About Citrix Receiver for Chrome 2.1

Aug 11, 2016

Citrix Receiver for Chrome is a native Chrome packaged app which enables users to access virtual desktops and hosted applications from Chrome devices. Resources delivered by XenDesktop and XenApp are aggregated in a StoreFront store and made available through a Citrix Receiver for Web site.

With the Citrix Receiver for Chrome app installed, users can access desktops and applications within their web browsers; no additional configuration or deployment options are required on StoreFront.

About release 2.1.0.133

Citrix has released an update to Receiver for Chrome version 2.1 to address a number of customer reported problems. Version 2.1.0.133 resolves the following issues:

- Cannot connect to older versions of StoreFront or NetScaler Gateway; a session would open in a browser instead of Citrix Receiver. [#653981]
- A session failed to launch from RDP or Citrix ICA double hop scenarios. [#653980]
- CTRL and SHIFT keys did not work when selecting files or text. [#654185]

New in this release

Enhanced configuration

Citrix Receiver for Chrome provides additional functionality that allows administrators greater configuration control permitting new ways to configure Receiver. With this release, administrators can configure Receiver using:

- Google Admin Policy
- Web.config in Storefront
- default.ica
- configuration.js

Using these methods, session settings like below can be configured:

- Show/hide the toolbar
- Enable/disable NACL
- Audio
- Graphics
- File Transfer

For more details, refer to the Configuring Citrix Receiver article.

> ### Tip
>
> The **configuration.js** file is located in the ChromeApp root folder. Administrator level credentials are required to edit this file; after editing the file, repackage the app to make additional modifications to toolbar elements.

Smart card authentication

Receiver for Chrome now allows users to authenticate using a Smart Card. Using this new feature, administrators can login to Receiver using a smart card and can also sign emails or access the websites in an ICA session using smart card credentials. For more details, refer to the *Smart Card* section in the Configuring Citrix Receiver article.

Serial port redirection

Citrix Receiver for Chrome allows users to redirect COM/serial port devices to XenApp and XenDesktop virtual apps and desktops. With this functionality, users can view and access COM/serial port based devices in an active Receiver session.

For more details, refer to the Configuring Citrix Receiver article.

Note

By default, Receiver for Chrome maps COM5 as a preferred serial COM port for redirection.

Single sign on (SSON)

Citrix Receiver for Chrome now supports single sign on (SSON) functionality into Chromebook devices as well as the Citrix XenApp/XenDesktop backend using Federated authentication. With this functionality, users do not have to retype passwords within a Citrix environment. SSON works by setting up SAML SSO into Chrome devices and Receiver sessions using the SAML cookies to login to NetScaler Gateway.

For more details, refer to the Configuring Citrix Receiver article.

Secure ICA

Prior to this release, Receiver for Chrome supported only basic encryption in case of connection without NetScaler. With this release, RC5 (128 bit) encryption is also supported.

Note

If any encryption format other than basic is set, then the Receiver for Chrome upgrades to RC5 (128 bit).

Tip

Citrix recommends that you use a SSL enabled VDA for end to end SSL encryption.

More USB devices

This release supports a wider range of USB peripherals. With this added functionality, an administrator can create a Google policy to identify the PID/VID of the device to enable its use in Citrix Receiver. This support extends to new USB devices,

including 3D Space mouse, additional composite devices, and Bloomberg keyboard.

> **Note**
>
> Refer to the Support Knowledge Center for information about Citrix tested USB devices with Receiver for Chrome.

Reload Store URL

A new button is added where store is loaded. By clicking the button, the cookies of the store get cleared and the store page is reloaded.

Unique ID

Receiver generates a unique name using the Directory API ID of the devices enrolled via Google Chrome Management. The generated name looks like CRxxxxxxxxxxxxxxxx. To change the prefix “CR”, refer to the Configuring Citrix Receiver article.

Known issues

This release of Receiver for Chrome has the following known issues:

- ENH ID 0652697: In some cases, the Google smartcard connector may crash. To resolve this issue, disconnect then reconnect the session to reenable smartcard redirection.

Previously reported issues at version 2.0 include:

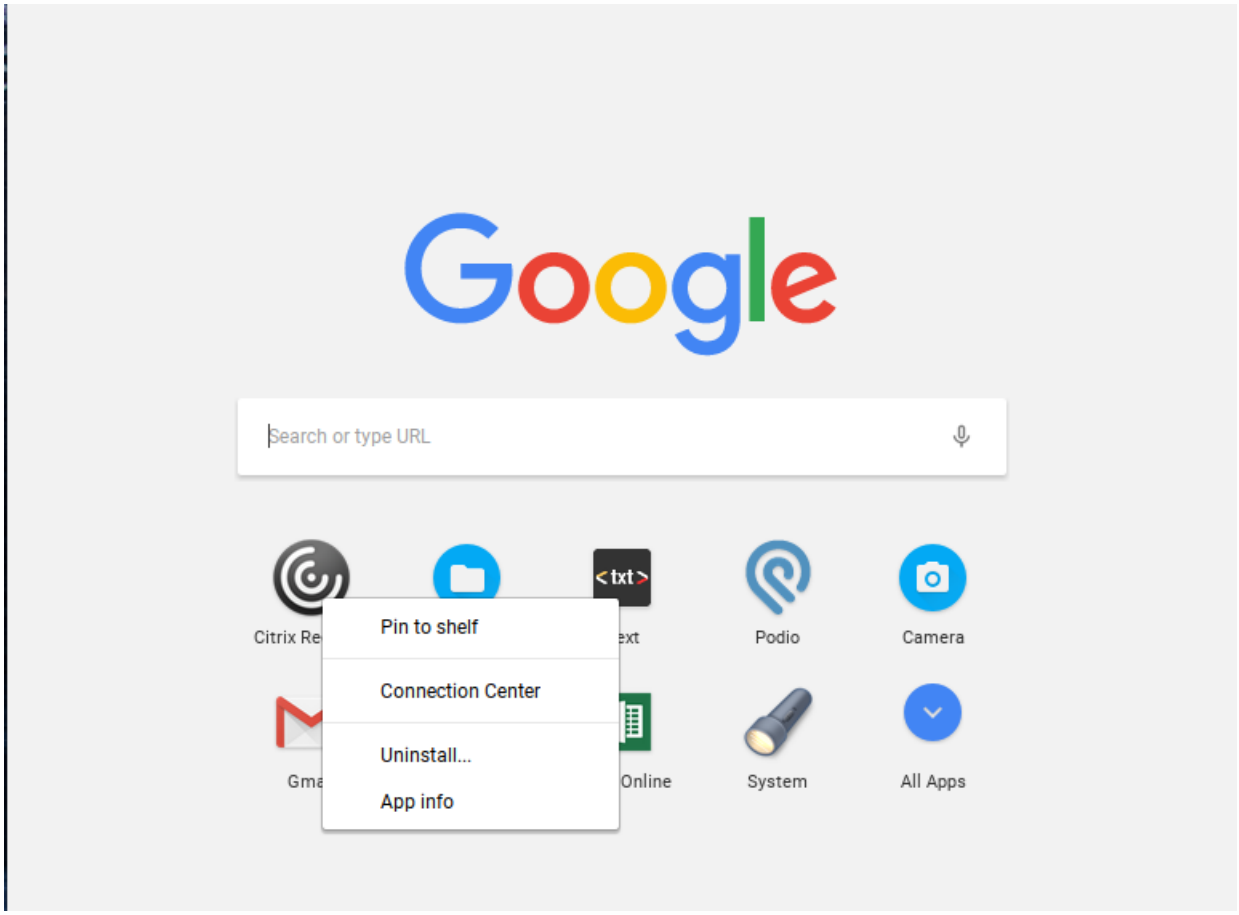
- The F5 key does not display the thumbprint view of apps, instead a thumbprint of VDAs displays all apps within a session. [#0615795]
- On Chrome OS taskbar along with the apps, the server name is also displayed in an active session. [#0616836]
- The work area of an active session is not updated when the Chrome book shelf position is changed or hidden. [#0623585]
- An app can be moved around an active session display when a modal dialogue window is present in the foreground. [#0625399]
- You may need to use Alt+Tab an extra time to switch between apps from different VDAs.
- A session may crash while copying and pasting a large amount of data inside a session. Citrix recommends copying less than 10 MB of data when using the clipboard.
  [#0586671]
- Citrix recommends that you use an absolute path rather than a relative path in File Transfer registry settings.
  [#0607455]
- Citrix Receiver for Chrome does not support cross language keyboard.
  [ENH0602652]
- When contents are copied from a document on Google drive (Gdrive) to a session the format of the copied content may not be maintained. To resolve this issue, open the document containing the copied content using the respective app (for example, Google docs, Microsoft Word or Excel) and perform clipboard operations. This should reserve the format at the session side.
  [#0606135]
- The keyboard combination ALT+F4 does not work as expected within a session. Click the **Search/Windows** key along with top row keys to simulate function keys on a Chrome book. You can also use the **Keyboard settings** option on the Chrome book to enable the 'Treat top-row keys as function keys' to enable direct use of the top row keys to simulate function keys.
  [#0607326]

User experience

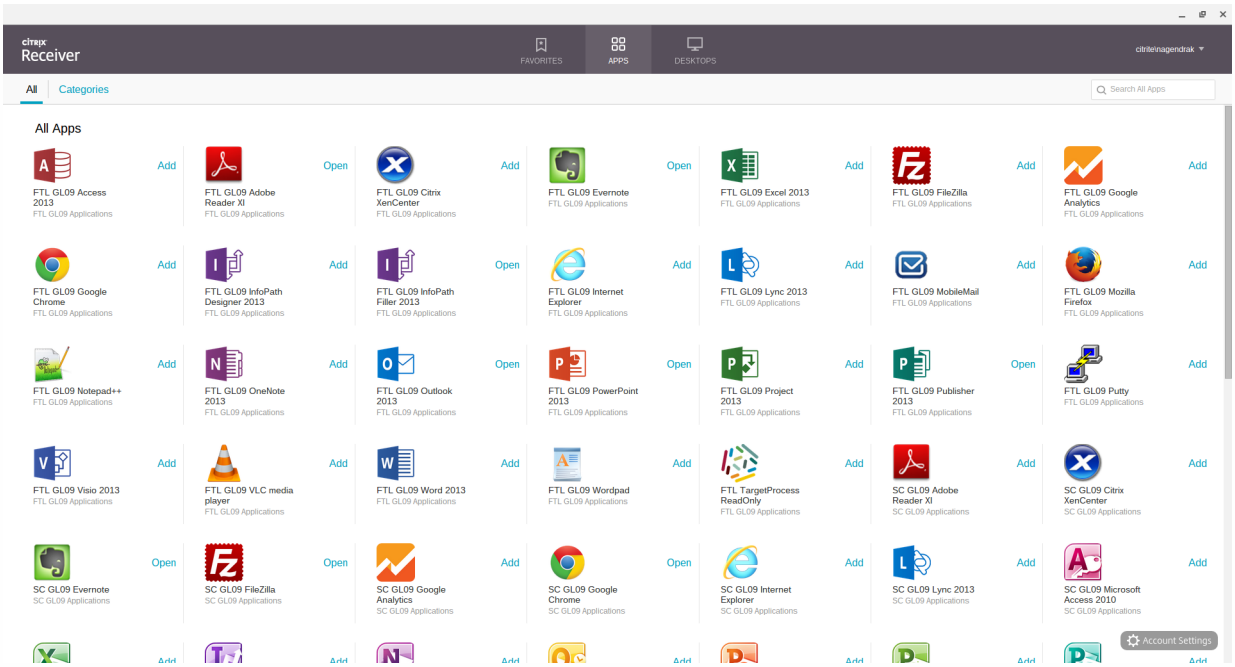
Dec 22, 2016

After installing and configuring Citrix Receiver for Chrome, users click the Citrix Receiver icon in the Chrome apps list to start Receiver for Chrome, as shown in the following figure.

You can uninstall Citrix Receiver for Chrome by navigating to the Chrome App list. In the list of Chrome Apps, right click on Citrix Receiver and select **Uninstall**.

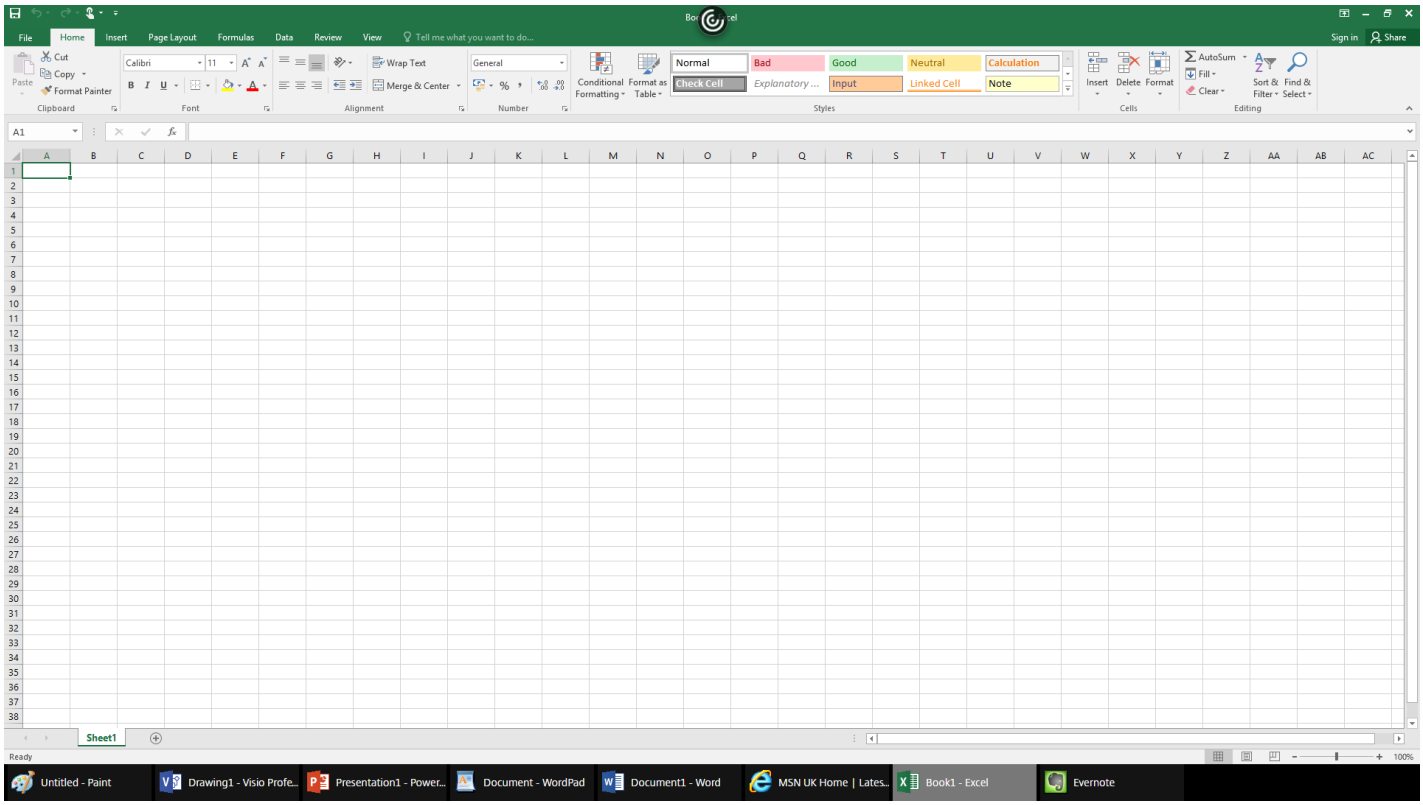


After they have logged on, users' desktops and applications appear, as shown in the following figure. Users can search for resources and click an icon to start a desktop or application in a new window.



When a user starts an additional application, Citrix 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.

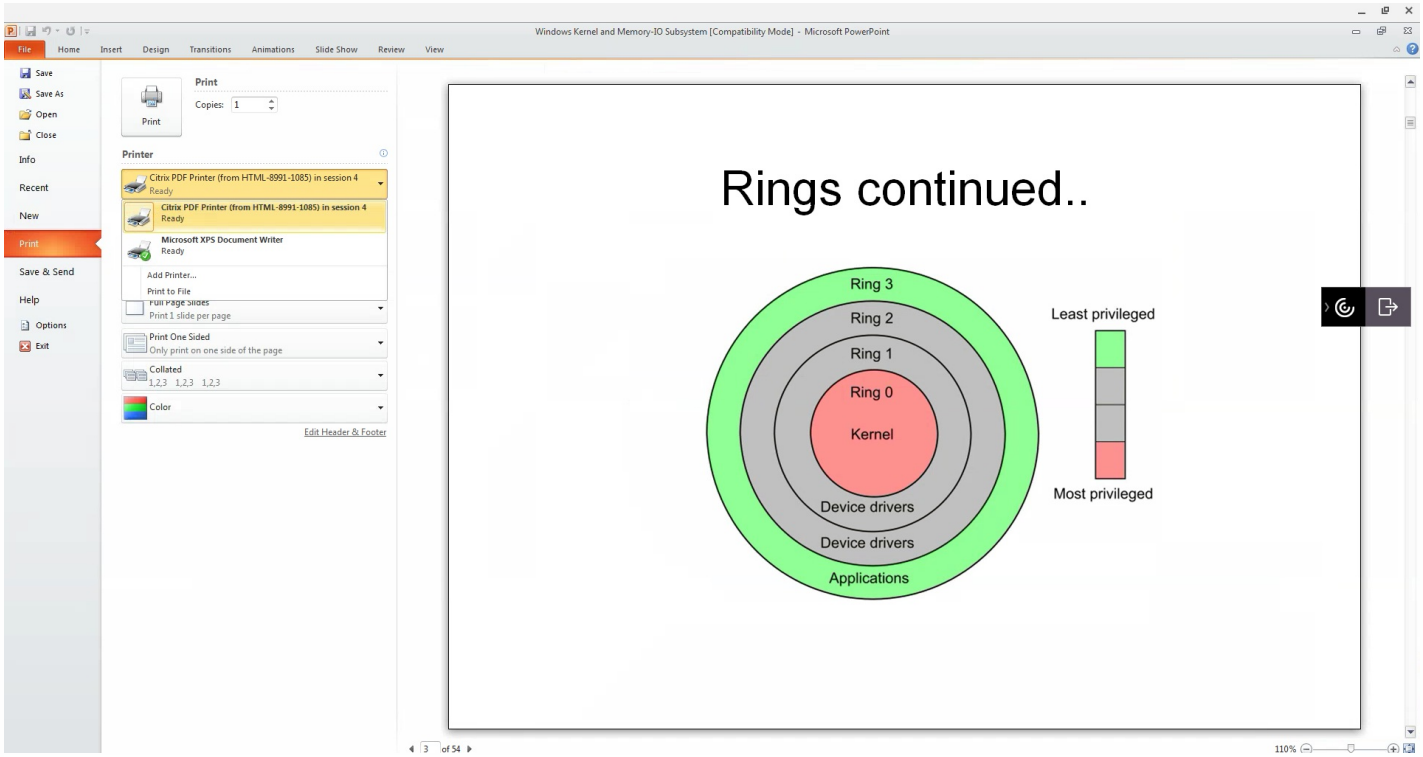


Users can use standard Windows shortcuts to copy data, including text, tables, and images, between hosted applications, both within the same session and between different sessions. Only Unicode plain text can be copied and pasted between hosted applications and the local clipboard on the device.

Users can use standard Windows keyboard shortcuts with Citrix 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 Citrix 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, as shown in the following figure. 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 Citrix Receiver for Chrome.

Note: See the features for this release for more information about Google Cloud Print support.



To enable logging for Citrix 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.

Enabling logging on user devices

To capture logs on a user device:

1. On the user device, click the button with a settings image on it in the bottom-right corner of the Citrix 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 the collection of logs on the user device.

Deploying Citrix Receiver

Aug 11, 2016

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

- You can use Google App management console to configure Citrix Receiver using Google policy. For more information, see CTX141844.
- You can repackage Citrix 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 Citrix 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 Citrix Receiver for Chrome. As the application is preconfigured, users can start working with Citrix Receiver for Chrome as soon as they have installed it without needing to perform additional configuration steps.
  You can deliver your custom Citrix 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 Citrix Receiver for Chrome from the Chrome Web Store by searching for Citrix Receiver and clicking Add to Chrome.
  Once installed, Citrix Receiver for Chrome must be configured with connection details for NetScaler Gateway and the Citrix Receiver for Web site providing users' desktops and applications. This can be achieved in two ways.
  - Generate a .cr file containing the appropriate connection details and distribute this file to users. To configure Citrix 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.
  - Provide users with the URL they must enter manually when they first start Citrix Receiver for Chrome.

To repackage Citrix Receiver for Chrome

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

1. Download the unpackaged version of Citrix 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 Citrix Receiver for Chrome root directory. Configuration files with different names or in other locations are not included when Citrix 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 Citrix Receiver for ChromeApp 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 Citrix Web site configuration file.

5. By default Citrix Receiver for Chrome can open any file extension in the Files App in a Chromebook intended for opening files in Google Drive using the FileAccess component in the VDA. If an administrator wants to disable this option to download the unpackaged version of Citrix Receiver for Chrome and edit the "file handlers" section in manifest.ison to resemble the following:

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

6. 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 Citrix Receiver for Chrome instances. You must whitelist your repackaged application to enable users to connect to a Citrix Receiver for Web site.
7. On the StoreFront server, use a text editor to open the web.config file for the Citrix 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.
8. Locate the following element in the file.
   `<html5 ... chromeAppOrigins="chrome-extension://haiffjcadagjlijoggckpgfnoeiflnem" ... />`
9. **Change the value of the** chromeAppOrigins **attribute to** chrome-extension://haiffjcadagjlijoggckpgfnoeiflnem|chrome-extension://*packageid*, where **packageid** is the ID generated for your repackaged application.

Configuring your environment

Aug 11, 2016

To enable Citrix 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.

Also in this article:

Configuring Receiver for Chrome

This section includes information about:

- Google Admin Policy
- Web.config in Storefront
- default.ica
- configuration.js

Configuring Receiver using Google Admin Policy

Prior to this release, only store/beacon related configuration could be pushed through Google Admin Policy. For additional information about this policy, refer to the Receiver for Chrome Configuration in the Support Knowledge Center.

With Citrix Receiver for Chrome version 2.1, other Chrome configurations can also be pushed through the Google Admin Policy.

> **Note**
>
> Citrix recommends using this method only when Citrix Receiver for Chrome is repackaged for users.

For more information, refer to the sample policy text below:

```
command                                                    COPY

{
```



```
"settings": {

        "Value": {

                "settings_version": "1.0",

                "store_settings": {

                        "name": "RTST",

                        "gateways": [

                                {

                                        "url":“https://yourcompany.gateway.com",

                                         "is_default": true

                                 }

                        ],

                        "beacons": {

                            "internal": [

                                    {

                                            "url":

“http://yourcompany.internalwebsite.net"

                                                }

                                ],

                                "external": [

                                        {
```

```
                                        {
                                          "url":
“http://www.yourcompany.externalwebsite.com"
                                        }
                                ]
                        },
                        "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": {
                                                "enable": true
                                        }
                                }
                        }
                }
        }
}
```

Configuring Receiver for Chrome using Web.config in StoreFront

To change the configuration using the Web.config file:

1. Open the **web.config** file for the Citrix Receiver for Website. This file is typically located in **C:\inetpub\wwwroot\Citrix\storenameWeb**, where *storename* is the name specified for the store when it was created.
2. Locate the **chromeAppPreferences** field and set its value with the configuration as a JSON string.

For example:
chromeAppPreferences = '{"ui": {"toolbar": {"menubar": false}}}'

> **Note**
>
> Citrix recommends that you use the **web.config** file method for configuration purposes only when a Store version of Receiver for Chrome is being used.

Configuring Receiver for Chrome using the default.ica file

To change the configuration using the **default.ica** file:

1. Open the default.ica file typically located at **C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica** for Web interface customers, where **sitename** is the name specified for the site when it was created.
   In case of Storefront customers, **default.ica** file is typically located at **C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica**, where **storename** is the name specified for the store when it was created.
2. Add a new key at the end of the file, **chromeAppPreferences** with its value set to configuration as the JSON object.

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

> **Note**
>
> Citrix recommends that you use the **default.ica** file method for configuration purposes only for Web Interface users.

A sample **default.ica** file might resemble:

;

; ICA Override File

;

; Add ICA file settings that you want to be sent to client devices

; to this file. Settings contained in this file override any

; settings generated by 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=pdc0w.dll
DriverNameWin32=pdc0n.dll

[EncRC5-40]
DriverNameWin16=pdc40w.dll
DriverNameWin32=pdc40n.dll

[EncRC5-56]
DriverNameWin16=pdc56w.dll
DriverNameWin32=pdc56n.dll

[EncRC5-128]
DriverNameWin16=pdc128w.dll
DriverNameWin32=pdc128n.dll
```

[Compress]

DriverNameWin16=pdcompw.dll

DriverNameWin32=pdcompn.dll

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

Configuring Citrix Receiver for Chrome using the configuration.js file

The **configuration.js** file is located in the ChromeApp root folder. Access this file directly to make changes to Citrix Receiver for Chrome.

> ## Tip
>
> Administrator level credentials are required to edit the **configuration.js** file; after editing the file, repackage the app to make additional modifications to toolbar elements.

> ## Note
>
> In Kiosk mode, the toolbar is hidden by default. When editing the **configuration.js** file to enable the toolbar, ensure that Kiosk mode is disabled. Citrix recommends that you use one of the alternative methods (for example, the **default.ica** file) to enable the toolbar.

Enabling smart card authentication

Receiver for Chrome provides support for USB smart card readers with StoreFront. You can use smart cards for the following purposes:

- Smart card logon authentication to Receiver for Chrome.
- Smart card-aware published apps to access local smart card devices.
- Applications such as Microsoft Word and Outlook that are launched in ICA sessions can access smart cards for signing documents and email.

Supported smart cards include:
- PIV cards
- common access cards

Smart card for your Chrome device has the following prerequisites:
- smart card authentication to StoreFront versions 3.6 and above

> ## Important
>
> For smart card authentication to StoreFront 3.5 or earlier, users require a custom script to enable smart card authentication. Contact Citrix Support for details.

- XenDesktop 7.6 and above
- XenApp 6.5 and above

To configure smart card support on your Chrome device:

1. Install the smart card connector application. Note that the smart card application is required for PCSC support on the Chrome device. This application reads the smart card using the USB interface. You can install this application from the Chrome website.

2. Install the middleware application. Note that a middleware application (for example, Charismathics, or CACKey) is required because it serves as an interface which communicates with the smart card and other client certificates.

- To install the Charismathics smart card extention, refer to the instructions on the Chrome website.
- To install the CACKey, refer to the instructions on the Chrome website.

> **Note**
>
> For more information about middleware applications and smart card authentication, refer to the Google support site.

3. Configure smart card authentication using NetScaler Gateway. Refer to the instructions located on the Product Documentation Site.

> **Important**
>
> Mandatory client authentication is required when a session is being launched. To prevent this from occurring, refer to the instructions noted in the **Third reduction (one PIN prompt)** section in the NetScaler product documentation.

Smart card authentication support has the following limitations:

- The smart card certificate is cached even after the smart card is removed from the Chrome device. This is a known issue that exists in Google Chrome. Restart the Chrome device to clear the cache.
- When Receiver for Chrome is repackaged, administrators should get the appID whitelisted by Google to ensure that the smart card connector application passes through.
- Only one smart card reader is supported at a time.

Configuring serial COM port redirection

To configure serial COM port redirection, enable the feature by applying XenApp/XenDesktop port redirection policy settings. For more information, refer to the policy settings article.

> **Note**
>
> By default, Receiver for Chrome maps COM5 as a preferred serial COM port for redirection.

After enabling serial COM port redirection policy settings in XenApp/XenDesktop, configure Receiver for Chrome using one

of the following methods:

- Google Admin Policy
- Using the configuration.js file
- Changing the default mapping by issuing a command in an active ICA session.

Using Google Admin Policy to configure COM port redirection

Use this method to redirect the serial COM port by editing the policy file.

> **Tip**
>
> Citrix recommends that you configure the COM port using the policy file only when Receiver for Chrome is repackaged.

Edit the Google Admin Policy by including the following:

command COPY

```
{
        "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
```

```
                                }

                            }

                        }

                    }



    }
```

Using the configuration.js file to configure COM port redirection

Use this method to redirect the serial COM port by editing the **configuration.js** file. Locate the portname field in the configuration.js file and edit the value by changing the port number.

For example:

"com" :{

"portname" : "COM4"

}

> ## Note
>
> Citrix recommends using the configuration.js file method to configure serial port redirection only when Receiver for Chrome is repackaged and republished from StoreFront.

Issuing a command in an ICA session to configure COM port redirection

Use this method to redirect the serial COM port by executing the following command in an active ICA session:

command COPY

```
net use COM4 : \\Client\COM5
```

> **Tip**
>
> In the example above, COM4 is the preferred serial port used for redirection.

Configuring single sign on (SSO) with Google and Citrix using SAML authentication

To configure SSO:

1. Setup the third party Identity provider (IdP) for SAML authentication if it's not already configured (for example, ADFS 2.0). For more information, refer to How to Configure NetScaler SAML to Work with Microsoft AD FS 2.0 IDP.

2. Setup SSO with Google Apps using SAML IdP; this enables users to leverage third party identity to use Google apps instead of the Google Enterprise account. For more information, refer to Set up Single Sign-On (SSO) for Google Apps accounts using third party identity providers.

3. Configure Chrome devices to logon via SAML IdP; this enables users to logon to Chrome devices using a third party identity provider.

4. Configure NetScaler Gateway to logon via SAML IdP; this enables users to logon to NetScaler Gateway using a third party identity provider. Refer to the article describing how to configure SAML authentication.

5. Configure XenApp and XenDesktop for Federated Authentication to allow login to XenApp/XenDesktop sessions using dynamically generated certificates after the SAML logon process instead of typing username/password combinations. For more information, refer to the article describing Federated Authentication.

6. Install and configure SAML SSO for Chrome app extension on Chrome devices. For more information, refer to the Google website for more information. This extension retrieves SAML cookies from the browser and provides to Citrix Receiver. This extension needs to be configured with the following policy to allow Receiver to get SAML cookies:

```
command
```

COPY

```
{

  "whitelist" : {

    "Value" : [

      {

      "appId" : "haiffjcadagjlijoggckpgfnoeiflnem",

      "domain" : "saml.yourcompany.com"

      }

    ]

  }

}
```

> **Tip**
>
> If you are repackaging Receiver for Chrome, change the **appId** accordingly. In addition, change the domain to your company's SAML IdP domain.

7. Configure Receiver to user NetScaler Gateway configured for SAML logon. This enables users to use the NetScaler Gateway configured for SAML logon. Refer to the Support Knowledge Center for more information.

Enabling Google Cloud printing and the Citrix Universal Print Driver

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 through Google Cloud Print.

> **Important**
>
> Local PDF printing is only supported on XenApp/XenDesktop 7.6 and later.

Requirements

To access the Citrix Receiver for Chrome download page, you need a MyCitrix account.

Download the Citrix PDF Printer from the Citrix Receiver for Chrome download page.

To enable users to print documents opened with hosted applications or applications

1. Download the Citrix PDF Printer 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.

Enabling and disabling access to Google Drive

With Google drive support your users can open Windows file types, edit them, and save them from a Chrome device running Citrix Receiver. While running a Google Chrome device, your users can seamlessly use existing Windows-based applications (for example, Microsoft Word) and access the files residing on Google Drive

For example, if one of your users opens a file in Google Drive (for instance, an .DOC file attachment downloaded from Gmail), edits it, and saves it to Google Drive, the file can be accessed in a XenApp hosted application. The file can be viewed, edited, and saved to Google Drive.

Requirements

To enable Google Drive access you must install the Citrix File Access component (FileAccess.exe) on your users' VDAs and enable file type associations in Citrix Studio. You can download Citrix File Access from the Citrix Receiver for Chrome download page.

To enable Google Drive access from Citrix Receiver

1. Install FileAccess.exe on each XenApp/XenDesktop VDA.
2. Configure the appropriate FTAs for published applications in Citrix AppCenter/Desktop studio.
3. On the XenApp/XenDesktop VDA https://accounts.google.com and https://ssl.gstatic.com have to be trusted and cookies from these sites should be enabled.

Only files from Google drive (only 'My Drive' folder) can be opened using Citrix receiver. To open a file from google drive, right click on the file, and open with Citrix Receiver.

Citrix recommends that you associate one File Type with only one published application.

To disable Google Drive access from Citrix Receiver

In the manifest.json file, replace:

```
"file_handlers" : {
    "all-file-types" : {
      "extensions" : [
        "*"
```

```
        ]
      }
    },
```

with:

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

Enabling and configuring KIOSK mode

Citrix Receiver for Chrome KIOSK mode provides the ability to run all apps in the same window. Using this feature, you can run Citrix Receiver apps in KIOSK mode, and then launch any Windows app or Desktop using the same mode. In addition, KIOSK mode allows you to publish remote apps or desktops as a dedicated Chrome package using a persistent URL.

You can control this feature set by adjusting the KIOSK settings in the Chrome admin panel for managed Chrome devices.

Refer to the Google support site for instructions on enabling the Receiver app to run in KIOSK mode on managed and non-managed Chrome devices.

If you are deploying a Receiver app, you should publish using the visibility options set to Public/unlisted to ensure interoperability with KIOSK mode. Go to the Chrome Web Store Developer Dashboard.

The Store URL is read-only when KIOSK mode is active, and cannot be edited using the Account settings screen. However, you can change this setting by either repackaging the app with the .cr file or through Google Policy Management using the Google Admin Console.

.cr file example

COPY

```
<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>
```

If you are using the Google Admin Console, edit the policy.txt file containing the Receiver configuration. Replace the value of “url” under “rf_web” with a persistent URL.

example COPY

```
{
"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 "

}

}

}

}

}
```

System requirements

Aug 11, 2016

User device requirements

All devices should meet the minimum hardware requirements for the installed operating system.

Users devices require the Google Chrome operating system (version 50 or later) to access desktops and applications using Citrix Receiver for Chrome. Citrix recommends that you use Citrix Receiver for Chrome with releases from the stable channel of Google Chrome. Citrix Receiver for Chrome is only supported on Chrome OS.

Citrix server requirements

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

- StoreFront 3.6
- StoreFront 3.5
- StoreFront 3.0
- StoreFront 2.5
- Web Interface 5.4

Citrix Receiver for Chrome can be used to access desktops and applications delivered by the following product versions:

- LTSR (XenApp) CU1, LTSR (XenDesktop) CU1 - 7.6.1000
- XenDesktop 7.9
- XenApp 7.9
- XenApp 6.5

> ### Note
>
> Citrix Receiver for Chrome supports all the supported versions of XenApp and XenDesktop as stated in the Citrix support lifecycle. See the Product Matrix for details.

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 Citrix Receiver for Chrome is deployed. Citrix Receiver for Chrome enables user access to desktops and applications from public networks with the following versions of NetScaler Gateway.

- NetScaler Gateway 11.1
- NetScaler Gateway 11.0
- NetScaler Gateway 10.5

Citrix Receiver for Chrome now supports CloudBridge disabling compression and printer compression as well as using HDX Insight analytics to display in CloudBridge Insight Center.

- CloudBridge 7.4