Citrix® Application Streaming Guide

Citrix Presentation Server™ 4.5 for Windows®
## Contents

### Chapter 1  Overview of the Application Streaming Feature
- Benefits of the Application Streaming Feature ................................................. 8
- Components Overview .................................................................................. 10
  - The Citrix Streaming Profiler ................................................................. 12
  - The Citrix Streaming Client ................................................................. 12

### Chapter 2  Creating Resource Profiles
- Task Overview of Profiling an Application .................................................. 14
- Application Profiling Overview ................................................................. 14
  - Targets ..................................................................................................... 15
  - Operating System .................................................................................. 16
  - Service Pack Level ................................................................................ 17
  - System Drive Letter ............................................................................... 17
  - Operating System Language .................................................................. 17
  - Command Line Parameters .................................................................... 18
- Preparing a System to Profile Resources ...................................................... 19
- Installing and Starting the Profiler ............................................................... 20
- Setting Profiler Preferences ....................................................................... 21
  - Setting Default User Profile Security ..................................................... 22
  - Disabling and Enabling Profile Signing .................................................. 22
- Planning a Profile ....................................................................................... 23
- Creating a Profile and its Initial Target ....................................................... 23
  - Installing a Single Application through Quick Install ............................. 25
  - Installing Multiple Resources through Advanced Install ..................... 26
  - Completing Target Creation .................................................................. 28
- Viewing Profile and Target Information ..................................................... 31
Chapter 3 Managing Streamed Applications

Task Overview of Working with Streamed Applications ........................................... 61
Overview of Publishing Streamed Applications ....................................................... 62
Selecting the Delivery Method for Streamed Applications ...................................... 64
  Selecting the Application Type ............................................................................ 64
  Specifying a Policy for the Application Delivery Method .................................. 66
Streaming Applications to Presentation Server ....................................................... 68
Providing Offline Access to Applications Streamed to Desktop .............................. 70
  Creating the List of Users Who Have Offline Access Permission ....................... 71
  Selecting the License Setting for Offline Users .................................................. 74
  Enabling an Application for Offline Access ....................................................... 75
  The User’s Experience with Offline Access ....................................................... 75
Pre-deploying Applications to Clients ................................................................. 76
  Running the Pre-deployment Utility .................................................................. 76
Chapter 4

Managing Streaming Clients

Introduction to Streaming Clients. .................................................. 88
   About Program Neighborhood Agent. ........................................... 88
   About the Streaming Client. ...................................................... 89
System Requirements ................................................................. 90
Installing the Streaming Client. .................................................... 90
Configuring the Streaming Client. ............................................... 92
Installing Program Neighborhood Agent ........................................ 93
Configuring Your Installation Files .............................................. 94

Index ......................................................................................... 99
Overview of the Application Streaming Feature

This book describes how the application streaming feature of Citrix Presentation Server functions and how you can use it to augment application deployment not only to users’ desktops, but also to servers in your server farms.

This book is intended for system administrators and includes the following information:

• Architecture and component overview
• Managing Citrix streaming application profiles
• Publishing streamed applications
• Managing Citrix Streaming Clients

This chapter presents an introduction to the application streaming feature of Citrix Presentation Server and includes the following topics:

• Benefits of the Application Streaming Feature
• Component Overview

Understanding these topics provides you with a context for the remaining chapters of this book.
Benefits of the Application Streaming Feature

The application streaming feature simplifies application deployment to end users. With the application streaming feature, you can install and configure an application on one file server and deliver it to any desktop or server on demand. Upgrading or patching an application is simple, because you are required only to update or patch an application stored in one place: on the file server.

The application streaming feature offers the following benefits to enterprises:

- Cost effective, scalable application delivery to end users and servers
- Lower cost of installing and maintaining applications and servers in large farms
- Access any application, anywhere, anytime regardless of connection

There are additional benefits when streamed applications are run on client desktops:

- Optimal utilization of computing resources
- Elimination of application compatibility issues
- Elimination of peripherals-access issues

Your organization can profit from these benefits by taking advantage of the many streaming features included with this release of Presentation Server.

The application streaming feature offers the following:

**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 clients 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 manufacturer’s supplied update program. The update is performed once on the profiler workstation and delivered to clients in a manner similar to that used in the initial delivery.

**Application isolation.** Applications run within isolation environments that keep the applications from interfering with others running on the same client. The application’s specific data files, 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 to allow faster access the next time the application is launched. Before an application runs, cached files are automatically updated 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 Win32 execution platform can host a streamed application. Specifically, the streaming client operating systems are: Windows XP Professional and Windows 2000 Professional. With dual mode streaming, target environments are increased to include all supported Presentation Server clients.

**Dual mode streaming.** Configure Presentation Server to stream software to client desktops; otherwise, virtualize from Presentation Server. If launching a streamed application fails on the client device, Presentation Server seamlessly streams the application to the server, which then presents the application to the client device through an ICA connection.

**Easy deployment of applications to farm servers.** When publishing applications in a server farm, you can choose to stream applications to the server, which can simplify application deployment. Instead of installing applications on your farm servers, you stream them to the servers from a central file share. Update the application on the file share, and you update the application on all the farm servers.

**Consistent end-user experience.** Icons for applications that can be accessed through the server appear next to other application icons that the user is accustomed to either within the Web Interface, Program Neighborhood Agent, or on the desktop. The user does not have to know where and how the application is executing.

**Offline access.** Once 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 easily replaced.
Components Overview

The components related to a server farm that makes streamed applications available can be separated into the following categories:

- **Licensing** – For information about licensing, see *Getting Started with Citrix Licensing*.
- **Administration** – For information about administration, see *Citrix Presentation Server Administrator’s Guide*.
- “The Citrix Streaming Profiler” on page 12.
- “The Citrix Streaming Client” on page 12.

Each of these functional areas consists of software running on one or more workstations or servers. Each of these functional areas presents a unique set of tasks for the administrator.

The following diagram shows the components that make up each of these four functional areas and a general summary of the types of tasks administrators must perform.

1. **Licensing.** Consists of the license server and License Management Console. Use the License Management Console to manage licensing.
2. **Administration (server farm).** Consists of the following:
   - farm servers
   - IMA database
   - The Web Interface
   - Access Management Console. Use the Access Management Console to configure manage the server deployment and to publish streamed applications.
3. **Streaming Profiler.** Use the profiler to create streaming application profiles.
4. **Streaming Client and optional Program Neighborhood Agent.** Program Neighborhood Agent enumerates available applications for the user and the Streaming Client finds the correct application for the client workstation, sets up an isolation environment in which the application runs, and streams application files on demand.

If streaming to the client desktop fails, the streaming client running on the server can stream the application to the server for presentation on the client workstation. Alternatively, you can opt to stream applications to servers instead of desktops and have the servers present the applications to devices...
that have Presentation Server clients installed. This eases deployment of applications to servers in your farm.

This diagram shows the components related to a server farm that make up a deployment; licensing, server farm, Streaming Profiler, and Program Neighborhood Agent and Streaming Client.
The Citrix Streaming Profiler

You use the Citrix Streaming Profiler to profile applications that your users’ clients stream to their desktops. Using the profiler, you can create several targets within an application profile that can match a variety of your client workstations. In this way, you can create a single profile that can accommodate a variety of user environments. You can also use the profiler to update applications in the profile and provide other resources that you find your users need.

For more information about using the profiler and managing streaming application profiles, see Chapter 2, “Creating Resource Profiles.”

The Citrix Streaming Client

When a user runs an application enumerated by Program Neighborhood Agent or through a Web Interface site, the streaming client finds the correct applications in the profile on the file server, sets up the isolation environment on the client, and then streams the application from the file server to the safety of the isolation environment set up on the client.

To authenticate profiles accessed by the client, you can also install the clients with a digital certificate. The streaming client then streams applications only from profiles that match the digital certificate.

To provide offline access to streamed applications, the streaming client operates with Program Neighborhood Agent.

For more information about installing and configuring the streaming clients, see Chapter 4, “Managing Streaming Clients.”
This chapter describes how to use the Streaming Profiler to create resource profiles for use through Presentation Server and clients. After you install and configure the profiler and create and deploy application profiles, use Presentation Server to publish, administer, and monitor the use of profiles.

In addition to presenting task and general overviews of the Streaming Profiler and application profiles, this chapter presents the following topics:

- Preparing a System to Profile Resources
- Installing and Starting the Profiler
- Setting Profiling Preferences
- Planning a Profile
- Creating a Profile and its Initial Target
- Viewing Profile and Target Information
- Viewing and Editing Profile Properties
- Viewing and Editing Target Properties
- Adding a Target to a Profile
- Deleting a Target from an Application Profile
- Updating a Target
- Deleting an Obsolete Version of an Updated Target
- Isolation Environment Rules
- Profile Contents on the File Server
Task Overview of Profiling an Application

Some important tasks you perform when profiling an application are:

• Initializing a new profile and target
• Installing an application into a target
• Running an application in the profiler
• Selecting applications for listing in the profile
• Saving a profile to a file share

The next sections contain an overview of the profiler and instructions on how to use it to create and update profiles.

Application Profiling Overview

The profiler is an independent application that enables you to prepare commercial or custom Windows applications, Web applications, browser plug-ins, files, folders, and registry settings streamed to your users’ workstations.

Resources you prepare with the profiler are called *profiles*. You create a profile by installing applications or other resources on an independent computer running the profiler. The profiler bundles files and configuration settings that the client accesses to stream to end-user desktops, or laptops, or stream to end point.

After you create a profile, you make it available for publishing by saving it to a network file share.

A profile can contain a single application or suite of applications. For example, you can profile Microsoft Word by itself, or you can profile the entire Microsoft Office suite in a single profile.

Depending on the environment of clients, you can also profile prerequisites, such as Java Runtime Environment, with a 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.
Using the profiler, you configure applications to run in one or more target environments based on particular operating systems and language configurations, such as:

- Windows 2000 Professional Service Pack 4 - English
- Windows 2000 Professional Service Pack 4 - German
- Windows 2000 Professional Service Pack 4 - Japanese
- Windows 2000 Professional Service Pack 4 - Spanish
- Windows XP Professional Service Pack 4 - English

The range of target environments an application can be configured to run in depends, in part, on the type of application being profiled, the profiler operating system, and organizational needs.

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 operating system and language.

Applications that require packaging for a variety of environments can be contained within a single profile. Individual targets within a profile represent one or more end-user environments. After you publish the application on a server running Presentation Server, when a user runs a streamed application, the Streaming Client, which is running on the user’s workstation, automatically chooses the correct target that matches the workstation environment.

### Targets

A target is a collection of disk files, registry data, and other information used to represent an application isolation environment. 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 a number of other selection criteria.

The Streaming Client selects a target for execution based on the following criteria:

- Operating system version
- Service pack level
- System drive letter
- Operating system language
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 client systems, which simplifies profile creation.

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

The only requirement from the profiler regarding targets is that overlapping definitions are not permitted: only one target in a profile can be a correct match for any client system at application launch.

The profiler maintains multiple versions of each target in a profile. An administrator can update a profile and target at any time without affecting already active executions on client workstations. 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. However, you can 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.

**Operating System**

You can configure a target to be correct for any of the full set of supported client operating systems. The supported client operating systems are the following:

- Windows 2000 Professional, Service Packs 3 and 4
- Windows XP Professional, Service Packs 1 and 2
- Windows XP Professional 64-Bit Edition, Service Pack 1
- Windows 2003 Server, Service Pack 1
- Windows 2003 Server, R2
- Windows 2003 Server 64-bit Edition

By design, future operating systems are not supported, and the execution environment refuses to execute an application if the client system is on 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, you can 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 Citrix Streaming Client. Choose **Not required** or service packs that match those listed in previous section, “Operating System.”

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 can define a set of criteria that best associates a given target with a given client workstation.

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

Operating System Language

The following is a list of languages supported by the profiler:

- English
- French
- German
- Japanese
- Spanish
Using the English version of the profiler, you can also create targets for the following operating system languages:

- Korean
- Simplified Chinese
- Traditional Chinese

Additionally, you can create targets in all languages.

You can use the profiler to create targets in languages other than those listed here, but doing so is not fully supported. Citrix recommends that you use the English language version of the profiler when creating such targets.

**Command Line Parameters**

You can provide command line arguments for running a streamed application by modifying its properties in the profile’s target. You can also use placeholders in the profile, which will be replaced by command line arguments that are specified in the published applications. You modify an application’s properties after you install it during the target creation process (in the New Profile or Add New Target wizards) or by editing application properties after you’ve created the target.

**Note** 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**

The ** placeholder was added to the Command line parameters (optional) text box in the profiler. The placeholder is replaced with the published application’s command line arguments.

1. Specify the following arguments and placeholder in the profiled application.
   
   `app.exe /a ** /b`

2. Publish the application with the following arguments. (%* specifies the content redirection arguments.) For information about publishing streamed applications, see “Overview of Publishing Streamed Applications” on page 62.
   
   `/x %* /y`
3. Launch the application with content redirection, on a file named my.doc.
   The steps are:
   A. The profiled application command line is used.
      \texttt{app.exe /a ** /b}
   B. The ** placeholder is replaced with the published application arguments.
      \texttt{app.exe /a /x %* /y /b}
   C. The file for content redirection replaces the %*, producing the final command line.
      \texttt{app.exe /a /x my.doc /y /b}

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.

\textbf{Preparing a System to Profile Resources}

Configure the profiler workstation to provide a run-time environment that is as close to your end-user run-time environment as possible. Other than standard operating system software and utilities, do not run other software applications on the profiler workstation.

The server or workstation on which you install the profiler must be one of the following:
\begin{itemize}
  \item Windows 2000 Professional, Service Packs 3 and 4
  \item Windows XP Professional, Service Packs 1 and 2
  \item Windows XP Professional 64-Bit Edition, Service Pack 1
  \item Windows 2003 Server, Service Pack 1
  \item Windows 2003 Server, R2
  \item Windows 2003 Server 64-bit Edition
\end{itemize}

In addition, Microsoft XML 2.0 must be installed. It is recommended that you use Windows Update to ensure you have installed all the recent Internet Explorer updates.
The optimal configuration for profiling and executing applications varies based on the application. In many cases, you can use a single target for executing an application on all possible execution operating systems. In other cases, specific profiling and execution are needed per operating system. Experimentation provides the outcome for specific applications.

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 2000 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 for 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.

In addition to matching the oldest operating system your users are running:

- Computers that create targets for your profiles must match primary drive letters. For example, if your users have computers whose main drives are E, to create targets for them, use a packaging computer that also has a main drive of E.

- When creating language-specific targets for clients running English, French, German, or Japanese operating systems, for best practice, the computer creating the target should match the operating system language. For example, use an English language operating system when creating a target that contains an English language application, and use a German language operating system when creating a target for a German version of the application.

- When creating targets for clients running Korean, Simplified Chinese, or Traditional Chinese, use a profiler running on an English language operating system.

The next section describes how to install the profiler on a workstation.

## Installing and Starting the Profiler

After you identify the correct workstation to use for creating profiles and targets, and ensure it is clean of other software applications, install the profiler on it.

**To install the profiler**

1. Insert the Presentation Server Components CD into the workstation you want to use to profile resources.

2. To install the profiler, in the autorun window, choose *Presentation Server Utilities*, then *Install Citrix Streaming Profiler for Windows*. 
3. Choose a language for the installer interface.

4. After installation, restart the workstation.

To simplify the creation or modification of profiles, you can set packaging preferences after installing the profiler.

To start the profiler, from the Start menu, choose Programs > Citrix > Streaming Profiler > 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 these four main components:

- **Menu and toolbar**. Located at the top. The toolbar contains buttons that initiate the following actions:
  - Start the New Profile wizard to create a profile
  - Open an existing profile on a file share
  - Save the current profiler to a file share

- **Profile tree**. Located middle left. When populated, lists a profile and its targets.

- **Profile and target information**. Located middle right.

- **Status bar**. Located across the bottom.

For more information about viewing profile and target information, see “Viewing Profile and Target Information” on page 31.

### Setting Profiler Preferences

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

Preferences save time and improve usability by enabling you to store relevant settings for use in future packaging tasks.

- You can save default security settings you want for all profiles you create. This relieves you of specifying whether you want enhanced or relaxed security.

- If you are not signing profiles, you can specify not to show the Sign Profile page in the wizards.
To set these default preferences, from the **Edit** menu of the profiler window, choose **Preferences**.

**Setting Default User Profile Security**

Use the **User Profile Security** tab of **Preferences** to set the default for how restrictive you want client isolation environments to be. You can also use the **User Profile Security** tab to prevent the User Profile Security pages from appearing in the New Profile and Target wizards.

**To prevent the User Profile Security pages from appearing in the profiler’s wizards**

1. On the **User Profile Security** tab, check **Use these settings**.
2. Choose the security setting you want to use as your default.
   
   Use the option buttons to select between the following:
   
   - **Enhanced security**. Does not permit any executable files to run other than those included in the target. For example, if the client is running an Internet Explorer plug-in included in the target, the enhanced security setting prevents the client from running any other plug-ins that the user might download.
   
   - **Relaxed security**. Permits executable files to run that are accessed through the profiled resource.

To remove default settings and restore the User Profile Security pages to the profiler wizards, clear the **Use these settings** check box.

**Disabling and Enabling Profile Signing**

If you are not signing profiles, use the **Digital Signature** tab of **Preferences** to prevent the digital signature pages from appearing in the New Profile and Target wizards.

If you later decide to sign profiles, use the **Digital Signature** tab of **Preferences** to restore the digital signature pages to the wizards.
Planning a Profile

Using the profiler, you can create a resource profile that consists of targets that offer any of the following:

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

Packaging a standard application in a target is called a *quick install*. Packaging multiple applications and other resources in a target is called an *advanced install*.

With both quick and advanced installs, you specify criteria the Streaming Client matches. The target criteria are the following:

- Operating system and, optionally, service pack
- System drive letter
- Language

In addition to target criteria, for the entire profile, choose whether to

- Digitally sign the profile
- Have strict or relaxed security settings

The remaining sections in this chapter describe how to use the profiler to create a profile and targets that use a variety of these profiler options.

Creating a Profile and its Initial Target

This section describes how to create a profile, set some properties for the entire profile, and begin creating the initial target.

When you create a profile, set the following profile properties:

- Profile name
- User profile security settings

After setting profile properties, begin creating the first target. When you initialize the target, choose the following client-matching criteria for it:

- Operating system and service pack
- Language
After you initialize a profile and target, install resources in the target through either advanced or simple installation procedures. The sections following this procedure describe how to perform advanced and simple installations of resources in targets.

**To initialize a new profile and target**

1. To start the New Profile wizard, 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 the client uses to identify targets. For example, do not include a version number in the profile name.

3. Set the user profile security.

   Select the level of user profile security you want for the profile. Use the option buttons to select between the following:

   - **Enhanced security**. Does not permit any executable files to run other than those profiled in the target. For example, if the client is running a profiled Internet Explorer plug-in, the enhanced security setting prevents the plug-in from running any applications other than those installed in the target. Examples are plug-ins or DLLs that are not included in the target.

   - **Relaxed security**. Permits executable files accessed through the profiled resource to run.

4. Set at least one target operating system and language.

   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 packaging workstation.

   A. 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.

   B. If you want the client to consider the service pack level, click **Set Service Pack**. By default a target matches all service packs of the operating systems it supports.

   C. 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.
D. 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, you can ensure the current target you are adding does not conflict with other targets in the profile by clicking Check for Conflicts.

5. Choose an installation option.

You choose an installation option according to the type of resource or number of resources you want to install in a target.

- **Quick Install**. if the application you are installing has an installation program, such as setup.exe (recommended for normal installations).

- **Advanced Install**. if you are installing Internet Explorer plug-ins, editing registry settings, installing an application manually, or installing from multiple installers.

Advanced install provides the opportunity to repeat the installation procedure as many times as you need, so you can add a variety of multiple resources to a target.

The next section describes how to continue profile creation with a quick install of an application in a target.

For instructions about continuing profile creation with an advanced install, see “Installing Multiple Resources through Advanced Install” on page 26.

**Installing a Single Application through Quick Install**

This section describes how to install an application in a target after selecting Quick Install as the installation type. You install an application in a target as part of the New Profile and New Target wizards.

**To install an application in a target**

1. Choose an installer. 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 only choosing the installer, not running it. If needed, enter required command-line arguments, then click **Next**.

2. Run the installer. In Run Installer, ensure the installation program and command-line parameters are correct, then click **Launch Installer**.
After you launch the installer, the Back button is disabled. Do not click Next until the installer finishes.

After the application installer finishes, if the application you are installing requires restarting, the profiler detects it and performs a virtual restart.

If, after you are sure the application installer is finished, you want to force a virtual restart, before clicking Next, check Perform virtual restart. When you click Next, instead of restarting your packaging workstation, the profiler simulates a system restart.

After running the installer, perform the tasks that complete the creation of the profile and target. For instructions about finishing target creation, see “Completing Target Creation” on page 28.

Installing Multiple Resources through Advanced Install

This section describes how to install multiple resources in a target after selecting Advanced Install as the installation type. You can perform an advanced install when creating a profile or adding a target.

To install multiple resources in 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. For instructions, see “Installing a Single Application through Quick Install” on page 25.
   - To install Internet Explorer and plug-ins, choose Install IE plugins. For more information, see “Installing Internet Explorer Plug-Ins” on page 27.
   - To add files and folders that might be needed on the client workstation, or to remove unneeded files and folders, choose Select files and folders.
   - You might need to include required files that are on the packaging workstation, but might not be on the client workstation. For more information, see “Including Files and Folders” on page 27.
   - To customize the registry as viewed by the client workstation, choose Edit registry. For more information, see “Including Registry Settings” on page 28.

Each of these options provides you with the opportunity to return to this screen and install additional resources.
2. After installing all the resources you want to include, choose **Continue with none of the above**, which enables you to finish creating the target.

For instructions about finishing target creation, see “Completing Target Creation” on page 28.

**Installing Internet Explorer Plug-Ins**

This section provides some details about installing Internet Explorer and its plug-ins into a target. You can install Internet Explorer and plug-ins by choosing the Advanced Install option while running the New Profile or New Target wizards.

**To install Internet Explorer and its plug-ins**

1. If you have Internet Explorer running, close it.
2. From the **Select Install Method** window of the wizard, choose **Install IE plugins**.
3. Click **Launch Microsoft Internet Explorer**. This command runs Internet Explorer in an isolation environment.
4. Using Internet Explorer, install all the plug-ins to be made available to your users.

After installing the plug-ins, continue with “Completing Target Creation” on page 28.

**Including Files and Folders**

This section provides some details about including files and folders in a target. You may need to include specific files and folders that are not installed by an application installer but are required for the application to run.

You can include files and folders in a target by choosing the Advanced Install option while running the New Profile or New Target wizards.

**To include files and folders in a target**

1. From the Select Install Method window of the wizard, choose **Select files and folders**.
2. Select the files and folders you want to include.
   
   A. To select files and folders for inclusion in the target, use the **Look in** pull-down menu to choose a folder.
   
   B. In the **Selected files** list, select the files you want to include in the target and click the arrow between the **Select files and Current files** lists.
C. To create new folders, rename files and folders, or delete files and folders in the **Current files** list, use the buttons at the bottom of the **Current files** list.

D. After you include all the files and folders the application requires, you can simulate a system restart by checking **Perform virtual restart**.

After including files and folders in the target, see “Completing Target Creation” on page 28.

**Including Registry Settings**

This section provides some details about including customized registry settings in the isolation environment of a target. You provide customized registry settings in a target by choosing the Advanced Install option while running the New Profile or New Target wizards.

---

**Caution**

Using Registry Editor 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.

---

**To include customized registry settings**

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

2. From the Select Install Method window of the wizard, choose **Edit registry**.

3. Click **Launch Windows Registry Editor**.

4. Use Windows 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 packaging workstation.

5. After saving the registry settings, you can simulate a system restart in the target by checking **Perform virtual restart**.

After saving the registry settings, finish the installation by seeing the next section “Completing Target Creation,” or install additional resources.

**Completing Target Creation**

This section describes how to finish target and profile creation and save the profile to a network file share.
After you install all the necessary resources in a target, you perform the following:

- Run the application to enter a license code or accept a license agreement.
- Select applications to make them available for you to publish.
- Sign the profile with a digital signature.
- Review profile details and, if necessary, edit the profile.
- Save the profile to a file share.

The sections that follow describe in more detail how to complete each of these tasks.

**Running an Application in the Profiler**

If on the initial running of the application you are installing, it requests a license key or acceptance of a license agreement, from the New Profile, Add Target, and Update Application wizards, you can perform these tasks for your users by adding the application to the Applications list and running the application.

- 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.

Before clicking Next, perform necessary initialization operations for the application.

In the New Profile, Add Target, and Update Applications wizards, after running applications, you select the ones you want to make available for publishing by listing them in the profile.

**Selecting Applications for Listing in the Profile**

You use the Add Applications pane of the New Profile, New Target, and Update Application wizards to list applications in the target and make them available for publishing. After listing applications, it is important to use the Add Applications pane to ensure applications are available in all targets.

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 you must modify the application name. If the names of applications in multiple targets match, those applications are considered available in those targets.
Availability indicates whether or not the discovered applications are in other targets and whether or not the applications in other targets are in the current target. If a discovered application is similar to unavailable applications in other targets, you can modify the name of the discovered application so that it matches the applications in the other targets.

You list applications in the profile by adding, deleting, modifying, and recovering them in the Select Applications pane.

If the Applications list is not populated, click Recover. Recover finds newly installed applications and populates the Applications list.

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 only removes the applications 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. After you click Modify, you can change the following properties:

- Name
- Version number
- Location of the executable
- Current working directory

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 you remove the version number or change the name so the application is recognized as existing in other targets. When the profiler recognizes the application as existing in all targets, it changes the application availability to Available.

After listing the applications in a profile, you have the opportunity to sign it with a digital signature.

Signing a Profile

If you installed and configured your code-signing certificates, you can sign profiles through the New Profile, New Target, and Update Target wizards.

To sign a profile, you must know the password for the certificate you are using to sign.
In the Sign Profile pane:

- To sign the profile using a certificate residing on 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 packaging workstation, choose **Sign using locally installed certificate**.

You can also sign a profile at any time by opening the profile and from the **Tools** menu choosing **Sign Profile**.

After signing a profile, you have the opportunity to review profile information.

### Reviewing and Editing Profile Information

Before saving a profile from the New Profile, New Target, or Update Target wizards, you have the opportunity to review profile information and edit profile and target settings.

In the Build Profile window, review the settings of your newly created target. If you need to make changes use the **Back** button.

### Saving a Profile to a File Share

When saving a profile to a file share, for **UNC Path**, type the path to the network file share where you want to store the profile. Note that **Save To** displays the location where you are saving the profile based on what you provide for the UNC path and the name you provide for the profile. Here is an example of what might be entered for the UNC path:

```plaintext
\citrixserver\profiles
```

Here is the actual storage location based on the values of **UNC Path** and **Profile Name**:

```plaintext
\citrixserver\profiles\Profile Name\Profile Name.profile
```

You can also at this point change the name of the profile.

After you save your profile to a file share, you can use other workstations to add unique targets to the profile.

### Viewing Profile and Target Information

You can view profile and target information by using the profiler to open the profile.

**To open a profile and view information about it**

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. (Alternatively, click **Open Profile** on the Welcome screen.) Here is an example:

```
\hostname\fileshare\Profile Name\Profile Name.profile
```

When you open a profile, the profiler displays profile information in the right pane. The right pane displays the following tabs:

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

4. To view information about a target, select it in the left pane of the profiler. The right pane displays the following tabbed information about the target:

- Information
- Applications
- File Types

For more descriptions of information displayed in the profiler, see the profiler online help.

**Viewing and Editing Profile Properties**

After creating a profile, you can view and edit some of its properties. Profile properties consist of the following:

- General properties, which are the name, description, location, size, and creation and modification dates of a profile
- Application properties, which are the settings of all applications from all targets and their availability
- File types, which are the file type associations used in publishing to invoke the profile
- User profile security, specifying whether or not files can be run from the user’s profile directory
• Pre-launch analysis, which, before streaming the applications in the target, ensures the existence of required applications on the client computer and required registry entries in the client’s registry

• Pre-launch/post-exit scripts, which indicates scripts to run prior to and following the execution of applications in the target

You can view profile and target information by using the profiler to open the profile.

To open a profile and view its properties

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. Here is an example:
\hostname\fileshare\Profile Name\Profile Name.profile

4. After the profiler opens the profile, from the Edit menu, choose Profile Properties.

The sections that follow describe the information in the Profile Properties dialog box and, if available, how you can modify these properties.

Editing Profile Name, Description, or Location

The General tab of the Profile Properties dialog box contains the following information about a profile:

• Name. Manifest name and location 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 UNC path; for example:
\hostname\FileShare\Profile Name\Profile Name.profile

• Description. Modify the description of the profile by typing a description in the Description field of the General tab.

• Location. Modify the location of the profile by moving it on the file share.

• Created. Set automatically by the profiler.

• Last Updated. Set automatically by the profiler.

Profile size is also set automatically by the profiler.
Viewing Details about Applications in a Profile

The Applications tab of the Profile Properties dialog box lists all applications installed in the targets of a profile and indicates whether or not each application is available in all targets. When an application is available, you can use the Access Management Console to publish it on computers running Presentation Server.

To view more information about an application included in the target, select the application in the Applications tab 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
- Command-line parameters that are passed to the application when it is started

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.

You can also click Find Application if the application is missing from the target.

You can modify the remainder of the properties by updating the target in which the application is installed. For more information about updating a target, see “Updating a Target” on page 47.

Viewing File Type Associations Set in a Profile

The File Type tab displays information about the types of files. They are used during application publishing so that opening a file of a certain type on the client invokes this streamed application. The File Types tab displays the following information about the file types:

- Extension
- Description of the file type
- Application invoked by the file
- Whether the application is currently available to users

You can modify these properties by updating the target in which the application is installed. For more information on updating a target, see “Updating a Target” on page 47.
Adjusting User Profile Security Settings

The User Profile Security tab displays whether or not the application can invoke executable files it writes to its current working directory on the client.

To disable an application from running executable files it writes to its current working directory on the client, choose Enhanced Security. Selecting enhanced security might restrict or prevent the operation of some applications.

To allow an application to run executable files it writes to its current working directory on the client, choose Relaxed Security. Choosing relaxed security can enable the client to download and run potentially malicious software.

Checking for Profile Prerequisites

To check for resource prerequisites on a client workstation before starting an application in a profile, use the Pre-launch Analysis tab of Profile Properties. Use the Pre-launch Analysis tab to choose resources that are prerequisite for running applications in a profile.

When packaging an application, the administrator ensures all prerequisites are met. Because not all client workstations have the required resources installed, you can use the Pre-launch Analysis tab to inspect the client workstation for prerequisites before streaming the profiled application.

If pre-launch analysis determines a client workstation does not have the prerequisites for the profiled application to run correctly, profile execution stops and alerts the user of the problem.

Determine if you require pre-launch analysis by testing profiles you create.

You can establish pre-launch analysis for the entire profile and for individual targets. The types of resources for which pre-launch analysis can look are:

- Applications and versions (specific or a range)
- Binary files and versions (specific or a range)
- Registry entries

To establish pre-launch analysis

1. On the Pre-launch Analysis tab of Profile Properties, check Enable pre-launch analysis.
2. Click Add Item under the section appropriate to what you want to add: Applications and Files or Registry Entries.

The sections that follow describe how to perform each of the operations of adding applications and files and adding registry entries.
Checking 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:

- Choose the application you want to identify as a prerequisite. (Note that the list of applications is static.)
- Browse to and choose the binary file you want to identify as a prerequisite.
- Select whether or not you want to check for a specific version or range.


Checking 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:

- From the Registry Type drop-down list, choose one of the following:
  - 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.

- From the Hive drop-down list, choose the registry hive in which the registry entry resides. Your choice of hives is:
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
  - HKEY_CURRENT_CONFIG
• Type the name of the key. The following is an example:
  Environment

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

• To select the matching registry type for the prerequisite you are choosing, use the **Type** pull-down menu. Your choice of registry types is:
  • String Value (REG_SZ)
  • Binary Value (REG_BINARY)
  • DWORD Value (REG_DWORD)
  • Multi-String Value (REG_MULTI_SZ)
  • Expandable String Value (REG_EXPAND_SZ)

When you select a type, the Value Data updates to reflect the select type.

**Invoking Pre-Launch and Post-Exit Scripts for a Profile**

After testing a profile, if you determine that certain operations are required before or after the running of the profile applications, you can use the **Pre-launch & Post-exit Scripts** tab of Profile Properties to invoke scripts you wrote. Use the **Pre-launch & Post-exit Scripts** tab to add and delete scripts and to control the order in which the Streaming Client runs them.

By default, scripts you define at the profile level apply to all targets in the profile. If you want to invoke scripts only for a selected target within a profile, see “Invoking Pre-Launch and Post-Exit Scripts for a Target” on page 41.

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.

For example, if you must copy dynamic files each time a user launches a certain application, you can create a VB Script or batch file that copies those files or runs a utility each time the application starts and exits.

**To add default pre-launch or post-exit scripts for the current profile**

1. From the **Pre-launch and Post-exit Scripts** tab of **Profile Properties**, click **Add**.

2. Choose the type of script you want to add by clicking one of the option buttons **Use pre-launch script** or **Use post-exit script**.
3. 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**.

4. To select the script you want to use, click **Browse**.

5. Specify any command-line parameters required by the script.

After you add pre-launch and post-exit scripts, use the **Pre-launch and Post-exit Scripts** tab to delete or change the order in which the client runs the scripts. The client runs scripts in the order they are listed.

After you click **OK** and save the profile to the file share, all new invocations of applications in the targets invoke the pre-launch or post-exit scripts in the way you specified.

### Viewing and Editing Target Properties

If your users experience problems running applications in a profile, you can solve some of those problems by editing target properties.

Target properties consist of the following:

- **General properties.** Contains name, description, and creation and modification dates of the current target.

- **Application properties.** 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.

- **Operating system and language.** Specifies which clients can run applications installed in the target.

- **Pre-launch analysis.** Ensures the existence of required applications on the client desktop and required registry entries in the client isolation environment, before streaming the applications in the target.

- **Pre-launch/post-exit scripts.** Specifies the scripts to run prior to and following the execution of applications in the target.

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

You can view profile and target information by using the profiler to open the profile.

### To open a target and view its properties

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. Here is an example:
   \hostname\fileshare\Profile Name\Profile Name.profile

   After the profiler opens the profile, in the left pane, choose the target whose properties you want to view or edit.

4. From the Edit menu, choose Target Properties.

   In Target Properties, the tabs for Pre-launch & Post-exit Scripts and Pre-launch Analysis are identical to those in Profile Properties.

   For instructions about how to use the Pre-launch & Post-exit Scripts tab, see “Invoking Pre-Launch and Post-Exit Scripts for a Profile” on page 37.

   For instructions about how to use the Pre-launch Analysis tab, see “Checking for Profile Prerequisites” on page 35.

   For instructions about how to modify the remaining target properties, see the sections that follow.

## Modifying 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. You can modify or add a description. You can also view the creation and modification time stamps of a target. These are set by the profiler at the time you save a target.

## Modifying Application Properties

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

The Application tab 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.

- **Application version number.** Manually set from the profiler by the administrator who installed the application into the profile.

- **Path.** Set by default by the application installer but can be changed by the administrator during the installation. This 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.

You can modify the list of applications by doing the following:

- **Recovering or adding applications to the list:**
  If you suspect the list of applications is not complete, you can have the profiler recover all applications installed in the target by clicking **Recover**.
  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.

- **Deleting 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. You can add a deleted application to the list by clicking **Recover** or **Add**.

- **Modifying an entry in the list:**
  You might want to modify an application in the list if the application name is different from other similar applications in other targets or contains a version number.

  To modify the application, select its entry in the list and click **Modify**.

### Modifying Target Operating System and Language Properties

To expand or restrict the different clients that can run applications in a target, use the **Target OS and Language** tab of **Target Properties** to modify these properties.

**To modify the operating system and language properties of a target**

1. Under Target Operating Systems, check the operating systems you want clients to match to access the current target.
2. To modify the service packs required for a match, click **Set Service Packs** and then specify the service pack criteria.

3. Under Target Language, check the languages you want clients to match to access the current target.

The updated settings apply to targets when you save the changes.

**Establishing Pre-Launch Analysis for a Target**

If after testing a profile you determine that a target requires pre-launch analysis or analysis that is different from the default for the profile, you can use the Pre-launch Analysis tab of Target Properties to establish pre-launch analysis for the current target. For further information, see “Checking for Profile Prerequisites” on page 35.

**Invoking Pre-Launch and Post-Exit Scripts for a Target**

By default, you define scripts for a profile and all its targets. You can use the **Pre-launch & Post-exit Scripts** tab of Target Properties to override the default profile-level scripts and use different scripts you design specifically for a particular target.

**To specify scripts other than the default for the current profile**

1. Clear the **Use profile scripts** check box.
2. Specify the scripts you want to use.
3. To use pre-launch or post-exit script, check the **Use pre-launch script** or **Use post-exit script** check box, and click **Browse** to select the scripts you want to use. You can also specify command-line parameters for the scripts.

For more information about pre-launch and post-exit scripts, see “Invoking Pre-Launch and Post-Exit Scripts for a Profile” on page 37.

**Managing Isolation Environment Rules for a Target**

Use the **Rules** tab of Target Properties to modify the isolation environment rules. The list of rules on the **Rules** tab 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, you can 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 packaging workstation (ignore rule)
- If you must isolate a subdirectory of an ignored directory on the client (ignore and isolate rules)
- If you must support multiple versions of an application running on the client (strictly isolate rule)

For information about isolation environment rules, see “Isolation Environment Rules” on page 49.

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. For descriptions of each of these operations, see the sections that follow.

**Adding a Rule**

To add a rule to the currently defined set of rules, from the Rules tab of Target Properties, click Add. Use the New Rule wizard to define the new rule.

**To use the New Rule wizard to create a rule:**

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

### Copying a Rule

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. You can further modify the name, action, or object of the rule.

### Modifying 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. When you modify a rule, you can modify the action and objects, but not the object type.
To use the Modify Rule wizard to modify a rule

1. Select the action and then click Next.

2. On the Select Objects page, you can 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, you can modify the name of the rule.

Deleting a Rule

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

Adding a Target to a Profile

Add a target to a profile to make applications available to clients that match additional and unique combinations of target criteria. An example is adding separate targets for English, French, German, and Japanese language-based operating systems.

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 conflicts with any other target in the profile.

To ensure the target you are adding does not conflict with other targets in the profile, the New Profile and New Target wizards offer a Check for Target Conflicts option.
To open a profile and add a target to it

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. Here is an example:
   \hostname\fileshare\Profile Name\Profile Name.profile

4. After the profiler opens the profile, from the profiler Edit menu, choose Add New Target.

5. Set target operating system and language.
   Setting the target and 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 packaging workstation.

   To support other operating systems and languages, select the check boxes associated with the those you want to support.

   When selecting target operating systems and languages, to prevent target conflicts, do not select those languages for which you are going to create other targets. You must select at least one operating system and at least one language.

   By default, service pack levels are not considered when matching a target to a client. If you want the client to consider the service pack level, click Set Service Pack.

   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. Then, 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.

   To ensure the target you are adding does not conflict with other targets in the profile, check Check for Conflicts.

6. Choose an installation option.

   Choose an installation option according to the type of resource or number of resources you want to install in a target.

   • If you want to add a single application to a target without adding any additional files, folders, or registry entries, choose Quick Install.
Quick install does not offer you the opportunity to repeat the installation procedure.

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

  Advanced install provides the opportunity to repeat the installation procedure as many times as you need, so you can add a variety of multiple resources to a target.

For instructions about how to continue profile creation with quick install of an application, see “Installing a Single Application through Quick Install” on page 25.

For instructions about continuing profile creation with an advanced install, see “Installing Multiple Resources through Advanced Install” on page 26.

Deleting a Target from an Application Profile

The profiler provides a facility to help you delete a target from a profile.

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. Here is an example:
   \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, note the location.
6. From the Edit menu, choose Delete Target.

When you save the profile, the profiler deletes the associated target cabinet (CAB) files from the profile on the file share and removes associated entries from the profile manifest.
Updating a Target

If you want to upgrade an application within a target, or add resources to a target, you update it. You can 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, clients 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.

For instructions about how to remove an obsolete version of a target from an updated profile, see “Deleting an Obsolete Version of an Updated Target” on page 48.

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

To update a target

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. Here is an example:
   \hostname\fileshare\Profile Name\Profile Name.profile
4. In the left pane of the profiler, select the target whose application you want to update.
5. From the Edit menu, choose Update/Install Application.
6. Choose an installation option.
   Choose an installation option according to the type of resource or number of resources 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.
Quick install does not offer you the opportunity to repeat the installation procedure.

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

Advanced install provides the opportunity to repeat the installation procedure as many times as needed, so you can add a variety of multiple resources to a target.

For instructions about how to continue profile creation with quick install of an application, see “Installing a Single Application through Quick Install” on page 25.

For instructions about continuing profile creation with an advanced install, see “Installing Multiple Resources through Advanced Install” on page 26.

### Deleting an Obsolete Version of an Updated Target

To recover disk space on the file share that hosts your streaming application profile, you can 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.

**To remove an old version of an updated target**

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. Here is an example:
   \hostname\fileshare\Profile Name\Profile Name.profile
4. In the left pane of the profiler, select the target whose application you updated.
5. In the right pane, on the **Information** tab, note the path to your updated CAB file.
   The trailing integers of the CAB file name represent the target version number. For example, the version of the following file is “2”:
   \hostname\fileshare\Profile Name\720edd68-0972-49e6-aa00-80974eb81d5b_2.cab
   To choose CAB files that are obsolete, identify the ones that have trailing integers of the least value.
6. Use Windows Explorer to delete the obsolete CAB file from the profile on your file share.

For instructions about how to delete a target whose version is listed in the profiler, see “Deleting a Target from an Application Profile” on page 46.

Isolation Environment Rules

The Streaming Client uses isolation environments to control application compatibility and accessibility. The client 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, you can alter the default set of rules, as needed, to exert control over application interactions with client operating system resources.

Types of Isolation Environment Rules

The following sections describe the general types of rules you can create and best practice information for such rules.

Isolation Rules

When you 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 default behavior relieves most application conflicts and allows applications to run correctly.

Isolation rules ensure that per-user and per-application level versions of files and keys are created. This is the primary method used to isolate applications from each other.

- Isolation per user. Creates an individual copy of each resource that a particular user accesses.

- Isolation per isolation environment. Creates a single copy of a resource for a particular isolation environment.

You can add one of these rules to ensure that there is one copy of a resource per isolation environment. For example, you can 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, you can create a rule that isolates this particular registry hive for the isolation environment.
Ignore Rules

You can use the rules engine to define “holes” in the isolation environment so that an application can write to the underlying system. Such rules are called Ignore rules.

There are instances when an application inside an isolation environment needs to share data with an application outside the isolation environment. For example, in a scenario where users can print to network printers available within an ICA session, these printers are automatically created when the user connects to a published application. If the published application is running within an isolation environment, called *My_AIE*, which has an isolation rule applied to it, auto-creation of network printers fails because a copy of the registry hive HKEY_CURRENT_USER\Printers is created for each user. You can ensure printer auto-creation occurs by creating a rule for *My_AIE* that ignores the registry hive HKEY_CURRENT_USER\Printers.

Redirect Rules

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, you can redirect those files to c:\aietemp\%USERNAME%, regardless of the user.

For example, if UserA runs the application in an isolation environment, c:\temp\data.txt is created in c:\aietemp\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:\aietemp on a per-user basis, the administrator can clean up the temporary data easily at startup.

Prioritization of Rules

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.

For instance, if you create 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 isolation rule for C:\Documents and Settings\%USERNAME%\Windows because you want to isolate 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. For a list of the default rules applicable to isolation environments, see “Default Rules for Isolation Environments” on page 55.

- **You can 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.** You can create a rule to alter the behavior of individual files or of 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\fil`, the rule applies only to a file or directory called `c:\temp\fil`. The rule does not apply to any files or directories that have `c:\temp\fil` 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 as explained previously).

### 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 Presentation Server.

You can also use environment variables to 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_FINSTALLROOT`. 
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. For a list of the default rules that apply to an isolation environment, see “Default Rules for Isolation Environments” on page 55.

**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.

The environment variables available for isolation environments are as follows:

<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIE_COMMON APPLICATION DATA</td>
<td>Common application data location</td>
<td>C:\Documents and Settings\All Users\Application Data</td>
</tr>
<tr>
<td>AIE_COMMON DESKTOP</td>
<td>Common desktop location</td>
<td>C:\Documents and Settings\All Users\Desktop</td>
</tr>
<tr>
<td>AIE_COMMON STARTMENU</td>
<td>Common Start menu location</td>
<td>C:\Documents and Settings\All Users\Start Menu</td>
</tr>
<tr>
<td>AIE_FSINSTALL ROOT</td>
<td>File system install root</td>
<td>C:\Program Files\Citrix\RadeCache\MyAIE</td>
</tr>
<tr>
<td>AIE_FSUSERROOT</td>
<td>File system user root</td>
<td>C:\Documents and Settings\Administrator\Application Data\Citrix\RadeCache\MyAIE</td>
</tr>
<tr>
<td>AIE_METAFRAME</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_REGINSTALL ROOT</td>
<td>Registry install root</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\RadeCache\MyAIE</td>
</tr>
<tr>
<td>AIE_REGUSER ROOT</td>
<td>Registry user root</td>
<td>HKEY_CURRENT_USER\SOFTWARE\Citrix\RadeCache\MyAIE</td>
</tr>
<tr>
<td>AIE_USER APPLICATION DATA</td>
<td>User’s global application data location</td>
<td>C:\Documents and Settings\Administrator\Application Data</td>
</tr>
<tr>
<td>Environment Variable</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AIE_USERLOCAL DATA</td>
<td>User’s local application data location (including temporary files)</td>
<td>C:\Documents and Settings\Administrator\Local Settings\Application Data</td>
</tr>
<tr>
<td>AIE_USERDESKTOP TOP</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_USERSTART MENU</td>
<td>User Start menu location</td>
<td>C:\Documents and Settings\Administrator\Start Menu</td>
</tr>
</tbody>
</table>
## Default Rules for Isolation Environments

<table>
<thead>
<tr>
<th>File System Rules</th>
<th>Ignore %AIE_METAFRAME%\Installer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ignore %SystemRoot%\explorer.exe</td>
</tr>
<tr>
<td></td>
<td>Ignore %SystemRoot%\system32\mydocs.dll</td>
</tr>
<tr>
<td></td>
<td>Ignore %SystemRoot%\system32\shell32.dll</td>
</tr>
<tr>
<td></td>
<td>Ignore %SystemRoot%\system32\shell\PRINTERS</td>
</tr>
<tr>
<td></td>
<td>Ignore %USERPROFILE%</td>
</tr>
<tr>
<td></td>
<td>Ignore A:\</td>
</tr>
<tr>
<td></td>
<td>Ignore B:\</td>
</tr>
<tr>
<td></td>
<td>Isolate</td>
</tr>
<tr>
<td></td>
<td>%AIE_USERAPPLICATIONDATA%\Microsoft\Internet Explorer\Quick Launch</td>
</tr>
<tr>
<td></td>
<td>Isolate %AIE_USERDESKTOP%</td>
</tr>
<tr>
<td></td>
<td>Isolate %AIE_USERSTARTMENU%</td>
</tr>
<tr>
<td>Registry Rules</td>
<td>Ignore HKEY_CURRENT_USER\Control Panel\Desktop</td>
</tr>
<tr>
<td></td>
<td>Ignore HKEY_CURRENT_USER\Control Panel\Mouse</td>
</tr>
<tr>
<td></td>
<td>Ignore HKEY_CURRENT_USER\Printers</td>
</tr>
<tr>
<td></td>
<td>Ignore HKEY_CURRENT_USER\SOFTWARE \Microsoft\Windows NT\CurrentVersion</td>
</tr>
<tr>
<td></td>
<td>Ignore HKEY_CURRENT_USER\SOFTWARE \Microsoft\Windows\CurrentVersion\Explorer\Shell Folders</td>
</tr>
<tr>
<td></td>
<td>Ignore HKEY_CURRENT_USER\SOFTWARE \Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders</td>
</tr>
<tr>
<td></td>
<td>Ignore HKEY_LOCAL_MACHINE\SOFTWARE \Citrix\AppCloning</td>
</tr>
<tr>
<td></td>
<td>Ignore HKEY_LOCAL_MACHINE\SOFTWARE \Citrix\CtxHook</td>
</tr>
<tr>
<td></td>
<td>Ignore HKEY_LOCAL_MACHINE\SOFTWARE \Citrix\IMS</td>
</tr>
</tbody>
</table>
Profile Contents on the File 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 section describes the structure of profile directories and the files in them. Citrix recommends that you do not modify these files directly. Use only the profiler to modify these files.

A profile folder on a file share contains the following:

- Profile manifest file (.profile), an XML file that defines the profile
- Target CAB files 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

<table>
<thead>
<tr>
<th>Named Object Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore ??\pipe\lsarpc</td>
</tr>
<tr>
<td>Ignore ??\pipe\netlogon</td>
</tr>
<tr>
<td>Ignore ??\pipe\ntsvcs</td>
</tr>
<tr>
<td>Ignore ??\pipe\Pipe$CtxSandbox_ADF</td>
</tr>
<tr>
<td>Ignore ??\pipe\Pipe$CtxSandbox_MSI</td>
</tr>
<tr>
<td>Ignore ??\pipe\samr</td>
</tr>
<tr>
<td>Ignore ??\pipe\srvsvc</td>
</tr>
<tr>
<td>Ignore ??\pipe\svectl</td>
</tr>
<tr>
<td>Ignore ??\pipe\wkssvc</td>
</tr>
<tr>
<td>Ignore \pipe\Pipe$CtxSandbox_ADF</td>
</tr>
<tr>
<td>Ignore \pipe\Pipe$CtxSandbox_MSI</td>
</tr>
<tr>
<td>Ignore \pipe\srvsvc</td>
</tr>
<tr>
<td>Ignore \KernelObjects</td>
</tr>
<tr>
<td>Ignore \NLS</td>
</tr>
<tr>
<td>Ignore \SECURITY</td>
</tr>
<tr>
<td>\LSA_AUTHENTICATION_INITIALIZED</td>
</tr>
<tr>
<td>Ignore global\</td>
</tr>
<tr>
<td>Ignore local\mmhook*</td>
</tr>
<tr>
<td>Ignore local\sehook20shmem</td>
</tr>
<tr>
<td>Ignore OleDirRoot*</td>
</tr>
<tr>
<td>Ignore RPC Control</td>
</tr>
<tr>
<td>Ignore semain30*</td>
</tr>
<tr>
<td>Ignore shell.*</td>
</tr>
<tr>
<td>Ignore smartcardsessionreconnect</td>
</tr>
<tr>
<td>Ignore WinSta0_DesktopSwitch</td>
</tr>
</tbody>
</table>
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.cab (the target CAB), first version
- Hashes.txt
- Icondata.bin
- Scripts folder

The following sections describe the purpose and contents of each of these profile components.

**Manifest File**

The manifest 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

**Targets**

Each target consists of a cabinet file (CAB file) representing a compressed subdirectory structure within the profile structure.

Target CAB 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 client workstation. 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 client workstation also includes the version number of the target. In this way, when you update a target, client devices are assured that the execution InstallRoot accurately reflects the install root of the target you defined. For speed, the client workstation locally updates the internal file cache when a target version is updated rather than reloading from the file 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. You can then use and 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 same process is conducted for all of the profile level files. The Sha1 of the hashes.txt file at the profile level is stored in the manifest, and the Sha1 of each target in the profile is stored in the manifest. Because the manifest file is digitally signed, the Sha1 of each file listed in each hashes.txt file can be authenticated.

**Icons**

To keep the manifest file size small, the binary data that represents the application icons is stored in a separate file called icndata.bin. The profiler stores all icons for the installed application. You can change the icon when you publish the streamed application, choosing among the set of icons that the application installed or other icons that you prefer.

**Scripts**

The Streaming Client can execute scripts associated with a profile or target according to both of the following:

- Before the client executes the first application from a profile
- After the client 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 executable by Windows. You create pre-launch and post-exit scripts independent of the profiler and add them to the profile using the profiler. A script consists of the following:

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

After creating a script, use the profiler to add the script to a target. 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, you can add a script for the DLL file and disable it. The DLL file is available for the script to load, but the client does not run the disabled DLL. For example, you can use this technique to add a signed DLL to the profile even though it is not executed.
Managing Streamed Applications

This chapter presents instructions for the following:

- Task Overview of Working with Streamed Applications
- Overview of Publishing Streamed Applications
- Selecting the Delivery Method for Streamed Applications
- Providing Offline Access to Applications Streamed to Desktop
- Streaming Applications to Presentation Server
- Pre-deploying Applications to Clients
- Setting Streamed Application Properties

These sections describe the main features for publishing, configuring, deploying, and maintaining streamed applications.

Task Overview of Working with Streamed Applications

After you install a server farm, you can use the Access Management Console to configure it. Some important configuration tasks you perform are:

- Creating a Web Interface site or a Program Neighborhood Agent site
- Creating Citrix administrator accounts and delegating areas of administration
- Publishing applications
- Enabling offline access and reserve licenses for its use
- Setting individual server properties, which take precedence over farm properties

The next section describes how to start and use the Access Management Console to perform these and other tasks.
Overview of Publishing Streamed Applications

Before you can publish a streamed application, you must use the Streaming Profiler to profile it. For information about profiling applications for use with the application streaming feature, see Chapter 2, “Creating Resource Profiles.”

An integral function of Presentation Server is to make profiled applications available to users. When you publish an application, you also make choices about the following application properties:

- Display name and description of the application
- Application type and streamed delivery method
- The application profile you are publishing
- Offline access options
- Users and groups who can access the application
- How the application shortcuts are presented on the user desktop
- Immediate availability of the application
- Requirement for access through Access Gateway Enterprise filters
- Content redirection
- An alternate profile for connections from specific IP addresses
- Least-privileged user accounts

Use the Publish Application wizard in the Access Management Console to publish streamed applications in your farm.

To publish an application

1. Open the Access Management Console, and if necessary, run discovery.
2. Open the farm on which you want to publish the application.
3. Select the Applications node and from the Common Tasks pane choose New > Folder. Create a folder for the application you are publishing.
4. Select the folder you created and from the Common Tasks pane choose New > Published Application.

Follow the instructions in the Publish Application wizard. Detailed help for each step is available by clicking Help.

For tips about using the publishing wizard, see the next procedure.
To use the Publish Application wizard

**Note** Steps and options in the wizard vary depending on the application type you select. This procedure describes the basic options available for streamed applications.

1. On the **Name** page, provide a display name and application description.
2. On the **Type** page:
   - Select **Application**.
   - Select the delivery method. For more information, see “Selecting the Delivery Method for Streamed Applications” on page 64.
3. On the **Location** page:
   - Select the application profile containing the application you want to publish. To select the profile, click **Browse** and or type the UNC path to the manifest, which is a .profile file. For example: `\citrixserver\profiles\Adobe Reader\Adobe Reader.profile`
   - After you select a profile, the application drop-down list is populated with the applications in the profile. From the drop-down list, select the application you want to publish.
4. On the **Offline Access** page, specify whether or not you want the published application to be available offline to configured users.
   
   For more information about this option, see “Providing Offline Access to Applications Streamed to Desktop” on page 70.
   
   If you enable the application for offline access:
   - Specify how you want the client to cache the necessary application files on the user workstation: at logon or at launch.
   - You can click the **Configure Offline Access Users** to open the farm property for **Offline Access > Users** and create the Configured Users list of users and groups that have permission to run enabled applications in offline mode. You can also configure this list later. For more information, see “Creating the List of Users Who Have Offline Access Permission” on page 71.
5. On the **Users** page, create the Configured Users list for users or groups who have access to the application. For more information, see “Creating the List of Users Who Can Access the Application” on page 80.
6. On the **Shortcut presentation** page, you can change the icon for the application and choose how the application is enumerated on the user’s workstation. For more information, see “Configuring Icon Presentation” on page 82.

7. On the **Publish immediately** page, choose whether or not to make the published application immediately available to your users.

   - By default, the published application is available when you click *Finish*. The option to **Disable application initially** is not selected.
   - To prevent users from accessing the application until you manually enable it through application properties, select **Disable application initially**.
   - To view and select advanced options, check **Configure advanced application settings now**. You can also modify the advanced settings using the application properties described in the following sections:
     - “Controlling Access Connection Types” on page 82
     - “Associating an Application with File Types” on page 83
     - “Specifying Alternate Profiles” on page 84
     - “Assigning a Least-Privileged User Account” on page 85

The remaining sections in this chapter describe detailed procedures or features related to streamed applications.

**Selecting the Delivery Method for Streamed Applications**

As you publish applications in the presentation server farm, you select the delivery methods to the clients. With the application streaming feature, you can configure profiled applications to stream to the server or the user’s desktop.

**Selecting the Application Type**

Configure the application delivery method as you publish the application in the Access Management Console. Publish the application using the Publish Application wizard and continue to the Type page.

---

**Note** Before you can publish a streamed application, 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. For information about application profiling, see Chapter 2, “Creating Resource Profiles.”
To specify an application type, select **Application**, and then select the delivery method from the **Server application type** drop-down list, as follows:

- **Streamed to client.** Enables users to stream a profiled application from the file share to their client desktops and launch it locally. Users must have the streaming client installed and access the application using the Windows version of the Program Neighborhood Agent or a Web Interface site.

  If selected, clients that do not support application streaming (such as non-Windows clients) or do not have the streaming client installed locally cannot launch the application.

- **Accessed from a server.** Enables users to launch an application from your server using ICA.

  Select the type of application users can access:

  - **Installed application.** Enables users to launch an application installed on your server.

  - **Installation Manager packaged application.** Schedules Installation Manager for an installation on your server, and then enables users to launch an application installed in the package.

  - **Streamed to server.** Enables clients to stream a profiled application from the file share to your server, and users launch the application on the server.

  - **Streamed if possible, otherwise accessed from a server** (also called **dual mode streaming**). Enables users to stream a profiled application from the file share to their client desktop and launch it locally. Alternatively, clients that do not support streamed applications instead access the application installed on or streamed to your server.

  Select the **alternative** delivery method for clients that do not support streaming to client:

  - **Installed application.** Enables users to launch an application that is already installed on the server.

  - **Installation Manager packaged application.** Schedules Installation Manager for an installation on your server, and then enables users to launch an application installed in the package.

  - **Streamed to server.** Enables clients to stream a profiled application from the file share to your server, and users launch the application on the server.
To change the application type after you publish the application, in the Access Management Console, from the Action menu, select All Tasks > Change application type, and follow the steps in the wizard.

See the table on page 67 for more information.

**Specifying a Policy for the Application Delivery Method**

You can use 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.

**To specify a farm-wide policy**

1. Open the Presentation Server Console (Start > All Programs > Citrix > Management Consoles > Presentation Server Console). Under the farm name, select Policies.

2. From the Action menu, select New > Policy, name the policy, and click OK.

3. Open the properties by selecting the policy name, and from the Actions menu, select Properties.

4. In the Properties dialog box, expand User Workspace > Streamed Applications > Configure delivery protocol.

5. Click Enabled and select an option:
   
   - **Force server access** (selected by default). 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.

   - **Force streamed delivery**. Clients always stream the application from the file share location to the client desktops. Users must have the streaming client installed and access the application using the Windows version of Program Neighborhood Agent or a Web
Interface site. For example, you might use this setting to prevent the use of server resources.

If you disable the rule or leave it not configured, the delivery method specified in the Publish Application wizard is used.

The following table describes the default delivery of each application type and the results of setting the policy. The policy 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: Force Server Access</th>
<th>With policy: Force streamed Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Streamed to client</strong></td>
<td>Streaming Client streams application from file share to desktop.</td>
<td>Connection fails</td>
<td>Connection works</td>
</tr>
<tr>
<td><strong>Accessed from a server:</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>— Installed application</td>
<td>Any ICA client accesses application installed on server (not streamed).</td>
<td>Policy does not apply</td>
<td>Policy does not apply</td>
</tr>
<tr>
<td>— IM packaged application</td>
<td>Any ICA client accesses IM packaged application installed on server (not streamed).</td>
<td>Policy does not apply</td>
<td>Policy does not apply</td>
</tr>
<tr>
<td>— Streamed to server</td>
<td>Streaming Client streams application from file share to the server and any ICA client accesses streamed application on server location.</td>
<td>Policy does not apply</td>
<td>Policy does not apply</td>
</tr>
<tr>
<td><strong>Streamed if possible; otherwise accessed from a server (dual mode):</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>— Installed application</td>
<td>Dual mode: Streaming Client streams application from file share to desktop. Otherwise, any ICA client accesses application installed on server.</td>
<td>An ICA client always connects to application installed on server</td>
<td>Streaming Client always streams application to desktop</td>
</tr>
<tr>
<td>— IM packaged application</td>
<td>Dual mode: Streaming Client streams application from file share to desktop. Otherwise, any ICA client accesses IM packaged application installed on server.</td>
<td>An ICA client always connects to IM packaged application installed on server location</td>
<td>Streaming Client always streams application to desktop</td>
</tr>
<tr>
<td>— Streamed to server</td>
<td>Dual mode: Streaming Client streams application from file share to desktop. Otherwise, application streams from file share to server location and any ICA client accesses application on server.</td>
<td>Streaming Client always streams application to server location</td>
<td>Streaming Client always streams application to desktop</td>
</tr>
</tbody>
</table>
Streaming Applications to Presentation Server

To simplify deployment of applications to servers in a server farm, you can stream applications to servers running the Enterprise edition of Presentation Server, and those servers can then present the applications through an ICA connection to users’ desktops.

Before publishing an application that is streamed to server, complete the following tasks:

- Ensure your Web Interface sites and Program Neighborhood Agent sites are configured to run one of the following application types:
  - Remote applications only
  - Dual mode streaming (stream to the client, otherwise virtualize from Presentation Server)

  For information about managing application types on Web Interface sites, see The Web Interface Guide.

- Using Citrix Profiler installed on a server running a Citrix Presentation Server environment, create a target or application profile intended for Windows Server 2003. For more information about creating targets, see “Creating a Profile and its Initial Target” on page 23.

After you ensure all of these tasks are complete, you publish the application on each server as streamed to server.

To publish an application that is streamed to servers in a farm

1. Under the Presentation Server node of the Access Management Console, expand the farm to which you want to stream an application.

   Select the Applications node, then, from Common Tasks, select New > Folder. Create a folder for the application you are publishing.

   Select the folder you created and from the Common Tasks pane choose New > Published Application.

2. In the Publish Application wizard, click Next.

   Provide a name and description for the published application, then click Next.

3. On the Type page:
   - Choose Application and Accessed from a server.
   - Then, from the Server application type drop-down menu, choose Streamed to server, then click Next.
4. On the **Location** page:

   - Select the application profile containing the application you want to publish. To select the profile, click **Browse** and or type the UNC path to the manifest, which is a .profile file. For example: \\citrixserver\profiles\Adobe Reader\Adobe Reader.profile

   - After you select a profile, the application drop-down list is populated with the applications in the profile. From the drop-down list, select the application you want to publish.

5. On the **Servers** page, to choose the servers in a farm to which you want to stream the application, click **Add**.

   Use the Select Servers dialog box to choose the servers, and click **OK** then **Next**.

6. On the **Users** page, create the Configured Users list for users or groups who have access to the application. For more information, see “Creating the List of Users Who Can Access the Application” on page 80.

7. On the **Shortcut presentation** page, you can change the icon for the application and choose how the application is enumerated on the user’s workstation. For more information, see “Configuring Icon Presentation” on page 82.

8. On the **Publish immediately** page, choose whether or not to make the published application immediately available to your users.

   - By default, the published application is available when you click **Finish**. The option to **Disable application initially** is not selected.

   - To prevent users from accessing the application until you manually enable it through application properties, select **Disable application initially**.

   - To view and select advanced options, check **Configure advanced application settings now**. You can also modify the advanced settings using the application properties described in the following sections:

      - “Controlling Access Connection Types” on page 82

      - “Associating an Application with File Types” on page 83

      - “Specifying Alternate Profiles” on page 84

      - “Assigning a Least-Privileged User Account” on page 85

For complete instructions about publishing streamed applications, see “Overview of Publishing Streamed Applications” on page 62.
Providing Offline Access to Applications Streamed to Desktop

Administrators can configure streamed applications so that users can disconnect from the company network and continue to run the applications in offline mode for a specified length of time. This capability is referred to as offline access.

When you make streamed applications available offline, the next time the user’s client connects to the server, the streaming client downloads the application and caches it on the user’s client.

Note 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.

To enable the offline access feature, configure the following settings using the Access Management Console:

• Configure the farm-wide properties for offline access. For information, see the following sections:
  • “Creating the List of Users Who Have Offline Access Permission” on page 71
  • “Selecting the License Setting for Offline Users” on page 74
• Configure the application properties for offline access. For information, see the following sections:
  • “Enabling an Application for Offline Access” on page 75
  • “Creating the List of Users Who Can Access the Application” on page 80

Users who have offline access permission for the farm and permission to access the published application must launch the application through the Program Neighborhood Agent client to use the offline access feature.
The Citrix Streaming Client caches each streamed application on the hard drive of the client workstation. 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.

**Note** You do not need to do any additional configuration in the streaming profiler to create application profiles or targets with applications that can be accessed offline. Save the profiles to a network file share normally so they are available for publishing using the Access Management Console.

### Creating the List of Users Who Have Offline Access Permission

Administrators must create a list of users who have offline access permission. Users or groups listed in this farm property (and who are also configured for the application) have permission to run offline-enabled applications in offline mode. Users or groups on this list require an offline license to launch applications regardless of whether they are online or offline.

**To configure users for offline access permission**

1. From the Access Management Console, select the farm.
2. Under Common Tasks, select **Modify farm property > Modify all properties**. From the **Farm Properties** dialog box, select **Offline Access > Users**.
3. To choose the user accounts that can have offline access, use the **Select directory type** drop-down box to select either **Citrix User Selector** or **Operating System User Selector**.
4. Click **Add** to open the **Select Users or Groups** dialog box:
   - If you selected **Citrix User Selector** (default selection), complete the following in the **Select Users and Groups** dialog box:
     - Select your account authority from the **Look in** drop-down list. The drop-down list contains all trusted account authorities configured on the servers in the farm. These include Novell Directory Services (NDS) trees, Windows NT domains, Active
Directory domains, and local servers. (NDS trees appear only if previously configured.)

**Note**  When you select an account authority, the user accounts that are part of the selected authority are displayed in the window below the drop-down list. By default, only user groups are displayed.

- Select **Show Users** to display all user names in the selected domain. This option displays every user in the selected domain. For NDS, alias objects are also displayed. The user accounts you select are listed in Configured Accounts.

**Note**  Instead of selecting names from the list, you can type them in a text box. To do this, click **Add List of Names** and use semicolons (;) to separate names.

- If you selected **Operating System User Selector**, use the standard Windows dialog box to select your user or group.

**Note**  This option has several limitations. You can browse only account authorities and select users and groups who are accessible from the computer running the Access Management Console. In addition, you can initially select users and groups outside the trust intersection of the farm that causes errors later. Other limitations include the inability to add NDS users and groups and Citrix built-in users.

5. Click **OK**.

The list of user accounts is added to the **Configured Accounts** list.
Creating the List While Publishing Applications

As you publish applications and configure the application for offline access, you can view or modify the users and groups who have offline access permission in the farm. To do this, click **Configure Offline Access Users** on the Users page of the Publish Applications wizard.

---

**Note**  You must also add the users to the configured users list for the applications that they can access offline. Users who are configured for the application in this wizard, but who are *not* added to the configured users list for offline access in the farm, can access the application online, but not offline.

---

Indirect Membership to the Offline Access User List

You can give users indirect permission for offline access by making them members of groups or subgroups that have offline access.

For example, if you add Group A to the offline user list, and User 1 is a member of Group A and is also added to the application user list, User 1 has offline access for the application.

---

**Group A is in the offline access user list**

Because User 1 is in the application’s user list and is in Group A, which has offline access permission, User 1 has offline access to the application.

A user who is in the application’s user list and is also a member of a group that has offline access permission, indirectly has offline access to the application.

You can specify subgroups of larger groups for indirect access. For example:

- Group A contains Subgroups B and C
- Users of Subgroup B have farm-wide permission for offline access
- Group A has permission for access to the application

With this grouping, only members of Group B can access the application offline or online (even though Group B is not explicitly added to the application user list), while Group C can access the application only when online.
Users in subgroups have their own access permissions as well as the indirect access permissions of any groups or subgroups to which they belong.

### Selecting the License Setting for Offline Users

The license specifies the time period that users can run streamed applications before they must renew the license. To access this dialog box, from the farm properties, select **Offline Access > Offline License Settings**.

The license period that you set in this property, 21 days by default, can range from 2 to 365 days. This number specifies the number of days that users can run the application both online and offline before they have to renew the license.

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.

For more information, see the *Getting Started with Citrix Licensing Guide*.

### Renewing Offline Licenses

When users with offline access log on to Program Neighborhood Agent, they automatically either check out an offline license or renew a license already checked out. Licenses extend for the specified license period, set in the farm property for **Offline License Settings**. If users stay logged on to Program Neighborhood Agent, 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 to Program Neighborhood Agent (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, online or offline.

**Enabling an Application for Offline Access**

You can configure streamed applications for offline access as you publish them or in the application’s properties:

- As you publish profiled applications in the Publish Applications wizard, click the *Enable offline access* check box on the Offline Access page.

- In the application’s properties page, select **Basic > Streaming settings > Offline Access**. Click the *Enable offline access* check box to enable the feature.

**Selecting the Caching Method**

The server fully caches applications enabled for offline access on client workstations; the entire application is sent to client workstations while the user is online so that the user can launch the application offline and have full functionality of the application. By default, applications are cached when a user logs on.

After you enable the feature, select the method of caching:

- **Pre-cache application at login**. Caches the application when the user logs on (selected by default). However, concurrent logons may slow network traffic.

- **Cache application at launch time**. Caches the application when users launch it. Use this option if the number of users logging on at the same time (and pre-caching their applications) could overload the network.

Pre-caching is also possible using third-party tools, such as Microsoft System Management Server (SMS) or Altiris. If you use a third-party caching method, you can ignore this setting because it is not used; that is, applications are not cached twice.

**The User’s Experience with Offline Access**

When users who are configured for a streamed application and have offline access permission run the Program Neighborhood Agent client, they automatically check out an offline license (or renew a currently held license).
In addition, applications download to users depending on the caching preference set for the farm:

- If you configured pre-caching at logon (selected by default), a notification message tells the users when the download starts and completes. After the download finishes, users can then disconnect from Program Neighborhood Agent and run the cached applications in offline mode until the period of time elapses.

- If you configured caching at launch, users must launch the application while connected to the network (online mode). After the download finishes, users can disconnect from Program Neighborhood Agent and run the cached application in offline mode until the period of time elapses.

When users are offline, application shortcuts are displayed as “available” if the license is still current or “unavailable” if the offline license has expired (these applications cannot launch).

To review the status of their cached applications, users can right-click the Citrix Program Neighborhood Agent icon in the notification area and select **Offline Applications**. The list includes the offline applications with their download status, total offline license period, and number of days remaining before the check-out period ends.

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 to Program Neighborhood Agent (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, online or offline.

**Pre-deploying Applications to Clients**

Citrix recommends that administrators pre-deploy the applications used most frequently by end users. Pre-deployment pushes new or updated application files to users’ workstations and helps avoid overloading the file servers or network.

The utility enables administrators to schedule pre-deployment overnight or during off hours.

**Running the Pre-deployment Utility**

The streaming client includes the pre-deployment utility called RadeDeploy.exe located on the components CD. After it is installed, locate the utility in `\Program Files\Citrix\` directory.
To run RadeDeploy

1. On the client desktop that has the Streaming Client installed, open a command prompt. Enter the command line with the UNC path to locate the manifest file (.profile) on the network file share, using the following example:

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

   Use the following commands:

   - To enumerate applications
     `radedeploy /enum`
   - To add applications
     `radedeploy [-m] /deploy:filename`
     where `filename` can be a .profile file. File names with embedded spaces should be quoted.
     and where [-m] means to monitor deployment until complete.
   - To delete applications
     `radedeploy /delete:BrowserName`

2. The utility selects the target and automatically deploys the best fit to bring the necessary files to the client.

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

The application properties are set when you publish an application. Application properties include the following:

- Name and description of the application
- Whether or not the application is enabled
- Whether or not the application is available offline
- Users or groups having access to the application
- Icon that represents the application
- How the application is listed (enumerated) on the user workstation
- Types of connections through which users access published applications
- File types associated with an application
- Alternate application profiles

The changes you make to application properties take effect the next time each user launches the application or reconnects to the network.

To view or modify properties for an application

1. From the console tree of the Access Management Console, expand the Presentation Server node.
2. Under the Application node, select an application.
3. Under Common Tasks, choose Modify application properties > Modify all properties.

The sections that follow describe the application properties that you can modify.

Naming and Describing the Application

You can change the application names and descriptions that appear in Web Interface. Changes take effect after the user reconnects or refreshes the client.

The Application Name is a character string used to identify the application in the farm. The character string (maximum 38 characters) is copied from the Display Name specified when the application is published.
From the Basic Properties page, choose Name to view or modify the following options:

- Application name displayed in the Access Management Console
- Application name
- Application description

The console updates the Application Name for the renamed application. If a duplicate Application Name is found in the farm, a four-digit hexadecimal number is appended to the original string. If the character limit is reached and duplicated, the console replaces the end characters with four-digit hexadecimal numbers, starting from the right. Application Name is displayed in the left pane of the Properties dialog box for an application.

Enabling and Disabling an Application

From the Basic Properties page, choose Name to enable or disable the application. Changes take effect after the user reconnects or refreshes the client.

Specifying the Application Location

From the Basic Properties page, choose Location to view or modify the these options.

To specify the application and location

1. In the Streaming Server profile address text box, type the Full Universal Naming Convention (UNC) path to the profile manifest file (.profile); for example, \citrixserver\profiles\Adobe Reader\Adobe Reader.profile.
2. Choose the application from the Application to launch from the Streaming application profile drop-down menu.
3. In the Extra command line parameters text box, type parameters to use when the profiled application includes ** as a placeholder for additional command-line parameters. If there is no ** in the command-line string, the extra parameters specified here are added at the end of the command-line. Administrators use the extra command line parameters to specify additional items on the command-line. For more information, see “Command Line Parameters” on page 18.
4. Click OK.

Changes take effect after the user reconnects or refreshes the client.
Creating the List of Users Who Can Access the Application

You can configure users for the application while you publish the application or in the application properties, as described in this section.

From the Basic Properties page, choose Users to view or modify the following options:

1. Select Allow only configured users (not selected by default).

2. To choose the user accounts that can have offline access, use the Select directory type drop-down box to select either Domain or Active Directory (Farm) or Domain or Active Directory (Local).

3. Click Add to open the Select Users or Groups dialog box:
   - If you selected Domain or Active Directory (Farm) (default selection), complete the following in the Select Users and Groups dialog box:
     - Select your account authority from the Look in drop-down list. The drop-down list contains all trusted account authorities configured on the servers in the farm. These include Novell Directory Services (NDS) trees, Windows NT domains, Active Directory domains, and local servers. (NDS trees appear only if previously configured.)

   **Note** When you select an account authority, the user accounts that are part of the selected authority are displayed in the window below the drop-down list. By default, only user groups are displayed.

   - Select Show Users to display all user names in the selected domain. This option displays every user in the selected domain.
For NDS, alias objects are also displayed. The user accounts you select are listed in Configured Accounts.

**Note** Instead of selecting names from the list, you can type them in a text box. To do this, click **Add List of Names** and use semicolons (;) to separate names.

- If you selected **Domain or Active Directory (Local)**, use the standard Windows dialog box to select your user or group.

**Note** This option has several limitations. You can browse only account authorities and select users and groups who are accessible from the computer running the Access Management Console. Also you can initially select users and groups outside the trust intersection of the farm that causes errors later. Other limitations include the inability to add NDS users and groups and Citrix built-in users.

When you click **OK**, the list of user accounts is added to the Configured Accounts list. For more information about configuring users for the application, see “Overview of Publishing Streamed Applications” on page 62.

**To remove users from the list**

1. From the **Basic Properties > Users** page, select the users you want to delete from the list.
2. Click **Remove**.
3. Click **OK**.

These users no longer have access.
Configuring Icon Presentation

Use Basic Properties > Shortcut presentation to configure the application shortcut presented to the client. With this page, you can view or modify the following:

- **Application Icon.** Displays the current icon associated with the application. To specify a different icon for the application, select Change Icon and browse for a different icon.

- **Application shortcut placement.** Displays the icon in the location on the client workstation where you specify. You can specify the following:
  - **Add to the client’s start menu.** Creates a shortcut to this application in the user’s local Start menu.
    - For Program Neighborhood Agent only, you can specify a folder under the Programs folder of the local Start menu by selecting the Place under Programs folder.
    - For example, to have the application appear in the Start menu (or Programs folder, if selected) under a folder called Reports, type Reports\HR\Survey.
  - **Add shortcut to the client’s desktop.** Creates a shortcut to this application on the user’s local desktop.

Changes take effect after the user reconnects or refreshes the client.

Controlling Access Connection Types

Use the Access control page of the Publish Application wizard or the application properties to specify the types of connections through which users can start sessions to access published applications on the farm.

If Access Gateway (Version 4.0 or later) is installed, select Access Control from the Advanced Application Properties page to specify the type of connections that allow the application to appear in the client's list of published applications.

For example, if Access Gateway is installed and the application has software requirements, you can define a filter in Access Gateway and apply the filter to the published application using Presentation Server.

**Important** To use this feature, set your servers that receive XML requests to trust those requests.
With this page, you can view or modify the following:

- **Allow connections made through Citrix Access Gateway Enterprise (Version 4.0 or later)**. This is the default. Select the type of connections that allow the application to appear in the list of applications:
  - **Any connection**. Allows connections made through Access Gateway (Version 4.0 or later), regardless of filters. This is the default.
  - **Any connection that meets any of the following filters**. Allows connections made through Access Gateway (Version 4.0 or later) that meet one or more of the connection filters specified in the list.
    
    To **Add** or **Edit** a filter, click the respective button and enter the predefined Access Gateway farm name and filter.
    
    To **Remove** a filter, select a filter from the list and then click **Remove**.
  - **Allow all other connections**. Allows all connections except those made through Access Gateway (Version 4.0 or later). This is the default.

Users who do not have the required software running on the client cannot access the published application

### Associating an Application with File Types

From the **Advanced Application Properties** page, choose **Content Redirection** to configure content redirection from client to server by associating the published application with specified file types. The application opens when a user double-clicks a file with one of the specified file type extensions. Published applications can be associated with one or more file types.

If you do not want specific users to automatically start published applications based on file type, do not assign those users to published applications that are associated with file types.

With this page, you can view or modify the following:

- The types of files that you want the application to open when a user double-clicks a file.
- **Select all**. Associates the published application with all available file types.
- **Deselect All**. Clears all previously chosen file types.
- **Show all available file types for this application**. This is the default. Lists all file types associated with the application. Clear the check box to display only the selected file types.
Specifying Alternate Profiles

You can specify a different application profile for connections that come from specific IP addresses. For example, you might use an alternate profile to allow one published application for users on either side of a WAN with file servers on their side.

With this page, you can view or modify the following:

- **Primary application profile location.** Location of the profile on the network file share. You cannot change this location on this page.

- **Alternate profile locations.** List of existing alternate profile locations, including their client IP ranges. You can add, modify, or remove alternate profile locations.

Changes take effect the next time the user launches the application.

**To add an alternate profile**

1. From the Advanced Application Properties page, choose Alternate Profiles.
2. Click Add.
3. In the Alternate profile location dialog box, type the starting and ending client IP range for which the alternate profile applies.
4. Type the full path of the profile on the network file share or browse to locate the profile; for example: \citrixserver\profiles\Adobe Reader\Adobe Reader.profile.
5. Click OK.

After you configure the range, clients from IP addresses within the specified range access the applications from the alternate profile instead of from the default profile.

**To edit the IP range or path**

1. Select the alternate profile.
2. Click Modify.
3. Make your changes and click OK.

After you make your modifications, clients from IP addresses within the specified range access the applications from the alternate profile instead of from the default profile.
To delete the alternate profile

1. Select the alternate profile.
2. Click **Remove**.
3. Click **OK**.

After you remove the alternate profile, clients access applications from the default profile.

**Assigning a Least-Privileged User Account**

For streamed applications only, use this setting to reduce the user privileges for the application, thus reducing security risks.

**To reduce users’ privileges for an application**

1. From the **Advanced Application Properties** page, choose **User privilege**.
2. Select **Run application as a least-privileged user account** (not selected by default). This setting configures all users, even those with an administrator account, to run the application with normal user privileges.

**Important** Before you select this option, test the application with a limited access configuration. Some applications expect users to have elevated privileges and might fail to operate correctly when launched by users with a least-privileged user account.

For more information about least-privileged user accounts, search the Microsoft Web site at www.microsoft.com.
Managing Streaming Clients

This chapter is for system administrators responsible for installing, configuring, deploying, and maintaining the Streaming Clients for Windows.

Before installing and configuring clients, be familiar with the following:

• The server farm to which your clients connect
• The operating system on the client device (Windows 2000 and Windows XP)

This chapter introduces Citrix clients for workstations running Windows operating systems, including 32- and 64-bit, as well as the following topics:

• Introduction to Streaming Clients
• System Requirements
• Installing the Streaming Client
• Configuring the Streaming Client
• Installing Program Neighborhood Agent
• Configuring Your Installation Files

Familiarity with these topics will help you to test the clients and deploy them to your users.
Introduction to Streaming Clients

Streaming clients are the components of the application streaming feature, which users run on their workstations to access published resources. Either of the following combinations are available with the application streaming feature:

**Streaming Client with Program Neighborhood Agent.** You can install the Streaming Client and Program Neighborhood Agent to make available the full set of application streaming features. Using the Streaming Client with Program Neighborhood Agent enables you to enumerate published applications in the desktop Start menu and create shortcuts on the desktop. In addition to desktop integration, Program Neighborhood Agent also enables end users to go offline with published applications.

**Streaming Client with a Web browser.** You can install the Streaming Client by itself on the end user desktop, and the user can access published applications through a Web browser using the Web Interface site you create. For this access method, only the Streaming Client is required. Offline access to applications and desktop integration is not available when using this access method.

About Program Neighborhood Agent

Program Neighborhood Agent is a client that supports the full application streaming feature set. It is centrally administered and configured in the Access Management Console using a Program Neighborhood Agent site created in association with a site for the server running the Web Interface.

**Access Method.** Program Neighborhood Agent enables your users to access all of their published resources from a familiar Windows desktop environment. Published resources are enumerated on the client desktop, including the Start menu and the Windows notification area, by icons that behave just like locally installed icons. Users can double-click, move, and copy icons; and create shortcuts in their locations of choice. Program Neighborhood Agent works in the background. Program Neighborhood Agent has a shortcut menu available from the notification area and a user interface to manage the client’s properties.

**Client Management and Administration.** Program Neighborhood Agent is configured at a site created in the Access Management Console and associated with the site for the server running the Web Interface. By using the Access Management Console in this way, you can dynamically manage and control your client population throughout your network from a single location and in real time. Because client-server data transfer occurs over standard HTTP or HTTPS protocols, you can use Program Neighborhood Agent with firewalls using port 80 (for HTTP) or 443 (for HTTPS).
About the Streaming Client

The Streaming Client provides streamed applications from a profile target on a file server to the user desktop. The Streaming Client performs the following:

- Runs as a service on the user workstation to invoke applications the user selects and Program Neighborhood Agent or the Web Interface site enumerates
- Finds the correct profile target for the user workstation, creates an isolation environment on the user workstation, and streams to the user desktop the necessary files for the application to run

The streaming client also checks the cache size of the end-user’s workstation. If the cache size exceeds a maximum limit, the client 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 client removes streamed application files starting with the one that was not used in the longest time.

You install the Streaming Client and Program Neighborhood Agent on the user workstation.
System Requirements

To run clients for use with the application streaming feature, client workstations must meet the following requirements:

- Standard PC architecture, 80386 processor or greater as required for the operating system.
- Have installed one of the following operating systems:
  - Windows 2000 Professional, Service Pack 3 or 4
  - Windows XP Professional, Service Packs 1 or 2
  - Windows XP Professional 64-bit Edition, Service Pack 1
  - Windows Server 2003 (Standard, Enterprise, or Datacenter Edition) with Service Pack 1 or 2
  - Windows Server 2003 R2, 32- or 64-bit Editions
  - Windows Server 2003 64-bit Edition, Service Pack 1
- Available memory as recommended for the operating system by Microsoft or the manufacturer of profiled applications.
- Microsoft XML 2.0. It is recommended that you use Windows Update to ensure you have installed all the recent Internet Explorer updates.
- For network connections to the server farm, a network interface card (NIC) and the appropriate network transport software are required.

In addition, installation of the clients requires administrator rights on the local computer on which you are installing the client.

Installing the Streaming Client

The Streaming Client is installed by default on a server when you install Presentation Server. This enables the server for further configuration of streaming to server and dual mode streaming. For more information, see “Streaming Applications to Presentation Server” on page 68.

For your users to streamed applications to their desktops, they or you must install the Streaming Client on their workstations.

To install the client, you must have local administrator privileges. After installation and restarting the workstation, the client runs as a service and, except for error and status messages, is not visible to your users.
Streaming applications to users desktops requires additional licensing.

**To install the Streaming Client**

1. From the Presentation Server Components CD, run **autorun.exe**.
   Click **Citrix Presentation Server Clients**, then **Install Citrix Streaming Clients for Windows**.

2. Choose the language in which you want the client installer to run. (In this step, you are only choosing the language for the installer, not the language of the client.)

3. On the Welcome screen, click **Next**, and then accept the license agreement.

4. On the Select Client screen:
   A. If you want to make offline applications available to your users, the version of Program Neighborhood Agent included with this version of Presentation Server is required.

   If you want to install Program Neighborhood Agent along with the Streaming Client, accept the default and see “Installing Program Neighborhood Agent” on page 93.

   B. If you do not want to install Program Neighborhood Agent, choose **Entire feature will be unavailable**. If you intend to provide access to applications through a Web page only, Program Neighborhood Agent is not required.

   C. Click **Next**.

5. On the Client Name screen: choose a unique name to represent the client to the server. It is recommended that you use the computer name as the client name (selected by default).

6. On the Use Local Name and Password, choose whether or not to pass your local user name and password to the server.
   A. If you are using single sign-on, choose **Yes**.

   B. Click **Next**.

7. Review the list of clients you chose to install. The applicable client for these installation instructions is **Citrix Streaming Client**.

   To begin the installation the Streaming Client, click **Install**.

8. After installation click **Finish** and restart the workstation.

After installing the Streaming Client and restarting your workstation, the Citrix Streaming Service starts automatically on the client computer and runs as the user Ctx_StreamingSvc.
To deploy the Streaming Client to your end-user workstations, use Microsoft System Management Server (SMS) or Microsoft Active Directory Services. For instructions about how to use these products to deploy applications, see the documentation for the product you are using.

The Streaming Client installer resides in the following location on the Presentation Server Components CD:

Clients\rade\Citrix Streaming Client.msi

The Streaming Client installer installs drivers and requires administrator privileges on the end-user workstations. For those users who have administrator privileges on their workstations, you can make available the client installer MSI file, and they can install it themselves. The Streaming Client installer does not require any configuration during installation.

If you install only the Streaming Client on an end-user workstation, you must access applications through a Web Interface site. Optionally, along with the Streaming Client, you can install Program Neighborhood Agent. The offline applications feature and desktop integration are available only if you install Program Neighborhood Agent as well as the Streaming Client.

**Configuring the Streaming Client**

When you run a streamed application either through Program Neighborhood Agent or from a Web page created through the Web Interface, by default, the Streaming Client caches application files on the primary, local drive of the client workstation at the following location:

%PROGRAMFILES%\Citrix\RadeCache

Before caching files, the streaming client checks the size of this cache. If the cache size exceeds a maximum limit, the client removes streamed application files from the cache until its size is smaller than the limit. The client 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.

You can change the default cache location or the default maximum cache size through use of a tool you run on the client workstation where the Streaming Client is installed.

To start the tool, open the following:

%PROGRAMFILES%\Citrix\Streaming Client\clientcache.exe
Running clientcache.exe on the workstation on which the Streaming Client 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 disk 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 disk.

Changes you make using clientcache take effect the next time you start the client or restart the Citrix Streaming Service.

### Installing Program Neighborhood Agent

Install Program Neighborhood Agent to enumerate applications published on the server. If you want to make applications available for offline use, install Program Neighborhood Agent.

Program Neighborhood Agent installation requires local administrator privileges.

**To install Program Neighborhood Agent**

1. From the Streaming Server components CD, run `Autorun.exe`.

   Click **Product installations and updates**, then click **Install Citrix Streaming Clients for Windows**.

2. Choose the language in which you want the client installer to run. (In this step, you are only choosing the language for the installer, not the language of the client.)

3. On the Welcome screen, click **Next**, and then accept the license agreement.

4. On the Select Client screen:
   A. Ensure Program Neighborhood Agent is selected for installation.
   B. Click **Next**.
5. To configure Program Neighborhood Agent, enter the URL to the server on which you created your Program Neighborhood Agent site through the Access Management Console. Here is an example:

http://server_name

For more information about creating a Program Neighborhood Agent site on your server, see the Web Interface Administrator’s Guide, which is available from the Document Center.

6. On the Select Folder Name screen, choose a folder name that Program Neighborhood Agent creates in the Start menu of the client workstation. This menu contains an enumeration of applications published on the server.

7. On the Client Name screen: choose a unique name to represent the client to the server. It is recommended that you use the computer name as the client name.

8. On the Use Local Name and Password, choose whether or not to pass your local user name and password to the server.
   A. If you are using single sign-on, choose Yes.
   B. Click Next.

9. Review the clients you chose to install. The applicable clients for installation for use with Streaming Server are:

   • Citrix Streaming Client
   • Program Neighborhood Agent

   To begin the installation of selected clients, click Install.

10. After installation, click Finish and restart the workstation.

After installing Program Neighborhood Agent and restarting the computer, the Program Neighborhood Agent icon appears in the notification area of the client desktop.

For information about configuring Program Neighborhood Agent after installation, see the Clients for Windows Administrator’s Guide, which is available through the Document Center.

### Configuring Your Installation Files

You can install and configure the Citrix Streaming Clients by using command-line parameters and through the use of transforms.
To install the clients by using command-line parameters

1. On the computer where you want to install the client package, type the following at a command prompt:

   msiexec.exe /i "path/Citrix Streaming Clients.msi" [Options]

   where path is the location of the MSI package and [Options] can be any of the traditional MSI command-line parameters.

2. Set your options as needed. Examples of some parameters that are supported:

   - /qn executes a completely silent installation.
   - /qb shows simple progress and error handling.
   - /qb-! shows simple progress and error handling without displaying a Cancel button to the user.
   - /lv logfile creates a verbose install log where logfile is the path and filename for where to save the log. Use quotes for a path with spaces.
   - PROPERTY=Value
     Where PROPERTY is one of the following all-uppercase variables (keys) and Value is the value the user should specify.

     - PROGRAM_FOLDER_NAME=Start Menu Program Folder Name, where Start Menu Program Folder Name is the name of the Programs folder on the Start menu containing the shortcut to the Program Neighborhood Agent software. The default value is Citrix\Citrix Access Clients. This function is not supported during client upgrades.

     - INSTALLDIR=Installation directory, where Installation directory is the location where the client software is installed. The default value is C:\Program Files\CitrixICA Client.

     - CLIENT_NAME=Client Name, where Client Name is the name used to identify the client device to the server farm. The default value is %COMPUTERNAME%.

     - ENABLE_DYNAMIC_CLIENT_NAME={Yes | No}. To enable dynamic client name support during silent installation, the value of the property ENABLE_DYNAMIC_CLIENT_NAME in your installer file
must be **Yes**. To disable dynamic client name support, set this property to **No**.

- **CLIENT_UPGRADE={Yes | No}**. By default, this property is set to **Yes**. This installs the client if an earlier version of the client is already installed.

- **ENABLE_SSON={Yes | No}**. The default value is **No**. If you enable the SSON (pass-through authentication) property, set the **ALLOW_REBOOT** property to **No** to avoid automatic restarting of the client system.

---

**Important** If you disable pass-through authentication, users must reinstall the client if you decide to use pass-through authentication at a later time.

---

- **ALLOW_REBOOT={Yes | No}**. The default value is **Yes**.

- **DEFAULT_NDSCONTEXT=Context1 [,…]**. Include this parameter if you want to set a default context for Novell Directory Services (NDS). If you are including more than one context, place the entire value in quotation marks and separate the contexts by a comma.

  Examples of correct parameters:
  DEFAULT_NDSCONTEXT=Context1
  DEFAULT_NDSCONTEXT="Context1,Context2"

  Example of an incorrect parameter:
  DEFAULT_NDSCONTEXT=Context1,Context2

- **SERVER_LOCATION=Server_URL**. The default value is **Web Server**. Enter the URL of the server running the Web Interface. The URL must be in the format http://servername or https://servername.

---

**Note** Program Neighborhood Agent appends the default path and file name of the configuration file to the server URL. If you change the default location of the configuration file, you must enter the entire new path in the **SERVER_LOCATION** key.

---

- **CTX_ALLOW_CLIENT_DOWNGRADE={Yes | No}**. By default, this property is set to **No**. Do not change this property when using with streamed applications.
• REINSTALLMODE=<mode>. The default for this property is oums. Set to aums to overwrite later versions of the client. See Microsoft Windows Installer documentation for details.

Using the above procedure, a command-line configuration of your MSI package could resemble:

msiexec.exe /i "Citrix Streaming Clients.msi" /qb-! /l*v "c:\my logs\clients_install.log" SERVER_LOCATION=http://mywebinterface

This command:

• Installs all clients with visible progress dialog boxes, but the Cancel button is disabled for the user
• Logs the installation messages to “c:\my logs\clients_install.log”
• Specifies the URL (http://mywebinterface) of the server running the Web Interface that Program Neighborhood Agent references

To configure an MSI package using transforms

Important  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. Using your preferred tool for editing Windows Installer packages, open the Client Packager (Citrix Streaming Clients.msi).
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. 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.

For information about client configuration options, see the Clients for Windows Administrator’s Guide, which is available through the Document Center.
Index

A
access
  connection types 82
  offline 9, 63, 70, 73, 75, 82
  users 80
Access Gateway. See Citrix Access Gateway
Access Management Console. See Citrix Access Management Console
accessed from a server application 65
  Installation Manager packaged application 65
  installed application 65
  streamed to server application 65
administrator accounts 61, 85
alternate application profiles 84
application packages. See Citrix Streaming Profiler
application properties 78
  access connection types 82
  alternate application profiles 84
  application location 79
  applications and file types 83
  caching method 75, 76
  disabling an application 79
  enabling an application 79
  icon presentation 82
  indirect access 73
  offline access 63, 70, 82
  users having access 63, 69, 80
applications
  accessed from a server 65
  cache status 76
  caching 9
  delivery method 64, 65
  installing into target 25
  isolation 8
  isolation environments rules 49
  managing 61
  modifying properties 39
  policy for delivery method 66
  profiling overview 14
  properties 78
  publishing wizard 63
  running in the profiler 29
  selecting for listing in the profile 29
  streamed if possible, otherwise from a server 65
  streamed to client 65
  type 64
  viewing details 34
applications streaming
  benefits 8
  architecture diagram 11
  associations
  file type 83
B
benefits of application streaming 8
  application caching 9
  application isolation 8
  disaster recovery 9
  dual mode streaming 9
  install once, deliver anywhere 8
  multiple target environments 9
  offline access 9
  seamless updates 8
  stream to server 9
C
caching methods
  at application launch 75, 76
  pre-cache at log on 76
Citrix Access Gateway
  access connection type 83
  connection types 82
  trust relationships 82
Citrix Access Management Console
  application properties 78
  discovery 62
  managing applications 61
Citrix Streaming Clients
  installation 91
Citrix streaming clients 12
configuration 92
installation 90
overview 88, 89
Citrix Streaming Profiler 10, 12, 14
installing 20
running an application 29
starting 20
Citrix Streaming Service 91
clients
installation options with Citrix Streaming Server 97
Streaming Clients 90, 91
command line parameters 18
configuring
Citrix Streaming Client 92
installation files 94
msi package using command-line parameters 95
msi package using transforms 97
Program Neighborhood Agent 93
connection
access control 82
Citrix Access Gateway 83
types 82
creating
profile and its initial target 23
Ctx_StreamingSvc 91
customized registry settings 28
D
deleting
obsolete version of an updated target 48
rules 44
target from an application profile 46
delivery method
nonstreamed application 65
policy 66
streamed application 64
disabling profile signing 22
disaster recovery 9
discovery
in Access Management Console 62
dual mode streaming 9
E
editing
description 33
location 33
profile name 33
enabling profile signing 22
environment variables
constructing rules 52
F
file type associations 83
viewing 34
files and folders 27
I
icon presentation 82
ignore rules 50
indirect membership to access lists 73
installation
Citrix streaming client 90, 91
files 94
options for the clients 97
Program Neighborhood Agent 93
Installation Manager packaged application 65
Internet Explorer and plugins 27
invoking
pre-launch and post-exit scripts for a profile 37
pre-launch and post-exit scripts for a target 41
isolation environment rules 49
default 55
for a target 41
types 49, 50
isolation rules 49
L
language properties 40
least-privileged user account 85
licenses
offline license period 74
offline license type 74
renewing offline licenses 76
valid period 74
M
msi packages
configuring with command-line parameters 95
configuring with transforms 97
multiple resources
into a target 26
through advanced install 26
N
Novell Directory Services (NDS) support
preferred tree 71, 80
O
offline access 9, 75
caching methods 75
indirect membership 73
license period 74
license type 74
users 71, 73
operating systems 40
language 17
targets 16
overviews
application packaging 14
Citrix streaming clients 88, 89
Citrix Streaming Profiler 14
profiles 14

P
packages
alternate profiles 84
post-exit scripts
for a profile 37
for a target 41
pre-launch analysis for a target 41
pre-launch scripts
for a profile 37
for profiles 37
or a target 41
prerequisites
applications 36
binary files 36
profiles 35
registry entries 36
profiler. See Citrix Streaming Profiler
profiles
adding a target 44
adding default post-exit scripts 37
adding default pre-launch scripts 37
alternate 84
contents on the file server 56
disabling and enabling signing 22
editing properties 32
initializing 24
invoking pre-launch and post-exit scripts 37
opening and adding a target 45
overview 14
planning 23
post-exit scripts 37
pre-launch scripts 37
prerequisites 35
resources 19
saving to a file share 31
selecting applications 29
setting preferences 21
signing 30
specifying scripts 41
viewing details of applications 34
viewing file type associations 34
viewing information 31
viewing properties 32, 33
Program Neighborhood Agent 10, 12, 74, 75, 76, 82, 88
configuration 93
configuration file on Web Interface server 88
installation 93
properties
application 78
publishing applications
procedures 62
R
redirect rules 50
registry settings
configured 28
requirements
system 90
resources, installing multiple 26
reviewing profile information and re-editing 31
rules
adding 42
application isolation environments 49
copying 43
defaults for isolation environments 55
deleting 44
environment variables to construct rule 52
ignore 50
isolation environment 50
Modify Rule wizard 44
modifying 43
New Rule wizard 42
prioritization 50
redirect 50
restrictions 51
S
service pack level 17
setting properties
application 78
single application through quick install, installation 25
stream to server 9, 68
streamed if possible, otherwise from a server application 65
streamed to client application 65
streamed to server application 65
streaming clients. See Citrix streaming clients
system drive letter 17
system requirements 90
T
targets 15
adding to a profile 44
adding to profiles 45
creating 23, 28
deleting from a profile 46
deleting from an application profile 46
deleting obsolete version 48
editing properties 38
including files and folders 27
initializing 24
installing an application 25
installing multiple resources 26
invoking pre-launch and post-exit scripts 41
isolation environment rules 41
modifying language properties 40
modifying name and description 39
modifying the operating system 40
multiple resources 26
operating system 16
post-exit scripts 41
pre-launch analysis 41
pre-launch scripts 41
removing old version 48
updating 47
viewing information 31
viewing properties 38
trust relationships
    Citrix Access Gateway 82
U
users
    least-privileged accounts 85
    offline 71, 73
    profile root security settings 22, 35
W
Web Interface
    configuring Program Neighborhood Agent 88
wizards
    application publishing 63
    Modify Rule 44
    New Rule 42