Reflection X Advantage Help

Date

Attachmate®
Copyrights and Notices

Attachmate® Reflection® 2015

Copyright

© 2015 Attachmate Corporation. All rights reserved.

No part of the documentation materials accompanying this Attachmate software product may be reproduced, transmitted, transcribed, or translated into any language, in any form by any means, without the written permission of Attachmate Corporation.

Patents

This Attachmate software is protected by U.S. patents 6252607 and 6803914. Additional Patent Pending.

Trademarks

Attachmate, the Attachmate logo, and Reflection are registered trademarks of Attachmate Corporation in the USA. All other trademarks, trade names, or company names referenced in this product are used for identification only and are the property of their respective owners.

Attachmate Corporation
705 5th Avenue South
Suite 1100
Seattle, WA 98104
USA
+1.206.217.7100
http://www.attachmate.com (http://www.attachmate.com)

Third-Party Notices

This product contains software from third party suppliers.

Specific notices

This software includes RSA BSAFE cryptographic or security protocol software from RSA. Copyright © 2008 RSA Security Inc. RSA Secured and the RSA Secured logo are registered trademark of RSA Security Inc.

This product uses the FreeType library.

Additional third-party copyrights and notices, including license texts and other materials passed through in compliance with third party license terms, can be found in a thirdpartynotices.txt file in the program installation folder.
# Contents

1 Welcome to Reflection X Advantage ........................................ 7  
   Operating Modes: Domain vs. Standalone ................................... 8  
   The X Window System ................................................................ 9  

2 Installation and Migration ...................................................... 11  
   System Requirements .................................................................. 11  
   Install Reflection X Advantage on Windows ............................... 11  
      Associated Installers ................................................................ 12  
   Install on UNIX .......................................................................... 13  
   Which Reflection X Advantage Features Should I install? .............. 14  
   Upgrade and Migration ............................................................... 15  
      Upgrading from Earlier Versions of Reflection X Advantage ........ 16  
      Upgrading from Reflection X version 13 or 14 ......................... 17  
      Migrating Settings From Hummingbird Exceed ....................... 17  
   New Features Introduced in Version 5.0 .................................... 18  
   Optional Local Help File Installation ........................................ 19  
   Uninstall Reflection X Advantage ............................................. 19  
      Remove All Reflection X Advantage Files ............................... 20  

3 Getting Started ....................................................................... 21  
   X Manager - Initial Startup ...................................................... 21  
   X Manager for Domains - Initial Startup .................................... 21  
   Launch an X Client Application Using the Sample Definitions ....... 22  
   Make an XDMCP Connection Using the Sample Definitions ......... 24  
   Sample Definitions ................................................................... 25  
   The X Manager Interface .......................................................... 26  
   Reflection X Icons .................................................................... 27  
   Frequently Asked Questions ..................................................... 30  

4 X Manager and X Manager for Domains ................................... 33  
   How to..................................................................................... 33  
      Start X Manager ................................................................. 34  
      Configure an X Client .......................................................... 36  
      Configure a Desktop Connection .......................................... 37  
      Start a Client ........................................................................ 39  
      Stop a Session ....................................................................... 40  
      Organize your Definitions .................................................... 41  
      Sharing and Suspending Sessions ......................................... 41  
      Work with Colors .................................................................. 44  
      Work with Fonts .................................................................... 47  
      Work with Keyboard Maps .................................................... 52  
      Configure Reflection X Advantage to Use Your Local IME ....... 56  
      Export and Import Definitions .............................................. 57  
      Enable or Disable Extensions ............................................... 59  
      Configure Compression ....................................................... 59  
      Set Up Secure Shell (SSH) Connections ................................ 60  
      User Interface Reference ..................................................... 69  
         Import Migrated Settings and Templates dialog box ............. 69  
         Client Definition .............................................................. 70  
         XDMCP Connection Definition ........................................ 85  
         Launch Group Definition .................................................. 86  
         Session Definition ............................................................ 87  
         Offered and Joined Sessions ............................................... 123
## 5 Remote Session Services in Standalone X Manager

- X Manager Basic Session ........................................... 145
- X Manager (Standalone) Distributed Session ..................... 146
- How to Configure a Distributed Session in Standalone Mode ........ 147

## 6 Domain Administration

- Reflection X Advantage Domain Components ...................... 149
- Reflection X Advantage Session Processes ......................... 150
- X Manager for Domains Basic Session ............................ 150
- X Manager for Domains Distributed Session ....................... 151
- Setting up Domain Components ...................................... 153
  - Set Up the Domain Controller ................................... 153
  - Start and Stop the Reflection X Service ......................... 154
  - Set Up an Administrator Workstation ............................ 155
  - Set Up Domain Nodes ............................................. 155
  - Remove a Domain Node ........................................... 156
  - Set Up User Workstations ........................................ 157
- Domain Authentication ................................................. 159
  - How Domain Access is Controlled ................................ 159
  - Configure and Test User Authentication .......................... 160
  - Set Up LDAP Authentication ....................................... 161
  - Set Up Reflection X Advantage Internal Authentication .......... 161
  - Add or Remove Domain Users ..................................... 162
  - Unlock a Domain .................................................. 162
- Sample Domain Configurations ........................................ 163
  - Domain Setup: Improve Performance Over a Slow Network ........ 163
  - Domain Setup: Leave a Session and Rejoin from a Different Computer 165
  - Domain Setup: Centralize Session Configuration .................. 168

## 7 X Administrative Console

- How to ................................................................. 173
  - Start the X Administrative Console ................................ 173
  - Add or Remove Domain Administrators .............................. 174
  - Configure Load Balancing ........................................ 175
  - Raise a Domain Node Priority for Running Sessions .......... 175
  - Stop a Session .................................................... 175
  - Monitor Sessions .................................................. 176
  - Change a User Password .......................................... 176
  - Share Settings with Domain Users ................................ 176
  - Add a Trusted Host Key for all Domain Users .................. 177
  - Import a Trusted Host Key Using the Administrative Console .... 178
- Interface Reference ................................................... 178
  - Domain Composition Tab .......................................... 178
  - Domain Status .................................................... 181
  - Domain Definitions Tab .......................................... 185
  - Authentication Tab ................................................ 188
  - Administrative Console Menus .................................... 189
8 Customizing and Deploying Reflection X Advantage

Deploying Software - Overview .......................................................... 195
Deploying Settings - Overview ......................................................... 196
Using a Response File to Install on UNIX Systems .............................. 198
Deploying Sessions Using a Custom Template .................................... 200
Managing Installations on Windows Workstations ............................... 201
  Performing a Basic Deployment ...................................................... 202
  Performing an Advanced Deployment .............................................. 202
  Install from the Command Line ................................................... 203
  Create an Administrative Installation Point .................................... 204
  Installation Customization Tool ................................................... 205
  Creating and Editing Transforms .................................................. 206
  Creating and Editing Companion Installer Packages ......................... 210
Deploying Sessions with the Administrative WebStation ....................... 212
  Configure Sessions using the Administrative WebStation .................. 213
  Setting up a Session using the Security Proxy ................................. 213
  Managing Upgrades for WebStation Sessions .................................. 215
  Administrative WebStation Mode ............................................... 215
  WebStation User Mode ................................................................ 215
  Save Settings (Administrative WebStation Mode) .............................. 216
  Discard Settings (WebStation User Mode) ....................................... 216

9 Administrator Reference ............................................................... 217

Reflection X Advantage Data Files .................................................... 217
Ports used by Reflection X Advantage ................................................ 218
Feature Guide for Upgrading from Reflection X version 13 or 14 .......... 219
File Access Restrictions for Files With Sensitive Information ................ 222
Changing the JRE ........................................................................ 223
Upgrade Digital Certificates used by Reflection X Advantage Domains .... 226
Command Line Utilities ..................................................................... 227
  rxmgr Command Line - Standalone X Manager ................................. 227
  rxmgrdomains Command Line - X Manager for Domains ................ 229
  rxmigrate Command Line Utility - Migrate Settings ....................... 231
  rxconfig Command Line Utility - Domain Configuration .................. 233
Using PKI Services Manager with Reflection X Advantage .................... 235
  Setting up PKI Services Manager on Windows ................................. 236
  Setting up PKI Services Manager on UNIX .................................... 239
  Configure Reflection X Advantage to Connect to PKI Services Manager ...... 243

10 Troubleshooting .......................................................................... 245

Troubleshooting Tools ....................................................................... 246
  Log Files ................................................................................... 246
  Create a Trace ........................................................................... 247
Application Fails to Start .................................................................... 248
Display Problems ............................................................................ 249
Connection Problems ........................................................................ 250
Performance Problems ....................................................................... 251
Port Conflicts .................................................................................. 251
Domain Logon Problems .................................................................... 251
Domain Node is Unavailable .............................................................. 252
IME Troubleshooting ........................................................................ 252
Key Mapping Problems ...................................................................... 253
Welcome to Reflection X Advantage

Reflection X Advantage is an X server that allows you to view your UNIX desktop and work with X client applications from a remote workstation. Reflection X Advantage provides two modes of operation—Standalone mode and Domain mode.

**Standalone mode** is provided by a single application—X Manager, which is installed by default. For users of earlier Reflection X products, Reflection X Advantage in standalone mode will be familiar territory: a bulletproof X server that provides reliable, seamless access to your mission-critical X applications.

**Domain mode** offers all the functionality of standalone mode and complements that power with additional features that help enhance productivity without increasing costs. Domain mode consists of multiple components—X Manager for Domains, the X Administrative Console, and the Reflection X Service. These features are not installed by default; and different systems within the domain require different components.

Whichever mode you choose, you’ll have access to the following features:

- **Multiple platform support**: Using Reflection X Advantage, users can access X hosts and applications from a broader-than-ever array of desktop environments, including Windows, Linux, Solaris, HP-UX, and AIX.
- **Real-time collaboration**: The session sharing features in Reflection X Advantage allow colleagues to look at the same applications concurrently, and even transfer control of the session from one user to another.
- **Improved performance options**: Using Reflection X Advantage, you can address problems with low bandwidth or high latency connections using remote session services. When you configure distributed Reflection X Advantage sessions, only the protocol required to update the display is sent over the network. This results in dramatically improved performance where high latency is a problem. Where low bandwidth is a problem, Reflection X Advantage automatically compresses the protocol sent to remote X servers.
- **Fully-integrated Secure Shell with FIPS 140-2 validation support**: With Reflection X Advantage, you get a single-vendor security solution that is integrated with the X server.
- **X11 Extension Support**: Reflection X Advantage provides support for key X11 extensions including GLX, Render, Damage, Shape, and XFixes.
- **Native IME support for input of double-byte characters**: Native IME support lets you use your workstation’s input method editor (IME) to compose characters (including Japanese, Korean, and Chinese). The X11 Input Method (XIM) server provided by Reflection X Advantage obtains the composed text from your IME and passes it to XIM-aware clients. This means that you can work with varied X clients without having to learn new input techniques.
- **X.509 certificate authentication**: Secure Shell connections require both user and host authentication. In addition to supporting standard options for user authentication (passwords and public keys), Reflection X Advantage also supports authentication using X.509 certificates. Certificates can be stored in the Reflection X Advantage Store, a local directory, the Windows Certificate Store, or on a Smart card or similar device. Also, by downloading and installing Reflection PKI Services Manager, you can configure Reflection X Advantage to authenticate hosts that present X.509 certificates. Reflection PKI Services Manager is available at no additional charge.
Additional features available in Domain mode include:

- **Centralized session configuration:** Reflection X Advantage domain features can help simplify session setup for end users. Administrators can create and maintain client and session definitions in a single centralized location and provide users with access to these definitions. Users can get started quickly using these centrally configured sessions, and can also create and configure individual sessions on their own workstations.

- **Flexible, instant access to an established session from the office, at home, or on the road:** Leave a running session from one location and rejoin the same session from another location. No time is spent on reestablishing the client connection.

- **Session protection:** When you run a distributed session, you can use fault tolerance to safeguard against losing the session. This option enables you to return to your work exactly where you left it, even after a network or hardware failure.

- **Domain authentication services:** Leverage your current authentication process to provide Reflection X Advantage domain authentication. Use any of these authentication methods: Windows, PAM (Pluggable Authentication Modules), LDAP (Lightweight Directory Access Protocol), and Reflection X Internal.

- **Load balancing:** In a distributed session environment, Reflection X Advantage is installed on more than one computer, and sessions can run on multiple domain nodes. When a user initiates a session, the session is run on the least-loaded domain node.

### Operating Modes: Domain vs. Standalone

Reflection X Advantage can be operated in either "Standalone" or "Domain" mode.

**Standalone mode**

Standalone mode is provided by a single application—X Manager, which is installed by default. In this mode you use one application, **X Manager** to access X hosts and clients, configure and share sessions, and monitor session status — all from your own desktop. For a quick introduction to client and session configuration, see “Getting Started” on page 21.

**Domain mode**

Running Reflection X Advantage in Domain mode provides access to all the features in standalone mode, and also provides access to additional domain services. Domain administrators run the **X Administrative Console** to configure and manage Reflection X domains, and to handle load balancing, optimizing performance for a group of X sessions. Domain users run **X Manager for Domains** to access X hosts and clients. These applications connect to a central domain controller, which runs the Reflection X service and stores session definitions in a shared database. As an authorized domain user, you can start, join, leave, and share a running X session. You can use all public definitions created by administrators, as well as create private definitions available only to you. For information on setting up and configuring a Reflection X Advantage domain, see Reflection X Advantage Domain Administration (page 149).

### Feature comparison

<table>
<thead>
<tr>
<th>Standalone Mode (X Manager)</th>
<th>Domain Mode (X Manager for Domains)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch and interact with an X client application</td>
<td>x</td>
</tr>
</tbody>
</table>
The X Window System

The X Window System is a portable, multi-user graphical window system originally developed at MIT. "Portable" means that it can run on many types of host computers (including OpenVMS and a variety of Linux and UNIX hosts). "Multi-user" means that many users can have simultaneous access to X applications by connecting to the host over a network. As a window system, X allows users to run several applications at one time, each in its own window (similar to Microsoft Windows).

X applications (clients) provide the graphical user interface for many host-based environments — a few well-known environments are the GNOME Desktop Environment (GDE), the K Desktop Environment (KDE), and the Common Desktop Environment (CDE). X applications are also commonly developed for engineering, scientific, and manufacturing purposes.

The X Window System is based on a client/server model:

- The X "client" is an application program that runs on a host computer.
- The X display "server" is the intermediary software between the client application programs and the local display hardware and input devices (mouse and keyboard). The server tracks all input from these devices and conveys it to the relevant client applications.

  The server also responds to client requests for output, and updates the display to reflect the output. In Reflection X Advantage the display and the X server have been decoupled.

This division in the X Window System architecture allows the clients and the display server to reside on different types of computers. The client applications reside on UNIX hosts while the server runs on the local computer. With Reflection X Advantage this can be a Windows or UNIX computer.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Standalone Mode (X Manager)</th>
<th>Domain Mode (X Manager for Domains)</th>
</tr>
</thead>
<tbody>
<tr>
<td>XDMCP</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>X session sharing</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>X11 Extensions support</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Improved performance over slow networks</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Integrated Secure Shell</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>FIPS 140-2 support</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>X.509 certificate authentication</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Native IME support</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Centralized configuration of settings</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Leave and rejoin X sessions</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Fault tolerance for X sessions</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Domain authentication services</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Load balancing</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Because the X display server runs on a local computer, client/server terminology often seems reversed to people new to the X Window System. As a display server, the local computer provides the services of the local display, keyboard, and mouse to applications (clients) running on other computers.

**Requests, Replies, Events, and Errors**

The X server and X client applications communicate by the following means:

- Requests from clients to the server.
- Replies from the server to clients, in response to client requests.
- Events to be delivered to any clients that have registered to receive events.
  
  An event occurs when there is user input (the mouse is moved, or a key is pressed), or other information sent from the display server to the client application. After a client application receives a meaningful event, it may respond with more requests to the server for some sort of action affecting the display.
- Errors to be delivered to clients when a request fails, or is invalid.
Reflection X Advantage can be installed on Windows or UNIX systems. On Windows systems, it is installed as part of suite products which install Reflection X Advantage with additional applications. The UNIX installers install just Reflection X Advantage. In a distributed environment, you can install on either or both operating systems.

In this Chapter

- System Requirements (page 11)
- Install Reflection X Advantage on Windows (page 11)
- Install on UNIX (page 13)
- Which Reflection X Advantage Features Should I install? (page 14)
- Upgrade and Migration (page 15)
- New Features Introduced in Version 5.0 (page 18)
- Optional Local Help File Installation (page 19)
- Uninstall Reflection X Advantage (page 19)

System Requirements

System requirements information is available from the Micro Focus Technical Library.

- For information about supported platforms and additional system requirements, see Technical Note 2704 (http://support.attachmate.com/techdocs/2704.html).
- For updates about security issues related to Reflection X Advantage, see Technical Note 2505 (http://support.attachmate.com/techdocs/2505.html).

Install Reflection X Advantage on Windows

Reflection X Advantage is included as a component in Reflection X Desktop and Reflection Pro Desktop.

The following applications are installed by default:

- X Manager
  Provides complete support for connecting to X clients in standalone mode.
- Reflection Workspace
  Provides access to VT terminal sessions. With Reflection Pro Desktop, IBM terminal and printer support is also included.
- Reflection FTP Client
  Supports file transfer using both FTP and SFTP protocols.
A 64-bit installer is available for installing Reflection X Desktop and Reflection Pro Desktop on 64-bit Windows platforms. This installer includes 64-bit Reflection X Advantage and 32-bit Reflection Workspace and Reflection FTP client. (The 32-bit applications are supported on 64-bit platforms.) Legacy Reflection X is not included with the 64-bit installer.

If you are planning on running Reflection X Advantage in domain mode, you will need to install additional features on the computers running in your domain. These features are not installed by default. For a summary of some typical installation configurations for domain mode, see “Which Reflection X Advantage Features Should I install?” on page 14 For more detailed information, see “Setting up Domain Components” on page 153.

To install on Windows

1. Log on using a Windows account with administrator privileges.
2. Start the Setup program (Setup.exe). If you are installing from the download site, the following steps start this program:
   2a. From the download site, click the Windows download link and run the download program.
   2b. Select a location for the installer files, and then click Next. This extracts the files to the specified location and starts the Setup program.
3. The installer checks your system for required software prerequisites. If these are not present, the installer installs these packages before running the product installation.
4. To view and/or modify which features are installed, click the Feature Selection tab.

Installation Log File

An installation log file is created by default, but this file is deleted if the installation succeeds. If your installation does not succeed, you can use the log file to troubleshoot. The log file is saved to your temp directory with a generated name that begins with atm. To open this folder, enter %tmp% in the Start menu's "Search programs and files" text box or in the path box of a Windows Explorer window.

Associated Installers

When you install Reflection X Advantage on Windows, some features are installed using associated installers that run automatically as needed.

NOTE: If you install from a command line using setup.exe, prerequisite packages are installed automatically. If you install using msiexec.exe, prerequisite packages are not installed automatically. For details, see “Install from the Command Line” on page 203.

Java JRE Installation

All Reflection X Advantage features require Java, and the Java Runtime Environment (JRE) feature is selected by default. When this feature is selected, the associated installer installs a JRE that is correctly configured to fully support all Reflection X Advantage features. Micro Focus will supply updated Java installation packages as needed to provide customers with Java security updates. These packages can be downloaded and applied independently of any updates you apply to the main installer package. The JRE installed with Reflection X Advantage is uninstalled automatically when you uninstall Reflection X Advantage.

It is also possible to configure Reflection X Advantage to use a different JRE. For details about how to configure a non-default JRE, see “Changing the JRE” on page 223.
NOTE: The Micro Focus Java installer adds a separate entry in the Windows Programs and Features Control Panel. Uninstalling the Reflection program automatically uninstalls the Micro Focus Java entry if it is no longer being used by any application. If you uninstall using an msiexec command line, you need to uninstall the Java program as a separate step.

Microsoft .NET 4 Installation

All Reflection Workspace features require Microsoft .NET 4 to be installed on your system. If it is not on your system and you install Reflection X Desktop or Reflection Pro Desktop using the defaults (or include any Reflection Workspace features), Microsoft .NET Framework 4 Setup program is installed and started after the Reflection X Advantage installation completes. You must accept the Microsoft license agreement to complete this installation.

Microsoft .NET is a shared component and is not uninstalled when you uninstall Reflection. To uninstall Microsoft .NET, use the Windows Programs and Features Control Panel and uninstall each of the Microsoft .NET Framework 4 items.

If you are an administrator, you can use “Installation Customization Tool” on page 205 to configure a silent install that includes the Microsoft .NET installation without displaying the Microsoft .NET Setup user interface. If you create a transform that sets the user interface level to None, the Microsoft .NET Setup user interface is not displayed. If the user interface level is either Basic or Full, the Microsoft .NET setup user interface is displayed.

Visual Basic for Applications Installation

The Visual Basic for Applications feature is available with the Reflection Workspace emulators. Installations that include this feature install Microsoft VBA 6.5. Visual Basic for Applications is a shared component and is not uninstalled when you uninstall Reflection X Advantage.

Install on UNIX

Use this procedure below to install Reflection X Advantage on UNIX or Linux systems.

X Manager is installed by default. This application provides complete support for connecting to X clients in standalone mode. If you are planning on running Reflection X Advantage in domain mode, you will need to install additional features on the computers running in your domain. These features are not installed by default. For a summary of some typical installation configurations for domain mode, see “Which Reflection X Advantage Features Should I install?” on page 14 For more detailed information, see “Setting up Domain Components” on page 153.

NOTE: UNIX installers do not include the emulators and FTP Client, which are only available when you install on Windows.

To install Reflection X Advantage on UNIX systems

1. Download the installation package for your UNIX operating system from the download site.

   NOTE: The download files (*.zip) for each supported UNIX system include both 32-bit and 64-bit installers if both platforms are available.

2. Unzip the download file; for example:

   unzip -d rx-advantage-5.0.0.999-prod-linux.zip
The expanded download file contains binary files (*.bin) for installing on different platforms. Locate the appropriate file for your UNIX platform. The product installation package name begins with "rxa-5.n.n.nnn."

The package name that begins with "rxa_help-5.n.n.nnn installs local help files. Installing these files is optional. By default, Reflection X Advantage uses product Help located on the website. For more information, see “Optional Local Help File Installation” on page 19.

3 If you unzipped on a Windows computer, copy the installation file for your platform to your UNIX computer.

4 Log on as root and navigate to the directory that contains the installation file.

5 Change the permissions of the installation package to give execute permissions to the file owner. For example:

   chmod 744 rxa-5.0.0.999-prod-x86_84-linux.bin

6 Start the installation program. For example:

   ./rxa-5.0.999-prod-x86_84-linux.bin

   **NOTE:** The command above launches the InstallAnywhere installation program which requires an X11 Windows display. To initiate a command line installation, you can add the parameters -i console. For example:

   ./rxa-5.0.999-prod-x86_84-linux.bin -i console

7 You can modify the feature selections during the install. X Manager is installed by default.

   **NOTE:** If you are using the -i console option, you'll have an opportunity to specify which features you want to install by entering a comma-separated list in response to the prompt: "Please choose the Features to be installed by this installer: To install all features, you can type 1,1. For additional command line options, see Using a Response File to Install on UNIX Workstations (page 198).

### Installation Log File

On UNIX systems, an install log is created here: /opt/rxadvantage/<product_name>_InstallLog.log.

### Which Reflection X Advantage Features Should I install?

X Manager (standalone) is installed by default. If you plan on configuring a Reflection X Advantage domain, you need to install additional features. The following tables summarize some typical installation configurations.

- You can install and use any combination of Reflection X Advantage features on a single computer. The following table provides guidelines, but you are not limited to these configurations. For example, you may want to install and run both X Manager (standalone) and X Manager for Domains on the same computer.
A Java Runtime Environment (JRE) is required for all Reflection X Advantage applications and services. On UNIX systems this is always included as part of the installation. On Windows systems the JRE is listed as a separate feature in the installer. Include this feature with all installations unless you have installed and configured an alternate JRE (page 223).

The Template feature provides sample settings to help you get started. This feature is not required, but is recommended unless your administrator has customized your installation to provide custom settings for your environment.

### Standalone mode

- **Standalone user workstation**: X Manager, Templates
- **Optional remote session service node (page 146)**: Remote Session Services

**Java Runtime Environment (JRE)** (on Windows)

Review these guidelines if you are planning to run in **domain mode** (page 149).

### Domain mode

- **Domain user workstation**: X Manager for Domains, Templates
- **Domain administrator's workstation**: X Manager for Domains, X Administrative Console, Templates
- **Domain controller**: X Administrative Console, Domain Services, Domain Controller
- **Domain node**: Domain Services (without the domain controller), Java Runtime Environment (JRE) (on Windows)

**Java Runtime Environment (JRE)** (on Windows)

### Related Topics

- “Remote Session Services in Standalone X Manager” on page 145
- “Domain Administration” on page 149
- “Associated Installers” on page 12

### Upgrade and Migration

In this Section

- “Upgrading from Earlier Versions of Reflection X Advantage” on page 16
- “Upgrading from Reflection X version 13 or 14” on page 17
- “Migrating Settings From Hummingbird Exceed” on page 17
Upgrading from Earlier Versions of Reflection X Advantage

If you are upgrading from an earlier version of Reflection X Advantage (or any product that includes Reflection X Advantage as a feature), note the following:

- You can run the new installer with an installed version in place. The earlier version is uninstalled as part of the installation process. Your existing settings are saved and used automatically after the upgrade.

- Changes made in version 5.0 make it easier to configure and start sessions. Prior to version 5.0, there were three definition types: server, session and client. Before you could start your client, you needed to start a session, which in turn started a server and optional clients. In version 5.0, server settings have been incorporated into the session settings, and starting a client automatically starts an associated session. If you haven't defined an associated session, you are prompted at client startup to choose one. Your existing settings are updated automatically to work correctly – just double-click your migrated X client or XDMCP definitions to get started. For more information, see New Features Introduced in Version 5.0 (page 18).

- Your database files are migrated automatically to the current version the first time Reflection X Advantage is started.

- If you use the Remote Session Services feature to configure distributed sessions with the standalone X Manager, you must upgrade all components at the same time. This feature does not support mixed versions.

- If you distribute sessions using the Reflection Administrative WebStation (page 212), review the information in Managing Upgrades for WebStation Sessions. (page 215)

Upgrading Reflection X Advantage Domains

If you are upgrading from version 5.0 or later, you can upgrade domain components in stages:

1. Upgrade all systems running X Manager for Domains and the X Administrative Console before you upgrade the domain controller. These components are backward compatible, not forward compatible.
   These components will be able to connect to your (older) domain controller and will run using the version that is running on that domain controller. This means that features or bug fixes in the newer version will not yet be available.

2. Upgrade your domain controller and any configured domain nodes after all other computers in the domain have been upgraded.
   After the domain controller is upgraded, all domain components will run using the newer version; at this time the latest features and bug fixes become available to the upgraded systems running X Manager for Domains and the X Administrative Console.

What Reflection X Advantage version am I running?

For version information, go to Help > About X Manager. The information displayed always shows the currently installed version. If you are connected to an older domain controller, the display also shows the current running version. On Windows, Reflection X Advantage is installed as a feature in Reflection 2014 installers, and this information is also included.
Upgrading from Reflection X version 13 or 14

The first time you start Reflection X Advantage (either X Manager or X Manager for Domains), local settings from Reflection X version 13 or 14 are migrated automatically and saved to a Reflection X Advantage “definition file” on page 255. On this first start-up, the Import Migrated Settings and Templates dialog box opens and includes an option to import your migrated settings. This option is selected by default. Click Import to add these settings to Reflection X Advantage. Your existing Reflection X settings are not changed.

- To launch an X client or XDMCP connection, double-click the client name. Or, select a client, then click the start button:

You prior version server settings are migrated to a session definition named “config,” which is configured to start automatically when you start X Manager. If you created any additional X Server instances, these settings are migrated using the name you provided.

See “Feature Guide for Upgrading from Reflection X version 13 or 14” on page 219 for help finding features in Reflection X Advantage.

The Import Migrated Settings and Templates dialog box displays only once, but it is possible to import settings later if you do not import them on initial startup.

You can also migrate settings manually using the rxmigrate (page 231) command line utility. This is useful if you have configured settings in a shared network location; these settings are not migrated automatically.

Migrating Settings From Hummingbird Exceed

The first time that you start Reflection X Advantage (either X Manager or X Manager for Domains), local settings from Hummingbird Exceed products (versions 9.0 and higher) are migrated automatically and saved to a Reflection X Advantage “definition file” on page 255. On this first start-up, the Import Migrated Settings and Templates dialog box opens and includes an option to import your migrated settings. This option is selected by default. Click Import to add these settings to Reflection X Advantage. Your existing Hummingbird files are not changed.

- To launch an X client or XDMCP connection, double-click the client name. Or, select a client, then click the start button:

The Import Migrated Settings and Templates dialog box displays only once, but it is possible to manually import migrated settings later if you do not import them on initial startup.

You can also migrate settings manually using the rxmigrate (page 231) command line utility. This is useful if you have configured settings in a shared network location; these settings are not migrated automatically.
New Features Introduced in Version 5.0

Version 5.0 of Reflection X Advantage introduced many changes that make it easier to use and administer than earlier versions.

Easier to start clients

- To get connected, just double click on any definition under X Clients, XDMCP Connections, or Launch Groups. Clients now start sessions automatically, so you no longer need to start by launching a session first.
- New Automatically start options are available for all definition types. These enable you to create configurations that start automatically when you start Reflection X Advantage.
- The new Launch Groups option enables you to start multiple clients together.

Easier to configure

- New default settings are included that make it easier to establish your first connections.
- New templates provide sample definitions for connecting to different host types.
- There is no longer a separate X server definition category. All server settings are now incorporated into the session definition.
- Session definitions now use a tabbed interface that makes it easier to locate the settings you need.
- A new XDMCP Connections category makes it easier to configure this session type.

Easier to organize

- New options are available to help you organize your definition lists. You can now drag and drop definitions within the list. Or, use the new sorting button to alphabetize the list.

Easier to upgrade from legacy Reflection X

- Your Reflection X 13 and 14.settings are imported automatically and now work the same way they did in those earlier versions. All you need to do to get connected is double-click the imported X client and XDMCP definitions.
- The Reflection X server, named config in versions 13 and 14, is migrated to a session named config. As it did in the prior versions, this server now runs automatically when you start Reflection X Advantage.

Easier to administer

- Create custom templates that are automatically available to users the first time they start X Manager or X Manager for Domains.
- Use a new command-line option to launch Reflection X Advantage in slimmed-down mode that enables users to see and use the definitions you have provided without allowing access to features for editing settings.
Optional Local Help File Installation

By default, Reflection X Advantage opens product help from the web. If you prefer to use locally installed help files on Windows systems, you need to run a separate Help installer after you install the product installation.

- For Windows systems, you will need to download the Help installer from the product download site. Select either the 32-bit or 64-bit installer to match the option you used for your product installation.
- For UNIX systems, the Help installation package is included with the product download for your UNIX operating system.

After you install the local help files, you need to configure each installed Reflection X Advantage application to use the installed help system.

- Go to File > Preferences in X Manager, X Manager for Domains, or X Administrative Console to configure your help preference for that application.

If the help system you specify is not available, Reflection X Advantage will automatically attempt to use the other option.

Uninstall Reflection X Advantage

**NOTE:** These procedures uninstall the Reflection X Advantage application. Reflection X Advantage databases, which contain your configuration information, are not removed.

**To uninstall on Windows**

1. Log on as an administrator.
2. From the Windows Control Panel, open Programs and Features (or Windows Add or Remove Programs, depending on your version of Windows.)
3. Select Micro Focus Reflection X Advantage, click Uninstall (or Remove).

**To uninstall on UNIX**

1. Log on as root.
2. Open a terminal window and navigate to the Uninstall_rxadvantage directory, which is located in the Reflection X Advantage installation directory. The default location is:

   /opt/rxadvantage/Uninstall_rxadvantage

3. Enter the following command to initiate the uninstall and follow the uninstaller instructions.

   ./Uninstall_rxadvantage

**NOTE:** The command above launches the InstallAnywhere installation program which requires an X11 Windows display. To initiate a command line uninstall, you can add the parameters -i console as shown here:

   ./Uninstall_rxadvantage -i console
Remove All Reflection X Advantage Files

Uninstalling Reflection X Advantage does not remove its associated files and directories. Use these procedures to remove all associated files and directories.

To remove files from a Windows installation

1. In the %ALLUSERSPROFILE% (page 258) folder, remove the .attachmate folder and all of its subfolders.

   NOTE: This folder contains the database and logs used by X Manager for Domains.

2. In the %USERPROFILE% (page 258) folder of any user who has configured X Manager, remove the .attachmate folder and all of its subfolders.

   NOTE: This folder contains the database and logs used by X Manager.

To remove files from a UNIX installation

1. Delete the installation directory. The default location is:
   /opt/rxadvantage
   For example, navigate to the opt folder and enter:
   rm -fr rxadvantage

   NOTE: The db and logs subdirectories of the installation directory contain the database and logs used by X Manager for Domains.

2. Navigate to the home directory of any user who has configured X Manager and remove the .attachmate directory and all of its subdirectories:
   rm -fr .attachmate

   NOTE: The .attachmate directory located in the user’s home directory contains the database and logs used by X Manager.
Getting Started

In this Chapter

- “X Manager - Initial Startup” on page 21
- “X Manager for Domains - Initial Startup” on page 21
- “Launch an X Client Application Using the Sample Definitions” on page 22
- “Make an XDMCP Connection Using the Sample Definitions” on page 24
- “Sample Definitions” on page 25
- “The X Manager Interface” on page 26
- “Reflection X Icons” on page 27
- “Frequently Asked Questions” on page 30

X Manager - Initial Startup

This procedure describes what you see the first time you run the standalone X Manager. See “X Manager for Domains - Initial Startup” on page 21 if you run in domain mode.

Before you begin

- Install Reflection X Advantage using defaults. (This includes the X Manager and Templates features).

To start X Manager and import templates and migrated settings

1. Start X Manager. (On Windows, go to Start > All Programs > Micro Focus Reflection > X Manager.)

   The first time you run X Manager, the **Import Migrated Settings and Templates** dialog box opens. This dialog box includes a list of sample connection settings for different host types. Migrated settings are also listed if you are running on a system with local settings used by earlier Reflection X products (typically version 13 or 14), or Hummingbird Exceed. (This dialog box does not open if you are upgrading from an earlier version of Reflection X Advantage.

2. Do one of the following:
   - Select the settings you want to import and click **Import**. This imports the selected settings plus a set of default sample definitions.
   - Click **Cancel**. When you cancel, Reflection X Advantage does not import any of the listed settings, but does import the default sample definitions.

X Manager for Domains - Initial Startup

Use this procedure to get started with X Manager for Domains running on a Windows system. See “X Manager - Initial Startup” on page 21 if you run in standalone mode (which is the default).
NOTE: This procedure assumes that a Reflection X Advantage domain has already been setup by an administrator. For information about setting up a domain, see Reflection X Advantage Domain Administration (page 149).

Before you begin

- Obtain your Reflection X Advantage domain name and logon credentials from your administrator. (In most cases your username and password are the same as those you use to log onto the system running X Manager for Domains.)
- Install X Manager for Domains. (This is not installed by default when you install Reflection X Advantage.)

To start X Manager for Domains and import templates and migrated settings

1. Start X Manager for Domains. (On Windows, go to Start > All Programs > Micro Focus Reflection > X Manager for Domains.)
2. In the domain logon dialog box:
   - For **User name** and **Password**, enter your logon credentials (either the username and password you use to start your system, or the credentials provided by the Reflection X Advantage administrator.)
   - For **Domain**, enter the domain name you received from your administrator. (After your first successful logon, this name is entered automatically for you.)
3. Depending on how your domain is configured, you may see the **Import Migrated Settings and Templates** dialog box. If you see this dialog box, you can use it to select optional sample settings for import. Do one of the following:
   - Select the settings you want to import and click **Import**. This imports the selected settings plus any available default definitions.
   - Click **Cancel**. When you cancel, Reflection X Advantage does not import any of the listed settings, but does import the default definitions.

When X Manager for Domains opens, the list of settings available under **My Definitions** may include any of the following:

- Default definitions that were imported automatically.
- Custom definitions that were imported automatically. (These can be configured in templates created by an administrator and added to a customized installer.)
- Connection settings and migrated definitions that you selected in the **Import Migrated Settings and Templates** dialog box.
- Public definitions that have been created and shared by your administrator. These definitions are read-only and are identified with a different icon (page 27).

Launch an X Client Application Using the Sample Definitions

Reflection X Advantage installs several “Sample Definitions” on page 25 by default. In many cases you can get connected without making any changes to these sample settings. You can then use the samples as a model for making additional connections.

To connect using a sample X client definition

1. Start X Manager or X Manager for Domains.
2 Under X Clients on the left, select one of the sample definitions. You can use the generic "xterm" definition. Or, if you imported templates for your host type, select one of these (such as "Linux - xterm" or "VMS - DECterm"). Connect using any of these methods:

- Double-click the definition name.
- Select the definition, then in the toolbar click Start.
- Right-click the definition name and click Start.

3 Enter your host and user name in reply to the prompt.

If the host is available and supports Secure Shell connections, you see the Host Key Unknown message the first time you connect. Click Always to trust the host key. Reflection X Advantage saves this key and uses it in subsequent connections to confirm that you're connecting to the correct host.

4 Enter your password in response to the prompt.

If your connection is successful, a window opens on your desktop showing your host command prompt.

You can clone the sample client definition to create a duplicate copy. By cloning a definition, you create a new definition with the same settings and preserve the original definition to use as a reference. To clone a definition:

- Right-click the client definition and select Clone Client.

You can edit the cloned definition. Changes are saved automatically as you work. For example:

- Enter values for Host name and User name.
- Change the value of Host type. This changes the list of sample commands available to you.
- Edit the Command to start a different X client application. Use the drop-down arrow to view sample commands that typically work for the host type you selected.
- For more information about client commands, see “Configure an X Client” on page 36.

Troubleshooting

If you don't see sample definitions listed under X Clients:

- When you upgrade from a previous version of Reflection X Advantage, no changes are made to your existing settings. This means that after an upgrade, the sample definitions are not imported, even if the correct template is installed. You can use the File > Import command to manually import templates. Look for installed templates in the templates subfolder in the installation folder, typically:

  C:\Program Files\Micro Focus\Reflection\templates

- For help creating a new definition without using the sample definitions, see “Configure an X Client” on page 36.

If you're unable to make a connection using one of the sample definitions:

- Look at the status bar at the bottom of the X Manager window for information. For additional information about each error, click the information button, 🔄.
- Error messages remain in the status bar. Click the delete button, 🗑, to clear messages between tests.

Here are a few common errors.
Make an XDMCP Connection Using the Sample Definitions

Reflection X Advantage installs several “Sample Definitions” on page 25 by default. In many cases you can get connected without making any changes to these sample settings, then use the sample as a model for making additional connections. This procedure makes an XDMCP connection using the sample ‘Direct connection’ definition.

NOTE: XDMCP must be enabled on your UNIX host.

To connect using the sample XDMCP connection

1. Start X Manager or X Manager for Domains.
2. Under XDMCP Connections on the left, locate the sample definition called “Direct connection” and connect using any of these methods:
   - Double-click the definition name.
   - Select the definition, then in the toolbar click Start.
   - Right-click the definition name and click Start.
3. Enter your host name in reply to the prompt.
   - If the connection is successful, an X terminal desktop window opens showing your host login screen.
4. Enter your login credentials for the host.

You can clone the sample “Direct connection” XDMCP definition to create a duplicate copy. By cloning a definition, you create a new definition with the same settings and preserve the original definition to use as a reference. To clone the definition:
   - Right-click the client definition and select Clone XDMCP connection.
You can edit the cloned definition. Changes are saved automatically as you work. For example:

- Use **Name** to specify a descriptive name for your connection.
- Enter a value for **Host name** to connect to the same host each time. Or, change **Type** to **Broadcast** to see a list of available hosts based on a broadcast sent to the address (or addresses) you configure.

**Troubleshooting**

If “Direct connection” isn’t listed under **XDMCP Connections**:

- When you upgrade from a previous version of Reflection X Advantage, no changes are made to your existing settings. This means that after an upgrade, the sample definitions are not imported, even if the correct template is installed. You can use the **File > Import** command to manually import the template called `generic_templates.rxd`.

If you’re unable to make a connection using the “Direct connection” definition:

- If you see a message saying Unknown host: <hostname>, the host name you specified isn’t reachable. Check your entry or try specifying a host IP address instead of using the host name.
- If the X terminal desktop window opens and is followed by an XDMCP timeout message, XDMCP may not be configured on the host. On some networks, you can see a list of hosts that support XDMCP by changing **Type** to **Broadcast**. Or, try configuring a desktop connection using an X Client command rather than using XDMCP.

**Sample Definitions**

The sample definitions described below are imported automatically the first time you start X Manager or X Manager for Domains. In addition to these default definitions, you may see additional samples if you imported templates when you first started X Manager or X Manager for Domains.

<table>
<thead>
<tr>
<th>Definition Name</th>
<th>Description</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>xterm</td>
<td>Prompts you for host and user information, and sends an <code>xterm</code> command to this host. If the command is successful, you see a terminal session on your desktop.</td>
<td>This client starts the &quot;My desktop&quot; session. The sample command requires the xterm command to be in the path on your host. If this command fails, try changing the <strong>Host type</strong> to match your system, then select xterm from the <strong>Command</strong> drop-down list.</td>
</tr>
<tr>
<td>Direct connection</td>
<td>Prompts you for a host name and starts an XDMCP connection to this host.</td>
<td>This client automatically starts the &quot;X terminal desktop&quot; session. XDMCP must be enabled on the host. Try changing <strong>Type</strong> to <strong>Broadcast</strong>. In some networks, this displays a list of hosts available for XDMCP connections.</td>
</tr>
<tr>
<td>X terminal desktop</td>
<td>Starts an X server configured to display clients within an X terminal window on your desktop.</td>
<td>This session uses all default settings. Use this session for XDMCP connections and X client definitions that launch a desktop environment (such as KDE, CDE or GNOME).</td>
</tr>
<tr>
<td>My desktop</td>
<td>Starts an X server configured to display clients in separate windows on your desktop.</td>
<td>This session enables <strong>Show clients on my desktop</strong>. All other settings use defaults.</td>
</tr>
</tbody>
</table>
In some cases you may not see these definitions:

- The definitions listed above are imported automatically from a generic settings template (generic_templates.rxd), which is installed by default. If this template isn't installed, you won't see these settings.
- If you upgraded from a previous version of Reflection X Advantage, no changes are made to your existing settings. This means that after an upgrade, these definitions are not imported even if the correct template is installed. You can use File > Import to manually import the template called generic_templates.rxd. This template is located in a folder called templates in your product installation folder.
- Administrators can customize the installed templates. If your administrator has customized your installation, you may see different default definitions.

**The X Manager Interface**

The X Manager interface includes a navigation pane on the left, and a definition pane on the right.

**Navigation pane**

As you work with the navigation pane, you can:

- Click a definition to view and/or modify its settings in the definition pane on the right.
- Right-click a definition to display a menu of available actions.
- Select a definition and move it using the up \(\uparrow\) and down \(\downarrow\) arrow icons next to the section title.
- Drag and drop a definition to move it within a section.
- Drag an X client or XDMCP definition onto a session definition to start it with that session.
- Drag an X client or XDMCP definition onto a launch group definition to add it to that launch group.
- Sort definitions in a section alphabetically using the sort icon \(\ \uparrow\downarrow\).\n- Show and hide sections using the expand \(\Box\) and contract \(\Box\) icons.
- Hide sections, or change the order in which they appear, using File > Preferences > Section Visibility.
As you work in the definition pane, note the following:

- As you make edits, observe that there are no **OK** or **Apply** buttons — your changes are automatically saved.
- You can edit the sample definitions and any additional definitions you have created. If you are running X Manager for Domains, you may also see public definitions created by an administrator and shared to domain users. You cannot edit these definitions.
- Running sessions appear under the session definition. Click on a running session to view session status information in the definition pane.
- Changes you make to a session definition while a session is running do not take effect until the session is stopped and restarted.
- Hover over a setting to view a tooltip with information about that setting. For additional information about the current definition pane, click the help icon.

## Definition pane

As you work in the definition pane, note the following:

- As you make edits, observe that there are no **OK** or **Apply** buttons — your changes are automatically saved.
- You can edit the sample definitions and any additional definitions you have created. If you are running X Manager for Domains, you may also see public definitions created by an administrator and shared to domain users. You cannot edit these definitions.
- Running sessions appear under the session definition. Click on a running session to view session status information in the definition pane.
- Changes you make to a session definition while a session is running do not take effect until the session is stopped and restarted.
- Hover over a setting to view a tooltip with information about that setting. For additional information about the current definition pane, click the help icon.

## Reflection X Icons

The icons displayed in the left panel of X Manager show the status of the X Manager components available to you.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Create</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete the currently selected definition</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="image" alt="Move up" /></td>
<td><strong>Move up</strong>&lt;br&gt;Move selected definition up in the section.</td>
</tr>
<tr>
<td><img src="image" alt="Move down" /></td>
<td><strong>Move down</strong>&lt;br&gt;Move selected definition down in the section.</td>
</tr>
<tr>
<td><img src="image" alt="Sort alphabetically" /></td>
<td><strong>Sort alphabetically</strong>&lt;br&gt;Sort the items alphabetically in a section of the navigation pane.</td>
</tr>
<tr>
<td><img src="image" alt="Hide" /></td>
<td><strong>Hide</strong>&lt;br&gt;Hide a section of the navigation pane.</td>
</tr>
<tr>
<td><img src="image" alt="Expand" /></td>
<td><strong>Expand</strong>&lt;br&gt;Expand a section of the navigation pane.</td>
</tr>
<tr>
<td><img src="image" alt="X client definition" /></td>
<td><strong>X client definition</strong>&lt;br&gt;Configuration settings for starting an X client application.</td>
</tr>
<tr>
<td><img src="image" alt="Public X client definition" /></td>
<td><strong>Public X client definition</strong>&lt;br&gt;(domain mode only) X client definition created by the administrator, and available to all users in the domain. Only the administrator can modify the settings in this shared definition.</td>
</tr>
<tr>
<td><img src="image" alt="XDMCP definition" /></td>
<td><strong>XDMCP definition</strong>&lt;br&gt;Configuration settings for making an XDMCP connection.</td>
</tr>
<tr>
<td><img src="image" alt="Public XDMCP definition" /></td>
<td><strong>Public XDMCP definition</strong>&lt;br&gt;(domain mode only) XDMCP connection definition created by the administrator, and available to all users in the domain. Only the administrator can modify the settings in this shared definition.</td>
</tr>
<tr>
<td><img src="image" alt="Launch group definition" /></td>
<td><strong>Launch group definition</strong>&lt;br&gt;List of X Client and/or XDMCP definitions to launch as a group.</td>
</tr>
<tr>
<td><img src="image" alt="Public launch group definition" /></td>
<td><strong>Public launch group definition</strong>&lt;br&gt;(domain mode only) A launch group definition created by the administrator, and available to all users in the domain. Only the administrator can modify the items in this list.</td>
</tr>
<tr>
<td><img src="image" alt="Session definition" /></td>
<td><strong>Session definition</strong>&lt;br&gt;Configuration settings for a session.</td>
</tr>
<tr>
<td><img src="image" alt="Public session definition" /></td>
<td><strong>Public session definition</strong>&lt;br&gt;(domain mode only) Session definition created by the administrator, and available to all users in the domain. Only the administrator can modify the settings in this shared definition.</td>
</tr>
<tr>
<td><img src="image" alt="Running session that is being viewed" /></td>
<td><strong>Running session that is being viewed</strong>&lt;br&gt;The session has been started, and is currently being viewed on this computer.</td>
</tr>
<tr>
<td><img src="image" alt="Running session that is not being viewed" /></td>
<td><strong>Running session that is not being viewed</strong>&lt;br&gt;The session has been started, but is not currently being viewed on this computer.</td>
</tr>
</tbody>
</table>
When working with Fonts, Secure Shell Keys, and Color Schemes, the following icons display:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Trashcan" /></td>
<td>Trashcan</td>
</tr>
</tbody>
</table>

Find the trashcan icon in the toolbar. If the trashcan is full (as shown here) there are one or more definitions available in the trashcan that you can still restore. Click the icon to open the **Definition Trashcan** dialog box and restore a deleted definition.

The following icons appear in the X Administrative Console.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="User key" /></td>
<td>User key</td>
</tr>
<tr>
<td><img src="image" alt="Trusted host key" /></td>
<td>Trusted host key</td>
</tr>
<tr>
<td><img src="image" alt="Public trusted host key" /></td>
<td>Public trusted host key</td>
</tr>
<tr>
<td><img src="image" alt="Font collection" /></td>
<td>Font collection</td>
</tr>
<tr>
<td><img src="image" alt="Public font collection" /></td>
<td>Public font collection</td>
</tr>
<tr>
<td><img src="image" alt="Color scheme" /></td>
<td>Color scheme</td>
</tr>
<tr>
<td><img src="image" alt="Public color scheme" /></td>
<td>Public color scheme</td>
</tr>
<tr>
<td><img src="image" alt="Keyboard map" /></td>
<td>Keyboard map</td>
</tr>
<tr>
<td><img src="image" alt="Public keyboard map" /></td>
<td>Public keyboard map</td>
</tr>
</tbody>
</table>

Available from the **Authentication** pane when **Authentication system** is set to Internal.

Registered node (online) On the Domain Composition pane. Indicates that the listed domain node is online.

Registered node (not online) On the Domain Composition pane. Indicates that the listed node is not available.
Frequently Asked Questions

How do I start my X client?

You can use the default sample definitions to help you get started. See "Launch an X Client Application Using the Sample Definitions" on page 22. Once you have a client definition, there are a variety of ways to start the client from X Manager and X Manager for Domains: double-click the definition, select the definition and click the start arrow on the toolbar, right-click the definition and select Start, or use the Action >> Start on the menu. If the client does not have a default session configured, you'll be prompted to select a session. You can also use shortcuts and command-line options to start clients.

I see "Client failed to connect to the X server" when I try to make a connection. How can I troubleshoot this problem?

If you see this message in the status bar it means that Reflection X Advantage was able to connect to your host, but that the command specified to launch the client isn't valid on your host. This can mean that the X client application isn't in the directory path given, or that it isn't available on your host. The Command box in the Client Definition pane includes a drop-down list of sample commands. The list of sample commands changes based on the current value for Host type. If Host type is set to Generic UNIX, change it to match your host type and try other sample commands. To launch an X client that isn't in the list determine the correct path to your client application and edit this portion of one of the sample commands.

Starting a client changed in version 5.0. What has changed? Will settings I created with an earlier version still work?

Changes made in version 5.0 make it easier to configure and start sessions. You can now use your client definitions to start an X server and connect to your host. Your existing settings are updated automatically to work correctly – just double-click your migrated X client or XDMCP definitions to get started. For more information about changes in version 5.0, see "New Features Introduced in Version 5.0" on page 18.

How and where are my settings saved?

Settings are saved automatically to the Reflection X Advantage database (page 217) while you work.

Can I undo an action?

There is no undo option for edits you’ve made to a definition. However, you can easily recover deleted definitions. Click the definition trashcan icon 🗑️, or go to File > Definition Trashcan. This opens a dialog box with a list of deleted definitions. You can select any item on the list and click Restore Item. By default, the trashcan is deleted when you exit. You can modify this behavior using File > Preferences.

Should I use standalone or domain mode?

Standalone mode is provided by a single application—X Manager, which is installed by default. In this mode, all you need to do to get started is install using defaults. Sample settings are included that make it easy for you to get connected to your host applications. Running Reflection X Advantage in Domain mode provides access to all the features in standalone mode, and also provides access to additional domain services. These additional services include support for centralized configuration of settings, the ability to leave sessions running and rejoin them in progress from the same computer or another computer in the domain, and fault tolerance to ensure that running sessions remain available even if your system crashes or you lose your connection. For a comparison of features, see Operating Modes: Domain vs. Standalone. (page 8) For diagrams showing some typical domain configurations, see Sample Domain Configurations. (page 163)
How do I set up a Reflection X Advantage domain?

To configure a domain, you'll need to install a domain controller and Administrative Console; add domain nodes; and install X Manager for Domains on user workstations. For details, see Setting up Domain Components. (page 153)

Why can't I edit a client or session definition?

If you are running X Manager for Domains, you may see public client and session definitions that have been made available to you by the domain administrator. You can use these to start sessions, but only the administrator can edit them.

Who can share definitions?

The ability to create public definitions (page 256) is available when using the Reflection X Advantage Administrative Console, and is limited to administrators only. This feature is not available in standalone mode. In either mode it is possible to export and import definitions to share them with other users.

Can I share my display?

Anyone can share a display from either X Manager or X Manager for Domains. Select the running session and look at the Session Status section on the right.

If you are running X Manager, click Share. This generates a connection URL. Click Copy URL to copy this and send it to other users, who can join your session using Action > Join.

If you are running X Manager for Domains, edit the Allowed Users list. Users you add here will see your session under Offered Sessions.

Can I edit my client and session definitions while a session is running?

Yes. The changes you make do not affect running clients and sessions, but are applied the next time you start the client or session.

What happens when I start a session?

Starting a session starts an X server that will display your X client applications and receive keyboard and mouse input. Starting a session also starts session processes (page 150) that manage client connections and protocol routing. You can start a session before you start your clients, but you won't see a display until you start a client.

What happens when I start an X client or XDMCP connection?

A session must be running before Reflection X Advantage can display your X client application or desktop. When you start an X client or XDMCP connection, Reflection X Advantage checks to see if the definition specifies a default session. If there is no default session, you're prompted to select one. If there is a default session, Reflection X Advantage checks to see if it is already running and starts it if it isn't. Once the session is running, Reflection X Advantage starts your client and displays it using the settings you've configured for that session.

Can I configure Reflection X Advantage to start my sessions and client applications automatically?

Yes, each definition type includes a setting to start that definition automatically when you start X Manager or X Manager for Domains. For example, if you select Automatically start session in your session definition, the session starts automatically. This can save time when you launch your clients. It is also useful if you prefer to start clients from a terminal session; you can start X Manager and run it in the background, knowing that your X server is automatically running and available.
What is a launch group?
A launch group provides a way to start multiple applications. You can add any defined X clients or XDMCP connections to a group, and all added items start when you start the launch group. If you enable **Automatically start launch group**, all your applications start automatically when you start X Manager or X Manager for Domains.

**Administrator questions**

**How can I create and deploy custom settings to end users?**
In domain mode, create and share public sessions. (page 168) In standalone mode, use Management and Security Server (sold separately) to deploy settings. In both domain mode and standalone mode, install custom templates. (page 200) For more information about these options, see Deploying Settings - Overview. (page 196)

**Can I use a command line to start Reflection X Advantage?**
Yes, use `rxmgr` (page 227) to start X Manager and `rxmgrdomains` (page 229) to start X Manager for Domains. These command-line utilities include options for starting specific clients and sessions, and also for limiting user access to the user interface.

**Can I provide users with read-only access to settings and prevent users from creating their own settings?**
You can do this using the `rxmgr` (page 227) and `rxmgrdomains` (page 229) command-line utilities. Use the `-execOnly` option to launch Reflection X Advantage in a slimmed-down mode that enables user to see and use the definitions you have provided without allowing access to features for editing settings.

**Related Topics**
- “Troubleshooting” on page 245
The procedures and reference information provided in this section of the user guide apply to both the standalone X Manager and X Manager for Domains.

X Manager is a tool that you can use to configure, start, and monitor X sessions. To start an X session, you need a "session definition" on page 257.

X Manager for Domains connects you to a Reflection X domain. With this tool, you can start public sessions that have already been configured by the domain administrator; and you can also configure, start, and monitor your own sessions.

In this Chapter

- “How to...” on page 33
- “User Interface Reference” on page 69

How to...

The topics in this section describe the tasks you can perform with X Manager and X Manager for Domains.

In this Section

- “Start X Manager” on page 34
- “Configure an X Client” on page 36
- “Configure a Desktop Connection” on page 37
- “Start a Client” on page 39
- “Stop a Session” on page 40
- “Organize your Definitions” on page 41
- “Sharing and Suspending Sessions” on page 41
- “Work with Colors” on page 44
- “Work with Fonts” on page 47
- “Work with Keyboard Maps” on page 52
- “Configure Reflection X Advantage to Use Your Local IME” on page 56
- “Export and Import Definitions” on page 57
- “Enable or Disable Extensions” on page 59
- “Configure Compression” on page 59
- “Set Up Secure Shell (SSH) Connections” on page 60
Start X Manager

Reflection X Advantage can be operated in either Standalone (page 258) or Domain (page 259) mode; and you can start X Manager in either mode from the graphical user interface (GUI) or the command line.

When starting X Manager in Domain mode, users must log on to the domain, providing the proper credentials for the authentication method used by the domain.

NOTE

• The default Reflection X Advantage authentication method depends on the operating system of the computer on which the domain controller is installed. The domain administrator can change defaults and set up authentication from the Administrative Console.

• Reflection X Advantage migrates settings from previous Reflection X Advantage versions (v. 13 or 14) and from Hummingbird Exceed products. The first time you start X Manager or X Manager for Domains, your local settings are migrated automatically, and you are prompted to import the settings. If you choose not to import the settings, you can use Reflection X Advantage to import them later.

Start in Standalone Mode

You can start X Manager from the graphical user interface (GUI) or the command line.

To start X Manager from your computer desktop:

<table>
<thead>
<tr>
<th>On</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>From the Start menu, point to All Programs &gt; Micro Focus Reflection &gt; X Manager.</td>
</tr>
<tr>
<td>UNIX</td>
<td>From the Applications menu, point to Micro Focus Reflection &gt; X Manager. (On Solaris Java Desktop, you may need to log out after your initial install, then log in again to see this menu item.)</td>
</tr>
</tbody>
</table>

To start X Manager from the command line

1. From a command prompt, navigate to your Reflection X Advantage program folder. The default location is:

   **NOTE:** On Windows the program folder is added to the path by the installer, so this step is optional.

   - **Windows:** C:\Program Files\Micro Focus\Reflection
   - **UNIX:** /opt/rxadvantage

2. Use the following command to start X Manager for Domains:

   - **Windows:** rxmgr
   - **UNIX:** ./rxmgr

   **NOTE:** Command line options are available. For example, you can specify sessions and clients that you want to start. For details, see `rxmgr Command Line (page 227)`. The options described apply to the startup command on all platforms.
Start in Domain Mode

You can start X Manager for Domains from the graphical user interface (GUI) or the command line.

To start X Manager for Domains from your computer desktop

1. Start X Manager for Domains:

<table>
<thead>
<tr>
<th>On</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>From the Start menu, point to All Programs &gt; Micro Focus Reflection &gt; X Manager for Domains.</td>
</tr>
<tr>
<td>UNIX</td>
<td>From the Applications menu, point to Micro Focus Reflection &gt; X Manager for Domains. (On some platforms, you may need to log out after your initial install, then log in again to see this menu item.)</td>
</tr>
</tbody>
</table>

2. Log on to the Reflection X domain:
   - For Username and password, enter your credentials to log onto the Reflection X Advantage domain. If your domain is configured to use the default authentication option (Windows authentication on Windows systems and PAM authentication on non-Windows systems), you can log on using the same credentials you use to log on to your computer.
   - For Domain, enter the Reflection X Advantage domain name. (The Reflection X Advantage domain name is always the same as the name of the computer running the domain controller.)

3. (Optional) Once you are logged on, to log onto a different domain, from the File menu, choose Log Off, and then select Log On.

To start X Manager for Domains from the command line

1. From a command prompt, navigate to your Reflection X Advantage program folder. The default location is:

   **NOTE:** On Windows the program folder is added to the path by the installer, so this step is optional.

   **Windows:** C:\Program Files\Micro Focus\Reflection
   **UNIX:** /opt/rxadvantage

2. Use the following command to start X Manager for Domains:

   **Windows:** rxmgrdomains
   **UNIX:** ./rxmgrdomains

   **NOTE:** Command line options are available. For example, you can specify domain name; logon credentials; and sessions and clients that you want to start. For details, see rxmgrdomains Command Line (page 229). The options described apply to the startup command on all platforms.
Configure an X Client

In many cases you can make your first connection using the installed sample definitions and then use the sample as a model for connecting to other clients. For details, see “Launch an X Client Application Using the Sample Definitions” on page 22. Use the procedure below to configure a new client without using the sample definitions.

Configure the connection

1. Click the plus sign, +, next to X Clients to create a new client definition.
2. For Name, enter a descriptive name for this client definition.
3. For Host name, specify the name or IP address of the computer that hosts your X client application.
4. Select your Host type from the drop-down list. The host type you select affects:
   - The syntax and selection of sample commands shown in the Command drop-down list.
   - The default xauth command, which is used for user-based authorization. (Click Advanced to view or edit this command.)
   - (For Telnet and Rlogin) The default login sequence. (Click Advanced to view or edit the login sequence.)
5. Select a Connection method. The default is Secure Shell (page 72). Other options are Telnet (page 76), Rexec (page 80), Rlogin (page 81), and Rsh (page 82).
6. (Optional) Enter a value for User name. If you leave this blank, you'll be prompted for your user name when you connect.

   **NOTE:** If you're configuring Telnet, Rexec, or Rlogin, you also have the option of entering a password. Passwords are stored as clear text in the Reflection X Advantage database and in exported definition files. Leaving this blank is a more secure option; you'll be prompted for your password when you connect.

7. For Application, leave the default, Single command, selected. Using this option provides access to sample commands, which are not available when Multiple command is selected. For most situations, it's easiest to create a new client definition for each client you want to launch.
8. Click the Command down-arrow to display a list of sample commands for the host type you selected. For your initial tests, it's a good idea to try one of the listed commands (such as xterm). If this works, you can modify the command to start your own client application. Additional Information about configuring commands follows this procedure.
9. From the Session list, select a default session to start when you start this client.
   - If you want your client application to run on your desktop, select a session configured to Show clients on my desktop. The sample session called "My desktop" uses this configuration.
   - If your client command launches a desktop environment such as KDE, CDE or GNOME, select a session configured to Show clients on X terminal desktop. The sample session called "X terminal desktop" uses this configuration. For these clients, also enable Always start on new instance.
10. (Optional) Click Advanced to configure additional settings for your connection. The options available depend on the connection method.
Configuring the client command

Use the sample commands in the Command list as a starting point for creating your own commands. These commands demonstrate the use of macros (%IP#% is one example). Macros are replaced by appropriate values when the command is sent to the client host. Macros can be used to specify the IP address for the display, the display number, the host name for the display, and additional information. For a complete list of supported macros and their descriptions, see “X Client Commands - Macro Reference” on page 71.

The following examples demonstrate frequently used features of command-line syntax:

The following command demonstrates using the %IP#% macro to specify the IP address and display number to be used for the client display.

```
xterm -display %IP#%
```

The next example adds a screen number.

```
xterm -display %IP#2%
```

The last example adds an ampersand to the command and encloses it in parentheses. This is the syntax you'll see in the Reflection X Advantage sample commands. When the command is sent to the host, it runs in a subshell in the background. This format may be required with some Telnet connections to keep the application running.

```
(/usr/bin/xterm -display %IP#% &)
```

**NOTE:** For most connections, you can omit the parentheses and ampersand. If you do use this syntax in Secure Shell sessions, the ampersand is removed from your command before it is sent to the host. (The trailing ampersand isn't supported in combination with X11 forwarding).

Configure a Desktop Connection

These procedures describe two ways to display a host desktop. The first procedure creates an XDMCP connection. The second procedure creates an X client definition to launch a desktop environment such as KDE, CDE or GNOME.

**NOTE:** XDMCP is not available if you are running in FIPS mode.

**To configure a desktop session using XDMCP**

1. Click the plus sign, +, next to XDMCP Connections.
2. For Name, enter a descriptive name for this connection.
3. For Type, select one of the following:
Reflection X Advantage Help

For Default session, specify a session configured to Show clients on X terminal desktop. The sample session called "X terminal desktop" uses this configuration.

NOTE: If you are connecting through a VPN and are having problems using XDMCP to connect to a session, you may be able to resolve the problem by using a distributed session. With this configuration, the client connector that originates the XDMCP request runs on the X application host and the request does not have to travel through the VPN router. (VPN routers typically block XDMCP connection requests.) If you're using X Manager, see "How to Configure a Distributed Session in Standalone Mode" on page 147. If you're using X Manager for Domains, see "Domain Setup: Improve Performance Over a Slow Network" on page 163.

To configure an X client command that launches a desktop environment

1. Click the plus sign, +, next to X Clients to create a new client definition.
2. For Name, enter a descriptive name for this client definition.
3. For Host name, specify the name or IP address of the host.
4. (Optional) Change the Connection method and specify a User name.
5. Select your Host type from the drop-down list.
6. Click the Command down-arrow and select a command that displays a desktop environment.

NOTE: Different host types support different desktop environments. The sample commands in the list change based on the host type you selected. For example, for VMS hosts, Session Manager starts the DecWindows Desktop Environment. For Solaris hosts, Xsession starts the Common Desktop Environment (CDE). For Linux hosts, startkde starts the K Desktop Environment (KDE) and gnome-session starts the GNOME Desktop Environment. The commands actually supported on your host depend on your host configuration; not all hosts have a desktop environment installed.

7. For Default session, specify a session configured to Show clients on X terminal desktop. The sample session called "X terminal desktop" uses this configuration.
8. Enable Always start on new instance. This ensures that a new X terminal desktop window will open when you start this client.
Start a Client

Reflection X Advantage provides a variety of ways to start your X client applications or XDMCP desktop connections.

A session must be running before a client application can be displayed. You can associate a default session definition with each of your X client applications, or configure these definitions to prompt you for a session name when you start the client. If the associated session is not already running, Reflection X Advantage starts the session when you start the client. It is also possible to start a session directly, without first starting a client. This may be useful if you start your clients directly from a terminal session.

To start a client manually

Configure an X client or XDMCP connection and do any of the following:

- Double-click the definition name.
- Select the definition, then in the toolbar click **Start**.
- Right-click the definition name and click **Start**.
- Drag the X client or XDMCP definition onto a session definition to start the client using that session.

To start a client automatically when you start X Manager or X Manager for Domains

- For an X client definition: In the **Client Definition** pane, select **Automatically start client**.
- For an XDMCP connection: In the **XDMCP Connection Definition** pane, select **Automatically start XDMCP session**.

To start clients using a desktop shortcut

This option is available if you are running on a Windows system.

1. Right-click an X client or XDMCP definition.
2. Select **Create Shortcut**.
3. Double-click the shortcut to start the session.

To attach a client to an already running session

This option is available for definitions under **X Clients**. You cannot start XDMCP connections this way.

1. Start a session using any of the following techniques:
   - Double-click the definition name.
   - Select the definition, then in the toolbar click **Start**.
   - Right-click the definition name and click **Start**.
   - Configure the session to start automatically when you start X Manager by enabling **Automatically start session**.
2 Launch your client application using either of the following techniques:
   • Drag an X client definition onto the running session.
   • Right click an X client definition, select Start on, then select the session name.

To start clients from the command line

There are a number of options for starting clients from a command line. The following examples start a client called myclient and its associated session without showing the Reflection X Advantage user interface. For additional information about command line options, see rxmgr (page 227) (for the standalone X Manager) and rxmlgrdomains (page 229) (for X Manager for Domains).
   • Standalone X Manager:
     rxmgr -client myclient -noUI
   • X Manager for Domains:
     rxmlgrdomains -client myclient -noUI

   NOTE: When you run this command, you are prompted to log into the Reflection X Advantage domain before you see any required host logon prompts.

Stop a Session

While a session is running, you see a running session entry under the session definition in the left pane. This entry shows the joined session icon, , and the name of the host on which the session is running.

To configure a session to stop automatically when the last client application exits
   • In the Session Definition pane, on the General tab, set On last client to Stop Session.

To stop sessions automatically when you exit X Manager

By default, you see a prompt when you close X Manager with one or more session running. Make this change to stop sessions without the prompt:

1 Go to File > Preferences
2 Set On exiting X Manager to Stop all sessions.

To stop a session manually

Use either of these methods to stop a session manually. This stops all clients running on this session.

   • Select the running session, then in the toolbar click the stop button.
   • Right click the running session and click Stop.

Related Topics
   • “Suspend and Resume (X Manager for Domains)” on page 43
Organize your Definitions

By default, all definition types are displayed, and each new definition you add within a section is added to the bottom of the list. Use the following approaches to organize your lists.

To change the order of items within a section

Use any combination of these methods:
- Drag and drop items within any definition group.
- Select an item, then move it using the up \& down arrow icons.
- Click the sorting icon to sort items alphabetically.

To change the order of sections in the definition pane

1. Go to File > Preferences.
2. Under Section Visibility, select a section title and move it using the up \& down arrow icons.

To change which definition lists are visible in the definition pane

1. To hide the definitions within a section, use the hide button. (The section title remains.)
2. To view the definitions in a hidden category, use the expand button.
3. To remove a section from the display (including the section title), go to File > Preferences and clear the checkbox for that section under Section Visibility.

Sharing and Suspending Sessions

In this Section
- “Share a Session” on page 41
- “Join a Session (X Manager for Domains)” on page 42
- “Join a Session (X Manager Standalone mode)” on page 43
- “Take Control of a Joined Session” on page 43
- “Suspend and Resume (X Manager for Domains)” on page 43

Share a Session

Using the Reflection X Advantage sharing feature, you can allow other users to join an X session that you have started. If you are operating Reflection X Advantage in Domain mode, from X Manager for Domains you can share running sessions with other users that log onto the domain. For those operating in Standalone mode, X Manager supports peer-to-peer sharing by generating a connection URL that allows other users to connect to your running session.

**NOTE:** Reflection X Advantage must be enabled for FIPS to join a peer-to-peer session started in FIPS mode.

To share a session from X Manager for Domains

1. From the Session Definitions list, select the running session that you want to share.
   Statistics for the session are displayed to the right.
2 From the Allowed Users list on the right, click the plus sign (+).

The Share with Users dialog box appears, displaying a list of the users that belong to the domain. It is not necessary for these users to be logged into the domain to be included on this list.

3 Select the user(s) with whom you want to share the session, and then click OK.

When a user in this list opens X Manager and logs into the Reflection X domain, the session is listed under Offered Sessions.

4 (Optional) Select Allow users to take control of session to provide session users with the ability to control the session.

**NOTE:** To end a user's access to a shared session from X Manager for Domains, remove the user from the list of allowed users. This terminates that user's session.

**To share a session from X Manager (standalone)**

1 From the Session Definitions list, select the running session that you want to share.

   Statistics for the session are displayed to the right.

2 In the Session Status section on the right, to share the session and generate a connection URL, click Share.

   **NOTE:** The Share button is not available if the running session is configured to use Remote Session Services (page 88).

3 Send the connection URL to whoever you want to join the session. (Copy URL adds the URL to the clipboard.)

   When invited users start X Manager and go to Action > Join, they can join the shared session by providing the connection URL.

4 (Optional) Select Allow users to take control of session to provide session users with the ability to control the session.

   To end access to a shared session from X Manager, click Unshare. This terminates all shared sessions.

**Join a Session (X Manager for Domains)**

In X Manager for Domains, if you leave your session (by clicking Leave or by closing the root window), it continues to run although you are not viewing it — the session is persisted in memory. You can rejoin your session, or, if another user has made his or her session available for sharing, you can join it. The steps are similar, whether you are joining an offered session (under Offered Sessions), or rejoining your own session (under Session Definitions).

**To join an X session**

1 Right-click the session you want to join under Session Definitions or Offered Sessions, and then select Join.

   The session window opens on your computer.

2 Offered sessions only: If the user who created the session has selected Allow users to take control of session, you can right-click the session and select Take Control.

   Having control of a session allows you to use the keyboard and mouse. Only one user at a time can have control of a session.
Join a Session (X Manager Standalone mode)

X Manager supports peer-to-peer session sharing by generating a connection URL that allows users to connect to a specific running session.

If another Reflection X Advantage user shares a session and gives you the connection URL, you can join the session.

**NOTE:** X Manager must be enabled for FIPS to join a peer-to-peer session started in FIPS mode.

To join an X session

1. From the **Action** menu, choose **Join**.
2. In the **Join Session** box, in the **Connection URL** field, enter the URL you received from the user who shared the session.
   
   The session window opens on your computer.
3. If the user who created the session has selected **Allow users to take control of session**, right-click the session, and select **Take Control**.
   
   You can now control the session through your computer mouse and keyboard. Only one user at a time can have control of a session.

Take Control of a Joined Session

One user can start a session, offer it to other users, and then allow those users to take control of the session. The following procedure applies to the user who has been allowed to join a session. When you take control, your keyboard and mouse provide input to the session, and the user from whom you took control stops providing input.

**NOTE:** This option is available only if the user who started the session has selected **Allow users to take control of session**.

To take control of a session in X Manager for Domains

1. Under **Offered Sessions**, right-click the session name and then select **Join**.
2. Right-click the session and select **Take Control**.

To take control X Manager (standalone)

1. Choose **Action > Join**, and then enter the connection URL provided by the user who shared the session.
2. Under **Joined Sessions**, right-click the session and select **Take Control**.

Suspend and Resume (X Manager for Domains)

If you are running X Manager for Domains, you can configure sessions that support the ability to leave the session without actually terminating the connection with the X client application. After you leave a session, the display closes, but the session is persisted in memory on a domain node. When you join the session, you see your client display as you left it — there’s no need to restart your client application or start a new session.
To leave a session without stopping the session or the client

1. Configure a Reflection X Advantage domain with at least one domain node (page 155).
2. Configure a session definition to support suspend and resume. (On the General tab, under Remote Session Services, select any of the options that include Session suspend/resume.)
3. Configure your client to use this session and start the client.
   Under the session definition, you should see a running session appear. The host shown for this session will be one of the domain nodes.
4. To leave the session, select the running session and click the leave icon, or right-click the session and click Leave. The running session icon changes to show that the session is now suspended. You can close X Manager for Domains at this point and the session will remain active and suspended on the domain node.

To rejoin the suspended session

1. Log into the Reflection X Advantage domain from any computer with X Manager for Domains running that has access to the domain controller. This can be the same computer from which you suspended the session or a different computer. You should see your running, suspended session.
2. To rejoin the session, select the suspended session click the join icon, or right-click the session and click Join. The client display reopens as you left it.

Work with Colors

Colors displayed on your monitor are created by combining various intensities of red, green, and blue (RGB). The colors are defined in color schemes (page 255), which list color names and the amount of red, green, and blue needed to display each color. These color schemes are used to translate color names requested by X client applications into RGB values.

NOTE: Not all X clients request colors by name — many clients request colors by RGB value or other methods, instead of specifying a color name. Changing the color scheme changes the colors the X server displays only when clients request colors by name.

For many client applications, you can use the default color scheme provided by Reflection X Advantage. However, if a client application requires specific color names that are not defined in the default color scheme, you will need to define a custom color scheme. You can also specify a custom color scheme to control the look and feel of the application. With Reflection X Advantage, you can:

- "Select a Color Scheme" on page 45
  Assign a different color scheme to a session definition, satisfy requests from client applications for specific color names, or control the look-and-feel of applications.
- "Import a Color Scheme" on page 45
  Support colors, in Reflection X Advantage, required by X client applications you are running on native systems or on previous versions of Reflection X Advantage.
- "Customize a Color Scheme" on page 46
  Change, add, or remove color values or string names to match those requested by client applications.
Select a Color Scheme

By default, Reflection X Advantage includes only one color scheme that is automatically referenced by each new session definition. This default scheme works for many client applications. However, if you have created other color schemes to satisfy client application requests for specific color names, or to change the look and feel of an application, you will need to select which scheme to use when you create a session definition.

**NOTE:** Not all X clients request colors by name — many clients request colors by RGB value or other methods, instead of specifying a color name. Changing the color scheme changes the colors the X server displays only when clients request colors by name.

To select an alternate color scheme from X Manager or the Administrative Console

1. (Administrative Console only) Click the **Domain Definitions** tab.
2. In the left pane, select a session.
3. Click the **Display** tab.
4. From the **Color scheme** list, select a scheme that is compatible with the client application to which you are connecting.

**NOTE:** The **Color Scheme** list includes the default color scheme, all of the schemes you have created or imported, and all of the public schemes created by the administrator(s).

Import a Color Scheme

If you are running X client applications on native systems or with previous versions of Reflection X Advantage, you can ensure that Reflection X Advantage supports the colors required by these applications by importing RGB text files as color schemes.

For example, if you are running a client application on a UNIX workstation X server console, you can find the RGB text file that the X server is using and import it into Reflection X Advantage as a color scheme.

To import a color scheme

1. From X Manager, click **Tools > Color Schemes**, and then click **Import**.
   -or-
   From Administrative Console, select the **Domain Definitions** tab and then click **Action > Import Color Schemes**.
2. In the **Scheme name** box, enter the name of the color scheme as you would like it to appear in the Reflection X Advantage interface.
3. In the **RGB file** box, enter or browse to an RGB text file (for example, rgb.txt).
Customize a Color Scheme

Color schemes translate color names requested by client applications into red, green, and blue (RGB) values. If you are using a client that explicitly references a color name (for example, "rosybrown") that is not in the default color scheme, you will need to customize the session's color scheme to include the name.

For some client applications, you can determine which colors are required by examining the command line that starts the application. For example, the following command starts an xterm with a gray2 foreground and a cyan2 background:

```
/usr/bin/X11/xterm -fn 6x13 -sb -ls -d %IP#% -fg gray2 -bg cyan2 &
```

For other clients, an error message that references the missing color is displayed when the client fails to start. In the following example, the leaf application cannot start because the color rosybrown is missing.

```
Can't allocate named color rosybrown
leaf: Can't create window
```

To customize a color scheme

1. Using X Manager, click **Tools > Color Schemes**, and select a scheme from which to make a customized copy, and then click **Clone**.
   - or-
     Using Administrative Console, from the **Domain Definitions** side tab, under **Color Schemes**, select a scheme from which to make a customized copy, and then click **Action > Clone**.

2. For the Scheme name, use the name provided, or enter your own.

3. On **Colors In Scheme**, click the plus sign (+).
   - A "new color" entry is added to the end of the color table.

4. Click **new color** and enter the name of the color required by the client application.

5. Click the **RGB** tab and set the RGB values for the new color.

6. Click **Close**.
   - The **Color Schemes** window closes.

7. In each of the session definitions that you want to reference it, use the **Display** tab to select the new customized color scheme.

**NOTE**: On existing running sessions, color changes will take effect only after restarting the session.

X Window System Color Support

Color handling in the X Window System is complex because of the need for portability to many different types of displays. The X Window System supports color using colormaps and a color name database. It is not necessary to read the information in this topic to configure Reflection X Advantage: it is here for those users who desire a better understanding of X Window System color support.

Colormaps

Colors that you see on your monitor are defined by a combination of the intensities of red, green, and blue. This is called the **RGB color model**, and is the most commonly used model for color displays. RGB color definitions are stored in the elements (called **colorcells**) of lookup tables (called
colormaps), which are stored on the server. All X servers create a default colormap that is available to (and shared by) clients that require a small number of colors. Clients that are more color-intensive may create their own private colormaps.

When client applications attempt to use color, they do not specify a pixel value, or the color to put in that cell to draw in a given color. Instead, they request access to a colorcell in a colormap, and are returned a pixel value.

The range of colors available on the screen is a function of the number of bit planes (the pixel depth, which determines the number of colors that can be displayed) and the width of the hardware color registers (if eight bits are available for each primary, then the range of colors is about 16 million).

The X Window System supports virtual colormaps so that any number of colormaps can be maintained, even though the number that may be in use at a time may be limited. Virtual colormaps are swapped in and out of hardware colormap "slots" by the window manager.

Visual

A visual describes the display format for a particular screen. It contains information about one way to use the capabilities of the display hardware. There may be several applicable visuals.

The six visual classes distinguish between color or monochrome, whether the colormap is read/write or read-only, and whether a pixel value provides a single index to the colormap or is composed of separate indices for red, green, and blue values. A comparison of the visual types follows:

<table>
<thead>
<tr>
<th>Visual Type</th>
<th>Read/Write</th>
<th>Read-Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monochrome/Gray</td>
<td>GrayScale</td>
<td>StaticGray</td>
</tr>
<tr>
<td>Single index for RGB</td>
<td>PseudoColor</td>
<td>StaticColor</td>
</tr>
<tr>
<td>Separate indices for RGB</td>
<td>Direct Color</td>
<td>TrueColor</td>
</tr>
</tbody>
</table>

A screen that supports the DirectColor class can theoretically support any of the six visual classes. Screens that support the PseudoColor visual class can also support GrayScale, StaticColor, or StaticGray visual classes. If the screen supports the GrayScale visual class, it can also support StaticGray.

Even though a certain visual class can theoretically be supported by the capabilities of a display hardware system, the server implementation determines whether that visual class is supported.

Work with Fonts

When an X client requests a font, the Reflection X server receives the font name supplied by the client, and then searches for it among the font collections (page 258) in the Server Font Path list. The font collections are searched in the order in which they are specified in the list.

Reflection X Advantage provides default font collections commonly required to support X client applications. To provide additional fonts, improve search performance, or troubleshoot font problems, you can:

- “Add Font Collections” on page 49

  Provide fonts that are not included in the default font collections, to resolve display problems caused by missing fonts.
• “Modify the Server Font Path List” on page 51
  Add font collections used by a particular X session definition to the Server Font Path list, or improve search performance by changing the order of the font collections in the list. (If a font collection is used frequently, you can improve performance by moving it up in the list.)

• “Log Font Activity” on page 51
  Troubleshoot font related errors — log font activity, repeat the steps that are causing the error, and then review your log file.

Related Topics
• “Default Font Collections” on page 48

Default Font Collections

Reflection X Advantage provides font collections (page 258) commonly required to support X client applications. All of the X11R7 fonts for The Open Group are available at 75 and 100 dpi (dots per inch resolutions). Font collections are also available from Hewlett-Packard, Digital Equipment Corporation, Sun, and IBM, along with fonts for Japanese hosts and for Unicode (where supported).

The Reflection X server has access to all of the fonts in the Server Font Path list. When an X server receives a protocol request about fonts from a client application, it searches these font collections to satisfy the request.

X.Org 75 dpi Fonts

The X.Org 75 dpi font collection works well with VGA resolution displays.

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Display Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>800 x 600</td>
<td>15” and 17”</td>
</tr>
<tr>
<td>1024 x 768</td>
<td>19”</td>
</tr>
<tr>
<td>1152 x 900 or 1280 x 1024</td>
<td>21”</td>
</tr>
</tbody>
</table>

X.Org 100 dpi Fonts

The X.Org 100 dpi font collection works well with high resolution displays.

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Display Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>800 x 600 or 1024 x 768</td>
<td>13” and 14”</td>
</tr>
<tr>
<td>1024 x 768</td>
<td>15” and 17”</td>
</tr>
<tr>
<td>1152 x 900 or 1280 x 1024</td>
<td>19”</td>
</tr>
<tr>
<td>1600 x 1200</td>
<td>21”</td>
</tr>
</tbody>
</table>

X.Org Misc Fonts

The X.Org misc font collection contains a basic set of fonts for X clients, including the “cursor” font frequently used for different cursors needed by X clients, and the “fixed” font that is required for the X server to start.
HP Fonts
These 75-dpi fonts are required by HP VUE and other X clients designed to run on Hewlett-Packard hosts.

DEC Fonts
These 75-dpi fonts are required by many X clients designed to run on Digital Equipment Corporation hosts.

IBM Fonts
These 75-dpi fonts are required by AIX windows, and by many X clients that run on IBM RISCsystem/6000 (AIX) hosts.

Sun Fonts
These 75-dpi fonts are required by X clients designed to run on Sun Microsystems hosts.

Japanese Common Fonts
This is a collection of 75-dpi fonts for generic Japanese hosts.

Unicode Fonts
This is a collection of Unicode-compliant 100- and 75-dpi fonts for those applications that support Unicode display.

TrueType Fonts
This is a collection of TrueType fonts for applications that support the advanced font scaling capabilities offered by the TrueType format.

Related Topics
- “Font Collections” on page 98
- “Fonts tab” on page 97

Add Font Collections
A font collection is either a set of font files or a reference to a font server.

Reflection X Advantage provides default font collections that include fonts commonly required by X client applications.

All of the X11R7 fonts for The Open Group are available at 75 and 100 dpi (dots per inch resolution). Default font collections also include fonts for Hewlett-Packard, Digital Equipment Corporation, Sun, and IBM hosts, along with fonts for Japanese hosts and for Unicode (where supported). If clients require other fonts, you will need to add font collections that include those fonts. You can add a font collection by loading a directory of font files or by referencing an X font server.

Font Paths
Because it supports running in a distributed model, Reflection X Advantage cannot resolve font directory paths explicitly referenced in client application requests. Instead of using font directories, Reflection X Advantage uses font catalog names to identify font collections. To satisfy client requests that include font directory paths, use one of the following approaches:

- Change the request the client sends the server, so that the font directory path is replaced with the font catalog name. For example, if you are using Xset to specify font paths, you can change the directory /usr/X11/myfonts to the catalog name myfonts, as follows:
Xset -fp /usr/X11/myfonts +fp rx/myfonts

- or -

- Load the requested fonts into a new font collection, and then enter the requested font path in the Alternate paths box, as described below (the alternate path entry is an alias for the catalog name). For example, if an X client requests /usr/X11/myfonts, and does not start unless those fonts are found, load the fonts into a new font collection and add /usr/X11/myfonts as an alternate path for the collection.

To add a font collection

1 From the Administrative Console, click the Domain Definitions side tab. The Font Collections section lists all font collections currently available to you.

- or -

From X Manager, choose Tools > Font Collections.

2 The Font Collections dialog box opens.

3 At the top of the Font Collections list, click the plus sign (+) and do one of the following:

   Select                               To
   New Font File Set Collection         Load a directory of font files into a new font collection on the domain.
   New Font Server Collection          Add a font collection that is a reference to a font server.

4 In the Collection name box, enter the collection name as you want it to appear in the Font Collections list.

5 In the Catalog name box, enter the collection name as you want it to be referenced by client applications.

6 Do one of the following:

   If you chose to load a directory of font files into a font collection:
   
   6a If client applications explicitly reference a font path when requesting this font, enter that font path in the Alternate paths box.
   
   6b Click Load Fonts, and then browse to a valid X11 font directory that contains the fonts that you want to load.

   Once loaded, the original directory of fonts is no longer required.

- or -

If you chose to add a font collection that is a reference to a font server, in the Font server box, enter the fully qualified name and port of the X font server as follows:

   tcp/host:port

   For example, the following URL specifies to connect to the font server on the computer wilson:

   tcp/wilson.myco.com:7100

   - If no transport is specified, tcp (the default) is assumed.
   - If no port is specified, 7100 (the default) is assumed.

If you are a domain administrator, you can make the font collection available to anyone who is using the domain. From the Font Collections section in the Administrative Console’s Domain Definitions tab, right-click the font collection name and choose Make Public from the action menu.
Modify the Server Font Path List

When an X client application requests a font, the X server searches for it in the font collections in its Server Font Path list. These font collections are searched in the order in which they appear in the list.

You can improve session performance by changing the order of the font collections in the list, or by removing unnecessary font collections from the list.

**NOTE:** To modify the X server font path list of a public definition, you must own the definition. If you are not the definition owner, you can clone the session definition, and then modify the new session definition.

To modify the Server Font Path list

1. Start X Manager or the Administrative Console.
2. (Administrative Console only) Click the Domain Definitions tab.
3. In the left pane, select a session.
4. Click the Fonts tab.
5. To change the order in which a font appears in the Server Font Path list, select the font and click the up or down arrows at the top of the list. To add or remove a font collection to or from the Server Font Path list, use the arrows to the right of the list.

Log Font Activity

When an X client requests a font, the Reflection X server receives the font name supplied by the client, and then searches for it among the font collections (page 258) in the Server Font Path list. The font collections are searched in the order in which they are specified in the list. A name can match the actual font name or an alias for the font.

All of this font activity — the requests and the procedure Reflection X Advantage uses to respond to those requests — is written to your log file when the Log font activity option is selected. If you are getting font-related errors, select this option, repeat the steps that caused the error, and then review your log file.

By default, Log font activity is not selected. This option takes effect when the session is started.

To log font activity

1. From X Manager, under Session Definitions on the left, select a session.
   - or-
   From the Administrative Console, click the Domain Definitions tab, and then under Session Definitions on the left, select a session.
2. Click the Logging tab.
3. Select Log font activity.
Work with Keyboard Maps

Change the Keyboard Map Used by a Session

Reflection X Advantage includes a default keyboard map that is automatically referenced by each new session definition. This default keyboard map works for many client applications. Additional predefined keyboard maps are also available. In addition to these predefined options, you can create your own custom keyboards using the “Keyboard Maps” on page 106 dialog box. To use an alternate keyboard map, use the following procedure to create a session definition that uses the alternate map, then configure your clients to use this session.

To modify a session to use an alternate keyboard map

1. In the left pane, select a session.
2. Click the Keyboard tab.
3. From the Keyboard Map list, select a keyboard map that you want to use in the session definition.

   **NOTE:** The list shows default keyboard maps and any custom keyboard maps you have created or imported. If you are running in domain mode, the list may also include public keyboard maps created by the administrator(s).

4. (Optional) Click Edit to edit or review the selected keyboard map.

   **NOTE:** Domain administrators can also configure Keyboard Maps from Administrative Console, using the Domain Definitions tab.

Find the Current Mapping of a Key

You can use the Find option to locate a key and view its current behavior. If the results you see are the characters you expect and they are in the list of supported characters, no mapping is required. This sample procedure shows how to find the current mapping of the 4 key.

To find the current mapping of the 4 key (unshifted and shifted)

1. In X Manager or X Manager for Domains, click Tools > Keyboard Maps.
2. In the Keyboard Maps dialog box, click the Find button on the lower right.
3. In the Find Key dialog box, type 4 in the Press a key field.
4. Note the text in the Results box, which indicates that this key sends the number 4:

   Character "4" (Unicode 0034, X Keysym "4") is in the list of supported characters.

5. Click Reset.
6. In the Find Key dialog box, press the Shift key and type 4 in the Press a key field.
7. Note the text in the Results box. On a U.S. keyboard, the results indicate that a dollar sign is being sent for this combination.

   Character "$" (Unicode 0024, X Keysym "dollar") is in the list of supported characters.
Related Topics

- “Keyboard Maps” on page 106
- “Troubleshooting (Keyboard Maps)” on page 114

Map a Function Key

You can use these steps as a guideline for mapping any key that is listed in the Explicitly mapped keys on the Map Key tab in the Keyboard Maps dialog box.

Suppose that your X client requires a function key (such as F23) that you don't have on your keyboard. You can map one of your function keys (such as F10) to send the F23 X Keysym (page 257).

To map the unshifted F10 to send the F23 X Keysym

1. In X Manager or X Manager for Domains, click Tools > Keyboard Maps.
2. For Select Keyboard Map, select an editable keyboard map.

   **NOTE:** The default keyboard maps are not editable. Click Clone to create a new custom keyboard map based on an existing keyboard map.

3. Use the Map Key tab (displayed by default).
4. In the list of Explicitly mapped keys on the left side of the tab, select the F10 key. (As an alternative, you can click the + sign in Explicitly mapped keys to open the Add or Find Key dialog box. With your cursor in the Press a key field, press F10, then click OK.)
5. With the F10 key selected, click the first Change Mapped X Keysym button (next to the Unshifted key description).
6. In the Change Mapped X Keysym dialog box, use the following steps to select F23. (Since this is not a physical key on your keyboard, you must select it from the list.)
   6a. Set Filter X Keysym list by category to Function Keys.
   6b. In Select X Keysym from list, select F23.
7. Click OK.
8. The Map Keys tab now shows that the F10 key is mapped to the F23 X Keysym.

   **NOTE:** Administrators can also configure Keyboard Maps from the Domain Definitions tab

Use a Compose Sequence to Specify an X Keysym

You can use a compose sequence to map any Unicode character to an X Keysym. For example, suppose that your X client requires the pi symbol (π) that you don't have on your keyboard. You can map one of your function keys (such as F11) to send it.

To map the unshifted F11 to send the pi (π) X Keysym

1. In X Manager or X Manager for Domains on a Windows machine, click Tools > Keyboard Maps.
2. For Select Keyboard Map, select an editable keyboard map.

   **NOTE:** The default keyboard maps are not editable. Click Clone to create a new custom keyboard map based on an existing keyboard map.
3 Use the Map Key tab (displayed by default).

4 In the list of Explicitly mapped keys on the left side of the tab, under Key, select F11. (As an alternative, you can click the + sign in Explicitly mapped keys to open the Add or Find Key dialog box. With your cursor in the Press a key field, press F11, then click OK.)

5 With the F11 key selected, click the first Change Mapped X Keysym button (next to the Unshifted key description).

6 In the Change Mapped X Keysym dialog box, specify the pi symbol. Although this is not a physical key on your keyboard, you can use a compose key sequence to specify it.

   To locate the correct X Keysym using a compose sequence:
   
   6a Position your cursor in the Press a key to locate corresponding X Keysym field.
   6b Hold down the Alt key, then enter 227 on the numeric keypad. (This is the Windows value for composing pi; other platforms have similar compose key options.) Release the Alt key, and the X Keysym name Greek_pi is displayed.

7 Click OK.

8 The Map Keys tab now shows that the F11 key is mapped to the Greek_pi.

---

**NOTE**

- When you explicitly map a key as described here, you do not need to add it to the list of supported characters on the Characters tab.
- Reflection X domain administrators can also configure Keyboard Maps from the Domain Definitions tab.

---

**Map a Keyboard Shortcut to an X Keysym**

You can map a key or a key sequence to an X Keysym (page 257). For example, you can map the Alt key combined with the `~ key to send a Euro symbol (€).

**To map a Euro symbol to a Keyboard Shortcut**

1 In X Manager or X Manager for Domains, click Tools > Keyboard Maps.

2 For Select Keyboard Map, select an editable keyboard map.

   **NOTE**: The default keyboard maps are not editable. Click Clone to create a new custom keyboard map based on an existing keyboard map.

3 In the Keyboard Maps dialog box, click the Keyboard Shortcuts tab.

4 In the Shortcut column, click the + sign.

5 In the Specify Shortcut Key Combination dialog box, select Alt. Position your cursor in the Press a key field and click the `~ (backquote/tilde) key. If you don't have this key on your keyboard, select another key.

6 Click OK.

Alt+Back Quote is now selected in the Shortcut list.

7 Click the Send X Keysyms button and then click the + sign to the right of X Keysyms to send.

8 In the Select X Keysym dialog box, select the EuroSign.

   8a To find the Euro symbol quickly, type "euro" in the Only list X Keysyms whose names contain field.
   8b Select EuroSign from the Select X Keysyms from list field, then click OK.
NOTE: Administrators can also configure Keyboard Maps from the Domain Definitions tab.

Map a Keyboard Shortcut to a String

You can map a key to a character string that you must type frequently (such as a department name).

To map a key to send the string "Engineering Department"

1. In X Manager or X Manager for Domains, click Tools > Keyboard Maps.
2. For Select Keyboard Map, select an editable keyboard map.

   NOTE: The default keyboard maps are not editable. Click Clone to create a new custom keyboard map based on an existing keyboard map.

3. In the Keyboard Maps dialog box, click the Keyboard Shortcuts tab.
4. In the Shortcuts column, click the + sign.
5. In the Specify Shortcut Key Combination dialog box, select Alt and type \ (backslash), then click OK.
6. Alt + Backslash is now highlighted in the Shortcuts column.
7. Click Send String and type the string Engineering Department. Whenever you press Alt + Backslash, Reflection X Advantage will send the characters Engineering Department as if you had typed them.

NOTE: Administrators can also configure Keyboard Maps from the Domain Definitions tab.

Add an Unsupported Character

Some characters are not supported by default. If you need to use unsupported characters, you can add them to the list of supported characters. This sample procedure adds Greek characters to the supported list.

NOTE: If you map characters explicitly (page 53), you do not need to add them to the supported character list. If you add supported characters, you do not need to map them explicitly.

To add Greek symbols to the list of supported characters

1. In X Manager or X Manager for Domains, click Tools > Keyboard Maps.
2. For Select Keyboard Map, select an editable keyboard map.

   NOTE: The default keyboard maps are not editable. Click Clone to create a new custom keyboard map based on an existing keyboard map.

3. In the Keyboard Maps dialog box, click the Characters tab.
4. Select Greek under Unsupported (available for mapping).

   NOTE: If you need only one or two characters from the set, you can select and move them individually.

5. Click the < button in the middle of the tab to move these characters to the list of characters that are Supported (already included in keymap).
Configure Reflection X Advantage to Use Your Local IME

If you already use an IME (Input Method Editor) (page 256) that is available on your workstation, you may want to enable Native IME Support. This feature lets you use your workstation’s IME to compose text. The XIM server provided by Reflection X Advantage obtains the composed text from your IME and passes it to XIM-aware clients. This means that you can work with varied X clients without having to learn new input techniques.

The Reflection XIM server supports:

- On-the-spot and over-the-spot editing
- All Unicode characters, including Japanese, Chinese, and Korean characters

Before you begin, review the following requirements:

- You must have a native IME (such as Windows IME) installed on your workstation.
- The X client must use the XIM protocol.
- The client locale (usually specified by the LANG environment variable) must be one of the following: ja_JP.UTF-8, ja_JP.EUC-JP, ja_JP, C, en_US.UTF-8, ko_KR.UTF-8, ko_KR. (Additional locales can be specified using the Reflection X Advantage command-line parameter, “rxaim.locales”.)

To configure Reflection X Advantage to use your local IME

1. Under Session Definitions, select an existing session or create a new one.
2. In the Session Definition pane, click the Keyboard tab.
3. Select Launch XIM Server.
4. Select Force X clients to use Reflection’s XIM server.
5. Under X Clients, select a client definition:
   5a. For Session, select the name of the session you just modified to launch the XIM server.
   5b. Add "XMODIFIERS=@im=RXAIM" to the beginning of your command line. This configures the XMODIFIERS environment variable to identify the Reflection X Advantage XIM server. For example:

   XMODIFIERS=@im=RXAIM /usr/bin/gedit --display=%IP#%

   **NOTE:** In some cases, you may not need to set the XMODIFIERS variable. If your client is already configured to use a different XIM server, selecting Force X clients to use Reflection’s XIM server automatically redirects the client to the Reflection X Advantage XIM server. In other cases, additional modifications may be required. For more information see “IME Troubleshooting” on page 252.


   You can now start your local input editor and enter text as you usually do. Depending on your X client, you may see on-the-spot or over-the-spot editing.

   **NOTE:** If you complete this procedure and you are still unable to use your local IME to enter text into the X client, review the information in IME Troubleshooting (page 252).
Export and Import Definitions

Reflection X Advantage stores your client and session settings in a database. Using the Export/Import Definitions features in Reflection X Advantage, you can share your private Reflection X Advantage definitions (session, X client, X server, color scheme, font collection, and Secure Shell host and user key definitions) with other users.

- **Export Definitions** (page 57)
  Copy selected definitions from the Reflection X Advantage database to an .rxd definitions file.

- **Import Definitions** (page 58)
  Select and import definitions from an .rxd definitions file into your active product database (the local database when using the standalone X Manager, or the domain database when using X Manager for Domains).

When you import settings in domain mode, they are available for your use as private settings definitions. If you are a domain administrator, you can use the Administrative Console to make your imported private definitions public. Public domain definitions are visible and usable by all users in the domain.

You can also use this feature to import configuration settings that have been migrated from Reflection X Advantage version 13 or 14, or from Hummingbird Exceed products. The migrated settings are added to the active Reflection X Advantage database as definitions.

Export a Definition

You can copy selected definitions from the Reflection X Advantage database to a definition file (.rxd) that can be used to save or share settings. This file can be read and imported by X Manager or X Manager for Domains on any platform.

**To export definitions**

1. From X Manager, click **File > Export**.
   The **Export Definitions** dialog box appears.

2. Under **Available Definitions** on the left, select the definitions you want to add to the export .rxd file.
   The definitions that you select are added to the **Definitions Pending Export** list on the right.

3. (Optional) Clear **Automatically include referenced definitions**. Clear this option to export only those items you select under **Available Definitions**.
   When this option is enabled, all referenced definitions are automatically added export list under **Definitions Pending Export**. For example, if you select a client definition for export, the session, font, keyboard, and color scheme definitions referenced by that client definition are also added to the export list.

4. (Optional) Clear the check box **Remove passwords from exported definitions**. (By default, stored password strings are removed from the definitions you are exporting.)

5. Click **Export**.
   All definitions on the **Definitions Pending Export** list are exported.

6. From the **Select Export File** dialog box, specify the name and location of the file to which definitions are exported.

7. Click **Save** to complete the export process.
Import a Definition

You can import definitions from an .rxd definition file into your active product database (the local database when using the standalone X Manager, or the domain database when using X Manager for Domains).

To import definitions

1. From X Manager, click File > Import.
2. From the Select Definition File dialog box, locate and open an .rxd definition file.
3. The Import Definitions dialog box appears.
4. Under Available Definitions on the left, select the definitions you want to import. The definitions that you select are added to the Definitions Pending Import list on the right.
5. (Optional) Select Automatically include referenced definitions. This ensures that related definitions stay together when transferred. When this option is enabled and you select an available definition that references other definitions, all of the related definitions are added to the Definitions Pending Import list. For example, if you select a client definition for import, the session definition used by that client is also added to the Import list — provided the referenced definition is present in the .rxd file. This feature is particularly helpful if your sessions reference custom fonts, keyboards, or color schemes.
6. Click Import. All definitions on the Definitions Pending Import list are imported.

NOTE: If a conflict is detected, the Import Conflicts Found dialog box appears. In this case, choose Resolution options to resolve each definition conflict that is presented. After all conflicts have been addressed, the pending import definitions will be processed based on your selections.

NOTE: In domain mode, when you import settings, they are available for your use as private settings definitions. If you are a domain administrator, you can use the Administrative Console to make your imported private definitions public. Public definitions are visible and usable by all users in the domain.

Import Installed Templates

If templates are available on your system, the Import Migrated Settings and Templates (page 69) dialog box opens the first time you start X Manager or X Manager for Domains. This dialog box does not open again; and it does not open at all after an upgrade from an earlier version. Use this procedure to import templates manually.

NOTE: If you are running on Windows, you can confirm that the templates are installed using the Windows Programs and Features Control Panel. Select your installed Reflection product and click Change. On the Feature Selection tab, under Reflection X Advantage confirm that the items under Templates are installed.

To import templates after your initial startup

1. From X Manager or X Manager for Domains, click File > Import.
2. Browse to the templates folder. This is located in the product installation folder. For example:
Select the template files (*.rxd) you want to import.

In the **Import Definitions** dialog box, click ![select all] to select all the definitions.

Click **Import**.

**Import Migrated Settings**

The first time you X Manager or X Manager for Domains, your legacy settings are migrated and saved to a “definition file” on page 255 and the **Import Templates and Migrated Settings** (page 69) is displayed. This dialog box does not display again. Use this procedure to import migrated settings you did not select during the initial startup.

To import migrated settings from a definition file:

1. From X Manager or X Manager for Domains, click **File > Import**.
2. Browse to your Windows user profile folder (page 258) to locate the definition file that contains your migrated settings. The definition file name identifies the product and version whose settings were migrated.
   
   On most Windows operating systems the default location is:
   
   `\Users\<user>\Documents\.attachmate\rx\migration\`
   
   On Windows XP, the default location is:
   
   `\Documents and Settings\<user>\.attachmate\rx\migration\`
3. In the **Import Definitions** dialog box, click ![select all] to select all the definitions.
4. Click **Import**.

**Enable or Disable Extensions**

Whether or not the X server supports extensions sometimes affects client behavior. Clients may paint better, run faster, or avoid other problems by changing which extensions are enabled.

To enable or disable extensions from X Manager or the Administrative Console

1. (Administrative Console only) Click the **Domain Definitions** tab.
2. Under **Session Definitions** on the left, select a session definition.
3. Click the **Extensions** tab.
4. In the **Available Extensions** list, select or clear extensions as required.

**Configure Compression**

Enabling compression may improve performance where your network connection is limited by low bandwidth.

When remote session services are enabled, session components are set up on a remote computer. This can be on the X client host or on a nearby computer (as shown in this diagram). With this configuration, protocol that passes between the domain node and your workstation is compressed. (Protocol that passes between the client and the domain node is not compressed.)
Before you begin

Configure support for remote session services:

- If you are connecting from standalone X Manager, see "How to Configure a Distributed Session in Standalone Mode" on page 147.
- If you are connecting from X Manager for Domains, see "Domain Setup: Improve Performance Over a Slow Network" on page 163.

To enable compression

1. Start X Manager or X Manager for Domains.
2. Select the session definition you will use for this connection. On the General tab, under Remote session services, select any option other than none.
3. Click the Advanced tab. For Compress protocol to remote X server displays, select one of the following settings:

   - **Dynamic** (Default) Reflection X Advantage measures the bandwidth of data traveling from the protocol router to each remote X server and automatically compresses the protocol when the bandwidth is low enough to be likely to affect performance.
   - **Always** This option may provide better performance where CPU and memory resources are less limiting than bandwidth.
   - **Never** This option may improve performance if bandwidth is less limiting than CPU or memory.

Set Up Secure Shell (SSH) Connections

Reflection X Advantage uses Secure Shell by default for client definitions. To connect using Secure Shell, the computer running your X client must also be running a Secure Shell server. You can use installed sample definitions to get started:

- Launch an X Client Application Using the Sample Definitions. (page 22)

To configure non-default Secure Shell settings:

- Use the Advanced Secure Shell Settings (page 72) dialog box.

How it works

Reflection X Advantage performs the following actions when it establishes a Secure Shell connection.
NOTE: In the context of the Secure Shell protocol, Reflection X Advantage — an X server — acts as a client. The Secure Shell server resides on the same host that’s running the X client application. Reflection X Advantage runs as a Secure Shell client that must authenticate the Secure Shell server, and must authenticate to this server as a client.

1. Establish a secure connection
   Reflection X Advantage negotiates with the Secure Shell server running on the X client host. This negotiation establishes a shared key and cipher to use for session encryption, and a hash to use for data integrity checking.

2. Authenticate the host (page 61)
   The host sends identifying information to Reflection X Advantage to confirm its identity. By default, Secure Shell servers send the public key of a public/private key pair. Secure Shell servers can also be configured to use X.509 certificates for authentication. If you connect to hosts with this configuration, you can install and configure PKI Services Manager (page 235) to support certificate validation.

3. Authenticate the user (page 63)
   The user sends identifying information to the Secure Shell server to confirm the user's identity. By default, this is done by entering a password or passphrase. You can also configure Reflection X Advantage to use public keys or certificates for user authentication.

4. Forward X11 communications through a secure tunnel
   A secure tunnel is established between Reflection X Advantage and the X client host. All X11 data is sent securely through this tunnel.

Host Authentication for Secure Shell Sessions

Host authentication enables Reflection X Advantage to reliably confirm the identity of the host on which an X client is running. Reflection X Advantage supports host authentication using public keys or certificates.

Public Key Authentication

By default, Secure Shell servers use public key authentication. For this authentication, the server sends the public key of a public/private key pair to establish its identity. The first time you make a Secure Shell connection to a host, you see the Host Key Unknown dialog box because the key sent by the host is unknown to Reflection X Advantage. You can add the key to a list of trusted hosts in the Reflection X Advantage database. Once a key is added to the list, the stored key is used for subsequent authentication, which means you won’t see the Host Key Unknown dialog box again when you make connections to this host.

To add a new host key to the trusted host list
   - Manually import the host key using the Import Host Key dialog box (page 62).
   -or-
   - In response to a Host Key Unknown prompt, click Always (page 62).

NOTE: If you run Reflection X Advantage in Domain mode, the domain administrator can install a host key in the domain database and make it available to all domain users. Doing this avoids the potential confusion and security risk of having users respond to the Host Key Unknown prompt. For details, see “Add a Trusted Host Key for all Domain Users” on page 177.
Certificate Authentication

Like public key authentication, certificate authentication uses public/private key pairs to verify the host identity. However, with certificate authentication, public keys are contained within digital certificates. The host obtains a certificate and an associated private key from a Certificate Authority (CA). The certificate is sent to the client during the authentication process. To verify the integrity of the information coming from the host, the client must establish that the certificate is valid. Reflection X Advantage uses a utility called PKI Services Manager (page 235) to perform certificate validation services. If you are connecting to X client hosts that use certificates for host authentication, you can download this free utility from the Micro Focus website.

Add Trusted Host Keys to the Database

Trusted host keys authenticate a Secure Shell server. If the host's public key has not previously been installed in the host key database, the first time you makes a Secure Shell connection, you see the Host Key Unknown dialog box. This dialog box includes a fingerprint that identifies the Secure Shell host. To be sure that this is the correct host, you can contact the Secure Shell server system administrator who can confirm that this is the correct fingerprint. Without confirmation, there is a risk of a "man-in-the-middle" attack, in which another server poses as the Secure Shell server.

Use this procedure to add an unknown key to the database. Once a key is stored in the Reflection X Advantage database, the stored public key is used for subsequent authentication, which ensures a connection to the correct host. Once the key is saved you won’t see the Host Key Unknown dialog box when you make subsequent connections.

To add a host key to the database

1. From X Manager, configure an X client that uses Secure Shell as the connection method.
2. Start the client.
   
   The first time you connect, you are prompted with the Host Key Unknown dialog box.
3. Click Always to add the host key database.

NOTE: In the context of the Secure Shell protocol, Reflection X Advantage — an X server — acts as a client. The Secure Shell server resides on the same host that's running the X client application. Reflection X Advantage runs as a Secure Shell client that must authenticate the Secure Shell server, and must authenticate to this server as a client.

Manually Import a Trusted Host Key

Use this procedure if you have a copy of a host key and want to manually import it into the database.

To import a trusted host key and add it to the Trusted Host Keys list

1. From X Manager, go to Tools > Secure Shell Host Keys.
2. At the top of the Trusted Host Keys list, click the plus sign (+).
   
   The Import Host Key dialog box appears.
3. Enter the Host name.
4. Specify the location of the host's public key file.
5. Click Import.
Configure Host Authentication Using Certificates

Reflection X Advantage uses a utility called PKI Services Manager (page 235) to perform certificate validation services. If you are connecting to X client hosts that use certificates for host authentication, you can download this free utility from the Micro Focus website.

The following procedure outlines the basic steps that need to be performed by an administrator to support host authentication using certificates. Use the links to view procedure details.

To configure host authentication using certificates

**NOTE:** PKI Services Manager can be installed and configured in a central location for access by multiple users (steps 1 and 2). Once this is done, all Reflection X Advantage users can connect to that PKI Services Manager server (step 3). In domain mode, individual users don't need to configure this connection; the domain administrator uses the Administrative Console to configure a single connection to PKI Services Manager that is available to all domain users.

1. Install PKI Services Manager on Windows (page 236) or UNIX (page 240).
2. Configure PKI Services Manager on Windows (page 237) or UNIX (page 241). You will install trusted certificates, configuring certificate revocation checking, and designate which hosts can authenticate with a valid certificate.
3. "Configure Reflection X Advantage to Connect to PKI Services Manager" on page 243.

User Authentication for Secure Shell Sessions

User authentication enables the Secure Shell server to reliably confirm the identity of the Reflection X Advantage user.

Reflection X Advantage supports three methods of user authentication: public key (including X.509 certificates), keyboard interactive, and password. By default all three methods are allowed — new Secure Shell sessions first try to authenticate by public key method, then try the keyboard interactive method, and finally use a password prompt. To change the allowed authentication methods, use the Authentication (page 74) tab of the Advanced Secure Shell Settings dialog box.

Password and Keyboard Interactive Authentication

Both of these authentication methods prompt the user for information during the connection process. With password authentication the prompt will always be for the user password. With keyboard Interactive authentication the prompts depend on the host and may include a simple password prompt or may ask for other information. Both of these authentication methods are available by default and require no additional configuration.

Public Key Authentication

With public key authentication, the user holds a public/private key pair and sends the public key to the host during the authentication process. You can create key pairs using Reflection X Advantage. You also need to upload your public key to the host and configure the server to use this key for user authentication. For more information, see “Configure User Key Authentication” on page 64.

Certificate Authentication

Like public key authentication, certificate authentication uses public/private key pairs to verify the host identity. However, with certificate authentication, public keys are contained within digital certificates. Reflection X Advantage supports user certificate authentication. To configure this, you need access to a personal certificate and its corresponding private key.
You can configure Reflection X Advantage to authenticate using any of the following:

- Certificates you have imported into the Reflection X Advantage database.
- Personal certificates in the Windows Certificate Store.
- Certificates stored on PKCS#11 (page 256)-compliant hardware devices such as smart cards or USB tokens.

To use certificate authentication, you need to configure both Reflection X Advantage and the Secure Shell server on the host computer. For more information, see "Configure User Certificate Authentication" on page 65.

Configure User Key Authentication

Public key user authentication is an optional feature of the Secure Shell protocol. To configure user authentication, you must use X Manager to configure user keys and then configure the Secure Shell Server to accept these keys.

To create new user keys

1. Launch X Manager or X Manager for Domains.
2. From the Tools menu, select Secure Shell User Keys.
3. By default Reflection X Advantage Store is selected under User Key Sources.
   - To store keys in the Reflection X Advantage database, leave this option selected.
   - To store keys in a local directory, click the plus sign (+) and select Add local directory. For Directory, enter or browse to the local directory. Because this location contains a user's private keys it should be a location that is readable only by the user who authenticates with these keys.
4. Click Generate.
5. Specify a name that identifies the key pair you are creating.
6. (Optional) Change the key algorithm type and/or key length.
7. Enter a passphrase (page 256) for this key. You will need to enter this passphrase when the key is used for authentication.

   CAUTION: To help ensure security, all user keys should be passphrase protected. If you don’t specify a passphrase, the private key is stored in unencrypted form in the key store, and anyone who gains access to the key can authenticate using it. In standalone mode keys are stored on the same computer as X Manager. In domain mode, keys in the Reflection X Advantage Store are stored in the database on the domain controller and the administrator of that computer will be able to read these keys.

8. Retype the passphrase.
9. Click OK.

   The key is added to the selected key store.

To add an existing key to your key store

1. In the Secure Shell User Keys dialog box, click Import.

   NOTE: If you are using a local directory, it is possible to copy keys manually to your directory, but using the Import feature is recommended because Reflection X Advantage sets correct permissions on imported keys and ensures that the key uses a supported file format.
2 Browse to locate the key you want to add.

3 For **File passphrase** enter the passphrase that currently protects the file. This is required to decrypt the file and import the key.

4 Specify a **Key name** to identify this key in the User Keys list.

5 Enter a value for **Key passphrase**. This can be the same as the original file passphrase or different.

6 Click **Import**.

**To configure the host**

1 From the **X Manager Secure Shell User Keys** dialog box, select the key you just created, and then click **Export**.

2 Specify the name and location you want to use for the exported public key file.

3 Specify a key file format. Two formats are available. SecSH format is used by Reflection products, F-Secure, and SSH Corporation. OpenSSH format is used in OpenSSH implementations.

4 Click **Export**.

5 Copy the public key you just exported to the public key location used by the Secure Shell server running on the host. Configure the server to allow public key authentication and to accept this key.

   Procedures for doing this vary between Secure Shell servers. For details, refer to your Secure Shell server documentation.

**NOTE:** In the context of the Secure Shell protocol, Reflection X Advantage — an X server — acts as a client. The Secure Shell server resides on the same host that's running the X client application. Reflection X Advantage runs as a Secure Shell client that must authenticate the Secure Shell server, and must authenticate to this server as a client.

**Configure User Certificate Authentication**

User certificate authentication (a variation of public key authentication) is an optional feature of the Secure Shell protocol. Both **X Manager** and the Secure Shell server need to be configured to support this.

You can configure Reflection X Advantage to authenticate using any of the following:

- Certificates you have imported into the Reflection X Advantage database.
- Personal certificates in the Windows Certificate Store.
- Certificates stored on **PKCS#11 (page 256)**-compliant hardware devices such as smart cards or USB tokens.

The procedures in this section describe how to configure Reflection X Advantage for each of these certificate stores. After you complete the procedure, you can connect to hosts that have been configured to support certificate authentication.
NOTE

- To help ensure security, you should always specify a passphrase when you use certificates for user authentication. You will need to enter the passphrase each time you connect to the host.
- If you have multiple certificates configured, the first time you connect to a host you may be prompted to select a certificate from a list of available certificates. After your first successful connection, Reflection X Advantage will automatically attempt subsequent connections using the same certificate.

Authenticate with Certificates in the Reflection X Advantage Store

Use this procedure to configure Reflection X Advantage Secure Shell sessions to authenticate users with certificates stored in the Reflection X Advantage store.

NOTE: The Secure Shell server administrator must configure the server to accept and validate user certificates. The procedure depends on the server. Refer to the Secure Shell server documentation for details.

Before you begin:

Obtain a personal certificate from a certificate-granting authority and copy it to a secure location on the computer running X Manager. Private keys and PKCS#12 packages should be placed in a folder that is readable only by the owner.

You can use:

- A certificate file and its associated private key. The two files must be in the same location and the certificate must have the same name as the key with a *.cer or *.crt file extension.
- or-

- A PKCS#12 (page 256) package file (*.p12, or *.pfx) that contains both the certificate and its associated private key.

You will also need to know the passphrase that has been used to protect the private key or certificate package file.

To authenticate with a certificate in the Reflection X Advantage store

1. Launch X Manager or X Manager for Domains.
2. From the Tools menu, select Secure Shell User Keys.
3. Click Import.
4. Browse to locate the private key file or certificate.
5. For File passphrase enter the passphrase that currently protects the file. This is required to decrypt the file and import the key.
6. For Key name enter a name for this certificate. This name shows up in the list of user keys and also appears in the prompt a user sees when this certificate is used to make a connection.
7. Enter a value for Key passphrase. This can be the same as the original file passphrase or different.

CAUTION: To help ensure security, you should always specify a passphrase when you import a certificate. This passphrase protects the private key associated with the certificate. If you don’t specify a passphrase, the private key is stored in unencrypted form in the Reflection X database, and anyone who gains access to the private key can authenticate using it. In standalone mode
keys are stored on the same computer as X Manager. In domain mode all user keys are stored in
the database on the domain controller and the administrator of that computer will be able to read
these keys.

8 Click **Import**.

The imported certificate is added to the **User Keys** list. As long as you leave **Reflection X
Advantage Store** in the list under **User Key Sources**, Reflection X Advantage attempts to use
certificates in this list when it connects to a host that supports certificate authentication.

### Authenticate with Certificates in a Local Directory

Use this procedure to configure Reflection X Advantage Secure Shell sessions to authenticate users
with certificates stored locally (on the computer running X Manager or X Manager for Domains).

**NOTE:** The Secure Shell server administrator must configure the server to accept and validate user
certificates. The procedure depends on the server. Refer to the Secure Shell server documentation
for details.

**Before you begin**

Obtain a personal certificate from a certificate-granting authority and copy it to a secure location on
the computer running X Manager. Private keys and PKCS#12 packages should be placed in a folder
that is readable only by the owner.

You can use:

- A certificate file and its associated private key. The two files must be in the same location and the
certificate must have the same name as the key with a *.cer or *.crt file extension.

  -or-

- A [PKCS#12](page 256) package file (*.p12, or *.pfx) that contains both the certificate and its
associated private key.

You will also need to know the passphrase that has been used to protect the private key or certificate
package file.

**To authenticate with a certificate in a local directory**

1. Launch X Manager or X Manager for Domains.
2. From the **Tools** menu, select **Secure Shell User Keys**.
3. Next to **User Key Sources** click the plus sign (+) and select **Add Local Directory**.
4. For **Directory**, specify the directory you want to use as for your store. Because this location
contains a user's private keys it should be a location that is readable only by the user who
authenticates with these keys.
5. Click **Import**.

**NOTE:** Using the **Import** feature is recommended for adding keys to your directory. Reflection X
Advantage sets correct permissions on imported keys and ensures that the key uses a
supported file format.

6. Browse to locate the private key file or certificate.
7. For **File passphrase** enter the passphrase that currently protects the file. This is required to
decrypt the file and import the key.
8 For **Key name** enter a name for this certificate. This name shows up in the list of user keys and also appears in the prompt a user sees when this certificate is used to make a connection.

9 Enter a value for **Key passphrase**. This can be the same as the original file passphrase or different.

**Authenticate with Certificates in the Windows Certificate Store**

If you are running on Windows, you can configure Reflection X Advantage Secure Shell sessions to authenticate using personal certificates in the Windows certificate store.

**NOTE**

- The certificate in the Windows store must use an RSA key pair; DSA keys are not supported.
- The Secure Shell server administrator must configure the server to accept and validate user certificates. The procedure depends on the server. Refer to the Secure Shell server documentation for details.

**Before you begin**

Confirm that the required RSA certificate is installed in your Windows Personal store. (You can view and manage certificates from the Windows Control Panel using ![Internet Options > Content > Certificates > Personal](Image).)

**To use a certificate in the Windows Certificate Store**

1. Launch X Manager or X Manager for Domains.
2. From the **Tools** menu, select **Secure Shell User Keys**.
3. Next to **User Key Sources** click the plus sign (+) and select **Add Windows Certificate Store**.

The certificates list displays any certificates you have in your Windows personal certificate store. As long as you leave **Windows Certificate Store** in the list under **User Key Sources**, Reflection X Advantage attempts to use these when you connect to a host that supports certificate authentication.

**Authenticate using Smart Cards or other PKCS#11-compliant Devices**

Use this procedure to configure Reflection X Advantage Secure Shell sessions to authenticate using PKCS#11 (page 256)-compliant hardware devices such as smart cards or USB tokens.

**NOTE**

- PKCS#11 is not supported in the 64-bit version of Reflection X Advantage.
- The Secure Shell server administrator must configure the server to accept and validate user certificates. The procedure depends on the server. Refer to the Secure Shell server documentation for details.

**Before you begin**

Install the software supplied by your card or token provider. You will need to know the name and location of the library file (*.dll or *.so) used by that provider to provide access to your hardware device. On Windows, this is typically installed to the Windows system folder. You may need to contact the device manufacturer to determine the correct file.

**To configure authentication using a smart card or other PKCS#11-compliant device**

1. Launch X Manager or X Manager for Domains.
2 From the **Tools** menu, select **Secure Shell User Keys**.

3 Next to **User Key Sources** click the plus sign (+) and select **Add PKCS#11 Provider**.

   An item called "PKCS#11 Provider" is added to your list of certificate stores. You can edit this provider name.

4 For **Library**, specify the full path to the library file (*.dll or *.so) used by your device software.

---

**NOTE**

- In order to view the certificates or authenticate with your device, you will need to enter information (such as a PIN) required by the provider.
- The first time you make a connection, you see two entries to authenticate with your device. The first entry is for authentication using the certificate in your device. The second entry is for standard public key authentication using the public key associated with that certificate. Authentication using the public key entry requires that your key be added to the server's list of authorized keys.

---

**User Interface Reference**

Use the topics in this section to understand the features and functionality provided by the different areas in X Manager and X Manager for Domains.

**In this Section**

- “Import Migrated Settings and Templates dialog box” on page 69
- “Client Definition” on page 70
- “XDMCP Connection Definition” on page 85
- “Launch Group Definition” on page 86
- “Session Definition” on page 87
- “Offered and Joined Sessions” on page 123
- “Menus” on page 123
- “Toolbar” on page 143
- “Task Status Pane” on page 143

**Import Migrated Settings and Templates dialog box**

The **Import Migrated Settings and Templates** dialog box opens on initial startup if migrated settings and/or templates are available on your system. This dialog box opens the first time you start X Manager. If you run X Manager for Domains, it opens the first time you log onto any available domain.

This dialog box includes a list of sample connection settings for different host types. You can deselect the settings for host types you don't use. If you're not sure which host types you need, you can import them all and delete the ones you don't need later.

Migrated settings may also be available for import if you are running on a system where a prior version of Reflection X (for example 13.x or 14.x) or Hummingbird Exceed was installed. You can import these settings now or later. Importing these settings into Reflection X Advantage has no effect on your original settings file.
| **Import** | Imports settings for the selected items. |
| **Cancel** | Closes the dialog box without adding any of the listed templates or migrated settings. |

**NOTE**

- This dialog box displays only on initial startup, but it is possible to manually import templates and migrated settings later if you do not import them on initial startup.
- Sample templates for different host types are included if you installed the "Templates" feature when you installed Reflection X Advantage. This feature is included in a default installation, and by default includes templates for a variety of host types.

---

**Client Definition**

The **Client Definition** pane appears whenever you create or select a definition under **X Clients**. Use this pane to specify settings for launching an X client on a remote host.

| **Name** | A descriptive name for this client definition. |
| **Host name** | The name or address of the X client host computer. You can enter the IP address of the host (for example, 123.12.23.4), or, if you are using a domain name server for address resolution, you can enter just the host name. If you leave this blank, you are prompted for a host name when you start the connection. |
| **Host type** | Sets default values appropriate for the selected host type. The host type you select affects: |
| | - The syntax and selection of sample commands shown in the **Command** drop-down list. |
| | - The default login sequence. |
| | - The default xauth command, which is used when user-based authorization is enabled for a session. |
| | **NOTE:** Two Linux options are available. Use the Legacy option for older Linux systems that store X client applications in `/usr/x11R6/bin`. (Newer systems use `/usr/bin`). |
| **Connection method** | The protocol used for the connection. The options are: |
| | - Secure Shell (page 72) (the default) |
| | - Telnet (page 76) |
| | - Rexec (page 80) |
| | - Rlogin (page 81) |
| | - Rsh (page 82) |
| | - Remote Session Services (page 83) (standalone X Manager only) |
| **User name** | Your user name on the host. If you omit this, you are prompted to enter your user name when you make a connection. |
| **Password** | Your password on the host. If you leave this blank, you are prompted for a host name when you start the connection. This option is available only when **Connection Method** is Telnet, Rexec, or Rlogin. |
| | **NOTE:** The password is replaced by asterisks in the display, but is saved as clear text in the database.
You can use the macros listed below to provide information in a host command.

**NOTE:** The Command field in the Client Definition pane includes a drop-down list that shows sample commands that demonstrate the use of macros. The sample commands change when you change the Host type to show examples that typically work with the selected host type.
### Specifying a screen number

To specify a screen number, add the screen number to the `%IP#` macro. For example, `%IP#2%` for screen 2. The following command line configures an xterm display on screen 2.

```bash
/usr/bin/X11/xterm -display %IP#2%
```

### Secure Shell Connection Method

Secure Shell (also called SSH) is the default connection method. The Secure Shell protocol provides a secure alternative to Telnet, rexec, rlogin, or rsh. Secure Shell connections require both host and user authentication, and all communications pass between hosts over an encrypted communication channel.

Saved passwords are not supported for Secure Shell connections. Depending on how your host is configured, you may see a simple password prompt when you connect, or you may be prompted for addition information.

The Secure Shell protocol also supports the use of public/private key pairs or certificates for user authentication. For details, see Set Up Secure Shell Connections (page 60).

### Advanced Secure Shell Settings

#### Getting there

**From the Administrative Console and X Manager**

1. (Administrative Console only) Click the **Domain Definitions** tab.
2. Under **X Clients** on the left, select a client definition.
3. Set **Connection Method** to **Secure Shell**.
4. Click the **Advanced** button.

---

### Macro Expands to

<table>
<thead>
<tr>
<th>Macro</th>
<th>Expands to</th>
</tr>
</thead>
<tbody>
<tr>
<td>%IP%</td>
<td>IP address of the display.</td>
</tr>
<tr>
<td>%IP#%</td>
<td>IP address and display number.</td>
</tr>
<tr>
<td>%#%</td>
<td>Display number only. Using the display number alone (without either IP or HN) is not supported for Secure Shell connections with X11 forwarding enabled (the default).</td>
</tr>
<tr>
<td>%HN%</td>
<td>Host name of the display.</td>
</tr>
<tr>
<td>%HN#%</td>
<td>Host name and display number.</td>
</tr>
<tr>
<td>%T%</td>
<td>The client definition name as specified on the Client Definition pane in the Name field.</td>
</tr>
<tr>
<td>%USER%</td>
<td>User name on the client host.</td>
</tr>
<tr>
<td>%PASSWORD%</td>
<td>User password on the client host. Not supported for Secure Shell connections.</td>
</tr>
<tr>
<td>%C%</td>
<td>This option is supported when user-based authorization is enabled. It is typically used to configure the xauth command that places an MIT cookie in the user’s .XAuthority file. It expands to the authorization protocol name and hex encoded authorization data (example: MIT-MAGIC-COOKIE-1 c48da9bfcd34ed8050e4d3910bf1675e).</td>
</tr>
</tbody>
</table>
Use the following tabs to configure Secure Shell settings:

- General (page 73)
- Authentication (page 74)
- Encryption (page 75)
- SOCKS Proxy (page 76)
- Proxy (page 75)

**NOTE:** These settings are client-specific.

### General Tab - Advanced Secure Shell Settings

**Getting there**

**From the Administrative Console and X Manager**

1. (Administrative Console only) Click the **Domain Definitions** tab.
2. Under **X Clients** on the left, select a client definition.
3. Set **Connection Method** to **Secure Shell**.
4. Click the **Advanced** button.
5. Click the **General** tab.

The options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Enter the port number on which the SSH server is listening. The default is 22.</td>
</tr>
<tr>
<td>Enable Secure Shell compression</td>
<td>Compress all data (including stdin, stdout, stderr, and data for forwarded X11 connections) using Zlib compression.</td>
</tr>
<tr>
<td>Tunnel X11 connections</td>
<td>Automatically forward all data sent from the remote X11 port through the secure tunnel to the correct local port.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> The xauth command options are not available when <strong>Tunnel X11 connections</strong> is enabled (the default).</td>
</tr>
<tr>
<td>Use alternate xauth command</td>
<td>Select this option to configure an alternate xauth command. The xauth command affects sessions in which <strong>Network Security (page 100) &gt; User-based authorization</strong> is enabled.</td>
</tr>
<tr>
<td>Xauth command</td>
<td>Specify an alternate command to place an MIT cookie in the .XAuthority file in the user’s home directory.</td>
</tr>
<tr>
<td></td>
<td><strong>Macros (page 71)</strong> are supported. For example, in the following command, %IP#% provides the IP address and display number, and %C% specifies MIT-MAGIC-COOKIE-1 authorization and provides the required hex encoded authorization data.</td>
</tr>
<tr>
<td></td>
<td><code>xauth add %IP#% %C%</code></td>
</tr>
<tr>
<td>Quiet mode</td>
<td>This option is available only when <strong>Use alternate xauth command</strong> is selected.</td>
</tr>
<tr>
<td></td>
<td>Suppress banner messages sent by the host.</td>
</tr>
</tbody>
</table>
Authentication Tab - Advanced Secure Shell Settings

Getting there

From the Administrative Console and X Manager

1. (Administrative Console only) Click the Domain Definitions tab.
2. Under X Clients on the left, select or add a client definition.
3. Set Connection Method to Secure Shell.
4. Click the Advanced button.
5. Click the Authentication tab.

The options in this tab apply to Secure Shell sessions, and determine how host and user authentication are negotiated for the X client definition you are currently configuring.

Host authentication

Specify which authentication methods Reflection X Advantage can use to authenticate the host, and in what order.

In most cases, you don't need to modify the default configuration. However, if the host you are connecting to is configured to support both public key and certificate authentication and you haven't configured Reflection X Advantage to validate host certificates, you may see an error message saying "No PKI server configured". To resolve this problem without configuring PKI Services Manager, clear the X.509 certificate option or move it to the bottom of the list. Secure Shell protocol allows only one attempt to authenticate the host. By forcing public key authentication first, you can authenticate to the host using its public key.

X.509 certificate enables the following host authentication methods, which are attempted in this order: x509v3-rsa2048-sha256, x509v3-sign-rsa, x509v3-sign-dss.

SSH Public key enables the following host authentication methods, which are attempted in this order: ssh-rsa-sha2-256@attachmate.com, ssh-rsa, ssh-dss.

User authentication

Specify one or more user authentication methods (Public key, Keyboard interactive, and Password) in order of preference.

Secure Shell protocol allows multiple attempts at user authentication. Reflection X Advantage attempts the selected authentication methods in order from top to bottom until the connection is successful or all supported methods have failed.

NOTE: Public key authentication requires configuration on both Reflection X Advantage and the host.

Always prompt for user key during public key authentication

This setting is relevant if you have configured authentication using public keys or certificates and more than one key or certificate is available. (This option is not available from the Administrative Console.)

When this setting is cleared, Reflection X Advantage displays a list of available keys only if you have not previously connected to a host. After you make a successful connection, Reflection X Advantage automatically uses the successful key or certificate for subsequent connections.

When this setting is selected, Reflection X Advantage always shows the list of available keys and certificates.
Encryption Tab - Advanced Secure Shell Settings

Getting there

From the Administrative Console and X Manager

1. (Administrative Console only) Click the Domain Definitions tab.
2. Under X Clients on the left, select a client definition.
3. Set Connection Method to Secure Shell.
4. Click the Advanced button.
5. Click the Encryption tab.

Use the settings on the Encryption tab to configure the encryption algorithms available for use by the Secure Shell connection, and define the order of preference for their use.

Use the arrow buttons to move a selected algorithm up or down in the list.

Cipher Algorithms

Specify one or more cipher algorithms to use for encrypting the session, in order of preference. The cipher used for a session is the first item in this list that is also supported by the server.

NOTE: If FIPS mode is enabled, the list of available cipher algorithms is restricted to FIPS-compatible algorithms.

HMAC Algorithms

Specify a series of HMAC (hash-based message authentication code) algorithms, in order of preference. Secure Shell connections use HMACs to ensure data integrity. The client and server independently compute a hash for each packet of transferred data. If the message has changed in transit, the hash values are different and the packet is rejected. The HMAC used for a session is the first item in this list that is also supported by the server.

NOTE: If FIPS mode is enabled, the list of available MAC algorithms is restricted to FIPS-compatible algorithms.

Key Exchange Algorithms

Specify one or more key exchange algorithms by which the client and server negotiate a shared session key, in order of preference.

Proxy Tab - Advanced Secure Shell Settings

Getting there

1. Launch a session from the Management and Security Server Administrative WebStation.
2. Under X Clients on the left, select a client definition.
3. Set Connection Method to Secure Shell.
4. Click the Advanced button.
5. Click the Proxy tab.

This tab is available for client configuration if you use Management and Security Server (available separately from Micro Focus) to manage sessions and you launched the session from the Administrative WebStation.
Use Reflection security proxy
Configure this client to use the Reflection Security Proxy for the server connection.

Security proxy
The drop-down list shows available servers.

Proxy port
The drop-down list shows available ports.

Proxy cipher suites
A read-only list of cipher suites supported by this Reflection proxy host and port.

Socks Proxy Tab - Advanced Secure Shell Settings

Getting there

From the Administrative Console and X Manager

1. (Administrative Console only) Click the Domain Definitions tab.
2. Under X Clients on the left, select a client definition.
3. Set Connection Method to Secure Shell.
4. Click the Advanced button.
5. Click the Socks Proxy tab.

SOCKS proxy support is available for Secure Shell Connections on a per client basis.

<No SOCKS Proxy> When <No SOCKS Proxy> is selected, SOCKS is not enabled. (This is the default.)
To enable SOCKS for this X client definition, select an available proxy from the list.

Configure
Opens the SOCKS Proxies (page 141) dialog box, which you can use to add new proxy servers to the list of available proxies, or modify the settings of existing proxies.

Restore Defaults
Restores the default <No SOCKS Proxy> setting for this client connection. This button has no effect on the list of configured proxies.

Client Definition - Telnet Connection Method

When Telnet is the selected protocol, you can save both your username and password.

NOTE: The password is replaced by asterisks in the display, but is saved as clear text in the database.

You can use Advanced Telnet Settings (page 77) if you need to modify the command sequence used for logging into the host.

NOTE: Telnet is not available if you are running in FIPS mode.

The following additional option is available for this connection type when Application is set to Multiple commands.
Prompt  Specifies the host prompt for this command. Enter a host prompt or keep the default setting, `%prompt%`, which accepts multiple host prompts. To view or modify the value of `%prompt%`, click Advanced and configure the Command prompt option.

If Optional is selected, and the host does not display the specified prompt, Reflection X Advantage skips to the next command line.

Advanced Telnet Settings - Client Definition

Getting there

From the Administrative Console and X Manager

1. (Administrative Console only) Click the Domain Definitions tab.
2. Under X Clients on the left, select a client definition.
3. Set Connection Method to Telnet.
4. Click the Advanced button.

Use the settings in this dialog box to configure the string that precedes the command that launches the X client.

**Port**

The default port number is 23.

**Use alternate login sequence**

When cleared (the default), the default Telnet sequence is used for the selected host type; when selected, configure the strings for Telnet.

NOTE: To reset the default login sequence, clear this check box.

**Commands**

Specify one or more commands to use as the alternate sequence for starting the X client. This option is available only when Use alternate login sequence is selected.

**Prompt**

Use a regular expression to specify the sequence preceding the response. Typically this is a username and password prompt.

**Response**

Specify the response to send to the host when the corresponding prompt is detected. A carriage return is automatically appended to the prompt response you enter.

**Optional**

Clear to have Reflection X fail the login attempt if the host prompt is not displayed; select to have Reflection X skip to the next line of the script if the host does not display the specified prompt — Reflection X will send the response that corresponds to whichever prompt is recognized first.
**Command prompt**

Use a regular expression to specify the expected host command prompt. This is the string that is used when the **Prompt** column in the main panel of the X Client Definition pane lists `%prompt%`. It is not necessary for a prompt string to be complete — just enter as much of the latter part of the string as you need to differentiate it from the other prompts that Reflection X will see. For example, a single colon (:) is not a good prompt because it is used as the final character in too many different prompts (such as Login: and Password:).

To specify multiple possible prompts at a particular point in the login script, separate the alternatives with a vertical bar (|).

**Prompt timeout**

This timeout controls how long to wait for a host prompt to appear when executing the login and application commands. Each time a prompt is matched the timeout is reset.

**Use alternate xauth command**

Select this option to configure an alternate xauth command. The xauth command affects sessions in which Network Security (page 100) > User-based authorization is enabled.

**Xauth command**

Specify an alternate command to place an MIT cookie in the .XAuthority file in the user's home directory.

Macros (page 71) are supported. For example, in the following command, `%IP#%` provides the IP address and display number, and `%C%` specifies MIT-MAGIC-COOKIE-1 authorization and provides the required hex encoded authorization data.

```bash
xauth add %IP#% %C%
```

This option is available only when **Use alternate xauth command** is selected.

**Never close connection**

Select to force the client starter to maintain the connection. When cleared (the default), the host connection closes after sending the X client command(s).

---

### Regular Expression Basic Syntax

You can use regular expressions to specify expected prompts for advanced Telnet and advanced Rlogin settings. The following table includes the basic elements of regular expressions:

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>\ (backslash)</td>
<td>Escape character used to represent characters that would otherwise be a part of a regular expression.</td>
<td>&quot;..&quot; = the period character.</td>
</tr>
<tr>
<td>[abc]</td>
<td>Match any character listed within the brackets.</td>
<td><code>[abc]</code> matches a, b or c.</td>
</tr>
<tr>
<td>\d, \w, and \s</td>
<td>Shorthand character classes matching digits 0-9, word characters (letters and digits) and whitespace respectively. Can be used inside and outside character classes.</td>
<td><code>\[\d\s\]</code> matches a character that is a digit or whitespace.</td>
</tr>
<tr>
<td>\D, \W, and \S</td>
<td>Negated versions of the above. Should be used only outside character classes.</td>
<td>\D matches a character that is not a digit.</td>
</tr>
<tr>
<td>Character</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>\b</td>
<td>Word boundary. Matches at the position between a word character (anything matched by \w) and a non-word character (anything matched by [^\w] or \w) as well as at the start or end of the string if the first or last characters in the string are word characters or an alphanumeric sequence. Use to perform a &quot;whole words only&quot; search using a regular expression in the form of \bword\b. \b also matches at the start or end of the string if the first or last characters in the string are word characters. \B matches at every position where \b cannot match.</td>
<td>\b4\b matches 4 that is not part of a larger number.</td>
</tr>
<tr>
<td>\B</td>
<td>Non-word boundary. \B is the negated version of \b. \B matches at every position where \b does not. Effectively, \B matches at any position between two word characters as well as at any position between two non-word characters.</td>
<td>\B. \B matches b in abc.</td>
</tr>
<tr>
<td>.</td>
<td>(period) Match any single character.</td>
<td>&quot;. &quot; matches x or any other character.</td>
</tr>
<tr>
<td>x</td>
<td>(reg character) Match an instance of character &quot;x&quot;.</td>
<td>x matches x.</td>
</tr>
<tr>
<td>^x</td>
<td>Match any character except for character &quot;x&quot;.</td>
<td>[^a-d] matches any character except a, b, c, or d.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(pipe) Match either the part on the left side, or the part on the right side. Can be strung together into a series of options. The pipe has the lowest precedence of all operators. Use grouping to alternate only part of the regular expression.</td>
</tr>
<tr>
<td>(abc)</td>
<td>(parentheses) Used to group sequences of characters or expressions.</td>
<td>(Larry</td>
</tr>
<tr>
<td>{ }</td>
<td>(braces) Used to define numeric qualifiers</td>
<td>a{3} matches aaa.</td>
</tr>
<tr>
<td>{N,}</td>
<td>Match must occur at least &quot;N&quot; times</td>
<td>z{1,} matches when &quot;Z&quot; occurs at least once.</td>
</tr>
<tr>
<td>{N,M}</td>
<td>Match must occur at least &quot;N&quot; times, but no more than &quot;M&quot; times</td>
<td>a{2,4} matches aa, aaa or aaaa.</td>
</tr>
<tr>
<td>?</td>
<td>(question mark) Makes the preceding item optional or once only. The optional item is included in the match if possible.</td>
<td>abc? matches ab or abc.</td>
</tr>
<tr>
<td>*</td>
<td>(asterisk) Match on zero or more of the preceding match. Repeats the previous item zero or more times. As many items as possible will be matched before trying permutations with less matches of the preceding item, up to the point where the preceding item is not matched at all.</td>
<td>&quot;go*gle&quot; matches ggle, gogle, google, gooogle, and so on.</td>
</tr>
</tbody>
</table>
When Rexec is the selected method you can save both your username and password.

**NOTE:** The password is replaced by asterisks in the display, but is saved as clear text in the database.

Use "Advanced Rexec Settings" on page 80 to modify the xauth command.

**NOTE:** Rexec is not available if you are running in FIPS mode.

### Advanced Rexec Settings

#### Getting there

**From the Administrative Console and X Manager**

1. (Administrative Console only) Click the Domain Definitions tab.
2. Under X Clients on the left, select a client definition.
3. Set Connection Method to Rexec.
4. Click the Advanced button.

The options are:

- **Use alternate xauth command**: Select this option to configure an alternate xauth command. The xauth command affects sessions in which Network Security (page 100) > User-based authorization is enabled.

- **Xauth command**: Specify an alternate command to place an MIT cookie in the .XAuthority file in the user's home directory.

  Macros (page 71) are supported. For example, in the following command, %IP## provides the IP address and display number, and %C% specifies MIT-MAGIC-COOKIE-1 authorization and provides the required hex encoded authorization data.

  ```
  xauth add %IP## %C%
  ```

  This option is available only when Use alternate xauth command is selected.
Rlogin Connection Method

When Rlogin is the selected protocol, you save both your user name and password.

NOTE: The password is replaced by asterisks in the display, but is saved as clear text in the database.

You can use Advanced Rlogin Settings (page 81) if you need to modify the command sequence used for logging into the host.

NOTE

- The Rlogin method is only available when Reflection X Advantage is running on a Windows computer.
- Rlogin is not available if you are running in FIPS mode.

The following additional option is available for this connection type when Application is set to Multiple commands.

Prompt  Specifies the host prompt for this command. Enter a host prompt or keep the default setting, %prompt%, which accepts multiple host prompts. To view or modify the value of %prompt%, click Advanced and configure the Command prompt option.

If Optional is selected, and the host does not display the specified prompt, Reflection X Advantage skips to the next command line.

Advanced Rlogin Settings

Getting there

From the Administrative Console and X Manager

1  (Administrative Console only) Click the Domain Definitions tab.
2  Under X Clients on the left, select a client definition.
3  Set Connection Method to Rlogin.
4  Click the Advanced button.

Use the settings in this dialog box to configure the string that precedes the command that launches the X client.

Use alternate login sequence  When cleared (the default), the default Rlogin sequence is used for the selected host type; when selected, configure the strings for Rlogin.

NOTE: To reset the default login sequence, clear this check box.

Commands  Specify one or more commands to use as the alternate sequence for starting the X client. This option is available only when Use alternate login sequence is selected.

Prompt  Use a regular expression to specify the sequence preceding the response. Typically this is a username and password prompt.
Reflection X Advantage Help

Client Definition - Rsh Connection Method

To use Rsh, you must also configure either an .rhosts file (in your home directory) or a /etc/hosts.equiv file on the host. This file specifies allowed hosts and users. For X Manager, add the computer name and user name of the computer running Reflection X Advantage. For X Manager for Domains, add all computers that are registered as domain nodes. The user for all domain nodes is the user of the computer running X Manager for Domains.

Only a user name, host, and command are required to connect using Rsh, and the command must start an X client.
NOTE

- The Rsh method is only available when Reflection X Advantage is running on a Windows computer.
- Rsh is not available if you are running in FIPS mode.

Advanced Rsh Settings

Getting there

From the Administrative Console and X Manager

1. (Administrative Console only) Click the Domain Definitions tab.
2. Under X Clients on the left, select a client definition.
3. Set Connection Method to Rsh.
4. Click the Advanced button.

The options are:

- **Use alternate xauth command**
  Select this option to configure an alternate xauth command. The xauth command affects sessions in which Network Security (page 100) > User-based authorization is enabled.

- **Xauth command**
  Specify an alternate command to place an MIT cookie in the .XAuthority file in the user's home directory.

  Macros (page 71) are supported. For example, in the following command, %IP#% provides the IP address and display number, and %C% specifies MIT-MAGIC-COOKIE-1 authorization and provides the required hex encoded authorization data.

  ```
  xauth add %IP#% %C%
  ```

  This option is available only when Use alternate xauth command is selected.

Remote Session Services Connection Method

This connection method is available for the standalone X Manager only.

Setting Connection method to "Remote Session Services" has the following effects:

- Protocol sent from the client connector to the protocol router is encrypted using the cipher specified for Encrypt protocol to remote X server displays using cipher (page 116).
- This option lets you authenticate with a single logon without having to save your password when you've configured remote session services on your X client host. For details, see "How to Configure a Distributed Session in Standalone Mode" on page 147.

This connection type has one option:

- **User name**
  Enter the user name for authentication to the X client host. This should be the same user name that you specified under High-latency network performance (page 88).
Advanced Remote Session Services Settings

Getting there

From the Administrative Console or the standalone X Manager

1. (Administrative Console only) Click the Domain Definitions tab.
2. Under X Clients on the left, select a client definition.
4. Click the Advanced button.

The options are:

**Use alternate xauth command**
Select this option to configure an alternate xauth command. The xauth command affects sessions in which Network Security (page 100) > User-based authorization is enabled.

**Xauth command**
Specify an alternate command to place an MIT cookie in the .XAuthority file in the user’s home directory.

Macros (page 71) are supported. For example, in the following command, %IP#% provides the IP address and display number, and %C% specifies MIT-MAGIC-COOKIE-1 authorization and provides the required hex encoded authorization data.

```
xauth add %IP#% %C%
```

This option is available only when **Use alternate xauth command** is selected.

**Select Session Dialog Box**

This dialog box opens when you start a client that has Session set to "<Prompt for session>".

**Remember this choice**
Saves your selection to your client definition. The next time you start the client it uses the session you selected without prompting you again.

**OK**
Starts the client using the currently selected session.

**Cancel**
Closes the dialog box without starting a session or client.

**Start Client Log**

If you need to troubleshoot why a client was not starting, click on the Information icon on the Task Status pane in X Manager.

Two tabs provide client startup log information.

**Command Output**
This tab shows terminal connection messages, and displays information only if the connection type you have chosen provides this kind of output.

**Activity Log**
This tab shows the X Manager connection messages, regardless of the terminal connection type.
XDMCP Connection Definition

For XDMCP connections, the X Display Manager Control Protocol is used to communicate with the XDM (X display manager) running on a particular host. This means that the host controls how the X environment is configured and which clients are run. The host must be configured to support XDMCP. XDMCP sessions reset when you log off of the host.

**XDMCP connection name**
- Enter a name for this connection definition.

**Type**
- Specify the type of XDMCP method to use to send a request over the network to launch the XDM client on a host.

**Broadcast**
- Reset and then send a request to all available hosts based on what you enter for **Broadcast Address**. Any display manager that is willing to service the request responds.

**Direct**
- Reset and then send a request to the X display manager running on a specific host. Use **Host name** to specify the host name or IP address.

**Indirect**
- Reset and then send a request to a single initial host. Use **Host name** to specify the host name or IP address. This host may do one of the following, depending on how it is configured at your site:
  - Provide a dialog box to choose another host.
  - Automatically pass the request to another host.
  - Handle the XDM request itself.

**Broadcast Address**
- By default, the XDMCP broadcast address is 255.255.255.255, which is called a "limited broadcast." A limited broadcast is not forwarded by routers. If routers on your network are configured to pass specific subnet broadcasts but not a universal broadcast, changing the default value of may allow the broadcast to reach more subnets.

If you have multiple subnets and you want an XDMCP broadcast to reach all of them, you can specify multiple IP addresses in this text box. Separate the entries with a comma.

The following example will list all of the addresses in the subnet 214.156.255.255, plus the particular host whose IP address is 110.68.17.1.

214.156.255.255, 110.68.17.1

Host names can be used for individual hosts. IP addresses must be used to designate subnet-directed broadcasts.
Select XDMCP Host

This dialog box appears when a network broadcast is sent to determine which hosts are configured to run an X Display Manager (xdm). The hosts that respond are listed here. If you want to establish an XDMCP connection now, select a host from the list and click OK. Next, you will see the login prompt.

Related Topics

- “Configure a Desktop Connection” on page 37

Launch Group Definition

Use launch groups to launch multiple client applications as a group. You can add any defined X clients or XDMCP connections to a group.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name</td>
<td>Enter a host name or IP address. This option is available when Type is Direct or Indirect. If Direct is selected, the X server sends a request for the login window to the XDM on the specified host. If Indirect is selected, the X server sends a request to the specified host with the expectation that the request will be forwarded to a number of secondary display managers on different hosts. The initial host (also known as the primary display) may also accept the request. The initial host will then display a &quot;chooser window&quot; that presents a list of available hosts.</td>
</tr>
<tr>
<td>Connection timeout</td>
<td>Sets the maximum number of seconds that Reflection X Advantage will try to make an XDMCP connection. A value of 0 is interpreted as an infinite timeout.</td>
</tr>
<tr>
<td>Default session</td>
<td>A session must be running before an X client application can be displayed. Use the drop-down list to select a default session definition for this client. If prompt for session is selected, you'll be prompted to select a session when you start the client. If the session is not already running, Reflection X Advantage starts it when you start the client.</td>
</tr>
<tr>
<td>Automatically start XDMCP session</td>
<td>Select this option if you want the XDMCP connection to start automatically when you start X Manager.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Launch group name</td>
<td>Enter a name for this client group.</td>
</tr>
<tr>
<td>Items to launch</td>
<td>Click the green plus symbol to select which X client and/or XDMCP definitions you want to add to this group. NOTE: You can also add an item to a launch group by dragging an X client or XDMCP definition onto the launch group definition name.</td>
</tr>
<tr>
<td>Automatically start launch group</td>
<td>Select this option if you want the launch group to start automatically when you start X Manager.</td>
</tr>
</tbody>
</table>
Session Definition

Each session definition you configure consists of a combination of settings that affect how Reflection X Advantage manages and displays your connections. You can associate a default session definition with each of your X clients (including XDMCP connections), or configure these definitions to prompt you for a session name when you start the client.

To configure a session, select the session name in the left pane, then use the tabs in the right pane to modify the session settings.

In this Section
- “General tab” on page 87
- “Display tab” on page 91
- “Fonts tab” on page 97
- “Security tab” on page 100
- “Mouse tab” on page 101
- “Extensions tab” on page 101
- “Keyboard tab” on page 104
- “Keyboard Maps” on page 106
- “Advanced tab” on page 116
- “Logging tab” on page 118
- “Session Status” on page 119

General tab

Getting there

From X Manager, X Manager for Domains, or the X Administrative Console

1 (Administrative Console only) Click the Domain Definitions tab.

2 In the left pane, select an existing session definition or click + next to Sessions Definitions to create a new one.

3 In the Session Definition pane on the right, click the General tab.

The options are:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session name</td>
<td>The name for this session definition. This name identifies your session in the Session Definitions list.</td>
</tr>
<tr>
<td>Show clients on X terminal desktop</td>
<td>Select to run all clients in a single window, and have your display appear similar to the standard display of an X terminal. This is sometimes referred to as “single window” mode. This option is required for XDMCP connections.</td>
</tr>
<tr>
<td>Show clients on my desktop</td>
<td>Select to run clients in separate windows like operating system applications. This is sometimes referred to as “multiple window” mode.</td>
</tr>
<tr>
<td>On last client</td>
<td>Specify what action should happen when the last client is closed. For X Client sessions, this action occurs after the amount of time specified by Delay (secs). For XDMCP connections, this action occurs immediately when you log out.</td>
</tr>
</tbody>
</table>
Remote Session Services

Remote session services are available if you have installed support for running Reflection X Advantage session components on other computers. The options available to you depend on whether you are running in standalone or domain mode. For details, see:

Remote Session Services - (X Manager) (page 88)
Remote Session Services - (X Manager for Domains) (page 90)

Related Topics

- “Manage Session Persistence and Performance” on page 158
- “Domain Administration” on page 149
- “How to Configure a Distributed Session in Standalone Mode” on page 147

Remote Session Services - X Manager

Getting there

1. In X Manager, under Session Definitions on the left, select a session definition.
2. In the Session Definition pane on the right, click the General tab.
You can configure remote session services from X Manager to improve performance in networks with high latency or low bandwidth. For step-by-step instructions, see “How to Configure a Distributed Session in Standalone Mode” on page 147.

NOTE: The default Remote session services option is None, which requires no additional setup beyond installing X Manager. To configure High-latency network performance you need to install the Reflection X Advantage Remote Session Services feature on your X client host (or on a UNIX computer with a fast connection to that host).

The options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>With this option, all session processes run on your X Manager workstation.</td>
</tr>
<tr>
<td>High-latency network performance</td>
<td>Use this option to improve performance when you connect to an X client over a high-latency network (typically one in which your X Manager workstation is located far from the X client host computer).</td>
</tr>
</tbody>
</table>

NOTE: The next items configure the connection to the host running Remote Session Services. If you omit any of these, you'll see a prompt to authenticate to the remote session services host when you make a connection. This will be followed by a second prompt, if required, to authenticate to the X client host.

Host name A UNIX host on which you have installed the Remote Session Services feature.

User name A valid user account on this host.

Password (optional) The password for the specified account. This password is stored in the Reflection X database.

The password is saved as clear text and must be updated here whenever it is changed on the host. If you prefer not to save your password, and you've installed Remote Session Services (the service) on your X client host, you can use the connection method, also called "Remote Session Services." This allows you to log in with a single prompt without requiring you to save your password. For details, see Improve Performance over a Slow Network (page 147).

How it works

The protocol router runs on a remote UNIX system that is running the Reflection X service. (You install this service when you install the Remote Session Services feature.) Reflection X Advantage measures the latency of your network connection to determine whether or not to create a headless X server with the protocol router.

- If the delay is small (less than or equal to 10 ms), an X server display is created on the X Manager workstation and all protocol is forwarded directly from the protocol router to this X server display.
- If the delay is greater than 10 ms, an X server display is created on the X Manager workstation and a headless X server is created with the protocol router. By short circuiting many protocol queries, this configuration reduces the number of round trips and the amount of data that needs to pass over the network to the X server display on your workstation.
- Reflection X Advantage remeasures latency periodically to detect changing network performance. If a headless X server is running, it will be discarded if the latency drops below 5 ms, and reinstated if latency rises again above 10ms.
Remote Session Services - X Manager for Domains

Getting there

From X Manager for Domains

1. In X Manager for Domains, under Session Definitions on the left, select a session definition.
2. In the Session Definition pane on the right, click the General tab.

From the Administrative Console

1. In the Administrative Console, click the Domain Definitions tab.
2. Under Session Definitions on the left, select a session definition.
3. In the Session Definition pane on the right, click the General tab.

Remote session services options are available from X Manager for Domains and from the Administrative Console. Use these settings to manage session persistence and to improve performance in high latency networks.

NOTE

- The default Remote session services setting is None. To use any of the other remote session services, you must be connected to a domain with at least one domain node (page 155) available.

- When you exit X Manager for Domains, your currently running sessions may stop or they may continue to run as suspended sessions. What happens depends on your setting for Remote Session Services, your setting for On exiting X Manager, and whether or not you leave the session before you exit X Manager for Domains. For example, if Remote Session Services = Session/suspend resume, On exiting X Manager = Stop all sessions, and you exit X Manager for Domains with a session window still open, Reflection X Advantage automatically stops the session. If On exiting X Manager = Leave all sessions if possible and you exit X Manager for Domains with a session window still open, or with a session suspended, the session will continue to run as a suspended session.

- When Remote session services is set to anything other than None, the client connector (which is responsible for launching X clients) runs on a domain node. If you specify "localhost" for Host name in a client definition that uses this session, the host name resolves to the machine on which the domain node is running, and the specified command is executed on that domain node. You can use this approach to start X clients on the same node as a running session.

The options are:

None

With this option, your session remains available as long as X Manager for Domains is running.

How it works:

The protocol router and X server run on the X Manager for Domains workstation. You can leave and rejoin the session as long as X Manager for Domains is running, but the session always ends when you close X Manager for Domains.

Session suspend/resume

Use this option to be able to rejoin a session even after you close X Manager for Domains and shut down your workstation. (With this configuration, your session does not persist if your workstation shuts down unexpectedly.)
How it works:
The protocol router runs on a remote domain node and creates an X server display on the X Manager for Domains workstation. When you leave the session or close X Manager for Domains, the X server display closes and a headless X server is created on the domain node. The headless server maintains your session. You can log back into the domain from any computer with access to the domain and rejoin the session.

Session suspend/resume; High-latency network performance

Use this option to improve performance when you connect to an X client over a high-latency network (typically one in which your X Manager for Domains workstation is located far from the X client host computer).

How it works:
The protocol router runs on a remote domain node. Reflection X Advantage measures the latency of your network connection to determine whether or not to create a headless X server on the domain node.

- If the delay is small (less than or equal to 10 ms), an X server display is created on the X Manager workstation and all protocol is forwarded directly from the protocol router to this X server display.
- If the delay is greater than 10 ms, an X server display is created on the X Manager workstation and a headless X server is created with the protocol router. By short circuiting many protocol queries, this configuration reduces the number of round trips and the amount of data that needs to pass over the network to the X server display on your workstation.
- Reflection X Advantage remeasures latency periodically to detect changing network performance. If a headless X server is running, it will be discarded if the latency drops below 5 ms, and reinstated if latency rises again above 10 ms.

Session suspend/resume; High-latency network performance; Network fault tolerance

Use this option to ensure that your session remains running even in the event that your workstation shuts down unexpectedly. You can also configure an automatic shutdown after being suspended for a specified time.

How it works:
The protocol router runs on a remote domain node and Reflection X Advantage always creates a headless X server on the domain node in addition to the X server display that runs on your workstation.

Stop suspended session after <n> minutes

Use this option to shut down the session automatically if it has been suspended for the specified time without being rejoined. This setting applies if the session is suspended because of an unexpected shutdown, and also if you suspend the session by selecting Leave in response to the Confirm Exit prompt. This option is not available when Remote Session Services is set to None.

Display tab

Getting there

From X Manager, X Manager for Domains, or the X Administrative Console

1. (Administrative Console only) Click the Domain Definitions tab.
2 In the left pane, select an existing session definition or click next to Sessions Definitions to create a new one.

3 In the Session Definition pane on the right, click the Display tab.

The options are:

**Backing store**
Select to retain the contents of unmapped or obscured windows.

**NOTE:** There is a trade-off between increased network traffic and memory on your local computer — by saving the contents of a window, the server can avoid requests over the network to repaint the window. However, selecting this option may increase the memory requirements of the server.

- **Disabled**
  Disable backing store.

- **By request**
  Use backing store when a client requests it.

- **By request with save unders**
  Use backing store when a client requests it, and enable save unders (page 259) (the default).

  Clients that explicitly disable backing store can still receive save under support.

- **When mapped**
  Use backing store whenever the window is mapped and the client does not specify a backing store window attribute. In X terminology, a window is "mapped" when it is eligible for display on the screen.

  This setting, which is the recommended setting for low bandwidth sessions, reduces network traffic. However, it may also require more memory than the By request setting.

- **When mapped with save unders**
  Enable backing store as for When mapped, and enable save unders (page 259).

  Clients that explicitly disable backing store can still receive save under support.

**Selection bound to clipboard**
Determines which X selection atom (page 259) to link to the native clipboard.

Selections are the primary mechanism for the exchange of information between X clients (for example, copying and pasting between windows).

A selection in an X client is associated with a selection atom. The X client chooses the selection atom to use. If the X client chooses the selection atom that matches the atom in Selection bound to clipboard, then the selection will be copied to the native clipboard.

The value selected in the Selection bound to clipboard list defines which X selection atom (PRIMARY, SECONDARY, or CLIPBOARD) or cut buffer (CUT_BUFFER<n>) is linked to the native clipboard.

**NOTE:** If you're using WordPerfect for UNIX, set this option to CUT_BUFFER0. With the HP Visual Editor (ved), the option must be set to anything except PRIMARY.

- **PRIMARY**
  Choose PRIMARY (the default) if your X client uses the PRIMARY atom to store a text selection. The selection text is placed on the native clipboard. The data stays on the native clipboard until another selection is made.

- **SECONDARY**
  When the X client uses the SECONDARY atom to store a text selection, the selection is placed on the native clipboard. The data stays on the native clipboard until another selection is made.
Screen Definition

Each X server instance can have one or more X screens associated with it, and each screen can be configured differently. Use the options in the Screen Definition table to customize each X screen.

Monitor

The monitor on which you would like Reflection to place an X screen.

To span two or more monitors with a single X screen, select **All**.

If your display encompasses more than one monitor, you can move a screen from the monitor where it initialized to another monitor in your display. However, if the X server is reset, the screen returns to its initial position rather than to its most recent one.

Default Visual Type

The visual type and pixel depth of the X terminal desktop. X clients often inherit this visual type on windows that they create.

**<Best Visual>**

Allow Reflection X to choose the most appropriate default visual type, based on the display adapter setting for the specified monitor.

For example, if the monitor's display adapter is configured for 256 colors, Reflection chooses **PseudoColor, 8-bit depth**. If the display adapter is configured for 24- or 32-bit True Color, Reflection chooses **TrueColor, 24-bit depth**. If the display adapter is configured in a way that doesn't correspond to any supported X visual, Reflection defaults to **True Color, 24-bit depth**.

**PseudoColor, 8-bit depth**

Specify a graphics card with a pixel depth of 8 bits (256 colors). This visual type is supported on displays with changeable hardware color maps.

An X client application can select exactly the color it wants — as long as your display hardware is capable of displaying it — and can change the color at will.

Also see the option for **Set maximum colormaps to 1**.

**TrueColor, 24-bit depth**

Give a pixel consisting of RGB subfields of 8 bits each. The color intensity of each subfield ramps from 0 (fully off) to 255 (fully on), and cannot be changed.

If you are running X clients that try to change colors, you cannot use **TrueColor, 24-bit depth** as a color model; select **PseudoColor, 8-bit depth** instead. X clients in this category include xfshtank and ico2 (with colors specified). See "Display Problems" on page 249 in the Troubleshooting section for more information.
**Virtual Width (Pixels)**

The width of the virtual screen (in pixels).

Width and height dimensions can exceed the actual size of your display, creating a virtual screen for the X server root window.

**Virtual Height (Pixels)**

The height of the virtual screen (in pixels).

Width and height dimensions can exceed the actual size of your display, creating a virtual screen for the X server root window.

**Width (mm)**

The physical width (in millimeters) of the screen.

This number is provided to X clients when they query the X server for the screen size. It does not affect the way the server operates. If both the width and height are 0, Reflection X obtains the settings from your screen's current pixel resolution and density (dots per inch).

**Height (mm)**

The physical height (in millimeters) of the screen.

This number is provided to X clients when they query the X server for the screen size. It does not affect the way the server operates. If both the width and height are 0, Reflection X obtains the settings from your screen's current pixel resolution and density (dots per inch).

**Black and White Pixels**

Sets the pixel value for black and white in dynamic, indexed color maps such as PseudoColor, 8-bit.

The default is Black=0; White=255.

**NOTE:** For static or direct color maps, such as TrueColor, 24-bit, the black pixel value is always 0 and the white pixel is always 255 (or the maximum color intensity).

**Allocate B&W in Client Maps**

Allocates black and white pixels as shared (read-only) when an X client's color map entry is created.

If this option is disabled, black and white pixels are not allocated at all, and their colors could subsequently be changed by any X client. However, colors are still associated as specified in the Black and White Pixels settings.

**Linear Visuals**

Sets an RGB (gamma) correction value on the X terminal window, which makes it possible for a client to interpret colors more correctly given the hardware installed on the computer.

**Single Depth Visuals**

Forces the X server to advertise only visuals that have the same depth as the depth of the visual specified for Default Visual Type.

Also see the option for Set maximum colormaps to 1.

**Hide Title Bar**

Causes the Reflection X screen to fill the physical computer screen such that no title bar is visible (and the Reflection X menu in the upper-left corner of the title bar cannot be accessed). To minimize the X screen, click Minimize from the Reflection X context menu (to access this menu, right-click the client icon from the taskbar).
Colors

Color scheme
Lists your color schemes, including all of the schemes you have created or imported. In X Manager for Domains the list also includes all of the public schemes created by the administrator(s). Color schemes translate string color names requested by clients into red, green, blue (RGB) values. If a client requests colors by name, the color scheme determines which colors are displayed by the X server. By changing the color scheme, you can change the displayed colors.

NOTE: Not all X clients request colors by name — many clients request colors by RGB value or other methods, instead of specifying a color name. Changing the color scheme changes the colors the X server displays only when clients request colors by name.

If you change a color scheme that is in use by a running session, the changes do not affect the session until it is restarted.

Edit
Opens the Color Schemes (page 95) dialog box, from which you can change, create, or import a color scheme.

You cannot modify the Default color scheme. To create an editable color scheme, click Edit, then Clone.

Administrators can also create color schemes from the Administrative Console's Domain Definitions tab.

For additional information, see “Customize a Color Scheme” on page 46.

Set maximum colormaps to 1
Forces the maximum number of colormaps advertised to clients to be the same as the minimum number of colormaps. Some poorly written X clients expect this behavior from the X server.

The associated X clients will be told that a maximum of one colormap is available and, since one colormap will be installed at a time, the client's colors will be rendered by the most recently installed colormap (not necessarily the colormap associated with the window).

You should also set the following options in the Screen Definition table:

- Set Default Visual Type to PseudoColor, 8-bit depth
- Enable Single Depth Visuals

Related Topics
- “Display Problems” on page 249

Color Schemes Dialog Box (X Manager)

Getting there

From X Manager or X Manager for Domains

1. Click Tools > Color Schemes.
2. To create an editable copy of the default color scheme, set Select scheme to Default, and click Clone.

From the X Administrative Console

1. Click the Domain Definitions tab.
2 On the left pane, expand **Color Schemes**.

3 To create an editable copy of the default color scheme, right-click **Default** and select **Clone Color Scheme**.

From this dialog box you can view and change the colors in a "color scheme" on page 255. You can select another scheme, create a new scheme, or import a scheme from a color map file. You can also edit any of the colors in a scheme, or create a new color for a scheme.

**NOTE:** When you import or save schemes, they are saved in your personal settings. These "personal" color schemes are available to you the next time you log on to Reflection X.

### Available Color Schemes

<table>
<thead>
<tr>
<th><strong>Select scheme</strong></th>
<th>Select a personal color scheme. This list includes the default color scheme and schemes that you have imported or created and saved.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Import</strong></td>
<td>Opens the <strong>Import Color Scheme</strong> dialog box, from which you can import an existing RGB color text file to create a new color scheme.</td>
</tr>
<tr>
<td><strong>Clone</strong></td>
<td>Copy the current color scheme. In X Manager for Domains, if you copy a public definition that is read-only, you can edit the copy.</td>
</tr>
<tr>
<td><strong>Scheme name</strong></td>
<td>The name of the color scheme definition. Use the one provided, or enter your own.</td>
</tr>
</tbody>
</table>
| **Colors in scheme** | Displays the entries in the RGB color scheme in a two-column table. The first column shows how the color appears on your display; the second shows the name of the color.  

**NOTE:** Many of the colors have two names: a single name with mixed case (for example, ForestGreen), and another in all lowercase (for example, forest green). Both names are included because X clients might request the color by either name.  

| **+ and –controls** | Add or remove colors from the scheme. |
| **Color column sorts by** | Specify the way you want the Color column to sort: by hue (the default), saturation, or brightness. |
| **HSB** | Displays hue, saturation, and brightness (HSB) values for the color selected in the Color column. Use the slider on the HSB tab to change the HSB values of the selected color.  

**NOTE:** The HSB slider is not displayed for default color schemes because these schemes cannot be modified.  

| **RGB** | Displays the red, green, and blue (RGB) values for the color selected in the Color column. Use the sliders on the RGB tab to change the RGB values of the selected color.  

**NOTE:** The RGB slider is not displayed for default color schemes because these schemes cannot be modified.  

| **Preview** | Shows how the color selected in the Color column will appear. |
Import Color Scheme Dialog Box (X Manager)

Getting there

From the Administrative Console
1. Select the Domain Definitions tab.
2. Click Action > Import Color Scheme.

From X Manager
1. Click Tools > Color Schemes.
2. From the Color Schemes dialog box, click Import.

You can import RGB text files that define color schemes.

The options are:

<table>
<thead>
<tr>
<th>Scheme name</th>
<th>The name for the scheme you are importing. (This name is added to the Color Scheme list.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGB File</td>
<td>An RGB text file. The format for an RGB text file consists of a series of rows that define red, green, and blue (RGB) values for color names. Each row has three decimal values that define red, green, and blue values, followed by a string that defines the color name; for example:</td>
</tr>
<tr>
<td></td>
<td>255 250 250 snow</td>
</tr>
<tr>
<td></td>
<td>248 248 255 ghost white</td>
</tr>
<tr>
<td></td>
<td>248 248 255 GhostWhite</td>
</tr>
<tr>
<td></td>
<td>245 245 245 white smoke</td>
</tr>
<tr>
<td></td>
<td>245 245 245 WhiteSmoke</td>
</tr>
<tr>
<td></td>
<td>220 220 220 gainsboro</td>
</tr>
<tr>
<td></td>
<td>255 250 240 floral white</td>
</tr>
<tr>
<td></td>
<td>255 250 240 FloralWhite</td>
</tr>
<tr>
<td></td>
<td>253 245 230 old lace</td>
</tr>
</tbody>
</table>

Fonts tab

Getting there

From X Manager, X Manager for Domains, or the X Administrative Console
1. (Administrative Console only) Click the Domain Definitions tab.
2. In the left pane, select an existing session definition or click next to Sessions Definitions to create a new one.
3. In the Session Definition pane on the right, click the Fonts tab.

The options are:
In this Section

- “Font Collections” on page 98
- “Advanced Font Path Settings” on page 99

Font Collections

Getting there

1. From X Manager: Click Tools > Font Collections.

2. From the Administrative Console: Click Domain Definitions and find the list of Font Collections in the left-hand panel.

2. Click the plus sign (+), and then select New Font File Set Collection or New Font Server Collection.

Reflection X Advantage provides default font collections that include fonts commonly required by X client applications.

Use these options to create an additional font file collection (load a directory of font files into a new font collection), or font server collection (add a font collection that is a reference to a font server).

Server Font Path Displays the font collections (page 258) that Reflection X searches when a client application requests a font. Font collections are searched in the order in which they appear in this list.

NOTE: Changing the list order so that commonly used fonts are at the top of the list and removing unused font collections improves search performance.

Font Collections Displays all of the available font collections.

Use font server on X client host If a client application requests a font that is not in the font collections specified under Server Font Path, Reflection X Advantage looks for a font server on the X client host on port 7100. If Reflection X Advantage finds a font server running, it passes the unresolved font request to that font server.

Allow font scaling If a client application requests a font in a size that is not available, Reflection X Advantage scales the closest matching font.

Allow font substitutions Substitutes fonts when client applications request fonts that are not available.

Permit client to set font path Allows the client to set the font path. Click Advanced (page 99) to configure font path options. If deselected, X clients are silently prevented from changing the font path. No protocol error is generated if an X client attempts to change the path.

Font Collections

Lists the available font collections.

Collection name Defines the name of a font collection as it appears in the Font Collections list.

Catalog name Defines a name that client applications can use to reference the font collection. A client can use the following format to refer to the catalog name in its font path:

rx/catalogName

For example:

rx/myfonts
**Alternate paths**  Associates font directory paths with the font collection to handle clients that use explicit directories in their font paths. Reflection X Advantage uses these paths as an alias for the catalog name. (This option is shown only for font file collections.)

Add alternate paths in a comma separated list.

UNIX style example:
/usr/share/X11/fonts/misc,/usr/share/X11/fonts/100dpi,/usr/share/X11/fonts/75dpi

Windows style example:
C:/Program Files/Micro Focus/Reflection/x/fonts/75dpi,cC:/Program Files/Micro Focus/Reflection/x/fonts/100dpi,cC:/Program Files/Micro Focus/Reflection/x/fonts/misc

**Font count**  The number of font files in a font collection. Each file includes the definition for a specific font. (This option is shown only for font file collections.)

**Load Fonts**  Opens the Select Font Directory dialog box, from which you can select the font directory where your font files are located. (This option is shown only for font file collections.)

**Font server**  Defines the fully qualified network address of the X font server for this collection.

This option is visible only after you have added a font collection that is a reference to a font server (page 49) (click ‡) and you have selected the font server.

Use the following format to specify the font server:

tcp/host:port

- If no transport is specified, tcp (the default) is assumed.
- If no port is specified, 7100 (the default) is assumed.

The following URL specifies to connect to the font server on the computer wilson:
tcp/wilson.mycompany.com:7100

---

**Advanced Font Path Settings**

**Getting there**

**From X Manager, X Manager for Domains, or the X Administrative Console**

1  (Administrative Console only) Click the Domain Definitions tab.
2  In the left pane, select an existing session definition or click ‡ next to Sessions Definitions to create a new one.
3  In the Session Definition pane on the right, click the Fonts tab.
4  Click Advanced.

These settings configure options when Permit client to set font path is enabled. The options are:
Treat font server as an invalid font path element

Any attempt to add a font server to the font path will be treated as invalid. Enabling this setting may resolve problems when an unreachable font server causes the client to become unresponsive. When disabled, client can specify one or more font servers in the font path.

Discard invalid font path

Controls whether invalid font paths are discarded (with or without a protocol error) or retained. Some poorly behaved clients rely on invalid font paths being accepted by the X server.

Send error when an invalid font path is seen

If the setting Discard invalid font path is enabled, a protocol error is sent when an invalid font path is seen and discarded. Some clients will not operate correctly or will stop if they receive a protocol error when an invalid font path is set.

Security tab

Getting there

From X Manager, X Manager for Domains, or the X Administrative Console

1. (Administrative Console only) Click the Domain Definitions tab.

2. In the left pane, select an existing session definition or click next to Sessions Definitions to create a new one.

3. In the Session Definition pane on the right, click the Security tab.

The options are:

Allow remote IP connections

When cleared, only local X clients can connect to Reflection X Advantage. Client connectors (page 255) set up a listening socket only on the local loopback interface.

NOTE: When you connect to a client using Secure Shell as the connection method (the default), the X11 data is forwarded to Reflection X Advantage from a local port. This means that, for Secure Shell clients, you can clear Allow remote IP connections to help ensure access only from clients running on authenticated hosts.

Host-based authorization

When this option is selected, clients that use this session will be able to connect only to the hosts you include in the Authorized Hosts list.

Authorized Hosts

This option is visible when Host-based authorization is selected. To create or edit the Authorized Hosts list, type host names in the text box, separating each name by new lines, spaces, commas or semi-colons.

User-based authorization

When selected, clients are allowed to run only if they can be verified using MIT-MAGICCOOKIE-1 authorization.

NOTE

- To edit the xauth command that Reflection X Advantage uses to put an MIT cookie in the user’s .XAuthority file, go to the client definition pane; under Connection method click Advanced.

- If both user-based and host-based authorization are enabled, the client connection succeeds if either authorization succeeds; so enabling both reduces your level of security.
Authorization timeout (secs)  This option is visible only when User-based authorization is selected.

After all clients have stopped, the MIT-MAGIC-COOKIE-1 cookie created for a session remains valid for the specified duration (in seconds). In most cases, there is no reason to change the default. Because Reflection X Advantage creates a new cookie for each new client started from Reflection X Advantage, this setting has no effect on clients you launch from X Manager. Only clients launched from outside X Manager might use an existing cookie.

Mouse tab

Getting there

From X Manager, X Manager for Domains, or the X Administrative Console

1 (Administrative Console only) Click the Domain Definitions tab.

2 In the left pane, select an existing session definition or click next to Sessions Definitions to create a new one.

3 In the Session Definition pane on the right, click the Mouse tab.

The options are:

Mouse wheel scroll  Use this option to change the mouse wheel scroll mapping or disable the scroll wheel.

Enable middle button emulation  Gives your two-button mouse the ability to act as a mouse with three buttons. Pressing the left and right buttons simultaneously acts as if middle button was pressed.

Middle button detection speed  Adjusts the maximum amount of time Reflection X Advantage waits for a second button to be pressed. Detection speed is 1 - 1000 milliseconds.

Movement limit  When you move the cursor past this distance (measured in pixels), Reflection X Advantage responds immediately to the currently pressed button.

Test area  Use the Test area to click right, left, and simultaneous left and right buttons to confirm mouse behavior and speed.

Extensions tab

Getting there

From X Manager, X Manager for Domains, or the X Administrative Console

1 (Administrative Console only) Click the Domain Definitions tab.

2 In the left pane, select an existing session definition or click next to Sessions Definitions to create a new one.

3 In the Session Definition pane on the right, click the Extensions tab.

Available Extensions

The following server-side extensions are available in Reflection X Advantage.

Damage  Allows applications to be notified of the regions of windows and pixmaps that are changed by rendering.
<table>
<thead>
<tr>
<th>Extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GP MIT Shared Memory</td>
<td>Required by certain applications. Reflection X Advantage does not support any functional capabilities of this extension. However, its presence allows these applications to operate.</td>
</tr>
<tr>
<td>GLX</td>
<td>Select and configure to run interactive X client applications that produce still or animated three-dimensional color objects, with shading, lighting, and other effects. See GLX Extension Options (page 103) for more information.</td>
</tr>
</tbody>
</table>
| **NOTE**                | - GLX is the OpenGL extension to the X Window System; OpenGL is an industry-standard three-dimensional graphics API.  
- Support for GLX requires access to an OpenGL implementation that supports Pbuffers.                                                                                                                                                                                                                                                                                                                    |
| MIT Shared Memory       | Required by certain applications. Reflection X Advantage does not support any functional capabilities of this extension. However, its presence allows these applications to operate.                                                                                                                                                                                                                                                                                                                                 |
| MIT Sundry              | Permits an application to query and change the server setting that controls tolerance of old (version X11R3) X protocol bugs. The server setting applies to all applications. It is typically safe to leave this extension enabled.                                                                                                                                                                                                                                                                                                     |
| Render                  | Select and configure to use the three-dimensional graphics capabilities of newer video cards. This extension allows applications to use features such as anti-aliased fonts, drop shadows, and translucency. See Render Extension Options (page 103) for more information.                                                                                                                                                                                                                                           |
| Shape                   | Used to create and manipulate non-rectangular windows. Some applications do not appear correctly when this extension is disabled.                                                                                                                                                                                                                                                                                                                                                                     |
| Sync                    | Synchronizes clients on different hosts running different operating systems. Support of this standard is important for multimedia applications, where audio, video, and graphics data streams are being synchronized. The extension also provides internal timers within the X server to which client requests can be synchronized, allowing simple animation applications to be implemented without any round-trip requests and making the best use of buffering within the client, network, and server.                                                                                     |
| X Big Request           | Enables an application to send protocol requests that exceed 262,140 bytes in length.                                                                                                                                                                                                                                                                                                                                                  |
| X Direct Access         | Required by certain applications. Reflection X Advantage does not support any functional capabilities of this extension. However, its presence allows these applications to operate.                                                                                                                                                                                                                                                                                                      |
| X Fixes                 | Supports notification of selection changes, tracking and naming of cursor images, and region objects. Also improves the reliability of embedded applications. The Damage extension uses the region object support of this extension.                                                                                                                                                                                                                                          |
| XFree86 Big Font        | Removes duplicate font metric (size) data for large fonts. This compresses QueryFont replies and reduces the amount of memory used for displaying large fonts.                                                                                                                                                                                                                                                                                                                                    |
| X Input                 | Allows X clients to use the X Input extension APIs to query, change, and modify the core input devices (mouse and keyboard).                                                                                                                                                                                                                                                                                                                                                                    |
| X Test                  | Allows an application to test the X server automatically, with no user intervention, primarily by allowing synthesis of input device events. **NOTE:** It is typically safe to leave this extension enabled. However, it is only required by automated test applications.                                                                                                                                                                                                                                           |
GLX Extension Options Dialog Box

Getting there

From X Manager, X Manager for Domains, or the X Administrative Console

1 (Administrative Console only) Click the Domain Definitions tab.
2 In the left pane, select an existing session definition or click next to Sessions Definitions to create a new one.
3 In the Session Definition pane on the right, click the Extensions tab.
4 From the Available Extensions list, select GLX, and then click Configure.

From this dialog box, you can troubleshoot problems with the rendering of OpenGL graphics. Selecting one or more of the options can help you determine whether or not your video card is faulty.

GLX Extension Options

Advertise stereo capabilities  Find or advertise any stereo functionality on your video card.

Advertise direct rendering  Force Reflection X Advantage to always reply with a 'true' to a glXIsDirect request, even if the renderer context is actually indirect.

Limit to GLX version 1.1  Override the default support for GLX version 1.4 to prevent a client from sending GLX version 1.2 - 1.4 specific protocol. This results in Reflection X Advantage advertising only GLX version 1.1.

Render Extension Options Dialog Box

Getting there

From X Manager, X Manager for Domains, or the X Administrative Console

1 (Administrative Console only) Click the Domain Definitions tab.
2 In the left pane, select an existing session definition or click next to Sessions Definitions to create a new one.
3 In the Session Definition pane on the right, click the Extensions tab.
4 From the Available Extensions list, select Render, and then click Configure.

From this dialog box, you can set the colormap policy. This policy controls how the Render extension allocates colors when it draws pictures in dynamic, indexed visual types (specifically, GrayScale and PseudoColor).

A picture consists of a drawing surface (a core X window or pixmap), and a picture format that controls how pixel data is interpreted. If the surface is a window, the picture format always corresponds to the window's visual. If the surface is a pixmap, the picture format can correspond to any visual, or it can be just Alpha data used in conjunction with another picture.

Picture formats that correspond to indexed visuals have a colormap associated with them. If the visual is the same as the screen's default visual, the screen's default colormap is used. In this case, the Render extension allocates colors based on the colormap policy setting and the number of available (unallocated) pixels in the colormap. If the visual is not the same as the screen's default visual, a new colormap is allocated for use by all pictures of that visual type, and colors are allocated as if the setting were All.
Colormap policy

**Default**

The Render extension chooses an appropriate colormap policy according to the depth and type of the associated visual (see the individual colormap policy descriptions for more information):

- For this visual/depth type
  - 8 or higher/PseudoColor: **Color**
  - 8 or higher/GrayScale: **Gray**
  - All others: **Mono**

**Mono**

Allocates only black and white colors (two entries).

**Gray**

Extends Mono to include 11 intermediate grayscale colors between black and white (13 entries).

**Color**

Extends Gray to include colors found in a 4x4x4 color cube. This color cube includes combinations of red, green, and blue at four intensities between fully off and fully on.

The intensities (over the range of 0x00 - 0xFF) are 00, 55, AA, and FF. The color cube overlaps the Mono and Gray colors at RGB=000000, 555555, AAAAAA, and FFFFFF. Sixty-four colors are allocated for the color cube plus nine other intermediate grayscale colors (73 entries).

**All**

Allocates the largest possible color cube (up to 6x6x6) and then allocates as many additional grayscale colors within the cube as possible.

For example, a depth 8 visual (with 256 colormap entries available) would be allocated as follows:

- 6x6x6 cube = 216 entries
- Intermediate grayscale entries, 8 per cube grayscale segment x 5 segments = 40 entries

On the grayscale, then, the following RGB values are allocated (rounding to 8-bit quantities):

- 000000 (part of 6x6x6 cube)
- 060606 (intermediate grayscale)
- 0B0B0B
- 111111
- 171717
- 1C1C1C
- 222222
- 282828
- 2E2E2E
- 333333 (part of 6x6x6 cube)
- 393939 (intermediate grayscale)
- 3F3F3F

Keyboard tab

Getting there

**From X Manager, X Manager for Domains, or the X Administrative Console**

1. (Administrative Console only) Click the Domain Definitions tab.
2 In the left pane, select an existing session definition or click next to Sessions Definitions to create a new one.

3 On the Session Definition pane, click the Keyboard tab.

The options are:

**Backspace sends**

Select what should be sent to the host when the Backspace key is pressed.

- **Backspace**
  - Have Backspace function as a backspace. This is the default. (To perform a delete when this option is selected, press Shift+Backspace.)

- **Delete**
  - Have Backspace function as Delete. (To perform a backspace when this option is selected, press Shift+Backspace.)

- **Control-h**
  - Have Backspace perform a backspace (as typically used under UNIX hosts).

**Permit X clients to remap the keyboard**

Some X clients (for example, xmodmap) perform keyboard remapping. If permitted, these client remappings override whatever is specified in the Reflection X keymap file.

By default, the Reflection X keyboard mapping is used, regardless of client requests. If a client attempts to do any remapping when such behavior is not permitted, a protocol error is returned to the client.

**Keyboard Map**

Displays the current keyboard map. If you're using X Manager or X Manager for Domains, click Edit (page 106) to modify keyboard mappings.

**Native IME Support**

If you already use an "IME (Input Method Editor)" on page 256 that is available on your workstation, you may want to enable Native IME Support. This feature lets you use your workstation's IME to compose text. The XIM server provided by Reflection X Advantage obtains the composed text from your IME and passes it to XIM-aware clients. This means that you can work with varied X clients without having to learn new input techniques.

The Reflection XIM server supports:

- On-the-spot and over-the-spot editing
- All Unicode characters, including Japanese, Chinese, and Korean characters

For configuration details, see Configure Reflection X Advantage to Use Your Local IME on page 56.

**Launch XIM Server**

Start an “XIM server” on page 258 which obtains composed text from the native IME and passes it to X clients.

**Force clients to use Reflection's XIM server**

Override an X client's choice of XIM server and force it to connect to the XIM server that uses the native IME.

You should always select this option. It helps ensure that the X Client will locate the Reflection XIM server, which is the only XIM server able to pass input from your local IME to the X client. (In rare instances you may want to clear this setting during troubleshooting.)
Related Topics

- “Keyboard Maps” on page 106
- “Work with Keyboard Maps” on page 52

Keyboard Maps

Getting there

From X Manager or X Manager for Domains

1. Click Tools > Keyboard Maps.
2. To create an editable copy of the default keyboard map, set Select Keyboard Map to Default Keyboard Map, and click Clone.

From the X Administrative Console

1. Click the Domain Definitions tab.
2. On the left pane, expand Keyboard Maps.
3. To create an editable copy of the default keyboard map, right-click Default Keyboard Map and select Clone Keyboard Map.

Reflection X Advantage includes a default keyboard map that automatically handles a wide variety of characters on multiple keyboards. If the default maps don't produce a character you need, or you want to add other keyboard mapping assignments, create a keyboard map to modify or add to the default mapping.

NOTE: Before mapping a key, use the Find key option to review the default behavior of a key. If the Results panel shows the keystroke produces the result you want, there may be no need to map a key.

To map a key, you must first Clone a keyboard map: you cannot change the mapping of the default keyboard map.

Select keyboard map
Select the default keyboard map or any other map you have added.

Clone
Click Clone to create a copy of the currently selected keyboard map. The Default keyboard map cannot be modified, and a clone of that map is a quick way to create a keyboard map.

Delete
Delete the currently selected keyboard map. You cannot delete the default keyboard map.

The Find (page 113) button at the bottom of the dialog box help you locate keys you want to modify and Troubleshooting (page 114) options review the behavior of currently mapped keys.

Keyboard Maps Tabs

“Map Key” on page 107
“Characters” on page 110
“Keyboard Shortcuts” on page 110
“Reserved Keycodes” on page 112
Map Modifiers” on page 113

Find and Troubleshooting Buttons

Use “Find Key” on page 113 to identify a key, and use Troubleshooting (page 114) options to view key and keymap behaviors.

Map Key

Getting there

1 In X Manager or X Manager for Domains, click Tools > Keyboard Maps.
2 In the Keyboard Maps dialog box, click Map Key.

NOTE: Administrators can also configure Keyboard Maps from the Domain Definitions tab.

Use Map Key to change the behavior of a key.

Adding or Finding a Key

Click the + sign to “Add or Find a Key” on page 108 that you plan to map. If the key is already in the list of explicitly mapped keys, it is highlighted in the Key column when you exit the dialog box. If the key is not in the list of explicitly mapped keys, it is added to the list when you exit the Add or Find Key dialog box.

Explicitly mapped keys

The keys in the list of Explicitly mapped keys include those that do not send characters (such as function or control keys). The Key and the “X Keysym” on page 257 entry in the left panel is a short summary of the mappings; select a Key to see complete mapping information in the right panel.

Although you can choose to add any key to this list, it’s likely that you can perform all necessary mapping using the keys listed here. Other keys (in particular, those that send characters) are implicitly mapped. Review these on the Characters tab.

Key... Maps to these Keysym(s)

The current behavior for an entry in the list of Explicitly mapped keys is displayed. To change it, use the “Change Mapped X Keysym” on page 108 options in the right panel (Unshifted, Shifted, Alt Gr, Shifted Alt Gr). In general, only one X Keysym (the one in the unshifted position) needs to be defined for any given key.

Require fixed keycode

You can also specify a specific “keycode” on page 256, although this is generally not necessary. Click Require fixed keycode and type in a value between 8 and 255. The keycode is a number that identifies a row in the keymap. The definition for the selected key will be placed in the specified row of the keymap.

Related Topics

- “Keyboard Maps” on page 106
- “Add or Find a Key” on page 108
- “Troubleshooting (Keyboard Maps)” on page 114
- “Work with Keyboard Maps” on page 52
- “Map a Function Key” on page 53
Add or Find a Key

Getting there

1. In X Manager or X Manager for Domains, click Tools > Keyboard Maps.
2. In the Keyboard Maps dialog box, click Map Key.
3. On the Map Key tab, click the + sign above the column of Explicitly mapped keys to open the Add or Find a Key dialog box.

NOTE: Administrators can also configure Keyboard Maps from the Domain Definitions tab.

You have two options for specifying a key you want to map:

- **Press a key.** Review the key description, then click OK.
  This is the most straightforward way to ensure that you’re mapping the key you want.

- Locate the key by selecting it from the Select a key name list and specifying the key location as needed.

If the key is already in the list of Explicitly mapped keys, the key you pressed or selected is highlighted in the list. Review the X Keysyms (page 257) associated with the key. If you want to change one of the X Keysym associated with the key, click the corresponding “Change Mapped X Keysym” on page 108button on the right. Although there are four buttons to change X Keysyms, it is likely that you will only need to map the Unshifted option.

Guidelines for Adding or Finding a Key

- The implicitly mapped keys on the Characters tab do not need to be mapped if they are already doing what you expect.

- Confirm that you have the appropriate key location selected when you use the Select a key name list. The Standard keyboard is appropriate location for control characters such as Tab or Caps Lock. However, if you want to select a key on the numeric keypad, you should select Numeric Keypad in the Select a key location list to specify the correct key. If you choose a key that is already explicitly mapped, it is highlighted on the Map Key tab when you exit this dialog box.

Related Topics

- “Map Key” on page 107
- “Keyboard Maps” on page 106
- “Map a Function Key” on page 53
- “Find the Current Mapping of a Key” on page 52

Change Mapped X Keysym

Getting there

1. In X Manager or X Manager for Domains, click Tools > Keyboard Maps.
2. Select an editable keyboard map (or click Clone to create a new editable map).
3. In the Keyboard Maps dialog box, click Map Key.
4. Select a key in the Explicitly Mapped Keys panel.
5. In the right panel, click Change Mapped X Keysym. (There are four buttons here; the Unshifted option is often the only one needed.)
NOTE: Administrators can also configure Keyboard Maps from the Domain Definitions tab.

There are four separate Change Mapped X Keysym buttons on the Map Key tab. In general, only one X Keysym (the one in the unshifted position) needs to be defined for any given key. However, a key can have different Keysyms associated with unshifted and shifted states.

Unshifted  The Keysym associated with this key when it is pressed by itself (without the Shift or AltGr keys). When the remaining X Keysyms are set to NoSymbol (the default), many X clients use this unshifted X Keysym regardless of the state of the Shift or AltGr keys. Use the additional mapping options only if you need a different behavior for shifted and unshifted states.

Shifted  The Keysym that is associated with the combination of the Shift key and this key.

Alt Gr  The Keysym that is associated with the combination of the Alternate Graphic key and this key. The Alternate Graphic key, also called Mode Switch or abbreviated AltGr, can be found to the right of the space key on most non-U.S. keyboards.

Shifted Alt Gr  The Keysym that is associated with the combination of the Shift key, the Alt Gr key,

Select the X Keysym that corresponds to:

The key that you are planning to change is listed here. Confirm that you have selected the correct Key in the Map Key tab before proceeding.

There are two ways that you can specify the X Keysym assignment for this change:

- **Press a key to locate corresponding X Keysym**
  
  The X Keysym corresponding to the key you press is displayed in this field. You can also use a compose sequence to generate a character and display the corresponding X Keysym (if one exists).

- **Select the X Keysym from a list. Apply filters for category or a character string to help you locate the X Keysym.**
  
  - **Filter X Keysym list by category**
    
    X Keysym categories limit the items shown in Select X Keysym from list.
  
  - **Only list X Keysyms whose names contain**
    
    Type a string to limit the list to X Keysyms that contain these characters.
  
  - **Select X Keysym from list**
    
    Select from the list of available X Keysyms.

After selecting an X Keysym and clicking **OK**, the new mapping is displayed in the list of Explicitly mapped keys.

Related Topics

- “Keyboard Maps” on page 106
- “Work with Keyboard Maps” on page 52
- “Map a Function Key” on page 53
- “Use a Compose Sequence to Specify an X Keysym” on page 53
Characters

Getting there

1 In X Manager or X Manager for Domains, click **Tools > Keyboard Maps**.
2 In the **Keyboard Maps** dialog box, click **Characters**.

**NOTE:** Administrators can also configure **Keyboard Maps** from the **Domain Definitions** tab.

On this tab, all X Keysyms (page 257) which correspond to the set of typed characters that you use in your X client applications are listed. By default, all Latin-1, Latin-2, Latin-3, Latin-4, Latin-8 and Latin-9 characters are supported. In most cases, if your keyboard can generate a character on the supported list, the correct X Keysym will automatically be sent to the X client; no additional mapping is required.

**Supported (already included in the keymap)**

The supported characters are listed on the left. Characters on the left are implicitly mapped, and will be handled appropriately if your keyboard has keys to produce them, or if you can use a sequence of keys to compose them.

**Unsupported (available for mapping)**

If you have a keyboard that includes characters that are not listed on the left (for example, Greek, Cyrillic, or Thai), use the + button to add them to the list of supported characters. No further (explicit) mapping is required.

When you press a key (or key sequence that generates a character) in the **Find key** dialog box, the results indicate if it is in the current keymap. Click **Go to definition** to see its location on the **Characters** tab.

Related Topics

- “Keyboard Maps” on page 106
- “Add an Unsupported Character” on page 55
- “Work with Keyboard Maps” on page 52
- “Troubleshooting (Keyboard Maps)” on page 114
- “Use a Compose Sequence to Specify an X Keysym” on page 53

Keyboard Shortcuts

Getting there

1 In X Manager or X Manager for Domains, click **Tools > Keyboard Maps**.
2 In the **Keyboard Maps** dialog box, click **Keyboard Shortcuts**.

**NOTE:** Administrators can also configure **Keyboard Maps** from the **Domain Definitions** tab.

Use this tab to map a string or a sequence of X Keysyms (page 257) to a key.

**Shortcut**

A shortcut key can include a Shift or Alt Key in combination with a key. Click the + sign in the **Shortcut** column to specify a shortcut key (page 111). After adding the key, associate it with a string or a sequence of X Keysyms.
Send string

Select Send string and type in a string that should be sent when the specified shortcut key is pressed.

Send X Keysyms

Select Send X Keysyms and then click the + sign next to the X Keysyms to send column to open the “Select X Keysym” on page 111 dialog box. Select the X Keysym you want to send and click OK. Continue to click + until you have added the entire X Keysym sequence for the shortcut.

Related Topics

- “Keyboard Maps” on page 106
- “Map a Keyboard Shortcut to a String” on page 55
- “Map a Keyboard Shortcut to an X Keysym” on page 54
- “Add an Unsupported Character” on page 55
- “Troubleshooting (Keyboard Maps)” on page 114

Specify Shortcut Key Combination

Click the + sign on the Shortcut list in the Keyboard Shortcuts tab to open the Specify Shortcut Key Combination dialog box.

There are two ways to identify the shortcut key combination you want to use for sending a string of characters or X Keysym, described below: You can also select a Shift or Alt combination for the key.

- Press a key.
- Select a key name and Select a key location.

  Confirm that you have the appropriate key location selected when you specify a key. The Standard location is appropriate for keys on the main part of the keyboard, such as Tab or Enter. Left or Right apply to keys such as Shift and Control. To select a key on the numeric keypad, select Numeric Keypad in the Select a key location list to specify the correct key.

Click OK to add the selection to the list of shortcut keys on the “Keyboard Shortcuts” on page 110 tab. You can then associate the key with a string (select the Send string option) or a sequence of X Keysyms (select the X Keysyms to send option).

Related Topics

- “Keyboard Maps” on page 106
- “Keyboard Shortcuts” on page 110
- “Work with Keyboard Maps” on page 52
- “Map a Keyboard Shortcut to a String” on page 55
- “Map a Keyboard Shortcut to an X Keysym” on page 54

Select X Keysym

Getting there

1 In X Manager or X Manager for Domains, click Tools > Keyboard Maps.
2 Select an editable keyboard map (or click Clone to create a new editable map).
3 In the Keyboard Maps dialog box, click the Keyboard Shortcuts tab.
4 In the Shortcuts column, add a shortcut key or select an existing shortcut key.
5 Select **Send X Keysyms**.

6 Click the + sign.

**NOTE:** Administrators can also configure **Keyboard Maps** from the **Domain Definitions** tab.

You can create a keyboard shortcut that is associated with an “X Keysym” on page 257 or a sequence of X Keysyms.

There are two ways you can specify an X Keysym that you want to include in the shortcut:

- **Press a key to locate the corresponding X Keysym.** Click **OK** to add the selection to the **X Keysyms to send** list.
- **Select an X Keysym** from a list.
  
  Since the list of X Keysyms is long, it's a good idea to use the filter options below:
  
  - **Filter X Keysym list by category.** For example, selecting Greek as a category will limit the **Select** list to Greek X Keysyms only.
  - **Only list X Keysyms whose names contain**: The **Select** list will include only those X Keysyms that contain the character or character sequence you type.

You can return to this dialog box to add other X Keysyms to the shortcut.

**Related Topics**

- “Keyboard Maps” on page 106
- “Keyboard Shortcuts” on page 110
- “Work with Keyboard Maps” on page 52

**Reserved Keycodes**

**Getting there**

1 In X Manager or X Manager for Domains, click **Tools > Keyboard Maps**.
2 In the **Keyboard Maps** dialog box, click **Reserved Keycodes**.

**NOTE:** Administrators can also configure Keyboard Maps from the Domain Definitions tab.

Use this pane to specify **keycodes** (page 256) that should not be used in the keymap.

In general, the default list of reserved keycodes should not have to be changed. However, some system applications ignore the contents of the keymap and intercept particular key codes. To prevent keys from being inadvertently mapped to such a key code value, click the + sign to add that key code to the list of **Reserved Keycodes**.

**Related Topics**

- “Keyboard Maps” on page 106
- “Troubleshooting (Keyboard Maps)” on page 114
- “Work with Keyboard Maps” on page 52
Map Modifiers

Getting there

1. In X Manager or X Manager for Domains, click **Tools > Keyboard Maps**.
2. In the **Keyboard Maps** dialog box, click **Map Modifiers**.

**NOTE:** Administrators can also configure **Keyboard Maps** from the **Domain Definitions** tab.

An X server uses a modifier map to identify special keys known as modifiers. A modifier map contains a set of keycodes being used for each type of modifier. The X protocol defines 8 types of modifiers: Shift, Lock, Control, Mod1 (Alt), Mod2 (Mode Switch), Mod3 (Meta), Mod4 (Super), and Mod5 (Hyper). The map supports up to four keycodes for each modifier. In practice, two keycodes are sufficient, because most (if not all) keyboards only have two keys that perform Shift, Control, or Alt functions.

Some keyboards include Meta, Super and/or Hyper keys. Applications that use these keys (notably emacs) usually treat Mod3 as Meta, Mod4 as Super, and Mod5 as Hyper. In Reflection X Advantage, by default, Mod3 is defined (as Meta_L and Meta_R keys) but Mod4 and Mod5 are left undefined.

To map a modifier

1. Click a table cell to enable that cell's drop-down control.
2. Select a Keysym from the drop-down list. Reflection X Advantage looks up the keycode for each X Keysym in the keymap table (page 116).

Find Key

Getting there

1. In X Manager or X Manager for Domains, click **Tools > Keyboard Maps**.
2. On the **Map Key** tab, click the **Find** button.

**NOTE:** Administrators can also configure **Keyboard Maps** from the **Domain Definitions** tab.

This is a good starting point for any keyboard mapping activity. You may find that the keystroke that has required explicit mapping in previous X servers is already implicitly mapped in the Reflection X Advantage keymaps.

Locate

You can identify the key you are looking for in either of two ways:

- **Press a key.**
  
  Click in the **Press a key** field, then press the key you want to investigate. You may also press a combination of keys that produce (compose) a character. If the key you pressed generates a character, the **Results** section displays the character that the key is producing, its “X Keysym” on page 257 name if available, and whether it is already in the keyboard map's list of supported characters. The **Results** section also indicates if the key (or combination of keys) is explicitly mapped, has been defined as a keyboard shortcut, or is undefined.

- **Select key name.**
Locate the key by selecting it from the **Select key name** list to see the character this key is producing.

Confirm the **Key location**; if the key is located on the Numeric keypad or with left and right instances, use this option to identify it.

**Results**

The **Results** box shows mapping information about the key in question.

- You press or select a key that is in the list of supported characters. You'll see the character set as it is commonly displayed, the corresponding Unicode value, and the name of the corresponding X Keysym if one exists.

  If the character is supported and is producing the result you expect, no additional mapping is required.

  Click **Go to definition** to see its membership in the list of supported characters on the **Characters** tab.

- You press, compose, or select a key that is not in the list of supported characters (such as pi, π).

  You'll see results that indicate the character is not in the list of supported characters. Click **Create definition** to add a new line to the list of **Explicitly mapped keys** with a NoSymbol Keysym. To change the mapping, click **Change Mapped X Keysym** in the right pane.

- You press or select a key that is explicitly mapped (such as F12). You'll see the associated X Keysym.

  If the character is producing the X Keysym you expect, no additional mapping is required.

  Click **Go to definition** to see its location in the list of **Explicitly mapped keys** on the **Map Key** tab.

  If necessary, you can change the mapping by clicking **Change Mapped X Keysym** on the right.

- You select a key that is not defined (such as F23 on many keyboards) that has not by default been explicitly mapped to an X Keysym).

  Click the **Create definition** button to add a new line to the list of **Explicitly mapped keys** with a NoSymbol Keysym. You can then change the mapping by clicking **Change Mapped X Keysym** on the right.

Use the **Test Keyboard Behavior** and **Test Keymap Behavior** options in **Troubleshooting** for additional analysis.

**Related Topics**

- “Keyboard Maps” on page 106
- “Test Keyboard Behavior” on page 115
- “Test Keymap Behavior” on page 115
- “View Compiled Keymap” on page 116
- “Work with Keyboard Maps” on page 52
- “Use a Compose Sequence to Specify an X Keysym” on page 53

**Troubleshooting (Keyboard Maps)**

“Test Keymap Behavior” on page 115

To view the X events sent by the X server in response to keys, type a key and view the resulting X events.
“Test Keyboard Behavior” on page 115

To identify a physical key and location, or to test a key or a key sequence, type a key and view the resulting keystroke events.

“View Compiled Keymap” on page 116

The compiled keymap is equivalent to the output of an "xmodmap" command. The table shows each keycode in the keymap, the associated key, and the X Keysyms corresponding to the unshifted, shifted, unshifted AltGr, and shifted AltGr positions.

Related Topics

- “Keyboard Maps” on page 106
- “Work with Keyboard Maps” on page 52
- “Find Key” on page 113
- “Key Mapping Problems” on page 253

Test Keymap Behavior

Getting there

1. In X Manager or X Manager for Domains, click **Tools > Keyboard Maps**.
2. In the **Keyboard Maps** dialog box, click **Troubleshooting**.
3. Click the **Test keymap behavior** tab.

**NOTE:** Administrators can also configure **Keyboard Maps** from the **Domain Definitions** tab.

This tab shows the X KeyPress and KeyRelease events that are sent to the X server in response to a key you press. The output is similar to that of the "xev" X client.

With this troubleshooting tool, you can confirm what event is being sent after mapping a key to an X Keysym.

Related Topics

- “Keyboard Maps” on page 106
- “Troubleshooting (Keyboard Maps)” on page 114
- “Work with Keyboard Maps” on page 52

Test Keyboard Behavior

Getting there

1. In X Manager or X Manager for Domains, click **Tools > Keyboard Maps**.
2. In the **Keyboard Maps** dialog box, click **Troubleshooting**.
3. Click the **Test keyboard behavior** tab.

**NOTE:** Administrators can also configure **Keyboard Maps** from the **Domain Definitions** tab.

This tab displays raw events for physical keys and key sequences, and can help identify the exact name and location of a key. It also shows the character generated by pressing a key or sequence of keys (compose sequence).
The physical key behavior shown here does not reflect what is sent from the X server; use the Test Keymap Behavior tab for that information.

Related Topics

- “Keyboard Maps” on page 106
- “Troubleshooting (Keyboard Maps)” on page 114
- “Work with Keyboard Maps” on page 52
- “Use a Compose Sequence to Specify an X Keysym” on page 53

View Compiled Keymap

Getting there

1. In X Manager or X Manager for Domains, click Tools > Keyboard Maps.
2. In the Keyboard Maps dialog box, click Troubleshooting.
3. Click the View compiled keymap tab.

NOTE: Administrators can also configure Keyboard Maps from the Domain Definitions tab.

The compiled keymap is equivalent to the output of an "xmodmap -pk" command on the UNIX host.

The table shows each “keycode” on page 256 in the keymap, the associated key, and the X Keysyms (page 257) corresponding to the unshifted, shifted, unshifted AltGr, and shifted AltGr positions.

- Keys that are explicitly mapped (for example, those with keycodes 8-103 in the default keymap) have an entry in the Key column.
  
  You can override this mapping: Select the key in the Map Key tab, then click Change Mapped X Keysym.

- Keys that are implicitly mapped (keys which generate characters already supported in the keymap) do not have an entry in the Key column.

  If the key on your keyboard is producing the X Keysym required by the X Client, then no additional mapping is required. To confirm this, click Find Key to verify that the key you press and its result is already included in the supported characters list of this keymap.

Related Topics

- “Keyboard Maps” on page 106
- “Work with Keyboard Maps” on page 52
- “Find Key” on page 113
- “Characters” on page 110
- “Map Key” on page 107

Advanced tab

Getting there

From X Manager, X Manager for Domains, or the X Administrative Console

1. (Administrative Console only) Click the Domain Definitions tab.
2 In the left pane, select an existing session definition or click next to Sessions Definitions to create a new one.

3 In the Session Definition pane on the right, click the Advanced tab.

The options are:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compress protocol to remote X servers</td>
<td>Specify one of the following. (For additional information, see “Configure Compression” on page 59)</td>
</tr>
<tr>
<td>Dynamic (default)</td>
<td>Reflection X Advantage measures the bandwidth of data traveling from the protocol router to each remote X server and automatically compresses the protocol when the bandwidth is low enough to be likely to affect performance.</td>
</tr>
<tr>
<td>The bandwidth thresholds are:</td>
<td>&lt; 1000Kbit/s = start compression</td>
</tr>
<tr>
<td></td>
<td>&gt; 2000Kbit/s = stop compression</td>
</tr>
<tr>
<td>Always</td>
<td>Compression is used for all connections to remote X servers. This option may be preferable where bandwidth is low and CPU and memory are not limiting.</td>
</tr>
<tr>
<td>Never</td>
<td>Compression is never used. This option may improve performance if CPU or memory is limited and bandwidth is not low.</td>
</tr>
<tr>
<td>Encrypt protocol to remote X server displays using cipher</td>
<td>Specify what encryption is used for protocol sent from the protocol router to X server displays on other computers. (Note: The 'none' option is not available if you are running in FIPS mode.)</td>
</tr>
<tr>
<td>Note:</td>
<td>This setting also controls what encryption is used for protocol sent between the protocol router and remote client connectors when the Remote Session Services (page 83) connection method is used to launch clients.</td>
</tr>
<tr>
<td>Preferred encoding</td>
<td>Specify the character set encoding required by the window manager to correctly display client names in window title bars. This is typically necessary when client names contain double-byte characters (such as Japanese Kanji). This setting applies to remote window managers only, that is, with servers configured for Show clients on X terminal desktop (page 87).</td>
</tr>
<tr>
<td>Perform IP keep alives</td>
<td>When selected, the primary function of this setting is to instruct TCP/IP to check for terminated client sockets to Reflection X Advantage. If TCP/IP reports a lost connection, Reflection X Advantage terminates the client and its resources. Unless you experience network disruptions, it is best to enable this setting so that Reflection X Advantage correctly receives updates from TCP/IP.</td>
</tr>
<tr>
<td>Trace Session</td>
<td>While troubleshooting a problem, Micro Focus Technical Support may request that you obtain one or more traces of program actions. After receiving your trace file, Technical Support can replay the trace to replicate the problem. Enable this setting to create a trace file (page 247). This setting takes effect the next time you launch this session and remains in effect until you clear the setting.</td>
</tr>
<tr>
<td>Configure for replay</td>
<td>Do not enable this setting; it is for use by technical support when replaying a trace.</td>
</tr>
</tbody>
</table>
Logging tab

Getting there

From X Manager, X Manager for Domains, or the X Administrative Console

1 (Administrative Console only) Click the **Domain Definitions** tab.
2 In the left pane, select an existing session definition or click the next to **Sessions Definitions** to create a new one.
3 In the **Session Definition** pane on the right, click the **Logging** tab.

Reflection X Advantage automatically creates Log Files (page 246). By default, with none of the logging options selected, these files include the following information:

- **Errors**: Serious problems typically caused by unexpected exceptions.
- **Warnings**: Unexpected but recoverable problems, typically caused by poor client protocol (for example, unmatched UngrabServer requests).
- **Info**: General information about major events in the session life cycle.

You can choose to add additional types of data to this log file by enabling the options below.

The options are:

- **Log session activity**: Adds session activity to the log file. Session activity includes information about when sessions are started, joined, left, or reset and when clients are started or shut down.

- **Log font activity**: Records each font request in the log file, indicating whether it was satisfied and with which font.
  
  When you start an X client, the font used is controlled by settings you specify (for example, by choosing the font for text on the command line in your xterm window), or internally by the X client. When a client attempts to find a font, Reflection X searches each font collection for the font name supplied by the client.
  
  If you are receiving font-related errors, select the **Log font activity** option, repeat the steps that caused the error, and then review the log file.

- **Log X protocol errors**: Adds X protocol error data to the log file. This includes server errors and warnings that occur while running Reflection X Advantage.

- **Log network activity**: Adds X client connect and disconnect events to the log file. If the disconnect is considered "not clean," the reason for the disconnect is also added to the log file.

- **Log keyboard activity**: Adds keyboard activity to the log file. This includes Java KeyPress/KeyRelease/KeyTyped events that occur during a session.

- **Log XIM activity**: Adds XIM activity data to the log file.

- **Log SSH debug output**: Adds SSH (Secure Shell) protocol messages to the log file.
Trace Session Dialog Box

Getting there

1 Under X Clients or XDMCP Connections, select the client you want to troubleshoot. Note the name of the Default session used by this definition. You'll modify this session to create the trace.

2 Under Session Definitions, select the session. On the Advanced tab, select Trace session.

3 Start your client.

Tracing creates a file that will help Micro Focus Support analyze and troubleshoot problems. After receiving your trace file, Micro Focus Support can replay the trace to replicate the problem.

NOTE: If you see this dialog box when you start a client, it means that tracing has been enabled for the session. If you don't want to trace the connection, click cancel to close the dialog box. Select the default session definition used by your client, click the Advanced tab, and then clear the Trace session checkbox.

The options are:

- **File name** Specify an output filename and location of the trace file.
  - If the session is configured to run on the local machine, the trace file will be saved to the local system, and you see full path information. You can save the trace to the default location shown, or browse to select an alternate location.
  - If the session is configured to run on a remote node, the trace file will be saved to that remote system and you see only a filename. (This occurs when Remote Session Services on the session definition's General tab is set to anything other than None.) When no path information is given, the trace file is saved to the Reflection X Advantage program location (typically C:\Program Files\Micro Focus\Reflection on Windows and /opt/rxadvantage on UNIX). You can add path information relative to this location, or specify full path information. In either case, the path specified must be valid and accessible on the remote system.

- **Trace session** Continues your connection and starts recording. The trace is saved to the location you specified when the session stops.

- **Cancel** Closes the dialog box and stops the connection. If you want to make the next connection without creating a trace, return to Advanced tab for your session definition and clear the Trace session checkbox.

Related Topics

- “Create a Trace” on page 247
- “Troubleshooting” on page 245

Session Status

Getting there

From the Administrative Console

1 Click the Domain Status tab.

2 From the Running Sessions tab, select a session to display details about the session.
From the X Manager

1 Under **Session Definitions**, running sessions appear beneath the session definition.

2 Select a running session to display the **Session Status** pane on the right with details about the session.

Includes details about a selected running session. When viewing these statistics in the Administrative Console, you may see a double arrow button that allows you to move quickly to other details about the client connectors and X servers associated with the session.

<table>
<thead>
<tr>
<th>Session Name</th>
<th>The session definition name on which this session is based.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>The computer that is running this session.</td>
</tr>
<tr>
<td>Owner</td>
<td>The user who started the session.</td>
</tr>
<tr>
<td>State</td>
<td>Session state — <strong>Starting</strong>, <strong>Stopping</strong>, <strong>Running</strong>, or <strong>Resetting</strong>.</td>
</tr>
<tr>
<td>Time in state</td>
<td>The length of time since the session state last changed.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The amount of time that has elapsed since the session was started.</td>
</tr>
<tr>
<td>Trace file</td>
<td>Visible only if you are tracing the session (page 247).</td>
</tr>
</tbody>
</table>

**Session Sharing Settings**

**Connection URL** *(Standalone mode only) (page 258)* The URL that can be used by other Reflection X servers to join a shared session.

If you are the creator of the session, click **Share** to share the session and generate a connection URL. Send the connection URL to those who you want to join the session. When users start X Manager and go to **Action > Join**, they can join the shared session by providing the connection URL.

**Share**
Choose to generate a connection URL that other X Manager users can use to join this session.

**Unshare**
Choose to stop sharing the current session and disconnect external users that joined it.

**Copy URL**
Choose to copy the **Connection URL** to the clipboard so that it can be distributed to other users via email.

**NOTE**
- These options can be disabled from the **General (page 87)** tab using **Disable sharing**.
- These options are not available if the running session is configured to use **Remote Session Services (page 88)**.

**Allowed Users** *(Domain mode only) (page 258)* All users allowed to join the session are listed here.

If you are the creator of the session, you can click the plus sign (+) to add users. When allowed users start the X Manager and log onto the domain, they can join the session listed under **Offered Sessions**.
Allow users to take control of session

If you are the creator of the session, while the session is running you can select this option to allow users to take control of a session they have joined.

- In Standalone mode, this option applies to all users who join the session using the session’s Connection URL.
- In Domain mode, this option applies to all Allowed Users.

Client Connectors

The client connectors for a session accept incoming connection requests from X clients and forward X protocol requests received from the X client to the session.

Location

The name of the computer on which the client connector is running.

Listening IP/Display

The network address and display number of the X session to which the client connector belongs. A single client connector might have more than one listening IP/display pair if more than one network card is present.

X clients locate an X session by this pair of values. This is done by setting the DISPLAY environment variable (or the X client command line option "-display") to <network address>:<display number>.

X Client Count

The number of X clients connected to this client connector.

X Servers

Shows details about the X servers connected to this session.

Location

The computer on which this X server is running.

User

The user running this X server.

Compression

Shows whether protocol is compressed between this server and the session’s protocol router. If protocol is compressed, or if this is a headless server, this column also displays additional statistics about the data exchange. For details, see “Session Statistics” on page 121.

Input Allowed

Mouse and keyboard input. If user input is enabled for this X server, the status is Yes. Input is allowed from only one X server at a time.

Latency

Displays the “latency” on page 256 (in milliseconds) of the connection between the computer running this server and the computer running the session’s protocol router.

If the server is running locally, this column shows "N/A".

Bandwidth

Displays the “bandwidth” on page 255 of the connection between the computer running this server and the computer running the session’s protocol router.

If the server is running locally, this column shows "N/A".

Session Statistics

When a session is running, the following session statistics are displayed in the X Servers status area in the Compression column.
**Compression Statistics**

Compression statistics are shown when compression is active (Compression = Yes). These statistics can help you determine the best configuration where low bandwidth is a problem.

Compression data is shown as name = value pairs. The following information is shown:

- **Total original bits** = <bit count of protocol entering the compressor>
- **Total encoded bits** = <bit count of protocol exiting the compressor>
- **Compression ratio** = <Original bits / Encoded bits>:1
- **Compression overhead** = <percentage of non-compression-related bits in encoded bits>%

**Headless X Server Statistics**

Headless X Server statistics are shown where the server is a locally connected headless server. These statistics can help you determine the best configuration where high latency is a problem.

- **Headless server** -- identifies the server as a Headless X server (an X server with no visible display)
- **Total requests** = <count of all protocol requests>
- **Short-circuited requests** = <count of all query requests> (<percentage of all requests>%)  
- **Round-trips saved** = <count of instances where clients waited for a query response>  
- **Total bits** = <bit count of all protocol requests and responses>  
- **Short-circuited bits** = <bit count of all query requests and responses> (<percentage of total bits>%)  

**Share with Users**

*Getting there*

**From the Administrative Console**

1. Click the **Domain Status** tab.
2. From the **Running Sessions** tab, select a running session.
3. Click the plus sign (+) next to **Allowed Users**.

**From X Manager for Domains**

1. Under **Session Definitions**, running sessions appear beneath the session definition.
2. Select a running session to display the **Session Status** pane on the right.
3. Click the plus sign (+) next to **Allowed Users**.

**NOTE:** This dialog box is available in Domain mode only (page 258).

This dialog box lists all of the users who have been added to the domain, and who are not already allowed users on the session.

**To share with users**

- Select a user, or use Shift + Click or Ctrl + Click to select multiple users, and then click **OK**.
  
  This allows the selected users to join the session (from X Manager for Domains, under **Offered Sessions**), from their computers.
Offered and Joined Sessions

Offered Sessions

The Offered Sessions list is available in X Manager for Domains. Shared sessions are available if an owner of a running session adds you to the Allowed Users list for the session.

Joined Sessions

The Joined Sessions list is available in the standalone X Manager. This list is empty until you join a session. To join session, you need a connection URL sent to you by the owner of the running session.

NOTE: If you don’t use session sharing, you can hide the Offered Sessions or Joined Sessions item from view using the “Preferences Dialog Box” on page 126.

Menus

X Manager provides the following menus:

File (page 123) Perform actions related to working with definitions, customize your view of X Manager, and manage deleted items stored in the Definition Trashcan.

(Domain mode only) (page 258) Connect to or disconnect from a domain, and view information about the domain to which you are connected.

Action (page 133) Perform actions related to working with sessions.

Tools (page 133) Configure color schemes, font collections, or SSH settings.

Help (page 142) Access the online help system, the Micro Focus Web site, and the Micro Focus Support site, and view licensing information about Reflection X Advantage.

File Menu

Using the commands from this menu, you can work with definitions, customize your view of X Manager, and manage deleted items stored in the Definition Trashcan. If using X Manager for Domains, you can connect to or disconnect from a domain, and view information about the domain to which you are connected.

New Creates a new definition. This is equivalent to using clicking the plus sign next to a definition type.

Clone Copies the selected definition. If you copy a read-only (public) definition, you will be able to edit the copy.

Delete Removes the selected definition. This is equivalent to clicking the minus sign with a definition selected.

Move Up Moves the selected item in the definitions list.

Move Down NOTE: You can also move items using drag-and-drop.

Create Shortcut Creates a shortcut to launch the selected session or client. (Supported on Windows systems.)

Log On (Domain mode only) (page 258) Logs the user onto a domain.
Enter Logon Information Dialog Box

Getting there

From the Administrative Console and X Manager for Domains

- From the File menu, select Log On.

To use X Manager for Domains or the Administrative Console, you need to log on to the Reflection X Advantage domain.

NOTE: In many cases you can log onto the Reflection X Advantage domain using the same user name and password you use to log onto your computer. Contact the Reflection X Advantage domain administrator for additional logon information.
**NOTE:** Notes for Reflection X Advantage domain administrators:

- If you are an administrator logging onto a newly created domain for the first time, you can log in for the first time using either X Administrative Console or X Manager for Domains. The name you specify for your initial login will be the default domain administrator. For details, see “Set Up the Domain Controller” on page 153.

- On UNIX systems PAM authentication is used to authenticate the first domain user. On some UNIX systems, the pam_securetty module is configured by default to allow root logins only if the user is logging in on a secure tty. On these systems you cannot log onto the Reflection X Advantage domain using root credentials.

- On Windows systems, the first domain user must be a user who is a member of the same Windows domain as the user who installs Reflection X Advantage.

- To log onto the Administrative Console, the user must be a Reflection X Advantage domain administrator.

- Administrators can use the Authentication tab of the Administrative Console to determine which users have access to the domain and which user or users can serve as domain administrator.

### Change Password Dialog Box

**Getting there**

**From the Administrative Console and X Manager for Domains**

1. Make sure that you are logged on to a domain that uses internal authentication (page 258).
2. From the **File** menu, select **Change Password**.

If you log on to a domain that uses internal authentication (page 258), you can change your password. After you change your password and log off from the Administrative Console or X Manager for Domains, the new password is in effect when you log on again.

**NOTE:** If you are a domain administrator, the password change applies to both Administrative Console and X Manager applications the next time you start either one.

### Change Password

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>(Read-only) The user name for the current logon.</td>
</tr>
<tr>
<td>Old password</td>
<td>Type in your current password.</td>
</tr>
<tr>
<td>New password</td>
<td>Type in your new password.</td>
</tr>
<tr>
<td>Retype password</td>
<td>Type in your new password again.</td>
</tr>
</tbody>
</table>
Logon Properties Dialog Box

Getting there

From the Administrative Console and X Manager for Domains

- From the File menu, select Logon Properties.

The Logon Properties dialog box provides the name of the domain to which you’re connected and who you’re logged onto the domain as.

The options are:

<table>
<thead>
<tr>
<th>Connected to</th>
<th>The name of the domain to which you are connected.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>The user who logged onto the domain.</td>
</tr>
<tr>
<td>FIPS mode</td>
<td>Shows the configuration of the domain for FIPS mode, configured in the Domain Composition (page 180) tab of the Administrative console.</td>
</tr>
<tr>
<td>Authentication system</td>
<td>Shows the authentication system in use for this domain, configured in the Authentication (page 188) tab of the Administrative console.</td>
</tr>
</tbody>
</table>

Related Topics

- “Domain Administration” on page 149

Preferences Dialog Box

Getting There

- From the File menu, select Preferences.

Section Visibility

Controls which sections of the X Manager navigation pane are displayed, and in which order. By default, all available sections are displayed.

Preferences Options

| Keep only one section expanded | Controls the number of sections expanded at one time. When enabled, only the selected section is open; all other sections are automatically closed. |
| Empty trash at log off/exit | Permanently deletes all items in the trash can when you log off of the domain (domain mode), or exit the application (standalone mode). |
| Automatically hide successful tasks | When enabled, messages about successfully completed tasks are automatically removed from the Task Status pane, located at the bottom of X Manager and the Administrative Console. Use Hide delay (secs) to specify the number of seconds that pass before a task message is removed. |

NOTE: Tasks with errors are not removed.
**FIPS mode**
Enforces the United States government Federal Information Processing Standard (FIPS) 140-2 for this connection. When **FIPS mode** is selected, all available settings use security protocols and algorithms that meet this standard. Encryption options that do not meet this standard are not available; only the Secure Shell connection method can be used to start X clients, and XDMCP is not available as a session startup option.

Each time you change the **FIPS mode** setting, you must restart X Manager or X Manager for Domains.

**FIPS mode** is not available if Reflection X Advantage is using a non-default JRE (page 223) that is not configured for unlimited strength cryptography.

A standalone X Manager can share sessions with other standalone X Managers running in the **same** mode. Thus FIPS X Managers are able to share only with other FIPS X Managers and non-FIPS X Managers are able to share only with other non-FIPS X Managers.

For domains, you must configure **FIPS mode** both in X Manager for Domains and the Administrative Console. In order to log onto a domain, the FIPS mode of X Manager for Domains must match the domain's FIPS mode.

**Preferred language**
Specify the preferred language for the user interface. This setting takes effect when you restart the program.

**On exiting X Manager**
Determines how X Manager handles running sessions with one or more clients running when closing X Manager (standalone) or when logging off X Manager for Domains.

**Prompt**
The user is prompted to decide how to handle running sessions:

- Stop the session
- Leave the session running
- Cancel the operation to close X Manager

**Stop all sessions**
X Manager closes running sessions when closing or logging off. If you are using the standalone X Manager, this setting stops all running sessions. If you are using X Manager for Domains and you have configured sessions that support session suspension, any sessions you leave before you close the window will continue to run.

**Leave sessions if possible**
(X Manager for Domains only).

The session continues to run if a session definition's **Remote session services** (page 90) is set to one of the following (any suspend/resume option other than **None**):

- Session suspend/resume
- Session suspend/resume, High-latency network performance
- Session suspend/resume, High-latency network performance, Network fault tolerance

If a session is not set to any of the above, the session closes when X Manager is closed.
On closing session window

Determines how X Manager handles closing a session configured to Show clients on X terminal desktop (page 87) when one or more clients are running.

Prompt

The user is prompted to decide how to handle running sessions:

- Stop the session
- Leave the session running
- Cancel the operation to close the session window

Stop session

X Manager closes the session when the session window is closed.

Leave session if possible

(X Manager for Domains only)

The session continues to run if a session definition's Remote session services (page 90) is set to one of the following (any suspend/resume option other than None).

- Session suspend/resume
- Session suspend/resume, High-latency network performance
- Session suspend/resume, High-latency network performance, Network fault tolerance

If Remote session services is set to None, the session closes when the session window is closed.

When displaying Help

By default help content is provided from the web. If you want help calls to go to locally installed files instead, download and run the optional local help installer (page 19), and change this setting to "Use installed help system."

If either local or web help is not available, Reflection X Advantage will automatically attempt to use the other option.

Related Topics

- "The X Manager Interface" on page 26

Confirm Exit

This dialog box is displayed when you attempt to exit X Manager when sessions are still running. You can choose to stop them, leave them, or cancel the exit operation. The choices you are offered depend on how you're running X Manager and how you have configured your preferences.

X Manager (standalone): You do not have the option to leave a session. You can stop the session or cancel your exit operation.

X Manager for Domains: The option to join and leave a suspended session is available when Remote session services (page 90) is configured for a suspend/resume option.

NOTE: As you exit X Manager for Domains, any sessions that you have already left will remain running.
This dialog box appears when the setting **On exiting X Manager** (page 126) is configured to **Prompt** in **Preferences**. You can change this behavior:

- Choose **Leave** (X Manager for Domains) or **Stop** and then select **Remember this choice**.
- Change the setting in the **Preferences** dialog box. You should also use this setting if you want to change this behavior again.

**Confirm Close**

This dialog box is displayed when you are configured to **Show clients on X terminal desktop** (page 87) (with all clients in a single window), and you attempt to exit a session that is still running. You can choose to stop it, leave it, or cancel the exit operation. The choices you are offered depend on how you're running X Manager and how you have configured your preferences.

**X Manager (standalone):** You do not have the option to leave a session. You can stop the session or cancel your exit operation.

**X Manager for Domains:** The option to join and leave a suspended session is available when **Remote session services** (page 90) is configured for a suspend/resume option.

This dialog box appears when the setting **On closing session window** (page 126) is configured to **Prompt** in **Preferences**. You can change this behavior:

- Choose **Leave** (X Manager for Domains) or **Stop** and then select **Remember this choice**.
- Change the setting in the **Preferences** dialog box. You should also use this setting if you want to change this behavior again.

**Definition Trashcan Dialog Box**

**Getting there**

- From X Manager, click **File > Definition Trashcan**, or select the **Definition Trashcan** toolbar button:
  ![Definition Trashcan toolbar button]

- or -

- From the Administrative Console, click **File > Trashcan**.

The Definition Trashcan provides temporary storage for definitions that you chose to delete. Items in the Trashcan remain there until you permanently delete them from the Reflection X Advantage database, or until you undelete and restore them to their original location. You can also use the option in the **Preferences** dialog box to **Empty trash at exit** (page 126).

**NOTE:** To export a definition and then import it again, you must delete the definition you exported, and you must also empty the trashcan before the import can proceed.

**Definition Trashcan**

<table>
<thead>
<tr>
<th>Empty Trash</th>
<th>Click to permanently remove the deleted definitions from the database. Definitions deleted from the Trashcan cannot be restored.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Item</td>
<td>Click to restore a selected definition to its original location.</td>
</tr>
</tbody>
</table>
Export Definitions Dialog Box

Getting there

From the File menu

- From the X Manager File menu, click Export.

From this dialog box, you can export available definitions (settings for clients, sessions, font collections, color schemes, keyboard maps, and trusted host and user keys) from the X Manager on the current computer and import those definitions into an X Manager on another computer. The exported definitions are saved in an .rxd definition file, and imported by copying the definition file to the destination computer, where the definitions are imported using X Manager. Administrators can also use exported definition files to create custom templates.

Available Definitions

<table>
<thead>
<tr>
<th>Available Definitions</th>
<th>Lists all definitions that are available for export.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Selects all items in the current category.</td>
</tr>
<tr>
<td></td>
<td>Clears all selections in the current category.</td>
</tr>
</tbody>
</table>

Export Options

<table>
<thead>
<tr>
<th>Automatically include referenced definitions</th>
<th>This option ensures that when you select an available definition that references other definitions, all the related definitions are added to the Definitions Pending Export list.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>For example, if you select a client definition for export, the session, font, keyboard, and color scheme definitions referenced by that client definition are also added to the Definitions Pending Export list</td>
</tr>
<tr>
<td>Remove passwords from exported definitions</td>
<td>Select to ensure that all stored password strings are removed from the definitions you are exporting.</td>
</tr>
</tbody>
</table>

Template configuration

**NOTE:** These items are relevant only if you are an administrator configuring templates (page 200) to add to a Reflection X Advantage deployment.

<table>
<thead>
<tr>
<th>Template name</th>
<th>If this .rxd file is present in the templates folder, the name you specify here shows up in the list of available templates in the Import Templates and Migrated Settings dialog box that displays on initial startup. (This name is not used if Automatically import template on first run is selected.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically import template on first run</td>
<td>If this .rxd file is present in the templates folder, the definitions in it are imported silently on initial startup.</td>
</tr>
</tbody>
</table>
Definitions Pending Export

Definitions Pending Export  Lists all definitions that will be added to the exported file.
Name  Identifies a definition to be exported.
Type  Indicates the type of definition that will be exported.
Reason  Indicates why the definition was added to the Definitions Pending Export list (either Selected or Included by Reference).
Export  Exports all definitions on the Definitions Pending Export list. Click to open the Select Export File dialog box, from which you can specify the name and location of the .rxd file to which definitions are exported.

Import Definitions Dialog Box

Getting there

From the File menu

- From the X Manager File menu, click Import.

From this dialog box, you can import available definitions (settings for sessions, clients, servers, font collections, color schemes, and trusted host and user keys) from a Reflection X Advantage .rxd definition file. Typically, .rxd files are created by running X Manager to export a set of definitions on one computer, and then copying the export file to a destination computer where the definitions will be imported.

Available Definitions

Choose File  Opens the Select Definition File dialog box, from which you can choose and open the definition file (.rxd) that contains definitions you want to import.
Available Definitions  Lists all definitions that are available for import.
Selects all items in the current category.
Clears all selections in the current category.

Import Options

Import file: <filename>  Identifies the path and name of the definition file that you have opened for import.
Automatically include referenced definitions  Select this option to ensure that when you select an available definition that references other definitions, all of the related definitions are added to the Definitions Pending Import list. This is important so that related definitions stay together when imported.

For example, if you select a session definition for import, the client, server, font and color scheme definitions referenced by that session definition are also added to the Import list.
Definitions Pending Import

Definitions Pending Import  Lists all definitions that will be added from the Import file.
Name  Identifies a definition to be imported.
Type  Indicates the type of definition that will be imported.
Reason  Indicates why the definition was added to the Definitions Pending Import list.
Import  Imports definitions on the Definitions Pending Import list. If the names of items to be imported are the same as definitions that already exist in the definitions database, the Import Conflicts Found dialog box opens, from which you can resolve any naming conflicts and complete the Import operation.

Related Topics

- “Import Conflicts Found Dialog Box” on page 132

Import Conflicts Found Dialog Box

When the names of items to be imported are the same as definitions that already exist in the definitions database, this dialog box appears. Using the Resolution settings, you can resolve any conflicts and complete the Import operation.

Conflict Details

Pre-existing definition's name  The name of an existing definition that conflicts with the definition you chose to import.
Last modified  Date and time that the pre-existing definition was last modified.
Importing definition's name  The name of the conflicting definition that is a candidate for import.
Last modified  Date and time that the importing definition was last modified.

Resolution

Use the following options to resolve conflicts one by one, or to apply a batch solution that resolves all conflicts in a single operation. Choose a resolution for the first reported conflict, and then click OK. If the import file contains another definition conflict, you'll be prompted to resolve it. Repeat the resolution process. After all conflicts have been addressed, pending import definitions are processed based on your selections:

Overwrite this definition  Overwrite the pre-existing definition with the settings in the importing definition.
Overwrite all conflicting writable definitions  For all conflicting definitions, overwrite the pre-existing definitions with the settings in the importing definitions.
Duplicate this definition  Import the conflicting definition and append (import duplicate) to the imported definition's name to distinguish it from the pre-existing definition.
Duplicate all conflicting definitions  Import all conflicting definitions and append (import duplicate) to the imported definitions' names to distinguish them from the pre-existing definitions.
Do not import this definition  Do not import the conflicting definition.
Action Menu

Using the commands from this menu, you can perform various actions related to working with sessions.

- **Start** Starts the selected session.
- **Stop** Stops the selected session.
- **Join** Join a session shared by another user. When using X Manager for Domains, Join also allows you to rejoin a session that you suspended using Leave.
- **Leave** (Domain mode only) Leave the selected session, which is persisted in memory. Use Join to rejoin the session you left.
- **Take Control** Take control of a shared session that you have joined.

Tools Menu

Options available from the Tools menu

- “Color Schemes Dialog Box (X Manager)” on page 95
- “Keyboard Maps” on page 106
- “Font Collections” on page 98
- “Secure Shell User Keys Dialog Box” on page 133
- “Secure Shell Host Keys Dialog Box” on page 138

Secure Shell User Keys Dialog Box

Getting there

From the X Manager Tools menu

- From the X Manager Tools menu, click Secure Shell User Keys.

Public key user authentication is an optional feature of the Secure Shell protocol. Reflection X Advantage supports both standard public key authentication and certificate authentication, which is a form of public key authentication.

**NOTE:** Keys or certificates you configure in this dialog box are available for all Secure Shell connections for which Public Key authentication is enabled (the default configuration). You can modify the supported authentication methods for individual clients using the Advanced Secure Shell dialog box Authentication tab (page 74).

From this dialog box, you can:

- Generate and import user keys for public key authentication.
- Import user certificates into the Reflection X Advantage key store for certificate authentication.
Configure Reflection X Advantage for user authentication with certificates in the Windows certificate store.

Configure Reflection X Advantage for user authentication with smart cards or other PKCS#11-compliant devices.

The options are:

**User Key Sources**

Modify this list to control which key store or stores Reflection X Advantage uses for making Secure Shell connections using the Public key authentication method.

Add or remove stores using plus (+) and (-).

The available stores are:

**Reflection X Advantage Store**

Use this store to authenticate with keys or certificates in the Reflection X Advantage store (page 66).

When this store is selected, you see a list of keys and/or certificates that you have added to the Reflection X Advantage database.

The following buttons are available when the Reflection X Advantage store is selected:

- **Generate**
  Opens the Generate Key Pair dialog box, from which you can create a new key pair to use for user authentication. The private key is added to the user key database.

- **Import**
  Opens the Import User Key Pair dialog box, from which you can add existing private keys to the user key database. Imported keys or certificates can be in SecSH, OpenSSH, or PKCS#12 format.

- **Export**
  Exports the public key associated with the selected private key and allows you to specify a file format for the exported key. Use the exported public key to configure the Secure Shell server to authenticate with this user key.

- **View**
  This button is available only if the selected item is an X.509 certificate. Click to view the contents of the certificate.

- **Delete**
  Removes the selected key from the Reflection X Advantage store.

**Local Directory**

Use this option to authenticate with keys or certificates stored locally (on the computer running X Manager or X Manager for Domains). Use **Directory** to specify the local directory. The **User Keys** list shows keys available in this directory.

The following buttons are available when a local directory store is selected:
**Windows Certificate Store**

This store is available if you are running on Windows. Add this store to the list to authenticate with personal certificates in your Windows certificate store (page 68).

When this store is selected, you see a list of certificates available in your Windows Personal store. Reflection X Advantage will use these certificates for authentication.

**NOTE**

- The certificate in the Windows store must use an RSA key pair; DSA keys are not supported.
- Access to the Windows certificate store is not supported if you have installed using the 64-bit Windows installer. If you're running on a 64-bit platform and require access to the Windows certificate store, install using the 32-bit installer.

The following button is available when the Windows certificate store is selected:

**View Certificate**  
Click to view the contents of the certificate.

**PKCS#11 Provider**

Use this store to authenticate using PKCS#11-compliant hardware devices such as smart cards or USB tokens (page 68). You can add one or more PKCS#11 stores.

Reflection X Advantage can authenticate using either the X.509 certificate in the smart card or token, or using the public key contained in the certificate. The first time you make a connection, you see two entries to authenticate with your device. The first entry is for authentication using the certificate in your device. The second entry is for standard public key authentication using the public key associated with that certificate. Authentication using the public key entry requires that your key be added to the server's list of authorized keys.

**NOTE:** PKCS#11 is not supported in the 64-bit version of Reflection X Advantage.

The following options are available when a PKCS#11 store is selected.
Getting there

1. From X Manager, click **Tools** > **Secure Shell User Keys**.
2. Select **Reflection X Advantage Store** (the default), or any configured local directory store.
3. From the **Secure Shell User Keys** dialog box, click **Generate**.

### Description
Specify a descriptive name to use to identify this provider.

### Library
The name and location of the library file (*.dll or *.so) used by the token provider to provide access to your hardware device. This is typically installed to the Windows system folder. You may need to contact the device manufacturer to determine the correct file.

### View Certificate
Click to view the contents of a certificate on your card or token.

**NOTE:** If a PIN is required, you may need to enter this value in order to see the list of certificates.

### Generate Key Pair Dialog Box

**Related Topics**

- “Secure Shell User Keys Dialog Box” on page 133

**Name**
The key name identifies the key in the user key database.

**Type**
Specifies the algorithm used for key generation.

**Length**
Specifies the key size. Up to a point, a larger key size improves security. Increasing key size slows down the initial connection, but has no effect on the speed of encryption or decryption of the data stream after a successful connection has been made. The length of key you should use depends on many factors, including: the key type, the lifetime of the key, the value of the data being protected, the resources available to a potential attacker, and the size of the symmetric key you use in conjunction with this asymmetric key. To ensure the best choice for your needs, we recommend that you contact your security officer.

RSA keys must be between 1024 and 4096 bits in 256-bit increments.

DSA keys must be between 512 and 1024 bits in 64-bit increments. (In FIPS mode, DSA keys must be 1024 bits.)

**No passphrase**
Select this option to create a key that is not protected by a passphrase.

**CAUTION:** To help ensure security, all user keys should be passphrase protected. If you don’t specify a passphrase, the private key is stored in unencrypted form in the key store, and anyone who gains access to the key can authenticate using it. In standalone mode keys are stored on the same computer as X Manager. In domain mode, keys in the Reflection X Advantage Store are stored in the database on the domain controller and the administrator of that computer will be able to read these keys.

**Passphrase**
Enter a “passphrase” on page 256 for this key. You will need to enter this passphrase when the key is used for authentication.

**Verify**
Retype the passphrase.
**Import User Key Pair or Certificate Dialog Box**

**Getting there**

1. From X Manager, click **Tools > Secure Shell User Keys**.

2. Under **User Key Sources**, select **Reflection X Advantage Store** (the default), or any configured local directory store.

3. From the **Secure Shell User Keys dialog box**, click **Import**.

**Private key, pfx, or p12 file**

For public key authentication:

- The private key of a public/private key pair. Imported keys can be in OpenSSH format or SecSH format.

For certificate authentication, either of the following:

- The private key associated with a certificate. The two files must be in the same location and the certificate must have the same name as the key with a *.cer or *.crt file extension.
- A PKCS#12 (page 256) package file (*.p12, or *.pfx) that contains both the certificate and its associated private key.

**File passphrase**

Enter the passphrase that protects the specified private key file.

**NOTE:** You must enter a file passphrase; you cannot import private keys or PKCS#12 package files that are not passphrase-protected.

**Key name**

The name identifies the key or certificate in the user key database.

**No passphrase**

Select this option to import the key without passphrase protection.

**CAUTION:** To help ensure security, all user keys should be passphrase protected. If you don't specify a passphrase, the private key is stored in unencrypted form in the key store, and anyone who gains access to the key can authenticate using it. In standalone mode keys are stored on the same computer as X Manager. In domain mode, keys in the Reflection X Advantage Store are stored in the database on the domain controller and the administrator of that computer will be able to read these keys.

**Key passphrase**

Enter a **"passphrase"** on page 256 for this key or certificate. You will need to enter this passphrase when the key or certificate is used for authentication.

**Verify**

Retype the passphrase.

**Related Topics**

- “Secure Shell User Keys Dialog Box” on page 133
- “Configure User Key Authentication” on page 64
- “Authenticate with Certificates in the Reflection X Advantage Store” on page 66

**Export User Key Dialog Box**

**Getting there**

1. From X Manager, click **Tools > Secure Shell User Keys**.

2. From the **Secure Shell User Keys** dialog box, select a key, and then click **Export**.

From this dialog box, you can export the public portion of a public/private key pair.
The options are:

**Filename** Specify the name and location you want to use for the exported public key file.

**File Format** Two formats are available. SecSH format is used by Reflection products, F-Secure, and SSH Corporation. OpenSSH format is used in OpenSSH implementations.

**Related Topics**

- “Secure Shell User Keys Dialog Box” on page 133

**Select User Key Dialog Box**

This dialog box is presented when your client session is configured to authenticate using Public key authentication and more than one key or certificate is available. Select the key you want to use for this connection.

**Remember user key for ...** When this option is selected Reflection X Advantage automatically uses the same key or certificate after a successful connection, so you won’t see this dialog box again when you connect to the same host.

**View Certificate** This button is available only if the selected item is an X.509 certificate. Click to view the contents of the certificate.

**NOTE**

- If you are authenticating use a smart card or hardware token, the first time you authenticate you will see two entries for this device. The first entry is for authentication using the certificate in your device. The second entry is for standard public key authentication using the public key associated with that certificate. Authentication using the public key entry requires that your key be added to the server’s list of authorized keys.
- If you’re running in FIPS mode, only FIPS-compliant keys are listed.
- If you prefer to select a key each time you connect using this client definition, go to Advanced Secure Shell Settings > Authentication and enable Always prompt for user key during public key authentication.

**Secure Shell Host Keys Dialog Box**

Use this dialog box to manage keys and certificates used for host authentication in Secure Shell session.

- Host Keys (page 138)
- PKI Configuration (page 140)

**NOTE**: Host keys and certificates you configure on these tabs are available for all Secure Shell connections.
Public key authentication of the Secure Shell server is a standard feature of the Secure Shell protocol. Use the **Secure Shell Host Keys** database to manage your list of trusted hosts.

The options are:

**Trusted Host Keys**

+ Click the plus sign (+) to manually import a key from the **Import Host Key** dialog box.

**Host** Displays the name of the host that authenticates with this key.

**Type** Indicates whether the key uses either an RSA or DSA algorithm.

**Fingerprint** Provides a way to reliably identify the host key.

When host is untrusted:

**Allow** Does not enforce strict host key checking. Reflection X Advantage connects without displaying a confirmation dialog box, and the host key is not added to your list of trusted keys.

**Prompt user** Reflection X Advantage displays the **Host Key Unknown** dialog box when you connect to an unknown host.

**Reject** Enforces strict host key checking. Reflection X Advantage does not connect unless the host is trusted. Before you can connect, you must add the host key to your host key database.

**Import Host Key Dialog Box**

**Getting there**

**From X Manager**

- From the **Tools** menu, click **Secure Shell Host Keys**, and then from the **Secure Shell Host Keys** dialog box, click the plus sign (+) at the top of the **Trusted Host Keys** list.

**From the Administrative Console**

1 Click the **Domain Definitions** tab.

2 In the left pane, click the plus sign (+) next to **Trusted Host Keys**.

From this dialog box, you can import trusted host keys. The options are:

**Host name** Type the name of the host.

**Public key file** Enter the name of the file, or use the **Browse** button (...) to locate the public key of the host public/private key pair.

**Import** Click to add the selected key to your trusted host keys.

**Host Key Unknown**

Host authentication enables the Secure Shell client to reliably confirm the identity of the Secure Shell server. This authentication is done using public key authentication. If the host public key has not previously been installed on the client, the first time you attempt to connect you see a message indicating that this is an unknown host. This message includes a fingerprint that identifies the host. To
be sure that this is actually your host, you should contact the host system administrator who can confirm that this is the correct fingerprint. Until you know that the host is actually your host, you are at risk of a "man-in-the-middle" attack, in which another server poses as your host.

The options are:

**Always**  Make the connection and add this host to the list of trusted hosts. You will not see this prompt for subsequent connections to the same host unless you remove the host from the trusted host list, or the host key changes.

**Once**  Make the connection but do not add the host to the trusted host list. You will see this prompt again the next time you make a connection to the same host.

**No**  Do not make the connection and do not add the host to the trusted host list.

**PKI Configuration Tab - Secure Shell Host Keys Dialog Box**

**Getting there**

**From X Manager**

- From the *Tools* menu, click *Secure Shell Host Keys*.

Use the **PKI Configuration** tab to configure connections to PKI Services Manager, a free add-on utility that provides X.509 certificate validation services. This utility is required if your X client host authenticates using certificates. Before you configure the options on this tab, you need to download and configure this free add-on utility.

**NOTE:** The options on this tab are not available if you are running X Manager for Domains. To configure connections to PKI Services Manager for a domain, you need to use the Administrative Console (page 180).

The options are:

**PKI server**  Specify the host name or IP address of the computer running PKI Services Manager.

**NOTE:** If PKI Services Manager is configured to use a non-default port, include the port value using *hostname:port* syntax. For example acme.com:18081.

**Public key**  These read-only items display information about a PKI Services Manager public key after it has been successfully imported.

**MD5 fingerprint**

**SHA1 fingerprint**

**Import Key**  Use this option to manually import the PKI Services Manager public key. First, copy the key from the PKI Services Manager computer (default locations are below) to any location available from Reflection X Advantage.

The default location on Windows is:

```
common application data
folder (page 258)\attachmate\ReflectionPKI\config\pki_key.pub
```

The default location on UNIX is:

```
/opt/attachmate/pkid/config/pki_key.pub
```
Download Key

Retrieves the public key from the specified PKI server and displays a dialog box that allows you to confirm this identity. To compare the presented fingerprint with the actual PKI Services Manager key open the PKI Services Manager console on the PKI server, and go to Utility > View Public Key.

When you click Yes to accept the key, the key is imported into the Reflection X Advantage database.

NOTE: Download Key is available if you are connecting to PKI Services Manager version 1.2 or later. If you are connecting to an older version, install the public key using Import Key.

Delete Key

Removes the PKI Services Manager key from the Reflection X Advantage database.

Verify Public Key Dialog Box

This confirmation appears when you download a key from PKI Services Manager. Use the displayed fingerprints to confirm that the key is the correct key for your PKI Services Manager. To compare the presented fingerprint with the actual PKI Services Manager key open the PKI Services Manager console on the PKI server, and go to Utility > View Public Key.

When you click Yes to accept the key, the key is imported into the Reflection X Advantage database.

SOCKS Proxies Dialog Box

Getting there

From the Administrative Console

1. Click the Domain Status tab.
2. From the Running Sessions tab, select a running session.
3. Click the plus sign (+) next to Allowed Users.

From X Manager for Domains

1. Under Session Definitions, running sessions appear beneath the session definition.
2. Select a running session to display the Session Status pane on the right.
3. Click the plus sign (+) next to Allowed Users.

Use this dialog box to configure connections to SOCKS proxy hosts. To add a SOCKS Proxy to the list, click Add and enter the following:
To configure an X client connection to use SOCKS

1. Use the **SOCKS Proxies** dialog box to configure a connection to one or more SOCKS proxy servers.
2. In your client definition, set **Connection method** to Secure Shell (the default), and click **Advanced** to open the **Advanced Secure Shell Settings** dialog box.
3. Click the **SOCKS Proxy** tab and select a SOCKS proxy from the drop-down list.

**NOTE:** To view information about the SOCKS proxy connection in the X Manager log file, select **Log SSH debug output** on the session **Logging** tab. You can use the `xmanager.log` file to confirm a successful connection through a configured SOCKS protocol. For example, a successful connection through a SOCKS5 protocol logs the following message: "Completed handshake using SOCKS5 protocol. Socket channel is connected."

### Help Menu

Using the commands from this menu, you can configure your view of the online Help and reach additional Help resources.

The options are:

- **Help Topics**
  - Access the online Help system.
- **Show Help Tips**
  - Select to display Help tips when hovering over items with the mouse.
- **Micro Focus Support Site**
  - Visit the Micro Focus Support Web site for the most recent technical information on Reflection X Advantage.
- **Contact Support**
  - Display contact information for Micro Focus Support.
- **About X Manager**
  - View licensing and copyright information about Reflection X Advantage.
**Toolbar**

**X Manager Toolbar**

Using the buttons from the X Manager toolbar, you can control sessions in Reflection X Advantage, as follows:

- **Start** Starts the selected session.
- **Stop** Stops the selected session.
- **Join** Join a session shared by another user. When using X Manager for Domains, **Join** also allows you to rejoin a session that you suspended using **Leave**.
- **Leave** (Domain mode only) Leave the selected session, which is persisted in memory. Use **Join** to rejoin the session you left.
- **Definition Trashcan** Manage the **Definition Trashcan**. Options include restoring or permanently discarding the deleted item(s) stored there.

**Task Status Pane**

Located at the bottom of X Manager and the Administrative Console, the Task Status pane displays messages about connection status and long-running tasks that are being handled. Typical messages include information about connecting to or disconnecting from a domain, and starting or stopping a session. Error messages are also displayed.

You can customize the behavior of the Task Status pane in the Preferences dialog box; for example, when you start an X session, the Task Status pane identifies the task, indicates progress of the task, and shows the result of the task — cancellation, error, or success.

For tasks related to unsuccessful client connections, click the Information ("i") icon on the Task Status pane to display the Start Client dialog box, which provides client information.

Reflection X Advantage log files are also a source of information.

Reflection X log files are created for the following applications and services:

<table>
<thead>
<tr>
<th>Application</th>
<th>Log file</th>
</tr>
</thead>
<tbody>
<tr>
<td>X Manager</td>
<td>xmanager.log</td>
</tr>
<tr>
<td>X Manager for Domains</td>
<td>xmanager.log</td>
</tr>
<tr>
<td>X Administrative Console</td>
<td>xadmin.log</td>
</tr>
<tr>
<td>rxsconfig</td>
<td>rxsconfig.log</td>
</tr>
<tr>
<td>rxmigrate</td>
<td>migration.log</td>
</tr>
</tbody>
</table>
### Service | Log file
--- | ---
Reflection X Service | rxs.log
Domain Controller (process of Reflection X Service) | domain.log
Domain Node (process of Reflection X Service) | node.log
Remote Session Services (process of Reflection X Service) | node.log

The locations of these log files vary by platform:

**Windows**

**Application log files:**

%USERPROFILE%\attachmate\rx\logs

**Service log files:**

%ALLUSERSPROFILE%\attachmate\rx\logs

**UNIX**

**Application log files:**

~/.attachmate/rx/logs

**Service log files:**

rxs.log (service launcher)

/var/log

rxs.log (log file for the service itself), domain.log, node.log, rxsconfig.log

/opt/rxadvantage/logs

**HP-UX**

**Application log files:**

~/.attachmate/rx/logs

**Service log files:**

rxs.log (service launcher)

/var/adm

rxs.log (log file for the service itself), domain.log, node.log, rxsconfig.log

/opt/rxadvantage/logs

### Related Topics

- “Connection Problems” on page 250
Remote Session Services in Standalone X Manager

In standalone mode, by default all session components run on the same system as X Manager. If your connection to the host system is slow, you may be able to improve performance by using Remote Session Services feature to configure a distributed session.

In this Chapter

- "X Manager Basic Session" on page 145
- "X Manager (Standalone) Distributed Session" on page 146
- "How to Configure a Distributed Session in Standalone Mode" on page 147

X Manager Basic Session

X Manager (the standalone session manager) is installed by default. When you run sessions from X Manager, all processes initially run on the X Manager workstation, data flows directly between the X Manager and the X client host, and the server display is created on the X Manager. (By sharing your session, you may create additional X server displays on remote computers.)

**NOTE:** All definitions used by the standalone X Manager are stored in the Reflection X Advantage database (page 217) on the X Manager workstation.

1. When you start X Manager, it retrieves session settings from the database on your workstation.
2. When you launch a session, a client connector and protocol router are created on your workstation, and X client applications connect to the client connector.
3. The X server display is created on your workstation, and all X protocol passes between the two computers.
X Manager (Standalone) Distributed Session

If you are running the standalone X Manager (which is installed by default), you can use the Remote Session Services feature to configure distributed sessions. A distributed session can improve performance where high "latency" or low bandwidth is a problem in your network (typically because your X client host is located far from your X Manager workstation). This configuration can also resolve problems using XDMCP when you are connecting through a VPN.

To configure a distributed session, you use the Remote session services setting on the General tab of the session definition. To support this functionality from the standalone X Manager, you need to install the Remote Session Services feature on the X client host or on a UNIX computer with a fast connection to that host, and configure your session to run on this host. For details, see “How to Configure a Distributed Session in Standalone Mode” on page 147.

NOTE: All definitions used by the standalone X Manager are stored in the Reflection X Advantage database (page 217) on the X Manager workstation.

Here is the sequence of events on a high latency network when Remote session services is set to High-latency network performance. In this example the Remote Session Services feature is installed and running on the X client host.

1. When you start X Manager, it retrieves session settings from the database on your workstation.
2. When you launch a session, a client connector and protocol router are created on the X Client host, and X client applications connect to the client connector.
3. The X server display is created on your workstation. Reflection X Advantage automatically measures the latency of the connection between the protocol router and the X server display, and creates a headless X server on the X client host if the delay is significant enough to affect performance. Only those X protocol commands that are required for the updating the display pass between the two computers.

NOTE: In high latency networks, this configuration improves performance by short circuiting some of the data exchange over the network. With the headless X server running on the client host, client/server exchanges that don't affect the display pass between the client and the headless X server, but aren't sent on to the X server display on the workstation. This reduces the number of round trip network messages, and this can improve the response time you see on your workstation. In addition, if the network exhibits low bandwidth, the protocol is compressed between the protocol router and the X server display.
How to Configure a Distributed Session in Standalone Mode

You can use remote session services to improve performance where your network configuration causes delays that make running a remote X client application difficult. This configuration can also resolve problems using XDMCP when you are connecting through a VPN.

Before you begin

- Install X Manager on the user's workstation. This feature is installed by default.
- Log on as root to the X client host (or a UNIX system with a fast connection to this host) and install Reflection X Advantage (page 13). Install the Remote Session Services feature.

To configure and start your session

1. From the user's workstation, start X Manager.
2. Under Session Definitions, create a new session (or select an existing session). In the General tab, under Remote session services, do the following:
   - Select High-latency network performance.
   - For Host name specify the name of the computer on which you installed Remote Session Services.
   - (Optional) For User name and Password, specify valid credentials on this computer. Note: The password is saved in clear text in the database.
3. Under X Clients or XDMCP Connections, create a new definition (or select an existing one) and enter the required connection information. For Default session, use the drop-down list to select the Remote Session Services session you just configured.
4. Start your X client or XDMCP connection.

If you did not specify a password under Remote Session services in the session definition, you'll see two prompts. The first is to authenticate to the Remote Session Services host. This is followed by a second prompt (if required) to authenticate to the X client host. If you don't want to save your password, and you're running Remote Session Services on the same host as the X client, you can avoid the second prompt by configuring single sign-on, as described in the next procedure.

In the Session Status display for your running session, under X Servers, you will see an entry for your workstation computer. If high latency is detected in your network connection, you'll see an additional entry for the headless X server. The headless X server will be located on the remote session node.

The next procedure uses a client connection method called "Remote Session Services." This connection type lets you authenticate with a single logon prompt without requiring you to save your password.

To configure single sign-on for sessions using remote session services

1. Under X Clients, select the client that uses your Remote Session Services session.
2. Set Connection method to "Remote Session Services."
Domain Administration

A Reflection X Advantage domain consists of one or more computers on which X session components run and are load-balanced. The domain also defines a group of users who can run and share sessions on those computers. All public and private definitions used by X Manager for Domains are stored in the Reflection X Advantage database (page 217) on the domain controller and can be accessed from any computer in the domain.

Reflection X Advantage domains can be set up in many different ways, with several optional components. To review some sample domain configurations, see “Sample Domain Configurations” on page 163.

In this Chapter

- “Reflection X Advantage Domain Components” on page 149
- “Reflection X Advantage Session Processes” on page 150
- “X Manager for Domains Basic Session” on page 150
- “X Manager for Domains Distributed Session” on page 151
- “Setting up Domain Components” on page 153
- “Domain Authentication” on page 159
- “Sample Domain Configurations” on page 163

Reflection X Advantage Domain Components

A Reflection X Advantage domain typically involves more than one computer.

The Administrative Console

Used by domain administrators to set up and centrally manage the domain. This application is typically installed on the domain controller. You can also install it on additional workstations to manage the domain from those computers.

X Manager for Domains

Used by domain users to run and configure sessions.

Domain Controller

The domain controller runs the Reflection X service, including the domain controller process. The service runs continuously and listens for requests to access the domain. The database (page 217) that centrally stores session information is located on the domain controller.

Domain Node

A domain node runs the Reflection X service and supports remote session services. The domain controller can act as a domain node. In addition you can create additional nodes by installing the Reflection X service (without the domain controller feature) and joining the node to the domain using the rxsconfig utility.
Reflection X Advantage Session Processes

In Reflection X Advantage, a traditional X server is broken into separate cooperating processes — a client connector and protocol router, and one or more X servers. This combination of processes is referred to as an "X session." These processes may be distributed on one or more computers, depending on your configuration.

Client Connector and Protocol Router

The client connector and protocol router run together on the same computer. The client connector receives X protocol data from the X client application, converts it to a proprietary Reflection X Advantage protocol, and then sends it to the protocol router.

The protocol router serves as the hub of traffic for a Reflection X Advantage session — it transmits the protocol it receives from the client connector to one or more X server displays connected to the session.

X Server

The X server receives and processes data from the protocol router. Reflection X Advantage has two types of X servers:

X server display

This server creates the X client application display and returns user input (for example, keyboard or mouse) to the protocol router, which sends it on to the client program. A shared session may have multiple X server displays.

Headless X server

This server has no physical display, yet processes all X protocol. When enabled, the headless X server can short-circuit inquiry-only requests, removing the need to forward these requests across slow connections to X server displays on user desktops. When a session is suspended, the headless server keeps it alive by continuing to process client requests.

X Manager for Domains Basic Session

A basic session is one in which all session components run on the user's workstation. This is the default X Manager for Domains configuration (Remote session services on the General tab is set to none). Remote session services (such as the ability to suspend and resume session, and improved performance in slow networks) are not available with this configuration. This configuration does support the ability of a domain administrator to provide users with predefined public session definitions. In addition, users can configure and run their own private sessions.

Here is the sequence of events when Remote session services is set to none:

1. When a user logs on to a domain, the domain controller authenticates the user, after which the user can access session definitions stored in the domain database.
When the user starts a session, the domain controller sets up the session components on the user's workstation. (See the arrow labeled 2 in the following illustration.)

The X protocol flows directly from the X client to the session on the workstation. (See the arrow labeled 3 in the following illustration.)

**X Manager for Domains Distributed Session**

Reflection X Advantage sessions that use **Remote session services** can have several advantages over basic sessions, including session persistence and improved performance in high latency or low bandwidth networks.

All of the following **Remote session services** options create a distributed session. In a distributed session, the client connector and protocol router are created on a remote domain node, not on the workstation running X Manager for Domains. Each of these options also supports creating a headless X server on that domain node. The difference between the options is in how they control creation of the headless X server.

- **Session suspend/resume**
  A headless X server is created on the domain node only when you leave the session or close X Manager for Domains. This enables you to rejoin the session at a later time.

- **Session suspend/resume; High-latency network performance**
  Reflection X Advantage automatically measures the latency of the connection and creates a headless X server if the delay is significant enough to affect performance. The headless X server helps improve performance by reducing the amount of data that needs to pass over the network.
- **Session suspend/resume; High-latency network performance; Network fault tolerance**

  This option forces creation of a headless X server whenever the session is running. This can improve performance where high-latency is a concern and also ensures that the session remains running even if a workstation is disconnected due to a power or network failure.

  Here is a sample sequence of events when **Session suspend/resume; High-latency network performance; Network fault tolerance** is enabled.

  1. The user logs into the domain. (See the arrow labeled 1 in the following illustration.)

  2. When the user starts a session, the domain controller sets up the session processes (a client connector, protocol router, and a headless X server) on a domain node. (See the arrow labeled 2 in the following illustration.) It also starts an X server display on the user's workstation (shown in the second illustration).

  3. The X client establishes a connection with the client connector. All X protocol passes to the headless X server on the domain node. (See the arrow labeled 3 in the following illustration.)

  4. The X protocol required to update the display is passed on to the X server display on the workstation. (See the arrow labeled 4 in the following illustration.)
NOTE: In high latency networks, this configuration improves performance by short circuiting some of the data exchange over the network. When a headless X server is running, client/server exchanges that don't affect the display pass between the client and the headless X server, but aren't sent on to the X server display on the workstation. This reduces the number of round trip network messages, and this can improve the response time you see on your workstation.

Compression to Remote Workstations

If you are connecting over a low bandwidth network, protocol compression can improve performance. Reflection X Advantage is configured by default to compress protocol to remote X servers automatically whenever it detects low bandwidth (Compress protocol to remote X server displays = Dynamic). When you configure a distributed session (as shown above), the protocol that passes between the domain node and the workstation (identified with the label 4 in the diagram above) will be compressed automatically if low bandwidth is detected.

Setting up Domain Components

Use the information in this section to set up the domain controller, start and stop the Reflection X Advantage service, set up administrator and user workstations, set up and remove domain nodes, and manage session persistence and performance.

In this Section

- “Set Up the Domain Controller” on page 153
- “Start and Stop the Reflection X Service” on page 154
- “Set Up an Administrator Workstation” on page 155
- “Set Up Domain Nodes” on page 155
- “Remove a Domain Node” on page 156
- “Set Up User Workstations” on page 157
- “Manage Session Persistence and Performance” on page 158

Set Up the Domain Controller

Each Reflection X Advantage domain requires one domain controller. You can run the domain controller on any supported platform.

To set up the Reflection X Advantage domain controller

1. Install the following features:
   - **X Administrative Console**
   - **Domain Services** (including the Domain Controller feature)
   - **Java Runtime Environment (JRE)** (Windows only)

   **NOTE:** The Reflection X Service, configured to run the domain controller, starts automatically.

To create an administrator's account for the domain, you'll log into the domain using the X Administrative Console.
To log on to the domain the first time

1. From the domain controller, start the X Administrative Console.
   You'll see the domain logon dialog box.

2. Enter the following information to log on to the domain:
   - For **User name** and **Password**, specify any user who can log onto your computer. The name you specify for your initial login will be the default domain administrator.
   - For **Domain**, enter the name of this computer. The Reflection X Advantage domain name is always the same as the name of the computer running the domain controller.

   **NOTE:** On Windows systems, the first domain user must be a user who is a member of the same Windows domain as the user who installs Reflection X Advantage.

   On UNIX systems PAM authentication is used by default for user authentication. On some UNIX systems, the pam_securetty module is configured by default to allow root logins only if the user is logging in on a secure tty. On these systems you cannot log onto the Reflection X Advantage domain using root credentials.

3. From the tabs located along the left-hand side of the window, click **Authentication**.
   Notice that your name is already added to the list of user accounts and is selected as the administrator. By default, the first user to log on is set as the Reflection X Advantage domain administrator.

Start and Stop the Reflection X Service

The Reflection X Service (RXS) starts automatically when you install it, and when the computer reboots. However, you may need to stop or restart the service as part of a troubleshooting procedure.

**NOTE:** If X Manager for Domains or the Administrative Console is open, you should log off before you stop or restart the Reflection X Advantage service.

To start, stop, or restart the Reflection X Service

<table>
<thead>
<tr>
<th>System</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Open the Windows Services Management Console. (From Control Panel, go to <strong>Administrative Tools &gt; Services.</strong>) Select <strong>Micro Focus Reflection X Service</strong> to start, stop, or restart the service.</td>
</tr>
<tr>
<td>UNIX and Linux</td>
<td>You can start, stop, or restart the service from the command line via the <strong>init.d</strong> system using the <strong>rxs</strong> command. For example:</td>
</tr>
<tr>
<td></td>
<td><code>/etc/init.d/rxs start</code></td>
</tr>
<tr>
<td></td>
<td><code>/etc/init.d/rxs stop</code></td>
</tr>
<tr>
<td></td>
<td><code>/etc/init.d/rxs restart</code></td>
</tr>
<tr>
<td></td>
<td>The path to <strong>init.d</strong> depends on your operating system:</td>
</tr>
<tr>
<td></td>
<td>Default: <code>/etc/init.d</code></td>
</tr>
<tr>
<td></td>
<td>HP-UX: <code>/sbin/init.d</code></td>
</tr>
<tr>
<td></td>
<td>Red Hat: <code>/etc/rc.d/init.d</code></td>
</tr>
</tbody>
</table>
Set Up an Administrator Workstation

A Reflection X Advantage domain administrator’s workstation can be the domain controller, or any computer that has access to the domain controller.

To set up the administrator’s workstation

1. Install the following features:
   - X Administrative Console
   - X Manager for Domains
   - Templates
   - Java Runtime Environment (JRE) (Windows only)
2. Start the X Administrative Console. To log, enter the username and password of the domain administrator. For instructions on creating this administrator account, see “Set Up the Domain Controller” on page 153.

Set Up Domain Nodes

Adding nodes to a Reflection X Advantage domain is optional. Typically, nodes are added in order to support either or both of the following:

- Run sessions on a node at or near a remote X client host to improve performance over a slow network.
- Run sessions on multiple nodes to provide load balancing where remote session services are required by many users.

To add a node to a Reflection X Advantage domain, you'll install the Reflection X Advantage service on the computer you want to add as a node, then use the `rxsconfig` utility to add this computer to the Reflection X Advantage domain. You can create a node on any supported platform.

Before you begin

- “Set Up the Domain Controller” on page 153.
- Know the name of the computer running the domain controller (this is the domain name for your Reflection X Advantage domain), and the user name and password of the Reflection X Advantage domain administrator.
- Have administrator (or root) credentials for the computer you want to add as a node.

To set up a domain node

1. Log onto the computer you want to designate as a node using an administrator (or root) account.
2 Run the Reflection X Advantage installer and select the feature called **Domain Services** (without including the **Domain Controller** feature). If you are running on Windows, also confirm that **Java Runtime Environment (JRE)** is selected. (For information about downloading and launching the installer, see “Install Reflection X Advantage on Windows” on page 11 or “Install on UNIX” on page 13.)

3 Open a Command Prompt window (Windows) or terminal window (UNIX).

   **NOTE:** For newer Windows systems (starting with Windows Vista and Windows Server 2008), you need to open the command window as an administrator. (In the Start menu, under **Accessories**, right-click **Command Prompt** and select **Run As Administrator**.)

4 Run the following command, where "domainname" is the name of the computer running the domain controller.

   ```
   rxsconfig join domainname
   ```

   Note: On UNIX systems, include full path information for **rxsconfig**. The default install location is shown in this example:

   ```
   /opt/rxadvantage/rxsconfig join domainname
   ```

5 You'll be prompted for Administrator credentials. Enter the user name and password of the Reflection X Advantage domain administrator. You'll see a message saying that node was successfully created. In this example, the node uses the default port, 22001.

   ```
   C:\>rxsconfig join domainname
   Initializing crypto library...
   Performing the join...
   Administrative user for domain: joe
   Password: <password>
   Created node 0.0.0.0:22001 for domain domainname.
   ```

6 On the computer on which you have installed the Reflection X Advantage Administrative Console, open the Console and log on using the domain administrator credentials. Click the **Domain Composition** side tab.

   You should see the node you just created listed under **Registered Nodes**.

7 (Optional) Edit the **Registration Details** for this node.

   **NOTE:** The **Participate in domain** setting is selected by default. This is required for domain participation. If you clear this setting, existing sessions can continue to run but new sessions won't be able to use this node.

8 (Optional) If you are adding multiple nodes, select a **Load balancing** scheme.

   **NOTE:** You can configure the domain controller to act as a domain node. To do this, use the procedure above, omitting step 2.

### Remove a Domain Node

Use the **rxsconfig** (page 233) command line utility to remove a node from a domain.

**To remove a domain node**

1 Log onto the computer that is currently configured to be a Reflection X Advantage domain node using and administrator (or root) account.

2 Open a Command Prompt window (Windows) or terminal window (UNIX).
NOTE: For newer Windows systems (starting with Windows Vista and Windows Server 2008), you need to open the command window as an administrator. (In the Start menu, under Accessories, right-click Command Prompt and select Run As Administrator).

3 Run the following command, where "domainname" is the name of the computer running the domain controller.

```bash
rxsconfig leave domainname
```

Note: On UNIX systems, include full path information for rxsconfig. The default install location is shown here:

```bash
/opt/rxadvantage/rxsconfig leave domainname
```

4 You'll be prompted for administrator credentials for the domain. Enter the user name and password of the Reflection X Advantage domain administrator. You'll see a message saying that node was successfully deleted.

NOTE: You can remove a domain node from the list under Registered Nodes in the Domain Composition tab of the X Administrative Console. If you do this, the node is no longer available to computers in your domain, but this change does not affect the configuration of the domain node. On that computer, the Reflection X service continues to run and listen on the port specified when the domain node was created. Using rxsconfig stops the listening process.

Set Up User Workstations

To run sessions in domain mode, install X Manager for Domains and log onto the domain.

To set up user workstations

1 Install the following feature.
   - X Manager for Domains
   - Templates
   - Java Runtime Environment (JRE) (Windows only)

2 Start X Manager for Domains.
   You'll see the domain logon dialog box.

3 Log on to the Reflection X Advantage domain.
   
   - For Username and password, enter your credentials to log onto the Reflection X Advantage domain. If your domain is configured to use the default authentication option (Windows authentication on Windows systems and PAM authentication on non-Windows systems), you can log on using the same credentials you use to log on to your computer.
   
   - For Domain, enter the Reflection X Advantage domain name. (The Reflection X Advantage domain name is always the same as the name of the computer running the domain controller.)

NOTE: From X Manager for Domains you can access any public session definitions that have been created in this domain. You can also configure your own private session definitions, which are not visible to other users. All session definition information is stored on the domain controller in the domain database.
Manage Session Persistence and Performance

If you are running in domain mode, you can use Reflection X Advantage remote session services to provide both session persistence and improved performance on some networks. Remote session services are configured on a per session basis from X Manager for Domains or the Administrative Console. These settings determine when and where sessions are held in memory.

NOTE

• The default Remote session services setting is None. To use any of the other remote session services, you must be connected to a domain with at least one domain node (page 155) available.

• When you exit X Manager for Domains, your currently running sessions may stop or they may continue to run as suspended sessions. What happens depends on your setting for Remote Session Services, your setting for On exiting X Manager, and whether or not you leave the session before you exit X Manager for Domains. For example, if Remote Session Services = Session/suspend resume, On exiting X Manager = Stop all sessions, and you exit X Manager for Domains with a session window still open, Reflection X Advantage automatically stops the session. If On exiting X Manager = Leave all sessions if possible and you exit X Manager for Domains with a session window still open, or with a session suspended, the session will continue to run as a suspended session.

To configure remote session services

1. Start X Manager for Domains.
2. Select a session. On the General tab, under Remote session services, select one of the following settings:

   None (Default)

   With this option, your session runs on your workstation, and remains available as long as X Manager for Domains is running. The session ends when you close X Manager for Domains or your workstation shuts down.

   Session suspend/resume

   Use this option to be able to rejoin a session even after you close X Manager for Domains and shut down your workstation.

   NOTE: With this configuration, your session does not persist if your workstation shuts down unexpectedly.

   Session suspend/resume; High-latency network performance

   Use this option to improve performance when you connect to an X client over a high-latency network (typically one in which your X Manager for Domains workstation is located far from the X client host computer).

   NOTE: With this configuration, your session may not persist if your workstation shuts down unexpectedly.

   Session suspend/resume; High-latency network performance; Network fault tolerance
Domain Authentication

To use the domain features you need to log into the Reflection X Advantage domain. When you start X Manager for Domains and the X Administrative Console, you'll be prompted for your domain credentials. The required credentials depend on how domain authentication is configured.

Reflection X Advantage supports the following authentication methods: Windows, PAM (Pluggable Authentication Modules), LDAP (Lightweight Directory Access Protocol), and Reflection X Advantage Internal.

In this Section

- “How Domain Access is Controlled” on page 159
- “Configure and Test User Authentication” on page 160
- “Set Up LDAP Authentication” on page 161
- “Set Up Reflection X Advantage Internal Authentication” on page 161
- “Add or Remove Domain Users” on page 162
- “Unlock a Domain” on page 162

How Domain Access is Controlled

You can leverage your existing authentication process to provide Reflection X Advantage authentication. The default Reflection X Advantage authentication method depends on the operating system of the computer on which you installed the domain controller.

You can set up your authentication system either to add users to the domain automatically when they log on, or to require that users must be added individually. (Requiring individual assignments allows you to provide access to only a subset of known users.)

Reflection X Advantage supports the following authentication methods:

- **Windows**
  
  The default authentication system when the Reflection X domain controller is installed on a Windows system.

- **PAM (Pluggable Authentication Modules)**
  
  This is the default authentication system when the Reflection X domain controller is installed on UNIX or Linux systems.

- **LDAP (Lightweight Directory Access Protocol)**
  
  A generic way of authenticating users that can be used with a number of directory servers that support LDAP. The configuration of LDAP authentication allows it to be used with different LDAP servers that have non-standard schema.
Reflection X Internal

A lightweight mechanism for authenticating users. The Reflection X Advantage administrator manually maintains a list of users.

NOTE: Automatically adding users is supported for all authentication methods except the Internal method.

Configure and Test User Authentication

Use the Administrative Console to test and configure user authentication. Basic procedures to help you get started are outlined here. For additional information, see “Domain Authentication” on page 159.

If you install your domain controller on a computer that is joined to a Windows domain, users with accounts in the same Windows domain can log onto the Reflection X Advantage using their Windows domain credentials. No additional configuration is needed. You can use the following procedure to test user authentication to the Reflection X Advantage domain.

To test authentication using Windows credentials

1. Start Reflection X Advantage Administrative Console and log on to the Reflection X Advantage domain.
2. From the tabs located along the left-hand side of the window, click Authentication.
3. Click Test Authentication to test credentials for any valid Windows domain user.

If you install your domain controller on a UNIX system, PAM authentication is used by default. Any user who can log onto the UNIX computer can log onto the Reflection X Advantage domain. You can use the following procedure to test user authentication to the Reflection X Advantage domain.

To test authentication on UNIX systems

1. Start Reflection X Advantage Administrative Console and log onto the Reflection X Advantage domain.
2. From the tabs located along the left-hand side of the window, click Authentication.
3. Click Test Authentication to test credentials for any valid account on the UNIX computer.

The internal authentication system is a light-weight authentication system that is available on all supported platforms. You may find it useful for testing or to set up a domain for a small group of users.

To configure Internal authentication

1. Start Reflection X Advantage Administrative Console and log onto the domain.
2. From the tabs located along the left-hand side of the window, click Authentication.
3. Set Authentication system to Internal.
4. Select a username, then click (or Action > Set user's password) to set the password in the Internal authentication database.

NOTE: Although an administrator account was created when you first logged on, the internal authentication database has no record of your password for this account because authentication was handled by Windows or PAM. You need to manually add users and set passwords when you use Reflection X Advantage Internal authentication. This is not required for the other
authentication methods because authentication for Windows, PAM, or LDAP is managed by those systems. If you change to Internal authentication from the default authentication, any user who was added automatically will not be able to log on until you set a password for that user.

5 Click **Test Authentication** and test your credentials to confirm that you can still log on to the domain using this account.

**CAUTION:** After changing the authentication system, always test the administrator account before you log off. Without a valid administrator account, you won't be able to log on to the domain. (If you do find yourself locked out of your domain, a recovery option (page 162) is available.)

6 Click ‼️ (or **Action > New User**) to add additional users to your domain. Enter a username and password for each user.

### Set Up LDAP Authentication

LDAP (Lightweight Directory Access Protocol) offers a generic way of authenticating users and can be used with a number of Directory Servers that support LDAP. The configuration of LDAP authentication allows it to be used with different LDAP servers that have non-standard schema.

**Before you begin**

- Add the computers that you have designated as domain components to the domain and configure the components.

**CAUTION:** Do not log off the domain without defining an administrative account. Without an administrative account, you cannot log on to the Administrative Console to manage your domain. (If you do find yourself locked out of your domain, a recovery option (page 162) is available.)

**To set up LDAP authentication**

1. On the computer on which the Reflection X Advantage Administrative Console is installed, use the Administrative Console to log on to the domain.
2. From the **Authentication** tab, in the **Authentication system** list, select LDAP and then click **Configure**.
3. From the **LDAP Configuration** dialog box, enter the configuration data for your LDAP server.
4. After you change authentication methods, make sure the domain has an administrative account and password that you can use to log on to the domain.
5. Click **Test Authentication** to make sure the account is valid.

### Set Up Reflection X Advantage Internal Authentication

The Internal authentication system is a lightweight mechanism for authenticating users.

**Before you begin**

- Add the computers that you have designated as domain components to the domain and configure the components.
CAUTION: Do not log off the domain without defining an administrative account. Without an administrative account, you cannot log on to the Administrative Console to manage your domain. (If you do find yourself locked out of your domain, a recovery option (page 162) is available.)

To set up Reflection X Advantage Internal Authentication

1. On the computer on which the Reflection X Advantage Administrative Console is installed, use the Administrative Console to log on to the domain.
2. From the Administrative Console Authentication tab, in the Authentication system list, select Internal.
3. On the User Accounts list, click +, and then from the Add user to domain dialog box, enter a user name and password for your administrative account.
4. In the Administrator column, choose to provide administrative permissions for the account.

Add or Remove Domain Users

You can set up your Reflection X Advantage domain so that users are automatically added to the domain when they log on. (This is supported for all authentication systems except the Internal system.) If you want to have more control over access, you can set up the domain so that users must be added or removed individually.

To allow access to all users in external authentication system

- In the Reflection X Advantage Administrative Console, from the Authentication tab, select Automatically create user account after successful logon.

All users who are in the authentication system are allowed access to the Reflection X Advantage domain. The first time a user logs on to the domain, his or her user account is added to the domain.

NOTE: If you are using Reflection X Advantage Internal Authentication, you cannot automatically create accounts when users log on.

To allow access to selected users only

1. In the Reflection X Advantage Administrative Console, from the Authentication tab, clear Automatically create user account after successful logon.
2. To add a user, on the User Accounts list, click +, then, from the Add User to Domain dialog box, enter the user name and password (if you are using Internal authentication) you want to add.
3. To give the new user account administrative permissions, select the box in the Administrator column.
4. To remove a user, in the User Accounts list, select the user name to remove and click –.

Unlock a Domain

You can be locked out of a domain if you forget the administrator password, change authentication methods without adding an administrative account, or experience a problem with the external authentication system.

You can unlock the domain using the rxsconfig (page 233) command line utility's recovery option.
To unlock a domain using rxsconfig

1. Log on the server on which the Domain Controller is installed as an administrator (Windows) or root (UNIX).
2. Open a command window.

   **NOTE:** On Windows systems (starting with Windows Vista and Windows Server 2008), you need to open the command window as an administrator. (In the Start menu, under **Accessories**, right-click **Command Prompt** and select **Run As Administrator**).

3. Enter the following command:

   rxsconfig recover

4. Restart the service (page 154).
5. Open the Administrative Console and log on to the domain with the following user name and password:

   user name: recovery
   password: recovery

   **NOTE:** Running the recover command allows access to the Administrative Console only once. After you log out, these login values for username and password won't work again. To log in again with these values you need to repeat steps 1 through 3.

6. Set **Authentication system** to the authentication system you want to use for the domain.
7. Click the plus sign (➕) to add a new administrative user account.
8. Select the check box under **Administrator** for the new account.
9. Click **Test Authentication** then enter the name and password for this account and click **Test** to make sure that the account is valid.

   **CAUTION:** Don't close the Administrative Console without first redefining and testing an administrative account. Without a valid administrative account, you won't be able to log back into the Administrative Console and you'll need to repeat this procedure from the beginning.

### Sample Domain Configurations

These sample configurations show how to set up domains that offer solutions to common problems.

**In this Section**

- “Domain Setup: Improve Performance Over a Slow Network” on page 163
- “Domain Setup: Leave a Session and Rejoin from a Different Computer” on page 165
- “Domain Setup: Centralize Session Configuration” on page 168

**Domain Setup: Improve Performance Over a Slow Network**

This sample configuration demonstrates how you can configure a Reflection X Advantage domain to improve performance where your network configuration causes delays that make running a remote X client application difficult.
NOTE: This configuration uses Reflection X Advantage domain components to provide remote session services for connections from X Manager for Domains. You can also configure remote session services for connections from the standalone X Manager. For details, see “How to Configure a Distributed Session in Standalone Mode” on page 147.

In this configuration, the session runs two joined X servers. An X server display runs on the user workstation (1). This server creates the visual display of the X client application. An additional “headless X server” on page 255 (3) runs on a domain node located on or near the X client application. When a session is established, all X protocol passes between the X client application (4) and the headless server. Only the protocol required to update the display is sent to the workstation. Because many X protocol queries don't need to be sent to the workstation, this configuration improves performance by reducing the amount of traffic that needs to pass over the network. Reflection X Advantage also automatically detects low bandwidth conditions, and compresses protocol that flows between the user workstation (1) and the domain node (3).

The components of this configuration are:

<table>
<thead>
<tr>
<th>Computer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User workstation (1)</td>
<td>Runs X Manager for Domains. The X server display is created on this computer.</td>
</tr>
<tr>
<td>Domain controller (2)</td>
<td>Runs the Reflection X Advantage domain controller. (In this example, the Administrative Console also runs on this computer.)</td>
</tr>
<tr>
<td>Domain node (3)</td>
<td>Runs a headless X server.</td>
</tr>
<tr>
<td>NOTE: The domain node can run on the X client host, or on a nearby computer (as shown above).</td>
<td></td>
</tr>
<tr>
<td>X client host (4)</td>
<td>The computer that runs the X client application.</td>
</tr>
</tbody>
</table>

To set up the domain components

1. On the domain controller, install the following features:
   - X Administrative Console
   - Domain Services (including the Domain Controller feature)
   - X Manager for Domains
   - Templates
   - Java Runtime Environment (JRE) (Windows only)
2 On the domain node, install the feature called **Domain Services** (without including the **Domain Controller** feature). If you are running on Windows, also confirm that **Java Runtime Environment (JRE)** is selected. Use the **rxsconfig** utility to add this node to your domain. For details, see “Set Up Domain Nodes” on page 155.

3 On user workstations, install the following features:

   - **X Manager for Domains**
   - **Templates**
   - **Java Runtime Environment (JRE)** (Windows only)

**To configure and start your session**

1 From domain controller, start X Manager for Domains and log on.
   - For **User name** and **Password**, specify any user who can log onto your computer. The name you specify for your initial login will be the default domain administrator.
   - For **Domain**, enter the name of this computer. The Reflection X Advantage domain name is always the same as the name of the computer running the domain controller.

   **NOTE:** On Windows systems, the first domain user must be a user who is a member of the same Windows domain as the user who installs Reflection X Advantage.

   On UNIX systems PAM authentication is used by default for user authentication. On some UNIX systems, the pam_securetty module is configured by default to allow root logins only if the user is logging in on a secure tty. On these systems you cannot log onto the Reflection X Advantage domain using root credentials.

   This initial logon creates an administrative account for the domain (using the default authentication method (page 159) for your system) and imports any settings you select.

2 Create a session definition that supports remote session services. To do this, in the **General** tab, under **Remote session services**, select any level of service that includes **High-latency network performance**.

3 Configure an X client or XDMCP connection and set **Session** to the session you created in step 2.

4 Start your X client or XDMCP connection.

5 In the **Session Definitions** list, select the running session to view the **Session Status** pane. Under **X Servers**, you will see an entry for your workstation computer. If high latency is detected in your network connection, you'll also see a second, headless X server running on the domain node.

**Doing more with this idea...**

Once you have this basic configuration running, you can build on it in a number of ways. For example:

   - Simplify connections for end users by configuring public sessions (page 168).
   - Add scalability by adding additional domain nodes.

**Domain Setup: Leave a Session and Rejoin from a Different Computer**

This sample configuration demonstrates how you can configure a personal Reflection X Advantage domain that makes it easy for you to continue working from home on a session you started on your work computer. You can pick up your work exactly where you left off.
The components of this configuration are:

<table>
<thead>
<tr>
<th>Computer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office computer (1)</td>
<td>Runs the domain controller, X Manager for Domains, and the Administrative Console. You can access your sessions from any computer running X Manager for Domains that has access to this computer.</td>
</tr>
<tr>
<td>Home computer (2)</td>
<td>Runs X Manager for Domains.</td>
</tr>
<tr>
<td>X client host (3)</td>
<td>The computer that runs the X client application.</td>
</tr>
</tbody>
</table>

**To set up the domain components**

1. On your office computer, install the following features:
   - **X Administrative Console**
   - **Domain Services** (including the **Domain Controller** feature)
   - **X Manager for Domains**
   - **Templates**

2. From your office computer, start the Administrative Console and log on using your Windows domain credentials. For domain name, enter your computer's name.

3. From the tabs located along the left-hand side of the window, click **Authentication**.

   Notice that your name is already added to the list of user accounts and is selected as the administrator. By default, the first user to log on is set as the Reflection X Advantage domain administrator. For this sample configuration, no additional authentication configuration is needed.

   The next step configures your office computer to act as a domain node. By creating a node, you enable your domain to maintain a suspended session even after you close X Manager for Domains.

4. Open a Command Prompt window (Windows) or terminal window (UNIX) and run the following command:
rxsconfig join localhost

You'll be prompted for Administrator credentials. Enter the user name and password you use to log onto this computer. You'll see a message saying that node was successfully created. In the Administrator Console you can now see your computer listed in the Domain Composition pane under Domain Nodes.

5 On your home computer, install X Manager for Domains.

To configure and start a session at work

1 From your work computer, start X Manager for Domains and log on with the same user name and password you used for the Administrative console. For domain, specify the name of your office computer.

2 Create a session definition that supports suspending sessions. To do this, in the General tab, under Remote session services, select Session suspend/resume.

3 Configure an X client or XDMCP connection and set Session to the session you created in step 2.

4 Start your X client or XDMCP connection and get some work done.

5 When it's time to go home, under Session Definitions, right-click the running session and click Leave.

6 Close X Manager and leave this computer running.

**NOTE:** Because you enabled session persistence and left the session running, the server remains active even though it is no longer producing a display. To confirm this, you can start the Administrative Console, click the Domain Status tab and view Running Sessions.

To join your session in progress from your home computer

1 Confirm that your home computer has network access to your running computer at work.

2 Start X Manager for Domains and log on with the same user name and password you used on your office computer. For domain, specify the name of your office computer.

3 Right-click your running session and click Join.

Persisting a Session on the X Client Host

In the configuration shown above, the session components run on your office computer, which means that you need to leave that computer running if you want to rejoin the session from home.

Another possible configuration is shown below. In this configuration, the domain controller and domain node run on the same computer that runs the X client application. To configure this, install the domain controller on the X client host and create a domain node on that host. With this setup, you can shut down both your home and office computer, and the session will remain active on the X client host.
Domain Setup: Centralize Session Configuration

This sample configuration demonstrates how an administrator can use a Reflection X Advantage domain to simplify session setup for end users. In this example, the administrator configures public session definitions. End users can launch these public sessions from their workstations, and can also create and start their own sessions.

The components of this configuration are:

<table>
<thead>
<tr>
<th>Computer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Workstation (1)</td>
<td>Runs X Administrative Console and X Manager for Domains. The administrator uses these to manage the domain, and to configure and share public session definitions.</td>
</tr>
<tr>
<td>Domain Controller (2)</td>
<td>Runs the Reflection X Advantage domain controller and X Administrative Console. Session information is stored on this computer in the domain controller database.</td>
</tr>
<tr>
<td>User workstations (3)</td>
<td>The user runs public sessions configured by the administrator and can optionally create additional private sessions.</td>
</tr>
<tr>
<td>Domain nodes (4)</td>
<td>(Optional) Run remote session components when sessions are configured to use remote session services.</td>
</tr>
<tr>
<td>X client hosts (5)</td>
<td>The computers that run X applications used in your organization.</td>
</tr>
</tbody>
</table>
The administrator uses the Administrative console (1) to configure the domain controller (2). When users start sessions, the domain controller can set up session components on user workstations (3) or domain nodes (4):

The X server displays are created on user workstations using the centrally managed configurations:
These are the basic steps for setting up this configuration. They are explained in detail below.

Step 1: Set up Reflection X Advantage domain components.

Step 2: Use X Manager for Domains on the administrative workstation to configure and test client and session definitions.

Step 3: Use the Administrative Console to make your definitions public.

Step 4: Use X Manager for Domains on the user workstation to connect using the public definitions.

**Step 1: Set up Reflection X Advantage domain components**

1. On the domain controller, install the following features:
   - Domain Services (including the Domain Controller feature)
   - Java Runtime Environment (JRE) (Windows only)

2. On the administrative workstation, install the following features:
   - X Administrative Console
   - X Manager for Domains
   - Templates
   - Java Runtime Environment (JRE) (Windows only)

3. On user workstations install the following features:
   - X Manager for Domains
   - Java Runtime Environment (JRE) (Windows only)

4. If you are using domain nodes, install Domain Services on these computers (without including the Domain Controller feature). If you are running on Windows, also confirm that Java Runtime Environment (JRE) is selected. Use the rxsconfig utility to add each node to your domain. For details, see “Set Up Domain Nodes” on page 155.

**Step 2: Configure and test a session**

In the steps that follow, you'll use X Manager for Domains to configure and test a client and session. It is also possible to these definitions using the X Administrative Console, but starting with X Manager for Domains is recommended because it enables you to test your configuration.

1. **From the administrator workstation, start X Manager for Domains and log on.**
   - For **User name** and **Password**, specify any user who can log onto your computer. The name you specify for your initial login will be the default domain administrator.
   - For **Domain**, enter the name of this computer. The Reflection X Advantage domain name is always the same as the name of the computer running the domain controller.

   **NOTE:** On Windows systems, the first domain user must be a user who is a member of the same Windows domain as the user who installs Reflection X Advantage.

   On UNIX systems PAM authentication is used by default for user authentication. On some UNIX systems, the pam_securetty module is configured by default to allow root logins only if the user is logging in on a secure tty. On these systems you cannot log onto the Reflection X Advantage domain using root credentials.

   This initial logon creates an administrative account for the domain (using the default authentication method (page 159) for your system) and imports any settings you select.

2. Configure an X client or XDMCP connection to connect to your X client application or your UNIX desktop.
Domain Administration

NOTE: If you are creating new client definitions, you should leave User name blank because you are going to share this session definition with others. After you make this session public, users can enter their name during the connection process.

3 (Optional) If you have configured domain nodes, you can configure a session in which Remote session services is set to something other than None. If you do this, specify this session as the default for your clients.

4 Start your X client or XDMCP connection.

If your connection is successful, you're ready to make this session definition available to other users.

Step 3: Make the session public

By default, a new session is private. A private session definition can be viewed, used, and modified only by the user who created it. To make your session available to other users, you need to make it public.

NOTE: When you make a client definition public, users also need access to the associated session and any other definition used by the client

1 From the administrator workstation, start the Administrative Console and log on using the same credentials you used to log onto X Manager for Domains.

2 Right-click the client definition and select Public. Note that the icon changes to indicate that this is now a public session.

3 If the client reference a session, right click the session definition and select Public.

Now that the administrator's work is done, all a user needs to know to get connected is:

- The name of the Reflection X Advantage domain. (The name of the computer running the domain controller.)
- Logon credentials for the Reflection X Advantage domain. (If you manually added users to the internal authentication database, you need to provide them with these credentials. If you use the default Windows or PAM for authentication, users can log on to the Reflection X Advantage domain using those credentials.)
- Logon credentials for the X client host.

Here's how it works...

Step 4: Make a connection from the user workstation using the public session

1 From the user workstation, start X Manager for Domains.

2 Enter the domain name provided by the administrator. If default domain authentication is used, the username and password required are the same ones you use to log onto this workstation.

3 Double click any public definition to make a connection, then log on to the host.

Doing more with this idea...

As an Administrator, you can further simplify the end-user experience using the Automatically start client setting in your public client definitions. Also ensure that each client has a default session configured. With this configuration, all a user has to do to start your public clients is log into the domain.
X Administrative Console

X Administrative Console is an application used by domain administrators to set up and centrally manage a Reflection X Advantage domain. Use it to manage domain authentication, centrally manage sessions, manage domain nodes, and domain security settings.

X Administrative Console is typically installed on the domain controller. You can also install it on additional workstations to manage the domain from those computers.

In this Chapter

- “How to...” on page 173
- “Interface Reference” on page 178

How to...

The topics in this section describe the tasks you can perform with the Administrative Console.

In this Section

- “Start the X Administrative Console” on page 173
- “Add or Remove Domain Administrators” on page 174
- “Configure Load Balancing” on page 175
- “Raise a Domain Node Priority for Running Sessions” on page 175
- “Stop a Session” on page 175
- “Monitor Sessions” on page 176
- “Change a User Password” on page 176
- “Share Settings with Domain Users” on page 176
- “Add a Trusted Host Key for all Domain Users” on page 177
- “Import a Trusted Host Key Using the Administrative Console” on page 178

Start the X Administrative Console

You can start the Administrative Console from your desktop user interface or from the command line.

To start the X Administrative Console from your computer desktop

1. Start the Administrative Console:
On the Reflection X domain:

For **Username** and **password**, enter your credentials to log onto the Reflection X Advantage domain. If your domain is configured to use the default authentication option (Windows authentication on Windows systems and PAM authentication on non-Windows systems), you can log on using the same credentials you use to log on to your computer.

For **Domain**, enter the Reflection X Advantage domain name. (The Reflection X Advantage domain name is always the same as the name of the computer running the domain controller.)

**To start the Administrative Console from the command line**

1. From a command prompt, navigate to your Reflection X Advantage installation folder:
   - On Windows:
     cd C:\Program Files\Micro Focus\Reflection
   - On UNIX:
     cd /opt/rxadvantage
2. Enter rxadmin (or ./rxadmin for UNIX).

When the Administrative Console opens, you are prompted to log on to a domain.

**Add or Remove Domain Administrators**

A domain administrator can assign the domain administrator role to other users in the domain. Only domain administrators can log on to the Administrative Console.

**To grant administrative privileges to selected domain users**

1. In the Reflection X Advantage Administrative Console, click the **Authentication** side tab.
2. In the **User Accounts** list, find the user to which you will grant Administrator permissions. Or, to add a user, on the **User Accounts** list, click +, then, from the **Add User to Domain** dialog box, enter the user name and password (if you are using Internal authentication) you want to add.
3. To give the user account administrative permissions, select the box in the **Administrator** column.

**NOTE**: If you configure multiple domain administrators, each administrator can view and edit all definitions, whether or not the owner has made them public.
Configure Load Balancing

You can adjust load balancing by setting the relative capacity of domain nodes. For example, although your domain might have several nodes with similar capacity, you may want to run most of your sessions on one node to leave the other nodes available for other system tasks. You could accomplish this by specifying a high relative capacity for that node.

To configure load balancing

1. From the Administrative Console Domain Composition tab, under Domain Properties, select the load balancing scheme that best suits your site:
   - Round Robin: Assign sessions to each domain node in sequential order.
     NOTE: Higher capacity nodes will appear more often in the sequence (a weighted round-robin).
   - Optimize CPU: Assign sessions to nodes based on available processing power.
   - Optimize Memory: Assign sessions to nodes based on available memory.

2. Under Domain Nodes, select the node.

3. Under Registration Details, adjust the Relative capacity slider to specify how much to "weigh" the node for load balancing. (If you set a high relative capacity for a node, Reflection X Advantage is more likely to start sessions on that node than on other nodes with similar capacity.)

4. Confirm that the option Participate in domain is enabled for the node. (This is the default.)

5. Repeat Steps 2-4 for each node.

Raise a Domain Node Priority for Running Sessions

You can customize a domain node to be the preferred location to run X Manager sessions.

To raise a domain node priority

1. From the Administrative Console Domain Composition tab, select the node.

2. Under Registration Details, adjust the Relative Capacity slider to the highest level. (If you set a high relative capacity, Reflection X Advantage is more likely to start sessions on this node than on other nodes with similar capacity.)

3. Confirm that the option Participate in domain is enabled for the node. (This is the default.)

Stop a Session

A user typically stops his or her own sessions. However, if necessary, you can stop sessions from the Administrative Console (for example, should a problem with a session arise, or if there is an abandoned session).

To stop a user's session

1. From the Administrative Console Domain Status tab, click the Running Sessions tab and then select the session you want to stop.

2. From the Action menu, choose Stop Session.
Monitor Sessions

From the Administrative Console, you can monitor all of the sessions on the domain. You can view the status of all sessions running on the domain. You can also view the load and memory usage of the domain node or nodes associated with each session.

NOTE: Depending on which options you select for the session, session components may run on more than one domain node.

To view session status details

1. From the Administrative Console Domain Status tab, click the Running Sessions tab.
   
   The Administrative Console displays all of the sessions running in the domain, along with the session names, owners, and the domain nodes on which they are running.

2. Select the session that you want to monitor.

   The Administrative Console displays session details such as how long the session has been running, the location of the client connectors, and all of the X servers that have joined the session.

3. Next to Location, click the double arrow button to display details about the domain node that is running the session.

   The Domain Nodes tab displays the domain node name, the state of the session, the current processing load of the node, and its memory use.

Change a User Password

If you are using the Reflection X Advantage Internal authentication system, you can change user passwords. For all other authentication systems supported by Reflection X Advantage (Windows, LDAP, PAM), passwords are maintained externally.

NOTE: If you change a user password while the user is logged on, the old password is valid until he or she logs off.

To change a user password

1. From the Administrative Console Authentication tab, from the User Accounts list, select a user.

2. From the File menu, select Change Password.

3. Type the new password, and then confirm it by typing it again.

NOTE: You do not have to provide the existing password to change a user password.

Share Settings with Domain Users

As an administrator, you can make definitions available to other Reflection X Advantage domain users. Only an administrator can make definitions public, and users cannot edit these definitions.

When you make a definition public, all of the associated components for that definition must also be public. For example, if you make an X client definition public, a session definition referenced in the client definition must also be public, as must any shared font collection or color scheme. If you are setting up a public Secure Shell client definition, you can make the host key public as well.
To create a public definition

1. Log on to X Manager for Domains with your Reflection X Advantage domain administrator account.
2. Configure and test the definitions you want to share.
3. If you are using a client definition that includes a telnet, rexec, or rlogin, clear any saved passwords before you make the definition public.
4. Log on to the X Administrative Console with your domain administrator account.
5. From the Domain Definition tab, right-click a definition and select Make Public.
6. Make all associated definitions public in the same way. For example, any session definitions used in your client definitions must be made public. If you make a launch group public, make all clients in that group public. If your session uses any non-default color schemes or font collections, also make these public.
7. To test your changes, log on to X Manager for Domains with an alternate Reflection X Advantage account. Logging on with a different account allows you to see and test your changes as a regular user. Start your public definitions to confirm that you have shared all required components.

Related Topics

- “Export and Import Definitions” on page 57

Add a Trusted Host Key for all Domain Users

Public key authentication of the Secure Shell server is a standard feature of the Secure Shell protocol. If the host public key has not previously been installed in the host key database, the first time a user makes a Secure Shell connection, he or she sees the Host Key Unknown dialog box. This dialog box includes a fingerprint that identifies the Secure Shell host. To be sure that this is the correct host, the user should contact the Secure Shell server system administrator who can confirm that this is the correct fingerprint. Without confirmation, the user is at risk of a "man-in-the-middle" attack, in which another server poses as the Secure Shell server.

By installing the host key in the host key database and making this key public, an administrator can ensure that the host is correctly authenticated without requiring users to respond to the Host Key Unknown dialog box.

NOTE: This procedure adds the key to the database by accepting an unknown key when you connect to the host. If you already have the host key, you can also import it directly to the domain and then make it a public host key. For details, see “Import a Trusted Host Key Using the Administrative Console” on page 178

To add a host key to the database and make it available to all users of a domain

1. From X Manager, configure an X client that uses Secure Shell as the connection method.
2. Start the client.
3. Confirm the key fingerprint is correct and click Always to add the host key to the host key database.
4. On the Administrative Console Domain Definitions tab, under Trusted Host Keys, select the key.
5. On the Action menu, choose Make > Public.
Import a Trusted Host Key Using the Administrative Console

Public key authentication of the Secure Shell server is a standard feature of the Secure Shell protocol. You can add trusted host keys to the domain. If you want anyone in the domain to be able to use these keys, you can share them as public keys.

To import a trusted host key to the domain

1. From the Administrative Console Domain Definitions tab, in the left-hand panel, next to Trusted Host Keys click +.
2. From the Import Host Key dialog box, enter the host name and then browse to the public key file.
3. To make the key public, select the key and, from the Action menu, choose Make Public.

Interface Reference

Use the topics in this section to understand the features and functionality provided by the Administrative Console.

In this Section

- "Domain Composition Tab" on page 178
- "Domain Status" on page 181
- "Domain Definitions Tab" on page 185
- "Authentication Tab" on page 188
- "Administrative Console Menus" on page 189

Domain Composition Tab

Getting there

- From the Administrative Console, click the Domain Composition side tab.

From the Domain Composition tab, you can configure:

Domain Nodes (page 178)
Domain Security (page 180)
PKI Configuration (page 180)

Domain Nodes - Domain Composition

Getting there

- From the Administrative Console Domain Composition tab, under Domain Nodes, select a node.
A Reflection X Advantage domain consists of one or more domain nodes (computers in the domain). Each domain must have one domain controller, which runs the domain controller service. Domains can also have additional domain nodes that are used to run sessions, which support session persistence. Domain nodes can also be installed on application hosts to enable compression from the host.

Registered Nodes

Shows nodes that have been configured for this domain. The node includes a port assignment if it is not the default value (22001).

Use the `rxsconfig` (page 233) utility to add and remove the registered domain nodes displayed here. For details, see “Set Up Domain Nodes” on page 155 and “Remove a Domain Node” on page 156. Although you can delete a node here, this will not remove its configuration on the domain node machine.

If the domain node icon shows a red slash, the node is unavailable. For troubleshooting, see “Domain Node is Unavailable” on page 252.

Registration Details

<table>
<thead>
<tr>
<th>Node</th>
<th>The DNS network name or IP address of the domain node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly name</td>
<td>Set the domain node name. This name is displayed in the Domain Composition and Domain Status tabs. Specify a name that easily distinguishes this domain node from others.</td>
</tr>
<tr>
<td>Alternate addresses</td>
<td>To connect to a domain node through a firewall that is using Network Address Translation (NAT), you must specify the alternate public address that Reflection X Advantage should use for the connection. Supply a comma delimited list of hosts and their associated ports. For example: <code>alternate.company.com:1234, 10.10.0.2:5678</code></td>
</tr>
<tr>
<td>Relative capacity</td>
<td>Set the performance capacity of this node relative to others in the domain to fine tune load balancing. For example, if you have two domain nodes (computers) with roughly the same CPU and memory, but you want to use one of them for other tasks, you can set the relative capacity of that server to the Low end of the scale. When the Reflection X Advantage Domain Controller performs load balancing, it is less likely to assign sessions to that node.</td>
</tr>
<tr>
<td>Participate in domain</td>
<td>Configures the node to service new sessions. When cleared, the node is removed from the load balancing scheme. The Reflection X Advantage Domain Controller does not start new sessions or client connectors on the node. This allows you to prepare a node for shutdown (or reboot) without impacting running sessions.</td>
</tr>
</tbody>
</table>

Load balancing

When your domain is supporting multiple sessions that are using session persistence, Reflection X Advantage may need to run more than one session on each domain node. Load balancing improves session performance by ensuring that the load is distributed among all of the nodes. The load balancing scheme you select here is used for the entire domain. To adjust load capacity for each domain node, use the Relative capacity slider.
Domain Security and PKI Configuration - Domain Composition

Getting there

- From the Administrative Console, click the Domain Composition side tab.

Domain security items apply globally to all of the nodes in the domain.

FIPS mode

Enforces the United States government Federal Information Processing Standard (FIPS) 140-2 for this connection. When FIPS mode is selected, all available settings use security protocols and algorithms that meet this standard. Encryption options that do not meet this standard are not available; only the Secure Shell connection method can be used to start X clients, and XDMCP is not available as a session startup option.

NOTE: Changes to the FIPS mode state will take effect only upon restart of the domain. You must also enable FIPS mode in X Manager for Domains. Each time you change the FIPS mode setting, you must restart the Reflection X Service on the Domain Controller.

PKI Configuration

Use the PKI Configuration items to configure connections to PKI Services Manager, a free add-on utility that provides X.509 certificate validation services. This utility is required if your client hosts authenticate using certificates. Before you configure the options on this tab, you need to download and configure this free add-on utility.

PKI service

Specify the host name or IP address of the computer running PKI Services Manager.

NOTE: If PKI Services Manager is configured to use a non-default port, include the port value using hostname:port syntax. For example acme.com:18081.

Public key

These read-only items display information about a PKI Services Manager public key after it has been successfully imported.

MD5 fingerprint

SHA1 fingerprint

Import Key

Use this option to manually import the PKI Services Manager public key. First, copy the key from the PKI Services Manager computer (default locations are below) to any location available from Reflection X Advantage.

The default location on Windows is:

c\common application data\folder (page 258)\Attachmate\ReflectionPKI\config\pki_key.pub

The default location on UNIX is:

/opt/attachmate/pkid/config/pki_key.pub
You can use the Administrative Console to configure a Reflection X domain to run in FIPS mode.

When Reflection X is configured to run in FIPS mode it enforces the United States government Federal Information Processing Standard (FIPS) 140-2. All available settings use security protocols and algorithms that meet this standard. Options that do not meet these standards are not available, and only the Secure Shell connection method can be used to start X clients.

The United States government's Federal Information Processing Standard (FIPS) 140-2 specifies security requirements for cryptographic modules. Cryptographic products are validated against a specific set of requirements and tested in 11 categories by independent, US government-certified testing laboratories. This validation is then submitted to the National Institute of Standards and Technology (NIST), which reviews the validation and issues a certificate. In addition, cryptographic algorithms may also be validated and certified based on other FIPS specifications. The list of certified products and the vendor's stated security policy (the definition of what the module has been certified to do) can be found at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm.

NOTE: Important note: If you are configuring Reflection X to use FIPS mode, you should ensure that you are running a version that has met all FIPS 140-2 standards. Contact Micro Focus Technical Support for more information.

Federal Information Processing Standard (FIPS)

Domain Status

Getting there

- From the Administrative Console, click the Domain Status side tab.

Use the tabs under Domain Status to view runtime statistics of the domain. You can view information about the X sessions or the nodes (computers) active in this Reflection X Advantage domain in the following sections:
Running Sessions - Domain Status

Getting there

From the Administrative Console

1. Click the **Domain Status** tab.
2. From the **Running Sessions** tab, select a session to display details about the session.

From the X Manager

1. Under **Session Definitions**, running sessions appear beneath the session definition.
2. Select a running session to display the **Session Status** pane on the right with details about the session.

You can view details about all of the running sessions, such as the session names, owners, and the computers on which they are running.

When you select a session, you can view additional details such as how long the session had been running, the location of the client connectors, and all of the X servers that have joined the session.

If you see a double arrow button next to **Location** (on the right side of the window), you can move quickly to a view that is centered on the node (computer) running the session.

<table>
<thead>
<tr>
<th>Session Name</th>
<th>The session definition name on which this session is based.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session ID</td>
<td>A unique identifier for each session. The session ID is useful for identifying log file messages that pertain to each running session.</td>
</tr>
<tr>
<td>Location</td>
<td>The computer in the domain that is running this session.</td>
</tr>
<tr>
<td>Owner</td>
<td>The user who started the session.</td>
</tr>
<tr>
<td>State</td>
<td>Session state — <strong>Starting</strong>, <strong>Stopping</strong>, <strong>Running</strong>, or <strong>Resetting</strong>.</td>
</tr>
<tr>
<td>Time in state</td>
<td>The length of time since the session state last changed.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The amount of time that has elapsed since the session was started.</td>
</tr>
<tr>
<td>Allowed Users</td>
<td>(Domain mode only) (page 258) All users allowed to join the session are listed here.</td>
</tr>
<tr>
<td>Allow users to take control of session</td>
<td>If you are the creator of the session, while the session is running you can select this option to allow users to take control of a session they have joined.</td>
</tr>
<tr>
<td></td>
<td>• In Standalone mode, this option applies to all users who join the session using the session's <strong>Connection URL</strong>.</td>
</tr>
<tr>
<td></td>
<td>• In Domain mode, this option applies to all <strong>Allowed Users</strong>.</td>
</tr>
</tbody>
</table>
Client Connectors

The client connectors for a session accept incoming connection requests from X clients and forward X protocol requests received from the X client to the session.

<table>
<thead>
<tr>
<th>Location</th>
<th>The name of the computer on which the client connector is running.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listening IP/Display</td>
<td>The network address and display number of the X session to which the client connector belongs. A single client connector might have more than one listening IP/display pair if more than one network card is present. X clients locate an X session by this pair of values. This is done by setting the DISPLAY environment variable (or the X client command line option &quot;-display&quot;) to &lt;network address&gt;:&lt;display number&gt;.</td>
</tr>
<tr>
<td>X Client Count</td>
<td>The number of X clients connected to this client connector.</td>
</tr>
</tbody>
</table>

X Servers

Shows details about the X servers connected to this session.

<table>
<thead>
<tr>
<th>Location</th>
<th>The computer on which this X server is running.</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>The user running this X server.</td>
</tr>
<tr>
<td>Compression</td>
<td>Shows whether protocol is compressed between this server and the session's protocol router. If protocol is compressed, or if this is a headless server, this column also displays additional statistics about the data exchange. For details, see “Session Statistics” on page 121.</td>
</tr>
<tr>
<td>Input Allowed</td>
<td>Mouse and keyboard input. If user input is enabled for this X server, the status is Yes. Input is allowed from only one X server at a time.</td>
</tr>
<tr>
<td>Latency</td>
<td>Displays the “latency” on page 256 (in milliseconds) of the connection between the computer running this server and the computer running the session's protocol router. If the server is running locally, this column shows &quot;N/A&quot;.</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Displays the “bandwidth” on page 255 of the connection between the computer running this server and the computer running the session's protocol router. If the server is running locally, this column shows &quot;N/A&quot;.</td>
</tr>
</tbody>
</table>

Related Topics

- “Reflection X Advantage Session Processes” on page 150
- “Operating Modes: Domain vs. Standalone” on page 8
- “Monitor Sessions” on page 176

Domain Nodes - Domain Status

Getting there

From the Administrative Console

1. Click the Domain Status tab.
2. From the Domain Nodes tab, select a node to display details about the node.
You can check each node to find the number of sessions running on the node, the node’s current processing load, and its memory use. You can also find the status of all the client connectors running on the node. (This information is presented in a node-centric view, rather than the session-centric view presented from the Running Sessions - Domain Status tab.)

**Node**
The DNS name or IP address of the domain node.

**Host OS**
The host operating system type of this node.

**State**
The node state is online, offline, or idle.

**Process ID**
The process ID of the running node. The process ID is useful for identifying log file messages that pertain to each node.

**Load**
The load is the percentage of CPU that the domain node process is using. It is not a measure of the overall CPU utilization on the machine.

**Memory use**
Memory use is a measure of the memory consumed by the domain node process.

### Sessions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Name</td>
<td>The name of the session running on this node.</td>
</tr>
<tr>
<td>Owner</td>
<td>The user who owns the session.</td>
</tr>
<tr>
<td>State</td>
<td>The session state — Starting, Stopping, Running, or Resetting.</td>
</tr>
<tr>
<td>X Client Count</td>
<td>The number of X clients connected to this session.</td>
</tr>
<tr>
<td>X Server Count</td>
<td>The number of X servers connected to this session.</td>
</tr>
<tr>
<td>Listening IP/Display</td>
<td>The network address and display number of the X session to which the client connector belongs. A single client connector might have more than one listening IP/display pair if more than one network card is present. X clients locate an X session by this pair of values. This is done by setting the DISPLAY environment variable (or the X client command line option &quot;-display&quot;) to &lt;network address&gt;:&lt;display number&gt;.</td>
</tr>
<tr>
<td>X Client Count</td>
<td>The number of X clients connected to this client connector.</td>
</tr>
</tbody>
</table>

### Client Connectors

The client connectors for a session accept incoming connection requests from X clients, and forward X protocol requests received from the X client to the session.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Name</td>
<td>The name of the session that this client connector is servicing.</td>
</tr>
<tr>
<td>Listening IP/Display</td>
<td>The network address and display number of the X session to which the client connector belongs. A single client connector might have more than one listening IP/display pair if more than one network card is present. X clients locate an X session by this pair of values. This is done by setting the DISPLAY environment variable (or the X client command line option &quot;-display&quot;) to &lt;network address&gt;:&lt;display number&gt;.</td>
</tr>
<tr>
<td>X Client Count</td>
<td>The number of X clients connected to this client connector.</td>
</tr>
</tbody>
</table>
Domain Definitions Tab

Getting there

- From the Administrative Console, click the Domain Definitions side tab.

The domain definitions listed include public definitions that you or other administrators have created and shared, or private session definitions that you have created for personal use.

NOTE

- The items listed in the Domain Definitions tab can all be configured using X Manager for Domains. Although you can also configure these definitions using the Administrative Console, you can't start sessions from the console. Because testing is easier from X Manager for Domains, it is generally preferable to use it when you are creating and editing definitions.

- Use the Domain Definitions tab to make your definitions available to other users. Select the definition you want to share, then click Action > Make Public. The ability to make definitions public isn't available from X Manager for Domains.

Color Schemes (Administrative Console)

Getting there

1. From the Administrative Console, click the Domain Definitions tab.
2. From the left pane, under Color Schemes, select a scheme or click the plus sign (+) to add a new definition.

The right pane displays details about the selected color scheme definition.

In the left pane, under Color Schemes is a list of all the color schemes you have created or imported, and all public schemes created by the administrator(s).

For many client applications, you can use the default color scheme provided by Reflection X Advantage. However, if a client application requires specific color names that are not defined in the default color scheme, you will need to define a custom color scheme. You can also specify a custom color scheme to control the look-and-feel of the application.
Available Color Schemes

**Color Schemes**

Lists your color schemes, including the default color scheme, all public color schemes, and any schemes that you own (schemes that you have imported or cloned).

Color schemes translate string color names requested by clients into red, green, blue (RGB) values. If a client requests colors by name, the color scheme determines which colors are displayed by the X server. By changing the color scheme, you can change the displayed colors.

**NOTE:** Not all X clients request colors by name — many clients request colors by RGB value or other methods, instead of specifying a color name. Changing the color scheme changes the colors the X server displays only when clients request colors by name.

If you change a color scheme that is in use by a running session, the changes do not affect the session until it is restarted.

**+** and **–** controls

Import or remove color schemes.

**NOTE:** You cannot remove public schemes that are owned by other administrators.

**Arrow controls**

Move the selected item higher or lower in the list.

Use options on the **Action** menu to manage color schemes for the domain:

**Clone**

Copy the current color scheme. In X Manager for Domains, if you copy a public definition that is read-only, you can edit the copy.

**Import Color Scheme**

Opens the **Import Color Scheme** dialog box, from which you can import an existing RGB color text file to create a new color scheme.

**Make Public**

Makes the color scheme available to anyone logged on to this domain. The scheme can be modified only by its owner.

**Color Scheme pane**

When you select a color scheme, color details associated with that scheme are displayed on the right. Use the options from the **Color Scheme** pane to view, edit, or remove colors in a scheme, or to create new colors for a scheme:

**Scheme name**

The name of the color scheme definition. Use the one provided, or enter your own.

**Colors in scheme**

Displays the entries in the RGB color scheme in a two-column table. The first column shows how the color appears on your display; the second shows the name of the color.

**NOTE:** Many of the colors have two names: a single name with mixed case (for example, ForestGreen), and another in all lowercase (for example, forest green). Both names are included because X clients might request the color by either name.

**+** and **–** controls

Add or remove colors from the scheme.

**Color column sorts by**

Specify the way you want the Color column to sort: by hue (the default), saturation, or brightness.
HSB Displays hue, saturation, and brightness (HSB) values for the color selected in the Color column. Use the slider on the HSB tab to change the HSB values of the selected color.

NOTE: The HSB slider is not displayed for default color schemes because these schemes cannot be modified.

RGB Displays the red, green, and blue (RGB) values for the color selected in the Color column. Use the sliders on the RGB tab to change the RGB values of the selected color.

NOTE: The RGB slider is not displayed for default color schemes because these schemes cannot be modified.

Preview Shows how the color selected in the Color column will appear.

Related Topics
- “Work with Colors” on page 44
- “Customize a Color Scheme” on page 46
- “Import a Color Scheme” on page 45
- “X Window System Color Support” on page 46

Trusted Host Keys

Getting there
- From the Administrative Console Domain Definitions tab, under Trusted Host Keys, select a key.

NOTE: You can use the administrative console to manage trusted host keys for all users of the domain. Individual users can also add trusted host keys using X Manager for Domains.

When you select a key under Trusted Host Keys, the following information is displayed.

Host Displays the name of the host that authenticates with this key.

Type Indicates whether the key uses either an RSA or DSA algorithm.

Public Indicates whether the host key is available to other users in the Reflection X Advantage domain. When an administrator uses the Administrative Console to make the key public, this host is trusted by other users in the domain. This means they can connect to the host without needing to respond to the unknown host prompt.

MD5 fingerprint Shows the key fingerprint in MD5 and SHA1 format. Fingerprints provide a way to reliably identify the host key.

SHA1 fingerprint

Import Host Key Dialog Box

Getting there

From X Manager
- From the Tools menu, click Secure Shell Host Keys, and then from the Secure Shell Host Keys dialog box, click the plus sign (+) at the top of the Trusted Host Keys list.
From the Administrative Console

1. Click the **Domain Definitions** tab.
2. In the left pane, click the plus sign (+) next to **Trusted Host Keys**.

From this dialog box, you can import trusted host keys. The options are:

- **Host name**
  - Type the name of the host.

- **Public key file**
  - Enter the name of the file, or use the **Browse** button (...) to locate the public key of the host public/private key pair.

- **Import**
  - Click to add the selected key to your trusted host keys.

## Authentication Tab

### Getting there

- From the Administrative Console, click the **Authentication** side tab.

A Reflection X Advantage domain authenticates each user before granting access. You can use Reflection X Advantage Internal authentication, or you can leverage your in-place authentication and security infrastructure. Reflection X Advantage supports the following authentication methods:

- Windows Domain (or Windows local) — the default when the Reflection X Advantage domain controller is installed on a Windows operating system
- Pluggable Authentication Modules (PAM) — the default when the Reflection X Advantage domain controller is installed on a non-windows operating system
- Lightweight Directory Access Protocol (LDAP)
- Reflection X Advantage Internal

Only one authentication mechanism can be configured and active for a domain at any given time.

<table>
<thead>
<tr>
<th>Authentication system</th>
<th>Specifies the authentication system to use for the domain. The supported systems depend on your platform:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>UNIX: Pluggable Authentication Modules (PAM) (the default), Reflection X Advantage Internal, and LDAP.</td>
</tr>
</tbody>
</table>

- **Configure**
  - Configure Reflection X Advantage for the authentication system you selected.

- **Test Authentication**
  - Tests the user or administrative account.

- **Automatically create user account after successful logon**
  - Specifies that all users who are in the authentication system are allowed access to the Reflection X Advantage domain. When a user logs on to the domain, his or her user account is added to the domain.

- **User Accounts**
  - Displays all of the user accounts in the domain. For each account, this table displays the user name, the last logon, and whether the account has Administrator permissions. (It also allows you to set or remove administrator permissions for an account.)

  **NOTE:** If you configure multiple domain administrators, each administrator can view and edit all definitions, whether or not the owner has made them public.
LDAP Configuration dialog box

Getting there

1. From the Administrative Console, click the Authentication side tab.
2. From the Authentication system list, choose LDAP and then click Configure.

Use the LDAP Configuration dialog box to set up your Reflection X Advantage domain for LDAP authentication. The options are:

- **LDAP host**: The host the LDAP server is running on.
- **LDAP port**: The port the LDAP service is listening on.
- **Use anonymous SSL**: Allows communication with the LDAP server to be encrypted. The anonymous SSL option supports standard SSL ciphers but does not verify the authenticity of the LDAP server's certificate.
- **Search base**: The area in the directory tree where the users reside. This is the location in the directory from which the LDAP search begins.
- **DN Schema**: The distinguished name schema (typically “distinguishedName”). An LDAP entry is referenced by a distinguished name that uniquely identifies the entry in the directory. It is typically composed of several relative distinguished names (RDN) separated by commas.
- **UID attribute**: The unique or user id attribute (for most LDAP users, this is uid. For Microsoft Active Directory users, this is “sAMAccountName”).
- **Perform authenticated search**: Allows you to enter credentials for a user with search permissions. This is used when the directory service does not allow anonymous searching.
- **User DN**: The distinguished name of a user with permissions to search the directory service.
- **Password**: The password for the distinguished name that you entered in User DN.

Related Topics

- “Domain Authentication” on page 159

Administrative Console Menus

**File Menu**

The File menu provides options for logging on and off, and configuring logon and status message preferences and passwords. It also provides access to the Definition Trashcan, with options to restore or permanently discard the deleted items that are stored there.

**Go Menu**

The Go menu provides options to move among the four administrative tabs in the console: Domain Composition, Domain Status, Domain Definitions, and Authentication.

**Action Menu**

The Action menu provides options for performing different tasks related to managing the group of domain features available from the currently active side tab.
Help Menu

Using the commands from this menu, you can configure your view of the online Help and reach additional Help resources.

The options are:

- **Help Topics**
  Access the online Help system.

- **Show Help Tips**
  Select to display Help tips when hovering over items with the mouse.

- **Micro Focus Support Site**
  Visit the Micro Focus Support Web site for the most recent technical information on Reflection X Advantage.

- **Contact Support**
  Display contact information for Micro Focus Support.

- **About Administrative Console**
  View licensing and copyright information about Reflection X Advantage.

File Menu

- **Log On**
  Log on to a domain.

- **Log Off**
  Log off from the domain.

- **Change Password**
  Change your password.
  
  **NOTE:** This option is available only when Reflection X Advantage domain authentication is set to **Internal**.

- **Logon Properties**
  See the name of the user and the domain that is currently logged on.

- **Preferences**
  Customize your view of the Task Status pane in the Administrative Console.

- **Definition Trashcan**
  Open the Definition Trashcan, from which you can restore or permanently discard the deleted items that are stored there.

- **Exit**
  Exit the Administrative Console.

Add User to Domain Dialog Box

Getting there

1. From the Administrative Console, click the **Authentication** side tab.
2. From the **Action** menu, choose **New User**.

Group Box Title

- **User name**
  Type in the name of the user you want to add to the domain.

- **New password**
  (Available only when using Internal authentication) Type the password for this user.

- **Retype password**
  (Available only when using Internal authentication) Retype the password for this user.
Logon Properties Dialog Box

Getting there

From the Administrative Console and X Manager for Domains

- From the File menu, select Logon Properties.

The Logon Properties dialog box provides the name of the “domain” on page 255 to which you're connected and who you're logged onto the domain as.

The options are:

Connected to The name of the domain to which you are connected.
User name The user who logged onto the domain.
FIPS mode Shows the configuration of the domain for FIPS mode, configured in the Domain Composition (page 180) tab of the Administrative console.
Authentication system Shows the authentication system in use for this domain, configured in the Authentication (page 188) tab of the Administrative console.

Related Topics

- “Domain Administration” on page 149

Preferences Dialog Box (Administrative Console)

Getting There

- From the File menu, select Preferences.

Preferences Options

Empty trash at log off/exit Permanently deletes all items in the trash can when you log off of the domain (domain mode), or exit the application (standalone mode).
Automatically hide successful tasks When enabled, messages about successfully completed tasks are automatically removed from the Task Status pane, located at the bottom of X Manager and the Administrative Console.

Use Hide delay (secs) to specify the number of seconds that pass before a task message is removed.

NOTE: Tasks with errors are not removed.

Preferred language Specify the preferred language for the user interface. This setting takes effect when you restart the program.

When displaying Help By default help content is provided from the web. If you want help calls to go to locally installed files instead, download and run the optional local help installer (page 19), and change this setting to Use installed help system.

If either local or web help is not available, Reflection X Advantage will automatically attempt to use the other option.
Action Menu

From Domain Composition tab

Delete Domain Node  Delete the selected domain node from the list under Registered Nodes.

NOTE: Using this command removes the node from the list in the Administrative Console, but this change does not affect the configuration on the domain node itself. See “Remove a Domain Node” on page 156 for information about how to use rxsconfig to stop the listening process on the domain node.

From Domain Status tab

Backward, Forward  Move between previously viewed selections on the Domain Status tab.

Stop Session  Stop the selected session.

From Domain Definitions tab

New  Creates a new definition. This is equivalent to using clicking the plus sign next to a definition type.

Clone  Copies the selected definition. If you copy a read-only (public) definition, you will be able to edit the copy.

Delete  Removes the selected definition. This is equivalent to clicking the minus sign with a definition selected.

Move Up  Moves the selected item in the definitions list.

Move Down  NOTE: You can also move items using drag-and-drop.

Import Color Scheme  Opens the Import Color Scheme dialog box, from which you can import an existing RGB color text file to create a new color scheme.

Import Host Key  Opens the Import Host Key dialog box, from which you can import the public key of a host's public/private key pair and add it to the Trusted Host Keys list.

Make Public  Makes the selected domain definition available to all domain users. A public definition is read-write for the owner (the creator of the definition) and read-only for all other users.

From Authentication tab

New User  Creates a new user in the domain.

Delete User  Deletes the selected user from the domain.

Change User's Password  Changes the Reflection X Advantage domain password for the selected user.

NOTE: This option is available only when Reflection X Advantage domain authentication is set to Internal.
## Import Color Scheme

### Getting there

**From the Administrative Console**

1. Select the **Domain Definitions** tab.
2. Click **Action > Import Color Scheme**.

**From X Manager**

1. Click **Tools > Color Schemes**.
2. From the **Color Schemes** dialog box, click **Import**.

You can import RGB text files that define color schemes.

The options are:

<table>
<thead>
<tr>
<th>Scheme name</th>
<th>The name for the scheme you are importing. (This name is added to the <strong>Color Scheme</strong> list.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RGB File</td>
<td>An RGB text file. The format for an RGB text file consists of a series of rows that define red, green, and blue (RGB) values for color names. Each row has three decimal values that define red, green, and blue values, followed by a string that defines the color name; for example:</td>
</tr>
<tr>
<td></td>
<td>255 250 250  snow</td>
</tr>
<tr>
<td></td>
<td>248 248 255  ghost white</td>
</tr>
<tr>
<td></td>
<td>248 248 255  GhostWhite</td>
</tr>
<tr>
<td></td>
<td>245 245 245  white smoke</td>
</tr>
<tr>
<td></td>
<td>245 245 245  WhiteSmoke</td>
</tr>
<tr>
<td></td>
<td>220 220 220  gainsboro</td>
</tr>
<tr>
<td></td>
<td>255 250 240  floral white</td>
</tr>
<tr>
<td></td>
<td>255 250 240  FloralWhite</td>
</tr>
<tr>
<td></td>
<td>253 245 230  old lace</td>
</tr>
</tbody>
</table>
Customizing and Deploying Reflection X Advantage

Reflection X Advantage supports a number of options for customizing and distributing Reflection X Advantage software, and centrally managing Reflection X Advantage sessions. Review the two overview sections at the start of this chapter to determine which options best fit the needs of your organization.

In this Chapter

- “Deploying Software - Overview” on page 195
- “Deploying Settings - Overview” on page 196
- “Using a Response File to Install on UNIX Systems” on page 198
- “Deploying Sessions Using a Custom Template” on page 200
- “Managing Installations on Windows Workstations” on page 201
- “Deploying Sessions with the Administrative WebStation” on page 212

Deploying Software - Overview

In addition to the basic installation options described under “Installation and Migration” on page 11, administrators can use the following approaches to deploy software to end users. For additional information about deploying customized settings to end users, see “Deploying Settings - Overview” on page 196.

Windows installations

For deployments to Windows systems, you will use the Windows Installer (page 201). You can use the Installation Customization Tool (page 205) to customize your installation.

Features

- Specify which features to install.
- Change the default installation location.
- Customize Windows Start menu shortcuts.
- Chain installations and/or run additional programs automatically with your customized installation.
- Install using silent command line options.

Requirements and limitations

- Deploys to Windows systems only.
- Software is not updated automatically after the install; an additional install must be made available to users.
UNIX installations

For deployments to UNIX systems, you can create a response file to manage customized unattended installations. See “Using a Response File to Install on UNIX Systems” on page 198.

Features

• Specify which features to install.
• Change the default installation location.
• Install using silent command line options.

Requirements and limitations

• Deploys to UNIX systems only.
• Software is not updated automatically after the install; an additional install must be made available to users.

Deploying Settings - Overview

Options for deploying customized settings to end users include:

• Install settings in a companion package (page 196)
• Share settings in a Reflection X Advantage domain (page 197)
• Install custom templates (page 197)
• Import settings using the command line (page 197)
• Distribute settings using Management and Security Server (page 198)

Install settings in a companion package

Deploy using the Windows Installer (page 201). Use the Installation Customization Tool (page 205) to deploy your custom settings.

Features

• Create a companion installer (page 210) to add templates or definition files to your installation.
• Create different companion packages for different users or groups in your organization.
• Configure the companion installer to run automatically with your product installation.
• Install shortcuts to launch Reflection X Advantage using custom command lines.
• Supported in standalone and domain mode.
• Create additional companion installers to add new settings and deploy these separately from the product installation.

Requirements and limitations

• Deploys to Windows systems only.
• Although you can deploy additional companion packages, you cannot modify settings you have already deployed.
Share settings in a Reflection X Advantage domain

Set up a Reflection X Advantage domain to support centralized session configuration. See “Domain Setup: Centralize Session Configuration” on page 168.

Features

- The domain administrator can provide preconfigured, public definitions for users.
- Updates to centralized definitions are automatically available to users.
- Users can configure and save personal definitions in addition to using public sessions.
- Supported on both Windows and UNIX systems.
- By setting up a domain, you can take advantage of other domain services; such as session suspend/resume, and improved performance in high-latency or low bandwidth networks.

Requirements and limitations

- The domain controller and any required nodes must be installed and configured.
- Supported in domain mode only. X Manager for Domains must be installed on user workstations.

Install custom templates

Use templates to install default definitions on user workstations. See “Deploying Sessions Using a Custom Template” on page 200.

Features

- Create custom definitions and export them to definition files (.rxd). Definition files installed to the templates subfolder in the program installation directory are automatically available to users on initial startup.
- Configure templates to import automatically or provide users with a choice of templates to install the first time they run the application.
- Supported in standalone and domain mode.
- Supported on both Windows and UNIX systems.
- On Windows systems, you can use the Installation Customization Tool to create a companion package to install your templates (page 211).

Requirements and limitations

- Template settings are imported only on first run. They cannot be used to update existing settings, and are not available for upgrading users.

Import settings using the command line

Start Reflection X Advantage using rxmgr (page 227) or rxmgrdomains (page 229), and use the -import option to specify a definition file to be imported.

Features

- A definition file with custom settings can be made available from a shared network drive or a web server.
- Supported in standalone mode (using rxmgr) and domain mode (using rxmgrdomains).
- Supported on both Windows and UNIX systems.
- Changes to the definition file are imported each time the command line is executed.
Requirements and limitations

- The administrator must configure and deploy a shortcut or command-line script for end users.
- Restarting using the import option overrides end-user modifications to imported settings. (The -execOnly option can be used in combination with -import to prevent user edits.)

Distribute settings using Management and Security Server

Configure and launch client connections using the Management and Security Server Administrative WebStation. See “Deploying Sessions with the Administrative WebStation” on page 212.

Features

- Manage sessions for multiple Reflection products from a single console.
- Configure sessions that launch X clients directly, without displaying the X Manager window.
- Provide updated settings to users as needed.
- Connections go through the Management and Security Server Security Proxy server, which provides SSL/TLS encryption to the proxy. The Security Proxy server can also restrict the visibility of your hosts over the network, which enables you to limit host access to authorized users and members of LDAP groups.

Requirements and limitations

- You must have Management and Security Server, which is sold and licensed separately from Reflection X Desktop.
- A Management and Security Server proxy server must be configured, clients must connect using Secure Shell, and Reflection PKI Services Manager must be installed and configured to validate the Security Proxy certificate.
- Administrator and user workstations must be Windows systems, and X Manager (standalone) must be installed on these computers.
- Users who launch sessions from Management and Security Server can't save X Manager settings.

Using a Response File to Install on UNIX Systems

You can use an InstallAnywhere response file to configure automated, silent installs on UNIX workstations.

Before you begin

- Download and unzip the installation file for your UNIX or Linux system as described in “Install on UNIX” on page 13.
- Change permissions on the installation file so that it is executable by root.

To deploy using a response file

1. Use a text editor to create and save a response file. See samples and options below.
2. Log on as root.
3. Launch the installer using a command that specifies your response file (called rxaresponse in this example):

   /path/rxa-n.n.n.nnn-prod-package-type.bin -f /path/rxaresponse
Response file format

Use INSTALLER_UI to specify a silent install. Use CHOSEN_INSTALL_FEATURE_LIST to list the features to be installed. CHOSEN_FEATURE_LIST is the list of features enabled. For silent installations these are typically the same. Use USER_INSTALL_DIR to specify the installation directory. All options are required. Leave other options as shown in these examples.

The following sample response file installs all Reflection X Advantage applications and services; and the generic sample template, which automatically imports the default sample settings.

```
INSTALLER_UI=silent
CHOSEN_INSTALL_SET=Custom
CHOSEN_FEATURE_LIST=RX,XMan,XManDom,AdminCon,Service,ServDC,ServRmt,TemplGrp,TemplGen
CHOSEN_INSTALL_FEATURE_LIST=RX,XMan,XManDom,AdminCon,Service,ServDC,ServRmt,TemplGrp,TemplGen
USER_INSTALL_DIR=/opt/rxadvantage
JDK_HOME=
JDK_DOT_HOME=$USER_INSTALL_DIR$$/$$jre
JAVA_EXECUTABLE=$USER_INSTALL_DIR$$/$$jre/bin/java
```

The following response file installs just the Reflection X Advantage service to create a domain node.

```
INSTALLER_UI=silent
CHOSEN_INSTALL_SET=Custom
CHOSEN_FEATURE_LIST=RX,Service
CHOSEN_INSTALL_FEATURE_LIST=RX,Service
USER_INSTALL_DIR=/opt/rxadvantage
JDK_HOME=
JDK_DOT_HOME=$USER_INSTALL_DIR$$/$$jre
JAVA_EXECUTABLE=$USER_INSTALL_DIR$$/$$jre/bin/java
```

Features are organized in a feature tree. To install a feature, include any features above it in the hierarchy. This example installs the Domain Controller:

```
CHOSEN_INSTALL_FEATURE_LIST=RX,Service,ServDC
```
Deploying Sessions Using a Custom Template

Templates are definition files that are installed to the Reflection X Advantage templates folder. Templates are imported for each user the first time the user runs X Manager or X Manager for Domains. Depending on how you create them, definition files may be imported silently or included in the Import Templates and Migrated Settings dialog box that displays on initial startup.

**NOTE:** If you run Reflection X Advantage in domain mode, you can create and share public settings definitions (page 168) instead of (or in addition to) creating and deploying custom templates. Unlike deployed templates, public definitions can be created and modified after X Manager for Domains has already been installed on user workstations.

To create a custom template

1. From X Manager or X Manager for Domains, click **File > Export**.
2. Select the definitions you want to include in the template.
3 Use the Template configuration options to configure how users will import this template.
   - If you want to enable users to select the template from a list, enter a Template name. This name shows up in the list of available templates in the Import Templates and Migrated Settings dialog box that displays on initial startup. (This name is not displayed if Automatically import template on first run is selected.)
   - To configure the template to be imported silently, select Automatically import template on first run.

4 Click Export. Enter a filename and click Save to complete the export process.

5 Put this template in the Reflection X Advantage templates folder. For deployments to Windows systems, you can use Installation Customization Tool to create a companion installer package for your templates and run this package automatically after the product installation. This ensures that templates are available to users on initial startup. See “Install Custom Templates with a Companion Installer Package” on page 211.

Managing Installations on Windows Workstations

If you are installing to Windows workstations, you install Reflection X Advantage using the Setup program (Setup.exe).

You can choose from several different approaches for installing and deploying Reflection X Advantage. Deciding which approach to use is typically based on a variety of factors, including your approved business processes, the scale of the deployment, your deployment tools, and whether you want to customize the installation.

For example, a small-scale deployment might consist of using the Setup program to install Reflection X Advantage on a few workstations, whereas an enterprise-wide deployment would probably involve extensive customization and testing.

Use one of the following approaches, depending on your requirements.

- **Perform a workstation installation on each workstation**
  Install all of the files for Reflection X Advantage to a PC hard drive. You might choose this approach if you are installing Reflection X Advantage on a small number of machines and you do not need to customize the installation.

- **Perform a basic deployment**
  Perform an administrative installation to copy Reflection X Advantage files to an administrative installation point. This is also referred to as creating an administrative installation image. Then, using deployment tools, you can access these files and create packages that are deployed to workstations. A basic deployment is a good choice when you need to deploy Reflection X Advantage to a large number of workstations, but do not need to customize the installation.

- **Perform a customized deployment**
  Perform an administrative installation to copy Reflection X Advantage files to an administrative installation point (just as you would for a basic deployment). Then, customize the installation to specify the way it installs, looks, and acts on the end users' computers. Customized deployments can be deployed to any number of workstations.

In this Section

- “Performing a Basic Deployment” on page 202
- “Performing an Advanced Deployment” on page 202
- “Install from the Command Line” on page 203
Performing a Basic Deployment

Perform a basic deployment when you need to install the default (uncustomized) Reflection X Advantage application on a large number of machines.

The following process is typical for a large-scale, basic deployment:

1. Perform an administrative installation (page 204) in a destination folder to create an administrative installation point.
2. Test the installation.
3. Deploy Reflection X Advantage from the administrative installation point. Because the installation package adheres to MSI standards, you can use Microsoft Active Directory or any other Microsoft Installer-compatible deployment tool.

Performing an Advanced Deployment

The following process is typical for large-scale, customized deployments.

1 Perform an administrative installation (page 204) in a destination folder to create an administrative installation point.
2 From the administrative installation point, start the Installation Customization Tool (page 205). The tool supports two editing modes:
   - Create a companion file (.msi) (page 210). Use this option to install custom files (including templates and other Reflection X Advantage definition files) on user workstations. You can also configure and add custom shortcuts.
   - Create a transform file (.mst) (page 206). Use this option to customize the feature set to be installed on user workstations, to customize Start Menu shortcuts, and to specify additional installation packages to run automatically with installations performed using setup.exe.

   **NOTE:** Details for working with the Installation Customization Tool are available from the tool's Help menu and from context-sensitive help topics for each panel.

3 Test the installation.
4 Deploy Reflection X Advantage using the transforms and companion packages you created. Because the transforms and companion installation packages adhere to Microsoft Windows Installer (MSI) standards, you can use a desktop shortcut, Microsoft Active Directory, or any other Microsoft Installer-compatible deployment tool.
Install from the Command Line

You can use the Setup program command line to install Reflection X Advantage from the distribution image, or from an administrative installation image. You can also include command-line options in a batch file to preset installation parameters, and limit user interaction while Reflection X Advantage is installing. You can even suppress installation dialog boxes to provide an unattended installation.

In addition, you can use command-line options to prepare Reflection X Advantage for installation by users. In general, any of the MSI command-line options can be used from the Setup program command line.

To install from the command line

- At the command prompt or the Start menu Run command, change to the directory in which the setup.exe file resides, and do one of the following:
  - To create an administrative installation image, type:
    setup.exe /install /admin TARGETDIR=path
    where path is the path to the administrative installation image on the server.
  - or-
  - To install to a workstation with typical settings, type:
    setup.exe /install INSTALLDIR=path
    where path is the path to the installation directory (INSTALLDIR=path is optional).

**NOTE:** To view a list of the command-line options for customizing installations, change to the directory in which the setup.exe file resides and enter:

setup.exe /?

To install directly with MSI

At the command prompt or Start menu Run command, change to the directory in which the msi file resides and enter:

msiexec.exe /i installation_file_name.msi

Handling prerequisites in command line installs

If you use setup.exe for your install, the setup program checks for any prerequisites required by the features you have selected and installs them automatically.

If you use msiexec.exe for your install, prerequisites are *not* installed automatically. You need to install them separately if they are not already on your users’ workstations. You can find installers for Reflection X Advantage prerequisites in the Prerequisites folder in the distribution media, or in your administrative installation. The prerequisites you need to install depend on which programs and features you are installing:

- All Reflection Workspace features require Microsoft .NET Framework 4.5.1. If you attempt an install using msiexec.exe and this prerequisite is not found, a message displays and the installer stops. To install the .NET framework, run the executable file in Prerequisites\DotNet451.
The **Visual Basic for Applications** feature requires Microsoft VBA 7.1. Use the core and language-specific *.msi packages in the Prerequisites\VB71 folder.

All **Reflection X Advantage** features require a Java Runtime Environment (JRE). Use MicroFocusJava.msi in the Prerequisites\JDK folder to install the JRE. If you install using msiexec.exe without installing this prerequisite, the install will run, but Reflection X Advantage applications will fail to run unless you have configured an alternate JRE.

**Handling upgrades in command line installs**

If you are upgrading a previous version of Reflection, the prior version must be uninstalled before you can install the current version.

If you use setup.exe for your install, the setup program checks for a previous versions of Reflection and uninstalls it automatically if one is found.

If you use msiexec.exe for your install, you must first manually uninstall any earlier versions. If you upgrade these products by deploying the .msi file directly and have not removed the earlier version, a message displays telling you to uninstall the older software first.

**Create an Administrative Installation Point**

To prepare your environment for deployment, create an administrative installation point. This is an installation option which installs all of the files required to install Reflection X Advantage as well as the administrative tools used for customization. This installation is different from simply copying the package files to a network location in the following ways:

- Any files that are compressed in the original package are uncompressed in the administrative installation point.
- When a service pack is released, you can update your administrative installation directly by applying the patch to it.

**NOTE:** We recommend that you create an administrative installation point on your administrative workstation before installing Reflection X Advantage. After you've created an administrative installation point, you can install Reflection X Advantage by running setup.exe from the administrative installation point. If you install Reflection X Advantage before you create the administrative installation, you'll need to create the administrative installation image using the command-line option described below.

**To create an administrative installation point**

1. Create a network share on a network file server.
2. Click the download link, and run the download program.
3. Select a location for the installer files, and then click **Next**.
   
   This extracts the files to the specified location and starts the Installation Customization Tool. (If you have already downloaded the files, click the setup.exe file to start the installation program.)
4. Click **Continue** and accept the license.
5. From the **Advanced** tab, click **Create an Administrative install image on a server**.
   
   Only selections on the **Advanced** and **File Location** tabs apply to this procedure. Selections made on other tabs are ignored. Administrative installations always include all files used by the package.
6. Click **Continue**.
7 Browse to the network share you want to use for the administrative installation image. For installations on a network share, specify the path to the network share as a UNC path (for example: \share_name\administrative_install_point).

Administrative installation images are typically created in a file server folder. However, you can create administrative installation images in any folder on a local hard disk. This can be useful for testing purposes.

8 Click Install Now.

To create an administrative installation from the command line

1 Open a command window, running as an administrator.
2 Use the following command syntax to start the installation:

<path_to_setup>\setup.exe /install /admin
TARGETDIR=<UNC_path_to_administrative_installation_point>

Installation Customization Tool

The Installation Customization Tool is a special mode of Setup program (setup.exe) that supports custom modifications to the primary install and includes some limited deployment facilities. These are accomplished with a simple user interface, and do not require additional software packages or training.

Use the Installation Customization Tool to create transforms or companion installer packages. Each type of customization has its own unique set of configuration panes, depending on your choice from the Select Customization pane.

Open the Installation Customization Tool

To open Installation Customization Tool

1 Create an administrative installation point (page 204).
2 On a command line, navigate to the administrative installation point and enter:

setup.exe /admin

-or-

If you have set up a shortcut to the Installation Customization Tool (page 206), double-click the shortcut.
3 The Select Customization dialog box prompts you to choose which mode you want to open.

<table>
<thead>
<tr>
<th>To do this</th>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new transform file (.mst) (page 206)</td>
<td>Create a new Setup customization file for the following product (the default).</td>
</tr>
<tr>
<td>Create a new companion install package (.msi) (page 210)</td>
<td>Create a new Companion installer.</td>
</tr>
<tr>
<td>Open an existing file of either type</td>
<td>Open an existing Setup customization file or Companion installer.</td>
</tr>
</tbody>
</table>
Set up a shortcut to the Installation Customization Tool

By default, the Installation Customization Tool can be opened only from a command line. However, you can create a file shortcut and set the shortcut properties to open this tool. Although creating this shortcut is optional, you will find that it saves time when you are working with ACT.

To set up a shortcut that opens the Installation Customization Tool

1. On your administrative installation point, right-click the setup.exe file then select Create Shortcut.
2. Right-click the shortcut and choose Properties.
3. In the Target field, add the /admin option to the end of the command line. For example:
   ```
   \\myServer\adminInstallPoint\setup.exe /admin
   ```
   
   **NOTE:** Make sure that the path in the Target field follows the Uniform Naming Convention (UNC) format. Do not use drive letters in the path name — this can cause problems when you try to use the shortcut on other workstations.
4. Rename the shortcut and save it to the desktops of your workstation and the server you are using for your administrative installation point.

Creating and Editing Transforms

You can use Installation Customization Tool to create Windows Installer transform files (.mst) that customize your Reflection X Advantage installation.

To create and use a transform file

1. Start Installation Customization Tool and select Create a new Setup customization file for the following product.
2. Make the modifications you want for your customized install. Typical changes include:
   - Set the user interface level.
   - Specify which product features to install (page 206).
   - Configure file shortcuts (page 207).
   - Add companion installers (or other programs) to run with this installation. (page 208)
3. Apply the transform to your installation (page 209).

Select Features, Components, and Languages

You can select which features, components, and languages to install for your end users. In addition, you can make features available to users for a later installation or hide them from view.

To select features, components, and languages to install

1. From your administrative installation point, open the Installation Customization Tool from a shortcut (page 206) or by typing the following command line:
   ```
   <path_to_setup>\setup.exe /admin
   ```
2 From the Select Customization dialog box, do one of the following:
   - Select Create a new Setup customization file for the following product.
   - Select Open an existing Setup customization file or Companion installer and select an .mst file.

3 From the Installation Customization Tool navigation pane, select Set feature installation states, and for each feature, choose from the following states:

   **Choose**                              **To do this**

   - Feature will be installed on local hard drive
     Add a feature to the installation.
     **NOTE:** Some features listed under a selected feature may not be included when you select to install the higher-level feature. The features that are included are the recommended defaults. If you select the higher level feature a second time, all sub-features will be included.

   - Feature will be installed when required
     Advertise a feature.

   - Feature will be unavailable
     Leave a feature uninstalled. End users will still be able to select and install the item from the Windows Program and Features or the Add or Remove Programs control panel.

   - Feature will be hidden from view
     Leave a feature uninstalled and hidden. The feature will not appear in the Windows Program and Features or the Add or Remove Programs control panel.

### Configure Shortcuts

You can change the attributes associated with the pre-defined Reflection X Advantage shortcuts. Also, you can configure shortcuts for files you've added to a custom install package.

**To configure shortcuts**

1. From your administrative installation point, open the Installation Customization Tool from a shortcut (page 206) or by typing the following command line:
   ```
   <path_to_setup>\setup.exe /admin
   ```

2. From the Select Customization dialog box, select any of the startup options. You can modify shortcuts in both transforms (.mst) and companion installers (.msi).

3. From the Installation Customization Tool navigation pane, choose Configure shortcuts.

4. Select the shortcut you want to configure, and then click Modify.
5 In the **Modify Shortcut** dialog box, enter the following settings:

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify where you want the shortcut to reside</td>
<td>In the <strong>Location</strong> list, enter or select the folder. <strong>NOTE:</strong> To specify a folder location, you can select any of the predefined options in the drop-down list. The list of available locations depends on whether your installation is user-specific (the default) or for all users. For example [PersonalFolder] for user-specific installations, or [ProgramFilesFolder] for all user installations. You can edit these paths to include additional path information. For example: [PersonalFolder]\Micro Focus\Reflection. You can also manually enter full path information. For example C:\demo\path. The location you specify must exist on all target computers.</td>
</tr>
<tr>
<td>Name the shortcut</td>
<td>In the <strong>Name</strong> box, enter a descriptive name.</td>
</tr>
<tr>
<td>Add a tooltip to the shortcut</td>
<td>In the <strong>Tooltip</strong> box, enter descriptive text to describe the shortcut.</td>
</tr>
<tr>
<td>Pass command line arguments to the program</td>
<td>In the <strong>Arguments</strong> box, enter the command-line arguments.</td>
</tr>
<tr>
<td>Specify the size of the application window</td>
<td>In the <strong>Run</strong> list, select an initial size for the application window.</td>
</tr>
</tbody>
</table>

### Add (Chain) Installations and Run Programs

Reflection X Advantage makes it easy to "chain" installs. You can set up an install to run companion install packages automatically before or after the primary installation. You can also specify to run other scripts or programs.

**NOTE:** This method of chaining installations applies only to installs performed with `setup.exe`. It does not apply to installs that use the MSI command line method.

---

**To chain installations and programs**

1. From your administrative installation point, open the Installation Customization Tool from a shortcut (page 206) or by typing the following command line:
   ```
   <path_to_setup>\setup.exe /admin
   ```
2. Select **Create a new setup customization file for the following product**, and then click **OK**.
3. From the navigation pane, select **User Interface** and then select **Use this customization with interactive installs using setup.exe**.
4. From the navigation pane, select **Add installations and run programs**.
5. Click **Add**.
   The **Add/Modify Program Entry** dialog box opens.
6. In the **Target** list, enter or select the folder where the program `.exe` file or the `.msi` file resides, and then enter the executable to run. For example:
   ```
   msiexec.exe
   ```
7. Under **Arguments**, enter the command-line arguments to execute. For example:
   ```
   /i my_installation.msi
   ```
8 To specify when to run the program, select one of the following:
  • Run this program after base product has been installed
  • Run this program before the base product has been installed.

**NOTE:** For most cases, select Run this program after the base product has been installed. If you select Run this program before the base product has been installed and the program fails, Reflection X Advantage is not installed.

1 Repeat these steps to add other programs or .msi files.
2 To change the execution sequence, use the arrows next to Move in the lower-left area of the pane. To remove a program from the list, select it in the list and click Remove.

### Apply a Transform to Your Installation

If you have created a transform to customize how Reflection X Advantage is installed, you need to deploy the transform with the primary installation. (This is in contrast to companion installation packages, which can be chained with the primary installation or installed separately.) Any install started with setup.exe or with command-line installs can include a transform.

**To add the transform to installs started with setup.exe**

1 Start Installation Customization Tool and select Create a new Setup customization file for the following product.
2 Go to the User interface panel.
3 Select Use this customization with interactive installs using setup.exe.
   When you save your transform with this option selected, the Installation Customization Tool automatically updates the setup.ini file to apply the transform to the Reflection X Advantage installation by adding the following line to the [Setup] section:

   CustomTransform=<your_transform.mst>

   This modification to setup.ini means that any install using setup.exe (using either the interactive user interface or using setup.exe on a command line) will automatically apply this transform.
4 Save the transform to the default location (the folder that includes setup.exe).
   The transform can now be deployed to end users via the setup.exe file. (Users can run setup.exe directly or setup.exe can be called from a script or initiated from a command line.)

**NOTE:** If the setup.ini file already specifies the transform file you want to install (as noted in step 3 of the previous procedure) do not specify the transform on the command line.

**To add the transform to a setup.exe command-line install**

• From the command line, use the following syntax:

   `<path_to_setup>\setup.exe /install TRANSFORMS=<transform.mst>`
Creating and Editing Companion Installer Packages

Create a companion installer package to install any files that are not automatically installed with Reflection X Advantage, including customized application settings. Companion installer packages are deployed independently of the installation. Therefore, you can upgrade the product without removing these support files. If you support several business units that require their own customized configuration files, you can create a companion installer package for each business unit.

Install the Companion Installer Package by adding it to your Reflection X Advantage install, or using any mechanism that supports Windows installer packages (.msi). Companion installer packages have no built-in user interface except a standard progress bar.

Basic steps for creating a companion package file

1. Configure and test the settings files you want to deploy to users.
2. Start Installation Customization Tool and select Create a new Companion installer.
3. Use the Specify package information panel to configure the program name you want to appear in the Windows Programs and Features control panel.
4. Use the Specify install locations panel to set the package either to install for all users (the default) or only the user who installs it. This setting can't be changed after you start adding files on the Add files pane.
5. Use the Add files pane to specify which files to include in the companion installer package, where to install them, and whether to include a shortcut for any of the added files.
6. If the application supports it, use the Modify user settings pane to customize user settings. The application must be installed on the administrative workstation.
   Your modified user settings appear in the Location column and are automatically included in the companion installer package.
7. Add the companion installer package to your installation (page 212).

Editing an existing companion package file

1. Start Installation Customization Tool and select Open an existing Setup customization file or Companion installer.
2. Make your edits, then go to File > Save.
3. This opens the Increase Package Version dialog box.
   - Click Yes to increase the version number. This is required if you want to support upgrades of the package on computers that have installed an earlier version. (If you use Reflection Security Gateway (http://www.attachmate.com/Products/Terminal+Emulation/security/rsg/reflection-security-gateway.htm) to deploy companion packages, you can configure it to deploy a newer version automatically to end users.)
   - Click No to keep the same version number. Use this option if you are editing a companion package that is not yet installed on user computers; or if you do not need to upgrade existing computers.
4. Save the file using the same name or a different name. (The Windows Installer uses an internal GUID, not the filename to identify the package.)
Install Custom Templates with a Companion Installer Package

Templates are definition files that are installed to the Reflection X Advantage templates folder. Templates are imported for each user the first time the user runs X Manager or X Manager for Domains. Depending on how you create them, definition files may be imported silently or included in the Import Templates and Migrated Settings dialog box that displays on initial startup.

NOTE: If you run Reflection X Advantage in domain mode, you can create and share public settings definitions (page 168) instead of (or in addition to) creating and deploying custom templates. Unlike deployed templates, public definitions can be created and modified after X Manager for Domains has already been installed on user workstations.

To create a custom template

1. From X Manager or X Manager for Domains, click File > Export.
2. Select the definitions you want to include in the template.
3. Use the Template configuration options to configure how users will import this template.
   - If you want to enable users to select the template from a list, enter a Template name. This name shows up in the list of available templates in the Import Templates and Migrated Settings dialog box that displays on initial startup. (This name is not displayed if Automatically import template on first run is selected.)
   - To configure the template to be imported silently, select Automatically import template on first run.
4. Click Export. Enter a filename and click Save to complete the export process.

You can use the Installation Customization Tool to create a companion file to install this template on Windows systems.

To create a companion package to install one or more custom templates

1. Create an administrative installation image (page 204).
2. From your administrative installation point, open the Installation Customization Tool from a shortcut (page 206) or by typing the following command line:
   
   `<path_to_setup>\setup.exe /admin`

3. From the Select Customization dialog box, select Create a new Companion installer and then click OK.
4. From the navigation pane, click Specify package information. Use this panel to specify the information your package will use in the Windows Programs and Features (or Add or Remove Programs) list.
5. From the navigation pane, click Specify install locations. On this panel, select Installs to all users of a machine. (The installation locations available change based on this setting and you need to install this template to the program files folder.)
6. From the navigation pane, click Add Files.
7. Under Add files to at the bottom of the panel, specify the templates subfolder in your program installation location; for example [ProgramFilesFolder]\Reflection\templates. (You can manually edit the pre-configured item [ProgramFilesFolder]\My Files.)
8. Click Add. Browse to locate your template file and click Open.
9 Choose File > Save As and enter a name for your installation package (for example RXATemplates.msi).
10 (Optional) Chain this installer (page 212) to have it run automatically after installations done using setup.exe.

Add a Companion Installer to your Installation

After you've created a companion package (.msi) with ACT, use this procedure to add it to your product installation. When end users run Setup.exe, any added packages are automatically installed after the primary installation is complete.

To add a companion installer package to your installation

1 From your administrative installation point, open the Installation Customization Tool from a shortcut (page 206) or by typing the following command line:
   `<path_to_setup>\setup.exe /admin`
2 Select Create a new setup customization file for the following product, and then click OK.
3 From the navigation pane, select User Interface and then select Use this customization with interactive installs using setup.exe.
4 From the navigation pane, click Add installation and run programs.
5 Click Add.
   The Add/Modify Program Entry dialog box opens.
6 In the Target list, browse to select the companion installer file (.msi).
7 Select Run this program after the base product has been installed.
8 Click OK.
9 Click File > Save As to save your transform.
   The Installation Customization Tool automatically updates the Setup.ini file, adding a [RunPrograms] section with instructions for installing your companion installer package.

Deploying Sessions with the Administrative WebStation

Management and Security Server (formerly Reflection Security Gateway) is a Micro Focus product that supports centralized management of Reflection sessions. If you have installed Management and Security Server, you can use the Reflection Administrative WebStation to administer Reflection X Advantage sessions. This allows users to connect through the Management and Security Server Security Proxy server, which provides SSL/TLS encryption to the proxy. Using Management and Security Server also enables you to restrict the visibility of your hosts over the network and to limit host access to authorized users and members of LDAP groups.

In this Section

- “Configure Sessions using the Administrative WebStation” on page 213
- “Setting up a Session using the Security Proxy” on page 213
- “Managing Upgrades for WebStation Sessions” on page 215
- “Administrative WebStation Mode” on page 215
- “WebStation User Mode” on page 215
Configure Sessions using the Administrative WebStation

Before you begin
- Install X Manager (standalone) on administrator and user computers. These must be Windows systems.
- Install Management and Security Server on a server. (This installs two servers, the Reflection Management Server and the Reflection Security Proxy.) Make sure you have administrative credentials to log onto the Reflection Management Server.

To deploy a session with the Administrative WebStation

1. In a Web browser, launch Management and Security Server and log on as an administrator. Click **Administrative WebStation**.
2. In the Administrative WebStation navigation pane, under **Activities** select **Session Manager**.
3. In the Session Manager, click **Add** to open the **Add New Session** page.
4. In the **Add New Session** page, select **X Advantage**, enter a session name, and click **Continue**.
5. By default **Start X Manager in notification area of taskbar** is enabled. With this option X clients are launched on user desktops and X Manager runs in the background on the user's machine. Users see only the clients that are configured to open at startup.
6. (Optional) In **X Manager Preferences**, make your selection for **FIPS mode**. Select this checkbox to enable FIPS, which enforces the United States government Federal Information Processing Standard (FIPS) 140-2 for this session.
7. (Optional) Add any comments that you want to have available for review in the Administrative WebStation.
8. Click **Launch**. This launches X Manager in "Administrative WebStation Mode" on page 215.
9. Configure one or more X clients that you wish to make available to your end users.
10. Test your connection. In response to the **Host Key Unknown** prompt, click **Always**. This adds the key to the known hosts list in the configuration you save to the web server so users won’t see the prompt.

**NOTE:** The option to save a host key by selecting **Always** is not available for sessions running in WebStation User Mode.

11. Go to **File > Exit**. Click **Save/Exit** to close your session and save the configuration to the Management and Security Server Administrative WebStation.
12. From the Management and Security Server Administrative WebStation, map access for your users.

Setting up a Session using the Security Proxy

The Management and Security Server Security Proxy server provides SSL/TLS encryption to the proxy.

Before you begin
- Install X Manager (standalone) on administrator and user computers. These must be Windows systems.
• Install Management and Security Server on a Windows or UNIX server. (This installs two
servers, the Reflection Management Server and the Reflection Security Proxy.) Make sure you
have administrative credentials to log onto the Reflection Management Server.

• Install PKI Services Manager on a Windows or UNIX server. See “Using PKI Services Manager
with Reflection X Advantage” on page 235 for information about installing and configuring this
tool.

**Configure PKI Services Manager to validate the Management and Security Server Security
Proxy certificate**

The method you use depends on how the Security Proxy is configured:

• If you’ve obtained a certificate for the Security Proxy from a Certification Authority (CA), add the
CA certificate to the PKI Services Manager trusted root store.

• If you’re using the proxy's default self-signed certificate, add this certificate to the PKI Services
Manager trusted root store. To obtain a copy of the default certificate, from the server running
Management and Security Server start the Security Proxy Wizard, and go to **Security Proxy
Certificates > Export**.

Note: PKI Services Manager supports the ability to map which entities can authenticate using
certificates. This is not used when validating the Security Proxy certificate, so you do not need to
configure identity mapping.

**To deploy a session with the Administrative WebStation**

1. Log into the **Administrative WebStation** and select **Session Manager**.
2. In the Session Manager, click **Add** to open the **Add New Session** page. Select **X Advantage**, enter a session name, and click **Continue**.
3. (Optional) On the **Configure a Windows-Based Reflection Session** page modify any of the
optional settings.
4. Click **Launch**. This launches X Manager in "Administrative WebStation Mode" on page 215.
5. Configure your X client settings.
6. For each configured client, click **Advanced** to open the **Advanced Secure Shell Settings**
dialog box.
   - On the Proxy tab select **Use Reflection security proxy**.
   - Under **Security proxy server**, select your proxy server and port from the drop-down lists.
   - Click **Close**.
7. Go to **Tools > Secure Shell Host Keys > PKI Configuration**.
   - For **PKI server**, enter the name of the computer running PKI Services Manager.
   - Click **Download key** and click **Yes** to accept the key.
8. Test your connection. In response to the **Host Key Unknown** prompt, click **Always**. This adds
the key to the known hosts lists in the configuration you save to the web server so users won’t
see the prompt.

**NOTE:** The option to save a host key by selecting **Always** is not available for sessions running
in WebStation User Mode.

9. Go to **File > Exit**. Click **Save/Exit** to close your session and save the configuration to the
Management and Security Server Administrative WebStation.
Managing Upgrades for WebStation Sessions

If you configured WebStation sessions for use with an older version of Reflection X Advantage, users can upgrade Reflection X Advantage and continue to use their existing sessions. When users launch sessions in WebStation User mode, session settings are migrated automatically to run on the newer version each time the users connect.

When you launch sessions in Administrative WebStation mode after upgrading Reflection X Advantage on your workstation, session settings are migrated automatically and this migration becomes permanent when you click Save/Exit. Don't make this change until all user workstations have been upgraded. Settings that have been migrated to the new version will no longer work for users who are still running an older version.

Administrative WebStation Mode

When you launch Reflection X Advantage from the Management and Security Server Administrative WebStation, the title bar displays X Manager- Administrative WebStation Mode. This mode provides additional security settings. These are configurable via the Proxy tab, which is only available in this mode. (To view the Proxy tab when running in WebStation mode, set Connection method to Secure Shell, and click Advanced.)

When X Manager is launched in Administrative Webstation mode, there are limitations on what you can do:

- Only one session is available. You can modify the settings for this session, but you cannot add additional sessions.
- One default X client definition is available. You can edit this client and create additional clients. You can also create and edit launch groups.
- XDMCP Connections are not supported.
- SSH is the only connection method available for clients.
- Changes you make to the session, client, and launch group definitions are not saved until you exit X Manager.
- When you close X Manager, you will be prompted to save your settings. Click File > Exit, and then click Save/Exit on the Save Settings dialog box. This saves your settings on the Management and Security Server Management Server. If you have just created the session, you will be prompted in the Administrative WebStation to map the session so that it is available to users.
- You cannot modify FIPS mode. (The setting for FIPS is configured using the Session Manager in the Administrative WebStation.)

WebStation User Mode

If you open X Manager after launching a session from the Links list of a Management and Security Server management server, the title bar displays X Manager- WebStation User Mode.

- When you launch an X Manager session in this mode, you have access to the X clients or launch groups created by the administrator.
Depending on how the session has been configured by the administrator, clients may start automatically or be started as needed. If X Manager runs in the notification area of the taskbar (the default), you must select the Show X Manager taskbar option to start a client manually.

You can add clients using X Manager, but they cannot be saved as part of the session, and will not be available the next time the session is launched from the Links list. You can, however, export the clients for later use.

Save Settings (Administrative WebStation Mode)

When you launch Reflection X Advantage from the Management and Security Server Administrative WebStation, you open X Manager in Administrative WebStation mode. You can add and edit X clients and launch groups, and edit the session definition. Use this dialog box to save these changes to the Management and Security Server Management Server.

Save/Exit

Any changes you have made using X Manager are saved to your Management and Security Server session. After you configure access in the Administrative WebStation, the session is available to users.

Discard

Any changes you have made will be discarded.

Cancel

Return to X Manager.

Discard Settings (WebStation User Mode)

When you launch a Reflection X Advantage session from the Links list of a Management and Security Server management server, the clients created for this session by the administrator are available to you. You can add clients if you open X Manager in user mode, but they will not be available the next time the session is launched from the Links list. You can export the clients if you wish to retain them for import when you open the session again.

Click Discard to exit X Manager. Any changes you have made will not be saved. Click Cancel to return to the session without exiting, then select File > Export if you wish to save your changes by exporting them.
Reflection X Advantage Data Files

Reflection X Advantage stores settings in a database file. Settings are saved automatically while you work. Administrators are not required to perform any direct maintenance for this database. However, it may be appropriate to include this file in your site’s general backup or archiving procedures. Backup procedures should include both the database folder (db) and the configuration folder (conf). The location of these folders depends on your operating system and whether you run the in standalone or domain mode.

X Manager (standalone) database file

The database file for the standalone X Manager is stored in the following user-specific locations.

On Windows systems:

The database is located in the Windows user profile folder. The default location depends on your version of Windows. For example:

C:\Users\<user>\.attachmate\rx\db\<version>
-or-
C:\Documents and Settings\<user>\.attachmate\rx\db\<version>

On UNIX systems:

The database is in the user’s home folder:

$HOME/.attachmate/rx/db

Domain database files

The database files for a Reflection X Advantage domain are located on the computer that is functioning as the “domain controller” on page 255.
On Windows systems:
The domain database is located in the Windows All Users profile folder (page 258). The default location depends on your version of Windows. For example:

C:\ProgramData\attachmate\rx\db\<version>
-or-
C:\Documents and Settings\All Users\attachmate\rx\db\<version>

On UNIX systems:
The domain database is in the following location:

/opt/rxadvantage/rx/db

Reflection X Service configuration files

The following domain mode configuration files are used by the Reflection X Service and stored in the conf directory. On Windows systems, this is located in the Windows All Users profile folder (page 258) (%AllUsersProfile%\attachmate\rx\conf). On UNIX, it is a subdirectory of the product installation directory.

NOTE: These files are not should be edited manually.

domains.xml  Configuration for domain controller. This file is created when you install the Domain Controller feature.

domain-nodes.xml  Configuration for domain nodes. This file is created and maintained using the rxsconfig command line utility.

host-nodes.xml  Configuration for remote session services. This file is created when you install the Remote Session Services feature.

The conf folder also stores private keys and certificates that are used for authenticating distributed session components.

Ports used by Reflection X Advantage

Reflection X Advantage uses the ports summarized below. Depending on your Reflection X Advantage configuration, you may need to configure a firewall to allow a port exception for one or more of these ports.

<table>
<thead>
<tr>
<th>Component</th>
<th>Default port</th>
</tr>
</thead>
<tbody>
<tr>
<td>X Manager</td>
<td>6000 (If you specify a fixed display number, the port used is 6000 + display number)</td>
</tr>
<tr>
<td>Domain Node</td>
<td>22001 (if you have more than one domain node configured, each must have a separate port)</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>22000 (default)</td>
</tr>
<tr>
<td>Remote Session Services</td>
<td>21999 (default)</td>
</tr>
</tbody>
</table>
Note: The domain controller, domain nodes, and remote session services are processes of the Reflection X Service. The ports listed above are defaults for these processes. You can run the `rxsconfig` (page 233) command line utility to determine which ports are actually configured on your system. The following command lists all configured Reflection X Service processes sorted by port number:

```
rxsconfig list
```

# Feature Guide for Upgrading from Reflection X version 13 or 14

If you are upgrading from legacy Reflection X products (version 13 or 14), use the following tables to find features in Reflection X Advantage.

## Client Settings

Legacy Reflection X client files (*.rxc) are migrated automatically to Reflection X Advantage X Clients and XDMCP Connections the first time you run Reflection X Advantage. See Upgrading from Legacy Reflection X (page 17).

<table>
<thead>
<tr>
<th>Reflection X version 13 or 14</th>
<th>Reflection X Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client file (.rxc)</td>
<td>All settings are saved to the Reflection X Advantage database (page 217)</td>
</tr>
<tr>
<td>X Client connection settings such as Method, Host name, User name, Password, and Command</td>
<td>Client definition.</td>
</tr>
<tr>
<td>Advanced client connection settings</td>
<td>Client definition &gt; select a Connection method &gt; click Advanced.</td>
</tr>
<tr>
<td>Secure Shell authentication and encryption</td>
<td>Client definition &gt; Connection method = Secure Shell &gt; Advanced button</td>
</tr>
<tr>
<td>Secure Shell key management</td>
<td>Tools &gt;Secure Shell User Keys, Tools &gt;Secure Shell Host Keys</td>
</tr>
<tr>
<td>XDMCP connection settings</td>
<td>XDMCP Connection definition</td>
</tr>
</tbody>
</table>

## Server Settings

Legacy Reflection X server settings are stored in the Windows registry. These settings are migrated automatically to Reflection X Advantage session definitions (page 257) the first time you run Reflection X Advantage. Server settings are migrated to a session definition called "config." (If you created any new X Server Instances, these settings are migrated using the name you provided.)

<table>
<thead>
<tr>
<th>Reflection X version 13 or 14</th>
<th>Reflection X Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Window Manager</td>
<td>General &gt;</td>
</tr>
<tr>
<td>Window mode</td>
<td>General &gt;</td>
</tr>
<tr>
<td>Microsoft Windows desktop or X terminal desktop</td>
<td>Show clients on my desktop or Show clients on X terminal desktop</td>
</tr>
</tbody>
</table>
Reflection X version 13 or 14

X display number

Display > Require display number (By default, Reflection X Advantage dynamically chooses a display number based on available ports.)

X Screen

Number of X screens > Specify total number

Display Click plus (+) in the title bar of the Screen Definition table to add a screen.

Virtual width pixels

Display > Screen Definition table > Virtual Width (Pixels)

Virtual height pixels

Display > Screen Definition table > Virtual Height (Pixels)

MM width dimension

Display > Screen Definition table > Width (mm)

MM height dimension

Display > Screen Definition table > Height (mm)

Place it on monitor(s)

Display > Screen Definition table > Monitor

Full size (no title bar)

Display > Screen Definition table > Hide Title Bar

Server

Backings store

Display > Backing store

Save unders

Enable X11R3 bug compatibility

Display > Permit X11R3 bugs

Exit when last client closed

General > On last client > Stop session and exit X Manager

Confirm close when clients are connected

File > Preferences > On exiting X Manager > Prompt

Extensions

Extensions

Log file

See “Log Files” on page 246

Log X protocol errors

Logging > Log X protocol errors

Fonts

Font path

Fonts > Server font path

Allow font scaling

Fonts > Allow font scaling

Log font activity

Logging > Log font activity

Try font server on client host

Fonts > Use font server on X client host

Allow font substitution

Fonts > Allow font substitutions

Color

Default visual type

Display > Screen Definition table > Default Visual Type
Reflection X version 13 or 14  Reflection X Advantage

Colormap preallocation  Display > Screen Definition table > Black and White Pixels and Allocate B&W in Client Maps

Set maximum colormaps to 1  Display > Set maximum colormaps to 1

Advertise linear visuals  Display > Screen Definition table > Linear Visuals

Advertise single depth visuals  Display > Screen Definition table > Single Depth Visuals

RGB Color file  Display > Color scheme > Edit > Import

Security

Host-based security  Security > Host-based authorization

Host access security file  Security > Authorized Hosts (this option is visible when Host-based authorization is enabled.)

User-based security  Security > User-based authorization

User authorization Duration  Security > Authorization timeout (this option is visible when User-based authorization is enabled.)

Network

Disable remote TCP/IP connections  Security > Allow remote IP connections

Enable keep alives  Advanced > Perform IP keep alives

Log server network activity  Logging > Log network activity

Keyboard settings

Backspace key sends  Keyboard > Backspace sends

Allow clients to remap keyboard  Keyboard > Permit X clients to remap the keyboard

Host keyboard  Keyboard > Keyboard Map (select a predefined keyboard)

Keyboard map  Keyboard > Keyboard Map > Edit (To create a custom keyboard map, start by cloning the default keyboard map.)

Mouse

Enable Mouse wheel scroll  Mouse > Mouse wheel scroll > Disable scroll wheel

Mouse wheel > Customize  Mouse > Mouse wheel scroll

Enable middle button emulation  Mouse > Enable middle button emulation

Middle button detection speed  Mouse > Middle button detection speed

Clipboard

Selection bound to clipboard  Display > Selection bound to clipboard
File Access Restrictions for Files With Sensitive Information

Some files used by Reflection X Advantage contain information that might pose a security risk if acquired or modified by a malicious user. When files with sensitive data are created, they are given file permissions that minimize this risk. You should not change these default permissions, as doing so creates an increased security risk. Depending on how you install and configure Reflection X Advantage, you may have files that contain the following sensitive information:

- Private keys used to authenticate a user to a remote X client host. Depending on your configuration, these files may be on your file system or stored within the Reflection X Advantage database.
- Saved passwords. Passwords are saved to the Reflection X Advantage database. Passwords in the database are not encrypted. The security of this information is maintained by the access restrictions on the database files.
- Reflection X Service settings identifying the nodes in a distributed Reflection X Advantage configuration, and the ports used by those nodes.
- Private keys used by Reflection X Advantage to authenticate programs and users during session sharing and use of remote session services.

Log File Warnings

When a Reflection X Advantage program or service uses a file that should be configured for restricted access and the file permissions have been modified in a way that presents a potential security risk, the program or service continues to use that file, but also logs a warning to the appropriate log file. See Logging (page 246) for information about where to locate log files.

For example, the following `xmanager.log` entry shows that the private key `demokey`, which was used to authenticate to an X client host, has insufficient access restrictions:

```
[ WARN]: Permissions incorrect for C:\Users\Joe\Documents\demokey. The permissions should be set to only allow Joe access.
```

Files with Access Restrictions

The files in the table below are created using the recommended access restrictions shown in the table. These permission settings should not be modified.

<table>
<thead>
<tr>
<th>Files</th>
<th>Location</th>
<th>Access Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Shell user keys</td>
<td>User-defined. Note: It is recommended that you put user keys in a directory that is owned by the user; however, placing keys in a shared location does not generate a warning as long as the keys themselves use the default access restrictions.</td>
<td>Readable and writable only by the user.</td>
</tr>
</tbody>
</table>
### Changing the JRE

By default Reflection X Advantage installs and uses a private Java Runtime Environment (JRE). This installed JRE is correctly configured to fully support all Reflection X Advantage features. It is also possible to configure Reflection X Advantage running on Windows to use a different JRE. The information that follows is provided for administrators who want to configure Reflection X Advantage to use a separately installed JRE.

<table>
<thead>
<tr>
<th>Files</th>
<th>Location</th>
<th>Access Restrictions</th>
</tr>
</thead>
</table>
| Stand-alone X Manager database (on the computer running X Manager) | **Windows:**
C:\ProgramData\.attachmate\rx\db
-or-
C:\Documents and Settings\All Users\.attachmate\rx\db

**UNIX:**
$HOME/\.attachmate/rx/db
| | Readable and writable only by the user |
| Domain database (on the computer running the Domain Controller) | **Windows:**
C:\ProgramData\.attachmate\rx\db
-or-
C:\Documents and Settings\All Users\.attachmate\rx\db

**UNIX:**
/opt/rxadvantage/rx/db
| | Readable and writable only by administrator |
| Reflection X Service configuration files: | **Windows:**
C:\ProgramData\.attachmate\rx\conf
-or-
C:\Documents and Settings\All Users\.attachmate\rx\conf

**UNIX:**
<xrxa_installation_directory>/conf
| | Writable only by administrator |
| Reflection X Service identity files: | **Windows:**
C:\ProgramData\.attachmate\rx\conf
-or-
C:\Documents and Settings\All Users\.attachmate\rx\conf

**UNIX:**
<xrxa_installation_directory>/conf
| | Readable and writable only by administrator |
| X Manager application and user private keys (not user-generated; these are used by X Manager for session sharing): | **Windows:**
C:\ProgramData\.attachmate\rx\identity
-or-
C:\Documents and Settings\All Users\.attachmate\rx\identity

**UNIX:**
$HOME/\.attachmate/rx/identity
| | Readable and writable only by the user |
NOTE

- Micro Focus will supply updated Java installation packages as needed to provide customers with Java security updates. These packages can be downloaded and applied independently of updates to the main Reflection X Advantage package. If you update the JRE using a Micro Focus Java package, your JRE will be correctly configured automatically. The information below is not required for these installations; it is provided for users who want to update their JRE without using the Micro Focus installer.

- If you want to use the private JRE installed by the Micro Focus Java package, you must select the **Java Runtime Environment (JRE)** feature in the installation feature tree. In addition to running the associated Java installer, this feature modifies settings in the Windows registry that configure Reflection X Advantage to use the private JRE.

---

**JRE Search**

Reflection X Advantage running on Windows uses the following search order to locate a JRE on your system.

- The private JRE installed with Reflection X Advantage when you include the feature "Java Runtime Environment (JRE)."
- The path specified in an environment variable called RXA_JRE_HOME. See instructions below for configuring this variable.
- A system JRE that has already been installed on your system using the Oracle installer. (Note that the default JRE installed from a browser does not include unlimited strength cryptography files and is for a "client" environment, not a "server" environment. Refer to the procedures that follow to configure a JRE that resolves these problems.)

If no JRE is available, the Reflection X Advantage applications will not run and the **Reflection X Advantage application log files** will include a message saying that the application failed to start because the JVM is not available. (This message also appears as a warning in the Windows Event log.)

The Reflection X Advantage **application logs** provide information about which JRE is used. Search for "JVM_EXE." For example:

```
INFO - [ INFO] : JVM_EXE is: C:\Program Files\Common Files\Micro Focus\JDK\Java7\jre\bin\java.exe
```

---

**JRE Error and Warning Messages in the Log Files**

If a JRE is found, Reflection X Advantage will check to see if the JRE meets all the conditions of the private JRE. (page 246)

If you run in domain mode, the JRE must be configured for unlimited strength cryptography.

- A fatal error is written to the *rsx.log* when you attempt to start the Reflection X Service using a JRE that is not configured for unlimited strength cryptography. To resolve this, see instructions below to apply Oracle’s Unlimited Strength Jurisdiction Policy Files to your JRE.

Warnings are written to the **application log files** if:

- The running JRE is older than the version shipping with this build of Reflection X Advantage.
- The running JRE is for a "client" environment, not a "server" environment. To resolve this, see the instructions below for installing a Java Development Kit (JDK) from the Oracle site.
- You run X Manager using a JRE that is not configured for unlimited strength cryptography. Neither export-controlled crypto algorithms nor FIPS mode will be available. To resolve this, see instructions below to apply Oracle’s Unlimited Strength Jurisdiction Policy Files to your JRE.
Installing and Configuring a JRE

Use the following procedures to configure Reflection X Advantage running on Windows to use a non-default JRE.

The default JRE installed from a browser is for a "client" environment, not a "server" environment. Reflection X Advantage requires the server JRE for full functionality. You can download and install this from the Oracle website.

Step 1: Install a Java JDK from the Oracle site


   Download and install the JRE using either the JDK download (which installs the server JRE) or the Server JRE download.

   Download the most recent update of the major version Java that was included with Reflection X Advantage. For version 5.1, download the most recent Java 8 update.

2. After installing the JRE, run the following command to confirm that the JRE version reported is the version you downloaded:

   `/<java-path>/bin/java -version`

   For example:

   `# /jdk/jdk1.8.0_<nn>/jre/bin/java -version`

   `java version "1.8.0_<nn>"
   Java(TM) SE Runtime Environment (build 1.8.0_<nn>-b01)`

The next procedure configures an environment variable that directs Reflection X Advantage applications to use the correct JRE.

Step 2: Configure the RXA_JRE_HOME variable

1. Open Windows System Properties (Start > Control Panel > System > Advanced system settings).

2. From the Advanced tab click Environment Variables.

3. Under System variables, click New, define a new variable as follows, then click OK.

   Variable name  RXA_JRE_HOME
   Variable value  The location of the Java JRE. Point to the JRE located in the JDK installation. This is the JRE configured for a server environment. For example:

   `C:\Program Files\Java\jdk1.8.0_<nn>\jre`

4. Click OK to close the open dialog boxes.

The next procedure applies the Java Unlimited Strength Jurisdiction Policy Files. This step is recommended for all installations. It is required to run the Reflection X Advantage domain services. It is also required if you enable FIPS Mode.
Step 3: Apply the Unlimited Strength Jurisdiction Policy Files to your JRE

NOTE: Each time you upgrade your JRE, you need to apply the unlimited strength policy files to the new JRE.

2. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.
3. Unzip the downloaded file and locate the following two policy files.
   - local_policy.jar
   - US_export_policy.jar
4. Copy the policy files to `<java home>\jre\lib\security`, replacing the existing files in your JRE folder. For example:
   C:\Program Files\Java\jdk1.8.0_<nn>\jre\lib\security

Uninstall the default JRE

If you're setting up an alternate JRE and have already installed the default JRE with Reflection, you must uninstall the default JRE. To do this, use the following procedure:

To uninstall the default Micro Focus JRE

1. To open the Programs and Features control panel go to Start > Control Panel > Programs and Features. (On older Windows systems, this Control Panel is called Add or Remove Programs.)
2. Select the entry with your Reflection product name — not the Java entry — and click Change.
3. On the Feature Selection tab, click the icon to the left of Java Runtime Environment (JRE) and select Feature will be Unavailable.
4. Click Continue.

Upgrade Digital Certificates used by Reflection X Advantage Domains

Digital certificates are used in domain mode for authenticating domain nodes and the domain controller. Starting with version 5.0, these certificates use a more secure signing algorithm. If you have upgraded from an earlier version, the domain continues to use your prior version certificates and logs the following warning message in the `rxs.log` (page 246) file:

[WARN]: The domain root certificate generated by an earlier version of Reflection X Advantage is signed using the SHA1withRSA algorithm. Current versions create certificates signed using the more secure SHA-256 RSA algorithm. You can upgrade certificates by removing existing certificates.

If you run in FIPS mode, you must upgrade your domain to use the more secure certificates before you can log into the domain. Until you upgrade the certificates, attempts to log into the domain will fail with the message "Authentication with the domain failed." The `domain.log` file will include a warning entry saying that the connection was rejected because the domain is set for FIPS mode, but has a public key of insufficient length. Use the procedure below to resolve this issue.
To upgrade your domain to use SHA-256 RSA certificates

1. Stop the Micro Focus Reflection X Service on the domain controller and on any domain nodes. (page 154)

2. Locate the Reflection X Service configuration files (page 217) on the domain controller and all domain nodes. The certificates are located in the `conf` subfolder. Delete all certificates (*.cer) and any associated private key files (same base file name as a certificate with no file extension) from the controller and nodes.

   **NOTE:** Do not delete the *.xml files in the `conf` folder.

3. Restart the service on the domain controller and nodes. This step generates new certificates and keys to replace the ones you deleted.

4. Log onto X Administrative Console and delete all node definitions. (These will all have a red slash through them indicating that they are not available.)

5. On each node, use `rxsconfig` to leave (page 156) the domain. You should see a message like the following:

   Unable to remove node 0.0.0.0:22001 from domain domainname. Proceeding with local deletion.
   Deleted node 0.0.0.0:22001 for domain domainname

6. Use `rxsconfig` to rejoin (page 155) each node to the domain.

## Command Line Utilities

### rxmgr Command Line - Standalone X Manager

You can run X Manager and start clients and sessions from a command line using the following syntax:

```
rxmgr [-client client_name] [-xdmcp xdmcp_definition |
[direct|indirect|broadcast,[host_address],[timeout],[onLastClient]]][-launchGroup launchGroup_Name] [-session session_name][-minimize] [-trayOnly] [-noUI]
[-execOnly] [-import filename_or_URL][-noStart] [-noMigrate] [-?]
```

### Examples

The following example starts the xterm client and the session associated with it. In this example X Manager will run minimized.

```
rxmgr -client xterm -minimize
```

The following examples show two ways to start multiple clients (and any sessions associated with these clients): you can include all the clients on the command line or use a saved launch group definition. Quotation marks are required around the client and launch group definition names in these examples because the names include spaces.

```
rxmgr -client "Client 1" -client "Client 2" -client "Client 3"
-or-
rxmgr -launchGroup "Work Group"
```

The following example starts an XDMCP connection to "Myhost" without using an existing definition and without showing the X Manager for Domains window. When the user logs out of the XDMCP session, the session will stop and X Manager will exit.
rxmgr -xdmcp direct,Myhost,,Exit -noUI

The following example launches X Manager with limited functionality. The user can launch existing definitions, but not add or modify definitions:

rxmgr -execOnly

## Options

The command line options are all optional. Options are case-insensitive. Use quotation marks around paths and definition names that include spaces.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-client client_name</td>
<td>Specify a client definition to start. To start multiple clients, use multiple client parameters (or configure a launch group.)</td>
</tr>
<tr>
<td>-xdmcp xdmcp_definition</td>
<td>Start an XDMCP connection using an existing definition name.</td>
</tr>
<tr>
<td>-launchGroup group_name</td>
<td>Launch all X clients and/or XDMCP connections in the specified launch group definition.</td>
</tr>
<tr>
<td>-session session_name</td>
<td>Specify a session definition to start. To start multiple sessions, use multiple session parameters.</td>
</tr>
<tr>
<td>-minimize</td>
<td>Start in a minimized state. This option is ignored if it’s not supported by the operating system. This option is ignored if trayOnly is also specified.</td>
</tr>
<tr>
<td>-trayOnly</td>
<td>Start with a tray icon but without opening the X Manager window. Note: When a session is started with this option, you can use either the tray icon or the Start menu to open the X Manager window.</td>
</tr>
<tr>
<td>-noUI</td>
<td>Start with an icon in the tray area and without allowing the user to open the X Manager window. With this option, the Open X Manager option is disabled from the tray icon; the Exit and Help Topics options remain available. Note: When a session is started with this option, it is not possible to open the X Manager window from the Start menu until the session is closed and you stop X Manager using the tray icon’s Exit option.</td>
</tr>
<tr>
<td>-execOnly</td>
<td>Start with the user interface restricted to a list of definitions (X Clients, XDMCP Connections, Launch Groups, Sessions) and the basic controls to start, stop, leave and join. Items that allow creating new definitions, deleting definitions, or accessing other features (such as keyboard maps and color maps) related to definitions are not available.</td>
</tr>
</tbody>
</table>

Do not use spaces after the commas in this option, and include a comma as placeholder for any option you don’t need to specify. For example:

- xdmcp direct,myhost,,E
rxmgrdomains Command Line - X Manager for Domains

You can run X Manager for Domains and start clients and sessions from a command line using the following syntax:

```
```

**Examples**

The following example logs the user Joe into the domain called "AcmeServer" and runs the client called xterm. In this example, X Manager for Domains will run minimized.

```
rxmgrdomains -domain AcmeServer -user Joe -password "secret" -client xterm -minimize
```

The following examples show two ways to start multiple clients (and any sessions associated with these clients). You can include all the clients on the command line or use a saved launch group definition. Quotation marks are required around the client and launch group definition names in these examples because the names include spaces. In these examples the domain user and password are omitted, so the user will be prompted for login credentials.

```
rxmgrdomains -domain AcmeServer -client "Client 1" -client "Client 2" -client "Client 3"
```

or

```
rxmgrdomains -domain AcmeServer -launchGroup "Work Group"
```
The following example starts an XDMCP connection to "My Host" without using an existing definition and without showing the X Manager for Domains window. This example is configured to log onto the domain as user Joe, who will be prompted for a password. When the user logs out of the XDMCP session, the session will stop and X Manager for Domains will exit.

```
rxmgrdomains -domain AcmeServer -user Joe -xdmcp direct,Myhost,,Exit
```

The following example launches X Manager for Domains with limited functionality. The user can launch existing definitions, but not add or modify definitions:

```
rxmgrdomains -execOnly
```

### Options

The command line options are all optional. Options are case-insensitive. Use quotation marks around paths and definition names that include spaces. If a domain name, user name, or password is not specified, the user is prompted to provide it.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-domain domain_name</td>
<td>The domain name. This is the name of the computer running the domain controller.</td>
</tr>
<tr>
<td>-user user_name</td>
<td>The name of a domain user.</td>
</tr>
<tr>
<td>-password password</td>
<td>The password for the specified domain user. Use quotation marks if the password includes special characters.</td>
</tr>
<tr>
<td>-client client_name</td>
<td>Specify a client definition to start. To start multiple clients, use multiple client parameters (or configure a launch group.)</td>
</tr>
<tr>
<td>-xdmcp xdmcp_definition</td>
<td>Start an XDMCP connection using an existing definition name.</td>
</tr>
<tr>
<td>-or-</td>
<td></td>
</tr>
<tr>
<td>-xdmcp direct</td>
<td>indirect</td>
</tr>
<tr>
<td>-launchGroup group_name</td>
<td>Launch all X clients and/or XDMCP connections in the specified launch group definition.</td>
</tr>
<tr>
<td>-session session_name</td>
<td>Specify a session definition to start. To start multiple sessions, use multiple session parameters.</td>
</tr>
</tbody>
</table>
Use `rxmigrate` on Windows systems to migrate settings from legacy Reflection X versions (v. 13 or 14) or from Hummingbird Exceed products. As `rxmigrate` runs, it displays messages to the console. In addition a `migration.log` file is created in the `logs` (page 246) folder (typically \C:\Users\<user>\attachmate\rx\logs\migration.log).

### Option Description

- **-owner**
  - This is only valid when preceded by a `client`, `xdmcp`, `launchGroup`, or `session` option. It specifies the name of the user who created the preceding definition. When it is `owner` is not specified, the owner is assumed to be the currently logged in domain user.

  This option is used by X Manager for Domains in desktop shortcuts, and allows the shortcut to distinguish between a definition created by the domain logon user or an identically-named definition created by the administrator and made public. Users should never need to use this option.

- **-minimize**
  - Start in a minimized state. This option is ignored if it's not supported by the operating system. This option is ignored if `trayOnly` is also specified.

- **-trayOnly**
  - Start with a tray icon but without opening the X Manager window. Note: When a session is started with this option, you can use either the tray icon or the Start menu to open the X Manager window.

- **-noUI**
  - Start with an icon in the tray area and without allowing the user to open the X Manager window. With this option, the Open X Manager option is disabled from the tray icon; the Exit and Help Topics options remain available. Note: When a session is started with this option, it is not possible to open the X Manager window from the Start menu until the session is closed and you stop X Manager using the tray icon's Exit option.

- **-execOnly**
  - Start with the user interface restricted to a list of definitions (X Clients, XDMCP Connections, Launch Groups, Sessions) and the basic controls to start, stop, leave and join. Items that allow creating new definitions, deleting definitions, or accessing other features (such as keyboard maps and color maps) related to definitions are not available.

- **-noMigrate**
  - Affects initial startup actions as follows:
    - Disables automatic import of the "Sample Definitions" on page 25 in the template `generic_templates.rxd`, and any added templates configured for automatic import on first run.
    - Disables migration of settings from legacy Reflection X and Exceed.
    - Disables display of the Import Migrated Settings and Templates dialog box.

- **-? or -help**
  - Displays a summary of command line options.

### rxmigrate Command Line Utility - Migrate Settings

As `rxmigrate` runs, it displays messages to the console. In addition a `migration.log` file is created in the `logs` (page 246) folder (typically \C:\Users\<user>\attachmate\rx\logs\migration.log).
NOTE: Settings stored on your local system are migrated automatically the first time you run Reflection X Manager or Reflection X Manager for Domains. Even if you choose not to import the settings on first run, you can manually import the migrated settings later. Settings in a shared network location are not imported automatically. You can use `rxmigrate` to migrate these settings.

To convert legacy Reflection X settings:

```
rxmigrate [-a] [-c client1.rxc ...] [-s server1.rxs ...] [-k known_hosts ...] -o output.rxd
```

To convert Exceed settings:

```
rxmigrate -product Exceed [-a] [-c client1.xs ...] [-s session1.ses ...] [-xc server1.xcfg...] -o output.rxd
```

Examples

The following command line shows the options used for a default migration of settings from Reflection X 14.0. It migrates all Reflection X client and server settings, and any known host keys used for Secure Shell connections. The output file is located in a `migration` folder in the Reflection X Advantage data folder.

```
rxmigrate -a -o "%userprofile%\.attachmate\rx\migration\Reflection X 14_0_1.rxd"
```

The following command converts all Reflection X client files (*.rxc) in the specified network share and saves them to the specified output file.

```
rxmigrate -c \sharedsettings\attachmate\rx\*.rxc -o "c:\migrated settings\RXsettings.rxd"
```

The following command migrates all Exceed settings and saves them to the specified output file:

```
rxmigrate -product Exceed -a -o c:\migrate\Exceedsettings.rxd
```

Options

Note: For options that specify filenames, wildcards are supported for file names but not for directory names.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-product</td>
<td>(Optional) Specifies the product to be migrated. Valid values are Reflection and Exceed. If this option is omitted, the utility performs Reflection migration.</td>
</tr>
<tr>
<td>-a</td>
<td>(Optional) Migrates all client and server settings found on the local machine. When no product is specified, this option converts all legacy Reflection X settings (including known hosts).</td>
</tr>
<tr>
<td>-c</td>
<td>(Optional) Migrates the client settings from the specified client files (for example, client1.rxc client2.rxc).</td>
</tr>
<tr>
<td>-s</td>
<td>(Optional) Migrates the server settings (Reflection X) or session settings (Exceed) from the specified server files (for example, server1.rxs server2.rxs).</td>
</tr>
<tr>
<td>-xc</td>
<td>(Optional) Migrates Exceed server settings from the specified server files.</td>
</tr>
<tr>
<td>-k</td>
<td>(Optional) Migrates the hosts found in specified files (for example, known_hosts). This option applies to Reflection migration only.</td>
</tr>
</tbody>
</table>
## rxsconfig Command Line Utility - Domain Configuration

Use **rxsconfig** to:

- Add the local computer (the one from which you run this utility) as a node to a Reflection X Advantage domain.
- Remove the local computer from the domain.
- Place a domain in recovery mode.
- Display a list of configured Reflection X services processes.

### General syntax

```bash
rxsconfig join | leave | recover | version | list
```

Use the following syntax to view the options available for each command:

```bash
rxsconfig <command> -help
```

### Join

Adds the local computer as a node on the specified domain. (See options below.) The **join** syntax is:

```bash
rxsconfig join [-u user] [-p password] [-f] [-a alternate-address[,....]] domain [node-listening-address]
```

For example, to add the computer from which you are running **rxsconfig** to a Reflection X Advantage domain running on rxa.domain.com:

```bash
rxsconfig join rxa.domain.com
```

### Leave

Removes the local computer from the domain. (See options below.) The **leave** syntax is:

```bash
rxsconfig leave [-u user] [-p password] [-f] domain [node-listening-address]
```

For example:

```bash
rxsconfig leave rxa.domain.com
```

### Recover

Instructs the domain to enter recovery mode the next time the service starts. Use recovery mode if you are locked out of a domain because you forgot the administrator password, changed authentication methods without adding an administrative account, or experience a problem with the external authentication system. The **recover** syntax is:

```bash
-recover
```

### Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-o</code></td>
<td>(Required) Specifies the path and file name of the output file to create (for example, output.rxd). Use quotation marks if the path includes spaces.</td>
</tr>
<tr>
<td><code>-version</code></td>
<td>Displays Reflection X Advantage version information.</td>
</tr>
<tr>
<td><code>-?</code> or <code>-help</code></td>
<td>Displays a summary of command line options.</td>
</tr>
</tbody>
</table>
rxsconfig recover [-f] [domain_listening_address]

For additional information about using the recover option, see "Unlock a Domain" on page 162.

**Version**

Displays Reflection X Advantage version information. The version syntax is:

```bash
rxsconfig version
```

**List**

Displays configured Reflection X Service processes (domain controllers, domain nodes, and remote session service nodes) sorted by port number. Each line contains the listening address and a brief description. The list syntax is:

```bash
rxsconfig list
```

**NOTE**

- You must have root/administrative privileges on the computer in order to use rxsconfig.
- On UNIX systems, the installer does not add rxsconfig to the path. Run it from the install directory, include complete path information, or add it to your path. On UNIX systems, the default location is /opt/rxadvantage/rxsconfig.
- For newer Windows systems (starting with Windows Vista and Windows Server 2008), you need to open the command window as an administrator. (In the Start menu, under Accessories, right-click Command Prompt and select Run As Administrator).

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-u user</code></td>
<td>(optional) Specifies a Reflection X Advantage domain administrator. You will be prompted for a user name if this parameter is not specified.</td>
</tr>
<tr>
<td><code>-p password</code></td>
<td>(optional) Specifies the Reflection X Advantage domain user’s password. You will be prompted for a password if this parameter is not specified.</td>
</tr>
<tr>
<td><code>-f</code></td>
<td>(optional) Runs rxsconfig in non-interactive mode. In this mode, <code>-u</code>, <code>-p</code>, and domain are required parameters. The default response is used for any unspecified options.</td>
</tr>
<tr>
<td><code>-a alternate-address</code></td>
<td>(optional) Defines a comma delimited list of one or more alternate addresses for the domain node. Use this option if the node you are configuring resides behind a firewall that uses Network Address Translation (NAT). For example: alternate.company.com:1234, 10.10.0.2:5678 You can omit the port and specify only an IP address. In this case, the port from the primary listening address is used. Note: You can also add or modify alternate addresses for a node from the X Administrative Console Domain Composition tab.</td>
</tr>
<tr>
<td><code>domain</code></td>
<td>(required for join or leave) The name of the Reflection X Advantage domain controller, such as rxa.company.com.</td>
</tr>
</tbody>
</table>
Advantage

Reflection PKI Services Manager is a service that provides X.509 certificate validation services. If you configure Secure Shell connections to X client hosts that authenticate using certificates, you need to download and install this application. It is available at no additional charge from the Reflection X Desktop and Reflection Pro Desktop download pages.

- Reflection PKI Services Manager is required for Secure Shell connections that use certificates for host authentication. (It is not required for user authentication with certificates.)
- Reflection PKI Services Manager is required if you configure connections using the Management and Security Server Administrative WebStation that use the Security Proxy. For these connections PKI Services Manager validates the Security Proxy's certificate.
- Reflection PKI Services Manager is supported on both Windows and UNIX platforms.
- Reflection PKI Services Manager supports central management of PKI settings. You can install and configure a single instance of PKI Services Manager to provide certificate validation services for all supported Micro Focus products. (Because Reflection X Advantage settings allow only one entry for the PKI Services Manager address and port, this configuration creates a potential single point of failure. If PKI Services Manager is unreachable or the server is not running, all

Using PKI Services Manager with Reflection X Advantage

Reflection PKI Services Manager is a service that provides X.509 certificate validation services. If you configure Secure Shell connections to X client hosts that authenticate using certificates, you need to download and install this application. It is available at no additional charge from the Reflection X Desktop and Reflection Pro Desktop download pages.

- Reflection PKI Services Manager is required for Secure Shell connections that use certificates for host authentication. (It is not required for user authentication with certificates.)
- Reflection PKI Services Manager is required if you configure connections using the Management and Security Server Administrative WebStation that use the Security Proxy. For these connections PKI Services Manager validates the Security Proxy's certificate.
- Reflection PKI Services Manager is supported on both Windows and UNIX platforms.
- Reflection PKI Services Manager supports central management of PKI settings. You can install and configure a single instance of PKI Services Manager to provide certificate validation services for all supported Micro Focus products. (Because Reflection X Advantage settings allow only one entry for the PKI Services Manager address and port, this configuration creates a potential single point of failure. If PKI Services Manager is unreachable or the server is not running, all
authentication attempts using certificates will fail. In order to provide load balancing and failover, you can define a round-robin DNS entry for the PKI Services Manager host name or place the PKI Services Manager host behind a load balancing server.

- You can run Reflection PKI Services Manager on the same host as a Reflection X Advantage domain controller or on a different host.

This user guide provides basic information about installing PKI Services Manager and configuring Reflection X Advantage to use it for certificate validation services. For additional information, refer to the PKI Services Manager documentation at http://support.attachmate.com/manuals/pki.html (http://support.attachmate.com/manuals/pki.html).

**How it Works**

1. The X client host presents a certificate to Reflection X Advantage for host authentication.
2. Reflection X Advantage connects to Reflection PKI Services Manager and verifies its identity using an installed public key.
3. Reflection X Advantage sends the certificate and host name to PKI Services Manager.
4. PKI Services Manager determines if the certificate is valid and uses mapping rules to determine whether the host is allowed to authenticate with this certificate.
5. If the certificate is valid and the host presenting it is an allowed identity for this certificate, Reflection X Advantage validates the host's digital signature. If the digital signature is verified, host authentication is successful.

**In this Section**

- “Setting up PKI Services Manager on Windows” on page 236
- “Setting up PKI Services Manager on UNIX” on page 239
- “Configure Reflection X Advantage to Connect to PKI Services Manager” on page 243

**Setting up PKI Services Manager on Windows**

**In this Section**

- “Install and Uninstall PKI Services Manager on Windows” on page 236
- “Configure PKI Services Manager on Windows” on page 237
- “Start and Stop the PKI Services Manager Service on Windows” on page 239

**Install and Uninstall PKI Services Manager on Windows**

Reflection PKI Services Manager is a service that provides X.509 certificate validation services. If you configure Secure Shell connections to X client hosts that authenticate using certificates, you need to download and install this application. It is available at no additional charge from the Reflection X Desktop and Reflection Pro Desktop download pages. Use this procedure to install Reflection PKI Services Manager on Windows systems.
NOTE: Reflection PKI Services Manager supports central management of PKI settings. You can install and configure a single instance of PKI Services Manager to provide certificate validation services for all supported Micro Focus products.

To install Reflection PKI Services Manager

1 Log in as an administrator.

2 Start the Setup program (Setup.exe). If you are installing from the download site, the following steps start this program:
   2a From the download site, click the Windows download link and run the download program.
   2b Select a location for the installer files, and then click Next. This extracts the files to the specified location and starts the Setup program.

3 Accept the default settings on the Advanced tab. (Creating an administrative installation image does not actually install the product — instead, it places the install files on a network location for later installation to multiple workstations.)

4 Start the service (page 239).

NOTE

- On Windows, starting the console or the service for the first time initializes PKI Services Manager. This creates the required data folders and default settings files. If these folders already exist, they are not changed; PKI Services Manager uses your existing data files and folders. (On UNIX the install script automatically initializes PKI Services Manager if required, and starts the service.)
- Before Reflection PKI Services Manager can validate certificates you need to edit the default configuration and map files.

To uninstall Reflection PKI Services Manager

1 Log in as an administrator.

2 From the Windows Programs and Features (or the Add or Remove Programs) control panel, select Micro Focus Reflection PKI Services Manager.

3 Click Uninstall (or Remove).

Configure PKI Services Manager on Windows

To configure client host authentication using certificates, you need to install and configure Reflection PKI Services Manager. Use the following procedure to get started. Many variations are possible. For more information about each of the steps below, see the Reflection PKI Services Manager User Guide, which is available from the PKI Services Manager console, and from http://support.attachmate.com/manuals/pki.html (http://support.attachmate.com/manuals/pki.html).

Before you begin

- Install PKI Services Manager (page 236).
Determine which trusted CA certificate and intermediate certificates are needed to validate the certificate that will be presented by the host you are connecting to. PKI Services Manager can use certificate files that you copy to your system, or trusted root certificates installed to the Windows certificate store for use by the local computer.

Determine how certificate revocation checking should be handled for the host certificate. You can configure PKI Services Manager to use CRL lists, OCSP responders, or to contact a CRL distribution point specified within the certificate.

To configure PKI Services Manager

1. Log in as an administrator on the computer running PKI Services Manager.
2. Start the PKI Services Manager console:
   Programs > Attachmate Reflection > Utilities > PKI Services Manager
3. Put a copy of the certificate (or certificates) you want to designate as a trust anchor into your certificate store. The default PKI Services Manager store is in the following location:
   common application data folder (page 258)\Attachmate\ReflectionPKI\local-store
   (This step is not required if you are using certificates in the Windows store or you have a copy of the trust anchor available somewhere else on your system.)
4. From the Trusted Chain pane, add your trust anchor (or anchors) to the list of trust anchors.

To use this store | Do this
---|---
Your local certificate store or a certificate file on your system | Click Add. Select either Local store certificate or Certificate file, click Browse and select the certificate for your trust anchor.

The Windows certificate store | Under Search order to use when building path to trust anchor, select "Windows certificate store."
   Click Add.
   From the Add Trust Anchor dialog box, select Windows certificate then click Browse to select an available certificate.
   NOTE: PKI Services Manager uses only those certificates that are installed for use by the local computer (not certificates installed for the current user) and are in either the trusted root certification authorities list or the trusted intermediate authorities list. To view and manage the local computer certificates, use the Microsoft Management Console. Add the Certificates Snap-in and configure it to manage certificates for the computer account.

5. From the Revocation pane, configure certificate revocation checking.

   **NOTE:** By default PKI Services Manager looks for CRLs in the local store. If you use this configuration, you need to copy the CRLs to your local store.

6. From the Identity Mapper pane, click Add to determine which client hosts can authenticate with a valid certificate.
   For example, to allow client hosts to connect if the host name is specified in the Common Name value of the certificate’s Subject field:
   - Set Select type of certificate that is to be mapped to Host Certificate
   - Click the drop-down arrow for Choose certificate identity to insert and select Subject Common Name.
Refer to the PKI Services Manager documentation for additional information about mapping rules.

7  Click File > Save.

8  Start the PKI Services Manager service (page 239) if it isn't already running. If the service is already running, reload your settings (Server > Reload).

Start and Stop the PKI Services Manager Service on Windows

NOTE: The PKI Services Manager service starts automatically when you restart Windows.

To start the service

• From the PKI Services Manager console, click Server > Start.
  -or-
• From a DOS command window, enter the following command:
  winpki start
  -or-
• Open the Windows Services console (Control Panel > Administrative Tools > Services), select Attachmate Reflection PKI Services Manager and click Start.

To stop the service

• From the PKI Services Manager console, click Server > Stop.
  -or-
• From a DOS command window, enter the following command:
  winpki stop
  -or-
• Open the Windows Services console (Control Panel > Administrative Tools > Services), select Attachmate Reflection PKI Services Manager and click Stop.

To check the service status

• Start the PKI Services Manager console and look for status information on the status line at the bottom of the console window.
  -or-
• From a DOS command window, enter the following command:
  winpki ping
  -or-
• Open the Windows Services console (Control Panel > Administrative Tools > Services) and view the status of Attachmate Reflection PKI Services Manager.

Setting up PKI Services Manager on UNIX

Use this information to install, uninstall, and configure PKI Services Manager on UNIX.
Install and Uninstall Reflection PKI Services Manager on UNIX

Reflection PKI Services Manager is a service that provides X.509 certificate validation services. If you configure Secure Shell connections to X client hosts that authenticate using certificates, you need to download and install this application. It is available at no additional charge from the Reflection X Desktop and Reflection Pro Desktop download pages. Use this procedure to install Reflection PKI Services Manager on UNIX systems.

To install Reflection PKI Services Manager

1. Log in as root.
2. Copy the installation package file to your computer and navigate to the directory that contains this file.
3. Use gzip to unzip the package:

   ```
   gzip -d package_name.tar.gz
   ```

   For example:

   ```
   gzip -d pkid_1.3.0.999-i386-solaris.gz
   ```
4. Use tar to expand the file:

   ```
   tar -xf package_name.tar
   ```

   This creates a directory based on the package name. For example:

   ```
   pkid_1.3.0.999--i386-solaris/
   ```
5. Change to this directory. For example:

   ```
   cd pkid_1.3.0.999-i386-solaris
   ```
6. Run the install script:

   ```
   ./install.sh
   ```
7. You are prompted to specify installation locations. To accept the default locations (recommended), press Enter in response to these prompts.

   **NOTE**
   - On UNIX the install script automatically starts the service.
   - Before Reflection PKI Services Manager can validate certificates you need to edit the default configuration and map files.

To uninstall

1. Log in as root.
2. Run the uninstall script. This script is installed to the bin directory in the PKI Services Manager data folder. The default path is:

   ```
   /opt/attachmate/pkid/bin/uninstall.sh
   ```
NOTE: The uninstall script renames your existing configuration directory (\opt\attachmate\pkid\config\ by default) using a name based on the current date, and time. For example, config.20140101143755. Your local-store directory and any certificates you have added to this directory remain unchanged.

Configure PKI Services Manager on UNIX

To configure client host authentication using certificates, you need to install and configure Reflection PKI Services Manager. Use the following procedure to get started. Many variations are possible. For more information about each of the steps below, see the Reflection PKI Services Manager User Guide, which is available from the PKI Services Manager console, and from http://support.attachmate.com/manuals/pki.html.

Before you begin

- Install PKI Services Manager (page 240).
- Obtain the trusted CA certificate and any intermediate certificates that are needed to validate the certificate that will be presented by the host you are connecting to.
- Determine how certificate revocation checking should be handled for the host certificate. You can configure PKI Services Manager to use CRL lists, OCSP responders, or to contact a CRL distribution point specified within the certificate.

To configure PKI Services Manager

1 Log in as root on the Reflection PKI Services Manager server.
2 Install Reflection PKI Services Manager.
3 Put a copy of the certificate (or certificates) you want to designate as a trust anchor into your certificate store. The default PKI Services Manager store is in the following location:
   /opt/attachmate/pkid/local-store
4 Open the PKI Services Manager configuration file in a text editor. The default name and location is:
   /opt/attachmate/pkid/config/pki_config
5 Use the TrustAnchor keyword to identify your trust anchor. For example:
   TrustAnchor = trustedca.crt
   -or-
   TrustAnchor = CN=SecureCA,O=Acme,C=US
   NOTE: To configure multiple trust anchors, add additional TrustAnchor lines.
6 Configure certificate revocation checking. For example:

<table>
<thead>
<tr>
<th>To</th>
<th>Sample Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use CRLs stored on an LDAP server.</td>
<td>RevocationCheckOrder = crlserver CRLServers=ldap://crlserver</td>
</tr>
<tr>
<td>Use an OCSP responder.</td>
<td>RevocationCheckOrder = ocsp OCSPResponders = <a href="http://ocspresponder">http://ocspresponder</a></td>
</tr>
</tbody>
</table>
NOTE: By default PKI Services Manager looks for CRLs in the local store. If you use this configuration, you need to copy the CRLs to your local store.

1 If intermediate certificates are required by the chain of trust in your certificates, configure access to these certificates. For example:

   To  Sample Configuration

   Use intermediate certificates you have added to your local store. CertSearchOrder=local

   Use certificates stored on an LDAP server. CertSearchOrder=certserver CertServers=ldap://ldapserver

2 Save your changes to the configuration file.

3 Open the PKI Services Manager map file in a text editor. The default name and location is:

   /opt/attachmate/pkid/config/pki_mapfile

4 Add one or more rules to determine which client hosts can authenticate with a valid certificate. For example, to allow client hosts to connect if the host name is specified in the Common Name value of the certificate’s Subject field:

   RuleType = host {acme.com}

5 Test for valid PKI Services Manager configuration:

   /usr/local/sbin/pkid -k

   No errors. Configuration is valid:

6 Restart Reflection PKI Services Manager.

   /usr/local/sbin/pkid restart

Start and Stop the Service on UNIX

The PKI Services Manager service starts automatically after installation. A script is installed, which you can use to start, stop, restart, and check the status of the service.

The following procedures use the installed pkid script. For additional options available using the pkid daemon, see PKI Services Manager Command Reference or refer to the man page: man pkid

To start the service

   • On Linux and Solaris: /etc/init.d/pkid start
   • On AIX: /etc/rc.d/init.d/pkid start

To stop the service

   • On Linux and Solaris: /etc/init.d/pkid stop
   • On AIX: /etc/rc.d/init.d/pkid stop

To check the service status

   • On Linux and Solaris: /etc/init.d/pkid status
   • On AIX: /etc/rc.d/init.d/pkid status
Configure Reflection X Advantage to Connect to PKI Services Manager

Reflection X Advantage needs to connect to Reflection PKI Services Manager for host certificate verification. The procedure for configuring this connection depends on whether you are running in standalone or domain mode.

- In standalone mode, use X Manager to configure the connection to PKI Services Manager. This connection must be configured individually on each computer running X Manager.
- In domain mode, you need to use the Administrative Console to configure the connection to PKI Services Manager. This enables you to configure the connection once for all domain users. The connection information is used for all Secure Shell client connections in the domain that require host certificate authentication.

Before you begin

- Install PKI Services Manager (page 240).
- Configure PKI Services Manager. See “Configure PKI Services Manager on Windows” on page 237 or “Configure PKI Services Manager on UNIX” on page 241.

To configure X Manager to connect to PKI Services Manager

1. Start X Manager.
2. From the Tools menu, click Secure Shell Host keys.
3. Click the PKI Configuration tab.
4. For PKI server, specify the host name or IP address of the computer running PKI Services Manager. (You can specify localhost if you're running X Manager and PKI Services Manager on the same computer.)

   **NOTE:** If PKI Services Manager is configured to use a non-default port, include the port value using hostname:port syntax. For example acme.com:18081.

5. Click Download key. This retrieves the public key from the specified PKI server and displays a dialog box that allows you to confirm this identity. To compare the presented fingerprint with the actual PKI Services Manager key open the PKI Services Manager console on the PKI server, and go to Utility > View Public Key.

   When you click Yes to accept the key, the key is imported into the Reflection X Advantage database.

To configure a X Manager for Domains to connect to PKI Services Manager

1. Start the Administrative Console.
2. Click the Domain Composition tab.
3. For PKI server, specify the host name or IP address of the computer running PKI Services Manager. (You can specify localhost if you're running the Reflection X Advantage domain controller and PKI Services Manager on the same computer.)

   **NOTE:** If PKI Services Manager is configured to use a non-default port, include the port value using hostname:port syntax. For example acme.com:18081.
4 Click **Download key**. This retrieves the public key from the specified PKI server and displays a dialog box that allows you to confirm this identity. To compare the presented fingerprint with the actual PKI Services Manager key open the PKI Services Manager console on the PKI server, and go to **Utility > View Public Key**. When you click **Yes** to accept the key, the key is imported into the Reflection X Advantage database.
Troubleshooting

Reflection X Advantage provides tools and tips to help you pinpoint problems you may encounter:

Information and Error Messages

- Information about long-running tasks and error messages is displayed in the Task Status area at the bottom of the X Manager and Administrative Console windows. For tasks related to unsuccessful client connections, click the Information ("i") icon pane to display the Start Client dialog box. Two tabs in this dialog box provide client information.
- For additional information, refer to Reflection X Advantage Technical Notes (http://support.attachmate.com/techdocs/index/RXA.html).

Common Problems

Review the help topics in this section for tips on addressing issues with connections (page 250), displays (page 249), performance (page 251), and “Port Conflicts” on page 251.

Logging

- Domain-related messages and messages generated by X Manager and the X Administrative Console are automatically captured in a log file (page 246).
- To enable additional logging, use the session definition's Logging tab. Information captured is added to the log file.

Trace

If you still can't resolve a problem, you may need to “Create a Trace” on page 247 and send it to Technical Support (http://www.attachmate.com/Support/).

If you send a trace to customer support, include the basic information about the product version you are running from the About box (Help menu > About).

In this Chapter

- “Troubleshooting Tools” on page 246
- “Application Fails to Start” on page 248
- “Display Problems” on page 249
- “Connection Problems” on page 250
- “Performance Problems” on page 251
- “Port Conflicts” on page 251
- “Domain Logon Problems” on page 251
- “Domain Node is Unavailable” on page 252
- “IME Troubleshooting” on page 252
- “Key Mapping Problems” on page 253
Troubleshooting Tools

Use the Logging features and Trace Utility to narrow down the source of a problem in Reflection X Advantage.

- “Log Files” on page 246
- “Create a Trace” on page 247

Log Files

Messages related to the domain, and messages from X Manager and the Administrative Console are automatically logged. You can send additional information (for example font, keyboard, network activity, X protocol errors, and so on) to the log files on a per-session basis by enabling the options on the session definition Logging tab.

Reflection X log files are created for the following applications and services:

<table>
<thead>
<tr>
<th>Application</th>
<th>Log file</th>
</tr>
</thead>
<tbody>
<tr>
<td>X Manager</td>
<td>xmanager.log</td>
</tr>
<tr>
<td>X Manager for Domains</td>
<td>xmanager.log</td>
</tr>
<tr>
<td>X Administrative Console</td>
<td>xadmin.log</td>
</tr>
<tr>
<td>rxsconfig</td>
<td>rxsconfig.log</td>
</tr>
<tr>
<td>rxmigrate</td>
<td>migration.log</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service</th>
<th>Log file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reflection X Service</td>
<td>rxs.log</td>
</tr>
<tr>
<td>Domain Controller (process of Reflection X Service)</td>
<td>domain.log</td>
</tr>
<tr>
<td>Domain Node (process of Reflection X Service)</td>
<td>node.log</td>
</tr>
<tr>
<td>Remote Session Services (process of Reflection X Service)</td>
<td>node.log</td>
</tr>
</tbody>
</table>

The locations of these log files vary by platform:

Windows Application log files:

%USERPROFILE%\attachmate\rx\logs

Service log files:

%ALLUSERSPROFILE%\attachmate\rx\logs
Create a Trace

While troubleshooting a problem, Micro Focus Technical Support may request that you obtain one or more traces of program actions. After receiving your trace file, Technical Support can replay the trace to replicate the problem.

To create a trace file

1 Under X Clients or XDMCP Connections, select the client you want to troubleshoot. Note the name of the Default session used by this definition. You'll modify this session to create the trace.

2 Under Session Definitions, select the session. On the Advanced tab, select Trace session.

3 Start your client.

4 The Trace Session dialog box opens and you can use it to specify an output filename and location.
   
   If the session will run on the local machine, you see full path information. You can save the trace to the default location shown, or browse to select an alternate location.

   If the session will run on a remote node, the trace file will be saved to that remote system and you see only a filename. (This occurs when Remote Session Services on the session definition's General tab is set to anything other than None.) When no path information is given, the trace file is saved to the Reflection X Advantage program location (typically C:\Program Files\Micro Focus\Reflection on Windows and /opt/rxadvantage on UNIX). You can add path information relative to this location, or specify full path information. In either case, the path specified must be valid and accessible on the remote system.

5 Click Trace session to continue your connection and start recording.

   The trace is saved to the location you specified when the session stops.

6 Return to Advanced tab for your session definition and clear the Trace session checkbox.

7 Upload the trace file as a binary file to http://upload.attachmate.com. If the problem relates to a service request you are currently working on with a technician, include the service request number with the trace and let the technician know when the file is uploaded.
Application Fails to Start

These problems may prevent Reflection X Advantage applications from launching:

- No Java Runtime Environment (JRE) was found
- Database may be in inconsistent state (page 248)
- Insufficient Memory (page 249)

No Java Runtime Environment (JRE) was found

Reflection X Advantage applications require a JRE on your system. On Windows systems, the JRE is included as a separate feature in the installation -- called Java Runtime Environment (JRE). If this feature has not been installed and no additional JRE is available on your system, you see a message saying that the application "failed to start because no Java Runtime Environment was found." To resolve this, install the JRE using the procedure below.

If the JRE feature is not installed and an alternate JRE is found on your system, Reflection X Advantage will start using the alternate JRE, but you will see errors or warning messages in the log files if this JRE is not correctly configured. For information about these messages, see “Changing the JRE” on page 223.

To install the default JRE

1. To open the Programs and Features control panel go to Start > Control Panel > Programs and Features. (On older Windows systems, this Control Panel is called Add or Remove Programs.)
2. Select your Reflection product and click Change.
3. On the Feature Selection tab, click the icon to the left of Java Runtime Environment (JRE) and select Feature will be installed on local hard drive.
4. Click Continue.

Database may be in inconsistent state

Reflection X Advantage applications store data in a database file (flatfiledb-data.xml). During some operations a backup file (flatfiledb-data.xml.bak) is created temporarily. If the backup file is still present in the database folder when you start X Manager, X Manager, or X Administrative Console, you may see a message saying that the "Database may be in inconsistent state" and the application will not start.

To restore the database when a .bak file is present

1. Navigate to the database file location displayed in the error message and locate flatfiledb-data.xml and flatfiledb-data.xml.bak.
2. Create a backup copy of both files in a secure location.
3. Check the dates and sizes of both files.
4. If one file is larger, delete the smaller file and try to start the application. If starting with the larger file doesn't work, replace it with the smaller file from the backup location.
5. If the files are the same size, delete the older file and try to start the application. If starting with the newer file doesn't work, replace it with the older file from the backup location.
Insufficient Memory

When Reflection X Advantage applications start, they request a block of memory from the computer system. If your system's memory is limited or fragmented, you may see an error saying "Application failed to start due to insufficient memory." This is more likely to occur if you have installed the 32-bit version of Reflection X Advantage. If you are running on a 64-bit system and have access to the 64-bit installer, you should install that version. If you are on a 32-bit system, restarting Windows may resolve the problem. If you continue to see this message, you may be able to resolve it by reducing the maximum memory available to the Reflection X Advantage JVM. For details, see Technical Note 2657 (http://support.attachmate.com/techdocs/2657.html).

Display Problems

Use the following topic to troubleshoot color- and display-related problems:

Scattered Desktop Display

When configuring a desktop session using an X client command (for example gnome-session, startkde, or Xsession), your desktop elements appear scattered on your Windows desktop. This can be the result of your session settings. Change your session definition to use Show clients on X terminal desktop.

Color Allocation

You may see one of the following errors if an X client makes an unsuccessful color request, typically because the client wants to create a new color and cannot:

* X Error of failed request: BadAlloc
  Major opcode of failed request: 84 (XAllocColor)

* X Error of failed request: BadAlloc
  Major opcode of failed request: 86 (XAllocColorCells)

* X Error of failed request: BadAlloc
  Major opcode of failed request: 87 (XAllocColorPlanes)

To resolve color allocation errors

* Change the Default Visual Type setting in the session Display tab from a static color model (TrueColor, 24-bit depth) to a dynamic color model (PseudoColor, 8-bit depth).

OpenGL Applications

Many OpenGL applications require a TrueColor visual. On the session Display tab, check the Default Visual Type. If this is set to PseudoColor, 8-bit depth, you'll see colors flashing when 3D graphics are displayed. Configure the session to use a higher color depth to eliminate the flashing. Select either <Best Visual> or TrueColor, 24-bit depth.

TrueColor

If the X client application you are running expects a default visual type that allows the colormap to be changed, you cannot use TrueColor, 24-bit depth as the Default Visual Type. Doing so may prevent the client from starting, and result in an error message.

For example, attempting to run the ico2 client using the following command:

ico2 -faces -dbl -colors gray blue yellow

...results in an error message, as follows:
"Server can't support dynamic colormaps"

-or-

"BadMatch (invalid parameter attribute)"

If you attempt to run the X client `xfishtank` with TrueColor, 24-bit depth selected as the Default Visual Type, the following error message appears:

"Don't know how to format image for display of depth 24"

Some clients do not return an error message. Instead, gray, hatched patterns are displayed in place of the correct colors.

If you are running an X client that exhibits any of these problems, select PseudoColor, 8-bit depth as the Default Visual Type.

NOTE: A Default Visual Type setting of <Best Visual> often results in a setting of TrueColor, 24-bit depth.

Connection Problems

If you are having difficulty connecting to an X client or an XDMCP desktop, review the following tips:

- If you are trying to connect to an X client and see "Client failed to connect to the X server" in the Status bar, the specified Command may not be valid on your host. Try changing the Host type and use the command drop-down list to test with a different sample command. For additional information, click the Information icon to open the Start Client log. Review the log for terminal and X Manager activity messages.

- You may need to configure your firewall for the ports being used by Reflection X Advantage. See “Ports used by Reflection X Advantage” on page 218 for a summary of these ports.

- If you are connecting through a VPN and are having problems using XDMCP to connect to a session, you may be able to resolve the problem by using a distributed session. With this configuration, the client connector that originates the XDMCP request runs on the X application host and the request does not have to travel through the VPN router. (VPN routers typically block XDMCP connection requests.) If you're using X Manager, see “How to Configure a Distributed Session in Standalone Mode” on page 147. If you're using X Manager for Domains, see “Domain Setup: Improve Performance Over a Slow Network” on page 163.

- If your host name resolves to an IPv6 address, try specifying an IPv4 address for the host instead of using the host name.

- If you are having trouble establishing an XDMCP connection, try starting a desktop session without using XDMCP.

- If you have configured X Manager to use remote session services (page 147), the connection to the remote UNIX host uses PAM authentication. On some UNIX systems, the pam_securetty module is configured by default to allow root logins only if the user is logging in on a secure tty. On these systems you cannot log on using root credentials.
Performance Problems

If you're experiencing performance problems with Reflection X Advantage, try the following:

- Review the Session Statistics of a running session to determine if low bandwidth or high latency is a problem in your network. For information about using remote session services to improve performance with X Manager (standalone), see “How to Configure a Distributed Session in Standalone Mode” on page 147. If you're running X Manager for Domains, see “Domain Setup: Improve Performance Over a Slow Network” on page 163.

- On the session definition Display tab, set Backing store to When mapped with save unders. This will reduce network traffic from X clients.

- Monitor sessions from the Domain Status tab on the X Administrative Console to find the source of the problem.

- If you are running in domain mode, configure load balancing to set the load balancing scheme and to ensure that the load is properly balanced among the domain nodes.

Port Conflicts

TCP port 6000 is the standard X11 listening port. Both Reflection X Advantage and Reflection X version 14.0 listen on port 6000 by default. If you are running both products, each product should listen on a different port.

Reflection X Advantage will choose an available port unless Require display number (Session Definition > Advanced) is set. To use a specific display number, set the Require display number option.

Related Topics
- “Ports used by Reflection X Advantage” on page 218

Domain Logon Problems

If you are having trouble logging into a domain from X Manager for Domains or X Administrative Console, check the following:

- Check to see if you entered the correct Reflection X Advantage domain name (not your Windows domain) in the Enter Logon Information dialog box. The Reflection X Advantage domain name is always the name of the computer running the Reflection X Advantage domain controller. Get this information from the Reflection X Advantage domain administrator.

- Ensure that the version of X Manager for Domains running on your workstation is the same or newer than the version running on the domain controller.

- Ensure that the domain controller service is running and that the host is available on your network.

- If you upgraded from version earlier than 5.0 and run in FIPS mode, the certificates used to authenticate domain components need to be upgraded. See “Upgrade Digital Certificates used by Reflection X Advantage Domains” on page 226.
If you are having trouble logging into a domain from the X Administrative Console, check the following:

- You can be locked out of a domain if you forget the administrator password, change authentication methods without adding an administrative account, or experience a problem with the external authentication system. You can unlock the domain without losing your configuration data by using the `rxjsconfig` utility. For details, see “Unlock a Domain” on page 162.

- If you are running on a UNIX system and cannot log in as root, log in using a different account name. On some UNIX systems, the `pam_securetty` module is configured by default to allow root logins only if the user is logging in on a secure tty. On these systems you cannot log onto the Reflection X Advantage domain using root credentials.

**Domain Node is Unavailable**

If a registered domain node appears with a red slash in the X Administrative Console, the node is unavailable. This could be caused by any of the following:

- The domain node host is not running.
- The domain node is running on a Windows computer in "sleep" mode.
- The network connection to the domain node is down.
- The domain node and domain controller are not running the same version of Reflection X Advantage.
- The node was removed from the domain using `rxjsconfig`, but the utility was unable to reach the domain controller to update the list of registered nodes.
- The domain node is running on a system with insufficient memory. See Technical Note 2657 (http://support.attachmate.com/techdocs/2657.html).

**IME Troubleshooting**

Review this information if you’ve configured Reflection X Advantage to use your local Input Method Editor (IME) and you’re still unable to use your IME to enter text into the X client. For additional information, see Technical Note 2504 (http://support.attachmate.com/techdocs/2504.html).

**Logging XIM activity**

Enable XIM logging and review the output log to determine if your X client is XIM-aware and to see if it is configured to use the Reflection X Advantage IME server.

**To log XIM activity**

1. Under **Session Definitions**, select the session you have configured to use native IME support.
2. In the **Session Definition** pane, expand **Logging**, then select **Log XIM activity**.
3. Start your client and attempt to use the local input editor.
4. Review the log information in the appropriate log file (page 246).

**Platform-specific steps for configuring hosts to support use of your local IME**

Use the following platform-specific steps to configure X clients to use the X input method (XIM), which is a requirement for configuring Reflection X Advantage to use your local IME.
Red Hat 5

The Red Hat 5 desktop is configured to use SCIM (Smart Common Input Method), and all GTK (GNOME Toolkit) applications use SCIM by default. To be able to use your local IME with these clients, you need to configure them to use the X Input method (XIM). You can configure clients to use XIM by using a context menu that allows you to change the input method, however the context menu is not available by default. Use the following procedure to enable and use this context menu.

To enable the context menu and configure a client to use the XIM server

1. Start your session
2. Execute the following command to enable the context menu.
   
gconftool-2 --type bool --set '/desktop/gnome/interface/show_input_method_menu' true

   **NOTE:** You need to execute this command only once for each user of the system; doing this will make the context menu available for subsequent sessions.
3. Right-click in the client window.
4. Select X input method from the context menu.

HP CDE

Select a supported language before you log on to your XDMCP session. Supported languages are: ja_JP.UTF-8, ja_JP.EUC-JP, ja_JP, C, en_US.UTF-8, ko_KR.UTF-8, ko_KR

Key Mapping Problems

Pressing Backspace doesn't produce expected behavior

The recommended way to modify the behavior of the Backspace key is to configure the Backspace sends setting on the Keyboard tab for each session definition. (Note that this change is saved to your session definition, not to a keyboard map.) If you also apply a custom keyboard map to your session definition, do not change the mapping of the Backspace key in that map, as any changes you make in your custom map may override your Backspace sends setting preference.

Functionality in the Keyboard Maps dialog box is disabled

The default keyboard map is not editable. In the Keyboard Maps dialog box, Click Clone to create a new editable keyboard map, or use Select Keyboard Map to select a keyboard map that you have already created.

Custom Keyboard Map settings are not taking effect

Select the session definition used by your client, and click the Keyboard tab. Check to see if Keyboard Map is set to use your modified keyboard map.
bandwidth. The rate of transmission of data across the network; the maximum amount of information (Kbits/second or Mbits/second) that can be transmitted along a channel.

cipher. A cipher is an encryption algorithm. The cipher you select determines which mathematical algorithm is used to obscure the data being sent after a successful Secure Shell connection has been established.

client connector. Accepts incoming connection requests from X clients and forwards X protocol requests received from the X client to the protocol router. The client connector also receives X protocol replies, events, and errors from the protocol router and forwards these to the appropriate X client.

color scheme. Color schemes translate string color names requested by clients into RGB (red, green, blue) values.

compressor. Compresses X protocol messages, sends them across the network, decompresses them, and forwards them.

client definition. Contains configuration information for starting one or more X client applications on a host.

controlling X server. The X server in a session that has control of keyboard and mouse input.

definition. A set of related settings used to configure some aspect of a session. Definitions are stored locally or in a domain. Definition types include X Clients, XDMCP Connections, Launch Groups, and Session Definitions.

definition file. Definition files (*.rxd) contain Reflection X Advantage configuration information in XML format. This file format is used to export and import settings to and from Reflection X Advantage.

distributed X session. An X session whose session components are running on more than one computer.

domain. A Reflection X Advantage domain consists of one or more computers on which X session components are run and load-balanced. The domain also defines a group of users who can run and share X sessions on those computers.

domain controller. This term applies to the computer that runs the domain controller software component, and is responsible for:

- Providing a way for domains and their domain nodes to locate each other.
- Giving domains the ability to start or stop session components on various domain nodes.
- Authenticating users before granting access to the domain.
- Centralized storage of settings.

domain node. A computer on which Reflection X Advantage is installed that an administrator has included in a Reflection X Advantage domain.

headless X server. A special type of X server that has no display. It maintains display contents in memory and serves to keep a session "alive" when no other X servers are connected. It can also provide short-circuiting of certain X protocol requests.
IME (Input Method Editor). An input method editor is an application that allows you to enter characters and symbols that are not available on your keyboard.

Internal authentication. A proprietary authentication system that can be used by Reflection X Advantage to grant users access to domain features. If the domain is configured to use internal authentication, Reflection X Advantage maintains an internal database of the user names/passwords that are authorized by the system.

JVM. Java Virtual Machine. A virtual machine that interprets and executes Java bytecode. Because Reflection X Advantage is a Java application, a JVM must exist on every machine that runs Reflection X Advantage.

Keycode. In the X Window System, every individual, physical key is associated with a number in the range 8–255, called its keycode. A keycode only identifies a key, not a particular character or term among the ones that may be printed on the key. (See X keysym.)

Keysym. See X keysym.

Latency. The time delay between when an action is initiated and when its effect is detectable. In a network, a delay in the reception of data packets can be caused by several factors, such as the transmission medium, and the number of network devices between the sending and receiving points. In general, the greater the physical distance between your workstation and your host, the greater the chance of encountering latency.

Passphrase. A passphrase is similar to a password, except it can be a phrase with a series of words, punctuation, numbers, white space, or any string of characters. Passphrases improve security by limiting access to secure objects, such as private keys and/or a key agent.

PKCS. PKCS (Public Key Cryptography Standards) is a set of standards devised and published by RSA laboratories that enable compatibility among public key cryptography implementations. Different PKCS standards identify specifications for particular cryptographic uses. Reflection X Advantage uses the following PKCS standards:

- PKCS#5 is used to provide password-based encryption for private keys stored in the Reflection X Advantage database.
- PKCS#11 provides support for authentication using hardware devices, such as smart cards or USB tokens.
- PKCS#12 is used for storage and transportation of certificates and associated private keys. Files in this format typically use a *.pfx or *.p12 extension.

Private definition. Configuration settings (for an X Client, XDMCP connection, launch group, or session) that can only be viewed and used by the user who created it. A private definition is read-write for the user who created it.

Protocol router. Receives X protocol requests from client connectors and forwards them to all of the X servers in the session. It synchronizes the processing of requests and device events to ensure that all the X servers in the session remain in identical states.

Public definition. Configuration settings (for an X Client, XDMCP connection, launch group, or session) that an administrator has made available to users in a Reflection X Advantage domain. A public definition is read-write for the administrator and read-only for all other users.

Reflection X Service. A service (or daemon) on a computer that can be configured as a domain controller, domain node, and/or support remote session services. (The services supported depend on which features you installed (page 14).)
**remote session.** In a remote session, the Reflection X Advantage session processes (the client connector and protocol router) run on a different computer than X Manager or X Manager for Domains.

**session.** A running session consists of several running components (client connectors, a protocol router, and X servers) whose configuration is determined by the session definition. A running session may or may not have X client applications connected to it, but a session must be running before a client application can be displayed. You can associate a default session definition with each of your X client applications, or configure these definitions to prompt you for a session name when you start the client. If the associated session is not already running, Reflection X Advantage starts the session when you start the client.

**session definition.** A combination of settings that affect how Reflection X Advantage manages and displays your connections. You can associate a default session definition with each of your X clients (including XDMCP connections), or configure these definitions to prompt you for a session name when you start the client. If the associated session is not already running, Reflection X Advantage starts the session when you start the client.

**standalone X session.** An X session whose components are running on a single computer.

**suspended X session.** A running X session that does not have an X server display currently associated with it. When a user leaves a session, its display state is maintained in memory on a member node within the domain.

**X Administrative Console.** X Administrative Console is a management tool for configuring and managing Reflection X Advantage domains. You can use it to control user access to a domain; share client and session definitions; configure load balancing; and monitor sessions.

**X Keysym.** An X Keysym is an encoding of a symbol on the cap of a key. The set of defined X Keysyms includes the ISOLatin character sets, Katakana, Arabic, Cyrillic, Greek, Technical, Publishing, APL, Hebrew, Thai, Korean, and other keys found on keyboards such as Return, Help, and Tab.

A list of X Keysyms is associated with each keycode. The list is intended to convey the set of symbols on the corresponding key. Standard rules for obtaining an X Keysym from a KeyPress event make use of only the first four X Keysyms associated with a keycode. Depending on the state of the Shift and ModeSwitch (AltGr) modifiers, one of the first four keysyms will be selected.

**X Manager.** A Reflection X Advantage tool that allows you to configure and launch X sessions locally, and permits session sharing. It does not use a Reflection X domain; nor does it allow users to leave and rejoin sessions.

**X Manager for Domains.** An application that connects to a Reflection X domain storing session definitions in a database. X sessions run locally, or on domain nodes, which support fault tolerance and protocol compression. It permits session sharing, and allows users to leave and rejoin sessions.

**X server.** The session component that provides a visual display of your X client applications. The controlling X server also manages input devices, such as keyboard and mouse. Each running session includes at least one running X server.

**X server display.** An X server with a visual display or "viewer," as opposed to a headless X server, which has no display.

**XDMCP.** XDMCP (X Display Manager Control Protocol) supports display of a remote desktop on an X server. XDM (the X Window Display Manager) must be configured on the remote host.
**XIM server.** XIM (X Input Method) is an X11 protocol that supports composed character input. The XIM server provided by Reflection X Advantage can obtain composed text from an IME running on the Reflection X Advantage workstation and pass this text to XIM-aware X clients. (Reflection X Advantage does not support passing composed text to other input methods that may be provided by your operating system, such as XIMP and SCIM.)

**Windows user profile folder.** The user profile folder is configurable by the Windows system administrator. The default is:

- Windows 7, Windows Server 2008:
  \Users\username\n
- Windows Server 2003:
  \Documents and Settings\username\n
**font collection.** A set of font files or a reference to a font server. Font collections can be either private or public.

**Windows all users profile folder.** The all user profile folder is configurable by the Windows system administrator. The default is:

- Windows 8, Windows 7, Windows Vista, Windows Server 2008:
  \ProgramData\n
- Windows XP, Windows Server 2003:
  \Documents and Settings\All users\n
**Windows common application data folder.** The application data folder is hidden by default. The default is:

- Windows 8, Windows 7, Windows Vista, Windows Server 2008:
  \ProgramData\n
- Windows XP, Windows Server 2003:
  \Documents and Settings\all users\Application Data\n
**_popup_explaining_domain_mode_only.** This feature is available from X Manager for Domains and the Administrative Console — the applications that are used to operate Reflection X Advantage in Domain mode.

**_popup_explaining_standalone_mode_only.** This feature is available from the X Manager application, which operates Reflection X Advantage in Standalone mode. If you use the X Manager for Domains application, you are operating in Domain mode and this feature is not available.

**_popup_internal_authentication.** A proprietary authentication system that can be used by Reflection X Advantage to grant users access to domain features. If the domain is configured to use internal authentication, Reflection X Advantage maintains an internal database of the user names/passwords that are authorized by the system.

**_popup_definition_of_standalone_mode.** Reflection X Advantage operates in standalone mode by default. You use one application, **X Manager**, and do not have to set up a Reflection X Advantage domain. Use the basic X Manager to access X hosts and clients, configure and share sessions, and monitor session status, all from your own desktop.
**popup - definition of domain mode.** Using Reflection X Advantage in Domain mode gives you access to domain services that support centralized administration of X session definitions, session persistence and backup, and control over authentication services for users participating in the domain. To use these features, an administrator must install Reflection X Advantage as a distributed application on two or more computers, and set up a domain.

To log on and participate in a domain, use the Domain mode applications: X Manager for Domains and the Administrative Console.

**popup_definition_x_atom_element.** "Atom" is a generic term for an element of information in the X Window System. A selection is a type of atom.

**shared save unders definition.** Save unders is a window attribute that instructs the X server to preserve the area under a pop-up window, and repaint it when the pop-up window is closed. This option decreases the network traffic when menus or other pop-up windows are displayed.