting Screen Resolution - Please Wait")

[RFHTMCRM-1118]

- Cuando se reproduce audio en una sesión, al cambiar desde la ventana de la sesión activa a otra, el audio puede sonar distorsionado.

[RFHTMCRM-1122]

- En una sesión de escritorio, la calidad y el rendimiento de un vídeo se degrada cuando se cambia de posición varias veces

la aplicación de reproducción de vídeo.

[RFHTMCRM-1167]

Problemas conocidos en Citrix Receiver para Chrome 2.1

- ENH ID 0652697: En algunos casos, el conector de tarjeta inteligente de Google podía dejar de responder. Para solucionar este problema, desconecte y luego reconecte la sesión para habilitar la redirección de la tarjeta inteligente.

Problemas conocidos en Citrix Receiver para Chrome 2.1:

- Una sesión puede dejar de responder al copiar y pegar una gran cantidad de datos dentro de la sesión. Citrix recomienda copiar menos de 10 MB cuando se use el portapapeles.

[#586671]

- Citrix Receiver para Chrome no respalda teclados de varios idiomas.

[#602652]

- Cuando se copia contenido desde un documento en Google Drive (Gdrive) a una sesión, es posible que no se conserve el formato del contenido copiado. Para resolver este problema, abra el documento que contiene el contenido copiado usando su aplicación respectiva (por ejemplo, Google Docs, Microsoft Word o Excel) y realice operaciones de portapapeles. Esto conservará el formato en el lado de la sesión.

[#606135]

- La combinación de teclado ALT+F4 no funciona como se espera dentro de una sesión. Haga clic en la tecla de Búsqueda/Windows junto con las teclas de la fila superior para simular las teclas de función en un Chromebook. También puede usar la opción Ajustes del teclado en el Chromebook para tratar las teclas de la fila superior como teclas de función y habilitar el uso directo de estas teclas para simular teclas de función.

[#607326]

- Citrix recomienda usar una ruta absoluta en lugar de una ruta relativa en los parámetros de Registro de Transferencia de archivos.

[#607455]

- La clave F5 no muestra la huella digital de las aplicaciones: en su lugar, una huella digital de los agentes VDA muestra todas las aplicaciones dentro de una sesión.

[#615795]

- El área de trabajo de una sesión activa no se actualiza cuando se cambia de posición o se oculta la estantería de Chrome.

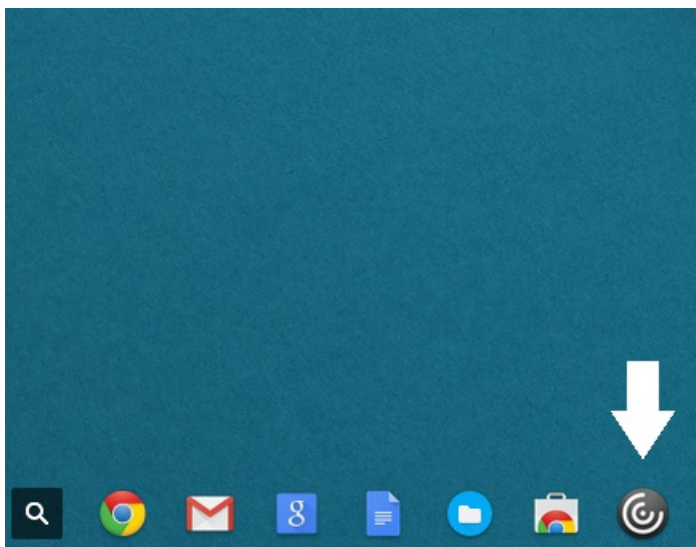
[#623585]

- Puede que tenga que presionar Alt+Tab una segunda vez para cambiar entre aplicaciones de distintos VDA.

Experiencia de usuario

Feb 08, 2017

Después de instalar y configurar Citrix Receiver para Chrome, los usuarios hacen clic en el icono de Citrix Receiver de la lista de aplicaciones de Chrome para iniciar Receiver para Chrome, como se muestra en esta imagen. Para quitar Citrix Receiver para Chrome de los dispositivos, los usuarios deben hacer clic con el botón secundario en el icono de Citrix Receiver en la lista de aplicaciones de Chrome y seleccionar Desinstalar.



Después de iniciar una sesión, aparecen los escritorios y aplicaciones de los usuarios. Estos pueden buscar recursos y hacer clic en cualquier icono para iniciar un escritorio o una aplicación en una ventana nueva.

Cuando un usuario inicia una aplicación adicional, Citrix Receiver para Chrome comprueba si ésta se puede iniciar en una sesión existente antes de crear una nueva sesión. Esto permite a los usuarios acceder a varias aplicaciones a través de una única conexión para que los recursos disponibles se utilicen de forma más eficaz.

Para poder aplicar el uso compartido de sesiones, las aplicaciones deben residir en la misma máquina y deben estar configuradas en el modo de ventana integrada con la misma configuración de parámetros como el tamaño de la ventana, la profundidad de color y el cifrado. El uso compartido de sesiones está habilitado de manera predeterminada cuando una aplicación alojada pasa a estar disponible.

Los usuarios pueden utilizar accesos directos estándar de Windows para copiar datos, incluidos texto, tablas e imágenes, de una aplicación alojada a otra, ya sea dentro de la misma sesión o entre distintas sesiones. Solo se puede copiar y pegar texto Unicode sin formato entre las aplicaciones alojadas y el Portapapeles local del dispositivo.

Los usuarios pueden utilizar cualquier acceso directo estándar de teclado de Windows en Citrix Receiver para Chrome porque estos accesos directos se transfieren de Chrome OS a las aplicaciones alojadas. Del mismo modo, también se pueden usar accesos directos únicos a aplicaciones específicas, siempre que no entren en conflicto con ningún acceso directo de Chrome OS. Sin embargo, tenga en cuenta que la tecla de Windows también se debe presionar para que se reconozcan las teclas de función, por lo que se necesita un teclado externo. Para obtener más información sobre el uso de teclados de Windows con Chrome OS, consulte <https://support.google.com/chromebook/answer/1047364>. Los accesos directos específicos de Citrix, como los que se utilizan para cambiar de una sesión a otra y de una ventana a otra, no se pueden usar en Citrix Receiver para Chrome.

Al imprimir un documento abierto con una aplicación alojada o una aplicación activa en un escritorio virtual, el usuario tendrá la opción de imprimir el documento en PDF. Así, el PDF se transfiere al dispositivo local para verlo e imprimirlo desde una impresora conectada localmente o desde Google Cloud Print. Citrix Receiver para Chrome no almacena el archivo.

Para habilitar la captura de registros en Citrix Receiver para Chrome

Para ayudar a solucionar problemas de conexión, los registros se pueden generar tanto en el dispositivo de usuario como en las máquinas que proporcionan los escritorios y las aplicaciones a los usuarios.

Habilitar la captura de registros en los dispositivos de usuario

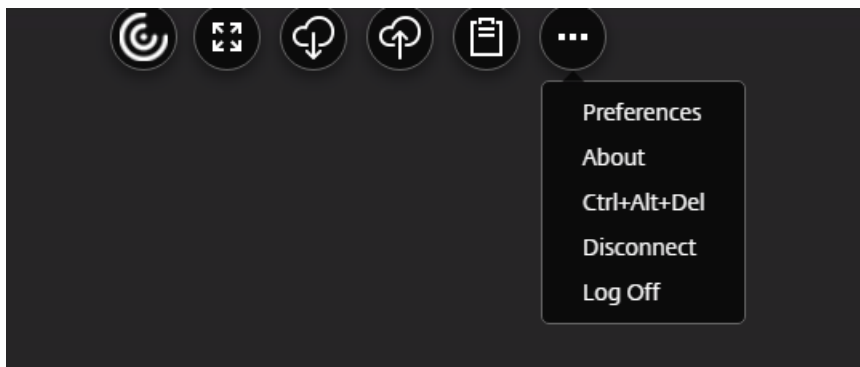
Para capturar registros en un dispositivo de usuario:

1. En el dispositivo de usuario, haga clic en el botón de parámetros, en la esquina inferior derecha de la página de inicio de sesión de Citrix Receiver para Chrome.
2. En el cuadro de diálogo **Parámetros**, haga clic en **Iniciar registro**.
En el cuadro de diálogo Parámetros aparece información detallada de los archivos de registro recopilados.
3. Haga clic en **Detener registro** para finalizar la recopilación de los registros del dispositivo de usuario.

Barra de herramientas rediseñada

Citrix Receiver para Chrome ofrece una barra de herramientas rediseñada para mejorar la experiencia del usuario. Esta mejora ofrece nuevas opciones accesibles desde la barra de herramientas para facilitar tareas comunes como:

- cambiar al modo de pantalla completa
- cargar o descargar un archivo
- copiar el contenido desde una sesión activa al portapapeles para poder compartirlo entre sesiones
- acceder a opciones adicionales



Configuración de la barra de herramientas rediseñada

De manera predeterminada, la barra de herramientas mejorada se instala y se habilita al instalar Citrix Receiver para Chrome.

Para ocultar la configuración de la barra de herramientas usando el archivo configuration.js:

El archivo configuration.js se encuentra en la carpeta raíz de ChromeApp. Edite este archivo directamente para hacer cambios en Citrix Receiver para Chrome.

Nota: Citrix recomienda hacer una copia de seguridad del archivo configuration.js antes de hacer cambios en él.

Nota: Se necesitan credenciales de nivel de administrador para editar el archivo configuration.js. Después de editarlo, vuelva

a empaquetar la aplicación para hacer modificaciones adicionales en los elementos de la barra de herramientas.

1. Abra el archivo configuration.js y defina el atributo "menubar" como "false".

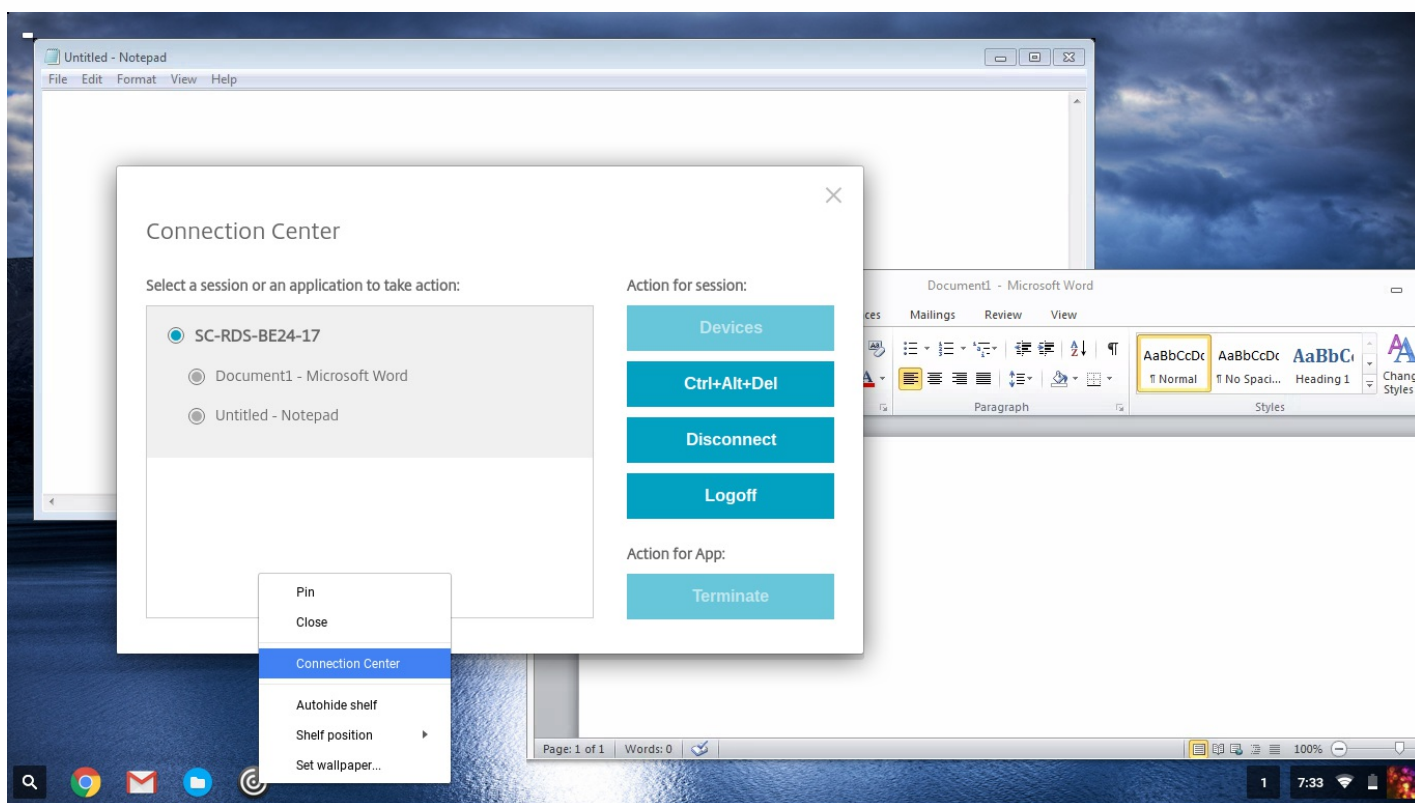
También puede ocultar un icono individual e impedir así que se muestre en la barra de herramientas. Por ejemplo, para ocultar el botón Ctrl+Alt+Supr en la barra de herramientas:

Abra el archivo configuration.js y defina el atributo "lock" como "false".

Central de conexiones

Citrix Receiver para Chrome ofrece funcionalidad en la Central de conexiones para facilitar la administración de aplicaciones en sesiones integradas. Esto se lleva a cabo mediante una barra de tareas que enumera todas las aplicaciones que están abiertas.

Para abrir la Central de conexiones, haga clic con el botón secundario en el icono de Citrix Receiver y haga clic en **Central de conexiones**:



Con el diálogo Central de conexiones, los usuarios pueden elegir una aplicación y:

1. Mostrar dispositivos.
2. Enviar un comando Ctrl+Alt+Supr.
3. Desconectarse de una sesión.
4. Cerrar la sesión.



Connection Center

Select a session or an application to take action:

☐ SC-RDS-BE24-17

☒ Document1 - Microsoft Word

☐ Untitled - Notepad

☐ C:\Windows\System32\cmd.exe

Action for session:

Devices

Ctrl+Alt+Del

Disconnect

Logoff

Action for App:

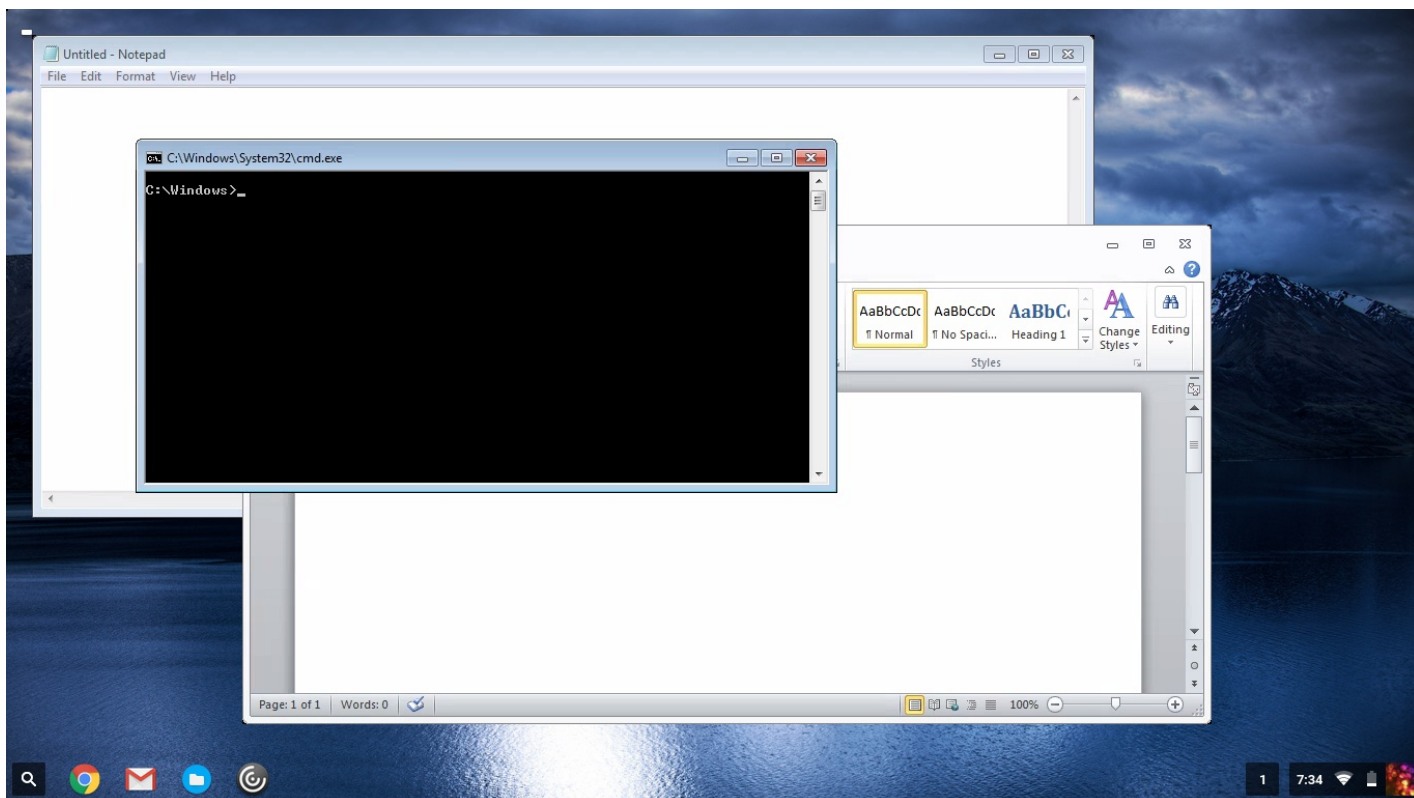
Terminate

También se puede poner fin a una aplicación usando la Central de conexiones, seleccionando el botón de opción de la aplicación en cuestión, luego haciendo clic en **Finalizar**.

Ventanas integradas

Citrix Receiver para Chrome mejora la experiencia del usuario permitiendo la integración de varias aplicaciones alojadas en ventanas distintas dentro de una sesión activa. Usando esta función, Citrix Receiver para Chrome le permite lanzar aplicaciones en una interfaz de usuario independiente en lugar de lanzar todas las aplicaciones de una sesión en una misma ventana.

Las aplicaciones integradas se pueden alojar en sus propias ventanas; con esta funcionalidad, las aplicaciones remotas se ejecutan de forma nativa en el dispositivo cliente.

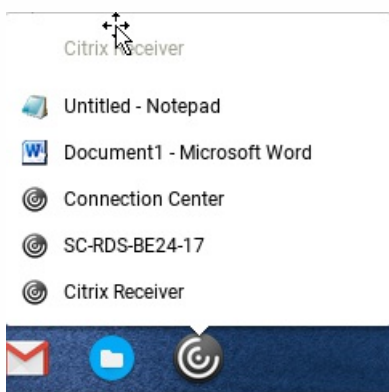


Limitaciones

Tenga en cuenta lo siguiente al usar esta funcionalidad:

- Aparecen entradas adicionales en la barra de tareas de Chrome; haga clic en cualquiera de ellas para traer al frente la sesión seleccionada.
- Todas las aplicaciones abiertas en una misma sesión activa se ejecutan en una misma ventana. Al centrar el foco en una aplicación de la sesión activa, se lleva el foco a su ventana junto con todas las demás aplicaciones que pertenecen a esa sesión.

Use la barra de tareas de la sesión integrada para moverse rápidamente entre las aplicaciones:



Sugerencia

Todas las aplicaciones de una sesión se ejecutan en una ventana única. Al mover una aplicación a un segundo monitor, todas las aplicaciones que forman parte de esa sesión se mueven al segundo monitor.

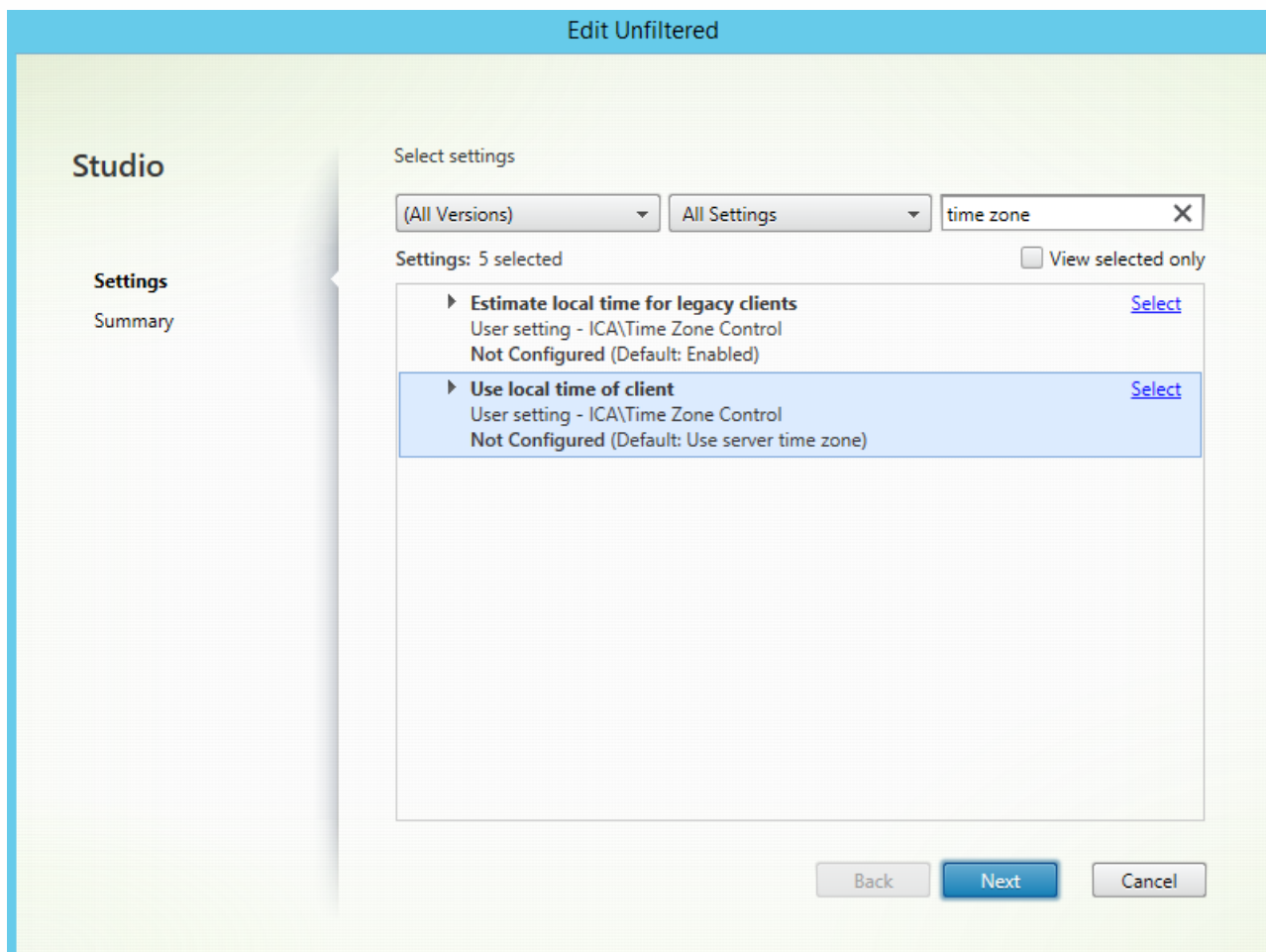
Botón para recargar la URL de la tienda

En Citrix Receiver para Chrome se ha añadido un botón para una operación de recarga. Al hacer clic en el botón, las cookies de la tienda o almacén se borran y la página de la tienda vuelve a cargarse.

Configuración de la zona horaria del cliente

Para habilitar la zona horaria en el cliente:

1. Abra Citrix Studio.
2. Abra la directiva **Usar la hora local del cliente**.
3. Defina la directiva con el valor **Usar zona horaria del cliente**.



Conectividad

Jan 20, 2017

Secure ICA

A partir de la versión 2.1, Citrix Receiver para Chrome se da respaldo al cifrado RC5 (de 128 bits).

Nota

Si hay algún otro formato de cifrado definido, distinto del básico, Citrix Receiver para Chrome actualiza el formato de cifrado a RC5 (128 bits).

Sugerencia

Citrix recomienda usar agentes VDA habilitados para SSL para conseguir cifrado SSL de extremo a extremo.

Implementación de Citrix Receiver

Feb 08, 2017

Existen diversas opciones para implementar Citrix Receiver para Chrome.

- Puede usar la consola de administración de Google Apps para configurar Citrix Receiver con una directiva de Google. Para obtener más información sobre la configuración de Chrome, consulte el artículo de Knowledge Center CTX141844.
- Puede reempaquetar Citrix Receiver para Chrome para incluir un archivo de configuración de Citrix Receiver (.cr) que usted haya generado previamente. El archivo .cr contiene los datos de conexión de NetScaler Gateway y del sitio de Citrix Receiver para Web que proporciona los escritorios y las aplicaciones de los usuarios. Los usuarios deben entrar en chrome://extensions y, a continuación, arrastrar y colocar el archivo de la aplicación reempaquetada (.crx) en la ventana de Chrome para instalar Citrix Receiver para Chrome. Como la aplicación está preconfigurada, los usuarios pueden comenzar a trabajar con Citrix Receiver para Chrome en cuanto éste se haya instalado, sin necesidad de realizar más pasos de configuración.

Puede entregar su versión personalizada de la aplicación de Citrix Receiver para Chrome a los usuarios de las siguientes maneras:

- Publique la aplicación reempaquetada para los usuarios a través de Google Apps for Business mediante la Consola de administración de Google.
- Proporcione el archivo .crx a los usuarios por otros medios, como, por ejemplo, por correo electrónico.
- Los usuarios instalan Citrix Receiver para Chrome desde Chrome Web Store. Para ello, deben hacer una búsqueda de Citrix Receiver y hacer clic en Añadir a Chrome.

Una vez instalado, Citrix Receiver para Chrome debe configurarse con los datos de conexión de NetScaler Gateway y del sitio de Citrix Receiver para Web que proporciona los escritorios y las aplicaciones de los usuarios. Esto puede hacerse de dos maneras:

- Puede generar un archivo .cr que contenga los datos de conexión adecuados y distribuir este archivo a los usuarios. Para configurar Citrix Receiver para Chrome, los usuarios deben hacer doble clic en el archivo .cr y hacer clic en Añadir cuando se les solicite. Para obtener más información acerca de la generación de archivos .cr desde StoreFront, consulte [Exportar archivos de aprovisionamiento de tienda para los usuarios](#).
- Puede proporcionar a los usuarios la URL que deben escribir la primera vez que inicien Citrix Receiver para Chrome.

Para volver a empaquetar Citrix Receiver para Chrome

Para simplificar el proceso de implementación para los usuarios, puede reempaquetar Citrix Receiver para Chrome con un nuevo archivo .cr y preconfigurar Citrix Receiver para Chrome con los datos de conexión adecuados al entorno. Los usuarios pueden comenzar a trabajar con Citrix Receiver para Chrome en cuanto éste se haya instalado, sin necesidad de realizar más pasos de configuración.

1. Descargue la versión sin empaquetar de Citrix Receiver para Chrome a una ubicación adecuada.
2. Descargue el archivo de configuración de ejemplo y modifíquelo para adaptarlo a su entorno.
3. Cambie el nombre del archivo de configuración modificado a default.cr y cópielo en el directorio raíz de Citrix Receiver para Chrome.
Los archivos de configuración con nombres distintos o situados en otras ubicaciones no se incluirán cuando Citrix Receiver para Chrome se reempaquete.

4. Si quiere habilitar la barra de herramientas de la sesión para que permita a los usuarios enviar la combinación de teclas

Ctrl+Alt+Supr a los escritorios y a las aplicaciones, complete los siguientes pasos.

Nota: Citrix recomienda hacer una copia de seguridad del archivo configuration.js antes de hacer cambios en él.

1. Utilice un editor de texto para abrir el archivo configuration.js en el directorio raíz de Citrix Receiver para Chrome.
2. Localice la siguiente sección en el archivo.

```
'appPrefs':{ 'chromeApp':{ 'ui' : { 'toolbar' : { 'menubar':false, 'clipboard': false
```

3. Cambie el parámetro del atributo menubar a **true**.

Al habilitar de este modo la barra de herramientas de la sesión, no es necesario habilitar la barra de herramientas en el archivo de configuración del sitio de Citrix Receiver para Web.

5. De manera predeterminada, Citrix Receiver para Chrome puede abrir cualquier extensión de archivo en la aplicación Archivos de Chromebook destinada a abrir archivos en Google Drive usando el componente FileAccess en el VDA. Si un administrador quiere inhabilitar esta opción para descargar la versión no empaquetada de Citrix Receiver para Chrome y editar la sección de "file handlers" en manifest.ison para que se asemeje a lo siguiente:

```
"file handlers" : {  
  "text" :  
    "extensions" : [  
      "ica",  
      "cr"  
    ]  
  }  
}
```

6. En Chrome, vaya a chrome://extensions, marque la casilla **Modo de desarrollador** de la esquina superior derecha de la página y, a continuación, haga clic en el botón **Empaquetar extensión**.

Por motivos de seguridad, StoreFront solo acepta conexiones de instancias conocidas de Citrix Receiver para Chrome. Debe poner en lista blanca la aplicación reempaquetada para que los usuarios puedan conectarse a un sitio de Citrix Receiver para Web.

7. En el servidor StoreFront, utilice un editor de texto para abrir el archivo web.config del sitio de Citrix Receiver para Web, que normalmente se encuentra en el directorio C:\inetpub\wwwroot\Citrix\storenameWeb\, donde *storename* es el nombre especificado para la tienda en el momento de su creación.
8. Localice el siguiente elemento en el archivo.
<html5 ... chromeAppOrigins="chrome-extension://haiffjcadagjlijoggckpgfnoeiflnem" ... />
9. Cambie el valor del atributo **chromeAppOrigins** a chrome-extension://haiffjcadagjlijoggckpgfnoeiflnem| chrome-extension://ID del paquete, donde **ID del paquete** es el ID generado por la aplicación reempaquetada.

Configuración del entorno

Feb 08, 2017

Para permitir que los usuarios de Citrix Receiver para Chrome puedan acceder a recursos alojados en XenDesktop y XenApp, debe crear una tienda o almacén de StoreFront. También debe habilitar las conexiones WebSocket en NetScaler Gateway, XenApp y XenDesktop, según considere necesario.

Configuración de Selective H.264

Configuración de Selective H.264 mediante web.config en StoreFront

Para cambiar la configuración de Selective H.264 usando el archivo web.config:

1. Abra el archivo web.config del sitio Web de Citrix Receiver para Web.
Este archivo se encuentra normalmente en la carpeta C:\inetpub\wwwroot\Citrix\Web, donde *Storename* es el nombre especificado para la tienda cuando se creó.
2. Busque el campo **chromeAppPreferences** y establezca su valor con la configuración en forma de cadena JSON; por ejemplo:
`chromeAppPreferences={"graphics":{"selectiveH264":false}}`

Configuración de Selective H.264 mediante el archivo configuration.js

El archivo configuration.js se encuentra en la carpeta raíz de ChromeApp. Edite este archivo para hacer cambios en Citrix Receiver para Chrome.

De manera predeterminada, Selective H.264 tiene el valor True.

Nota: Citrix recomienda hacer una copia de seguridad del archivo configuration.js antes de hacer cambios en él.

Nota: Citrix recomienda usar este método solo cuando reempaquete Citrix Receiver para Chrome para los usuarios.

Nota: Se necesitan credenciales de nivel de administrador para editar el archivo configuration.js. Después de editarlo, vuelva a empaquetar la aplicación para hacer modificaciones adicionales en los elementos de la barra de herramientas.

Para inhabilitar la configuración de Selective H.264 usando el archivo configuration.js:

1. Abra el archivo configuration.js y establezca el atributo selectiveH264 con el valor **false**.
Por ejemplo:

```
'graphics': {  
    'selectiveH264': false  
}
```

Configuración de la presentación multimonitor

La presentación multimonitor se puede configurar de dos formas.

De manera predeterminada, la función de presentación multimonitor está habilitada.

Nota

- Si usa Citrix Receiver para Chrome ejecutado en XenApp 6.5, configure la directiva de **remedo** como **Inhabilitada** para usar la presentación multimonitor.
- En una sesión de escritorio, cuando la ventana está en modo de pantalla completa, la opción de Resolución de pantalla en las Preferencias está desactivada.
- Los diálogos y barras de herramientas de la interfaz de usuario solo aparecen en el monitor principal. No obstante, los diálogos de tarjeta inteligente y USB abarcan los distintos monitores.

Para configurar la presentación multimonitor usando el explorador Web Chrome:

1. Abra un explorador Web e introduzca este comando:
chrome://flags
2. En la lista de funciones, busque UnifiedDesktopMode y configúrela como **Habilitada**.

Para configurar la presentación multimonitor usando Google Admin Policy

1. Inicie una sesión en la Consola de administración de Google.
2. Vaya a Administración de dispositivos > Administración de Chrome > Configuración de usuario.
3. Defina la política de Google "Escritorio unificado" con el valor **Hacer que el modo de escritorio unificado esté disponible para el usuario**.
4. Haga clic en Guardar.

La presentación multimonitor está disponible tanto para escritorios como para aplicaciones.

Cuando se usa la presentación multimonitor, la sesión de escritorio puede abarcar varios monitores de dos maneras:

1. Modo de ventana: La sesión de escritorio se muestra en modo de monitor único.
2. Modo de pantalla completa: Cuando se cambia la sesión de escritorio al modo de pantalla completa, la sesión se muestra en modo multimonitor.

En una sesión de aplicación, cuando hay dos monitores conectados y UnifiedDesktopMode está **Habilitado**, como se describe más arriba, la sesión se muestra automáticamente en modo multimonitor.

Nota

Cuando el modo de escritorio unificado está habilitado, la página de inicio de Citrix Receiver para Chrome aparece solo en el monitor principal.

HDX SDK para Chrome (API experimental)

Procedimiento para consumir la API en la aplicación Chrome de terceros

1. Instale la versión más reciente de Citrix Receiver para Chrome. Consulte la página de [descargas de Citrix](#) para ver más información.
2. Añada la aplicación Chrome de terceros a una lista blanca agregando el archivo de directiva de Citrix Receiver para Chrome usando los parámetros de administración de Chrome.
Para obtener más información, consulte [Administración de aplicaciones Chrome por unidad organizativa](#) en Google Support.

El archivo policy.txt de muestra para añadir la aplicación Chrome de terceros a una lista blanca es como el siguiente:

comando

COPIAR

```
{

  "settings": {

    "Value": {

      "settings_version": "1.0",

      "store_settings": {

        "externalApps": ["<3rdParty_App1_ExtnID>","<3rdParty_App2_ExtnID>"]

      }

    }

  }

}
```

Nota

<3rdParty_App1_ExtnID> se usa como ejemplo para el nombre de aplicaciones externas y puede enviar mensajes a Citrix Receiver para Chrome. Obtenga el **appid** desde el sitio <chrome://extensions>.

3. Lance la sesión de escritorio o de aplicación en Citrix Receiver para Chrome siguiendo estos pasos:

- Obtener el receiverId

```
var receiverId = " haiffjcadagjljoggckpgfnoeiflnem "; //
```

Nota: En este ejemplo, **receiverId** indica la versión de tienda de aplicaciones de Citrix Receiver para Chrome. Si usa la versión reempaquetada de Citrix Receiver para Chrome, use el receiverId apropiado.

- Convierta los datos ICA desde INI al formato JSON.

Nota: Normalmente, el archivo ICA se obtiene desde StoreFront como un archivo INI. Use la función auxiliar siguiente para convertir un archivo ICA de INI a JSON.

//Función auxiliar para convertir ICA en formato INI a formato JSON

```
function convertICA_INI_TO_JSON(data){
```

```
var keyVals = {};
```

```
if (data) {
```

```
var dataArr;
```

```
if(data.indexOf("\r")==-1){
```

```
dataArr = data.split("\n");
```

```
}else{
```

```
dataArr = data.split("\r\n");
```

```
}
```

```
for (var i = 0; i < dataArr.length; i++) {
```

```
var nameValue = dataArr[i].split('=', 2);
```

```
if (nameValue.length === 2) {
```

```
keyVals[nameValue[0]] = nameValue[1];
```

```
}
```

```
// Esto es necesario porque LaunchReference contendrá '=' también. El split('=',2) anterior no devolverá la referencia
```

```
// LaunchReference completa. Preferiblemente, debe usarse también algo como lo siguiente de modo genérico
```

```
// porque puede haber otras variables que usen el carácter '=' como parte de su valor.
```

```
if (nameValue[0] === "LaunchReference") {
```

```
var index = dataArr[i].indexOf('=');
```

```
var value = dataArr[i].substr(index + 1);
```

```
keyVals[nameValue[0]] = value;
```

```
}
```

```
}
```

```
console.log(keyVals); //para quitarlos
```

```
return keyVals;
```

```
}
```

```
return null;
```

```
}
```

- Envíe un mensaje ICA desde la aplicación Chrome de terceros a Citrix Receiver para Chrome.

```
var icaFileJson = {...}; // Archivo ICA pasado como pares de clave y valor de JSON.
```

```
var mensaje = {
```

```
"método": "launchSession",
```

```
"icaData": icaJSON
```

```
};
```

```
chrome.runtime.sendMessage (receiverId, mensaje, function(launchStatus) {
```

```
if (launchStatus.success) {
```

```
// gestionar success.console.log("Lanzamiento de sesión correcto");
```

```
console.log("Error al lanzar la sesión: ", launchStatus.message);
```

Para ver más detalles sobre los comandos sendmessage de la API, consulte estos enlaces:

<https://developer.chrome.com/extensions/runtime#event-onMessageExternal>

<https://developer.chrome.com/extensions/runtime#method-sendMessage>

Configuración de Citrix Receiver para Chrome

Esta sección incluye información acerca de:

- Directiva de administración de Google
- Web.config en StoreFront
- default.ica
- configuration.js

Configuración de Citrix Receiver para Chrome usando Google Admin Policy

Antes de la versión 2.1, solo se podía enviar configuración relacionada con tiendas o balizas mediante la directiva de administración de Google (Google Admin Policy). Para ver información adicional sobre esta directiva, consulte el artículo de Knowledge Center CTX141844.

Con Citrix Receiver para Chrome versión 2.1, otras configuraciones de Chrome también pueden enviarse a través de la directiva de administración de Google.

Nota

Citrix recomienda usar este método solo cuando reempaquete Citrix Receiver para Chrome para los usuarios.

Para obtener más información, consulte el siguiente texto de directiva de ejemplo:

comando

COPIAR

```
{  
  
  "settings": {  
  
    "Value": {  
  
      "settings_version": "1.0",  
  
      "store_settings": {  
  
        "name": "RTST",
```



```

        "rf_web": {

            "url": "http://yourcompany.storefrontstoreweb.net"

        }

    },

    "engine_settings":{

        "ui":{

            "sessionsize": {

                "windowstate": "fullscreen",

                "available" : {

                    "default" : "Fit_To_Window",

                    "values" : ["Fit_To_Window", "Use_Device_Pixel_Ratio", "
                }

            },

            "toolbar": {

                "menubar":true,

                "usb": true,

                "fileTransfer":true,

                "about":true,

                "lock":true,

                "disconnect":true.

```

```

        "logoff":true,

        "fullscreen":true,

        "multitouch":true,

        "preferences":true,

        "gestureGuide":true

    }

},

"features":{

"com":{

        "portname" : "COM5"

    },

    "graphics" : {

        "features" : {

            "graphics" : {

                "jpegSupport" : true,

                "h264Support" : {

                    "enabled" : true,

                    "losslessOverlays" : true,

```



```

        "dirtyRegions" : true,

        "yuv444Support" : false

    },

    },

    "filetransfer" : {

        "allowupload" : true,

        "allowdownload" : true,

        "maxuploadsize"      : 2147483647,

        "maxdownloadsize" : 2147483647

    },

    },

    "nacl" : {

        "supportNacl" : true,

        "graphics": {

            "enable": true

        },

        "video": {

            "enable": true

        },

        "audio": {

```



Configuración de Receiver para Chrome usando el archivo Web.config en StoreFront

Para cambiar la configuración usando el archivo Web.config:

1. Abra el archivo **web.config** del sitio Web de Citrix Receiver para Web. Típicamente, el archivo se encuentra ubicado en el directorio **C:\inetpub\wwwroot\Citrix\storenameWeb**, donde *storename* es el nombre que fue especificado para la tienda cuando fue creada.
2. Busque el campo **chromeAppPreferences** y defina su valor con la configuración como cadena JSON.

Por ejemplo:

```
chromeAppPreferences = '{"ui": {"toolbar": {"menubar": false}}}'
```

Nota

Citrix recomienda usar el método del archivo **web.config** para la configuración solo cuando se esté usando una versión de tienda de aplicaciones de Citrix Receiver para Chrome.

Configuración de Receiver para Chrome usando el archivo default.ica

Para cambiar la configuración usando el archivo **default.ica**:

1. Abra el archivo **default.ica**, ubicado normalmente en **C:\inetpub\wwwroot\Citrix\<nombre del sitio>\conf\default.ica** para los clientes de la Interfaz Web, donde **nombre del sitio** es el nombre especificado para el sitio cuando fue creado.
En el caso de clientes de StoreFront, el archivo **default.ica** se encuentra normalmente en **C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica**, donde **storename** es el nombre especificado para la tienda cuando fue creada.
2. Agregue una nueva clave al final del archivo, **chromeAppPreferences**, con el valor definido con la configuración como objeto JSON.

Por ejemplo:

```
chromeAppPreferences={"ui":{"toolbar":{"menubar": false}}}
```

Nota

Citrix recomienda usar el método del archivo **default.ica** con fines de configuración solo para usuarios de la Interfaz Web.

Un archivo **default.ica** es similar al siguiente:

```
;  
;  
; ICA Override File  
;  
;  
; Agregue parámetros de archivo ICA que quiera enviar a los dispositivos cliente  
; a este archivo. Los parámetros contenidos en este archivo pueden sobrescribir algunos  
; parámetros generados por Delivery Services.  
;
```

[WFClient]

Version=2

RemoveICAFile=yes

ProxyTimeout=30000

ProxyFavorIEConnectionSetting=Yes

ProxyUseFQDN=Off

[ApplicationServers]

Application=

[Application]

TransportDriver=TCP/IP

DoNotUseDefaultCSL=On

BrowserProtocol=HTTPonTCP

LocHttpBrowserAddress=!

WinStationDriver=ICA 3.0

ProxyTimeout=30000

AutologonAllowed=ON

;EncryptionLevelSession=RC5 (128 bit)

[EncRC5-0]

DriverNameWin16=cdc0w.dll

DriverNameWin32=cdc0n.dll

[EncRC5-40]

DriverNameWin16=cdc40w.dll

DriverNameWin32=cdc40n.dll

[EncRC5-56]

DriverNameWin16=cdc56w.dll

DriverNameWin32=cdc56n.dll

[EncRC5-128]

DriverNameWin16=cdc128w.dll

DriverNameWin32=cdc128n.dll

[Compress]

DriverNameWin16=pdcompw.dll

DriverNameWin32=pdcompn.dll

chromeAppPreferences={"ui":{"toolbar":{"menubar":false}}}

Configuración de Citrix Receiver para Chrome usando el archivo configuration.js

El archivo **configuration.js** se encuentra en la carpeta raíz de ChromeApp. Acceda a este archivo directamente para hacer cambios en Citrix Receiver para Chrome.

Nota

- Citrix recomienda hacer una copia de seguridad del archivo configuration.js antes de hacer cambios en él.
- Se necesitan credenciales de nivel de administrador para editar el archivo configuration.js. Después de editarlo, vuelva a empaquetar la aplicación para hacer modificaciones adicionales en los elementos de la barra de herramientas.
- En modo quiosco, la barra de herramientas está oculto de forma predeterminada. Cuando edite el archivo configuration.js para habilitar la barra de herramientas, asegúrese de que el modo quiosco está inhabilitado. Citrix recomienda usar uno de los métodos alternativos (por ejemplo, el archivo defaultica) para habilitar la barra de herramientas.

Cómo habilitar la autenticación con tarjeta inteligente

Receiver para Chrome respalda el uso de lectores de tarjetas inteligentes USB con StoreFront. Puede usar tarjetas inteligentes con estos fines:

- Autenticación de inicio de sesión con tarjetas inteligentes en Receiver para Chrome.
- Aplicaciones publicadas para acceder a dispositivos locales de tarjeta inteligente.
- Aplicaciones como Microsoft Word y Outlook que se inician en sesiones ICA pueden acceder a las tarjetas inteligentes para firmar documentos y correo electrónico.

Las tarjetas inteligentes respaldadas incluyen:

- Tarjetas PIV
- Tarjetas CAC (Common Access Card)

Requisitos previos:

- StoreFront versión 3.6 o posteriores

Important

Para la autenticación con tarjeta inteligente en StoreFront 3.5 o versiones anteriores, los usuarios necesitan un script personalizado para habilitar la autenticación con tarjeta inteligente. Póngase en contacto con el servicio de asistencia Citrix Support para obtener más información.

- XenDesktop 7.6 o versiones posteriores
- XenApp 6.5 o versiones posteriores

Para configurar el respaldo para tarjetas inteligentes en el dispositivo Chrome:

1. Instale la aplicación de conector de tarjeta inteligente. Tenga en cuenta que la aplicación de tarjeta inteligente es necesaria para el respaldo de PCSC en el dispositivo Chrome. Esta aplicación lee la tarjeta inteligente usando la interfaz USB. Esta aplicación puede instalarse desde el [sitio Web de Chrome](#).
 2. Instale la aplicación de middleware. Tenga en cuenta que se necesita una aplicación de middleware (por ejemplo Charismathics o CACKey) porque sirve de interfaz para comunicarse con la tarjeta inteligente y otros certificados del cliente.
- Para instalar la extensión de tarjeta inteligente de Charismathics o CACKey, consulte las instrucciones descritas en el [sitio Web de Chrome](#).

- Para obtener más información sobre las aplicaciones de middleware y la autenticación con tarjeta inteligente, consulte el [sitio de asistencia técnica de Google](#).
3. Configure la autenticación con tarjeta inteligente usando NetScaler Gateway. Para obtener más información, consulte [Configuración de la autenticación con tarjeta inteligente](#) en la documentación de NetScaler Gateway.

Important

Se requiere la autenticación del cliente obligatoria para lanzar una sesión. Para evitar que esto ocurra, consulte las instrucciones descritas en la sección [Third reduction \(one PIN prompt\)](#) de la documentación del producto de NetScaler.

El respaldo para autenticación con tarjetas inteligentes tiene las siguientes limitaciones:

- El certificado de tarjeta inteligente se guarda guardado en caché incluso después de quitar la tarjeta inteligente del dispositivo Chrome. Este es un problema conocido de Google Chrome. Para borrar la caché hay que reiniciar Chrome.
- Cuando Receiver para Chrome se reempaqueta, los administradores deben obtener el appId de la lista blanca de Google para asegurarse de que la aplicación de conector de tarjeta inteligente puede pasar.
- Solo se admite un lector de tarjeta inteligente a la vez.

Configuración de la redirección de puertos COM serie

Para configurar la redirección de puertos COM serie, habilite la función aplicando configuraciones de directiva de redirección de puertos de XenApp/XenDesktop. Para obtener más información sobre la redirección de puertos, consulte [Configuraciones de directiva de Redirección de puertos](#).

Nota

De manera predeterminada, Receiver para Chrome asigna COM5 como puerto COM serie preferido para la redirección.

Después de habilitar configuraciones de directiva de redirección de puertos COM serie en XenApp/XenDesktop, configure Citrix Receiver para Chrome usando alguno de los métodos siguientes:

- Directiva de administración de Google
- Usando el archivo configuration.js
- Cambiando la asignación predeterminada emitiendo un comando en una sesión ICA activa.

Uso de la directiva de administración de Google para configurar la redirección de puertos COM

Use este método para redirigir el puerto COM serie editando el archivo de directivas.

Sugerencia

Citrix recomienda configurar el puerto COM usando el archivo de directivas solo cuando Receiver para Chrome sea reempaquetado.

Edite la directiva de administración de Google incluyendo lo siguiente:

```
{

  "settings": {

    "Value": {

      "settings_version": "1.0",

      "store_settings": {

        "rf_web": {

          "url": "<http://YourStoreWebURL>"

        }

      },

      "engine_settings": {

        "features" : {

          "com" : {

            "portname" : "<COM4>", where COM4 indicates the port number that is set to

          }

        }

      }

    }

  }

}
```



Uso del archivo configuration.js para configurar la redirección de puertos COM

Use este método para redirigir el puerto COM serie editando el archivo **configuration.js**. Busque el campo "portname" en el archivo configuration.js y edite el valor cambiando el número de puerto.

Por ejemplo:

```
"com" :{  
    "portname" : "COM4"  
}
```

Nota

Citrix recomienda usar el método del archivo configuration.js para configurar la redirección de puertos solo cuando Receiver para Chrome sea reempaquetado y republicado desde StoreFront.

Emisión de un comando en una sesión ICA para configurar la redirección de puertos COM

Use este método para redirigir el puerto COM serie ejecutando el comando siguiente en una sesión ICA activa:



Sugerencia

En el ejemplo de arriba, COM4 es el puerto serie preferido para la redirección.

Configuración de Single Sign-on (SSO) con Google y Citrix usando autenticación SAML

Para configurar Single Sign-on:

1. Configure el proveedor de identidades (IdP) de terceros para la autenticación SAML si todavía no lo tiene configurado (por ejemplo, ADFS 2.0). Para obtener más información, consulte el artículo de Knowledge Center [CTX133919](#).
2. Configure Single Sign-on con Google Apps usando el proveedor de identidades SAML; esto permite a los usuarios usar la identidad de terceros para usar Google Apps en lugar de la cuenta de Google Enterprise. Para obtener más información, consulte [Set up Single Sign-On \(SSO\) for Google Apps accounts using third-party identity providers](#) en Google Support.
3. Configure los dispositivos Chrome para iniciar sesiones a través del proveedor de identidades SAML. Esto permite a los

usuarios iniciar sesión en los dispositivos Chrome usando el proveedor de identidades de terceros. Para obtener más información, consulte [Configure SAML Single Sign-On for Chrome devices](#) en Google Support.

4. Configure NetScaler Gateway para iniciar sesión a través del proveedor de identidades SAML. Esto permite que los usuarios inicien sesiones en NetScaler Gateway usando un proveedor de identidades de terceros. Para obtener más información, consulte [Configuración de la autenticación SAML](#).
5. Configure XenApp y XenDesktop para la autenticación federada para permitir el inicio de sesión en sesiones de XenApp/XenDesktop usando certificados generados dinámicamente después del proceso de inicio de sesión SAML en lugar de tener que escribir combinaciones de nombre de usuario y contraseña. Para obtener más información, consulte [Autenticación federada](#).
6. Instale y configure la extensión SAML SSO for Chrome en los dispositivos Chrome. Para obtener más información, consulte este sitio Web de Google. Esta extensión obtiene cookies de SAML del explorador Web y las suministra Citrix Receiver. Esta extensión tiene que estar configurada con la siguiente directiva para permitir que Receiver obtenga las cookies de SAML:

comando

COPIAR

```
{

  "whitelist" : {

    "Value" : [

      {

        "appld" : "haiffjcadagjljoggckpgfnoeiflnem",

        "domain" : "saml.yourcompany.com"

      }

    ]

  }

}
```

Si reempaqueta Citrix Receiver para Chrome, cambie el valor de appld como corresponda. Además, cambie el dominio por el dominio del proveedor de identidades SAML de su empresa.

7. Configure Receiver para usar NetScaler Gateway configurado para el inicio de sesión SAML. Esto permite a los usuarios usar el NetScaler Gateway configurado para el inicio de sesión SAML. Para obtener más información sobre la configuración

de Chrome, consulte el artículo de Knowledge Center [CTX141844](#).

Cómo habilitar la impresión de Google Cloud y el controlador de impresora universal de Citrix

El controlador Citrix PDF Universal Printer permite a los usuarios imprimir documentos abiertos con aplicaciones alojadas o aplicaciones ejecutadas en escritorios virtuales entregados por XenDesktop 7.6 y XenApp 7.6. Cuando un usuario selecciona la opción Citrix PDF Printer, el controlador convierte el archivo a PDF y transfiere el PDF al dispositivo local. El PDF se abre en una ventana nueva para verlo e imprimirlo desde Google Cloud Print.

Important

La impresión local en PDF solo recibe respaldo en XenApp y XenDesktop 7.6 o versiones posteriores.

Requisitos

Para acceder a la página de descarga de Citrix Receiver para Chrome, necesita una cuenta de MyCitrix.

Descargue la impresora Citrix PDF Printer desde la [página de descarga de Citrix Receiver para Chrome](#).

Para que los usuarios puedan imprimir documentos abiertos con escritorios y aplicaciones alojadas:

1. Descargue la impresora Citrix PDF Printer e instale el controlador Citrix PDF Universal Printer en cada máquina que entrega escritorios o aplicaciones a usuarios de Receiver para Chrome. Después de instalar el controlador de la impresora, reinicie la máquina.
2. En Citrix Studio, seleccione el nodo Directiva del panel izquierdo y cree una directiva nueva o modifique una directiva existente.
Para obtener más información sobre la configuración de directivas de XenDesktop y XenApp, consulte las [directivas de Citrix](#).
3. Establezca la configuración de directiva Crear automáticamente la impresora universal de PDF como **Habilitada**.

Cómo habilitar o inhabilitar el acceso a Google Drive

Con el respaldo para Google Drive, los usuarios pueden abrir, editar y guardar tipos de archivos de Windows desde un dispositivo Chrome que ejecute Citrix Receiver. Mientras están ejecutando un dispositivo Google Chrome, los usuarios pueden utilizar aplicaciones existentes basadas en Windows (por ejemplo, Microsoft Word) y acceder a los archivos que residen en Google Drive.

Por ejemplo, si un usuario abre un archivo en Google Drive (por ejemplo, un archivo .doc adjunto descargado de Gmail), lo edita y lo guarda en Google Drive, se puede acceder al archivo en una aplicación alojada de XenApp. El archivo puede verse, editarse y guardarse en Google Drive.

Requisitos previos

Para habilitar el acceso a Google Drive debe instalar el componente Citrix File Access (FileAccess.exe) en los VDA y habilitar la asociación de tipos de archivos en Citrix Studio. Citrix File Access se puede descargar desde la [página de descargas de Citrix Receiver para Chrome](#).

Para habilitar el acceso a Google Drive desde Citrix Receiver

1. Instale FileAccess.exe en cada VDA de XenApp o XenDesktop.
2. En Citrix Studio, configure las asociaciones de tipos de archivos adecuadas para las aplicaciones publicadas.
3. En el VDA de XenApp/XenDesktop, es necesario configurar <https://accounts.google.com> y <https://ssl.gstatic.com> como sitios de confianza y las cookies de estos sitios deben estar habilitadas.

Solo se pueden abrir archivos de Google Drive usando Citrix Receiver. Para abrir un archivo desde Google Drive, haga clic con el botón secundario y abra el archivo usando Citrix Receiver.

Citrix recomienda asociar un tipo de archivo con una sola aplicación publicada.

Para inhabilitar el acceso a Google Drive desde Citrix Receiver

En el archivo manifest.json, reemplace:

```
"file_handlers": {  
  "all-file-types" : {  
    "extensions" : [  
      ""  
    ]  
  }  
},
```

por:

Code

COPIAR

```
"file_handlers" : {  
  
  "cr-file-type" : {  
  
    "extensions" : [  
  
      "cr",  
  
      "ica"  
  
    ]  
  
  }  
  
},
```

Cómo habilitar y configurar el modo quiosco

El modo quiosco de Citrix Receiver para Chrome permite ejecutar todas las aplicaciones en la misma ventana. Con esta funcionalidad, se pueden ejecutar aplicaciones de Citrix Receiver en modo quiosco y luego iniciar cualquier escritorio o aplicación de Windows usando el mismo modo. Además, el modo quiosco permite publicar aplicaciones o escritorios remotos como paquetes Chrome dedicados usando una URL persistente.

Puede controlar esta funcionalidad ajustando los parámetros de quiosco en el panel de administración de Chrome para dispositivos Chrome administrados.

Consulte el [sitio de asistencia de Google](#) para obtener instrucciones sobre cómo habilitar la aplicación de Receiver para ejecutarse en modo quiosco en dispositivos Chrome administrados y no administrados.

Si está implementando una aplicación de Receiver, debe publicar usando las opciones de visibilidad configuradas como Pública/Ocultas (Public/Unlisted) para garantizar la interoperabilidad con el modo quiosco. [Vaya al Panel para desarrolladores de Chrome Web Store](#).

La URL de la tienda es de solo lectura cuando el modo quiosco está activo, y no se puede editar usando la pantalla de parámetros de Cuenta. No obstante, puede cambiar este parámetro reempaquetando la aplicación con el archivo .cr, o mediante la administración de directivas de Google en la consola de administración de Google.

Ejemplo de archivo .cr

COPIAR

```
<Services version="1.0">
```

```
<Service>
```

```
<rfWeb>http://your_RfWebURL_or_persistenturl</rfWeb>

<Name>Mystore</Name>

<Gateways>

<Gateway>

<Location>https://yourcompany.gateway.com</Location>

</Gateway>

</Gateways>

<Beacons>

<Internal>

<Beacon>http://yourcompany.internalwebsite.net</Beacon>

</Internal>

<External>

<Beacon>http://www.yourcompany.externalwebsite.com</Beacon>

</External>

</Beacons>

</Service>

</Services>
```

Si está usando la consola de administración de Google, edite el archivo policy.txt que contiene la configuración de Receiver. Sustituya el valor de “url” bajo “rf_web” por una URL persistente.

por ejemplo,

COPIAR

```
{

"settings": {

"Value": {

"settings_version": "1.0",

"store_settings": {

"beacons": {

"external": [

{

"url": "http://www.yourcompany.externalwebsite.com"

}

],

"internal": [

{

"url": "http://yourcompany.internalwebsite.net"

}

]

},

"gateways": [

{
```

```
"is_default": true,  
  
"url": "https://yourcompany.gateway.com"  
  
}  
  
],  
  
"name": "mystore",  
  
"rf_web": {  
  
"url": " http://your_RfWebURL_or_persistenturl "  
  
}  
  
}  
  
}  
  
}  
  
}
```

Fiabilidad de la sesión

Con la función de fiabilidad de la sesión, la sesión permanece activa en el servidor aunque se interrumpa la conectividad. Para indicar que se ha perdido conectividad, la pantalla del usuario deja de responder hasta que se recupera la conectividad. El usuario sigue teniendo acceso a la presentación en pantalla durante la interrupción y puede reanudar la interacción con la aplicación después de restablecerse la conexión de red.

La función Fiabilidad de la sesión vuelve a conectar a los usuarios sin pedirles que repitan la autenticación.

Nota

Puede usar la función de fiabilidad de la sesión con Transport Layer Security (TLS).

Uso de directivas de fiabilidad de la sesión

La configuración de directiva Conexiones de fiabilidad de la sesión permite o impide la fiabilidad de la sesión.

La configuración de directiva Tiempo de espera de fiabilidad de la sesión tiene un tiempo predeterminado de 180 segundos (tres minutos). Aunque puede ampliar la cantidad de tiempo que la fiabilidad de la sesión mantiene abierta una sesión, esta función está diseñada para la comodidad del usuario, por lo que no desconecta la sesión.

Sugerencia

Si se alarga la cantidad de tiempo que una sesión se mantiene abierta, se incrementa el riesgo de que un usuario se distraiga, se aleje del dispositivo y con ello facilite a usuarios no autorizados el acceso a la sesión.

Las conexiones entrantes de la función de fiabilidad de la sesión utilizan el puerto 2598, a menos que cambie el número de puerto definido en la configuración de directiva Número de puerto para fiabilidad de la sesión.

Nota

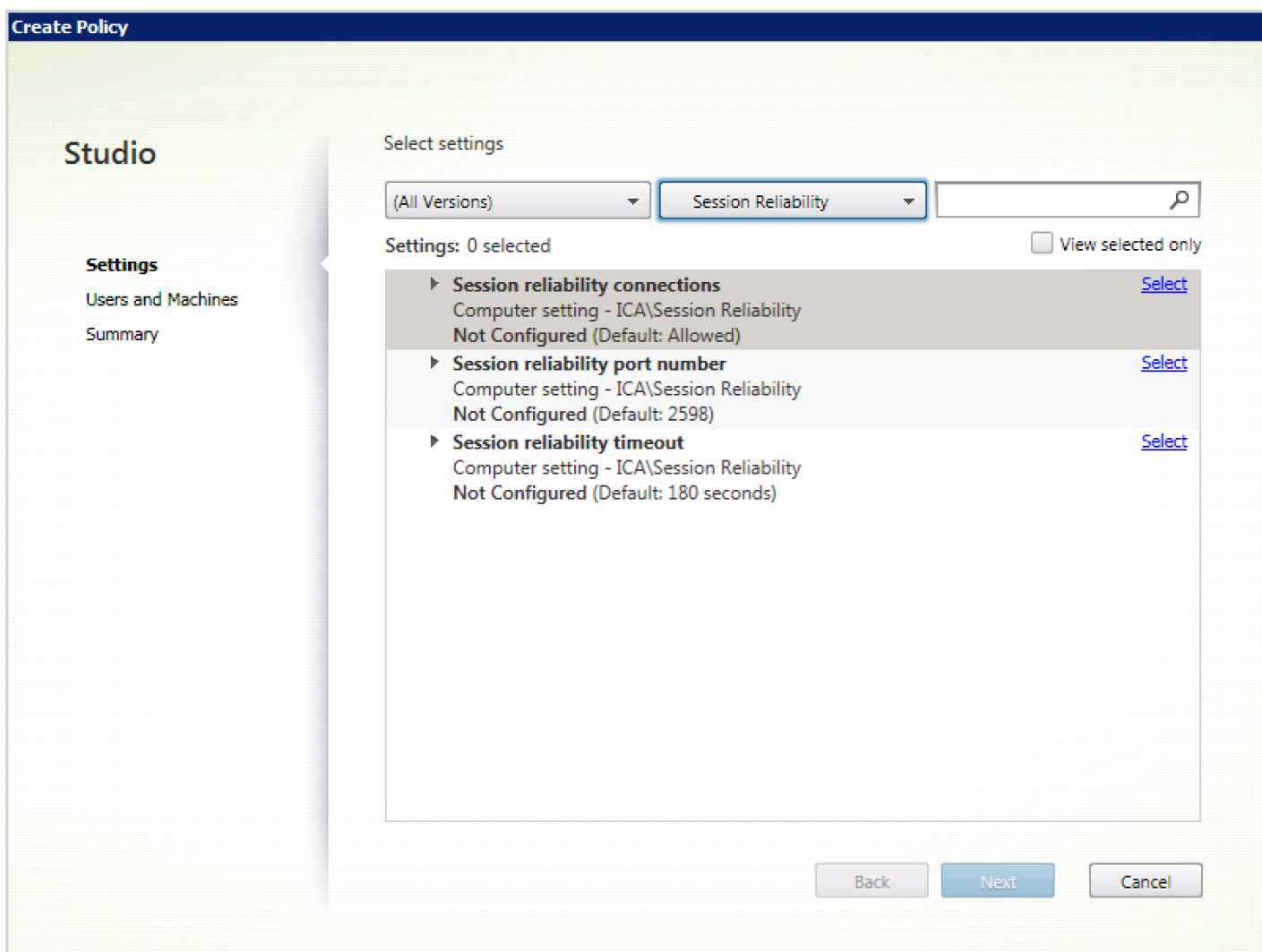
De forma predeterminada, la fiabilidad de sesión está habilitada en el servidor. Para inhabilitar esta función, configure la directiva administrada por el servidor.

Configuración de la fiabilidad de la sesión

De forma predeterminada, la fiabilidad de la sesión está habilitada.

Para inhabilitar la fiabilidad de la sesión:

1. Abra Citrix Studio.
2. Abra la directiva **Conexiones de fiabilidad de la sesión**.
3. Configure la directiva con el valor **Prohibida**.



Configuración del tiempo de espera de la fiabilidad de la sesión

Nota

La directiva Tiempo de espera de fiabilidad de la sesión se puede configurar solo en XenApp/XenDesktop 7.11 y versiones posteriores.

Para modificar el tiempo de espera de la fiabilidad de la sesión:

De manera predeterminada, el tiempo de espera de la fiabilidad de la sesión es 180 segundos.

1. Abra Citrix Studio.
2. Abra la directiva **Tiempo de espera de fiabilidad de la sesión**.
3. Modifique el valor del tiempo de espera.
4. Haga clic en **Aceptar**.

Configuración del nivel de transparencia de la interfaz de usuario durante la reconexión

La interfaz de usuario durante una sesión se muestra en pantalla durante los intentos de reconexión de la función de fiabilidad de la sesión. El nivel de transparencia de la interfaz de usuario se puede modificar mediante directiva en Studio.

De manera predeterminada, el nivel de transparencia de la interfaz de usuario es del 80%.

Para modificar el nivel de transparencia de la interfaz de usuario durante una reconexión:

1. Abra Citrix Studio.
2. Abra la directiva **Nivel de transparencia de la interfaz de usuario durante la reconexión**.
3. Cambie el valor.
4. Haga clic en **Aceptar**.

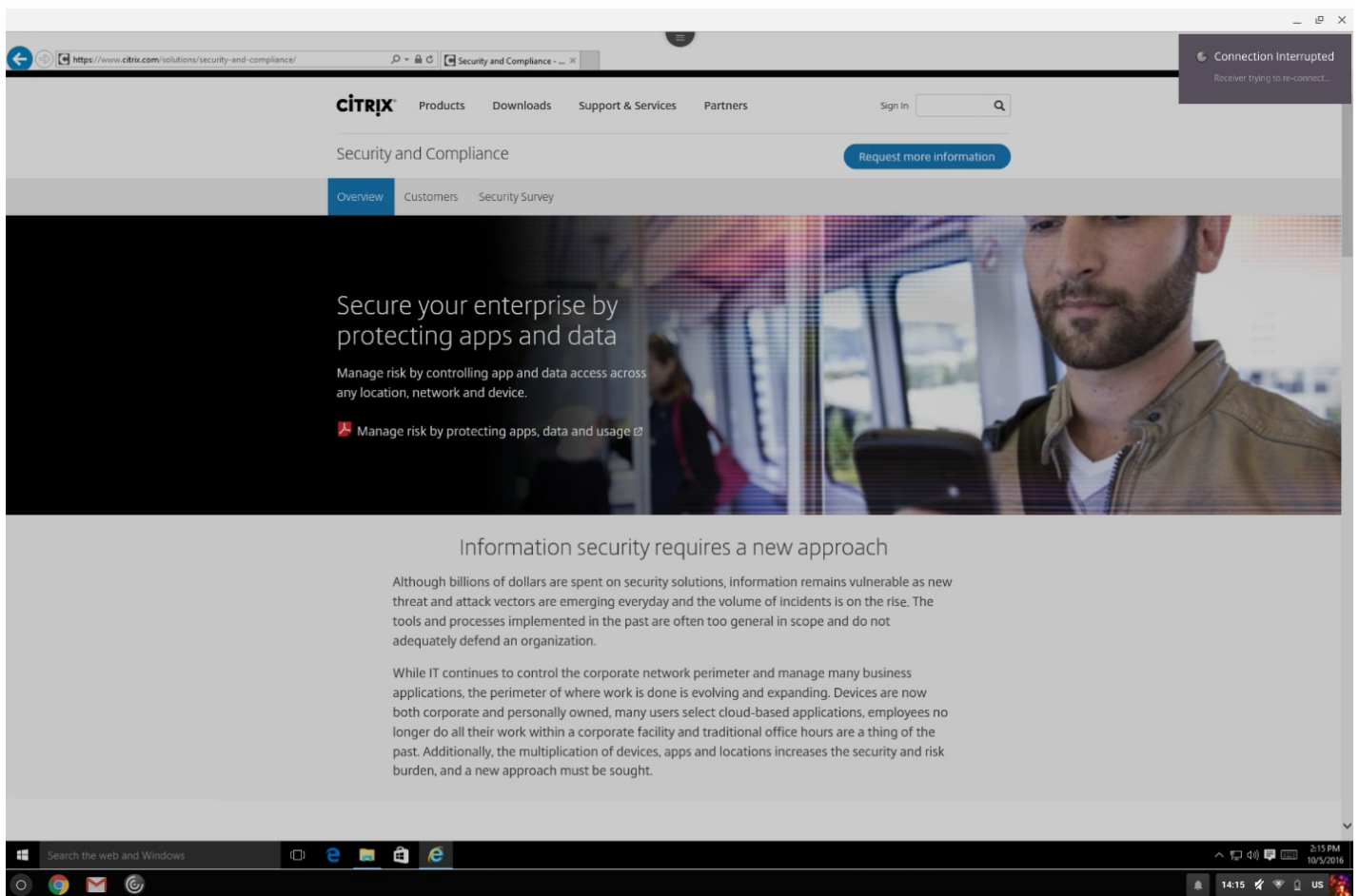
Para XenApp y XenDesktop 7.11 o versiones anteriores, use el archivo default.ica en StoreFront para modificar el tiempo de espera de la conexión de una sesión.

Parámetro	Ejemplo	Valor predeterminado
SessionReliabilityTTL	SessionReliabilityTTL=120	180

Cómo funciona la fiabilidad de la sesión

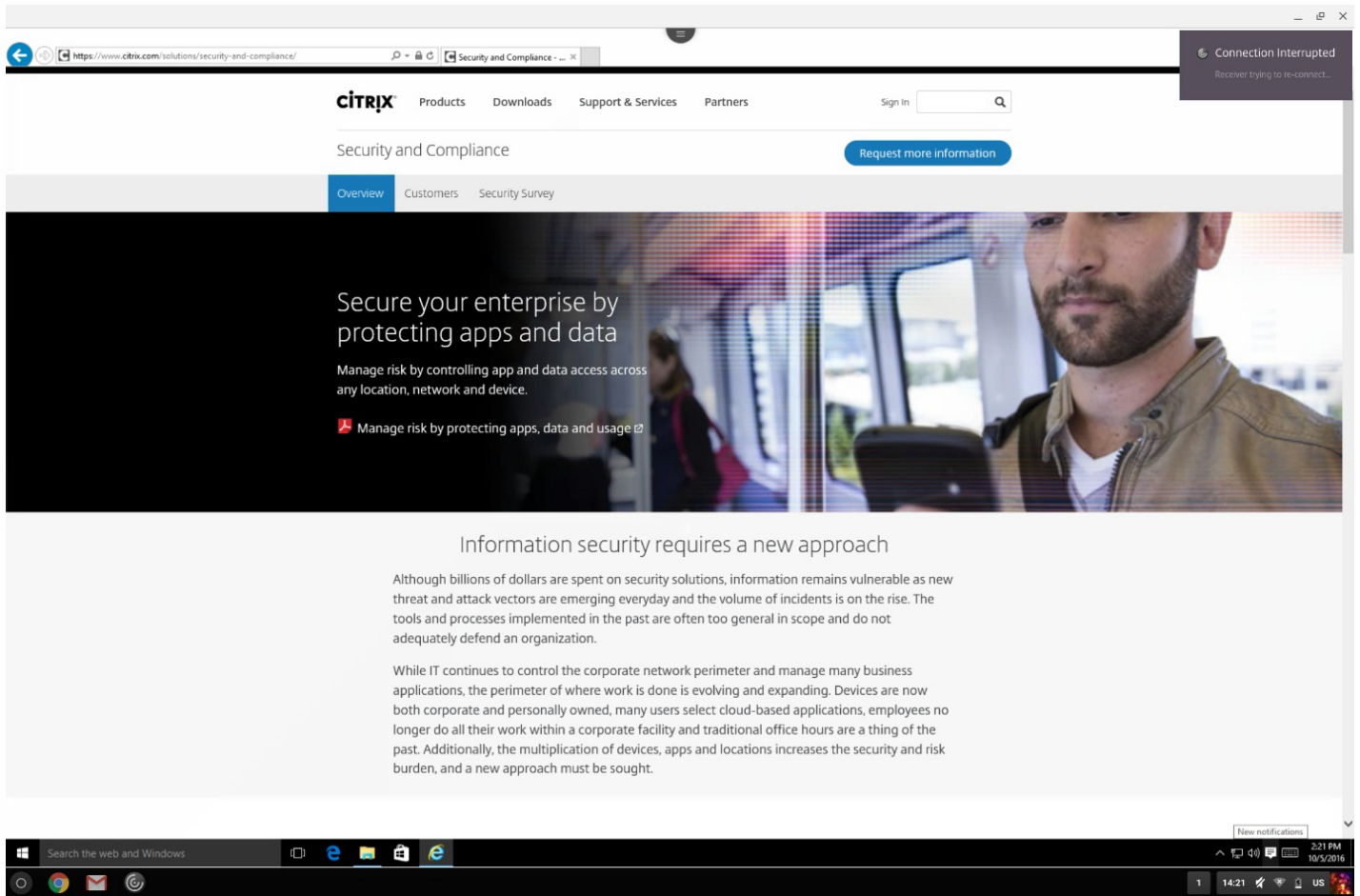
Cuando la fiabilidad de la sesión está habilitada, tenga en cuenta lo siguiente:

- La ventana de la sesión se oscurece mientras tiene lugar una reconexión. Cuando se supera el tiempo de espera, la sesión se desconecta.



Nota

Se puede modificar el brillo de la escala de grises utilizado para una sesión inactiva, usando Desktop Studio. De forma predeterminada, este valor está establecido en 80. El valor máximo es 100 (esto indica una ventana transparente) y el valor mínimo es 0 (esto indica una pantalla en negro).



Respaldo de portapapeles mejorado

Citrix Receiver para Chrome ahora da respaldo al formato HTML además de texto simple entre un cliente y el VDA en una sesión. Este respaldo es útil cuando se usan exploradores Web y aplicaciones de Microsoft Office. El respaldo mejorado para el portapapeles solo está disponible en exploradores Chrome y Safari.

Configuración del portapapeles

Puede copiar contenido HTML y conservar el formato cuando copia un enlace en Chrome. Se añade una etiqueta `<img>` en formato HTML, lo que permite copiar imágenes además de texto. Esta funcionalidad es más rica que el texto sin formato.

Para habilitar esta funcionalidad, agregue la siguiente entrada del Registro en el VDA:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\Virtual Clipboard\Additional Formats\HTML Format

"Name"="HTML Format"

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.

Nota

Para obtener información adicional sobre los problemas resueltos con la introducción de esta función, consulte los artículos de Knowledge Center ([CTX112063](#) y [CTX086028](#)).

Configuración de la redirección de dispositivos USB

Citrix Receiver para Chrome respalda una gama amplia de periféricos USB. Con esta funcionalidad adicional, un administrador puede crear una directiva de Google para identificar el PID/VID del dispositivo para habilitar su uso en Citrix Receiver. Este respaldo se extiende a nuevos dispositivos USB, incluido el mouse 3D Space, dispositivos compuestos adicionales y el teclado Bloomberg.

Para obtener más información sobre la configuración dispositivos USB, consulte el artículo de Knowledge Center [CTX200825](#).

Directivas de transferencia de archivos

Citrix Receiver para Chrome permite una transferencia de archivos segura entre el dispositivo del usuario y las sesiones virtuales de XenDesktop. Esta característica usa un canal virtual de transferencia de archivos en lugar de la asignación de unidades del cliente.

De manera predeterminada, los usuarios pueden:

- Cargar archivos desde una carpeta de descarga local o un periférico conectado
- Acceder de manera fluida a sus datos desde las sesiones de XenDesktop.
- Descargar archivos desde las sesiones de XenDesktop en una carpeta local o un periférico del dispositivo de usuario.

Los administradores pueden configurar la transferencia de archivos, y la carga o descarga de archivos, mediante directivas en Citrix Studio.

Requisitos previos

- XenApp o XenDesktop 7.6 o versiones posteriores, con:
 - Revisión hotfix ICATS760WX64022.msp en los VDA de SO de servidor (Windows 2008 R2 o Windows 2012 R2)
 - Revisión hotfix ICAWS760WX86022.msp o ICAWS760WX64022.msp en los VDA de SO de cliente (Windows 7 o Windows 8.1)
- Para cambiar las directivas de transferencia de archivos: Revisión hotfix de Administración de directivas de grupo (Group Policy Management) GPMx240WX64002.msi o GPMx240WX86002.msi en las máquinas que ejecutan Citrix Studio

Limitaciones

- Los usuarios pueden cargar o descargar un máximo de 10 archivos a la vez.
- Tamaño máximo del archivo:
 - Para cargas: 2147483647 bytes (2 GB)
 - Para descargas: 262144000 bytes (250 MB)
- Si alguna de estas directivas, 'Cargar archivos al escritorio' o 'Descargar archivos desde el escritorio', pero no ambas, están Inhabilitadas, la barra de herramientas siempre muestra los iconos Cargar y Descargar pero con la funcionalidad definida en la configuración de directiva. No obstante, si ambas directivas están configuradas como Inhabilitadas, los iconos de Cargar y Descargar no se muestran en la barra de herramientas.

Configuración de directivas de transferencia de archivos

Para configurar la transferencia de archivos usando una directiva de Citrix Studio

De forma predeterminada, la transferencia de archivos está habilitada.

Use Citrix Studio para cambiar estas directivas, ubicadas en Configuración de usuario > ICA > Redirección de archivos.

DIRECTIVA DE CITRIX STUDIO	Descripción:
Permitir transferencia de archivos entre escritorio y cliente.	Para habilitar o inhabilitar la función de transferencia de archivos
Cargar archivos al escritorio.	Para habilitar o inhabilitar la carga de archivos dentro de la sesión. Requiere que la directiva "Permitir transferencia de archivos entre escritorio y cliente" esté definida con el valor Verdadero (True).
Descargar archivos desde el escritorio.	Para habilitar o inhabilitar la descarga de archivos desde la sesión. Requiere que la directiva "Permitir transferencia de archivos entre escritorio y cliente" esté definida con el valor Verdadero (True).

Para configurar la transferencia de archivos usando el archivo configuration.js

El archivo configuration.js se encuentra en la carpeta raíz de ChromeApp. Edite este archivo directamente para hacer cambios en Citrix Receiver para Chrome.

Nota: Citrix recomienda hacer una copia de seguridad del archivo configuration.js antes de hacer cambios en él.

Nota: Se necesitan credenciales de nivel de administrador para editar el archivo configuration.js. Después de editarlo, vuelva a empaquetar la aplicación para hacer modificaciones adicionales en los elementos de la barra de herramientas.

Para ocultar la configuración de la barra de herramientas usando el archivo configuration.js:

1. Abra el archivo configuration.js y configure los parámetros como sigue:

PARÁMETROS DE CLIENTE DE TRANSFERENCIA DE ARCHIVOS	DESCRIPCIÓN
AllowUpload	Para habilitar o inhabilitar la carga de archivos desde el lado del cliente. De forma predeterminada tiene el valor "true".
AllowDownload	Para habilitar o inhabilitar la descarga de archivos desde el lado del cliente. De forma predeterminada tiene el valor "true".
MaxUploadSize	Para establecer el tamaño máximo de los archivos que pueden cargarse, en bytes. De manera predeterminada, está definido en 2147483648 bytes (2GB).
MaxDownloadSize	Para establecer el tamaño máximo de los archivos que pueden descargarse, en bytes. De manera predeterminada, está definido en 2147483648 bytes (2GB).

Los siguientes son casos de comportamiento cuando la directiva definida en Citrix Studio y la definida en el cliente son diferentes.

Directiva de Citrix Studio Carga / Descarga	Configuración en el cliente Carga / Descarga	Comportamiento resultante
INHABILITADO	HABILITADO	INHABILITADO
INHABILITADO	INHABILITADO	INHABILITADO
HABILITADO	INHABILITADO	INHABILITADO
HABILITADO	HABILITADO	HABILITADO

Nota

Cuando se produce un conflicto entre el valor definido para el **tamaño máximo del archivo para cargar o descargar** en el Registro y el valor definido en los parámetros del lado del cliente, se aplicará el valor que indique un tamaño menor.

Registros de transferencia de archivos:

Los registros de transferencia de archivos se pueden obtener desde el cliente y desde el servidor.

Para obtener registros de transferencia de archivos desde el cliente:

1. Abra un explorador Web.
2. Vaya a la siguiente dirección URL para iniciar el registro:
`<storefronturl>/clients/html5client/src/viewlog.html`
donde `<storefronturl>` es el FQDN o dirección IP del servidor StoreFront donde se configura el almacén.

Para obtener más información sobre la transferencia de archivos, consulte [Transferencia de archivos en Receiver para](#)

Requisitos del sistema

Feb 08, 2017

Requisitos del dispositivo del usuario

Todos los dispositivos deben cumplir los requisitos mínimos de hardware para el sistema operativo instalado.

Los dispositivos de los usuarios necesitan el sistema operativo Google Chrome (versión 50 o una más reciente) para acceder a los escritorios y las aplicaciones mediante Citrix Receiver para Chrome. Citrix recomienda utilizar Citrix Receiver para Chrome con las versiones del canal estable de Google Chrome. Citrix Receiver para Chrome solo está respaldado en Chrome OS.

Plataformas de servidor Citrix respaldadas

Citrix Receiver para Chrome respalda el acceso a escritorios y aplicaciones mediante las siguientes versiones de StoreFront. El acceso a los almacenes debe hacerse mediante sitios de Receiver para Web. Citrix Receiver para Chrome no respalda el acceso directo a almacenes de StoreFront, ya sea mediante la URL de la tienda o mediante la URL de los servicios XenApp.

- StoreFront 2.5 (o versiones posteriores)
- Interfaz Web 5.4

Citrix Receiver para Chrome se puede usar para acceder a escritorios y aplicaciones entregados por las siguientes versiones de producto:

- XenApp y XenDesktop 7.6 y versiones posteriores
- XenApp 6.5

Conexiones de usuario seguras

En un entorno de producción, Citrix recomienda proteger las comunicaciones entre los sitios de Receiver para Web y los dispositivos de los usuarios con NetScaler Gateway y HTTPS. Citrix recomienda usar certificados SSL con un tamaño de clave mínimo de 1024 bits en todo el entorno en el que se implementa Citrix Receiver para Chrome. Citrix Receiver para Chrome permite el acceso de los usuarios a escritorios y aplicaciones desde redes públicas con las siguientes versiones de NetScaler Gateway.

- NetScaler Gateway 10.5 y versiones posteriores

Citrix Receiver para Chrome permite a CloudBridge la inhabilitación de la compresión y compresión de impresora, así como el uso de análisis de HDX Insight para mostrarlos en CloudBridge Insight Center.

- CloudBridge 7.4 y versiones posteriores