About this release

Oct 05, 2016

Receiver for HTML5 is hosted on StoreFront servers and enables users to access virtual desktops and hosted applications from a web browser. Resources delivered by XenDesktop and XenApp are aggregated in a StoreFront store and made available through a Receiver for Web site. With Receiver for HTML5 enabled on the site, users can access desktops and applications within their web browsers without needing to install Receiver locally on their devices.

When used in conjunction with the centralized customization and branding capabilities of the StoreFront 3.0, users of this Receiver for HTML5 release will receive a centrally managed app and desktop selection experience from StoreFront. This is the same consistent user experience that can be received by the Windows and Mac desktop Receivers and Chrome web Receiver when associated with the StoreFront 3.0.

New at this release

File Transfer

Receiver for HTML5 provides secure file transfer between a user device and virtual XenDesktop sessions. This feature uses a file transfer virtual channel instead of client drive mapping.

By default, users can:

- Upload files from a local download folder or attached peripheral and seamlessly access the data from their XenDesktop sessions.
- Download files from their XenDesktop sessions to a folder or peripheral on their user device.

Administrators can selectively enable or disable file transfer, uploads, or downloads through policies in Citrix Studio.

Requirements

- XenDesktop 7.6 or XenApp 7.6, with:
  - Hotfix ICATS760WX64022.msp on server OS VDAs (Windows 2008 R2 or Windows 2012 R2)
  - Hotfix ICAWS760WX86022.msp or ICAWS760WX64022.msp on client OS VDAs (Windows 7 or Windows 8.1)
- To change file transfer policies: Group Policy Management (GPM) hotfix GPMx240WX64002.msi or GPMx240WX86002.msi on machines running Citrix Studio

Limitations

- A user can upload or download a maximum of 10 files at a time
- Maximum file size:
  - For uploads: 2147483647 bytes (2 GB)
  - For downloads: 262144000 bytes (250 MB)

File Transfer policies

By default, file transfer is enabled. Use Citrix Studio to change these policies, located under User Setting < ICA\File Redirection. Consider the following when using file transfer policies:

- Allow file transfer between desktop and client. Allows or prevents users from transferring files between a virtual XenDesktop session and their devices.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Upload file to desktop. Allows or prevents users from uploading files from their device to a virtual XenDesktop session.
- Download file from desktop. Allows or prevents users from downloading files from a virtual XenDesktop session to their device.

Session Reliability

Receiver for HTML5 now includes improved session reliability to provide mobile users with uninterrupted access to apps and virtual desktops when moving between network access points. This functionality improves the user experience by ensuring a constant state of active connectivity, even when the user's device power cycles when entering sleep mode.

Note: Sessions will only resume when network connectivity resumes after 180 seconds.

The following hotfixes are required to use this feature:

- ICATS760WX64022
- ICAWS760WX64022
- ICAWS760WX86022

Requirements
- NetScaler version 11.0 (build 55.23 or later)

Known issues

- Session reliability behavior is not consistent when using the Firefox browser. [#0564201]
- Cloud bridge is unable to parse connections. [#0566330]
- File transfer download does not work in Safari browser. [#0565281]
- Dragging and dropping to upload a file is not functioning in MS Edge. [#0565306]
- Use the toolbar button when attempting a file transfer from a session to a client. [#0565725, #0564879, #0564920]
- When file upload/download is disabled using Studio policy, the toolbar continues to display the button for these features. [#0564555]

System requirements for Receiver for HTML5 1.7

These are the supported Citrix product versions for this release and the requirements for users to access virtual desktops and hosted 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 following web browsers and operating systems to access desktops and applications using Receiver for HTML5.

Browsers

- Apple Safari 7
- Apple Safari 6
- Google Chrome 36 or later
- Microsoft Edge

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Microsoft Internet Explorer 11 (32-bit mode)
- Microsoft Internet Explorer 10 (32-bit mode)
- Mozilla Firefox 31 or later

Operating systems

- Windows 8.1 Pro and Enterprise (32-bit and 64-bit editions)
- Windows 8 Pro and Enterprise (32-bit and 64-bit editions)
- Windows 7 Service Pack 1 (32-bit and 64-bit editions)
- Mac OS X 10.9 Mavericks
- Mac OS X 10.8 Mountain Lion

Citrix server requirements

Receiver for HTML5 supports access to desktops and applications through the following versions of StoreFront. Stores must be accessed through Receiver for Web sites. Receiver for HTML5 does not support direct access to StoreFront stores, either using the store URL or the XenApp Services URL.

- StoreFront 2.6
- StoreFront 3.0

When users connect through NetScaler Gateway, Receiver for HTML5 can be used to access desktops and applications delivered by all the versions of XenDesktop and XenApp that are supported by StoreFront.

For direct connections through StoreFront without NetScaler Gateway, Receiver for HTML5 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. Receiver for HTML5 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.
Receiver for HTML5 now supports CloudBridge disabling compression and printer compression as well as using HDX Insight analytics to display in CloudBridge Insight Center.

- CloudBridge 7.3.1

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configure Receiver for HTML5

Mar 30, 2015

To enable users to access resources hosted on XenDesktop and XenApp in their browsers, you must create a StoreFront store and enable Receiver for HTML5. 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 HTML5 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 HTML5 supports Basic encryption only.

To enable connections to XenDesktop and XenApp using Machine Creation Services

If you plan to create machines using Machine Creation Services (MCS), on the master image, create a registry entry at HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\GroupPolicy\Defaults\ICAPolicies if it is not already present and then add the following registry keys.

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 gpresult command from a command prompt.

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

- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

To enable connections to XenDesktop and XenApp using Provisioning Services

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 HTML5 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 HTML5 users by increasing integration with XenDesktop and XenApp.

- 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 browser tab. 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 browser tab for viewing and printing from a locally attached printer.

1. If you plan to enable session sharing on your XenApp deployment, download the App Switcher installer. Ensure that .NET

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Framework 4.0.3 is installed and enabled, then install App Switcher on each machine providing applications for Receiver for HTML5 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 HTML5 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 enable Receiver for HTML5 on StoreFront

You must enable Receiver for HTML5 on the Receiver for Web site for the StoreFront store that provides the desktops and applications you want to make available to Receiver for HTML5 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 HTML5 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 HTML5 users and, in the Actions pane, click Deploy Citrix Receiver.
3. Enable Receiver for HTML5 by selecting one of the following options.
   - If want 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 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. If you changed the port used when you allowed WebSocket connections on XenDesktop or XenApp, complete the following steps to change the WebSocket port for the Receiver for Web site.
   1. 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\storenameWeb directory, where storename is the name specified for the store when it was created.
   2. Locate the following element in the file.
      `<html5 ... preferences="" ... />`
   3. Set the value of the preferences attribute to **wsPort:*portnumber*;**, where portnumber is the port that you configured in the policy.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Receiver for HTML5 user experience

Mar 30, 2015

Receiver for HTML5 integrates with Receiver for Web sites. To access their virtual desktops and hosted applications using Receiver for HTML5, users navigate to a Receiver for Web site using a compatible browser running on a supported operating system.

The user experience with Receiver for HTML5 is as follows:

- If you did not configure the site to always use Receiver for HTML5, the site attempts to determine whether Citrix Receiver is installed locally on devices running Windows and Mac OS X. When Citrix Receiver cannot be detected, users are prompted to download and install the appropriate Citrix Receiver for their platform. For users who are unable to install Citrix Receiver, this happens every time they log on to the Receiver for Web site. Users who already have Citrix Receiver installed locally must use this version to access resources from the site and are not given the option to use Receiver for HTML5. When you configure the Receiver for Web site to always use Receiver for HTML5, all users must access resources from the site through Receiver for HTML5 regardless of whether they have a locally installed version of Citrix Receiver.
- When users access a desktop or application through Receiver for HTML5, the resource starts in a new browser tab or window, according to the user's browser settings. You can configure Receiver for HTML5 so that resources are always started in the same tab as the Receiver for Web site. For more information, see To configure Receiver for HTML5 use of browser tabs.
- When a user starts an additional application, Receiver for HTML5 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.

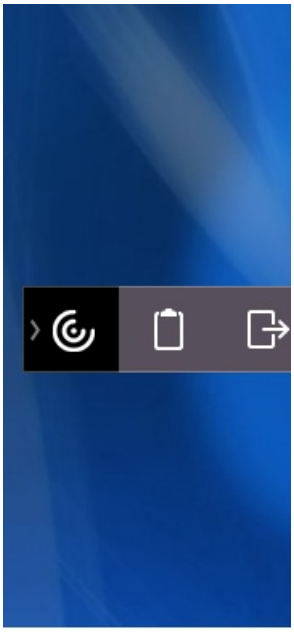
Session sharing

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.

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.

A floating toolbar containing controls for Receiver for HTML5 is displayed in the browser tab, as shown in the following figure. The clipboard button enables users to copy and paste Unicode plain text between the local clipboard on the device and the resource running in the browser. 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. Users can also send the CTRL+ALT+DELETE key combination to their desktops and applications using a button on the toolbar.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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. The file is removed from the device when the user closes the PDF.

A user who clicks a link in a document opened using a hosted application is given the choice of whether to open the URL in a hosted browser application within the session or to use the browser on the local device.

To view Receiver for HTML5 logs

To assist with troubleshooting issues, you can view Receiver for HTML5 logs generated during a session.

1. Log on to the Receiver for Web site.
2. In another browser tab or window, navigate to siteurl/Clients/HTML5Client/src/ViewLog.html, where siteurl is the URL of the Receiver for Web site, typically http://server.domain/Citrix/StoreWeb.
3. On the logging page, click Start Logging.
4. On the Receiver for Web site, access a desktop or application using Receiver for HTML5.
   The log file generated for the Receiver for HTML5 session is shown on the logging page. You can also download the log file for further analysis.

© 1999-2017 Citrix Systems, Inc. All rights reserved.