



Offline Plug-in for Windows 6.5

2015-02-24 13:40:51 UTC

© 2015 Citrix Systems, Inc. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

Contents

- Offline Plug-in for Windows 6.5** 3
 - New Features in This Release 5
 - System Requirements for Application Streaming..... 6
 - Deciding Which Receiver or Plug-in to Use for Application Streaming..... 9
 - Specifying Trusted Servers for Streamed Services and Profiles 11
 - Using the Merchandising Server and Citrix Receiver Updater to Deploy the Plug-ins . 14
 - To install the Offline Plug-in 15
 - To deliver the AppHubWhiteList to user devices..... 17
 - To create a virtual hard disk 18
 - To configure the cache size of the Offline Plug-in..... 20
 - To deploy the Offline Plug-in using the command-line 21
 - To configure an .MSI package for the Offline Plug-in using transforms 23
 - To deploy the Offline Plug-in to user devices through Active Directory 24
 - To deploy applications to user devices 25
 - To clear the streamed application cache on user devices..... 27
 - To clear merged rules for linked profiles on user devices 29

Offline Plug-in for Windows 6.5

The Offline Plug-in runs as a service on the user device to invoke applications the user selects and applications enumerated by Citrix Receiver or the Web Interface site. The Offline Plug-in finds the correct target in the profile in the App Hub, sets up the isolation environment on the user device, and then streams the application from the profile location to the safety of the isolation environment set up on the user device.

The Offline Plug-in installer does not require any configuration during installation, so those users who have administrator privileges on their computers can install it themselves.

The Offline Plug-in is installed by default on a server when you install XenApp. This enables the server for further configuration of streaming to server and dual-mode streaming.

To authenticate profiles accessed by the user devices, install the Offline Plug-in with a digital certificate. The Offline Plug-in then streams applications only from profiles that match the digital certificate. See also [Specifying Trusted Servers for Streamed Services and Profiles](#).

The Offline Plug-in also checks the cache size of the user device. If the cache size exceeds a maximum limit, the Plug-in removes streamed application files from the cache until its size is smaller than the limit. The default cache size limit is 1000MB (1GB) or 5% of total disk space, whichever is larger. The Offline Plug-in removes streamed application files starting with the one that was not used for the longest time.

The Offline Plug-in was previously known as the Streaming Client.

Finding the Version of the Offline Plug-in

To identify the version of your installed Plug-in, open the Windows program to add and remove programs and continue with the method for your operating system:

- For Windows Vista and Windows 2008, right-click a column heading and select More. In the Choose Details page, check to option to display the version.
- For earlier Windows operating systems, select Plug-in name, and click the link for support information.

To take advantage of the latest updates in application streaming, Citrix recommends installing the most current versions of the Offline and Citrix Receiver.

Related content

| | |
|---|---|
| Known Issues in XenApp 6.5 | Deciding Which Plug-in to Use for Application Streaming |
| System Requirements for Application Streaming | To install the Offline Plug-in |

| | |
|--|--|
| To configure the cache size of the Offline Plug-in | To deploy the Offline Plug-in using the command-line |
| To deliver the AppHubWhiteList to user devices | To deploy applications to user devices |

For information about profiling applications for streaming and then publishing them in XenApp, see the publishing section for your version of XenApp.

New Features in This Release

In addition to improved application compatibility on Microsoft Windows Server 2008 R2 SP1 and Windows 7 SP1, the 6.5 release provides the following enhancements for application streaming:

- **Increased support for streamed apps in pooled XenDesktop environments.** For faster application launch time on user devices, select the option to "Create a virtual hard disk" (VHD) while profiling. This feature copies the profile contents into the VHD and mounts it in the RadeCache location at application launch.
- **Compliance with new FIPS guidelines.** The Streaming Profiler in this release uses SHA-256 to create file hashes. To include SHA-1 hashes required by Offline Plug-ins 6.0, select the option for "Legacy Offline Plug-in support" while profiling.
- **Enhancements for creating AppHubWhiteList.** The registry key for creating the AppHubWhiteList is now consistent with other Citrix registry keys on 32-bit and 64-bit operating systems.
- **Ability to deliver AppHubWhiteList using Citrix Receiver Updater.** Ensure that unsigned profiles and services stream only from approved locations
- **AppCenter session reports include the names of streamed applications.** The reports of user sessions now include application names instead of just profile names.
- **Launch time improvements.** General performance improvements reduce launch time for streamed applications, including Microsoft Outlook.

System Requirements for Application Streaming

Version 6.5 of the Citrix Offline Plug-in and Streaming Profiler are supported on the following Microsoft operating systems:

- Windows XP Home and Professional editions, 32-bit edition, with Service Pack 3
- Windows XP Home and Professional editions, 64-bit edition, with Service Pack 2
- Windows Server 2008, 32- and 64-bit editions
- Windows Server 2003 R2
- Windows Server 2008 R2
- Windows Server 2008 R2, with Service Pack 1
- Windows Vista (Home, Business, Enterprise, and Ultimate editions), 32- and 64-bit editions, with Service Pack 1 or Service Pack 2
- Windows 7, 32-bit and 64-bit (Enterprise, Professional, Ultimate)

Version 6.5 of the Citrix Offline Plug-in and Streaming Profiler are supported on the following Citrix products:

Note: The list is accurate at the time of this release. For more information about supported versions, see:

<http://www.citrix.com/support/product-lifecycle/product-matrix>.

- Citrix XenApp 5, 6, and 6.5.
- Citrix XenDesktop 4, 5, and 5.5.
- Citrix XenServer: all supported versions.
- Citrix Receiver (Updater) for Windows 1.x, 2.x, and 3.0.
- Citrix Online Plug-in: Citrix recommends 13.0, which is installed with Citrix Receiver 3.0, but past versions 11.2 and 12.x are also supported.

The profiler workstation and user devices must meet the following requirements:

- Microsoft XML 2.0 installed (use Windows Update to ensure you installed all recent Internet Explorer updates).
- Standard PC architecture, 80386 processor or greater as required for the operating system.
- Administrator rights for the person installing.

- To profile and stream Microsoft Office applications to Windows Server 2003 operating systems, install the Windows Data Execution Prevention (DEP) hotfix on the server and profiling workstation. For information, see <http://support.microsoft.com/kb/931534>.

The profiler workstation must provide a run-time environment that is as close to your users' environment as possible. To stream applications to user devices, use the following guidelines for the profiling workstation:

- Choose a workstation that is a similar platform to your users' devices.
- Use a computer that is freshly reimaged so that there are no hidden files or registry settings for applications that you intend to profile.
- Install only the standard programs that are part of the company image, such as an antivirus program.
- Disable the User Account Control (UAC).
- To stream Microsoft Office 2007 or 2010 programs or to stream profiles enabled for inter-isolation communication, install .NET Framework 2.0 (3.0 or 3.5 optional).
- Do not install the Offline Plug-in on the profiler workstation. You can install Citrix Receiver.

Install the profiler in a path with single-byte characters only. Double-byte characters in the installation path are not supported.

The user devices must meet the following requirements:

- A network connection to the server farm, such as a network interface card (NIC).
- A supported browser: Microsoft Internet Explorer 6.0, 7.0, 8.0, or 9.0.
- To stream Microsoft Office 2007 or 2010 programs or to stream profiles enabled for inter-isolation communication, install .NET Framework 2.0 (3.0 or 3.5 is optional).
- Manually uninstall any previous version of the Streaming Client and Program Neighborhood Agent on user devices.
- To ensure availability of the features and functionality of XenApp for Windows Server 2008 R2 to your users, install the Offline Plug-in and the most recent version of Citrix Receiver (Enterprise), which includes the Online Plug-in. In addition:
 - Citrix recommends using Citrix Receiver Updater on user devices to install (and uninstall) Citrix plug-ins.
 - To stream applications to user desktops, install both the Offline Plug-in and Citrix Receiver (Enterprise) on user devices.
 - To stream applications to a server, install Citrix Receiver (Enterprise) on user devices. The Offline Plug-in is not required. If users launch applications from a Web Interface site, install Citrix Receiver (the Enterprise version is not needed) and add the site to the list of trusted sites.

Microsoft redistributable packages

The CitrixOfflinePlugin.exe and CitrixStreamingProfiler.exe installers include the following redistributables:

- Microsoft Visual C++ 2005 Redistributable Package 8.0.56336
- Microsoft Visual C++ 2005 Redistributable Package 8.0.50727.42
- Microsoft Visual C++ 2008 Redistributable Package 9.0.21022
- Microsoft Visual C++ 2008 Redistributable Package 9.0.30729
- Microsoft Visual C++ 2008 Redistributable Package 9.0.30729.4148

Backward compatibility. To take advantage of the latest updates in application streaming, Citrix recommends installing the most current versions of the Streaming Profiler, Citrix Plug-ins, and Citrix Receiver.

- Profiles created in the Streaming Profiler 6.5 are supported with:
 - Offline Plug-in 6.5
 - Offline Plug-in 6.0 (you must select the profiling option to support legacy Offline Plug-ins)
 - Note:** The Virtual Hard Disk feature is not supported for version 6.0.
 - Online Plug-in, which is included in Citrix Receiver 3.0 (with this release) or past versions 11.2 through 12.x.
- To continue using existing profiles with the plug-ins in this release, also install the latest profiler and update them (simply open them in the new profiler and re-save them).
- If upgrading is not possible, this release provides backward compatibility for streaming profiles created with profiler 5.2 through 6.0.

Streaming Microsoft Office 2007. For best practices for streaming Office 2007 applications, see <http://support.citrix.com/article/CTX118396> in the Citrix Knowledge Center.

Streaming Microsoft Office 2010. For best practices for streaming Office 2010 applications, see <http://support.citrix.com/article/CTX124565> in the Citrix Knowledge Center.

Update the profiler workstation and user devices with the latest Microsoft hotfixes, including:

- On Streaming Profiler workstations with Windows 7 (32-bit and 64-bit) only, download the hotfix from <http://support.microsoft.com/kb/2359223/en-US> (requires a computer restart).
- On Windows XP 32-bit platforms, install hotfix KB978835.
- On all Windows XP or Windows 2003 platforms, install hotfix KB973573. For more information, see <http://support.citrix.com/article/CTX124563> in the Citrix Knowledge Center.

Deciding Which Receiver or Plug-in to Use for Application Streaming

The delivery method for streaming that you select for published applications determines the Receiver and plug-ins to must install on servers and user devices.

Citrix recommends using the Citrix Receiver Updater to deliver the packages that you want to install on user devices:

Streamed to client desktops. With this method, you make available the full set of application streaming features. You can publish applications as "streamed to client" or any other method for streaming. When you stream applications directly to client desktops, some of the application files are cached locally and the application runs using the resources of the user device.

Install both the CitrixReceiverEnterprise.exe and CitrixOfflinePlugin.exe on user devices.

This combination enables you to:

- Enumerate published applications in the desktop Start menu and create shortcuts on the desktop.
- Provide dual-mode streaming. When you select "Streamed if possible, otherwise accessed from a server" and "Streamed to server," if streaming to the client desktop fails, applications automatically stream to a XenApp server and launch using the Citrix Receiver (Enterprise).
- Configure the application and users for *offline access*. When this configuration is completed, the entire application is fully cached on the user device. Users can disconnect from the network and continue using the application for the time specified in the offline license.

Accessed from a server. The profile is streamed from the App Hub to the XenApp server, where the Offline Plug-in is installed by default. The application displays on the user devices using the Receiver; the Offline Plug-in is not required on the user device. When you publish applications as "Accessed from a server" and "Streamed to server," users access the applications using the Receiver. This method does not support offline access to applications.

Select the package that fits your corporate needs:

- Install CitrixReceiverEnterprise.exe to stream applications to XenApp servers and launch them with the Receiver if you require native Program Neighborhood Agent (Applications in folders) or Smart Card authentication.
- Install CitrixReceiver.exe to stream applications to XenApp servers and launch them using Citrix Receiver self-service or a Web browser using a Receiver for Web or Web Interface site you create.

Important: For users to stream applications through a Web site using an Internet Explorer or Firefox browser, add the site to the trusted sites list in Internet Explorer on the user devices.

Streaming to a virtual desktop. To deliver applications to pooled XenDesktop environments, install both Receiver and the Offline Plug-in on the virtual desktop image. You must profile the applications with the option to create a virtual hard disk. When users launch the application, the profile contents are mounted in the RadeCache location from the AppHub.

- When profiling the application in the streaming profiler, select the option to [Create virtual hard disk](#).
- When publishing the application in XenApp, select the delivery option to stream to client desktop.

Note: Do not configure HTTP delivery for applications that stream to virtual desktops. Also, offline access is not supported on virtual desktops; if you enable offline access, the settings are ignored for this deployment.

- When creating the virtual desktop image, install both the CitrixReceiverEnterprise.exe and CitrixOfflinePlugin.exe.

Specifying Trusted Servers for Streamed Services and Profiles

To ensure that unsigned profiles and services stream only from approved locations, edit the registry on user devices to enable a whitelist of trusted servers:

- For unsigned profiles that include services, you must create a whitelist of approved server locations on the user device. If profiles attempt to stream a service from a location that is *not* on the whitelist, the service launch is denied and an event is sent to the event log.
- Optionally, to extend the whitelist requirement to unsigned profiles without services, create an additional registry setting.

Alternatively, signed profiles are always trusted, whether or not they include services, and a whitelist is not required for them.

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.

Creating a Whitelist of Locations for Unsigned Profiles with Services

To ensure that user devices run only *approved* services, edit the registry on user devices to enable a whitelist of approved server locations.

1. On the user device, create the following registry location:

64-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Rade

32-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Rade

Value: AppHubWhiteList

Type: REG_SZ

2. Add the server names (or local file system folder) plus the App Hub location in the registry value in a semicolon (;) or comma (,) delimited format, with or without spaces before or after the semicolon or comma.

For example:

- \\server\sharename
- \\server.example.net\sharename\directory

- `\\server.example.net\profiles`

If the application has been streamed from a web location (also called http streaming), the server name must be prefixed with http (or https) in the AppHubWhiteList registry entry. Also there is clear distinction between http and https servers.

That is, if a profile location is

`https://12.0.0.1/profiles/office/office.profile`, then the AppHubWhiteList must contain `https://12.0.0.1` or `https://12.0.0.1/profiles`.

The following examples are valid entries:

- `http://streamauto;https://12.0.0.1`
- `http://webshare.example.com/sharename`
- `12.0.0.1;streamauto;webshare.example.com`
- `12.0.0.1;c:\profiles;c:\folder with spaces;webshare.example.com`
- `12.0.0.1; c:\profiles; webshare.example.com`

After you create the registry entry and whitelist on user devices, unsigned profiles with services can load only from the locations on the whitelist. Signed profiles are always allowed.

Extending the Whitelist to Unsigned Profiles without Services

Optionally, to require all profiles, even those without services, to stream only from locations on the whitelist, after creating the registry entry and whitelist in the previous steps, create an additional registry entry:

1. On the user device, create the following registry location:

64-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Rade`

32-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Rade`

Value: `AppHubWhiteListRequired`

Type: `REG_DWORD`

2. Set the value:

- 1 - Enables the whitelist requirement to profiles without services
- 0 - Disables the whitelist requirement to profiles without services

After you create the registry entry and whitelist in the previous steps and then create and enable this registry entry on the user device, all unsigned profiles, with or without services, can load only from the locations on the whitelist. Signed profiles are always allowed.

Disabling Backward Compatibility

When you create a white list, by default, you can add both server names (as allowed by the 6.0 release) and the better protected share names (added in 6.5) to the AppHubWhiteList path. No registry change is needed for the default behavior.

To disable backward compatibility with the 6.0 release and allow only share names, create the following registry setting:

1. On the user device, create the following registry location:

64-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Rade\

32-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Rade\

Value: AppHubBackWardCompatible

Type: REG_DWORD

2. Set the value:

- 0 - Disables backward compatibility
- 1 - Enables backward compatibility

Note: To re-enable backward compatibility, either change the registry value or delete the registry entry.

Using the Merchandising Server and Citrix Receiver Updater to Deploy the Plug-ins

Citrix recommends using the Merchandising Server and Receiver Updater to deploy and update Receiver to a user device.

Citrix Merchandising Server administrator console. With the administrator console, you can upload the Receiver installation and metadata files, create reusable rules to define the delivery recipients, and create deliveries.

Citrix Receiver Updater client (Receiver Updater for Windows). After users install Receiver Updater on their user devices, Receiver Updater installs, updates, and starts Receiver without user interaction.

Users having the correct permissions to manage their Receiver can change the Citrix XenApp server that hosts their published resources. Right-click the Receiver icon in the Windows notification area and choose Preferences, then right-click the Citrix Receiver entry in the Plug-in Status, and choose Change Server.

Important: For Firefox to work correctly with Receiver for Windows, ensure that you or the user install Firefox before installing Receiver. If Receiver is already installed, uninstall it, install Firefox, and reinstall Receiver. Also ensure that the whitelists of trusted and untrusted servers contain the XenApp and Web Interface server names.

Upgrading Receiver with Receiver Updater

Updates are, by default, automatically installed on the user device. When an update is available, the Receiver Updater downloads and installs the updated Receiver.

Uninstalling Receiver with Receiver Updater

Receiver Updater upgrades Receiver when a newer Receiver is available. When users remove the Receiver Updater manually from the Add/Remove Programs utility (or Programs and Features for Windows Vista or Windows 7), Receiver is also removed. Additionally, the administrator can remove the Receiver Updater and all of its managed plug-ins through the Administrator Console.

For more information, see the Receiver Updater for Windows documentation.

To install the Offline Plug-in

Citrix recommends delivering the Offline Plug-in to user devices through the Receiver Updater. If users install the Receiver Updater, they should also update or remove plug-ins using only the Receiver Updater (instead of the Windows uninstall program). However, you can install the plug-in manually.

The CitrixOfflinePlugin.exe installer (formerly an .msi file) includes improvements for Microsoft Office applications and Microsoft Redistributable Packages.

Important: Before you install the Offline Plug-in, refer to the system requirements for application streaming for the supported platforms, system prerequisites, and the Microsoft redistributable packages included with the installation.

The Citrix installation media contains installation files for Citrix plug-ins in the Citrix Receiver and Plug-ins directory. The latest plug-ins are also available from the [Citrix Support Web site](#).

To take advantage of continuing improvements in the profiler, when you upgrade to the latest Offline Plug-in, also upgrade to the latest *Streaming Profiler* and either update your existing applications or re-profile the applications in the new profiler.

In addition, Citrix provides command-line utilities and transforms with the Offline Plug-in to perform actions on user devices.

Use one of the following methods:

- **Installing using the Receiver Updater.** Citrix recommends using the Receiver Updater to install plug-ins, which lets you deliver and update plug-ins automatically with the Merchandising Server. The Receiver Updater upgrades plug-ins when a newer version is available. For more information, see the section for Merchandising Server.
- **Installing manually.** The Offline Plug-in installer deploys drivers and requires administrator privileges on the user devices. For users who have administrator privileges, you can make the plug-in installer available, and they can install it themselves. The plug-in installer does not require any configuration during installation.

To install the Offline Plug-in manually

1. From the installation media or Citrix download site, navigate to Citrix Receiver and Plug-ins > Windows > Offline Plug-in and run CitrixOfflinePlugin.exe.

Note: On Microsoft Windows Server 2003 or 2008, Active Directory manages resources across the domain. These computers can handle only .msi files, not .exe files. For these platforms, select the .msi installer.

2. If the installer detects an installed version, the installer can upgrade or repair the installation.
3. Choose the language in which you want the plug-in installer to run. In this step, you are choosing the language for the installer, not the language of the plug-in.

To install the Offline Plug-in

4. After the Welcome screen, accept the license agreement and continue with the installation wizard.
5. After you finish the installation, restart the user device.

When you restart the user device, the Citrix Streaming Service (Ctx_StreamingSvc) starts automatically and runs in the background. Restarting the user device also ensures that other applications and plug-ins detect the Offline Plug-in.

To remove the Offline Plug-in

- If you used the Receiver Updater to install the plug-in, use only the Receiver Updater to remove it.
- If you installed the plug-in manually, you can uninstall it using the Windows uninstall program.

When users uninstall the Receiver Updater manually from their devices, all plug-ins are also removed. Additionally, the administrator can remove the Receiver Updater and all of its managed plug-ins through the Administrator Console.

To deliver the AppHubWhiteList to user devices

If you create an AppHubWhiteList to specify trusted servers for streamed services and profiles, beginning with the Offline Plug-in 6.0.2, use these methods to deliver the AppHubWhiteList along with the Offline Plug-in to user devices:

- If you manually install the Offline Plug-in 6.5 using command line parameters, during the installation, add the parameter CTX_APPHUB_WHITELIST and the IP address, FQDN, shared folders, folder on drive, and Web server address:

For example:

```
"[path]/CitrixOfflinePlugin.exe" /C:"setup /qr  
CTX_APPHUB_WHITELIST=" " "  
\\10.105.68.11\AppHub;C:\profiles;C:\folder with  
spaces;http://www.webshare.organization.com" " "
```

- If you manually install the Offline Plug-in 6.0.2 using command line parameters, during the installation, add the parameter CTX_APPHUB_WHITELIST and the IP address or FQDN of the share drive, and HTTP/HTTPS server path.

For example:

```
"[path]/CitrixOfflinePlugin.exe" /C:"setup /qr  
CTX_APPHUB_WHITELIST=" "10.105.68.11; webshare.organization.com;ht  
tp://www.webshare.organization.com;https://www.webshare.organizatio  
n.com" " "
```

- To deploy the AppHubWhiteList when users install the Offline Plug-in using Receiver, configure the AppHubWhiteList (optional parameter) in Citrix Merchandising Server. For more information, locate the Receivers and Plug-ins > Merchandising Server section and review *Configuring Plug-in Parameters*.

For more information about creating the AppHubWhiteList, see [Specifying Trusted Servers for Streamed Services and Profiles](#).

To create a virtual hard disk

For pooled XenDesktop environments, in the profiling wizard, Citrix recommends using the option to Create virtual hard disk (VHD) for this target to improve application launch time. This option is not needed in other deployments, but if enabled, it does not interfere with normal behavior.

Tip: If selected, the profiling workstation and the App Hub need up to twice the amount of disk space available as is normally used for the profile.

In addition to creating the normal directory files, this option creates a virtual hard disk (VHD) while profiling. If selected, the first time users launch the application:

- In pooled XenDesktop environments, the Offline Plug-in checks the UseVHD registry setting, and if it is set to mount the VHD, the launch copies all profile contents to the VHD in the RadeCache location in the App Hub. Subsequent launches access the files stored on the VHD, which speeds up launch time.

Note: If you provisioned the pooled XenDesktop through Citrix Provisioning Server or XenDesktop Controller, the Offline Plug-in automatically detects the need to mount the VHD, regardless of this setting.

- In other environments, the application launches from the directory files in the App Hub, as usual.

This option does *not* support:

- Applications streamed using HTTP protocol
- Offline access to streamed applications

For linked profiles (those enabled for inter-isolation communication), an application launches from a VHD only if the option is enabled for its individual profile. For example, if you profile the first application and select the VHD option, and then link the profile to a second profile without the VHD option, only the first application launches from the VHD; the second application launches from the directory files in the App Hub, as usual.

To unmount the VHD

With administrator privileges, from the command-line, use either of the following commands:

- `radecache /flush:GUID`
- `radecache /flushall`

To mount the VHD on non-pooled XenDesktop devices

If the RadeCache location for the "local" hard disk is across the network to a virtual infrastructure, you can manually set the UseVHD registry to mount the VHD (recommended by Citrix).

On the user device, create the registry key:

- For 32-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Rade\UseVHD
- For 64-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Rade\UseVHD

Set a DWORD value:

- 0: Do not mount (default on non-pooled XenDesktop devices).
- 1: Mount occurs. The VHD attempts to be mounted in the RadeCache folder at the time of sandbox creation.

To configure a fallback method manually

For situations where the VHD fails to mount, you can create a registry key with a fall-back option:

- For 32-bit: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Rade\ VHDErrorFallback
- For 64-bit:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Rade\VHDErrorFallback

Set a DWORD value:

- 0: Deny application launch if there is no VHD or mounting the VHD failed because of any other reason.
- 1: If the VHD is not present, launch the application, but if the VHD cannot be mounted, deny application launch (default behavior, even if registry entry is not created).
- 2: Launch the application.

To configure the cache size of the Offline Plug-in

When you run a streamed application either through Citrix Offline Plug-in or from a Web page created through the Web Interface, by default, the Plug-in caches application files on the primary, local drive of the user device at the following location:

`%PROGRAMFILES%\Citrix\RadeCache`

Before caching files, the Plug-in checks the size of this cache. If the cache size exceeds a maximum limit, the Plug-in removes streamed application files from the cache until its size is smaller than the limit. The Plug-in removes streamed application files starting with the one that was least recently used.

The default cache size limit is 1000MB (1GB) or 5% of total disk space, whichever is larger.

To change the default cache location or the default maximum cache size, use the ClientCache tool that you run on the user device where the Plug-in is installed.

To start the tool, run the following program:

`%PROGRAMFILES%\Citrix\Streaming Client\ClientCache.exe`

Running ClientCache.exe on the computer on which the Offline Plug-in is installed enables you to change the location of the cache and the maximum cache size. Entries you make using ClientCache.exe are stored in the registry and become the new defaults.

The following are some guidelines for changing these defaults:

Client cache directory. The cache location you specify must be on a local drive and can be on a volume other than the main volume.

Maximum client cache size. When specifying a cache size, use an integer representing the cache size in megabytes. For example, the following represents two gigabytes: 2000.

The maximum size of the cache is restricted to the size of the local drive.

Changes you make using this tool take effect the next time you start the Plug-in or restart the Citrix Streaming Service.

To deploy the Offline Plug-in using the command-line

To deploy the Offline Plug-in to user devices, use Microsoft System Management Server (SMS) or Microsoft Active Directory Services.

See <http://www.microsoft.com> for instructions about how to use these products to deploy applications.

To deploy the plug-in using command-line parameters, use the following steps:

1. On the computer where you want to install the Plug-in package, type the following at a command prompt to open the Offline Plug-in file and extract the CitrixOfflinePlugin.msi file:

```
"[path]/CitrixOfflinePlugin.exe" /C:"setup [Options]"
```

where *path* is the location of the .exe file.

2. Set the options. [Options] can be any of the traditional MSI command-line parameters. Set your extraction options as needed. Examples of parameters that are supported:

- /Q suppresses the extraction dialog box.
- /T: *full path* specifies the temporary working folder in which to extract the files.
- /C extracts files only to the folder when used also with /T. Use this only if you are not including a command-line.
- /C: [*Cmd*] overrides the install command, where *Cmd* is the command-line that runs after extracting the files to the temporary folder.

For *Cmd*, set command-line properties as needed. The following properties are supported to set the user interface level and other options:

- /qn executes a completely silent installation; no user interface.
- /qb shows simple progress and error handling; a basic user interface.
- /qf shows a full user interface (default).
- /qz shows a reduced user interface.
- /l ""[*logfile*]"" creates a verbose install log where *logfile* is the path and filename for where to save the log. Use double double-quotes for a path with spaces.
- /norestart prevents restarting of the user device following the installation.

To deploy the Offline Plug-in using the command-line

- `/restart` initiates a restart automatically (without prompting) upon successful completion of the installation.

Locations with spaces must be enclosed with quotes; however, only single sets of double quotes are allowed, and nested double quotes causes the command to fail. In cases where a nested quote is required inside the double quotes, use double double-quotes on each end of the expression.

Type the following at a command prompt, where `package` is the name of the Windows Installer installation package and `TransformList` is the list of the transforms that you want to apply:

```
CitrixOfflinePlugin /I package TRANSFORMS=[TransformList].mst
```

If you are applying multiple transforms, separate each transform with a semicolon.

The following examples demonstrate valid command-lines:

- To simply extract files: `"path\CitrixOfflinePlugin.exe" /C /T:"c:\Documents and Settings\Administrator\Desktop\Streaming Client"`
- To run a silent install with no options: `"path\CitrixOfflinePlugin.exe" /C:"setup /qr"`
- To add some options: `"path\X CitrixOfflinePlugin.exe" /C:"setup /qr INSTALLDIR=""C:\Program Files\Citrix\Streaming Client"" /norestart /l ""c:\Log Files\streaming.log"""`
- With some options and a transform: `"path\CitrixOfflinePlugin.exe" /C:"setup /qr INSTALLDIR=""C:\Program Files\Citrix\Streaming Client"" /norestart /l ""c:\Log Files\streaming.log"" TRANSFORMS=""C:\some_transform.mst"""`

To configure an .MSI package for the Offline Plug-in using transforms

Transforms manipulate the installation process by making changes to the installation database contained within a Windows Installer package. The following procedure should be attempted only by those familiar with transforms and their impact upon these settings.

1. After extracting the CitrixOfflinePlugin.msi file in a temporary folder, use Orca or your preferred tool for editing Windows Installer packages to open the .msi package.
2. Enter new values for the properties you want to change in the Property table.
3. Generate the transform file and save it with an .mst file extension.
4. To install the MSI package and use the transform you just created, follow the same steps as outlined above in the procedure dealing with command-line installations; that is, add the properties to the command-line. Additionally, however, you must add the following

```
PROPERTY=value
```

Here is an example:

```
TRANSFORMS="path\my.mst"
```

where *path* is the location of the transform and *my.mst* is its file name.

The following example demonstrates a valid command-line:

```
PROPERTY=Value | ANOTHER_PROPERTY="“a value with spaces””
```

To deploy the Offline Plug-in to user devices through Active Directory

On Microsoft Windows Server 2003 or 2008, Active Directory manages resources across the domain. These computers can handle only .msi files, not .exe files.

To install the Citrix Offline Plug-in on these user devices with an equivalent installation as with the .exe installation, use the following steps to apply a transform contained in the self-extracting package. You must be a domain administrator.

1. To extract the installation files to a file share, run:

```
CitrixOfflinePlugin.exe /C /T:"[fileshareDirectory]"
```

where the *fileshareDirectory* is the UNC path to a shared folder that is accessible to all the domain user devices on which you will install the Offline Plug-in.

2. From a computer in the domain:

- On Windows Server 2003, from Administrative Tools, open Active Directory Users and Computers, right-click the organizational unit, and select Properties. From the Group Policy tab, click New.
- On Windows Server 2008, open Group Policy Management, right-click Group Policy Objects, and select New.

3. Name the policy and click Edit.

4. In the Group Policy Object (or Management) Editor, under Computer Configuration > Software Settings, right-click Software installation.

Note: Assigning the package to a User Configuration is not supported.

5. Select New and then select Package.

6. In the Open dialog box, browse to the file share location and select XenAppStreaming.msi.

7. After selecting Open, select the Advanced deployment method.

8. After the properties dialog box opens, from the Modifications tab, click Add and then double-click streaming_client_ad.mst to open the transform.

This installation performs the equivalent installation of CitrixOfflinePlugin.exe, including installing the Offline Plug-in, starting the Citrix Streaming Service, and adding the Microsoft Visual C++ 2005 Redistributable Package on all user devices in the domain.

To deploy applications to user devices

Citrix recommends that administrators deploy the applications used most frequently by end users. Deployment pushes new or updated application files to user devices and helps avoid overloading the file servers or network. The utility enables administrators to schedule deployment overnight or during off hours. The Offline Plug-in located on the installation media includes the deployment utility called RadeDeploy.exe. After you install the plug-in, locate the utility in \Program Files\Citrix\ directory.

1. On the user device that has the Offline Plug-in installed, open a command prompt. Enter the path to locate the manifest file (.profile) on the network file share or Web server, using the following examples:

```
radedeploy /deploy:\\2003Server\packages\adobe\adobe.profile
```

```
radedeploy  
/deploy:"https://2003server/webpackages/office/office.profile"
```

The utility automatically selects the correct target for the user device and deploys the necessary files.

2. Set any additional commands. The following additional commands are available:

```
radedeploy /enum
```

```
radedeploy [-m] /deploy:profilename
```

```
radedeploy [-p] /delete:appname or profilename
```

where *appname* is the name of the application and *profilename* is the name of the profile as listed using the `radedeploy /enum` command, either a .profile or .rad file. Profile names with embedded spaces should be quoted, such as `deploy:"my profile"`.

Note: The `/delete` command does not delete subprofiles that are linked to inter-isolation communication profiles running on the user device. Instead, you must delete the inter-isolation communication profile that includes the linked profile.

3. Set your options as needed, including the following parameters:
 - `/enum` enumerates the applications currently deployed on the user device.
 - `/deploy` adds the profiled application on the user device.
 - `/delete` removes the profiled application from the user device.
 - `-m` monitors the deployment until complete.
 - `-p` deletes the application profile from the user device. Note that this command also removes any other applications deployed on the user device from this application profile.
4. Repeat for other applications, as needed.

To deploy applications to user devices

Alternatively, run the command-line in third-party software, such as Microsoft System Management Server (SMS) or Microsoft Active Directory Services (ADS) to deploy applications.

To clear the streamed application cache on user devices

Use the RadeCache command-line utility to clear the streamed application cache on user devices. For example, free space in the application cache or start with an empty cache while troubleshooting streaming issues. The RadeCache utility is included in the CitrixStreamingProfiler.exe and is installed automatically on the user device in Program Files > Citrix.

Note: Before using the RadeCache command, make sure that the application programs and processes are terminated on the user device. For large applications such as Microsoft Office, this can take up to 10 minutes.

1. On the computer where you want to clear the cache, type the following at a command prompt:

```
radecache [-i] [-if] [-ir] [-u] [-uf] [-ur]
```

```
[/flush:GUID]
```

```
radecache [/flushall]
```

```
radecache
```

```
radecache [/?]
```

where *GUID* is the unique GUID for the application streamed to user devices. GUIDs must not include spaces.

2. Set your options as needed, including the following parameters:

- `/?` displays the syntax for the utility and information about the options of the utility
- `-i` clears the registry and files in the install root
- `-if` clears only files in the install root
- `-ir` clears only the registry in the install root
- `-u` clears the registry and files in the user root
- `-uf` clears only the files in the user root
- `-ur` clears only the registry in the user root
- `/flush:GUID` clears the registry and files in both the install root and user root for the streamed application, and, for an application for pooled XenDesktop environments, unmounts the VHD

To clear the streamed application cache on user devices

- `/flushall` clears the registry and files in both the install root and user root for all streamed applications, and, for applications for pooled XenDesktop environments, unmounts the VHD

3. Repeat for other applications, as needed.

This method affects only the local user device.

To clear merged rules for linked profiles on user devices

The RadeStore folder contains the repository of registry hives, registry tab files, fonts, scripts, and merged rules of inter-isolation communication (IIC) profiles. If any of the execution targets of the IIC profile is updated, the merged rules are invalidated and then rebuilt automatically. Fonts are registered for each session from the RadeStore location.

The RadeStore location is created when you install the CitrixOfflinePlugin.exe on user devices. Clear the RadeStore location manually, as needed, such as when troubleshooting application issues for users.

To clear the RadeStore location:

1. On the computer where you want to clear the storage location, type the following at a command prompt:

```
radecache /flushstore:{all|rules|hives|tabs|fonts|scripts}
```

2. Set your options as needed, including the following parameters:

- `rules` clears the merged rules in the RadeStore location
- `hives` clears the registry hives in the RadeStore location
- `tabs` clears the registry tab files in the RadeStore location
- `fonts` clears fonts in the RadeStore location
- `scripts` clears scripts in the RadeStore location
- `/all` clears the merged rules, registry hives, registry tab files, fonts, and scripts in the RadeStore location

3. Repeat for other RadeStore locations, as needed.

This method affects only the local user device.