Application Streaming 6.6 for Windows
## Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Streaming 6.6 for Windows</td>
<td>5</td>
</tr>
<tr>
<td>Publishing Applications for Streaming</td>
<td>6</td>
</tr>
<tr>
<td>About the Offline Plug-in 6.6 and Streaming Profiler 6.6</td>
<td>8</td>
</tr>
<tr>
<td>System Requirements for Application Streaming</td>
<td>10</td>
</tr>
<tr>
<td>Application Streaming Overview</td>
<td>13</td>
</tr>
<tr>
<td>Components for Application Streaming</td>
<td>15</td>
</tr>
<tr>
<td>Evaluating Application Delivery Methods</td>
<td>18</td>
</tr>
<tr>
<td>Deciding Which Receiver or Plug-in to Use for Application Streaming</td>
<td>21</td>
</tr>
<tr>
<td>Providing Single Sign-on for Streamed Applications</td>
<td>23</td>
</tr>
<tr>
<td>Creating Application Profiles</td>
<td>24</td>
</tr>
<tr>
<td>Targets Overview</td>
<td>26</td>
</tr>
<tr>
<td>Service Pack Level</td>
<td>28</td>
</tr>
<tr>
<td>System Drive Letter</td>
<td>29</td>
</tr>
<tr>
<td>Operating System Language</td>
<td>30</td>
</tr>
<tr>
<td>Inter-Isolation Communication Overview</td>
<td>31</td>
</tr>
<tr>
<td>Isolating Services</td>
<td>32</td>
</tr>
<tr>
<td>Specifying Trusted Servers for Streamed Services and Profiles</td>
<td>33</td>
</tr>
<tr>
<td>Managing Isolation Environment Rules</td>
<td>36</td>
</tr>
<tr>
<td>Types of Isolation Environment Rules</td>
<td>37</td>
</tr>
<tr>
<td>Restrictions and Limitations for Rules</td>
<td>39</td>
</tr>
<tr>
<td>Creating Isolation Environment Rules for a Target</td>
<td>40</td>
</tr>
<tr>
<td>To create an isolation environment rule</td>
<td>41</td>
</tr>
<tr>
<td>To modify a rule</td>
<td>42</td>
</tr>
<tr>
<td>Using Environment Variables to Construct Rules</td>
<td>43</td>
</tr>
<tr>
<td>Preparing a Workstation for Profiling Applications</td>
<td>45</td>
</tr>
<tr>
<td>Known Limitations for Profiling</td>
<td>47</td>
</tr>
<tr>
<td>To install the profiler</td>
<td>48</td>
</tr>
<tr>
<td>To disable and enable profile signing</td>
<td>49</td>
</tr>
<tr>
<td>To start the profiler</td>
<td>50</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Creating a Profile and Its Initial Target</td>
<td>51</td>
</tr>
<tr>
<td>To create a profile and target</td>
<td>52</td>
</tr>
<tr>
<td>To allow users to update applications</td>
<td>55</td>
</tr>
<tr>
<td>To set up inter-isolation communication</td>
<td>56</td>
</tr>
<tr>
<td>To select an install option</td>
<td>58</td>
</tr>
<tr>
<td>To install multiple applications through Advanced Install</td>
<td>59</td>
</tr>
<tr>
<td>To choose an installation program for the application</td>
<td>60</td>
</tr>
<tr>
<td>To create a virtual hard disk</td>
<td>62</td>
</tr>
<tr>
<td>To support legacy plug-ins</td>
<td>64</td>
</tr>
<tr>
<td>To install Internet Explorer plug-ins</td>
<td>65</td>
</tr>
<tr>
<td>To include files and folders in a target</td>
<td>66</td>
</tr>
<tr>
<td>To include registry settings</td>
<td>67</td>
</tr>
<tr>
<td>To install an application in the profile</td>
<td>68</td>
</tr>
<tr>
<td>To run an application in the profiler</td>
<td>69</td>
</tr>
<tr>
<td>To select applications for listing in the profile</td>
<td>70</td>
</tr>
<tr>
<td>To sign a profile</td>
<td>71</td>
</tr>
<tr>
<td>Editing Profiles</td>
<td>72</td>
</tr>
<tr>
<td>To view profile information</td>
<td>73</td>
</tr>
<tr>
<td>To edit the profile name, description, or location</td>
<td>74</td>
</tr>
<tr>
<td>To view details about applications in a profile</td>
<td>75</td>
</tr>
<tr>
<td>To view File Type Associations set in a profile</td>
<td>76</td>
</tr>
<tr>
<td>To check for launch prerequisites</td>
<td>77</td>
</tr>
<tr>
<td>To check for prerequisite registry entries</td>
<td>78</td>
</tr>
<tr>
<td>To check for prerequisite applications and files</td>
<td>80</td>
</tr>
<tr>
<td>To specify pre-launch and post-exit scripts</td>
<td>81</td>
</tr>
<tr>
<td>To add a target to a profile</td>
<td>82</td>
</tr>
<tr>
<td>To resolve target conflicts</td>
<td>83</td>
</tr>
<tr>
<td>To resolve invalid shortcuts</td>
<td>85</td>
</tr>
<tr>
<td>To delete a target from a profile</td>
<td>86</td>
</tr>
<tr>
<td>To delete a folder from a profile</td>
<td>87</td>
</tr>
<tr>
<td>To remove a profile from a linked profile</td>
<td>88</td>
</tr>
<tr>
<td>Editing Targets</td>
<td>89</td>
</tr>
<tr>
<td>To edit the target name and description</td>
<td>90</td>
</tr>
<tr>
<td>To modify the application properties in the target</td>
<td>91</td>
</tr>
<tr>
<td>To modify the operating system and language properties of a target</td>
<td>93</td>
</tr>
<tr>
<td>To update a target</td>
<td>94</td>
</tr>
<tr>
<td>To remove an old version of an updated target</td>
<td>95</td>
</tr>
</tbody>
</table>
Application Streaming 6.6 for Windows

In This Section

Application streaming simplifies application delivery to users by virtualizing applications on client devices. Administrators can install and configure an application centrally and deliver it to any desktop on demand.

Use the application streaming feature to install and configure an application on one file server in your App Hub, publish the application using the XenApp publishing wizard, and deliver it to any desktop or server on demand. To upgrade or patch an application, you make the updates only in the location where you stored the application. Application streaming augments application delivery not only to user desktops and virtual desktops, but also to servers in your server farms.

<table>
<thead>
<tr>
<th>About This Release</th>
<th>Includes the new features in this release and the known issues.</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Requirements for Application Streaming</td>
<td>Read about the system requirements for the streaming components on your servers and user devices.</td>
</tr>
<tr>
<td>Creating Application Profiles</td>
<td>Install the streaming profiler to profile applications for streaming.</td>
</tr>
<tr>
<td>Deciding Which Plug-in to Use for Application Streaming</td>
<td>After you decide how to stream applications to users, learn what plug-ins are needed.</td>
</tr>
<tr>
<td>Offline Plug-in 6.6</td>
<td>Install the Offline Plug-in on servers and user devices to stream published applications.</td>
</tr>
</tbody>
</table>

For more information about how to publish applications for streaming, locate your version of XenApp and review the topics about using the Publish Applications wizard and managing the applications properties.

Can’t find what you’re looking for? If you’re looking for documentation for previously released versions of this product, go to the Citrix Knowledge Center. For a complete list of links to all product documentation in the Knowledge Center, go to http://support.citrix.com/. 
Publishing Applications for Streaming

After you create profiles for applications using the Streaming Profiler, you make them available for streaming to users by publishing the applications.

The Publish Application wizard in the Citrix AppCenter guides you through the process of selecting the streaming options. Configure the application streaming delivery method as you publish the application. Choose delivery options based on the users who will access the applications and their environments.

The profiled applications must be stored on a file share or Web server that is accessible from your XenApp server so you can publish the application, and it must be accessible by your users so they can launch the application.

Streaming Applications to User Devices

If you deliver streamed applications directly to user desktops, users can launch the streamed applications, which run in an isolation environment on their desktops and use local resources to run the applications. This delivery method offers the full set of application streaming options including desktop integration and offline access.

Before publishing an application to be streamed to client desktops, complete the following tasks:

- Install the Offline Plug-in locally, where it runs in the background to enable application streaming.
- Install the latest version of online plug-in locally.
- To stream to client devices across a network protected by a firewall, configure firewall policies to allow those applications access.

After all of these tasks are complete, publish the application as Streamed to client.

Streaming Applications to a XenApp Server

To simplify application delivery to servers in a server farm, stream applications to a XenApp server and virtualize the applications through an ICA connection to user devices.

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.

Before publishing an application that is streamed to server, ensure your Web Interface sites and Citrix XenApp sites are configured to run one of the following application types:

- Remote applications only, or
- Dual mode streaming (streamed if possible, otherwise accessed from a server)
Publishing Applications for Streaming

For information about managing application types on Web Interface sites, see *Technologies > Web Interface*.

After you ensure all of these tasks are complete, publish the application as *Streamed to a server*. 
About the Offline Plug-in 6.6 and Streaming Profiler 6.6

Readme Version: 1.0

What's New

In addition to general improvements, this release includes:

- Support for Microsoft Office 2010, Service Pack 1
- Support for Citrix personal vDisk
- Support for ShareFile Plug-in for Citrix Receiver

Fixed Issues

For a list of issues fixed in this release, see http://support.citrix.com/article/CTX124164 in the Citrix Knowledge Center.

Known Issues

- On pooled Windows XP XenDesktops, the RadeCache flush command does not flush the streamed contents. As a workaround, restart the pooled Windows XP XenDesktops and try the command again.

- On Windows 7 platforms, a locally installed Citrix ShareFile plug-in might fail to integrate when users stream Microsoft Outlook 2010. As a workaround, an administrator can add the ShareFile Adxloader.dll manually on the local device. To do this, in Outlook, from the File menu, select Options > Add-ins. In Manage COM Add-ins, click Go, and then click Add. Browse to "C:\Program Files\ShareFile\OutlookPlugins" and select Adxloader.dll. Alternatively, install the ShareFile plug-in locally on the user device. [#0269975]

- Automatic updates of some streaming applications fail on virtual desktops. For example, users can install and use Skype as a streamed application on their virtual desktops, but when prompted to update it, reinstallation may fail. As a workaround, while profiling the application, disable the third-party application's automatic update feature. When a new version of the application is released, update the profile and make it available to users. [#0276497]

- Before planning for Citrix personal vDisk Reset operation, run the RadeCache /Flushall command to clear the cache to prevent void mount points. [#0273501]
Issues for Profiling and Streaming Microsoft Applications


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

- Profiling and launching streamed Office 2010 applications on Windows Server 2003 and XP operating systems require Microsoft hotfixes. Symptoms of missing hotfixes include error messages appearing while profiling Office 2010 applications, or application launch on the user device consuming 100% of the CPU on the device. These third-party issues occur if you install Microsoft security update KB956572, but not the hotfixes KB973573 or KB978835 that correct a problem. [#229982, 227925]

To profile or stream Office 2010 applications, install these hotfixes on profiler workstations and user devices:

- Streaming Profiler 6.5 workstations only with Windows 7 (32-bit and 64-bit), download the hotfix from http://support.microsoft.com/kb/2359223/en-US (requires a computer restart). [#248727]

- 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.
System Requirements for Application Streaming

Version 6.6 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 6.6 of the 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, 5.5, and 5.6.
- Citrix XenServer: all supported versions.
- Citrix Receiver Updater for Windows 1.x, 2.x, and 3.x.
- Citrix Online Plug-in: Citrix recommends 13.0, which is installed with Citrix Receiver 3.0 and 3.1, 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 6.6 are supported with:
  - Offline Plug-in 6.5 and 6.6
  - 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 6.5.


**Streaming Microsoft Office 2010.** For best practices for streaming Office 2010 applications, see [http://support.citrix.com/article/CTX124565](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 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](http://support.citrix.com/article/CTX124563) in the Citrix Knowledge Center.
Application Streaming Overview

Application streaming simplifies application delivery to users by virtualizing applications on client devices. Administrators can install and configure an application centrally and deliver it to any desktop on demand.

Use the application streaming feature to install and configure an application on one file server in your App Hub, publish the application using the XenApp publishing wizard, and deliver it to any desktop or server on demand. To upgrade or patch an application, you make the updates only in the location where you stored the application. Application streaming augments application delivery not only to user desktops, but also to servers in your server farms.

Application streaming offers the following features:

**Install once, deliver anywhere**

Provides the ability to install an application once on a profiler workstation and have it replicated to file servers within the existing enterprise infrastructure. Once there, the applications are delivered to client devices that request access to the application, on-demand, as a result of end-user activity.

**Seamless updates**

No need to profile applications again. Updates are as simple as updating an application on a desktop using the update program supplied by the manufacturer. The update is performed once on the profiler workstation and delivered to client devices in a manner similar to that used in the initial delivery.

**Application isolation**

All streamed applications run within isolation environments that keep the applications from interfering with others running on the same client device. The isolation environment is specific for the application and user session, regardless of whether the user streams to the local client or virtualizes the streamed application from a server. The specific data files of the application, such as INI files and registry keys, are all isolated and maintained centrally for the streamed application.

**Application caching**

Application files can be cached on the client device to allow faster access the next time the application is launched. Before an application runs, cached files are updated automatically if there is a newer version on the file server. Note that application caching is strictly for performance reasons; there is no requirement to have the application cached for the application to run.

**Wide range of target environments**

Nearly any modern Windows platform can host a streamed application. Specifically, supported operating systems include Windows XP Professional, Windows Server 2003 and 2008, Windows Vista, and Windows 7. With dual mode streaming, target environments are
increased to include all supported XenApp client desktops.

**Dual mode streaming**

Configure XenApp to stream software to client devices; otherwise, virtualize from a XenApp server. If launching a streamed application fails on the client device, XenApp seamlessly streams the application to the server and virtualizes the application on the client device from XenApp.

**Easy delivery of applications to farm servers**

When publishing applications in a server farm, choose to virtualize applications from XenApp, which can simplify application delivery. Instead of installing applications on your farm servers, you stream them to XenApp from a central file share in your App Hub. Update the application in the central location, and you update the application on all the farm servers.

**Consistent end-user experience**

Applications that can be accessed through the server appear next to other applications that the user is accustomed to either within the Web Interface, Citrix plug-ins, or on the desktop. The user does not have to know where and how the application is executing.

**Offline access**

Once configured and delivered, applications are available to the user while disconnected from the network.

**Easy disaster recovery**

On-demand application delivery is a powerful concept for disaster recovery situations because the application and data are not lost if the profiles can be easily backed up, and servers and desktops can be replaced easily.
Components for Application Streaming

The components related to a server farm that make applications available for streaming can be separated into four categories. Each of these functional areas consists of software running on one or more workstations or servers. Before you install the components for application streaming, refer to the system requirements for application streaming.

The components that support virtualization on the user device, as shown in the diagram, include the XenApp server, Citrix Licensing, Streaming Profiler workstation, file servers, Web Interface, Citrix Receiver, and Offline Plug-in.
1. **Licensing.** Consists of the license server and License Management Console. Use the License Management Console to manage licensing. To install Citrix Licensing, see the licensing section in the Technologies node of Citrix eDocs.

For more information about licensing application streaming and offline access, see Application Streaming Licensing Explained (CTX112636).

2. **Administration (server farm).** Consists of the following components:
   - Farm servers.
   - IMA database.
Components for Application Streaming

- The Web Interface.
- The AppCenter, to configure and manage the server delivery and publish applications for streaming.

3. **Citrix Streaming Profiler.** Creates and maintains streaming application profiles. The Streaming Profiler is an independent application that enables you to profile Windows applications, Web applications, browser plug-ins, files, folders, and registry settings that can be streamed to user devices and servers.

   Use the profiler to create one or more targets within an application profile that can match all the platforms of your users. This strategy creates a single profile that can accommodate a variety of user platforms. The profiler can also update applications in the profile and provide other resources that your users need.

4. **Citrix Plug-ins.** The Offline Plug-in support streaming applications to the user's desktop. To provide offline access to applications and dual-mode streaming, install both the Offline Plug-in and Citrix Receiver (Enterprise), which includes the Online Plug-in, on user devices. When a user runs a published application enumerated by Citrix Receiver or through a 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.

   To support streaming applications to the server, install the Citrix Receiver on user devices. These applications must be published as "stream to server." When users run an application, it streams to the server and launches using an ICA connection on the user device. To stream to a Web Interface site, you must the site to the list of trusted sites.
Evaluating Application Delivery Methods

The application delivery method is a factor in determining the number of servers in a farm and their individual hardware requirements.

How you choose to deliver applications depends on your organization's needs and end-users' requirements. For example, some organizations use XenApp to streamline administration. In other organizations, the existing hardware infrastructure might affect the delivery method selected, as can the types of applications to be delivered. In addition, some end-users might run all applications while connected to the company network, while others might work in remote locations and run applications while disconnected from the network.

<table>
<thead>
<tr>
<th>Method/Description</th>
<th>Advantages</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Installed on the server:</strong></td>
<td>Applications are installed on the server, where the processing takes place, and accessed from the server. This is the traditional XenApp application delivery model. For many organizations, this provides the lowest cost of ownership for IT resources because it provides the greatest scalability.</td>
<td>Farm servers require sufficient resources to support the applications.</td>
</tr>
<tr>
<td></td>
<td>· This method provides a consistent user experience regardless of the user device.</td>
<td>Users must be connected to the server or network to run the applications (no offline access).</td>
</tr>
<tr>
<td></td>
<td>· You manage applications centrally.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· User devices do not require extensive resources, such as excessive memory or hard drive space. This delivery method supports thin clients.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· This method is effective for applications with components that are intertwined with the operating system (such as a .NET framework).</td>
<td></td>
</tr>
</tbody>
</table>
### Streamed to server:

Executables for applications are put in profiles and stored on a file server or Web server (the App Hub); however, when launched, they stream to the server, and application processing takes place on the server. Unlike installed applications, streamed applications are stored in the App Hub and provide application isolation by design.

- This method has similar advantages as for installed applications, including a consistent user experience, central management, and use of server resources instead of those of the user device.
- In many cases, streaming to server lets conflicting applications, such as multiple versions of the same application, run on the same server without needing to silo them.
- Updating applications is simplified because you update only a single application profile.

- Farm servers require sufficient resources to support the applications.
- Users must be connected to the server or network (no offline access).
- Some applications are not candidates for profiling, such as those using a .NET framework.

### Streamed to desktop:

Executables for applications are put in profiles and stored on a file server or Web server (the App Hub). When launched, the files required to execute the application are streamed to the user device, and application processing takes place on the user device instead of the XenApp server. When applications are streamed to the user device, the user experience is similar to running applications locally. After applications are cached on the user device, users can continue running the apps after disconnecting from the network (referred to as offline access).

- Users can have the local application experience, but you manage the applications centrally.
- Users might have a better experience when resource-intensive applications, such as graphics applications, are streamed to desktops.
- Using application properties and Citrix policies and filters for Offline Applications, you control the applications and users that have offline access, as well as the license period for offline use.

- User devices must have sufficient resources to run the applications locally; the user devices cannot be thin clients.
- User devices must run Windows operating systems, including Windows 7, XP, or Vista.
Dual mode delivery:
When you select “streamed if possible, otherwise accessed from a server” (referred to as dual mode or fallback), XenApp tries to stream the application to the user device first, but uses the backup access method if streaming to desktop is not supported on the user device. For example, you can specify that some users, such as sales personnel, run applications streamed to desktop when they are accessing the applications from Windows devices, and run them as installed applications when they are accessing them from handheld mobile or kiosk-type devices.

This method provides the most versatility for application delivery, offering all the advantages of streaming to desktops for supported user devices, plus a backup delivery method for the rest.

You control delivery options centrally using Citrix policies and filters, such as the server’s Load Balancing Policies for Streamed App Delivery.

For the backup method to occur, ensure that the application is either installed on the XenApp server or the streaming profile is configured for a target operating system that matches the server.

Choosing Between Published Desktops and Published Applications

Before selecting the method for delivering applications, decide if you want to publish the desktop or publish applications.

- Publishing the desktop - Presents users with an entire Windows Server desktop when they log onto XenApp. (For security, the desktop should be locked down.)

- Publishing applications - Publishes specific applications and delivers only those applications to users. This option provides greater administrative control and is used most frequently.

You can use policies to prevent users from accessing server drives and features with both methods of application delivery.
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 either Receiver package, the CitrixReceiverEnterprise.exe or CitrixReceiver.exe, and the 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.

- When deploying Citrix personal vDisk into virtual environments, the Offline Plug-in automatically moves the RadeCache and RadeStore location to the personal vDisk drive.
Providing Single Sign-on for Streamed Applications

Citrix extends the Single Sign-on feature for streamed applications. When Single Sign-on is installed locally, it recognizes streamed applications, even when launched in isolation environments, and manages logons as expected.

For Microsoft Internet Explorer, however, the Single Sign-on feature must install a file called BHO.dll. To allow this, when creating your application profile for Internet Explorer plug-ins, select the option to **Enable User Updates** (formerly called **Relaxed** security), which is deselected by default.

By enabling user updates for Internet Explorer, the application can download vendor-supplied updates over the Internet. These updates are stored within the user profile and are unique to that user. The next time the user device connects to the profiled Internet Explorer on a server or file share, the streamed application does not overwrite the updates, and Internet Explorer runs using the updates. Also with this setting, installers can run inside isolation, where they are able to install new add-ons or software updates to Internet Explorer. Local add-ons are compatible with Internet Explorer if you profile it with the default isolation rule of Isolate. Local add-ons might not install correctly if you change the isolation rule for the Internet Explorer profile to Strictly Isolate.
Creating Application Profiles

A profile is an application packaged for streaming using the Citrix Streaming Profiler. A profile can contain a single application or suite of applications. For example, you can profile Microsoft Word by itself or profile the entire Microsoft Office suite in a single profile, or you can profile applications separately and link them with inter-isolation communication. To create profiles, you must install the Streaming Profiler on a clean, independent computer, called the profiler workstation. The profiling wizard records the installation of applications and the metadata needed to stream the profiled applications. The profiler bundles files and configuration settings in what becomes the application profile.

Individual targets within a profile represent one or more defined user environments. The initial target matches the environment of the profiling workstation; however, you can create multiple targets to match specific user environments. For example, some commercial applications are capable of running on multiple operating systems and languages, while others, such as custom applications, might be capable of running only on a particular target operating system and language.

**Important:** Applications compiled as 64-bit applications are not supported for streaming. However, 32-bit applications can be profiled on 64-bit systems and configured to be streamed to 64-bit systems.

Depending on the environment of your users, you have the option to profile prerequisites, such as Java Runtime Environment, with the profiled application. In some cases, you might find it necessary to profile certain applications together to ensure functionality among applications or to apply a range of compatibility settings to ensure profiled applications launch and run successfully. In addition, you can use the profiler to link existing profiles using *inter-isolation communication* so that applications interact as needed, even though they are running in isolation environments.

After you create a profile and save it to a file share in your App Hub, configure users and publish the application in the profile for streaming using the publishing wizard in the Citrix AppCenter. When a user launches an application published to stream to the user device, the Citrix Plug-in running on the user device automatically chooses the correct target that matches the configuration of the user device.

For information on specific topics, refer to these documents on the Citrix Knowledge Center:

- *Application Streaming FAQs for Administrators* at [http://support.citrix.com/article/CTX118181](http://support.citrix.com/article/CTX118181)


- Additionally, select your product version of XenApp on the support Web site, click the *Technotes* tab, and then click *Application Streaming*. 

Note: The Streaming Profiler SDK offers a set of COM objects and .NET interfaces that give Citrix customers, distributors, and partners a programmatic interface into the profiler. For information, download the SDK and Readme from the Citrix Developer Network Web site at http://community.citrix.com/. 
Targets Overview

A target is a collection of disk files, registry data, and other information used to represent an application isolation environment. In addition, each target denotes a combination of operating system, service pack level, system drive letter, and language. Applications can be profiled for each combination of these values to support separate targets; for example: Microsoft Vista for all service packs, drive letter C, and English.

There can be multiple executables inside a target including multiple applications that normally receive an entry on the Start menu. As an example, “Microsoft Office” is a profile and “Microsoft Word” is an application inside that profile. A profile can support multiple targets where the target is a separate installation of the profile-level software targeted for execution on a specific version of the operating system or language. For example, create one target for Windows Vista and another target for Windows Server 2008.

User devices select targets for execution based on the computer configuration you specify while creating the target. By default, a target matches the operating system and configuration of the profiling workstation, but you can select different operating systems as well.

In addition, refer to information about the following selection criteria for creating targets:

- Service Pack Level
- System Drive Letter
- Operating System Language
- Inter-Isolation Communication Overview

You use the profiler to set criteria for each target in a profile. One or more administrators can run the profiler multiple times and from different packaging environments to achieve a complete set of differentiating targets. For many common scenarios, a single installation image supports a variety of computer configurations, which simplifies profile creation.

The criteria associated with each target is stored in a profile manifest, a .profile file, stored with the profile files.

Overlapping definitions are not permitted: only one target in a profile can be a correct match for any computer configuration at application launch.

An administrator can update a profile and target at any time without affecting already active executions on user devices. The cost for this support is that file-server disk space is consumed to maintain old versions. The profiler provides no facility to delete old versions of targets. Instead, manually delete old versions of targets to reclaim server-side disk space. When deleting targets, it is the responsibility of the administrator to ensure that the deleted versions are sufficiently old that no users are employing the target.

For the list of supported operating systems for application streaming, see the system requirements. By design, future operating systems are not supported, and the execution environment refuses to execute an application if the user device has an unsupported
operating system.
Service Pack Level

The service pack field is an optional component that augments the operating system version.

Because service pack level augments the operating system version, the profiler stores service pack selection criteria on a per-operating system basis. For each operating system, set the following rules for service pack selections:

- Not required (any service pack is acceptable)
- Minimum Service Pack Level
- Maximum Service Pack Level
- Range of Service Pack Levels
- A single, specified service pack level
- No service packs installed

When choosing supported service packs, ensure that you do not choose service packs that are not supported by the Offline Plug-in. Refer to the system requirements for supported platforms.
System Drive Letter

For best practices, Citrix recommends that you install all applications on the primary system drive. By packaging and executing using the primary system drive, you define a set of criteria that best associates a given target with a given user device.

The system drive letter must be a match between the target and the user device drive for a target to be the correct match for executing an application. There is no provision for the system drive to be variable. The system drive used on the profiler workstation must match the system drive on the user device.

To support user devices with different system drive letters, create a target for each drive letter.
Operating System Language

The following languages are supported by the profiler:

- English
- French
- German
- Japanese
- Spanish
- Simplified Chinese

Using the English version of the profiler, create targets for the following operating system languages:

- Korean
- Traditional Chinese

The profiler can create targets for all languages, including languages other than those listed here, but doing so is not fully supported. To create targets for other languages, Citrix recommends that you use the English language version of the profiler.
Inter-Isolation Communication Overview

Inter-isolation communication is a feature that links individual profiles so that applications in separate profiles can communicate with each other when launched on the user device. You can also use this feature if a streamed application fails because it needs data from another streamed application, but cannot detect it because both are running in isolation environments.

You can create two types of profiles that provide inter-isolation communication:

- An associated profile does not include any additional installation. You link existing profiles and set their hierarchy so that they can communicate when launched on the user device. For example, if you profile Microsoft Outlook and Adobe Reader in individual, simple profiles, the applications operate independently, but Outlook is not aware of the streamed Adobe Reader and therefore cannot call the application in the simple profile to open the .PDF attachment. By associating these two profiles, Outlook and the Reader can interact as users expect, even though the individual applications are profiled separately. This happens because they are now aware of each other and can interact as though they are profiled together.

- A dependent profile includes the installation of an application that depends on the presence of one or more other applications before its installation is complete. While you create the profile, to simulate this dependency, the existing profiles that you select are temporarily downloaded from the file server during the profiling process to establish the hierarchy and isolation rules that are used at runtime. You then install the application that is dependent on them. For example, you might include simple profiles with Office 2007 and Microsoft Dynamics in this profile before you install a .NET application that depends on them. That way, when users launch the .NET application, Office and Dynamics are also launched on the user device.

When you create a profile enabled for inter-isolation communication, applications launch on the user device and remain isolated from the system and from other isolated applications, but they can interact with each other.

The advantage of inter-isolation communication is that applications can be maintained separately and updates are included automatically in all the linked profiles in which the profile is included. This feature saves time for the administration of the profile set.

When you create a dependent profile, the additional properties added to any of the individual profiles in the linked profile are enabled for all the individual profiles. These properties include custom rules, pre-launch or post-exit scripts, and pre-launch analysis. When users stream applications from the inter-isolation communication profile, the combined properties of all the linked profiles execute in hierarchical order, from the lowest profile to the highest profile as listed in the profiling wizard and Linked Profiles property page.

However, if you create an associated profile, without installing a new application, additional properties are not available. You can add properties only to profiles that have installed applications.
Isolating Services

Certain applications, such as Microsoft Office 2010, require related services to run on the user device. Beginning with version 6.0 of the profiler, services that are required by applications are automatically installed with the application as you create application profiles.

**Important:** This feature requires that you create a whitelist of approved locations of profiles in the registry of user devices. After you create the whitelist and edit the registry for the user devices, only services from the approved locations can be loaded and run on the user device. For these steps, see *Specifying Trusted Servers for Profiles and Services.*

Based on its startup type, a service runs in an isolation environment on the user device with the application that requires it and continues until the session ends:

- **Automatic start:** These services start automatically at logon and continue running until the user shuts down or restarts the device.

- **Manual start:** These services start when called by an application in the profile and continue running until the application ends the service or the user shuts down or restarts the device.

To view or modify the services available for a target, from the profiler, from the **Edit** menu, select **Target Properties.** The **Services** tab lists the services, their paths, logon names, and start type.

**Considerations**

- Isolated services might extend launch time for the first launch of the application each time the device is restarted.

- When a service runs in isolation, it might not communicate all the needed information with services running outside isolation, such as locally installed services. If communication is required, consider removing the service from isolation and installing it locally on the user device.

- If the profile uses inter-isolation communication to link one or more subprofiles, all services within the linked profile are started.

- To update a service, open the existing profile in the Update Profile wizard. Citrix recommends updating services during off-peak hours because the procedure stops the service and closes that application for end users. After completing the update, the service restarts and users can relaunch the application.

- In any environment, only a single instance of the service launches in isolation. For example, in a multiuser environment, the service starts when the first user launches the application and then is shared by all subsequent users running the application.
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
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


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\n   - **32-bit:** HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Rade\n
   **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.
Managing Isolation Environment Rules

The Offline Plug-in uses isolation environments to control application compatibility and accessibility. The Plug-in creates isolation environments by defining a set of rules that specify how an application functions within its confines. The default rules for isolation environments are adequate for most environments. However, alter the default set of rules, as needed, to exert control over application interactions with operating system resources on the user device.

A rule for an isolation environment is based on a specific location: either a file path or a registry key path.

Rules are matched by the most specific path to the resource being accessed. A rule applies to the object (file, registry, or named object) specified and all the children of the specified object, unless a more specific rule exists.
Types of Isolation Environment Rules

Use isolation environment rules to improve application compatibility when users stream applications to their user devices. Rules can reduce conflicts between the streamed application and other locally installed, hosted, or streamed applications.

Choose from isolate, strictly isolate, ignore, and redirect rules, as needed.

Isolate Rule

This is the default behavior while profiling applications in the Streaming Profiler. The Isolate rule assures that a streamed application cannot affect locally installed components of the operating system or other applications. When user devices create a new isolation environment, its default behavior is to isolate everything with a few exceptions. When an application requests access to a system resource (such as a file, registry, or named object), a per-user version of the file or key is created as required. This behavior relieves most application conflicts and allows applications to run correctly.

Isolation rules ensure that per-user level versions of files and keys are created. This creates an individual copy of each resource that a particular user accesses.

Add this rule to ensure that there is one copy of a resource per isolation environment. For example, create a rule that isolates the registry hive, HKEY_LOCAL_MACHINE\SOFTWARE\classes, when you install Microsoft Office. Because each user does not require a separate version of this hive, create a rule that isolates this particular registry hive for the isolation environment.

Strictly Isolate Rule

This rule prevents the application from accessing the objects in the physical layer. The application never sees an object that is defined to be covered by this rule unless it was created within the isolation environment.

This rule is commonly used to support multiple versions of an application running on the user device. The existing isolate rule prevents an application from making changes in the global system, which might affect other applications running in the system. However, system changes made by other applications running on the system cannot be hidden from view of the isolated application.

Sometimes, such changes may need to be hidden from the application view for its proper functioning or for installation of an application in the sandbox. The Strictly Isolate rule allows the sandbox to hide selective changes made in the system from the view of the virtualized application.
Ignore Rule

The Ignore rule allows the rules engine to define “holes” in the isolation environment so that an application can write to the underlying system. Note that the Isolate rule is still the default behavior while profiling applications in the Streaming Profiler.

This rule allows a streamed application running inside an isolation environment to share data with an application outside the isolation environment. For example, if you try to open a file from streamed application A to use in locally installed application B, the applications can communicate normally, as though they are both locally installed.

Also, in a scenario where users can print to network printers available within a streamed-to-client session, these printers are created automatically when the user connects to a published application.

Redirect Rule

A Redirect rule redirects an application request for a file or registry key to a specified location. For example, if an application creates the file, c:\temp\data.txt, this rule can redirect those files to c:\guidtemp\%USERNAME%, regardless of the user.

For example, if UserA runs the application in an isolation environment, c:\temp\data.txt is created in c:\guidtemp\UserA\data.txt.

In this example, the administrator might choose to clean up the \temp directory each time the system starts up. By redirecting all access of c:\temp directory to c:\guidtemp on a per-user basis, the administrator can clean up the temporary data easily at startup.

Examples

Consider the effects of the following rules:

- An Ignore rule for the file path: C:\Documents and Settings\%USERNAME%

  Every file and directory created under C:\Documents and Settings\%USERNAME% is created in the system location because you specified, through the Ignore rule, that this directory location is not isolated. If an application opens the file C:\Documents and Settings\%USERNAME%\ApplicationData\CompanyA\foo.txt, the Ignore rule for C:\Documents and Settings\%USERNAME% applies.

- A per-user Isolate rule for: C:\Documents and Settings\%USERNAME%\Windows

  This rule isolates the per-user Windows directory, C:\Documents and Settings\%USERNAME%\Windows. If an application opens C:\Documents and Settings\%USERNAME%\Windows\Win.ini, the isolate per-user rule for C:\Documents and Settings\Windows applies.
Restrictions and Limitations for Rules

Consider the following restrictions and limitations when constructing or altering the rules for your isolation environment:

- **Do not modify or delete the default rules available for an isolation environment.** If you modify these rules, the isolation environment might be unable to run applications correctly.

- **Use an asterisk (*) as a wildcard character only at the end of an ignore named object rule.** For example, the rule ignore object* ignores all named objects with a name starting with object. Use of an asterisk is not allowed in isolate or redirect object rules.

  **Important:** Do not use the wildcard in a rule that applies to a file system or registry key. By definition, the rule applies to all the children of a path name.

- **File system rules can apply to either files or directories.** Create a rule to alter the behavior of individual files or directories and all of the files within them. For example, you might have a Redirect rule for C:\temp\fileA.txt, as well as one for C:\temp\subdir1.

- **Rules that specify a registry object apply only to registry keys.** They do not apply to registry values.

- **Rules for an isolation environment are interpreted at run time.** Any modifications to existing rules are interpreted the next time you launch an application associated with, or installed in, an isolation environment. If you are executing an isolated application and modify the rule definitions, these changes do not affect running applications. The modified rules are interpreted and take effect the next time the application is executed.

- **A rule must be specified in terms of a full directory or key level.** Matches are performed on the full name of a given hierarchy level. For example, if you create a Redirect rule for C:\temp\file, the rule applies only to a file or directory called c:\temp\file. The rule does not apply to any files or directories that have c:\temp\file as part of their name. For example, this rule does not apply to the file C:\temp\fileA.txt, the directory c:\temp\filledWithFiles\, or any files under that directory. The same principle applies for the file system, registry, and named objects (with the exception of wildcards and named object rules).
Creating Isolation Environment Rules for a Target

Use the Rules page of Target Properties to modify the isolation environment rules. The list of rules on the Rules page displays for each rule its name, the action to perform, and the object on which to perform the action.

To display more detailed information about a rule, select it in the list and Rule Description identifies the named object on which the rule operates.

After testing a profile, if you determine that your users might experience conflicts when running applications in their isolation environments, modify the isolation environment rules for the target.

Some of the indications that you may want to modify the isolation rules are:

- If an application creates a directory for per-user data that is stored in a nonstandard location (Ignore rule)
- If the profiler workstation has extra drive volumes and an installer writes to those drives while installing in a target (Ignore rule)
- If your file share volume is on your profiler workstation (Ignore rule)
- If you must isolate a subdirectory of an ignored directory on the user device (Ignore and Isolate rules)
- If you must support multiple versions of an application running on the user device (Strictly Isolate rule)

The Rules list shows the existing rules for the target and for each rule identifies:

- Arbitrary name for the rule
- Action, which is the isolation environment rule that is being called
- Object on which the action performs

The Rule Description box at the bottom shows the command represented by the currently selected rule.

To edit the set of rules, use the Add, Copy, Modify, and Delete buttons.
To create an isolation environment rule

To add a rule to the currently defined set of rules, from the Profiler, select the target, and from the Edit menu, select Target Properties. From the Rules tab, click Add. Use the New Rule wizard to define the new rule.

1. Select an action and the type of object on which you want the action to operate.

2. On the Select Objects page, click Add.
   - If for the action, you choose Ignore, Isolate, or Strictly Isolate:
     - If you selected Files and Folders as the object type, use the file browser to select the files and folders on which you want the rule to operate
     - If you selected Registry Entries as the object type, use the Choose Registry Entry dialog box to select a hive and type a key on which you want the rule to operate
     - If you selected Named Objects as the object type, use the Choose Named Object dialog box to type the name of the object on which you want the rule to operate
   - If for the action, you choose Redirect, specify the source path, registry entry, or named object and its destination.

3. If necessary, modify the default name of the rule. By default, the New Rule wizard creates a rule name consisting of the name of the action and the name of the object.

To copy a rule in the currently defined set of rules, from the Rules tab of Target Properties, select the rule and then click Copy. The copy operation adds the copied rule to the top of the list of rule set members. Use the property also to modify the name, action, or object of the rule.

To delete a rule from the currently defined set of rules, from the Rules page of the Target Properties, select the rule and click Delete.
To modify a rule

To modify a rule in the currently defined set of rules, from the Rules tab of Target Properties, select the rule and click Modify. Use the New Rule wizard to define the new rule. Modifying a rule lets you modify the action and objects, but not the object type.

1. Select the action.

2. On the Select Objects page, add or modify objects.

   - If the selected action is Ignore, Isolate, or Strictly Isolate:
     - If Files and Folders is the object type, use the file browser to select the files and folders on which you want the rule to operate
     - If Registry Entries is the object type, use the Choose Registry Entry dialog box to select a hive and type a key on which you want the rule to operate
     - If Named Objects is the object type, use the Choose Named Object dialog box to type the name of the object on which you want the rule to operate

   If the selected action is Redirect, specify the source path, registry entry, or named object and its destination.

3. If necessary, modify the name of the rule.
Using Environment Variables to Construct Rules

Use environment variables to construct rules that contain references to path locations that can change at run time. For example, an application data path can change depending on the language selected. This can lead to errors if you use the default rules for an isolation environment. Using an environment variable to construct path-specific segments (such as a language-specific application data location, AIE_COMMONAPPLICATIONDATA) ensures that an explicit rule is created for the selected language. At run time, AIE_COMMONAPPLICATIONDATA is substituted with the language-specific application data location such as C:\Documents and Settings\All Users\Application Data.

Citrix recommends that you use an environment variable to ensure universality of a rule when any of the following conditions are true:

- Path location contains a user name
- Translation issues can occur with standard application locations
- Relative locations can change; for example, the location where you install XenApp

Environment variables can also quickly check where certain paths are within a script. For example, to find out what the file system installation root for an isolation environment is, use AIE_FSINSTALLROOT.

All environment variables for isolation environments are prefixed with AIE_. When you create a new isolation environment, a number of default rules apply. These default rules use the environment variables listed in the following table to make the rules universally applicable. To view the default rules for application isolation environments, refer to the list in the Rules wizard.

**Note:** Exercise caution when using backslash characters (\) with these environment variables. Ensure that you insert a backslash (\) after an environment variable before adding additional path information; for example, AIE_USERAPPLICATIONDATA\MyData\Mine.

This table shows environment variables available for isolation environments:

<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIE_COMMONAPPLICATIONDATA</td>
<td>Common application data</td>
<td>C:\Documents and Settings\All Users\Application Data</td>
</tr>
<tr>
<td></td>
<td>location</td>
<td></td>
</tr>
<tr>
<td>AIE_COMMONDESKTOP</td>
<td>Common desktop location</td>
<td>C:\Documents and Settings\All Users\Desktop</td>
</tr>
<tr>
<td>AIE_COMMONSTARTMENU</td>
<td>Common Start menu location</td>
<td>C:\Documents and Settings\All Users\Start Menu</td>
</tr>
<tr>
<td></td>
<td>location</td>
<td></td>
</tr>
<tr>
<td>Environment Variable</td>
<td>Description</td>
<td>Location</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>AIE_FSINSTALLROOT</td>
<td>File system install root</td>
<td>C:\Program Files\Citrix\RadCache\MyAIE</td>
</tr>
<tr>
<td>AIE_FSUSERROOT</td>
<td>File system user root</td>
<td>C:\Documents and Settings\Administrator\Application Data\Citrix\RadCache\MyAIE</td>
</tr>
<tr>
<td>AIE_MERAFRAME</td>
<td>Installation location</td>
<td>C:\Program Files</td>
</tr>
<tr>
<td>AIE_NAME</td>
<td>Isolation environment name</td>
<td>MyAIE</td>
</tr>
<tr>
<td>AIE_REGINSTALLROOT</td>
<td>Registry install root</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\RadCache\MyAIE</td>
</tr>
<tr>
<td>AIE_REGUSERROOT</td>
<td>Registry user root</td>
<td>HKEY_CURRENT_USER\SOFTWARE\Citrix\RadCache\MyAIE</td>
</tr>
<tr>
<td>AIE_USERAPPLICATIONDATA</td>
<td>User global application data location</td>
<td>C:\Documents and Settings\Administrator\Application Data</td>
</tr>
<tr>
<td>AIE_USERLOCALDATA</td>
<td>User local application data location (including temporary files)</td>
<td>C:\Documents and Settings\Administrator\Local Settings\Application Data</td>
</tr>
<tr>
<td>AIE_USERDESKTOP</td>
<td>User desktop location</td>
<td>C:\Documents and Settings\Administrator\Desktop</td>
</tr>
<tr>
<td>AIE_USERSID</td>
<td>Unique security identifier for the current user; it is used extensively internally for security checking.</td>
<td>S-1-5-2001-......</td>
</tr>
<tr>
<td>AIE_USERSTARTMENU</td>
<td>User Start menu location</td>
<td>C:\Documents and Settings\Administrator\Start Menu</td>
</tr>
</tbody>
</table>
Preparing a Workstation for Profiling Applications

Configure the profiler workstation to provide a run-time environment that is as close to your user device environment as possible. For example:

- If applications are streamed to user devices, the profiler workstation should be a similar platform
- The profiler workstation should also include standard programs that are part of the company image, such as an antivirus program

For the full list of supported operating systems for targets, see the System Requirements for Application Streaming.

In addition, profiles created on one operating system automatically run on compatible operating systems. For example, targets created on Windows XP 32-bit platforms automatically run on Windows 2003 32-bit platforms (and vice versa). Compatible operating systems include:

- Windows XP 32-bit and Windows 2003 32-bit
- Windows XP 64-bit and Windows 2003 64-bit
- Windows Vista 64-bit and Windows 2008 64-bit

Important:

- Other than standard operating system software and utilities, ensure the workstation is clean of other software applications.
- Make sure that none of the applications or files you intend to add to the profile is installed on the profiling workstation. The profiler does not install files that already reside on the computer.
- Do not use the profiling workstation to store or stream applications.
- Do not install the Plug-in used for streaming, such as the Citrix Offline Plug-in or XenApp Streaming Plug-in, on this workstation.

Install the Citrix Streaming Profiler on a clean, nonproduction server or workstation. To achieve the ideal goal of a single target executing on multiple operating system versions, Citrix recommends in general to use the oldest candidate operating system for profiling, Windows XP Professional. If the created target works on all candidate execution operating systems, you are finished. If, however, a specific operating system level has issues with the multiple-operating-system target, rerun the profiler and create a new target specific to the failing operating system version. In this later case, for this target, run the profiler on the same level operating system that is intended for execution.
After installing the profiler, simplify the creation or modification of profiles by setting profiling preferences.
Known Limitations for Profiling

Certain applications cannot be profiled, including:

- Applications that include device drivers
- Applications that install COM+
- 64-bit applications
- Applications that install DCOM (limited support)
- Other applications such as Microsoft Internet Explorer, Microsoft Data Access Components (MDAC), and the .NET framework

**Important:** If you profile an application that requires User Access Control (UAC) rights elevation or administrator rights, make sure that you configure access to the published application only for users and groups that have the required rights on the user device.

If an application you are installing in a profile must interact with an application that cannot be profiled, Citrix suggests the following procedures:

1. Install the application that cannot be profiled, such as .NET framework, on the profiling workstation before you create a profile for the applications that interact with it.

2. While profiling the new application, enable pre-launch analysis to confirm that the non-profiled application is installed before the new application can launch.

3. Install the non-profiled application on user devices to run outside isolation so that the new application can interact with it as needed.

Refer also to the known issues and workarounds in this release of the Streaming Profiler and Offline Plug-in.
To install the profiler

For best results, use the Windows uninstall program to remove any previous version of the Citrix Streaming Profiler.

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

1. On the workstation you want to use to profile applications:
   - Insert the installation media, and in the autorun window, choose **Browse Media** to locate the Application Streaming Profiler folder and run **CitrixStreamingProfiler.exe**.
   - Navigate to the [Citrix Support Web site](https://support.citrix.com) for downloads and locate the most current version of the profiler for application streaming.
2. Choose a language for the installer interface and complete the installation wizard.
3. After installation, restart the workstation.
To disable and enable profile signing

If you are not signing profiles, use the profiler preferences to prevent the digital signature pages from appearing in the New Profile and Target wizards. To set this default preference for all new profiles, from the Edit menu of the profiler window, choose Preferences and then select the Digital Signature tab.

If you later decide to sign profiles, use the Digital Signature tab to restore the digital signature pages to the wizards.
To start the profiler

1. From the Start menu, choose Programs > Citrix > Streaming Profiler.
2. Select the Streaming Profiler.

When the profiler starts, the Welcome page appears. Use the Welcome page as an easy starting point for creating and modifying profiles.

To see the profiler interface, on the Welcome page, click Close.

The profiler interface includes four main components:

- **Menu and toolbar.** Located at the top. The toolbar contains buttons that initiate the following actions:
  - Starting the New Profile wizard to create a profile
  - Opening an existing profile
  - Saving the current profiler to a file share
  - Updating a target or application in the open profile
  - Adding a new target to the profile
- **Navigation pane.** Located on the left. When populated, lists a profile and its targets.
- **Profile and target information.** Located on the right.
- **Status bar.** Located across the bottom.

After starting the profiler for the first time, set profiler preferences that optimize how you create profiles and targets.

To set these default preferences for all new profiles, from the Edit menu of the profiler window, choose Preferences.

- Save the default User Profile Security settings for all profiles you create. This relieves you of specifying enhanced or relaxed security as you create profiles.

- If you are not signing profiles, use the Digital Signature setting to hide the Sign Profile page in the wizards.

Preferences save time and improve usability by enabling you to store relevant settings for use in future packaging tasks.
Creating a Profile and Its Initial Target

After installing the Streaming Profiler on a workstation to create profiles, prepare for the decisions needed to create profiles.

When you create a new profile, your first steps are to set the following profile properties:

- Profile name
- Ability for users to update applications
- Optionally, inter-isolation communication with existing profiles

As you continue, choose the following configuration-matching criteria for the target:

- Operating system
- Service pack level
- Language

Then you install applications in the target (although not on the workstation itself) through either advanced or quick installation procedures. Profiling a single, standard application in a target is called a quick install. If the target needs multiple applications or other resources, use an advanced install. You must complete a full installation and can then perform any initializations or customizations needed before users access the application. A target can offer any of the following resources:

- Applications
- Internet Explorer plug-ins
- Folders and files
- Registry settings

Finally you can opt to digitally sign the profile. After you build the profile, manually save it to a file share in your App Hub where you can publish the profiled application for streaming to your users.

Note that you can modify the profile at any time, including updating the application, add pre-launch or post-exit scripts, add pre-launch scripts, and modify the file type association. The changes are immediately available the next time users access the published application.
To create a profile and target

Ensure that a file share exists with the “everyone” group assigned READ access and the “administrators” group assigned WRITE access at both the share level and NTFS level.

From the profiler workstation, make sure that you have access to the executable for the application, but that the application is not installed on the workstation. Open the profiler from the Start menu.

1. To start the New Profile wizard, either select New Profile from the first screen, or if it is already open, from the File menu, choose New. Use the New Profile wizard to complete the remaining steps.

2. Name the profile.

When naming a profile, choose a simple name. Do not include any criteria that will be used to identify targets. For example, do not include a version number in the profile name.

3. Use the Enable User Updates page to enable users to update applications on their user devices (disabled by default). When the feature is enabled, executable files that are accessed through the application (such as product-update executables) run from the user profile root and launch on the user device. When disabled, the executable files launch from the install root location, which prevents most product-update executables from updating applications automatically and lets you maintain and deliver updates centrally.

4. Use the Set up Inter-Isolation Communication page to link existing profiles that need to communicate with each other on the user device (optional). If you are not setting up inter-isolation communication, do not make any entries on this page.

5. Set at least one target operating system and language. By default, the wizard selects all operating systems compatible with the profiling workstation.

To link existing profiles for inter-isolation communication only but not create any new targets, click the top check box (not selected by default). To create a new target or profile, ensure the check box is not selected.

Setting the target operating system and language criteria are the first steps in creating the initial target for a profile. The default operating system and language are those of the operating system installed on your profiler workstation.

a. If you selected profiles for inter-isolation communication, to associate those existing profiles without creating a new target (and skipping the installation pages of the wizard), check Minimal Target. When selected, the remaining target creation options are disabled and the wizard skips the installation pages. It goes directly to Step 12, signing the profile with a digital signature. To create a new target within the linked profile, make sure the option is not checked.
To create a profile and target

b. To support other operating systems and languages, select the check boxes associated with those you want to support. When selecting target operating systems and languages, do not select those languages for which you are going to create separate targets.

c. To consider the service pack level, click Set Service Pack. By default a target matches all service packs of the operating systems it supports.

d. When selecting the service pack supported by the target, use the Supported Service Pack Levels pull-down menu to choose a rule for considering the service pack level.

e. Type the number representing the service pack level in the applicable field for Minimum Level, Maximum Level, Exact Level, or, if for a range, Minimum Level and Maximum Level.

   Note: For subsequent targets, to ensure the current target you are adding does not conflict with other targets in the profile, click Check for Target Conflicts.

6. Choose an installation option according to the type of application or number of applications you want to install in a target:

   · Quick Install. Select this option if you are installing only one application and it has an installation program, such as setup.msi or .exe (selected by default and recommended for normal installations).

   · Advanced Install. Select this option only if you are installing Internet Explorer plug-ins, editing registry settings, installing an application manually, or installing from multiple installers.

7. On the Choose Installer page, click Browse to choose an executable file or a script you run to install the application in the current target. In this step you are just choosing the installer, not running it. If needed, enter required command-line arguments.

8. On the Run Installer page, ensure the installation program and command-line parameters are correct.

   Use advanced installations to select resources, including files, folders, registry settings, and Internet Explorer and plug-ins to add to the profile.

9. Click Launch Installer. Wait until the installer program launches on the workstation. For large applications, this can take several minutes. Then complete a full installation for the application. The destination path shown in the installer does not matter because the application is installed in the profile, so accept the default location.

10. When the application is fully launched and configured on the workstation, close the application and click Next in the profiling wizard. If a restart is required to complete the installation, the profiler automatically performs a virtual restart. After the virtual restart completes, the application is ready to run.

11. On the Run Application page, select and run the application. Close the application before clicking Next in the profiling wizard.

   Tip: After completing a full installation, which installs the application for all your users, run the application once to ensure that you complete all needed initializations before delivering the application to users. For example, you might have to enter a product serial number or license key. In addition, take some time to configure
To create a profile and target

preferences or options and to enable or disable features before you publish the application. For example, you might have to disable auto-updates to prevent users from receiving unwanted messages or files on their computers.

12. On the Select Application page, view the list of applications discovered in the current target. Use the buttons to modify the list of applications that you want to publish later using the AppCenter.

13. On the Sign Profile page, sign the profile with a digital signature, if needed.

14. Click Finish to build the profile. Before clicking Finish, you have the opportunity to review profile information and edit profile and target settings.

15. When the wizard closes, save the profile by typing the UNC path to the file share in your App Hub. Note that a subfolder is created with a name that matches the profile name.

For example, if you enter the following path:

\citrixserver\profiles

The following Save To storage location appears, based on the values of UNC Path and Profile Name:

\citrixserver\profiles\<Profile Name>\<Profile Name>.profile

If needed, change the name of the profile at this point.

Important: Windows File Explorer cannot handle file paths that exceed 256 characters. However, when profiling some applications, such as Microsoft Office 2010, the file paths might exceed that limit due to the high level of folder nesting. To prevent issues due to long file names, Citrix recommends using a utility such as Robocopy to replicate profile data without errors. This utility is available with Windows Resource Kit and is a feature in Windows Vista, Windows 7, and Windows 2008.

After you save your profile, use other workstations to add unique targets to the profile, if needed.
To allow users to update applications

Use the Enable User Updates setting in the profiling wizard to determine whether or not files for streamed applications are executed from the profile directory of the user. You can set this option only when you create a profile for the first time.

Citrix recommends disabling this option unless it is mandatory to enable it. In addition, Citrix recommends disabling the application’s automatic update feature. When updates are disabled, you can manage installations and updates centrally using the update wizard in the profiler. For example, automatic updates might fail for applications that stream to virtual desktops. Instead, when new versions are available, update the profile with the new version and make it available to users.

**Important:** After creating the first target, you cannot modify the setting for the profile. The setting that you select for the first target applies to all other targets that you add to this profile, even if you manually select a different setting for subsequent targets.

Additionally, to set a default for all profiles, from the Edit menu, select Preferences. Use the Enable User Updates tab to prevent the User Updates page from appearing in the profiling wizards.

Set the option for the profile:

- Select the check box to permit executable files that are accessed through the profiled application to run from the user profile root.

  If you profile the application with this setting selected, the application can download vendor-supplied updates over the Internet. Any updates are stored as part of the user root, so they are unique to that user. The next time the user device connects to the profiled application on a server or file share, the streamed application will not overwrite the updates, and the application runs using the updates.

  Selecting this setting is recommended for streamed macromedia plug-ins, which download extensions (DLLs) based on the content that is being processed. Also, some applications decompress DLLs during runtime that need to run from the user root.

- Clear the check box to ensure that all executables from the profile launch from the install root location and not from the user profile root location. Clearing this setting prevents most product-update executables from installing updates automatically on user devices and lets you manage the updates centrally through the wizards in the profiler. When cleared, the system specifically inhibits the ability to run code that is not streamed from the server.

  Administrators can enforce a cleanup policy to delete all session artifacts when the user closes the application or logs off.

  **Note:** If your testing finds that this setting does not prevent automatic updates for an application, look for a preference in the application installer to disable automatic updates when you run the application during profiling. Alternatively, disable or uninstall the update programs manually on user devices.
To set up inter-isolation communication

During the profiling process, set up inter-isolation communication for applications profiled independently that should interact as though they are integrated with other profiled applications.

The order in which profiles are listed determines the precedence of isolation rules and operations for the applications in the inter-isolation communication profile. The rules that exist for each profile are merged into a single list of rules, with the rules of highest priority taking precedence.

**Important:** Refer to the system requirements for user devices if you plan to deliver profiles with inter-isolation communication.

1. On the **Set up Inter-Isolation Communication** page of the profiling wizard, click **Browse** to locate the directory (not the files themselves) where your existing profiles are stored. To be linked, the profiles must all be located in the same directory.

   Make sure that each of the profiles you link has a target for the operating system of the profiling workstation.

2. In the **Browse for Profiles** box, click **Browse** to locate the directory where your existing profile directories are saved. For example, if you saved “Adobe.profile” in the following location:

   ```plaintext
   \\hostname\fileshare\Profiles\Adobe\Adobe.profile
   ```

   navigate to the Profiles directory (the grandparent of the profile file).

   To be added, all the profile directories must be located in a single directory, such as “Profiles” in the example.

3. Click the check box of the individual profiles to link in this profile.

4. When you highlight a profile, use the **Move Up** and **Move Down** buttons to set the order of priority.

   For example, if you create a linked profile for Microsoft Office 2007 and Adobe Reader (any version), make sure that Office 2007 is the top-level application in the profile, which ensures that the Office isolation rules take priority over those of Adobe Reader. This priority is required for Office applications to launch correctly.

5. For new profiles, continue in the wizard to the **Set Operating System and Language** page:

   - To link existing profiles only (the profiles you selected on the previous page) but not create any new applications or targets, called an **associated** profile, check the top check box (not selected by default). When you click **Next**, the wizard skips the installation pages and goes directly to the final step, signing the profile with a digital signature.
To create an additional target or application in this profile, called a dependent profile, make sure the top check box is not selected and continue using the wizard to create the new target or install the application in the profile. Use this option if the new target or application is to be dependent on the profiles you selected on the previous page.

6. On the lower part of the page, carefully review the lists of operating systems and languages.

**Important:** Each profile must contain a similar set of targets as all the other profiles in the linked profile, including a target that matches the profiling workstation. Note the superset of operating systems, service packs, and languages contained in all the linked profiles, and then check to make sure that each linked profile contains a target for all the operating systems, service packs, and languages in the superset. User devices must have a target in each of the linked profiles or they cannot launch any applications in any of the linked profiles.

- **Available.** This profile property is available in the common range of target configurations.
- **Not Available.** This profile property is missing in one or more target configurations.

Continue the installation using the profiling wizard, as normal. After you save the profile enabled with inter-isolation communication, publish the applications using the Citrix AppCenter in XenApp.

To view or modify the contents of the inter-isolation communication profile, from the navigation panel, select the profile; from the Edit menu, select Profile Properties; and from the navigation pane, select Linked Profiles.

Linked profiles are stored within the .profile file by name rather than by the path. At application launch, the profiler service searches the INSTALLROOT locations of the linked profiles.

When the user device runs a profile enabled for inter-isolation communication, the user-level settings that are stored on that user device by an application in one of the individual profiles are ignored, and the user-level settings of the application start fresh as if the application is being launched for the first time. To change this behavior, write a pre-launch script to migrate settings from specific applications whenever the linked profile is executed on the user device.
To select an install option

In the profiling wizard, choose an installation option according to the type of application or number of applications you want to install in a target:

- **Quick Install.** Select this option if you are installing only one application and it has an installation program, such as setup.msi or .exe (recommended for normal installations).

- **Advanced Install.** Select this option if you are installing Internet Explorer plug-ins, editing registry settings, installing an application manually, or installing from multiple installers. Also, use this option to update profiles built using a previous version of the profiler. Enhancements from the new version of the profiler are applied to the profile. You can perform more installations or finish the profile.
To install multiple applications through Advanced Install

The **Advanced Install** option of the profiling wizard provides the opportunity to repeat the installation procedure as many times as you need to add multiple applications to a target.

1. Choose the type of resource you want to install:
   - To install an application in the target, choose **Run install program or command line script**. This option runs a wizard similar to the quick install.
   - To install Internet Explorer and plug-ins so they run in isolation, choose **Install IE plug-ins**.
   - To add files and folders that might be needed on the user device or to remove unneeded files and folders, choose **Select files and folders**. For example, use this option to include required files that are on the profiler workstation, but might not be on the user device.
   - To customize the registry as viewed by the user device, choose **Edit registry**. Each of these options provides you with the opportunity to return to this screen and install additional applications.

2. After you complete an installation, you have the option to install additional resources in the target. If needed, check the option to **Run an application before the next installation**.

3. After installing all the applications you want to include, choose **Finish** or **Continue with none of the above**, which enables you to finish creating the target.
To choose an installation program for the application

Select the initial executable for the application in the profiling wizard. To update an application in an existing profile, open the profile, select the target, and from the Edit menu, select Update/Install Application.

On the Choose Installer page:

- Click Browse to choose an executable file or a script you run to install the application in the current target. In this step you are just choosing the installer, not running it.

  **Note:** Make sure that the application is not currently installed on the profiling workstation. Files that exist on the profiling workstation are not added to the profile, causing the application to fail when launched from the profile.

- Optionally, add a command-line script. Command-line arguments run a streamed application by modifying its properties in the target. If you add placeholders in the profile, they are replaced by command-line arguments specified when you publish the application. Command-line parameters can modify application properties after you install the application during the target creation process (in the New Profile or Add New Target wizards) or by editing application properties after you create the target.

  If you do not use a placeholder in the profile, the extra parameters specified when publishing an application are added at the end of the command-line.

**Example of Placeholders and Command-Line Parameters**

Use profile arguments to specify command-line arguments that you always want to apply during application launch, such as arguments necessary for the application to function. Use the published application’s command-line arguments to fine-tune the application.

If you add the ** placeholder to the **Command line parameters (optional) text box in the profiler, the placeholder is replaced with the command-line arguments for the published application.

To do this:

1. Specify the following arguments and placeholder in the professed application:

   ```
   app.exe /a ** /b
   ```

   where <app.exe> is the application executable that you are profiling.
To choose an installation program for the application

2. Publish the application with the following arguments. (%* specifies the content redirection arguments.)

   /x %* /y

Launch the application with content redirection. For example, on a file named my.doc, the steps are:

1. The profiled application command-line is used.

   app.exe /a ** /b

2. The ** placeholder is replaced with the published application arguments.

   app.exe /a /x %* /y /b

3. The file for content redirection replaces the %*, producing the final command-line.

   app.exe /a /x my.doc /y /b
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**

In addition to pooled XenDesktop environments, this option is also beneficial in environments that operate without a physical hard disk, such as XenApp running on virtual servers. If the RadeCache location for the “local” hard disk is across the network to a virtual
To create a virtual hard disk

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 support legacy plug-ins

By default, the Streaming Profiler 6.5 creates SHA-256 hashes, and the Offline Plug-in 6.5 uses SHA-256 to verify the contents of the profile and verify the integrity of strings and buffers.

The Offline Plug-in 6.0.x, however, launches applications only from profiles with SHA-1 hashes, such as from version 6.0 of the profiler. To enable 6.0.x plug-ins to launch profiles created with Streaming Profiler 6.5, select this option to provide the additional hashes. Use this option during a transition period where both hashes are needed until all Offline Plug-ins have been updated to 6.5.

SHA-2 is fully supported on Windows Server 2008 R2. For earlier Windows platforms, see the Microsoft documentation.

If selected, the time required to generate both hashes increases the profiling time.

To add the SHA-1 hashes in profiles created or updated with version 6.5 of the profiler:

- In the profiling wizard, on the Legacy Offline Plug-in Support page, select the option to Enable support for 6.0 offline plug-ins.

- To set the preference for all profiles, from the Edit menu, select Preferences > Legacy Offline Plug-in Support, and select the check box. The setting becomes the default in the profiling wizard for all profiles created or updated after setting this option.

For more information about security standards that apply to Citrix products, see XenApp 6 Security Standards and Deployment Scenarios in Citrix eDocs.
To install Internet Explorer plug-ins

Use this **Advanced Install** option while running the profiling wizard to make Microsoft Internet Explorer available as a streamed application so that it runs inside isolation on the end-user device.

1. If you have Internet Explorer running, close it.

2. While running the New Profile or New Target wizard, complete the initial options and choose the **Advanced Install** option.

3. From the **Select Install Method** window of the wizard, choose **Install IE plug-ins**.

4. Click **Launch Microsoft Internet Explorer**. This command runs Internet Explorer in an isolation environment.

5. Using Internet Explorer, install all the plug-ins to be made available to your users.
To include files and folders in a target

Use this option to include specific files and folders that are not installed by an application installer but are required for the application to run. This method can also profile applications that do not need to be installed to run.

1. While running the New Profile or New Target wizard, complete the initial options and choose the **Advanced Install** option.

2. From the **Select Install Method** window of the wizard, choose **Select files and folders**.

3. Select the files and folders you want to include.
   a. Use the **Look in** pull-down menu to select files and folders to include in the target.
   b. In the **Select files** list, select the files you want to include in the target and click the arrow to add them to the **Current files** list.
   c. Use the buttons at the bottom of the **Current files** list to create new folders, rename files and folders, or delete files and folders in the **Current files** list.

4. The profiler automatically performs a **virtual restart** if a restart is required to complete the installation.

5. Click **Finish Installations** and click **Next**.

6. On the **Run Application** page, click **Add** (do not select the Run option).

7. In the **Open** dialog box, enter a shortcut name and browse to the executable name that you want to run, but make sure to stay within the Device\C folder. Do not browse to the source location; the path is connected automatically.

8. Finish the profile, save it to the App Hub, and publish the application in the Citrix AppCenter.
To include registry settings

Use this option to provide customized registry settings in a target.

**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.

1. If you have Windows Registry Editor open, close it.

2. While running the New Profile or New Target wizard, complete the initial options and choose the **Advanced Install** option.

3. From the **Select Install Method** page of the wizard, choose **Edit registry**.

4. Click **Launch Windows Registry Editor**.

5. Use Registry Editor to make the registry changes you want to include in the target. The registry changes you make are included in the isolation environment of the target, not the registry on your profiler workstation.

6. The profiler automatically performs a virtual restart if a restart is required to complete the installation.
To install an application in the profile

In the profiling wizard, on the **Run Installer** page, ensure that the installation program and command-line parameters that you selected on the previous page are correct. This step performs a virtual installation of the application in the profile, but not on the profiling workstation.

1. Click **Launch Installer**. Wait until the installer program launches on the workstation. For large applications, this can take several minutes.

2. Complete a full installation for the application, including running the installation wizard. The destination path shown in the installer does not matter because the application is installed in the profile, so accept the default location.

3. When the application is fully launched on the workstation, close the application and click **Next** in the profiling wizard for the profiler to discover the newly installed application.

   If a restart is required to complete the installation, the profiler automatically performs a virtual restart. After the virtual restart completes, the application is ready to run on the next page of the wizard.
To run an application in the profiler

Many applications require initialization on the first launch of the program, such as accepting the license or supplying a license key. As a best practice, use the Run Applications page to perform these tasks for your users.

On the Run Application page:

- If the application is not already in the list, click Add and browse to and select the application executable file
- Select the application in the list and click Run

After the application is fully initialized, close it and continue in the profiling wizard by selecting the applications that you want to make available for publishing.
To select applications for listing in the profile

Use the **Select Applications** pane of the New Profile, New Target, and Update Application wizards to list applications in the target and make them available for publishing later in the Citrix AppCenter.

In the **Select Applications** pane, all previously listed applications from other targets in the profile are listed as well as applications discovered in the current target you are adding.

- **Application Name** gives you an indication as to whether or not you must modify the application name. If the names of applications in multiple targets match, those applications are considered available in those targets.

- To add other, undiscovered applications you installed in the target, click **Add** and browse to and select the applications you want to add to the **Applications** list.

- To remove applications from the list, select the unwanted applications and click **Delete**. This removes the applications only from the list. It does not delete the application from the target.

- If you want to change properties of the application before completing target creation, select the application whose properties you want to change and click **Modify**. Change properties including the name, version number, location of the executable, current working directory, application icon, and command-line parameters.

  An example of when you might want to change an application property is when the name of the application contains a version number or is different from the same or similar applications in other targets. In such a case, remove the version number or change the name so the application is recognized as existing in other targets.

- If the Applications list is not populated, click **Recover** to find newly installed applications and populate the **Applications** list.
To sign a profile

Application streaming to desktops can use digital signatures to authenticate the origin and integrity of profiles signed by a trusted publisher. The signed profile applies to all applications and files contained in the profile. Applications from signed profiles are checked by user devices that have a trust list installed and can authenticate the code-signed certificate against the trust list. When signing is enabled, the user device checks the integrity of each file as it is cached.

After you install and configure your code-signing certificates, sign profiles through the New Profile, New Target, and Update Target wizards. To view or modify the signature settings for the profile, from the Tools menu, select Sign Profile.

To sign a profile, you need a code-signing certificate on the profiler workstation and a Certificate Trust List certificate for certificate verification on the user device. Also, you must know the password for the certificate you are using to sign.

- To sign the profile using a certificate residing on the drive, choose Sign using key from selectable file and browse and select your certificate file

- To sign the profile using the code-signing certificate installed on your profiler workstation, choose Sign using locally installed certificate

Signing a linked profile created for inter-isolation communication does not sign the individual profiles automatically. Instead, each linked profile must be signed separately.

Remove a signature from a signed profile at any time by opening the profile, and from the Tools menu, select Unsign Profile.

Additionally, to set a default signature setting for profiles and skip this page in future profiling, you can set a preference to disable or enable profile signing.
Editing Profiles

After you create an initial profile and target, use the profiler to modify and maintain the profile. For example, to make applications available to more user devices, add targets to a profile that match additional and unique combinations of target criteria. For example, you can add separate targets for English, French, German, and Japanese language-based operating systems.

Use the profiler to add new targets, delete targets or folders from a profile, delete old profiles, and resolve invalid shortcuts or target conflicts.

**Note:** For steps to revert back to an older version of a profile, see [http://support.citrix.com/article/CTX120436](http://support.citrix.com/article/CTX120436).

To modify the profile properties, with the profile open in the profiler, select the profile name, and from the Edit menu, select **Profile Properties**.

Profiles have the following properties:

- **Information.** Contains general properties, which are the name, description, location, size, and creation and modification dates of a profile.

- **Applications.** Lists the settings of all applications from all targets and their availability.

- **File Types.** Lists the file types registered for the applications in the profile.

- **Linked Profiles** (visible for profiles set up for inter-isolation communication only). Lists the individual profiles included in the linked profile.

- **User Profile Security.** Specifies type of security enabled for the profile.

- **Pre-launch Analysis.** Enables the profile to examine the user device for the existence of required applications, files, or registry entries before streaming the application.

- **Pre-launch and Post-exit Scripts.** Adds scripts to run prior to and following the execution of applications in the target.
To view profile information

1. Start the profiler by opening the Start menu and choosing Programs > Citrix > Streaming Profiler > Streaming Profiler.

2. To open the profile, from the File menu of the profiler, choose Open.

3. Select the manifest (.profile) file of the profile stored on the file share. (Alternatively, click Open Profile on the Welcome screen.) For example: \hostname\fileshare\Profile Name\Profile Name.profile

When you open a profile, the profiler displays tabs for the following profile information:

- Information
- Targets
- Applications
- File Types
- Digital Signatures

From the Edit menu, choose Profile Properties to view the profile properties.

4. Select the target in the left pane of the profiler to view information about a target.

The right pane displays the following tabs for information about the target:

- Information
- Applications
- File Types

Select the target, and from the Edit menu, choose Target Properties to view the target properties.
To edit the profile name, description, or location

You set the name, description, and location of the profile while using the profiling wizard.

To view or modify the setting later, from the navigation panel, select the profile; from the Edit menu, select Profile Properties; and from the navigation pane, select General.

This page displays the following information about a profile:

- **Profile name.** Manifest name of the profile. To modify the name or folder location on the file share, select File > Save as, and enter the new Profile name or path; for example, a UNC might be: \hostname\FileShare\Profile Name\Profile Name.profile.

- **Description.** Add or modify a description of the profile.

- **Location.** The storage location of the profile.

- **Size.** The size of the profile.

- **Created.** The date set by the profiler.

- **Last updated.** The date set by the profiler.
To view details about applications in a profile

Use the application properties to view the settings for all the applications from all targets and their availability. When an application is available, you can publish it using the Citrix AppCenter included with XenApp.

To view the settings for the applications in the profile, from the navigation panel, select the profile; from the Edit menu, select Profile Properties; and in the navigation pane, select Applications.

The page lists the applications in the profile and whether or not the application is available in all targets in the profile.

To view more information about an application included in the target, select the application and click View Details. The details displayed about the listed application are:

- Name of the targets in which the application is installed
- Whether or not the application is available in all targets
- Version number of the application
- Path to the application within the isolation environment
- Working directory the application uses within the isolation environment

Note that the version number displayed here is not the same as the target version number. The version number displayed here is set by the application installer.

Alternatively, click Find Application if the application is missing from the target.

To modify the remainder of the properties, update the target in which the application is installed.
To view File Type Associations set in a profile

Specify the File Type Associations (FTAs) initially in the profiling wizard. FTAs are used during application publishing so that opening a file of a certain type on the user device invokes this streamed application. The profiler detects FTAs automatically for the application (adding custom FTAs is not supported in the profiler).

To view or modify the setting later, from the navigation panel, select the profile; from the Edit menu, select Profile Properties; and from the navigation pane, select File Types.

The File Types page displays the following information:

- File type extension.
- Description of the file type.
- Application invoked by the file.
- Whether or not the application is currently available to users. Use the options on the page to view the details about file types for each target in the profile.

To modify these properties, update the target in which the application is installed.
To check for launch prerequisites

After testing a profile, if you determine that user devices must have certain applications installed locally to run the application, such as a version of Microsoft Internet Explorer, you can enable a pre-launch analysis of the user device. When enabled, if a user device does not have the prerequisites for the profiled application to run correctly, profile execution stops and alerts the user of the problem.

To specify these requirements, from the Edit menu, select Profile Properties and use the Pre-launch Analysis page and check Enable pre-launch analysis to inspect the user device for prerequisites before streaming the profiled application. By default, you define analysis for a profile and all its targets.

If you determine that a target requires an analysis that is different from the default for the profile, select Edit > Target Properties, clear the Use profile settings check box, and specify the analysis for the target.

On the Pre-launch Analysis page, click Add Item under the section appropriate to what you want to add: Applications and files or Registry entries.

The prerequisites that pre-launch analysis can look at are:

- Applications and versions (specific or a range)
- Binary files and versions (specific or a range)
- Registry entries
To check for prerequisite registry entries

After clicking Add Item from the Registry entries section of the Pre-launch Analysis tab, use the Add Registry Entry dialog box to specify the registry entry you want to identify as a prerequisite.

To identify a registry entry, provide the required hive, key, value name, and type information:

1. From the Registry type drop-down list, choose a selection:
   
   - **Key exists.** The key must exist, whether or not it has subkeys or values.
   
   - **Key and value exist.** The key must have a value of the specified type, but the data is not checked.
   
   - **Key and value exist, and data matches.** The key must have a value of the specified type, and the data for the value must exactly match the specified data.
   
   - **Key exists, and data for default value matches.** The key must exist, and the data for its default value must match the specified data.

2. From the Hive drop-down list, choose the registry hive in which the registry entry resides:
   
   - HKEY_LOCAL_MACHINE
   
   - HKEY_CURRENT_USER
   
   - HKEY_CURRENT_CONFIG
   
   - HKEY_CLASSES_ROOT
   
   - HKEY_USERS

3. Type the name of the key. The following is an example: Environment

4. Type the value name. The following is an example: TEMP

5. To select the matching registry type for the prerequisite you are choosing, use the Type pull-down menu:
   
   - String value (REG_SZ)
   
   - Binary value (REG_BINARY)
   
   - DWORD value (REG_DWORD)
   
   - Multi-string value (REG_MULTI_SZ)
   
   - Expandable string value (REG_EXPAND_SZ)
To check for prerequisite registry entries

- QWORD value

6. When you select a type, the list updates to reflect the registry entries.
To check for prerequisite applications and files

After clicking Add Item from the Applications and files section of the Pre-launch Analysis tab, use the Add dialog box to add an application or binary file:

1. Choose the application you want to identify as a prerequisite. (Note that the list of applications is static.)

2. Browse to and choose the binary file you want to identify as a prerequisite.

3. Select whether or not you want to check for a specific version or range.

To specify pre-launch and post-exit scripts

After testing a profile, if you determine that certain operations are required before or after running the application, you can write scripts and add them to the profile.

To specify these operations, from the Edit menu, select Profile Properties and use the Pre-launch & Post-exit Scripts page to select scripts. By default, you define scripts for a profile and all its targets.

If you determine that a target requires scripts that are different from the default for the profile, select Edit > Target Properties, and on the Pre-launch & Post-exit Scripts page, clear the Use profile scripts check box, and specify the scripts for the target.

On the Pre-launch and Post-exit Scripts page:

1. Click Add Item next to Pre-launch scripts or Post-exit scripts.
2. Choose whether or not to run the script within the isolation environment by clicking one of the option buttons Isolate script or Do not isolate script.
3. Select the script you want to use.
4. Specify any command-line parameters required by the script.
5. Specify the order in which they run. The Offline Plug-in runs scripts in the order they are listed.

Pre-launch and post-exit scripts are commonly CMD files, but can be any file executable by Windows. You create pre-launch and post-exit scripts independent of the profiler. Valid file extensions are included in the PATHEXT environment variable, which shows a list of file extensions that are considered to be executable.

In addition to the default file extensions, add new file extensions, if needed, by adding them on the profiling workstation in the system variable PATHEXT. Complete these changes before you launch the profiler, or re-launch it to capture the updates. After you add them, they are read from the registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment in the PATHEXT element.

For example, to copy dynamic files each time a user launches a certain application, create a VB Script or batch file that copies those files or runs a utility each time the application starts and exits.
When adding a target to a profile, ensure the target is unique from other targets in the profile. The profiler does not permit saving a target that overlaps with any other target in the profile.

1. In the navigation pane of the profiler, select the profile.
2. From the profiler Edit menu, choose Add New Target.
3. Set target operating system and language. If the new target overlaps with other targets in the profile, a message box appears showing the target conflict.
   For more information, see To resolve target conflicts.
4. Choose an installation option according to the type of application or number of applications you want to install in a target, and finish the wizard.
To resolve target conflicts

After creating an initial target, additional targets cannot have overlapping operating systems, service pack levels, or languages.

To resolve target conflicts in the profiling wizard, you must either change the supported languages to remove the language overlap, or change the operating systems and service packs to remove the operating system overlap.

Conflicts occur when your new target overlaps or duplicates the configuration of an existing target. Target conflicts include all of the following situations:

- Operating system overlap. Both targets support an operating system and service pack level. For example, if both targets support Windows Vista with no service packs, there is an operating system overlap.
- Language overlap. Both targets have at least one language in common.
- System drive overlap. Both targets have the same boot drive. However, the boot drive of a target cannot be changed after the target is created.

More simply, two targets overlap if:

- There is an operating system overlap and
- There is a language overlap and
- The boot drive letters are the same

For example, the following targets overlap because they share an operating system, language, and boot drive, and they cannot coexist in the same profile:

- **Target A:**
  
  Windows XP Professional [SP 2 and above] and Windows Server 2003 with CPS [all service packs]

  English and French languages

  Boot drive C

- **Target B:**
  
  Windows XP Professional [all Service Packs]

  English language
To resolve target conflicts

Boot drive C
To resolve invalid shortcuts

If a message appears referring to invalid shortcuts, the profiler did not install the applications referred to by the shortcuts in the list. Whether or not this is an error depends on which programs you intend to publish.

**Important:** Files that exist on the profiler workstation's hard drive are not installed in targets.

Even if the profiler workstation appears clean and has no installed applications other than the profiler, sometimes essential programs like antivirus software include other program installations. In addition, some uninstallers do not remove all program files from the hard drive.

**What should you do?**

- If the missing application is not needed for your publishing, do nothing. Click OK and proceed.

- If the missing application is one that you intend to publish, cancel the wizard, exit the profiler, and remove the existing files from the profiler workstation. Then repeat the profiling operation.
To delete a target from a profile

1. Start the profiler by opening the Start menu and choosing Programs > Citrix > Streaming Profiler > Streaming Profiler.

2. To open the profile, from the File menu of the profiler, choose Open.

3. Open the manifest (.profile) file of the profile stored on the file share, such as: \hostname\fileshare\Profile Name\Profile Name.profile

4. In the left pane of the profiler, select the target you want to delete.

5. In the right pane, click the Information tab and note the location.

6. From the Edit menu, choose Delete Target.

When you save the profile, the profiler deletes the associated target directory from the profile on the file share and removes associated entries from the profile manifest.
To delete a folder from a profile

1. With the profiler open, select the target and click Update/Install Application.

2. When the updating wizard opens, select the Advanced Install option.

3. Click Select files and folders.

4. In the Current files pane, select the target files or folders and click the icon to delete them. Finish the profiling wizard.
To remove a profile from a linked profile

If a profile is linked to a profile that is enabled for inter-isolation communication, you can remove the link by editing the properties of the inter-isolation profile.

1. Open the profile enabled for inter-isolation communication.
2. From the Edit menu, open the Profile properties.
3. Click the Linked Profiles tab.
4. Clear the check box for the profiles that you want to remove from the inter-isolation communication profile.

When you save the linked profile, the profiler deletes the target directory from the profile on the file share and removes linked entries from the profile manifest.
Editing Targets

If users experience problems running applications in a profile, edit the target properties to resolve some of those problems. To view the targets, with the profile open in the Profiler, select the target and from the Edit menu, select Target Properties.

Targets have the following properties:

- **General.** Contains name and description, as well as the operating systems, languages, boot drive, version, location, and creation and modification dates of the current target.

- **Applications.** Contains names and version numbers of applications installed in the target, as well as the paths to the application executables, and whether or not the applications are available in all the other targets in the profile.

- **Target Operating System and Language.** Specifies the user devices that can run applications installed in the target.

- **Rules.** Governs how the isolation environment functions when running an application on the user device.

- **Pre-launch Analysis.** Ensures the existence of required applications on the user device and required registry entries in the isolation environment before streaming the applications in the target. If the check box to Use Profile settings is selected, the settings are identical to those in Profile Properties.

- **Pre-launch and Post-exit Scripts.** Specifies the scripts to run prior to and following the execution of applications in the target. If the check box to Use Profile settings is selected, the settings are identical to those in Profile Properties.

- **Services.** Lists the services installed in the profile that are available for the target, including the logon name, path, and start type (manual or automatic). When started, these services run in isolation on the user device.
To edit the target name and description

Modify the description of a target on the General tab of Target Properties. The target name that you select when you create the target cannot be changed except by the user. Use the properties to modify or add a description and view the creation and modification time stamps of a target. These are set by the profiler at the time you save a target.
To modify the application properties in the target

Use the Applications page of Target Properties to view information about or manage the applications installed in the current target.

The Application page displays the following information about listed applications:

- **Application name.** Manually set from the profiler by the administrator when the application is installed in the target.

- **Availability.** Specifies whether or not the application is available, not in this target, or not in other targets.

- **Version.** Set by the administrator who installed the application into the profile.

- **Path and Working Directory.** Set by the application installer. The path is not the true path to the application executable, but it is the path simulated by the isolation environment.

- **Command line parameters.** Manually set from the profiler by the administrator when the application was installed.

To modify the list of applications, use the following methods:

- **To recover or add applications to the list:**

  If you suspect the list of applications is not complete, click Recover to force the profiler to discover all applications installed in the target. If the operating system of the workstation on which you are currently running the profiler does not match the operating system of the current target, the recover function is not available.

  If you want to browse to an application and add it manually, click Add. When you add or recover an application, data about the application is added to the profile manifest file.

- **To delete files from the list:**

  You might want to delete an application from the list if it is auxiliary, as with an uninstall or update application.

  When you delete an application from the list, the profiler removes only application data from the profile manifest file. The profiler does not delete the application files. Add a deleted application back to the list by clicking Recover or Add.

- **To modify an entry in the list:**

  You might want to modify an application in the list if the application name or icon is different from other similar applications in other targets or contains a version number.
To modify the application properties in the target
To modify the operating system and language properties of a target

To expand or restrict the different user devices that can run applications in a target, use the Target Operating System and Language tab of Target Properties to modify these properties.

1. Under target operating systems, check the operating systems you want user devices to match to access the current target.

2. To modify the service packs required for a match, click Set Service Pack and then specify the service pack criteria.

3. Under target language, check the languages you want user devices to match to access the current target.

The updated settings apply to targets when you save the changes.
To update a target

To upgrade an application within a target or add applications to a target, use the profiler to update a target.

When you update a target, the profiler increments the version number and saves the target as a new file in the profile.

To provide uninterrupted service to your users, the profiler maintains multiple versions of each target. After you save the profile, user devices use the most recent version of the target for new application executions. Application executions that are in progress continue to use the version of the target that was current when the applications were invoked. This enables you to update targets without forcing your users to exit the applications and restart. The next time the users run the application, they run the newest version in the target.

After saving an updated profile, do not use the profiler to delete or modify previous versions of an updated target.

1. In the left pane of the profiler, with the profile open, select the target whose application you want to update.

2. From the Edit menu, choose Update/Install Application.

3. Choose an installation option according to the type of application or number of applications you want to install in a target.
   
   · If you want to update a single application in a target or add a single application to a target without adding any additional files, folders, or registry entries, choose Quick Install.

   · If you want to add multiple applications in a target or add Internet Explorer plug-ins, files and folders, or registry settings to the target, choose Advanced Install.

After you update the target, save the updated profile in the original location. The next time user devices connect, they stream the updated profile.

If user devices have a previous version of the cabinet file stored in the cache (such as applications enabled for offline access), the streaming service uses a technique called differential synchronization to open the cached cabinet file on the user device and compare it with the updated cabinet file in the profile. The service updates only the changed files and removes outdated files from the cabinet file in the cache. This feature reduces the time and bandwidth needed to update applications on the user device.
To remove an old version of an updated target

To recover disk space on the file share that hosts your streaming application profile, delete prior versions of a target that has been updated. The prior versions of an updated target are no longer available through the profiler. Do not manually remove the most recent version of a target.

1. In the left pane of the profiler, with the profile open, select the target whose application you updated.

2. In the right pane, on the Information tab, note the path to your updated target directory folder.

   The trailing integers of the folder name represent the target version number. For example, the version of the following folder is “2”:

   ```text
   \\hostname\fileshare\Profile Name\720edd68-0972-49e6-aa00-80974eb81d5b_2
   ```

   To choose directory folders that are obsolete, identify the folders that have trailing integers of the least value.

3. Use Windows Explorer to delete the obsolete folders from the profile on your file share.
Profile Contents on the Server

After you create and store an application profile on a file server, the profile consists of directories and subdirectories of files. For your reference, this topic describes the structure of profile directories and the files in them. Citrix recommends that you do not modify these files directly.

Use the profiler to modify the contents of the profile folder:

- Profile manifest file (.profile), an XML file that defines the profile
- Target directory providing isolation environment contents for applications in the targets
- Hash key file (Hashes.txt) for digital signatures and signing profiles
- Icons repository (Icondata.bin)
- Scripts folder for pre-launch and post-exit scripts

For example, if you create a profile called PDF Viewer with a single target, the profile, a folder called PDF Viewer, has contents similar to the following on the file share:

- PDF Viewer.profile (the manifest file)
- 720edd68-0972-49e6-aa00-80974eb81d5b_1 (the target directory folder, first version)
- Hashes.txt
- Icondata.bin
- Scripts folder
Manifest File

The manifest (.profile) is the top file in the data structure that defines a profile. The manifest file is an XML-formatted text file that describes a profile. Manifest files have the file extension .profile.

The information in a manifest file includes:

- Description
- Create date
- Modify date
- User profile security (Boolean)
- Scripts
- File type association
- Internet Explorer application (Boolean)
- Applications
- Targets

The manifest file of a profile created for inter-isolation communication includes references to the subprofiles and may or may not have targets listed in the manifest file.
Targets

Each target consists of a set of files representing a compressed subdirectory structure within the profile structure.

Target file names are based on the target GUID and version. The association to a user level concept, such as “MS Office,” comes from the profile manifest.

Each time a target is created, it is assigned a GUID so it can be uniquely identified and independently cached on the user device. The GUID is used to set the name of the isolation environment so that no two different installations of the same named target occupy the same location in the execution system cache. The directory used to store the isolation environment on the user device also includes the version number of the target. In this way, when you update a target, user devices are assured that the execution InstallRoot accurately reflects the install root of the target you defined. For speed, the user device locally updates the internal file cache when a target version is updated rather than reloading from the server.

If a profile is copied (including its targets), the GUID is unchanged. If a profile is new (when you use save as), the new profile has new targets, and new GUIDs are assigned for the targets in that profile. Use them to maintain each profile separately without conflicts if you update either one.
Digital Signature

You have the option of digitally signing the contents of a profile. The manifest file indicates if the profile is signed, and when signed, the manifest file is digitally signed to sign the entire profile. The hashes for all files in a target are stored in a single file, Hashes.txt.

The SHA-256 of the Hashes.txt file in the profile is stored in the manifest, and the SHA-256 hash of each target in the profile is stored in the manifest. Because the manifest file is digitally signed, the SHA 256 of each file listed in each Hashes.txt file can be authenticated.
To keep the manifest file size small, the binary data that represents the application icons is stored in a separate file called icondata.bin. The profiler stores all icons for the installed application. When you publish the streamed application, you have the option to change the icon by choosing among the set of icons that the application installed or other icons that you prefer.
Specify when the Citrix Offline Plug-in should execute scripts associated with a profile or target:

- Before the Plug-in executes the first application from a profile
- After the Plug-in terminates the last application from a profile

Intermediate applications executed from a profile do not invoke pre-launch or post-exit scripts.

Scripts are commonly .CMD files, but can be any file that Windows can execute. Create pre-launch and post-exit scripts independent of the profiler, and after creating a script, use the profiler to add the script to a target, including these settings:

- A disk file that is executed
- Arguments for the executable
- A Boolean value indicating whether or not the script is enabled

When you add a script to a target, the profiler copies the script file to the profile. The profiler also retains the original file name of the script.

If an .EXE script requires a .DLL file, add a script for the .DLL file and disable it. The .DLL file is available for the script to load, but the user device does not run the disabled .DLL. For example, use this technique to add a signed .DLL to the profile even though it is not executed.
To stream applications to user devices, start by reviewing the System Requirements for Application Streaming.

Before publishing an application for streaming, you must use the Citrix Streaming Profiler, a stand-alone utility, to create a streaming application profile and save the profile on a network file share or Web server (your App Hub). For instructions, search for Creating Application Profiles. In particular, see To create a profile and target, as well as other topics in that section.

After creating the application profile, continue by publishing the application to make it available to users. When you publish an application, you make choices about how to deliver the application and its properties. Use the Publish Application wizard in the Citrix AppCenter, the same wizard you use to publish installed applications. To review the general steps in the wizard, see To publish a resource using the Publish Application wizard.

In the wizard, select the delivery options to publish the application for streaming. For guidance, see To select a streaming delivery method. Continue by locating the application profile stored in your App Hub and finish the wizard.

In addition, refer to other topics about application properties and preferences and how to configure offline access (optional).

Finally, to prepare user devices for streaming, see Deciding Which Plug-ins to Use for Application Streaming, as well as other topics about the Citrix Plug-ins.

**Important:** To launch streamed applications, user devices must have sufficient RAM locally.
To select a streaming delivery method

You select the resource type in the Citrix AppCenter while running the Publish Application wizard.

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.

1. To open the Publish Application wizard, from the AppCenter, under the XenApp node, expand the farm or server to which you want to publish an application. Select the Applications node, and from the Actions pane, choose Publish application and follow the instructions in the wizard.

   Optionally, to change the delivery method after publishing an application, from the Action menu, select Other Tasks > Change application type and follow the instructions in the wizard.

2. In the Publish Application wizard, on the Type page, select Application.

3. Select a delivery method from the Application type list:

   - Accessed from a server. Users launch the application that runs on a XenApp server and uses shared server resources, or launch it from a Web browser using a Web Interface site you create. If you choose this option, you must then enter the location of the executable file for the application and the XenApp server on which it will run. This is the typical application type unless you intend to stream your applications to the client desktop. With this method, users access the applications using the Citrix Receiver. This method does not support desktop integration or offline access to applications.

   From the Server application type list, select the delivery method:

   - Installed application. Users launch the application installed on a XenApp server.

   - Streamed to server. The application in 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 Citrix Receiver; the Offline Plug-in is not required on the user device. With this method, users access the applications using the Citrix Receiver. This method does not support desktop integration or offline access to applications.

   - Streamed if possible, otherwise accessed from a server (called dual mode streaming). Grants users access to a profiled application that streams from the file share to their user devices and launches locally from within an isolation environment. Alternatively, user devices that do not support streamed applications (such as when they do not have the Offline Plug-in installed) instead use an ICA connection to access the application installed on or streamed from a XenApp server.
To select a streaming delivery method

From the **Server application type** list, select the *alternative* delivery method for user devices that do not support streaming to user device:

- **Installed application.** Users launch the application installed on a XenApp server.

- **Streamed to server.** The application in 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 Citrix Receiver; the Offline Plug-in is not required on the user device. With this method, users access the applications using the Citrix Receiver. This method does not support desktop integration or offline access to applications.

- **Streamed to client.** With this method, you make available the full set of application streaming features. When you stream applications directly to client desktops, some of the application files are cached locally and the application runs locally from within an isolation environment using the resources of the user device.

  - Users must have both the Offline Plug-in and Citrix Receiver installed locally.

  - With this delivery method, you can 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.

  - User devices that do not support client-side application virtualization (such as, they use a non-Windows client) or do not have the Offline Plug-in installed locally cannot launch the application.

**Note:** You can also force a delivery method for applications published as "Streamed to client" based on filters. To do this, configure the Load Balancing policy setting (located in the AppCenter) for **Streamed App Delivery**. The policy setting overrides the selection in the publishing wizard.
To force a delivery method for streamed applications

Use the Load Balancing Policies to apply settings to sessions that are filtered for Web access, specific users, client devices, IP addresses, or server. Use the delivery method policy to override the delivery method of applications published as stream to client.

If you disable the policy setting or do not configure it, the delivery method specified in the Publish Application wizard is used.

1. From the Citrix AppCenter, select the farm.
2. Under the server, select Load Balancing Policies.
3. From the Actions pane, configure the policy settings for Streamed App Delivery.
4. Select one of the following options:
   - Allow applications to stream to the client or run on a Terminal Server (default setting).
   - Force applications to stream to the client. User devices always stream the application from the App Hub to the user devices. Users must have the Offline Plug-in installed and access the application using the Citrix Receiver or a Web Interface site. For example, you might use this setting to prevent the use of server resources. User devices without the Offline Plug-in and Citrix Receiver cannot launch the application.
   - Do not allow applications to stream to the client. Users always launch streamed applications from the server. For example, you might use this option to prevent applications from streaming to specific clients. In addition:
     - If you publish a streaming application with Streamed if possible, otherwise accessed from a server (dual mode streaming), users always launch the application from the server using the alternative method you selected.
     - If you publish an application as Streamed to client (without dual mode), the connection fails.

This table describes the default delivery of each application type and the results of setting the policy. The policy setting overrides the delivery protocol for applications that are published as “streamed to client.”

<table>
<thead>
<tr>
<th>Application type</th>
<th>No policy (default delivery)</th>
<th>With policy: Do not allow stream to client</th>
<th>With policy: Force stream to client</th>
</tr>
</thead>
</table>
To force a delivery method for streamed applications

<table>
<thead>
<tr>
<th>Streamed to client</th>
<th>Offline Plug-in streams application to desktop.</th>
<th>Connection fails.</th>
<th>Connection works.</th>
</tr>
</thead>
</table>

**Accessed from a server:**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Policy does not apply.</th>
<th>Policy does not apply.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed application</td>
<td>Citrix Receiver delivers the application installed on XenApp (not streamed).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Streamed to server</td>
<td>Offline Plug-in streams application from file share to XenApp and Citrix Receiver delivers the application from XenApp.</td>
<td>Policy does not apply.</td>
<td>Policy does not apply.</td>
</tr>
</tbody>
</table>

**Streamed if possible; otherwise accessed from a server (dual mode):**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Policy does not apply.</th>
<th>Offline Plug-in always streams application to desktop.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installed application</td>
<td>Dual mode: Offline Plug-in streams application to desktop. Otherwise, Citrix Receiver connects to the application installed on server (not streamed).</td>
<td></td>
<td>Offline Plug-in always connects to application installed on server.</td>
</tr>
<tr>
<td>Streamed to server</td>
<td>Dual mode: Offline Plug-in streams application to desktop. Otherwise, Offline Plug-in streams application to the server.</td>
<td>Offline Plug-in always streams application to the server.</td>
<td>Offline Plug-in always streams application to desktop.</td>
</tr>
</tbody>
</table>
To provide HTTP or HTTPS delivery method

To stream a profile using the HTTP or HTTPS protocol delivery method, use the following example to configure a virtual directory on the Web server.

These steps assume that you already profiled the application and saved it to a file share using a UNC path.

To stream from an HTTPS address, see the additional steps at the end of this procedure. Note that HTTPS requires additional certificate setup. For assistance, contact your network administrator.

The Basic authentication scheme for HTTP is not allowed by default. To allow Basic authentication, create the following registry key:

- For 32-bit systems:
  HKEY_LOCAL_MACHINE\Software\Citrix\Rade\AllowUnsecuredHttpAuth

- For 64-bit systems: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Rade \AllowUnsecuredHttpAuth

  Type: REG_DWORD

  Value: 1

In the following example, the XenApp server, Web server, and file server are located on the same physical server. This is not a requirement.

To configure the Web server:

1. Create a file share, if one does not already exist. For example: Web server name: WebServer  Physical location on Web server: c:\webProfiles  The share name: webProfiles  An administrator must share this folder with the “everyone” group assigned READ access and the “administrators” group assigned WRITE access at both the share level and NTFS level. UNC path: \\WebServer\webProfiles

2. On the Web site hosting the profile, add the following MIME type information:

   - Extension: *

   - MIME type: application/octet-stream

   - Set "Execute Permissions" to NONE

   You can set this information for the Web site hosting the profiles or for a specific folder in the virtual directory that holds the profiles.

3. In addition, if the profile includes pre-launch or post-exit scripts, also add the following MIME type information for the file extension of each script, such as .bat or .com.
Extension: <file extension>, and MIME type: application/octet-stream

4. In the directory hosting the profiles:
   a. Open Properties and select the Directory tab.
   b. In the Configuration area, keep one application file extension (it doesn't matter which one you keep) and remove all the rest of the file extensions.
   c. Create a placeholder extension for application mapping; for example, ".testcitrix," which should not occur in the profile.
   d. Copy the settings from the file extension that remains (Step 4b) to the placeholder extension.
   e. Delete the file extension that remained in Step 4b, leaving only the placeholder extension from Step 4c.

5. Create a virtual Web site that points to the file share using the UNC path. For best results, do not use spaces in the URL. For example: HTTP (or HTTPS) path of virtual directory: http://WebServer.domain.com/webProfiles

6. Turn on Directory Browsing on the virtual Web site. Now you can test the configuration; continuing the example, browse to http://WebServer.domain.com/webProfiles/myApplication/myApplication.profile. If the Web server is configured correctly, the .profile file (not an error message). For HTTP, you have now completed the configuration of the Web server.

7. For HTTPS, additional binding configuration of the Web server is required. See the additional steps following this procedure, based on your operating system.

8. In the Citrix AppCenter, publish the application as Streamed to client, Streamed to server, or Streamed if possible, otherwise accessed from a server and continue in the wizard.

9. On the Location page, enter the full URL path (starting with HTTP or HTTPS) to the profile (browsing to an HTTP location is not supported at this time). Use a fully qualified domain name, not a relative domain name.

10. Click in the field titled Application to launch from the Citrix streaming application profile to select the application.

11. Finish the remaining pages of the wizard. The application is ready to stream to the client device using the HTTP delivery method.

To stream from an HTTPS address from Windows Server 2008 additional configuration is required on the Web server. An appropriate Web Server Certificate must be already installed:

1. From IIS, edit the Bindings for the Web Site.
2. In the Site Bindings dialog, click Add.
3. Under Type, choose https.
4. For **SSL certificate**, choose the installed Web Server Certificate.

5. Using the previous example, browse to `https://WebServer/webProfiles` on the Web server, which must be a member of the domain and have the root certificate installed.

To stream from an HTTPS address from Windows Server 2003, install a Web Server Certificate from a domain certificate authority:

1. From IIS, open **Properties** for the virtual Web site.

2. Click the **Directory Security** tab.

3. Under **Server Communications**, click **Server Certificate**.

4. Complete the Web Server Certificate wizard, and using the previous example, browse to `https://WebServer/webProfiles` on the Web server, which must be a member of the domain and have the root certificate installed.
Configuring Offline Access

Administrators can configure applications that are published to stream to desktops for offline access. This feature allows users to disconnect from the company network and continue to run their applications in offline mode for a specified length of time. No additional configuration is needed while profiling the application to create application profiles or targets that can be accessed offline.

After you configure the offline application policy settings and configure a streamed application for offline access, the next time the user device connects to XenApp, the Offline Plug-in downloads the application and caches it on the user device.

**Important:** Before you configure offline access, refer to System Requirements for Application Streaming for the supported platforms and system prerequisites for user devices.

- Step 1: Configure policy settings for offline access
- Step 2: Install the Citrix Receiver and Offline Plug-in on user devices
- Step 3: Publish the application for offline access

You can complete these steps in any order, but users cannot run applications in offline mode until all steps are completed.

**Step 1: Configure Policy Settings for Offline Applications**

Configure these Citrix policy settings for Offline Applications:

- **Offline app users** (required). Create a list of users or groups who have offline access permission and add that list both when creating the policy for Offline app users and when publishing the application.

  Users or groups listed in the offline app users policy setting and who are also configured for the application have permission to run offline-enabled applications in online and offline mode. Users who are configured for the application, but who are not added to the policy list can access the application online, but not offline.

  Users or groups on this list use an offline license to launch applications regardless of whether they are connected to the network or disconnected.

- **Offline app license period** (required). Specify the number of days applications can work offline before users have to renew the license (21 days by default, but can range from 2 to 365 days).

  For versions 1.0 through 5.1 of the plug-in, the license for each application in the profile is activated when the user launches the application the first time, for online or offline use. Beginning with version 5.2 of the plug-in, when the user launches an
application in the profile for the first time, for online or offline use, the offline license is activated for all other applications in the profile, as well. This occurs at the farm level. Thus, the offline license for all applications in the profile expires based on the date of the first application launched the first time, regardless of when the other applications are launched.

To configure licenses, administrators can use the License Management Console or command-line tools. They must also ensure they have a sufficient number of licenses to support the total number of users with offline access permission. Users who run XenApp hosted applications can also stream applications to user devices without requiring a separate license. For general information, in the topics for Licensing Your Product, see Getting Started with Citrix Licensing.

When users with offline access log on using the Receiver, they automatically either check out an offline license or renew a license already checked out. If users stay logged on, licenses are renewed automatically each day. If the license is near its expiration date while a user is running the application in offline mode, a notice appears reminding the user to log on (that is, change to online mode). When the user logs on, the offline license is renewed automatically if a license is available.

If the license expires and no license is available, the user cannot launch the application offline.

- **Offline app client trust** (optional). Use this setting to enable offline application user devices that have disconnected to recreate sessions when reconnecting, without authenticating again.

- **Offline app event logging** (optional). Use this setting to enable logging of offline application events to the event log on the server.

**Step 2: Install the Receiver and Offline Plug-in on User Devices**

To use the offline access feature, install both the Offline and the Receiver on the user device. The Offline Plug-in caches each streamed application on the hard drive of the user device. After the application is cached, the user can disconnect from the network or server and continue to run the application in offline mode for the period of time specified in the license.

**Step 3: Publish the Application for Offline Access**

The offline access feature is available only for applications that you publish as Streamed to client or Streamed if possible, otherwise accessed from a server.

In addition, when publishing an application for offline access, check the application's documentation and Web site to determine whether any special configuration is required on the user device to enable offline access of that application. For example, to stream Microsoft Outlook to the user device for offline access, users must enable the Microsoft Exchange Setting to “Use Cached Exchange Mode.”

Configure the application for offline access while publishing the application or later using the application properties:
Configuring Offline Access

- Enable the application for offline access and select the caching preference.
- Create a list of users or groups who have offline access permission and add that list both when creating the policy for Offline app users and when publishing the application.
## Offline Plug-in 6.6 for Windows

<table>
<thead>
<tr>
<th>About This Release</th>
<th>Deciding Which Receiver or Plug-in to Use for Application Streaming</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Requirements for Application Streaming</td>
<td>To install the Offline Plug-in</td>
</tr>
<tr>
<td>To configure the cache size of the Offline Plug-in</td>
<td>To deploy the Offline Plug-in using the command-line</td>
</tr>
<tr>
<td>To deliver the AppHubWhiteList to user devices</td>
<td>To deploy applications to user devices</td>
</tr>
</tbody>
</table>

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

The Offline Plug-in is the new name for the Streaming Client. 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.

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.
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`
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

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\`

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;http://www.webshare.organization.com;https://www.webshare.organization.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 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).
   · /qr shows a reduced user interface.
   · /I ""[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 /I “\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 /I “\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 | ANOTHERPROPERTY="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:

   

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 .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:


   [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.