

About Citrix Receiver for Chrome 1.4

Oct 09, 2015

Citrix Receiver for Chrome enables users to access virtual desktops and hosted applications from devices running the Google Chrome operating system. Resources delivered by XenDesktop and XenApp are aggregated in a StoreFront store and made available through a Receiver for Web site. Users access the site through Receiver for Chrome and their desktops and applications are displayed in a single window.

What's new

This release provides the following new features and enhancements.

Print to PDF. Users can convert documents opened with hosted applications or applications running on virtual desktops to PDF. The PDF is then transferred to the local device for viewing and printing from a locally attached printer or Google Cloud Print.

Clipboard operations. Users can copy and paste different types of data, including text, tables, and images, between hosted applications, both within the same session and between different sessions. Only plain text can be copied and pasted between hosted applications and files or applications running on the local device.

Enhanced session sharing. To make more efficient use of server resources, Receiver for Chrome checks whether a hosted application can be started within an existing session before creating a new session. Since applications running in the same session all appear in a single window, the optional App Switcher component can be deployed to provide a taskbar that enables users to switch between their applications.

Secure WebSocket connections. Receiver for Chrome supports secure WebSocket connections over Secure Sockets Layer (SSL) for direct connections to XenDesktop and XenApp without NetScaler Gateway.

Customize Receiver for Chrome. You can preconfigure Receiver for Chrome by repackaging it with a custom Citrix Receiver configuration (.cr) file. By editing the manifest file, you can also customize Receiver for Chrome, such as changing the application name, for example. You can publish the repackaged application for users through Google Apps for Business using the Google Admin Console.

End-user experience metrics. Receiver for Chrome collects and makes available various metrics on user sessions to enable you to monitor the user experience through Director.

Receiver unique ID per device. Receiver for Chrome generates a unique client name the first time a session is started and uses this name for all subsequent sessions, enabling you to track license usage for hosted applications.

Known issues

The following is a list of known issues in this release. **Read it carefully before installing the product.**

Text formatting lost when copying between different applications across sessions

Due to an issue with Windows applications, copying text between different applications, such as Word and Excel, running in separate sessions results in all formatting being lost. However this issue does not occur when copying within a session or when copying between separate instances of the same application running in different sessions. [#486356]

Receiver for Chrome and applications can become unresponsive when copying large amounts of data

Attempting to copy and paste more than 9 MB of data between sessions can cause both Receiver for Chrome and the application to which the data is pasted to become unresponsive. [#486290]

Some location-based time zones cannot be mapped

When you set the Use local time of client policy to Use client time zone in Studio, users accessing virtual desktops in time zones different from that of the desktop might not see the same time zone location and instead see the default time zone for the UTC offset. [#460538]

System requirements

Nov 17, 2014

This topic lists the supported Citrix product versions for Receiver for Chrome and the requirements for users to access virtual desktops and applications. It is assumed that all computers meet the minimum hardware requirements for the installed operating system.

User device requirements

Users require devices running the Google Chrome operating system (version 37 or later) to access desktops and applications using Receiver for Chrome. Citrix recommends that you use Receiver for Chrome with releases from the stable channel of Google Chrome. Receiver for Chrome is only supported on Chrome OS.

Citrix server requirements

Receiver for Chrome supports access to desktops and applications through the following versions of StoreFront. Stores must be accessed through Receiver for Web sites. Receiver for Chrome does not support direct access to StoreFront stores, either using the store URL or the XenApp Services URL.

- StoreFront 2.6
- StoreFront 2.5

When users connect through NetScaler Gateway, Receiver for Chrome can be used to access desktops and applications delivered by all the versions of XenDesktop and XenApp that are supported by StoreFront. For details, see the [StoreFront 2.6 system requirements](#) or the [StoreFront 2.5 system requirements](#), as appropriate.

For direct connections through StoreFront without NetScaler Gateway, Receiver for Chrome can be used to access desktops and applications delivered by the following product versions.

- XenDesktop
 - XenDesktop 7.6
- XenApp
 - XenApp 7.6
 - XenApp 6.5
 - Hotfix Rollup Pack 3 or later and the Group Policy Management 1.7 update must also be installed on the XenApp 6.5 server.

Secure user connections

In a production environment, Citrix recommends securing communications between Receiver for Web sites and users' devices with NetScaler Gateway and HTTPS. Citrix recommends using SSL certificates with a key size of at least 1024 bits throughout the environment in which Receiver for Chrome is deployed. Receiver for Chrome enables user access to desktops and applications from public networks with the following versions of NetScaler Gateway.

- NetScaler Gateway 10.5
- NetScaler Gateway 10.1

Note: Secure ICA does not work through Receiver for HTML5 specifically. Configuring encryption of applications within XenApp 6.5 will not allow the use of these Receiver version types since only SSL to Netscaler or secure WebSockets are supported.

Configure

Aug 03, 2015

To enable Receiver for Chrome users to access resources hosted on XenDesktop and XenApp, you must create a StoreFront store. You must also enable WebSocket connections on NetScaler Gateway, XenApp, and XenDesktop, as required. Additionally, you can enhance the user experience by installing optional components on the machines providing the desktops and applications.

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

To enable direct connections to XenDesktop and XenApp

Receiver for Chrome uses the WebSocket protocol to access virtual desktops and hosted applications. By default, WebSocket connections are prohibited on XenDesktop and XenApp. If you plan to enable users to access desktops and applications from the local network without connecting through NetScaler Gateway, WebSocket connections must be allowed on XenDesktop and XenApp.

WebSocket connections are also disabled by default on NetScaler Gateway. For remote users accessing their desktops and applications through NetScaler Gateway, you must create an HTTP profile with WebSocket connections enabled and either bind this to the NetScaler Gateway virtual server or apply the profile globally. For more information about creating HTTP profiles, see [HTTP Configurations](#).

Important: If you are using SecureICA to encrypt communications between users' devices and your XenDesktop or XenApp servers, note that Receiver for Chrome supports Basic encryption only.

1. In Citrix Studio, select the Policy node in the left pane and either create a new policy or edit an existing policy.
For more information about configuring XenDesktop and XenApp policies, see [Citrix policies](#).
2. Set the WebSockets connections policy setting to Allowed.
3. If you want to change the port used for WebSocket connections, edit the WebSockets port number policy setting.
By default, XenDesktop and XenApp use port 8008 for WebSocket connections. If you decide to use a different port, due to firewall or other network restrictions, for example, you must also configure the Receiver for Web site to use the new port.
4. To restrict access to XenDesktop or XenApp to specific trusted Receiver for Web sites, specify a comma-separated list of trusted site URLs for the WebSockets trusted origin server list policy setting.
By default, connections from all Receiver for Web sites are accepted.
5. On each machine providing desktops and applications for Receiver for Chrome users, verify that incoming TCP connections to the port you configured for WebSocket connections are not blocked by firewalls, that no other applications are using the port, and that traffic to the port is not being redirected to other ports.
6. If you are running XenDesktop, ensure that you have updated each machine providing desktops for Receiver for Chrome users with the latest available Virtual Delivery Agent updates and hotfixes.
7. If you plan to create machines using Machine Creation Services (MCS), on the master image, create a registry entry at HKEY_LOCAL_MACHINESOFTWARE\CitrixGroupPolicyDefaults\ICAPolicies if it is not already present and then add the following registry keys.
 - Create a registry key with a value type of REG_DWORD at HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies\AcceptWebSocketsConnections. Set

the value of the new key to 1.

- Create a registry key with a value type of REG_DWORD at HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies\WebSocketsPort. Set the value of the new key to the port you chose for WebSocket connections in the XenDesktop or XenApp policy. The default port is 8008.
- Create a registry key with a value type of REG_SZ at HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies\WSTrustedOriginServerList. For the value of the new key, either specify a comma-separated list of trusted Receiver for Web site URLs or set the value to * to accept connections from all Receiver for Web sites.

Do not apply the XenDesktop or XenApp WebSocket policies to machines provisioned using this master image. You can check whether the WebSocket policies are applied on the master image VM using the rsop.msc tool or by running the gpreresult command from a command prompt.

This workaround cannot be used with deployments delivered and managed with App Orchestration.

8. If you plan to deploy provisioned (non-persistent) machines using Provisioning Services, create the machine catalog and delivery group for which you want to enable Receiver for Chrome connections. Ensure that the WebSocket policies you configured apply to your machine catalog.

Machines must be restarted to apply the WebSocket policies. For Provisioning Services-based machines configured to use persistent write cache files and machines deployed using MCS (which have separate identity disks), the policies are persisted when the machines restart. However, for Provisioning Services-based machine catalogs configured to use temporary write cache files, these policies must be applied to the vDisk or they will not be implemented successfully on target devices.

Complete the following steps to ensure that the policies are correctly applied to the vDisk.

1. Using the Provisioning Services console, shut down a target device that is part of the machine catalog and delivery group. Change the access type of the target device from Production to Maintenance.
For details, see [Managing Target Devices](#). You must use a target device that is part of the machine catalog and delivery group or the policies will not be applied.
2. Create a new version of your vDisk and leave it with Access set to Maintenance.
For details, see [Manually Updating a vDisk Image](#).
3. Start the maintenance target device, selecting the maintenance vDisk version from the boot menu. Verify that the following keys are added to the registry.
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICAPoliciesAcceptWebSocketsConnections

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\WebSocketsPort

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\WSTrustedOriginServerList
4. Shut down the target device, change the target device access type back to Production, and promote the new vDisk version to production. Then, start the target device and restart any other target devices currently running from the existing vDisk.
If you do not use vDisk versioning, you can apply the policies to your base vDisk image by shutting down all the target devices that use the vDisk, placing the vDisk in Private Image mode, and then starting the target device to update the image.

To configure optional components

Two optional components are available that enhance the experience for Receiver for Chrome users by increasing integration between XenDesktop, XenApp, and Chrome OS.

- App Switcher enables users to switch between multiple applications running in the same session. When session sharing is enabled on XenApp, which it is by default, applications opened within the same session appear in the same window. App Switcher provides a taskbar running within the session that displays all the applications currently running in the session, enabling users to switch between them.
 - The Citrix PDF Universal Printer driver enables users to print documents opened with hosted applications or applications running on virtual desktops delivered by XenDesktop 7.6 and XenApp 7.6. When a user selects the Citrix PDF Printer option, the driver converts the file to PDF and transfers the PDF to the local device. The PDF is then opened in a new window for viewing and printing from a locally attached printer or Google Cloud Print.
1. If you plan to enable session sharing on your XenApp deployment, download the App Switcher installer. Ensure that .NET Framework 4.0.3 is installed and enabled, then install App Switcher on each machine providing applications for Receiver for Chrome users.
App Switcher is configured to run automatically in the background when users establish a session.
 2. If you want to enable users to print documents opened with hosted applications or applications running on virtual desktops delivered by XenDesktop 7.6 and XenApp 7.6, complete the following steps.
 1. Download the Citrix PDF Printing Feature Pack and install the Citrix PDF Universal Printer driver on each machine providing desktops or applications for Receiver for Chrome users. After installing the printer driver, restart the machine.
 2. In Citrix Studio, select the Policy node in the left pane and either create a new policy or edit an existing policy. For more information about configuring XenDesktop and XenApp policies, see [Citrix policies](#).
 3. Set the Auto-create PDF Universal Printer policy setting to Enabled.

To configure StoreFront for Receiver for Chrome

A StoreFront store with a Receiver for Web site is required to make desktops and applications delivered by XenDesktop and XenApp available for Receiver for Chrome users.

Important: In multiple-server StoreFront deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, [propagate your configuration changes to the server group](#) so that the other servers in the deployment are updated.

1. If you have not already done so, deploy StoreFront and create a store aggregating the desktops and applications you want to make available to Receiver for Chrome users.
A Receiver for Web site is created automatically for new stores. For more information about creating StoreFront stores, see [Create a store](#).
2. In the Citrix StoreFront management console, select the Receiver for Web node in the left pane. From the results pane, select the site providing resources for Receiver for Chrome users and, in the Actions pane, click Deploy Citrix Receiver.
3. Enable Receiver for HTML5 by selecting one of the following options. The experience for Receiver for Chrome users is the same in both cases, but differs for users of other devices depending on the option you select.
 - If you want other users to access desktops and applications from the site using a locally installed version of Citrix Receiver, where available, select Use Receiver for HTML5 if local install fails. Users who already have Citrix Receiver installed cannot use Receiver for HTML5 to access resources from the site. Windows and Mac OS X users without Citrix Receiver are prompted to install Citrix Receiver every time they log on to the site, but can use Receiver for HTML5 if they are unable to install Citrix Receiver.

- If you want all other users to access desktops and applications from the site through Receiver for HTML5 regardless of whether they have a locally installed version of Citrix Receiver, select Always use Receiver for HTML5.
4. Use a text editor to open the web.config file for the Receiver for Web site, which is typically located in the C:\inetpub\wwwroot\Citrix\storename Web directory, where storename is the name specified for the store when it was created.
 5. Locate the following element in the file.
`<html5 ... preferences="" ... chromeAppPreferences="" />`
 6. If you changed the port used when you allowed WebSocket connections on XenDesktop or XenApp, set the value of the chromeAppPreferences attribute to **wsPort:port number**, where port number is the port that you configured in the policy.
 7. If you want to enable the in-session toolbar that lets users send the CTRL+ALT+DELETE key combination to their desktops and applications, enter a value for the chromeAppPreferences attribute as shown below.
`chromeAppPreferences='{ "type": "update", "ui": { "toolbar": { "menubar": true } } }' />`

This setting is required to enable the in-session toolbar for users downloading Receiver for Chrome from the Chrome Web Store. If you decide to deliver a repackaged version of Receiver for Chrome to your users instead, you can enable the in-session toolbar by editing the Receiver for Chrome configuration file. For details, see [Deploy Receiver for Chrome to your users](#).

Deploy

Aug 03, 2015

There are a number of options for deploying Receiver for Chrome.

- You repackage Receiver for Chrome to include a Citrix Receiver configuration (.cr) file you have generated. The .cr file contains the connection details for NetScaler Gateway and the Receiver for Web site providing users' desktops and applications. Users browse to `chrome://extensions` and then drag and drop the repackaged application (.crx) file onto the Chrome window to install Receiver for Chrome. As the application is preconfigured, users can start working with Receiver for Chrome as soon as they have installed it without needing to perform any additional configuration steps. You can deliver your custom Receiver for Chrome application to users in the following ways.
 - Publish the repackaged application for users through Google Apps for Business using the Google Admin Console.
 - Provide the .crx file to users by other means, such as through email.
- Users install Receiver for Chrome from the Chrome Web Store by searching for Citrix Receiver and clicking Add to Chrome. Once installed, Receiver for Chrome must be configured with connection details for NetScaler Gateway and the Receiver for Web site providing users' desktops and applications. This can be achieved in two ways.
 - You generate a .cr file containing the appropriate connection details and distribute this file to users. To configure Receiver for Chrome, users double-click the .cr file and click Add when prompted. For more information about generating .cr files from StoreFront, see [Export store provisioning files for users](#).
 - You provide users with the URL they must enter manually when they first start Receiver for Chrome.

To repackage Receiver for Chrome

To simplify the deployment process for users, you can repackage Receiver for Chrome with a new .cr file to preconfigure Receiver for Chrome with the appropriate connection details for your environment. Users can start working with Receiver for Chrome as soon as they have installed it without needing to perform any additional configuration steps.

1. Download the unpackaged version of Receiver for Chrome to a suitable location.
2. Download the sample configuration file and modify it as appropriate for your environment.
3. Rename the modified configuration file to `default.cr` and copy it to the Receiver for Chrome root directory. Configuration files with different names or in other locations are not included when Receiver for Chrome is repackaged.
4. If you want to enable the in-session toolbar that lets users send the CTRL+ALT+DELETE key combination to their desktops and applications, complete the following steps.
 1. Use a text editor to open the `configuration.js` file in the Receiver for Chrome root directory.
 2. Locate the following section in the file.

```
'appPrefs': {  
  'chromeApp': {  
    'ui' : {  
      'toolbar' : {  
        'menubar': false,  
        'clipboard': false
```
 3. Change the setting for the `menubar` attribute to `true`.
When you enable the in-session toolbar in this way, it is not necessary to enable the toolbar in the Receiver for Web site configuration file.

5. In Chrome, browse to `chrome://extensions`, select the Developer mode check box in the top right corner of the page and then click the Pack extension button.

For security reasons, StoreFront only accepts connections from known Receiver for Chrome instances. You must whitelist your repackaged application to enable users to connect to a Receiver for Web site.

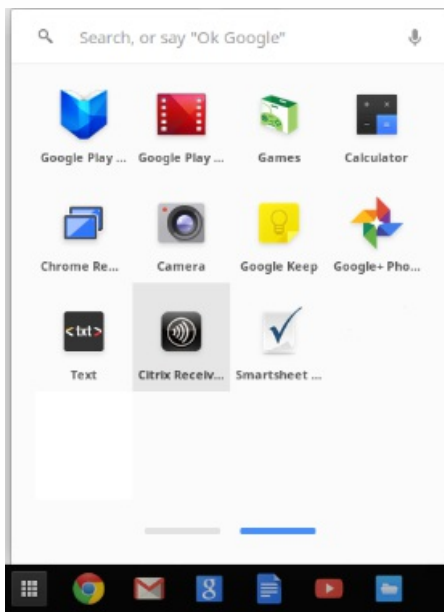
6. On the StoreFront server, use a text editor to open the `web.config` file for the Receiver for Web site, which is typically located in the `C:\inetpub\wwwroot\Citrix\storename Web` directory, where `storename` is the name specified for the store when it was created.
7. Locate the following element in the file.
`<html5 ... chromeAppOrigins="chrome-extension://haiffjcadagjljjoggckpgfnoeiflnem" ... />`
8. Change the value of the `chromeAppOrigins` attribute to **chrome-extension://haiffjcadagjljjoggckpgfnoeiflnem|chrome-extension://packageid**, where `packageid` is the ID generated for your repackaged application.

User experience

Sep 25, 2014

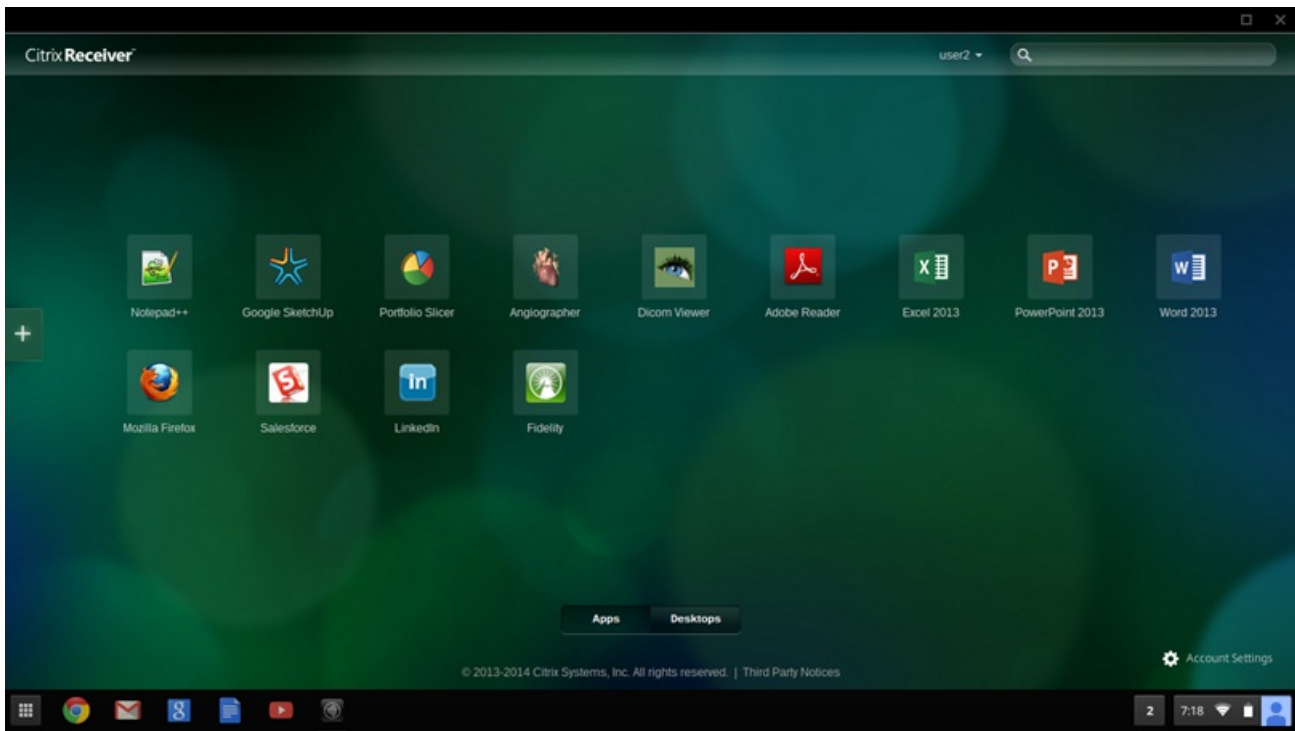
After installing and configuring Receiver for Chrome, users click the Citrix Receiver icon in the Chrome apps list to start Receiver for Chrome. To remove Receiver for Chrome from their devices, users must right-click the Citrix Receiver icon in the Chrome apps list and select Uninstall.

Citrix Receiver icon in the Chrome apps list



After they have logged on, users' desktops and applications appear. Users can search for resources and click an icon to start a desktop or application in a new window.

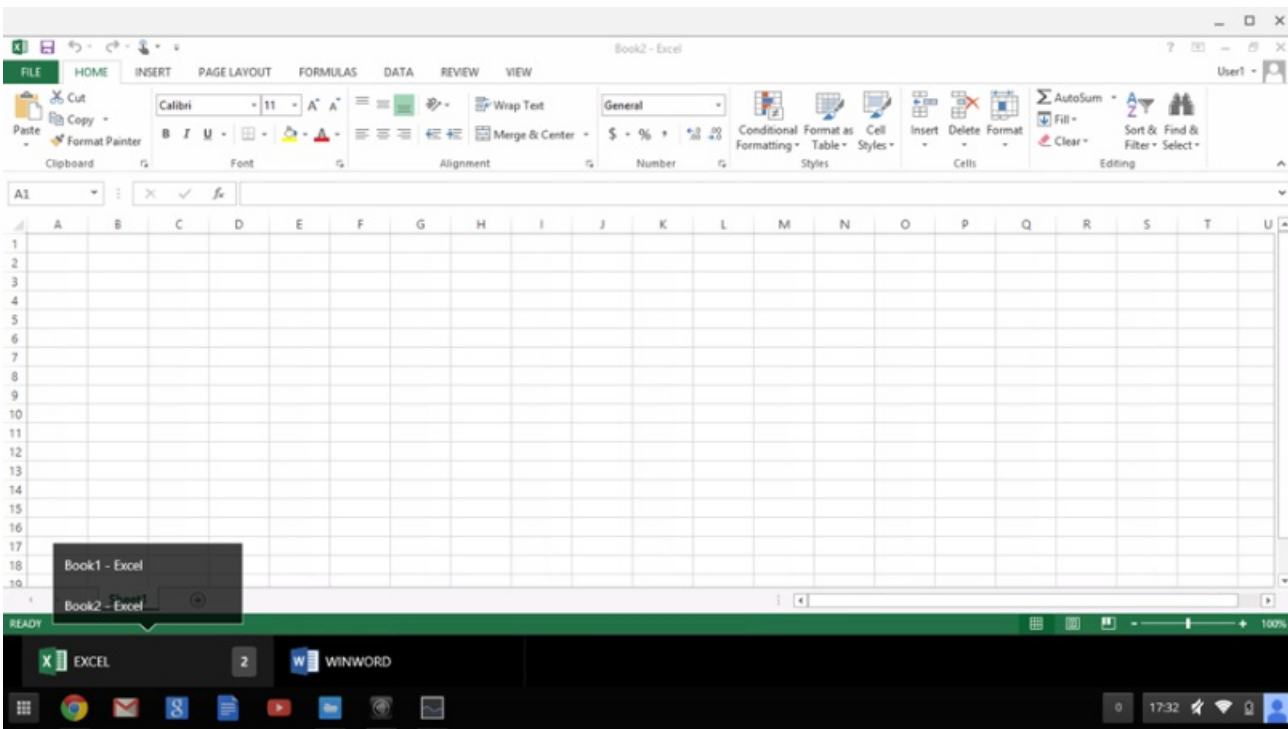
Available applications in Receiver for Chrome



When a user starts an additional application, Receiver for Chrome checks whether the application can be started within an existing session before creating a new session. This enables users to access multiple applications over a single connection so that the available resources are used more efficiently.

For session sharing to occur, the applications must be hosted on the same machine and must be configured in seamless window mode with the same settings for parameters such as window size, color depth, and encryption. Session sharing is enabled by default when a hosted application is made available. Applications running in the same session appear in the same window. If App Switcher is installed on the machine providing the applications, a taskbar appears at the bottom of the window. The taskbar displays all the applications currently running in the session, enabling users to switch between those applications. Users can configure the taskbar to auto-hide and switch to small icons to minimize the amount of space taken up by the taskbar.

App Switcher taskbar for switching between applications

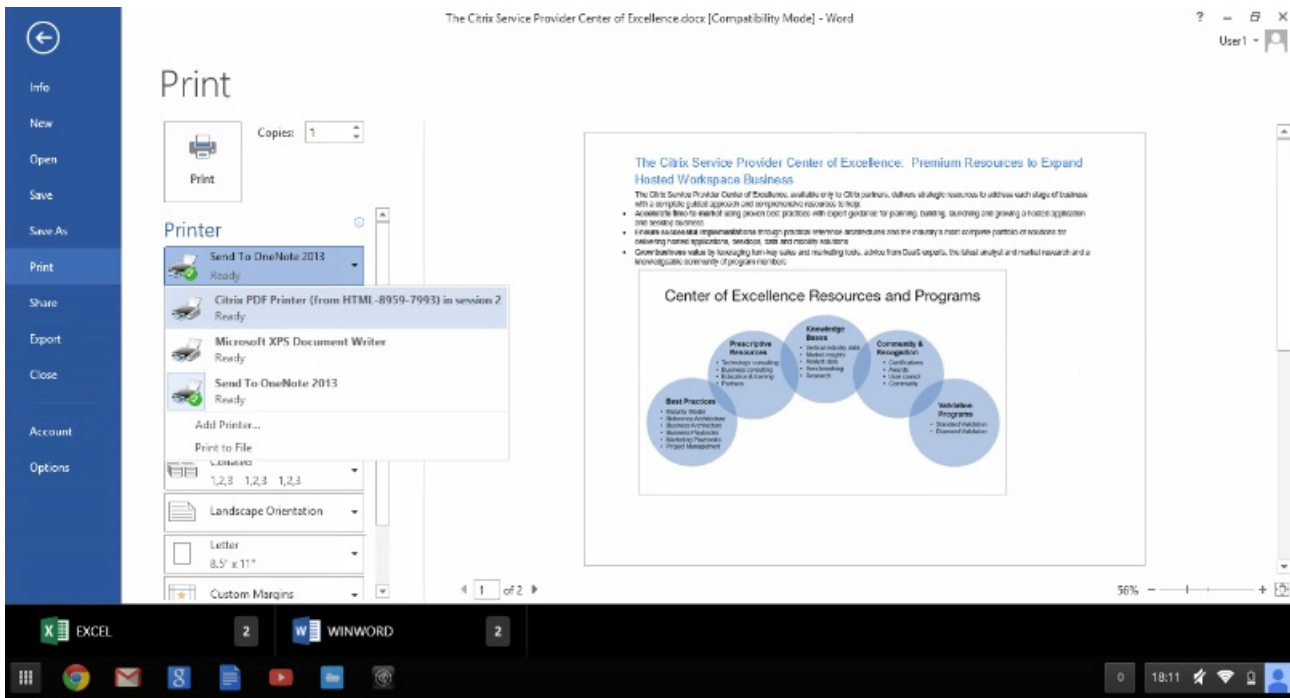


Users can use standard Windows shortcuts to copy data, including text, tables, and images, between hosted applications, both within the same session and between different sessions. Only Unicode plain text can be copied and pasted between hosted applications and the local clipboard on the device.

Users can use standard Windows keyboard shortcuts with Receiver for Chrome because these shortcuts are passed from Chrome OS to hosted applications. Similarly, shortcuts specific to particular applications can also be used, provided they do not conflict with any Chrome OS shortcuts. However, note that the Windows key must also be pressed for function keys to be recognized, so an external keyboard is required. For more information about using Windows keyboards with Chrome OS, see <https://support.google.com/chromebook/answer/1047364>. Citrix-specific shortcuts, such as those for switching between sessions and windows, cannot be used with Receiver for Chrome.

When printing a document opened with a hosted application or an application running on a virtual desktop, the user is given the option to print the document to PDF. The PDF is then transferred to the local device for viewing and printing from a locally attached printer or Google Cloud Print. The file is not stored by Receiver for Chrome.

Citrix PDF Printer for transferring documents to the local device



To enable logging for Receiver for Chrome

To assist with troubleshooting connection issues, logs can be generated on both the user device and the machines providing desktops and applications for users.

1. To capture logs of desktop and application launches on a user device, complete the following steps.

1. On the user device, click Account Settings in the bottom right corner of the Receiver for Chrome logon page.
2. In the Settings dialog box, click Start Logging.
Details of the collected log files are listed in the Settings dialog box.

3. Click Stop Logging to end collection of logs on the user device.

2. To enable logging for App Switcher on machines providing applications for users, complete the following steps.

1. Use a text editor to open the AppSwitcher.exe.config file, which is typically located in the C:\Program Files (x86)\Citrix\App Switcher directory.
2. Locate the following section in the file.

```
<applicationSettings>
  <Citrix.AppSwitcher.Properties.Settings>
    <setting name="TraceEnabled" serializeAS="String" >
      <value>False</value>
    </setting>
  </Citrix.AppSwitcher.Properties.Settings>
</applicationSettings>
```

3. Change the content of the <value> element to True to enable App Switcher logging.

The App Switcher log files are saved in the AppData\CitrixAppSwitcherLogs directory. The AppData directory is hidden by default.