Acerca de Citrix Receiver para Chrome 1.5

Nov 18, 2015

Citrix Receiver para Chrome permite a los usuarios acceder a los escritorios virtuales y a las aplicaciones alojadas desde dispositivos que ejecuten el sistema operativo Google Chrome. Los recursos entregados por XenDesktop y XenApp se combinan en un almacén de StoreFront o en la Interfaz Web y se ponen a disposición de los usuarios mediante un sitio de Receiver para Web o un sitio de Interfaz Web.

Los usuarios acceden al sitio a través de Receiver para Chrome, donde los escritorios y las aplicaciones se muestran en una única ventana.

Novedades en Receiver para Chrome

Receiver para Chrome presenta las siguientes novedades y mejoras:

- **Respaldo para portal Web personalizado de Interfaz Web**. Los usuarios pueden abrir archivos .ica en Citrix Receiver para iniciar sesiones de XenDesktop y XenApp. Los usuarios también pueden usar la URL de la Interfaz Web dentro de la aplicación de Citrix Receiver.
- **Conexión sólida con StoreFront**. Receiver para Chrome respalda el uso de balizas de StoreFront para determinar el estado de la conectividad de red.
- **Respaldo para HDX Insight**. Usted cuenta ahora con respaldo para NetScaler HDX Insight para el tráfico de Receiver para Chrome, que le permite supervisar aplicaciones iniciadas dentro de una sesión.
- **Respaldo para CloudBridge**. Receiver para Chrome ahora 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.
- **Configurar Citrix Receiver para Chrome por directiva de Google**. Puede usar directivas de Google para configurar la conexión a un almacén en Citrix Receiver para Chrome. La directiva de Google para esta configuración está disponible actualmente como función de Tech Preview de Google. Póngase en contacto con su representante de Google para obtener acceso a ella.

Nota: Para poder usar la versión de Citrix Receiver traducida a otro idioma, asegúrese de que el idioma del sistema operativo Chrome y el idioma preferido del explorador estén definidos en los parámetros de Chrome. Consulte información más detallada en https://support.google.com/chromebook/answer/1059490?hl=en y https://support.google.com/chromebook/answer/1059492?hl=en

Problemas conocidos

A continuación se presenta una lista de los problemas conocidos en esta versión. **Léala con atención antes de instalar el producto**.

- La sesión puede no iniciarse cuando se instala App Switcher por primera vez. Para corregir el problema, el administrador necesita reiniciar el host o VDA después de la instalación. [#525108]
- La movilidad entre sesiones puede no funcionar cuando Receiver para Chrome está configurado con Interfaz Web. [#524944]
- Es posible que los usuarios no puedan compartir sesiones si un mismo usuario inicia la aplicación y se origina desde el mismo host o VDA. [#521552]
- Los usuarios pueden tener problemas con la sincronización de audio y vídeo cuando reproducen vídeos que duran más de 5 minutos. [#524355]
- Las direcciones URL de balizas deben comenzar con "https://" o "http://"; de lo contrario, Receiver para Chrome no podrá

conectar el evento con la URL correcta. [#521288]

- Los usuarios pueden notar una demora hasta que aparece el mensaje “Receiving PDF File” después de hacer clic en Imprimir. [#518587]

Requisitos del sistema

Nov 18, 2015

En este tema, se enumeran las versiones de los productos de Citrix compatibles con Receiver para Chrome y los requisitos para que los usuarios puedan acceder a escritorios virtuales y a aplicaciones. Se considera que todos los equipos cumplen los requisitos mínimos de hardware para el sistema operativo instalado.

Requisitos del dispositivo del usuario

Los usuarios necesitan que los dispositivos con Google Chrome OS (versión 37 o una más reciente) puedan acceder a los escritorios y a las aplicaciones mediante Receiver para Chrome. Citrix recomienda utilizar Receiver para Chrome con las versiones del canal estable de Google Chrome. Receiver para Chrome solo está respaldado en Chrome OS.

Requisitos del servidor Citrix

Receiver para Chrome respalda el acceso a escritorios y a aplicaciones a través de las siguientes versiones de StoreFront. Los almacenes se deben acceder mediante los sitios de Receiver para Web. Receiver para Chrome no respalda el acceso directo a almacenes de StoreFront, ya sea mediante la URL del almacén o mediante la URL de los servicios XenApp.

- StoreFront 2.6
- StoreFront 2.5
- Interfaz Web 5.4

Cuando los usuarios se conectan a través de NetScaler Gateway, Receiver para Chrome se puede usar para acceder a escritorios y a aplicaciones entregados por cualquier versión de XenDesktop y XenApp respaldada por StoreFront. Para obtener más información, consulte los requisitos del sistema de StoreFront 2.6 o los requisitos del sistema de StoreFront 2.5 según corresponda.

Para las conexiones directas a través de StoreFront sin NetScaler Gateway, Receiver para Chrome se puede usar para acceder a escritorios y a aplicaciones entregados por las siguientes versiones de los productos.

- XenDesktop
  - XenDesktop 7.6
- XenApp
  - XenApp 7.6
  - XenApp 6.5
    El Hotfix Rollup Pack 3 (o una versión más reciente) y la actualización 1.7 de la Administración de directivas de grupo también deben estar instalados en el servidor 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 Receiver para Chrome. Receiver para Chrome permite el acceso de los usuarios a escritorios y a aplicaciones desde redes públicas con las siguientes versiones de NetScaler Gateway.

- NetScaler Gateway 10.5
- NetScaler Gateway 10.1

Receiver para Chrome ahora 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 7.3.1

Configuración

Nov 18, 2015

Para permitir que los usuarios de Receiver para Chrome puedan acceder a recursos alojados en XenDesktop y XenApp, debe crear un almacén de StoreFront. También debe habilitar las conexiones WebSocket en NetScaler Gateway, XenApp y XenDesktop, según considere necesario. Además, puede mejorar la experiencia de usuario mediante la instalación de componentes opcionales en las máquinas que proporcionan los escritorios y las aplicaciones.

Precaución: Si edita el Registro de forma incorrecta podrían generarse 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. Asegúrese de hacer una copia de seguridad del registro antes de modificarlo.

Para habilitar conexiones directas a XenDesktop y XenApp

Receiver para Chrome emplea el protocolo WebSocket para acceder a escritorios virtuales y a aplicaciones alojadas. De forma predeterminada, las conexiones WebSocket están prohibidas en XenDesktop y XenApp. Si quiere permitir que los usuarios accedan a escritorios y aplicaciones desde la red local sin que se conecten a través de NetScaler Gateway, debe permitir las conexiones WebSocket en XenDesktop y XenApp.

Las conexiones WebSocket también están inhabilitadas de forma predeterminada en NetScaler Gateway. Para los usuarios remotos que accedan a sus escritorios y aplicaciones a través de NetScaler Gateway, debe crear un perfil HTTP con conexiones WebSocket habilitadas y enlazarlo al servidor virtual de NetScaler Gateway o aplicar el perfil de forma global. Para obtener más información sobre la creación de perfiles HTTP, consulte Configuraciones HTTP.

Importante: Si utiliza SecureICA para cifrar las comunicaciones entre los dispositivos de los usuarios y los servidores XenDesktop o XenApp, tenga en cuenta que Receiver para Chrome admite únicamente el cifrado básico.

1. 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.
2. Establezca la configuración de directiva Conexiones de WebSockets en Permitida.
3. Si quiere cambiar el número de puerto que se utiliza para las conexiones WebSocket, modifique la configuración de directiva Número de puerto de WebSockets.
   Para las conexiones WebSockets, XenDesktop y XenApp utilizan de forma predeterminada el puerto 8008. Si decide usar un puerto diferente, por ejemplo, debido al firewall o a otras restricciones de red, también debe configurar el sitio de Receiver para Web para usar el puerto nuevo.
4. Para restringir el acceso de XenDesktop o XenApp a sitios de confianza específicos de Receiver para Web, especifique una lista separada por comas de las direcciones URL de los sitios de confianza para la configuración de directiva Lista de servidores de origen de WebSockets de confianza.
   Las conexiones de todos los sitios de Receiver para Web se aceptan de forma predeterminada.
5. Compruebe, en cada máquina que proporcione escritorios y aplicaciones a los usuarios de Receiver para Chrome, que ningún firewall bloquee las conexiones TCP entrantes al puerto que ha configurado para las conexiones WebSocket, que no haya ninguna otra aplicación usando el puerto y que el tráfico dirigido al puerto no se redirija a otros puertos.
6. Si ejecuta XenDesktop, compruebe que en todas las máquinas que proporcionan escritorios para los usuarios de Receiver para Chrome se han aplicado las actualizaciones y revisiones hotfix más recientes disponibles de Virtual Delivery Agent.

7. Si quiere crear máquinas mediante Machine Creation Services (MCS), cree, en la imagen maestra, una entrada de Registro en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies si no está ya presente y, a continuación, agregue las siguientes claves de Registro.
   - Cree una clave de Registro con un tipo de valor REG_DWORD en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies\AcceptWebSocketsConnections. Establezca el valor de la clave nueva en 1.
   - Cree una clave de Registro con un tipo de valor REG_DWORD en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies\WebSocketsPort. Establezca el valor de la clave nueva para el puerto que ha elegido para las conexiones WebSocket en la directiva de XenDesktop o XenApp. El puerto predeterminado es 8008.
   - Cree una clave de Registro con un tipo de valor REG_SZ en HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies\WSTrustedOriginServerList. Para el valor de la clave nueva, especifique una lista separada por comas de las direcciones URL de los sitios de confianza de Receiver para Web o establezca el valor en * para aceptar conexiones de todos los sitios de Receiver para Web.

   No aplique las directivas WebSocket de XenDesktop o XenApp a las máquinas aprovisionadas mediante esta imagen maestra. Puede comprobar si se aplican las directivas WebSocket en la VM de la imagen maestra con la herramienta rsop.msc o mediante el comando gpresult desde el símbolo del sistema.

   Esta solución no sirve con implementaciones entregadas y administradas con App Orchestration.

8. Si quiere implementar máquinas aprovisionadas (no persistentes) mediante Provisioning Services, cree el catálogo de máquinas y el grupo de entrega para los que quiere habilitar las conexiones de Receiver para Chrome. Compruebe que las directivas WebSocket que ha configurado se aplican al catálogo de máquinas.
   Las máquinas deben reiniciarse para aplicar las directivas WebSocket. Para las máquinas basadas en Provisioning Services que han sido configuradas para usar archivos caché de escritura persistentes y para las máquinas implementadas mediante MCS (las cuales tienen discos de identidad independientes), las directivas se conservan cuando las máquinas se reinician. No obstante, para los catálogos de máquinas basadas en Provisioning Services que han sido configuradas para usar archivos caché de escritura temporales, estas directivas deben aplicarse al disco virtual o no se implementarán correctamente en los dispositivos de destino.

   Complete los siguientes pasos para comprobar que las directivas se aplican correctamente al disco virtual.

   1. Mediante Provisioning Services Console, apague un dispositivo de destino que forme parte del catálogo de máquinas y del grupo de entrega. Cambie el tipo de acceso del dispositivo de destino de Production a Maintenance.
      Para obtener más información, consulte Administración de dispositivos de destino. Debe usar un dispositivo de destino que forme parte del catálogo de máquinas y del grupo de entrega o las directivas no se aplicarán.

   2. Cree una versión nueva del disco virtual y establezca Access en Maintenance.
      Para obtener más información, consulte Actualización manual de una imagen de disco virtual.

   3. Inicie el dispositivo de mantenimiento de destino; para ello, seleccione la versión del disco virtual de mantenimiento desde el menú de arranque. Compruebe que las siguientes claves se han agregado al Registro.
      HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICAPoliciesAcceptWebSocketsConnections

      HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\WebSocketsPort

      HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\WSTrustedOriginServerList

   4. Apague el dispositivo de destino, cambie el acceso al dispositivo de destino de nuevo a Production y establezca la versión nueva del disco virtual en producción. A continuación, inicie el dispositivo de destino y reinicie los demás

dispositivos de destino que se estén ejecutando en el disco virtual existente.
Si no utiliza el control de versiones de discos virtuales, puede aplicar las directivas a la imagen del disco virtual base si apaga todos los dispositivos de destino que utilicen dicho disco virtual, lo coloca en modo de imagen privada (Private Image) y, a continuación, inicia el dispositivo de destino para actualizar la imagen.

Para configurar componentes opcionales

Hay dos componentes opcionales disponibles que permiten mejorar la experiencia de los usuarios de Receiver para Chrome con una mayor integración entre XenDesktop, XenApp y Chrome OS.

- App Switcher permite a los usuarios cambiar de una aplicación a otra si estas están activas en la misma sesión. Cuando se habilita el uso compartido de sesiones en XenApp, lo cual se hace de forma predeterminada, las aplicaciones abiertas en la misma sesión aparecen en la misma ventana. App Switcher proporciona una barra de tareas en la sesión que muestra todas las aplicaciones activas de esta, lo que permite a los usuarios cambiar de una aplicación a otra.
- El controlador Citrix PDF Universal Printer permite a los usuarios imprimir documentos abiertos con aplicaciones alojadas o aplicaciones activas 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. Así, el PDF se abre en una ventana nueva para verlo e imprimirlo desde Google Cloud Print.

1. Si quiere habilitar el uso compartido de sesiones en el entorno de XenApp, descargue el instalador de App Switcher. Compruebe que .NET Framework 4.5 está instalado y habilitado y, a continuación, instale App Switcher en cada máquina que proporcione aplicaciones a los usuarios de Receiver para Chrome.
   App Switcher está configurado para ejecutarse automáticamente en segundo plano cuando los usuarios establecen una sesión.

2. Si quiere permitir que los usuarios impriman documentos abiertos con aplicaciones alojadas o aplicaciones activas en escritorios virtuales entregados por XenDesktop 7.6 y XenApp 7.6, complete los siguientes pasos.
   1. Descargue el Citrix PDF Printing Feature Pack e instale el controlador Citrix PDF Universal Printer en cada máquina que proporcione escritorios y aplicaciones a los 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 en Habilitada.

Implementación

Nov 18, 2015

Existen diversas opciones para implementar 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, consulte CTX141844.
- Puede reempaquetar 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 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 Receiver para Chrome. Como la aplicación está preconfigurada, los usuarios pueden comenzar a trabajar con 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 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 deben buscar Citrix Receiver y hacer clic en Añadir a Chrome para instalar Receiver para Chrome desde Chrome Web Store.
  Una vez instalado, Receiver para Chrome debe configurarse con los datos de conexión de NetScaler Gateway y del sitio de 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 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 Exportación de archivos de aprovisionamiento de almacenes para los usuarios.
  - Puede proporcionar a los usuarios la URL que deben escribir la primera vez que inicien Receiver para Chrome.

Para volver a empaquetar Receiver para Chrome

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

1. Descargue la versión sin empaquetar de Receiver para Chrome a una ubicación adecuada.
2. Descargue el archivo de configuración de ejemplo y modifíquelo para que se adecúe al entorno.
3. Cambie el nombre del archivo de configuración modificado a default.cr y cópielo en el directorio raíz de Receiver para Chrome.
   Los archivos de configuración con nombres distintos o situados en otras ubicaciones no se incluirán cuando 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.
   1. Utilice un editor de texto para abrir el archivo configuration.js en el directorio raíz de 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 Receiver para Web.

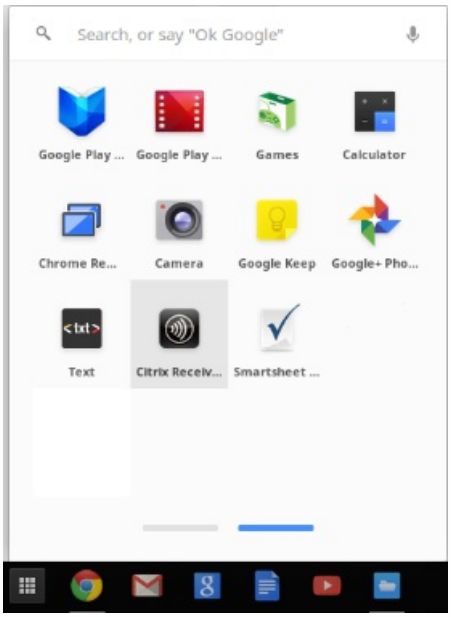
5. En Chrome, entre en chrome://extensions, marque la casilla Modo de desarrollador de la esquina superior derecha de la página y, a continuación, haga clic en el botón Empaquetar extensión.
   Por motivos de seguridad, StoreFront solo acepta conexiones de instancias conocidas de Receiver para Chrome. Debe poner en lista blanca la aplicación reempaquetada para que los usuarios puedan conectarse a un sitio de Receiver para Web.

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

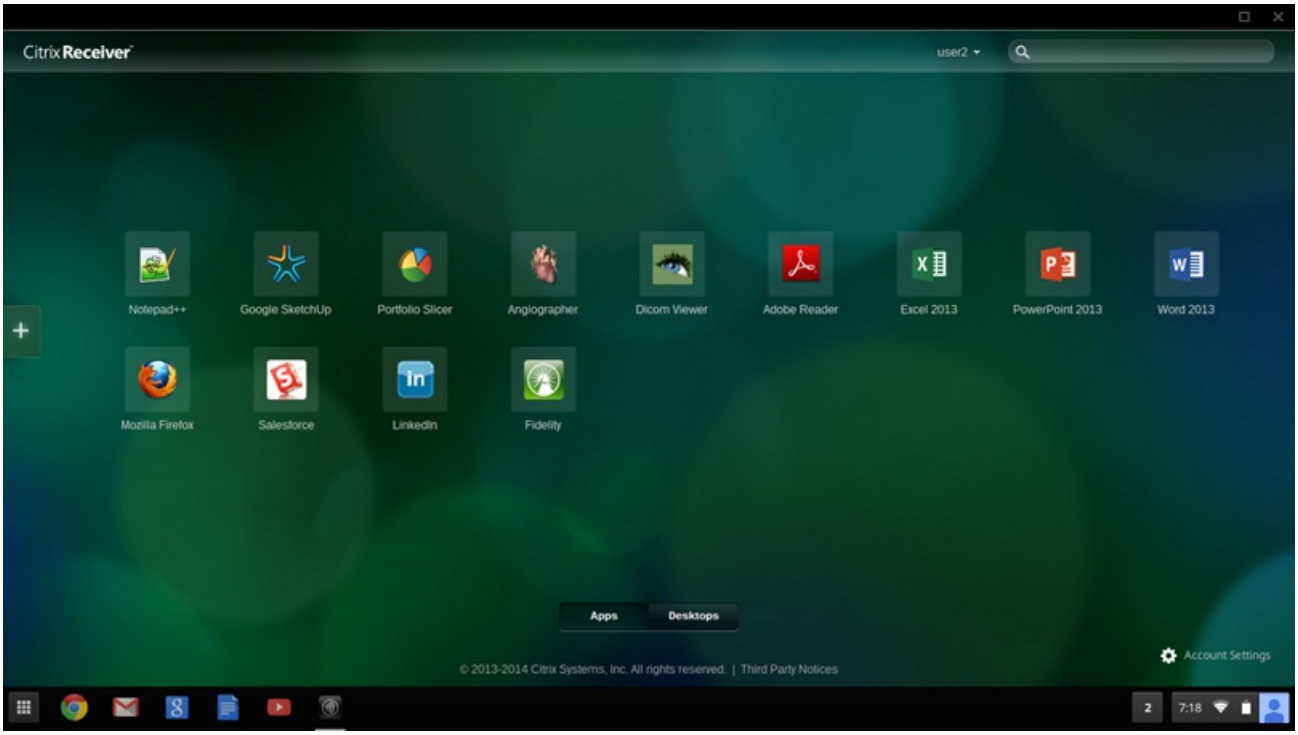
Experiencia de usuario

Nov 18, 2015

Después de instalar y configurar 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 Receiver para Chrome de los dispositivos, los usuarios deben hacer clic con el botón secundario en el icono de Citrix Receiver de la lista de aplicaciones de Chrome y seleccionar Desinstalar.



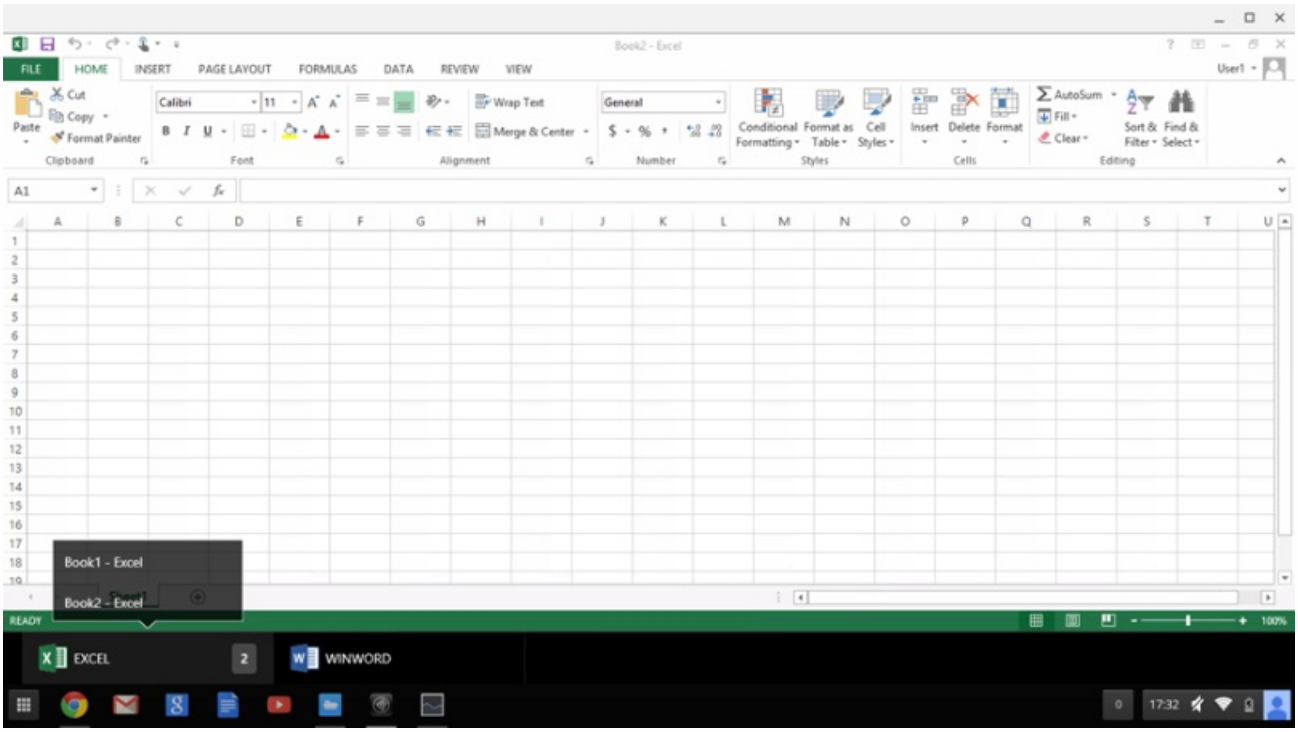
Una vez que han iniciado una sesión, aparecen los escritorios y las aplicaciones de los usuarios, como se muestra en esta imagen. Estos pueden buscar recursos y hacer clic en cualquier icono para iniciar un escritorio o una aplicación en una ventana nueva.



Cuando un usuario inicia una aplicación adicional, Receiver para Chrome comprueba si esta 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.

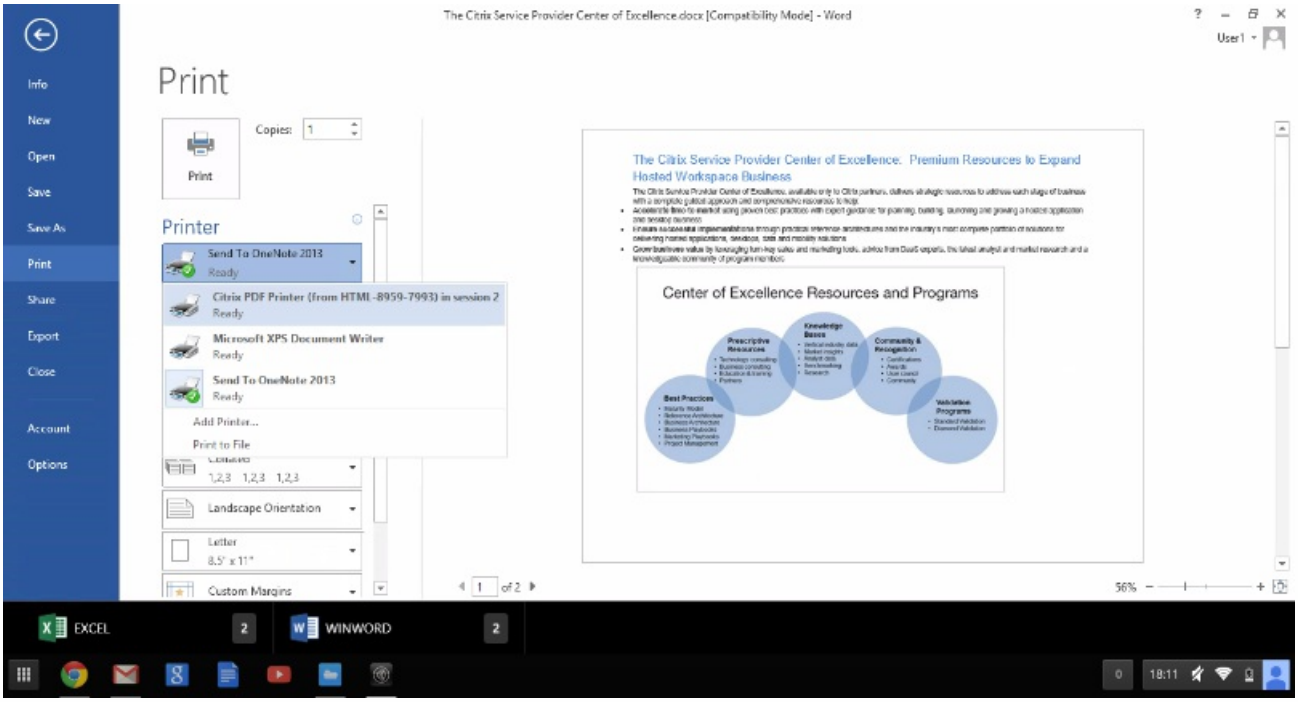
Las aplicaciones que se ejecuten en la misma sesión aparecen en la misma ventana. Si App Switcher está instalado en la máquina que proporciona las aplicaciones, aparece una barra de tareas en la parte inferior de la ventana, como se muestra en esta imagen. La barra de tareas muestra todas las aplicaciones activas de la sesión, lo que permite a los usuarios cambiar de una aplicación a otra. Los usuarios pueden configurar esta barra de tareas para que se oculte automáticamente y para cambiar a iconos pequeños y, así, reducir el espacio que ocupa la barra.



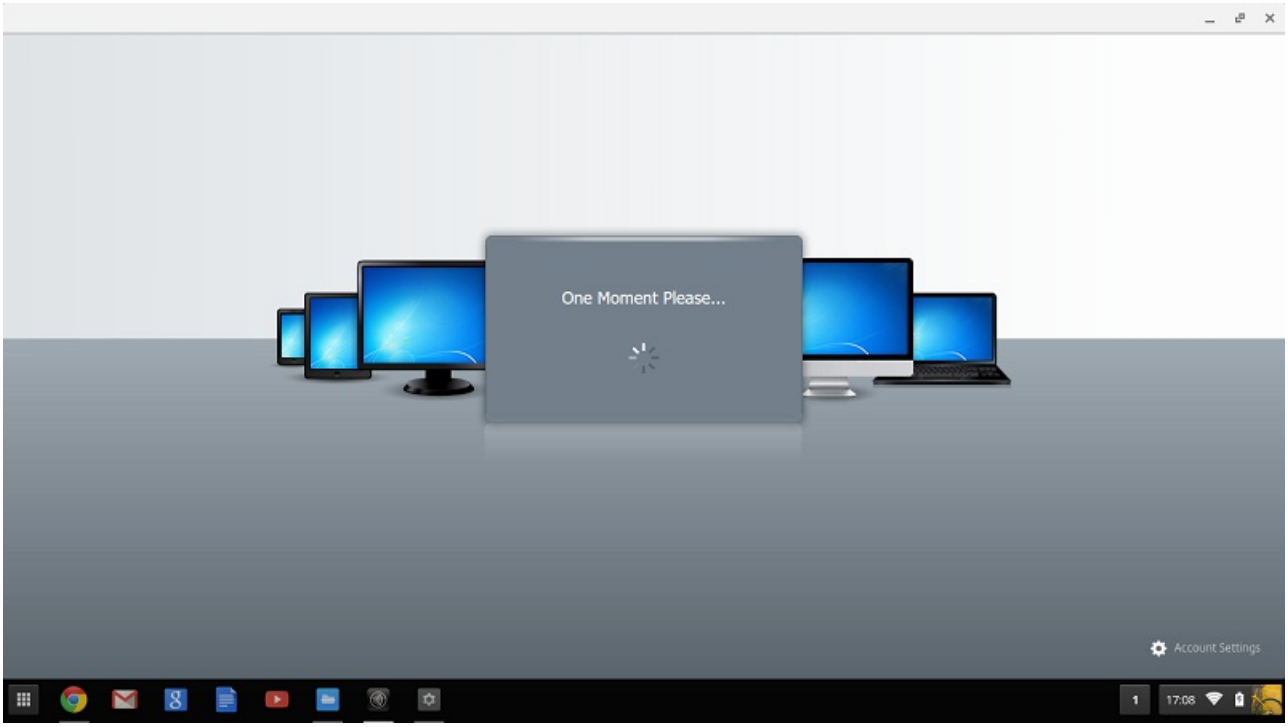
Los usuarios pueden utilizar accesos directos estándar de Windows para copiar datos, incluidos texto, tablas e imágenes, de una aplicación alojada a otra, ya sea dentro de la misma sesión o entre distintas sesiones. Solo se puede copiar y pegar texto Unicode sin formato entre las aplicaciones alojadas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

Los usuarios pueden utilizar cualquier acceso directo estándar de teclado de Windows en 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 Receiver para Chrome.

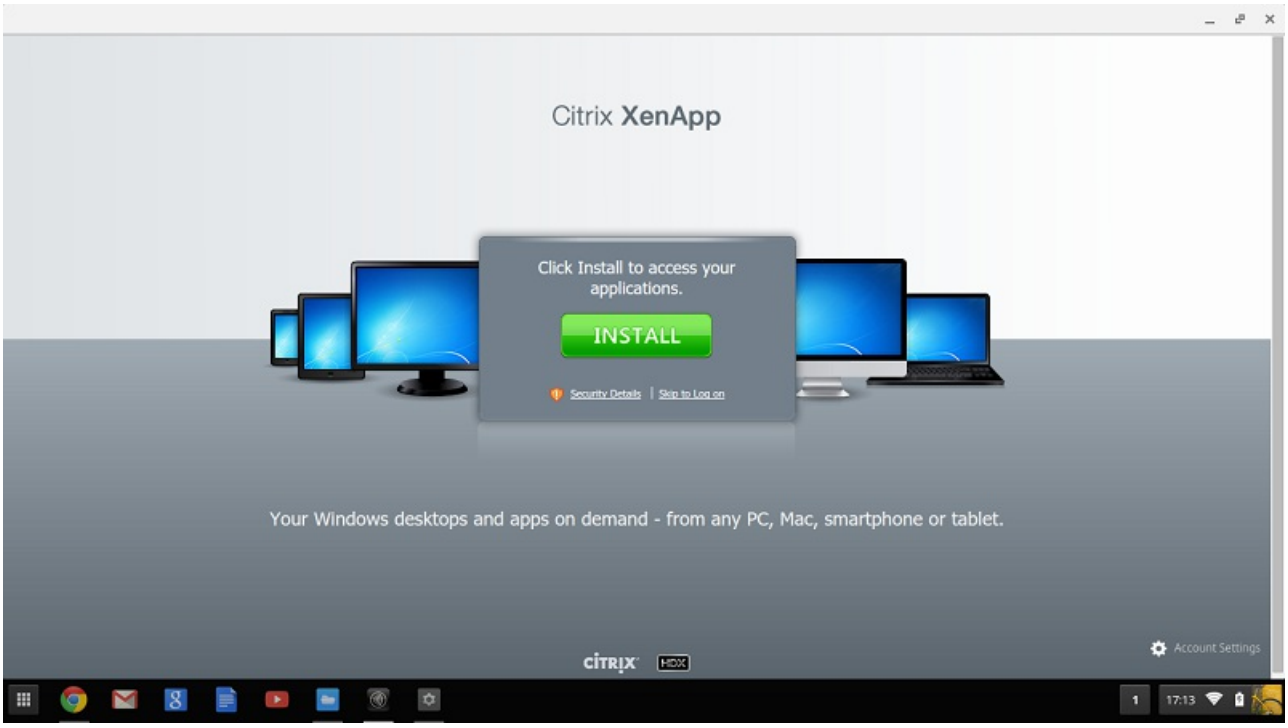
Al imprimir un documento abierto con una aplicación alojada o una aplicación activa en un escritorio virtual, el usuario tendrá la opción de imprimir el documento en PDF, como se muestra en esta imagen. Así, el PDF se transfiere al dispositivo local para verlo e imprimirlo desde una impresora conectada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



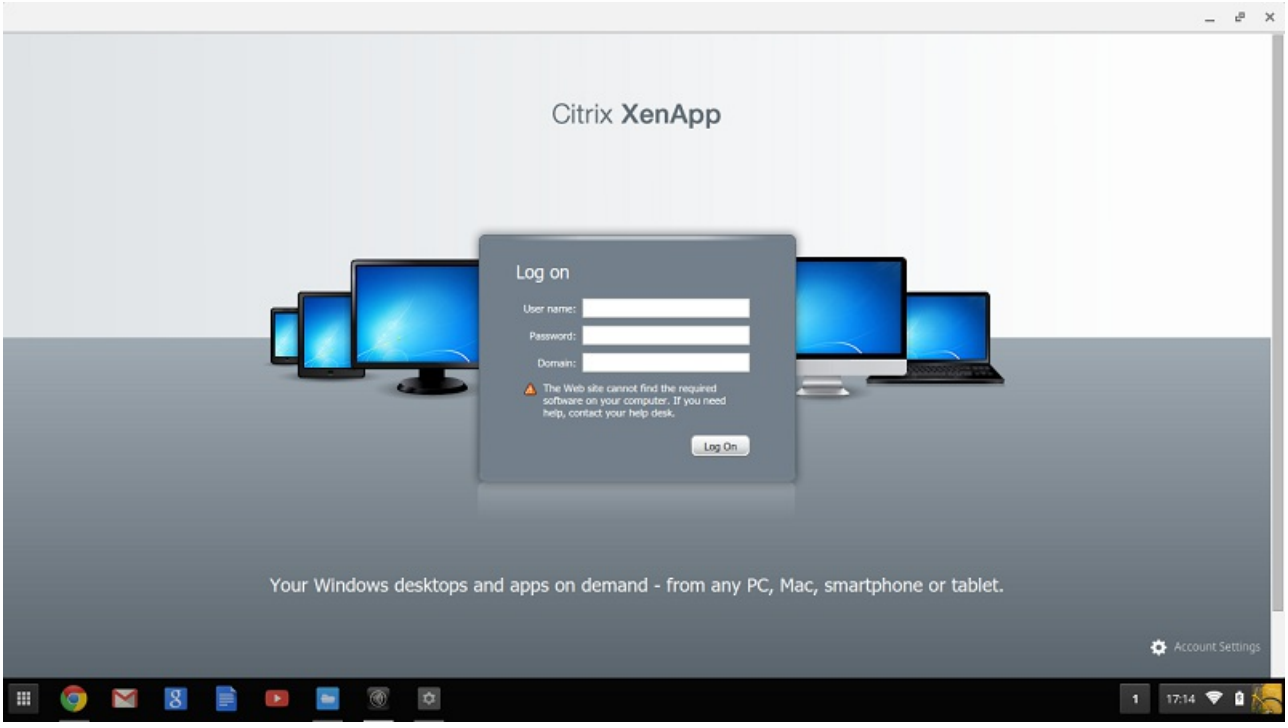
Ahora los usuarios pueden conectarse a la Interfaz Web y abrir aplicaciones y escritorios alojados. Necesitan configurar Receiver para Chrome para indicar la dirección URL de la Interfaz Web; por ejemplo: http://interfazWeb.suDominio.com/Citrix/



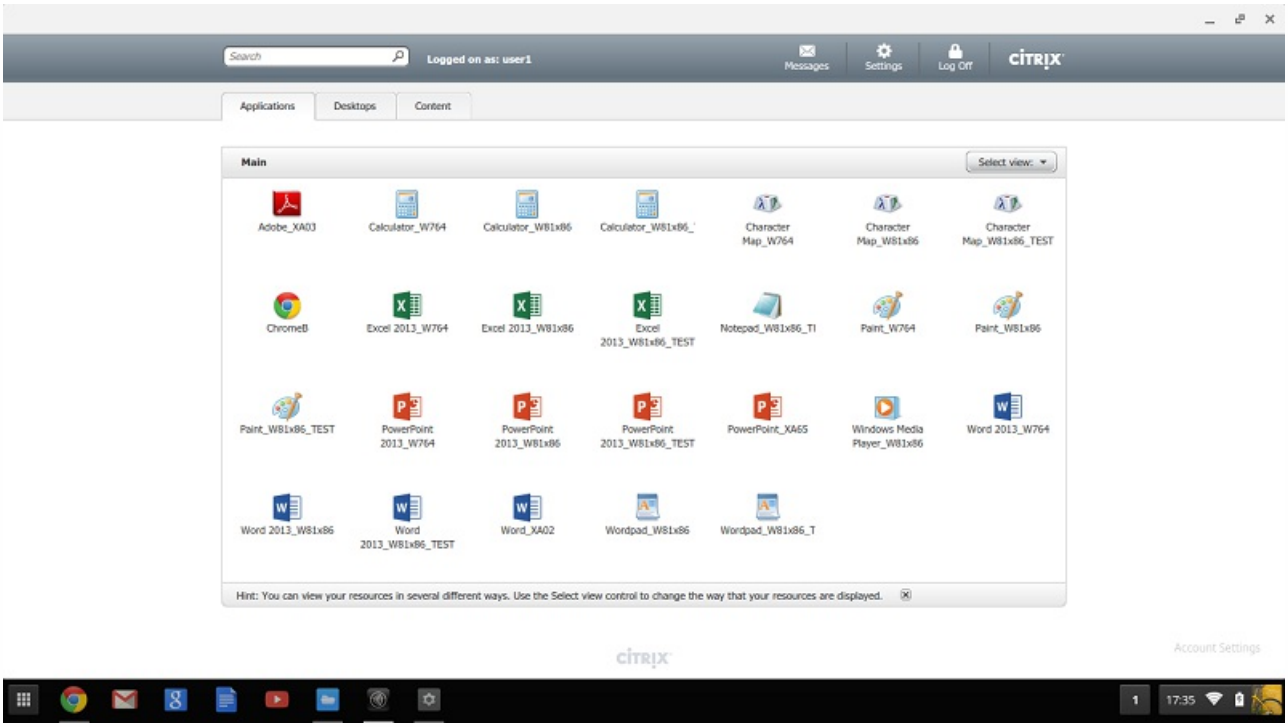
Los usuarios deben hacer clic en Omitir para iniciar sesión.



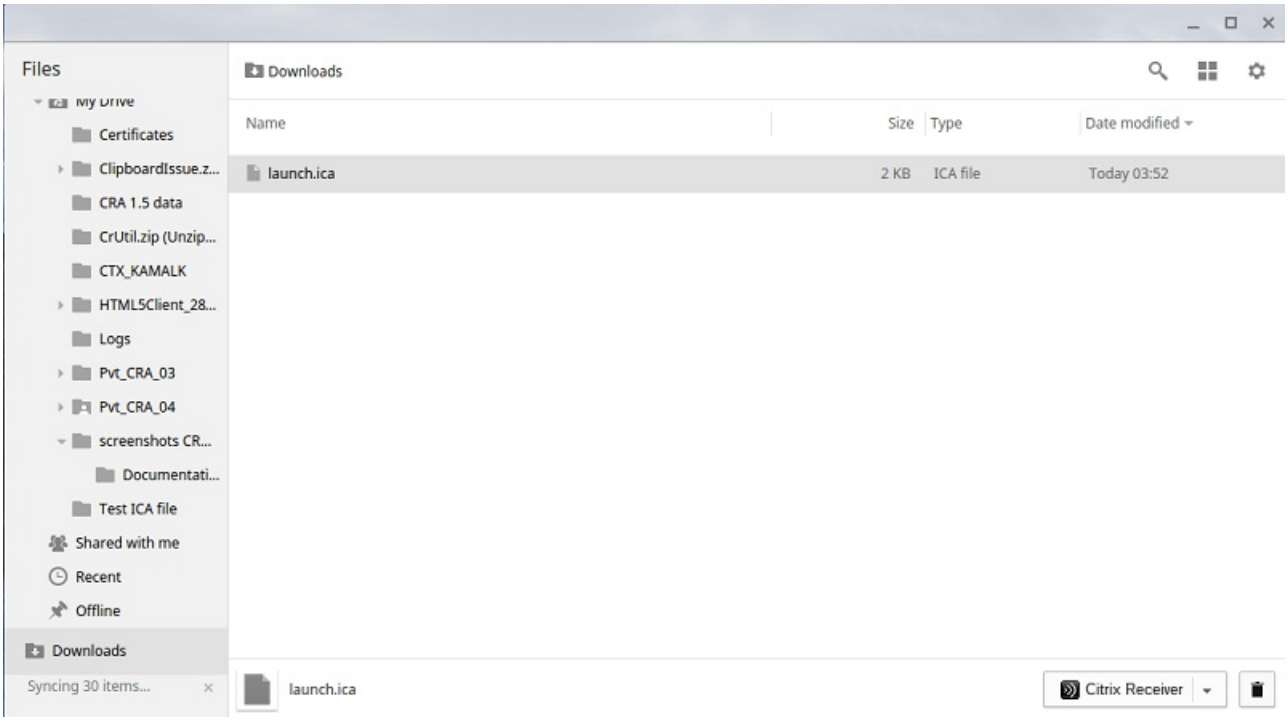
Nota: Para la pantalla anterior, siga las instrucciones indicadas en Interfaz Web 5.4.



Después de que los usuarios inician la sesión, aparecen sus escritorios y aplicaciones.



Los escritorios pueden abrir aplicaciones y escritorios alojados abriendo un archivo .ica con Receiver para Chrome.



Para habilitar los registros en 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.

1. Para capturar los registros de un dispositivo de usuario, lleve a cabo los siguientes pasos.
    1. En el dispositivo de usuario, haga clic en Parámetros de cuenta, en la esquina inferior derecha de la página de inicio de sesión de Receiver para Chrome.

2. En el cuadro de diálogo Parámetros, haga clic en Iniciar registro.
   A continuación, 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.

2. Para habilitar los registros de App Switcher en las máquinas que proporcionan aplicaciones a los usuarios, complete los siguientes pasos.
   1. Utilice un editor de texto para abrir el archivo AppSwitcher.exe.config, que generalmente se encuentra en el directorio C:\Archivos de programa (x86)\Citrix\App Switcher.
   2. Localice la siguiente sección en el archivo.
      False
   3. Cambie el contenido del elemento a True para habilitar los registros de App Switcher.
      Los archivos de registros de App Switcher se guardan en el directorio \AppData\Citrix\AppSwitcher\Logs. El directorio \AppData está oculto de forma predeterminada.