Installation Guide
Reflection for the Web
Reflection Security Gateway

Attachmate
Reflection®
Installation Guide
Reflection for the Web 2014 and Reflection Security Gateway 2014

rev.7/1/15

Attachmate
## Contents

Reflection for the Web and Reflection Security Gateway Installation Guide 5

1 Preparing to Install 7
   1.1 Reflection for the Web and Reflection Security Gateway Overview 7
   1.2 System Requirements 10

2 Installing Reflection for the Web and Reflection Security Gateway 13
   2.1 Using the Automated Installer 15
      2.1.1 Automated Installation and Configuration: Checklist and Defaults 15
      2.1.2 Installing and Configuring with Automated Utilities 18
      2.1.3 Using the Automated Installer In Console Mode 22
      2.1.4 Unattended Installation 22
   2.2 Manual Installation Procedures 22
      2.2.1 Applying the JCE Unlimited Strength Jurisdiction Policy Files 23
      2.2.2 Manual Installation: Multi-Component 24
      2.2.3 Installing on Other UNIX platforms 25
      2.2.4 Manual Installation: Individual Components 26
      2.2.5 Manual Installation: Management Server 26
      2.2.6 Manual Installation: Security Proxy 27
      2.2.7 Manual Installation: Metering Server 27
      2.2.8 Manual Installation: ID Manager 28
      2.2.9 Specifying the Location of Configuration Information 28
   2.3 Configuration Tools 29
      2.3.1 Initial Configuration and Configuration Upgrade Utilities 29
      2.3.2 Running the HTTPS Certificate Utility 30
      2.3.3 Running the IIS Integration Utility 31
      2.3.4 Running the Password Change Utility 32

3 Upgrading from a Previous Version 33
   3.1 Upgrading from Reflection for the Web 2014 or Reflection Security Gateway 2014 33
   3.2 Upgrading from Reflection for the Web 2011 33
   3.3 Upgrading from Reflection for the Web 2008 or Earlier 34
      3.3.1 Upgrading from Automatically Installed Versions: Reflection for the Web 2008 or Earlier 36
      3.3.2 Upgrading from Manually Installed Versions: Reflection for the Web 2008 or Earlier 37
   3.4 Additional Upgrade Modifications 40
   3.5 Upgrading Static Sessions 41

4 Starting the Administrative WebStation 43
   4.1 Starting the Servlet Runner 43
   4.2 Servlet Runner Launcher JVM Options 44

5 Configuring Components 45
   5.1 Management Server 45
   5.2 Security Proxy Server 45
Reflection for the Web and Reflection Security Gateway Installation Guide

This document provides steps for installing and configuring Reflection for the Web 2014 and Reflection Security Gateway 2014. It also includes a summary of architecture and system requirements.

This document is available on the Attachmate web site and is also available on the installation image.

If you are running a time-limited edition, the product will be fully functional for 60 days. During that time you can install, configure, and test Reflection for the Web or Reflection Security Gateway. Please contact Attachmate or your authorized reseller to obtain the full-use version of the software.
1 Preparing to Install

For each Reflection component, you can use either the automated installer (page 18) or the archive files to manually install (page 22) the component.

You will use an automated configuration utility as part of the automated install; in many cases, you can use an automated configuration utility after a manual install.

Follow these guidelines when installing:

- The Reflection Management Server must be installed. The Security Proxy Server, when available, is optional.
- Any Reflection for the Web or Reflection Security Gateway component currently running must be shut down before installing or upgrading. (The automated installer will close down components for you if you installed the earlier version with an automated installer.)
- Make sure that you have the necessary permissions to install components on the target server.

If you plan to use X.509 client certificates or secure LDAP access control, make sure the account used to run the Management Server has permission to write to the Java SDK certificate authority certificates file (cacerts). The default location in Windows is:

[MgmtServerInstall]\Attachmate\ReflectionServer\jre\lib\security

1.1 Reflection for the Web and Reflection Security Gateway Overview

Reflection for the Web and Reflection Security Gateway provide authentication, authorization and secure access to enterprise resources. They both deliver secure access to applications on IBM, HP, UNIX, Linux, Unisys, and OpenVMS hosts.

Reflection for the Web provides access to web-based terminal sessions. Reflection Security Gateway provides access to Windows-based terminal sessions. Reflection Security Gateway also provides the ability to secure your system with directory-based authorization, strong authentication, and centrally managed sessions and macros.
Support for either session type can be added to your existing product by using an activation file (page 55).

2. User authenticates to a directory server (LDAP/Active Directory) or other identity management system – optional.
3. Directory server provides user and group identity - optional.
4. Reflection Management Server sends emulation session to the authenticated client.
5. When optional Security Proxy Server is configured for use by a session, emulation applet makes SSL/TLS connection to Security Proxy Server and sends it a signed token.
6. When present, the Security Proxy Server validates session token and establishes a connection to the host:port it specifies.
7. When no Security Proxy Server is present or a session is not configured to use it, authenticated user connects directly to the host.
Management Server

The Reflection Management Server includes the Administrative WebStation and terminal emulation files, which are installed together on a web server computer.

After you install the Reflection Management Server, you can open the Administrative WebStation, which is a self-contained web site. Use the Administrative WebStation to manage and configure web-based terminal sessions. With Reflection for the Web, Java-based applets deploy terminal emulation sessions to your users. With Reflection Security Gateway, you can manage and configure Windows-based terminal sessions. Both options are available in combination by adding an activation file (page 55) to your Reflection product.

Security Proxy Server

If available with your edition of the product, install the optional Security Proxy Server component onto a server computer that will act as a proxy for terminal sessions, routing encrypted network traffic to and from user workstations.

All editions except Limited Editions of the product include the Security Proxy Server. For information on editions, see Technical Note 2321 (http://support.attachmate.com/techdocs/2321.html).

The Security Proxy Server component can be installed to the same server as the Reflection Management Server or on another system.

After installation, some additional configuration of the Security Proxy Server is necessary; see component configuration for the “Security Proxy Server” on page 45 for more information. The Administrative WebStation also contains information about configuring terminal sessions for secure connections.

Metering Server

Use the metering server to monitor use of terminal sessions. If you use the optional metering component, you can choose to install it onto the same web server as the Management Server or on another system.

Before you can meter use of terminal sessions, you must set up the metering server (page 50). The Administrative WebStation also contains information about configuring terminal sessions for metering.

ID Manager

The ID Manager allows you to pool terminal IDs, track ID usage, and manage inactivity timeout values for specific users, thus conserving terminal ID resources and significantly reducing operating expenses.

Configure the ID Manager settings in the ID Manager console and in the Administrative WebStation. See “Setting Up ID Manager” on page 54 for more information.

NOTE: After installation, two ID Manager console options appear in the Start menu under Attachmate Reflection for the Web 2014:

- ID Management Administration – opens with the Server Settings tab selected.
- ID Management Monitoring – opens with the Monitor IDs tab selected.
Utilities

A variety of utilities may be required after you complete the basic installation and configuration steps. See “Configuration Tools” on page 29 for a summary.

1.2 System Requirements

You can install Reflection for the Web or Reflection Security Gateway components on a single computer or on separate computers.

Reflection Management Server Requirements

The Reflection Management Server is platform-independent. It should be run on a server-class operating system. To run the Management Server, you need:

- A servlet engine or application server compliant with Java Servlet 2.3 specification and JSP (page 59) 1.2 such as Apache Tomcat, Oracle WebLogic, IBM WebSphere, or Oracle Java System Application Server.
- A machine running JRE 7 or later.
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

If you use an automated installer or a multi-component archive file to install Reflection Security Gateway or Reflection for the Web, a self-contained JRE and servlet runner are installed, and the JCE Unlimited Strength Jurisdiction Policy Files are applied for you.

NOTE: The JCE Unlimited Strength Jurisdiction Policy Files must be applied when you

- manually install Reflection Security Gateway or Reflection for the Web.
- upgrade your JRE (each time).

See Applying the JCE Unlimited Strength Jurisdiction Policy Files.

Administrative WebStation Requirements

- Any web browser using JRE 7 or later that can run trusted applets and supports JavaScript and cookies.
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

Although the Administrative WebStation is installed on a web server computer, it can run in a browser on any machine.

Reflection Terminal Session Requirements

- A web browser using JRE 7 or later that can run trusted applets. See Technical Note 1383 (http://support.attachmate.com/techdocs/1383.html) for a summary of supported web browsers.
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.
Metering Server and ID Manager Requirements

- Servlet engine or application server compliant with Java Servlet 2.3 specification and JSP 1.2 such as Tomcat, Oracle WebLogic, IBM WebSphere, or Oracle Java System Application Server.
- A machine running JRE 7 or later.
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files.

If you install using the automated installer or a multi-component archive file, a self-contained JRE, a servlet runner, and the JCE unlimited strength policy files are installed for you.

Security Proxy Server Requirements

- A server with JRE 7 or later
- Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files

If you install using the automated installer or a multi-component archive file, a self-contained JRE, a servlet runner, and the JCE unlimited strength policy files are installed for you.

Related Topic

Applying the JCE Unlimited Strength Jurisdiction Policy Files
Installing Reflection for the Web and Reflection Security Gateway

The procedure for installing the various components depends on how you answer these questions:

- Is this the first time you are installing or will you be upgrading from a previous version?
  
  If you are upgrading, first review "Upgrading from a Previous Version" on page 33.

- What operating systems are running on the machines where you want to install?
  
  See Installation Options (page 14).

- What servlet runner do you want to use?
  
  Using the automated installer requires that you run Tomcat, which is provided with the installer.

- How many machines are going to be used?
  
  You must have at least one Management Server. Other components such as the Security Proxy Server, Metering Server, and ID Manager can be installed on the same machine or on different machines.

Automated Installer

Using the automated installer is the simplest way to get up and running. You can use the automated installer on Windows, UNIX, and Linux. The installer installs Tomcat as the servlet runner.

You can also run the installation tool in console mode (page 22) for non-Windows systems, using a command line for input and output rather than a graphical interface.

Manual Installation and Configuration

A multi-component archive file (page 24) that includes the Tomcat servlet runner is available for a variety of platforms. If you install the product with this file, you can still use an automated configuration utility for configuration tasks.

If you choose to use a servlet runner other than the Tomcat servlet runner, or if you cannot run the automated installer for any other reason, you must use archive files to manually install components.

With a manual installation, you must also apply JCE Unlimited Strength Jurisdiction Policy Files. And, these policy files must be applied each time you update your JRE. For details, see Applying the JCE Unlimited Strength Jurisdiction Policy Files.
## Installation Options

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Web Server or Servlet Runner</th>
<th>Recommended Installation Procedure</th>
</tr>
</thead>
</table>
| Linux                 | Tomcat (default)             | **Reflection for the Web:**  
|                       |                              | Use the automated installer rweb<edition>-<version>-prod-linuxia32.sh or rweb<edition>-<version>-prod-linuxx64.sh.  
|                       |                              | **Reflection Security Gateway:**  
|                       |                              | Use the automated installer rsecuritygateway-<version>-prod-linuxia32.sh or rsecuritygateway-<version>-prod-linuxx64.sh.  |
| Windows               | Tomcat (default)             | **Reflection for the Web:**  
|                       |                              | Use the automated installer rweb<edition>-<version>-prod-w32.exe or rweb<edition>-<version>-prod-wx64.exe.  
|                       |                              | **Reflection Security Gateway:**  
|                       |                              | Use the automated installer rsecuritygateway-<version>-prod-w32.exe or rsecuritygateway-<version>-prod-wx64.exe.  |
| Windows with IIS (Internet Information Services) | Tomcat (default) | **Reflection for the Web:**  
|                       |                              | Use the automated installer rweb<edition>-<version>-prod-w32.exe or rweb<edition>-<version>-prod-wx64.exe.  
|                       |                              | **Reflection Security Gateway:**  
|                       |                              | Use the automated installer rsecuritygateway-<version>-prod-w32.exe or rsecuritygateway-<version>-prod-wx64.exe.  |
| Windows, Unix, Linux, or Macintosh | Oracle WebLogic, IBM WebSphere, etc. | Use the manual installation procedure for individual components and configure as a web application following the steps supplied with your servlet runner. |
Examples of automated installer names

- Enterprise edition, Linux, 32 bit
  rwebenterprise-12.<nn>.<build#>-prod-linuxia32.sh
- Enterprise edition, Linux, 64 bit
  rwebenterprise-12.<nn>.<build#>-prod-linuxx64.sh
- Reflection Security Gateway, Windows, 64 bit
  rsecuritygateway-12.<nn>.<build#>-prod-wx64.exe

2.1 Using the Automated Installer

It is recommended that you use the automated installer when one is available for your operating system.

Quick Start Installation

Before deploying Reflection for the Web or Reflection Security Gateway for your site, you can install in a test environment.

For initial testing, you can install on a workstation; however, Attachmate recommends installing on a server operating system for production.

Privilege Requirements

If you install servers on a Windows workstation, the installer must be launched by a user who is an Administrator. Administrators have administrative privileges, but applications run by administrators are run with standard user permissions unless the user specifically authorizes the application to use more elevated privileges. To configure the Start Menu icons to run with administrative privileges, right-click the shortcut and click Properties. On the Compatibility tab, select the Run this program as an administrator check box, and then click OK.

If you are installing on a UNIX/Linux platform, the installer must be launched by a user with root privileges. If you cannot obtain elevated privileges, you may need to use a manual installation process (page 22). If you also require installation of the ReflectionData folder, which stores site-specific Reflection content, to a non-default location (/var/opt/attachmate/reflectiondata), see “Specifying the Location of Configuration Information” on page 28.

2.1.1 Automated Installation and Configuration: Checklist and Defaults

This checklist summarizes the data that you must specify when running the installer and configuration utilities, lists the defaults, and provides a space for you to write your installation entries. Use this list to prepare for installation and keep track of your choices as you install Reflection for the Web or Reflection Security Gateway.

If you're upgrading: It is not necessary to uninstall the previous version of this product before running the automated installer. The automated installer will uninstall the earlier product and migrate user data when it is detected.
# Step 1: Installing

<table>
<thead>
<tr>
<th>Installation Option</th>
<th>Default</th>
<th>Your Installation Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component Selection</td>
<td>Reflection Server, Security Proxy Server</td>
<td></td>
</tr>
</tbody>
</table>
| Destination Directory       | Windows: C:\Program Files\Attachmate\ReflectionServer  
                              | Linux (dynamically determined)  
                              | SUSE Linux: /opt/attachmate/reflectionserver/  
                              | RedHat: /usr/local/bin/attachmate/reflectionserver |
| Start Menu Folder            | Attachmate Reflection for the Web 2014 or Attachmate Reflection Security Gateway 2014 (Windows only) |                         |
| Create shortcuts for all users | No (Windows only)                  |                         |
| Suppress creation of Start Menu folder | No (Windows only) |                         |

## Step 2: Configuration

### Initial Configuration

<table>
<thead>
<tr>
<th>Installation Option</th>
<th>Default</th>
<th>Your Installation Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation directory</td>
<td>Confirm the installation directory</td>
<td></td>
</tr>
</tbody>
</table>
|                              | Windows: C:\Program Files\Attachmate\ReflectionServer  
                              | SUSE Linux: /opt/attachmate/reflectionserver/  
                              | RedHat: /usr/local/bin/attachmate/reflectionserver |
| Services                     | Management service, Metering Service, ID Manager service |                         |
| VPA number                   | no default given                             |                         |
| Servlet runner HTTP port     | 80                                           |                         |
| Servlet runner HTTPS port    | 443                                          |                         |
| Security Proxy port          | 3000                                         |                         |
Installing Reflection for the Web and Reflection Security Gateway

Configuration Upgrade from a Previous Version

<table>
<thead>
<tr>
<th>Installation Option</th>
<th>Default</th>
<th>Your Installation Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Proxy monitor port</td>
<td>8080</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>none provided</td>
<td></td>
</tr>
<tr>
<td>Server name for URLs and Certificates</td>
<td>DNS name of computer on which the Management Server is installed</td>
<td></td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>your department name</td>
<td></td>
</tr>
<tr>
<td>Organization</td>
<td>your company name</td>
<td></td>
</tr>
<tr>
<td>City or locality</td>
<td>your city without abbreviation</td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>your state or province without abbreviation</td>
<td></td>
</tr>
<tr>
<td>Country</td>
<td>two-letter country code</td>
<td></td>
</tr>
</tbody>
</table>

Step 3: Starting Services

Before selecting startup options on a Windows machine, the automated installer detects if IIS is installed on your machine and offers to integrate IIS with Reflection for the Web or Reflection Security Gateway. The default is Yes.

<table>
<thead>
<tr>
<th>Installation Option</th>
<th>Default</th>
<th>Your Installation Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start server components now</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>
2.1.2 Installing and Configuring with Automated Utilities

The automated installer presents these steps with a complete installation of all components. Refer to your checklist as needed.

Step 1: Installation

1. Run the automated installer for your product and operating system.

   On Linux
   In the `/install-automated/` directory, run your product file.
   Reflection for the Web:
   `rweb<edition>-<version>-prod-linuxia32.sh`
   or
   `rweb<edition>-<version>-prod-linuxx64.sh`
   Reflection Security Gateway:
   `rsecuritygateway-<version>-prod-linuxia32.sh`
   or
   `rsecuritygateway-<version>-prod-linuxx64.sh`

   On Windows
   In the `{install-automated\}` directory, double-click the product file for your operating system.
   Reflection for the Web:
   `rweb<edition>-<version>-prod-w32.exe`
   or
   `rweb<edition>-<version>-prod-wx64.exe`
   Reflection Security Gateway:
   `rsecuritygateway-<version>-prod-w32.exe`

---

<table>
<thead>
<tr>
<th>Installation Option</th>
<th>Default</th>
<th>Your Installation Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL for Administrative WebStation</td>
<td><code>http://[management server DNS name] /rweb/AdminStart.html</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>An IP address can be used instead of a DNS name.</td>
<td></td>
</tr>
<tr>
<td>URL for Metering Administration</td>
<td><code>http://[management server DNS name] /rwebmeter/AdminStart.html</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>An IP address can be used instead of a DNS name.</td>
<td></td>
</tr>
<tr>
<td>URL for Metering Reports</td>
<td><code>http://[management server DNS name] /rwebmeter/MeteringReports.html</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>An IP address can be used instead of a DNS name.</td>
<td></td>
</tr>
<tr>
<td>URL for ID Manager Administration and Monitoring</td>
<td><code>http://[management server DNS name]/rwebidm</code></td>
<td></td>
</tr>
</tbody>
</table>
or

rsecuritygateway-<version>-prod-w64.exe

If you use FTP to transfer any of these files to be executed, you must also FTP the .jaw files located in the same directory.

2 Select a language. (This selection determines the language used only during installation. No matter which language you choose for the installation process, support for English, French, German, and Italian is included in the installed product.) Click Next to continue.

3 Read and accept the license agreement.

4 If prompted to run the uninstaller, click OK.

5 Destination directory: Accept the default installation folder, browse to a new directory, or enter the directory where you want to install. It is highly recommended that you do not use the same installation directory as a previous version. This directory should not be accessible to web servers or servlet runners.

   Note: When upgrading, the ReflectionData directory is copied from the previous location; you do not need to re-create your sessions.

6 Select the components to install, and then click Next.

   Reflection Server
   Select this check box to install the Reflection Management Server, which includes the Administrative WebStation and the terminal emulation files. The default servlet runner (Tomcat) is automatically installed. The metering server and the ID Manager are also installed.

   Security Proxy Server
   Select this check box to install the Security Proxy Server, if available with your product.

7 Start Menu Folder: On Windows, select the folder where you would like to create the program shortcuts. You also have the option to create shortcuts for all users, or to suppress the creation of a Start Menu folder.

8 The automated installer copies files to the designated directory.

Step 2: Configuration

The automated installer launches a configuration utility. If you are installing for the first time on this machine, run the Initial Configuration utility. If you are upgrading, run the Configuration Upgrade utility. You can also launch the configuration utilities separately (page 29).

NOTE: Do not close the installer when the configuration utility is launched. You must complete additional steps in the installer after completing configuration.
Initial Configuration

This utility enables the services you select for the Reflection Management Server; creates a ReflectionData directory under which site-specific Reflection content is stored; generates cryptographic keys and self-signed certificates for Tomcat, Reflection servers, and the Security Proxy; configures the Security Proxy if it was installed; sets the administrative password; and sets port values for Tomcat and the security proxy in configuration and HTML files.

1 Installation Directory: Confirm the location where the Reflection Management Server was installed. If the default value is not correct, browse to the correct location. The directory is called ReflectionServer.

2 Reflection Server Services: Select the services you want to enable. You must have a Management Server service running on one machine at your site, but metering and ID management components are optional and can be installed and run on separate machines. To enable the optional components later, use the Configuration Upgrade Utility. (page 29)

3 Volume Purchase Agreement number: Optional. Enter the Volume Purchase Agreement (VPA) number. You can modify the VPA number later in the Administrative WebStation or in the metering configuration pages.

4 Servlet Runner Ports: Accept the default entries or enter the port numbers that the servlet runner will use for HTTP and HTTPS connections. The default port number for HTTP is 80 and the default for HTTPS is 443.

5 Proxy Server Ports: If you chose to install the security proxy, specify the port numbers for the security proxy. The default listening port is 3000. The default monitor port is 8080. You can change security proxy settings after installation using the Security Proxy Wizard.

6 Administration Password: Enter a password. Use this password to open the Administrative WebStation, open the metering configuration pages, view metering reports, and administer ID management. You can create different passwords for each server later.

7 Server Names for URLs and Certificates: The certificate information that you enter on this and the following panel enable you to create self-signed certificates that will be used to make secure SSL connections to the Reflection Management Server and Security Proxy after installation. Enter a DNS name or IP address. The current DNS name is provided if available. If you want to change the servlet runner certificate later, use the HTTPS Certificate Utility (page 30).

8 Server certificates: organization and locality

The Server Certificates: organization and locality panel includes additional information for creating certificates.

Organizational Unit: Enter the name of your organizational unit. This is usually your department or division.

Organization: Enter the name of your organization, typically the legal name of your organization or company.

City or Locality: Enter your city without abbreviation.

State: Enter the full name of your state without abbreviation.

Country: Provide a two-letter ISO country code.

9 Confirm Configuration: Click Next to make the specified configuration changes.

10 Configuration summary: A summary of the configuration changes is created in configutil.log in the installation directory. Click Done to continue to Step 3: Start Services, below.
Configuration Upgrade

This utility enables the services for this Reflection Management Server, copies the Tomcat keystore from the previous location to the new location if necessary, copies the ReflectionData directory from the previous default location to the new default location (if a custom location was not configured), copies security proxy server configuration files from the old install directory to the new install directory, and updates port values in configuration and HTML files.

NOTE: The panels described below are not all displayed when upgrading to an installation that has only the proxy server.

1 Select your language.

2 Installation Directory: Confirm the location where the new version of the Reflection Server was installed. If the default value is not correct, browse to the correct location.

Previous Installation Directory: Confirm the location where the Reflection Server was installed. If the default value is not correct, browse to the correct location.

3 Services: Select the services you want to enable. You must have a Management Server service running, but metering, ID management, and the security proxy components can be installed and run on separate machines.

4 Servlet Runner Ports: Accept the default entries or enter the port numbers that the servlet runner will use for HTTP and HTTPS connections. The default port number for HTTP is 80; and the default for HTTPS is 443.

5 Server Name: The server name displayed is the basis for the URLs for starting components of Reflection. This is based on the name that you provided when creating self-signed certificates. If the self-signed certificates are not available, then the current DNS name is provided, if available. The entry should be in the format of a DNS name or IP address. If you want to change the servlet runner certificate later, use the HTTPS Certificate Utility (page 30).

6 Confirm Configuration: Click Next to make the specified configuration changes.

7 Configuration Summary: A summary of the configuration changes, configutil.log in the installation directory, is created. Click Done to continue to Step 3: Start Services, below.

Step 3: Start Services

After completing configuration, you return to the installer to select startup options and review the URLs for all enabled components.

The automated installer detects if IIS is installed on your machine and offers to integrate IIS with the product. You can also run the IIS Integration Utility (page 31) later to integrate or unintegrate with IIS.

1 Start Services: You can choose to start the server components now. If you do not start the server components at this time, you can later start them manually using the procedures for “Starting the Servlet Runner” on page 43 and “Running the Security Proxy” on page 49.

2 Installation Complete: A series of URLs for all the enabled components is provided.

After installing the Management Server, you can run the Administrative WebStation from any computer with a web browser. Go to the URL specified on the automated installer panel, which is in the form below. The URL will include a port number if it is other than 80, the default.

http://[server name]/rweb/AdminStart.html

If you installed the product on a Windows computer, you can also open the Administrative WebStation via the Start menu. Go to Start > All Programs > Attachmate Reflection for the Web or Attachmate Reflection Security Gateway > Administrative WebStation.
2.1.3 Using the Automated Installer In Console Mode

The options provided in the automated installer are available in console mode for non-Windows systems, using a command line for input and output rather than a graphical interface. All screens present their information on the console and allow you to enter the same information as in the automated installer. This option is useful if you want to run the automated installer on a headless or remote server.

Run the automated installer executable appropriate for your platform with a -c parameter.

You can also run the Initial Configuration Utility and the Configuration Upgrade Utility (page 29) in console mode.

2.1.4 Unattended Installation

Reflection for the Web and Reflection Security Gateway installations are based on install4j technology, which supports unattended mode. Unattended installation enables you to install the product the same way on a series of computers.

**NOTE:** The Reflection Configuration Utilities do not support an unattended mode. These utilities run with a graphical user interface (or in an attended console mode). For more information, see “Initial Configuration and Configuration Upgrade Utilities” on page 29, which are optional for many upgrade scenarios.

1. Install Reflection for the Web or Reflection Security Gateway on a machine using the automated installer. You can use the graphical interface or console mode (-c) to install the product.

   The installation process creates a text file, response.varfile, that contains the selected installation options.

2. Copy response.varfile to another machine where you would like to install Reflection for the Web or Reflection Security Gateway. On the original machine, response.varfile is located here:

   \[ReflectionServerInstall\].install4j

3. Locate the appropriate executable (see “Installing and Configuring with Automated Utilities” on page 18) to install the product. Launch the installation program using the -q argument and a -varfile argument that specifies the location of response.varfile.

For example, to install the Airlines Printer edition of Reflection for the Web on a 32-bit Linux platform with a response.varfile located in the same directory, use this command, where <nn.n.nnn> is the product version and build number:

```
rwebairlinesprinting-<nn.n.nnn>-prod-linuxia32.sh  -q -varfile response.varfile
```

You could also add the –c option to install in console mode, which would provide feedback such as "Extracting Files" and "Finishing Installation."

2.2 Manual Installation Procedures

Use the compressed archive files to manually install any needed components for your platform (located in the install_manual/components directory) if any of the following is true:

- You want to use a servlet runner other than the one automatically installed with the product (Tomcat).
You are installing on a platform for which an automated installer is not supported.
You cannot run the automated installer for any other reason.

You have several options for manual installation:

- **Manually Installing a Multi-Component Archive File**
  If you can use Tomcat as the servlet runner, use a multi-component archive file that is appropriate for your platform.

- **Manually Installing Components on Other UNIX Platforms**
  You can use a multi-component archive file that requires a version of the Java runtime environment other than the one provided by the installer.

- **Manually Installing Individual Components**
  Archive files for installing individual components are provided for installing on systems with a non-Tomcat servlet runner.

**Extracting Files**

**How to extract archive file contents**

To install a component manually, use the appropriate tool (for example, WinZip) to extract the contents. If you have the Java jar tool (part of the JDK) on the computer where you are installing the component, you can use the following jar command to extract the contents:

```
jar xf <archive file name>
```

**Using FTP**

If you are extracting the contents of an archive file to your local machine and then transferring the files to a server using FTP, make sure your FTP utility preserves the capitalization of the file names. Otherwise, Reflection components may not function correctly.

### 2.2.1 Applying the JCE Unlimited Strength Jurisdiction Policy Files

Reflection Security Gateway 2014 R2 and Reflection for the Web 2014 R2 require the Java Cryptography Extension (JCE) Unlimited Strength Policy Files. "Unlimited strength" policy files contain no restrictions on cryptographic strengths, in contrast to the "strong" but limited cryptography policy files bundled in a JRE.

When you use an automated installer to install Reflection Security Gateway or Reflection for the Web, the JCE Unlimited strength policy files are applied for you.

The JCE Unlimited Strength Jurisdiction Policy Files must be applied when you

- manually install Reflection Security Gateway or Reflection for the Web.
- upgrade your JRE (each time).

To apply the policy files:

1. Download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files from Oracle or IBM.

   Be sure to download the correct policy file updates for your version of Java:
Java 7 or 8: http://www.oracle.com/technetwork/java/javase/downloads/index.html


2. Uncompress and extract the downloaded file. The download includes a Readme.txt and two .jar files with the same names as the existing policy files.

3. Locate the two existing policy files:
   - local_policy.jar
   - US_export_policy.jar
   
   **On UNIX**, look in `<java-home>/lib/security/`
   
   **On Windows**, look in `C:/Program Files/Java/jre<version>/lib/security/`

4. Replace the existing policy files with the unlimited strength policy files you extracted.

### 2.2.2 Manual Installation: Multi-Component

If you plan to use Tomcat, the servlet runner included with the product, but you cannot use the automated installer, you should use the multi-component archive file that contains all necessary components. The archive file includes the following:

- Reflection Management Server
- Metering Server
- ID Manager
- Security Proxy Server
- Tomcat servlet runner
- The JRE for the appropriate platform

<table>
<thead>
<tr>
<th>Archive File</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reflection for the Web:</strong>&lt;br&gt;rweb&lt;edition&gt;-prod-w32-manual.zip</td>
<td>Multi-component zip file for Windows 32-bit systems</td>
</tr>
<tr>
<td><strong>Reflection Security Gateway:</strong>&lt;br&gt;rsecuritygateway-prod-w32-manual.zip</td>
<td>Multi-component zip file for Windows 32-bit systems</td>
</tr>
<tr>
<td><strong>Reflection for the Web:</strong>&lt;br&gt;rweb&lt;edition&gt;-prod-wx64-manual.zip</td>
<td>Multi-component zip file for Windows 64-bit systems</td>
</tr>
<tr>
<td><strong>Reflection Security Gateway:</strong>&lt;br&gt;rsecuritygateway-prod-wx64-manual.zip</td>
<td>Multi-component zip file for Windows 64-bit systems</td>
</tr>
<tr>
<td><strong>Reflection for the Web:</strong>&lt;br&gt;rweb&lt;edition&gt;-prod-linuxia32-manual.tar.gz</td>
<td>Multi-component archive file for Linux 32-bit systems</td>
</tr>
<tr>
<td><strong>Reflection Security Gateway:</strong>&lt;br&gt;rsecuritygateway-prod-linuxia32-manual.tar.gz</td>
<td>Multi-component archive file for Linux 32-bit systems</td>
</tr>
<tr>
<td><strong>Reflection for the Web:</strong>&lt;br&gt;rweb&lt;edition&gt;-prod-linuxx64-manual.tar.gz</td>
<td>Multi-component archive file for Linux 64-bit systems</td>
</tr>
<tr>
<td><strong>Reflection Security Gateway:</strong>&lt;br&gt;rsecuritygateway-prod-linuxx64-manual.tar.gz</td>
<td>Multi-component archive file for Linux 64-bit systems</td>
</tr>
</tbody>
</table>
Extract the files; then run the appropriate automated configuration utility (page 29). If you are upgrading (page 37), run the Configuration Upgrade Utility after extracting the files. For a new installation, run the Initial Configuration utility.

If you are planning to run individual components on multiple systems, you can use the archive file for the appropriate platform in all instances. After extracting the files, use a configuration utility to configure the components for each system. If you cannot run the configuration utility after extracting the files, you can complete the configuration manually. For example, you can disable the metering server and the ID Manager by simply deleting the folders for those components.

After you have installed the Management Server and completed this part of the configuration, you can start the servlet runner and run the Administrative WebStation (page 43). To configure the Security Proxy Server, generate or import a Management Server security certificate (page 46).

### 2.2.3 Installing on Other UNIX platforms

The following installation files are available with the product to support platforms that require a version of a Java runtime environment other than the one provided by the installer. Platforms that may use these files include z/OS, Mac, HP-UX, and other Linux systems.

**Automated installer**

This example shows the Enterprise edition of Reflection for the Web:

rwebenterprise-12.1.<build number>-prod-unix-nojre.sh

**Manual installer**

rwebenterprise-prod-unix-nojre-manual.tar.gz

**Manual Installer for Security Proxy only**

rwebproxy-prod-unix-nojre-manual.tar.gz

**Procedure for Installing with no JRE**

1. To use any of these -nojre- installation packages, confirm that a Java runtime environment appropriate for your platform is already installed. For example, to install Reflection Security Gateway or Reflection for the Web on a z/Linux machine, download the JRE from this location: http://www.ibm.com/developerworks/java/jdk/linux/download.html (http://www.ibm.com/developerworks/java/jdk/linux/download.html)

2. Expand the package you want to use (Automated Installer, Manual Installer, Manual Installer for Security Proxy only). The guidelines described for full multi-component install options (page 24) also apply here; however, these packages do not include a JRE so that the Java version installed on your platform can be used during installation.

   **Note:** Your JRE must be Java version 7 or higher.

3. Be sure that the JCE Unlimited Strength Jurisdiction Policy Files are applied, and apply them each time you upgrade your JRE. See Applying the JCE Unlimited Strength Jurisdiction Policy Files.
2.2.4 Manual Installation: Individual Components

If you are using a non-Tomcat servlet runner, check the following before you extract the individual component files:

- **A JRE must be installed on your computer.**
  
  If you do not already have one, download the latest JRE (http://www.oracle.com/technetwork/java/javase/downloads/index.html) from the Oracle web site. You should download a version of the JRE that includes the server JVM. The JRE that is provided with the JDK (page 59) includes the server JVM.

- **The JCE Unlimited Strength Jurisdiction Policy Files must be applied.** See Applying the JCE Unlimited Strength Jurisdiction Policy Files.

- **The computer must have a servlet runner.**
  
  The Management Server, Metering Server, and ID Manager must be installed as servlets within a servlet runner. Follow the installation information in the documentation for that servlet runner on where to install web applications and what settings to configure.

The following archive files for individual components are provided for installing on systems with a non-Tomcat servlet runner:

<table>
<thead>
<tr>
<th>Archive File</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>rweb.war</td>
<td>Reflection Management Server (page 26) (Emulation &amp; Administration)</td>
</tr>
<tr>
<td>rwebmeter.war</td>
<td>Metering Server (page 27)</td>
</tr>
<tr>
<td>rwebidm.war</td>
<td>ID Manager (page 28)</td>
</tr>
<tr>
<td>idmutils.zip</td>
<td>A zip file containing sample database script templates with examples of ID attributes and pool types for the &quot;ID Manager&quot; on page 54</td>
</tr>
</tbody>
</table>

There is an additional set of archive files for installing the Security Proxy Server (page 27) on a separate machine.

Some editions include components for features that are not supported in that particular edition. For example, the Security Proxy is not supported in the Reflection for the Web Limited Edition although the files are present.

If you need to download a version of Tomcat other than the one included with the product, it is available from apache.org (http://tomcat.apache.org).

2.2.5 Manual Installation: Management Server

If you are using a servlet runner other than Tomcat, you must install the Management Server as an individual component. Use rweb.war for your platform (located in the install_manual directory) to install the Management Server.

**Installing rweb.war**

Create an rweb directory and extract rweb.war into the rweb directory. Follow the installation information in the documentation for your servlet runner on where to install web applications and what settings to configure.
Configuring the Management Server

It is recommended that you use the default location for the ReflectionData directory. If you need to use a different location, see “Specifying the Location of Configuration Information” on page 28.

SSL port: If your servlet runner is using a non-default SSL port, you must manually change the Management Server's PropertyDS.xml entry to match the SSL port of the servlet runner. (Reflection uses port 443 for an HTTPS connection.) To do so:

1. Start the Reflection Management Server (with defaults) to generate the PropertyDS.xml file.
   Note: If there is a port conflict, the management server may fail to start or function correctly.
2. Open PropertyDS.xml in the ReflectionData directory.
3. In the following line, change the value from 443 to the appropriate port number:

   ```
   <CORE_PROPERTY NAME="sslport">
   <STRING>443</STRING>
   ```
4. Restart the Management Server, with the correct port.

2.2.6 Manual Installation: Security Proxy

You can install the Security Proxy Server as an individual component using an archive file for the appropriate platform. The archive file is appropriate whether or not you are using Tomcat as the servlet runner for the Reflection Management Server. The archive files are located in the \install_manual\ directory.

Installing the rwebproxy archive file

1. Locate the rwebproxy archive file in the \install_manual\ directory.

<table>
<thead>
<tr>
<th>FILE NAME</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rwebproxy-prod-linuxia32-manual.tar.gz</td>
<td>Archive file for the security proxy server for a Linux 32-bit system</td>
</tr>
<tr>
<td>rwebproxy-prod-linuxx64-manual.tar.gz</td>
<td>Archive file for the security proxy server for a Linux 64-bit system</td>
</tr>
<tr>
<td>rwebproxy-prod-w32-manual.zip</td>
<td>Archive file for the security proxy server for a Windows 32-bit system</td>
</tr>
<tr>
<td>rwebproxy-prod-wx64-manual.zip</td>
<td>Archive file for the security proxy server for a Linux 64-bit system</td>
</tr>
</tbody>
</table>

2. Extract the file into any directory. The default path in automated installations is as follows: \[MgmtServerInstall]\securityproxy\ 

After you install the security proxy server, generate or import a Management Server security certificate (page 46) and start the Security Proxy Server (page 49).

2.2.7 Manual Installation: Metering Server

When you use a servlet runner other than Tomcat, you must install the metering server as an individual component. The metering server must run as a servlet within a servlet runner. Use rwebmeter.war for your platform (located in the \install_manual\components directory) to install the metering server.
Installing rwebmeter.war

Create an rwebmeter directory within the appropriate directory, and extract rwebmeter.war into the rwebmeter directory. Follow the installation information in the documentation for your servlet runner on where to install web applications and what settings to configure.

After you install the metering server and complete this initial configuration, confirm that the servlet runner has started. See Setting Up Metering (page 50).

You can edit the web.xml file to specify the location of the ReflectionData directory, but it is not necessary if the ReflectionData directory is in the default location. See “Specifying the Location of Configuration Information” on page 28 for instructions.

2.2.8 Manual Installation: ID Manager

If you are using a servlet runner other than Tomcat, you must install the ID Manager as an individual component. The ID Manager must run as a servlet within a servlet runner. Use rwebidm.war for your platform (located in the install_manual\components directory) to install the ID Manager.

It is recommended that you install the ID Manager on a separate machine from the Reflection Management Server when you are running ID management in a high traffic production environment.

Installing rwebidm.war

Create an rwebidm directory within the appropriate directory, and extract rwebidm.war into the rwebidm directory. Follow the installation information in the documentation for your servlet runner on where to install web applications and what settings to configure.

After you install the ID Manager, confirm that the servlet runner has started. See “Setting Up ID Manager” on page 54.

You can edit the web.xml file to specify the location of the ReflectionData directory, but it is not necessary if the ReflectionData directory is in the default location. See “Specifying the Location of Configuration Information” on page 28 for instructions.

Installing idmutils.zip

This zip file, located in the \install_manual\components directory, contains sample database script templates with examples of ID attributes and pool types. Unzip this file into [MgmtServerInstall]\utilities\idmutils.

After completing these steps, see “Setting Up ID Manager” on page 54.

2.2.9 Specifying the Location of Configuration Information

ReflectionData is the root directory under which site-specific Reflection content is stored, including server configuration files, keystores, emulator session information, and more.

This folder is created automatically; there are no additional steps required for installation. If you have a special circumstance that requires a non-default location for ReflectionData, you can edit the web.xml file (instructions below) to specify the location of the ReflectionData directory.

Here are the default locations for ReflectionData, by operating system.

- On Windows Server 2012 and Windows Server 2008:
Installing Reflection for the Web and Reflection Security Gateway

If you need to specify the location of ReflectionData, edit the web.xml file as follows:

1. Open the web.xml file in a text editor, such as Notepad. For Tomcat, web.xml is within the
   ReflectionServer directory for each component:
   reflectionserver/apache-tomcat/webapps/rweb/WEB-INF/web.xml
   reflectionserver/apache-tomcat/webapps/rwebidm/WEB-INF/web.xml
   reflectionserver/apache-tomcat/webapps/rwebmeter/WEB-INF/web.xml

2. In the web.xml file, replace the value for rwebdata_location_placeholder with the location and
   name of the directory you define. For example:
   
   `<context-param>
   <param-name>ReflectionData</param-name>
   <param-value>/var/opt/attachmate/reflectionserver/reflectiondata</param-value>
   </context-param>

3. Save your changes and restart the servlet runner (page 43).

2.3 Configuration Tools

Prior to starting the Administrative WebStation, additional configuration steps may be required. These
are particularly useful for those who install the product using the manual installation procedure, but
they can be used regardless of the way you installed.

- “Initial Configuration and Configuration Upgrade Utilities” on page 29
- Set up certificates using the HTTPS Certificate Utility (page 30)
- Integrate with IIS on a Windows machine (page 31)
- Set up or change passwords (page 32)

2.3.1 Initial Configuration and Configuration Upgrade Utilities

These utilities require that Reflection was installed using either the automated installer or the multi-
component archive file (page 24).

You do not need to run these utilities separately if you ran the automated installer and linked to a
configuration utility as part of the installation and configuration process. For a summary of the
questions you will answer in these utilities, see “Installing and Configuring with Automated Utilities” on
page 18.

After installation, these utilities are located as listed below. Use -c to launch these utilities in console
mode.

Windows systems

[MgmtServerInstall]\utilities\bin\InitialConfigurationUtility.exe

and
You must have administrator privileges to run these utilities. If User Access Control is enabled and you run the utilities as a user who does not have administrative privileges, then you will be prompted to provide the credentials of a user with administrative rights. This prompt does not appear if you run the utilities when using the Administrator account.

Linux and UNIX systems

Initial Configuration Utility

This utility enables the services you select for the Reflection Server; creates a ReflectionData directory under which site-specific Reflection content is stored; generates cryptographic keys and self-signed certificates for Tomcat, the Reflection servers, and the Security Proxy; configures the Security Proxy if it was installed; sets the administrative password; and sets port values for Tomcat and the Security Proxy in configuration and HTML files.

Configuration Upgrade Utility

This utility enables the services for this Reflection Management Server, copies the Tomcat keystore from the previous location to the new location if necessary, copies the ReflectionData directory from the previous default location to the new default location (if a custom location was not configured), copies security proxy server configuration files from the old install directory to the new install directory, and updates port values in configuration and HTML files.

See the information in “Upgrading from a Previous Version” on page 33 for more information.

2.3.2 Running the HTTPS Certificate Utility

Use the HTTPS Certificate Utility to import a CA-signed certificate, create a new self-signed certificate, or copy the certificate used by the management server.

The HTTPS Certificate Utility requires that

- the product was installed using either the automated installer or the multi-component manual installation image.
- you use the HTTP Server functionality that is provided during installation.

The HTTPS Certificate Utility can be run at any time to manage the servlet runner certificate. Alternatively, you can also run the initial configuration utility to generate cryptographic keys and self-signed certificates for the provided servlet runner. Use of either utility will overwrite any existing keys.

You can configure Reflection to use either a self-signed certificate, or a CA-signed SSL server certificate. For details regarding Tomcat and CA-signed certificates, see Technical Note 1702 (http://support.attachmate.com/techdocs/1702.html).

Run HttpsCertificateUtility.exe (Windows) or HttpsCertificateUtility (Linux and UNIX) from this location:

- Windows 2012 or Windows 8: Start screen
Windows 2008 or Windows 7: Start > All Programs > Attachmate Reflection for the Web or Attachmate Reflection Security Gateway > HTTPS Certificate Utility

Linux/UNIX: [management server installation path]/utilities/bin

Follow the prompts in the utility to generate a new key pair and self-signed certificate, to import a CA-signed certificate and private key, or to copy the certificate and private key used by the Management Server.

**NOTE:** When needed, the HTTPS Certificate Utility can be run in console mode by using the -console application argument.

### Requiring HTTPS

Once your server supports HTTPS, use the Administrative WebStation (page 43) to restrict Reflection to the HTTPS protocol.

1. Choose **Security Setup** on the navigation bar or home page.
2. Choose the **Security** tab.
3. In the **Management server access protocol** section, select the **Require HTTPS - recommended** check box.
4. Click **Save Settings**.

#### 2.3.3 Running the IIS Integration Utility

If Microsoft Internet Information Service (IIS) is installed on your computer, the automated installer detects IIS and asks if you want to integrate your installation with IIS. You will see this question even if you are upgrading from a previous version that was already integrated with IIS.

- You can also run the IIS Integration Utility independently if you do not choose to integrate while installing the product.
- Running a configuration utility (initial configuration or configuration upgrade) after you install and configure the product may affect the integration with IIS that was performed previously. If you see this condition, you must reintegrate with IIS.

Use the IIS Integration Utility to remove the existing integration and perform IIS integration again. Follow the steps below to Integrate with IIS.

#### Reasons to Integrate Reflection for the Web or Reflection Security Gateway with IIS

By default, the Apache Tomcat web server is installed, so you do not need to integrate the product with IIS. However, you may choose to integrate Reflection for the Web or Reflection Security Gateway with IIS to be able to

- take advantage of the IIS Single Sign-on (SSO) functionality.
- use your existing web server certificates on IIS.
NOTE: When Reflection is integrated with the IIS web server, Reflection uses IIS and the IIS-configured server certificate for HTTPS communication. The Apache Tomcat certificate is ignored. Although the Tomcat certificate is not used after IIS integration, it is recommended that you do not delete this certificate. Once integrated with IIS, the expiration status of the Tomcat certificate does not affect the Reflection installation.

To integrate with IIS:

1 Run the IIS Integration Utility located in the \ReflectionServer\utilities\bin folder.
   If you are integrating with IIS 7 or IIS 8, use IIS7IntegrationUtility.exe.
   If you are integrating with IIS 6, use IIS6IntegrationUtility.exe. A list of all web sites managed by IIS will be listed.

2 To integrate IIS with Reflection for the Web or Reflection Security Gateway, select a site and click the Integrate button.

3 If you are prompted, confirm the installation directory (for example, C:\Program Files\Attachmate\ReflectionServer) and click Yes.

4 If you are prompted to install required IIS role services, click Yes. Installation of role services can take a few minutes.

5 If you are prompted to restart the Attachmate Reflection Server service, click Yes.

6 On the Integration Completed message box, click Yes to exit.

7 Restart the Reflection Management Server. (This step is not necessary if you are running the IIS 7 integration utility and you selected the option to restart the Reflection service.)
   - If you installed the product as a Windows service, go to Control Panel > Administrative Tools > Services > Attachmate Reflection Server. Stop and restart the service.
   - You can also use the -stop and -start commands (page 43) with ReflectionServer.exe.

8 Confirm that integration was successful by browsing to http://<serverName>[;port]/rweb/AdminStart.html where <serverName> is the IP address or alias of your Microsoft Windows machine running the Reflection Management Server, for example: http://myserver.mycompany.com/rweb/AdminStart.html

To change your settings or remove the integration, run the IIS integration utility again.

2.3.4 Running the Password Change Utility

Each time you log on to Reflection for the Web or Reflection Security Gateway as an administrator, you enter a password. If you lose or need to set the administrative password, use the password change utility to modify the administrative password without needing to log in to the Administrative WebStation.

On a Windows system, select Password Change Utility from the Start menu. You can also run the utility from this location: [MgmtServerInstall]\utilities\bin\PasswordChangeUtility.exe

On a UNIX or Linux system, run from this location:
[MgmtServerInstall]\utilities\bin\PasswordChangeUtility
3 Upgrading from a Previous Version

If an earlier version of Reflection for the Web or Reflection Security Gateway is installed on your local computers and servers, follow the instructions for the version from which you are upgrading.

To prepare for your upgrade, refer to the appropriate section:
- from an earlier version of Reflection for the Web 2014 (page 33)
- from an earlier version of Reflection Security Gateway 2014 (page 33)
- from Reflection for the Web 2011 (page 33)
- from Reflection for the Web 2008 or Earlier (page 34)

3.1 Upgrading from Reflection for the Web 2014 or Reflection Security Gateway 2014

To apply a service pack or hotfix, use the automated installer, when available.

The automated setup program will install the latest software and retain your current settings. You do not need to run a configuration upgrade utility as a separate step.

For a manual installation
- If you installed the product using a multi-component installer, you can use the same approach again. If you can use the Tomcat servlet runner included with the product, extract the multi-component archive file (page 24) appropriate for your platform, and then run the configuration upgrade utility to handle the upgrade of your settings.
- Make sure the earlier version of the software is not running when you run the configuration utility. This will avoid potential port conflicts and allow you to accept default port assignments.
- If you are upgrading a Linux or UNIX system, make sure no startup scripts are running.

3.2 Upgrading from Reflection for the Web 2011

Use the installation program to upgrade your copy of Reflection for the Web 2011. The setup program will install the latest software and will retain your current settings. You do not need to run a configuration upgrade utility as a separate step.

Upgrading from an automatically installed version of Reflection for the Web
- Upgrades for versions of Reflection for the Web 2011 that were installed with the automated installer require no additional steps.
If you use SiteMinder for Access Control and you are upgrading from a version of Reflection for the Web 2011 Hot Fix 5 or earlier, you must copy the SiteMinder Java Agent JAR file from your SiteMinder distribution media to the Reflection Management Server’s `lib` directory and restart the Tomcat servlet runner after the upgrade is complete. See Technical Note 2591 (http://support.attachmate.com/techdocs/2591.html) for details.

See “Additional Upgrade Modifications” on page 40 for other changes that may apply.

If you need to perform a manual installation

- If you installed using a multi-component installer, you can use the same approach again. If you can use the Tomcat servlet runner included with the product, extract the multi-component archive file (page 24) appropriate for your platform, and then run the configuration upgrade utility to handle the upgrade of your settings.

- Make sure the earlier version of the software is not running when you run the configuration utility. This will avoid potential port conflicts and allow you to accept default port assignments. If you are upgrading a Linux or UNIX system, make sure no startup scripts are running.

- If your Reflection for the Web 2011 installation still has the paths associated with an earlier version such as Reflection for the Web 2008 or earlier, follow the guidelines in “Upgrading from Reflection for the Web 2008 or Earlier” on page 34.

See “Additional Upgrade Modifications” on page 40 for other changes that may apply.

3.3 Upgrading from Reflection for the Web 2008 or Earlier

Additional steps are required to install Reflection for the Web 2014 or Reflection Security Gateway 2014 if your current version of the product is Reflection for the Web 2008 or earlier. Follow the guidelines in this chapter to perform this kind of upgrade.

The procedure below assumes a version of Reflection for the Web 2008 or Reflection for the Web 9.x.

Upgrade Scenarios

- Was the previous version of the product installed using an automated installer?

  Use the automated installer to install this version. The configuration upgrade utility will make most of the changes necessary for the upgrade.

- Was the previous version of the product installed manually?

  The automated installer is available on a wider variety of platforms than previous versions. It is recommended that you install using the automated installer and then run the configuration upgrade utility if one is available for your platform.

  After stopping services for the previous version, install the new version in a different target directory (accept the default provided) rather than using the directory of the previous version.

- If you can use Tomcat as the servlet runner and you want to install manually, extract the multi-component archive file (page 24) appropriate for your platform, and then run the configuration upgrade utility to handle the upgrade of many of your settings. It is recommended that you install the new version in a different target directory rather than using the directory of the previous version.

- Do you need to run a non-Tomcat servlet runner, or have a highly customized environment that was installed manually? You can still install manually and modify the files directly to upgrade your configuration settings.
In all cases, be sure you have copies of ReflectionData, cacerts, and server.xml.

**NOTE:** If you use SiteMinder for Access Control and you are performing an upgrade, you must copy the SiteMinder Java Agent JAR to the Reflection Management Server’s `lib` directory and restart the Tomcat servlet runner after the upgrade is complete. See Technical Note 2591 (http://support.attachmate.com/techdocs/2591.html) for details.

## Comparing Installation Defaults

As of Reflection for the Web 2011, several default locations have changed from previous releases, and the automated installer’s default directory structure also differs from previous releases. If you use the automatic installer, the upgrade utility will make the appropriate modifications.

- **Installation Target**
  
  The installation target for Reflection for the Web 2014 is as follows:

  **Windows:**
  
  C:\Program Files\Attachmate\ReflectionServer

  **SUSE Linux:**
  
  /opt/attachmate/reflectionserver/

  **RedHat:**
  
  /usr/local/bin/attachmate/reflectionserver

  Releases prior to 2011 did not include Attachmate in the path.

- **Tomcat Location**
  
  The path for the Tomcat server is `apache-tomcat`. Previous releases used `jakarta-tomcat`.

- **ReflectionData**
  
  The default location of ReflectionData is as follows:

  - On Windows 2003, the default location for ReflectionData is
    C:\Documents and Settings\All Users\Application Data\Attachmate\ReflectionServer\ReflectionData

  - On other supported Windows systems, the default location for ReflectionData is
    C:\ProgramData\Attachmate\ReflectionServer\ReflectionData

  - On UNIX and Linux, the default location for ReflectionData is
    /var/opt/attachmate/reflectionserver/reflectiondata

  Previous releases had ReflectionData located in the Management Server installation directory.

- **Service names changed.** Attachmate Reflection Server was Reflection Server, Attachmate Reflection Security Proxy was Reflection Security Proxy Server.

- **Services previously started with .bat or .sh files, and this is no longer true.**

- **Server.xml has a different format.**

- **The .install4j directory beneath the ReflectionServer directory contains log files related to the installation process. It contains runtime utilities and services, as well as other installation data. Do not delete this folder.**
3.3.1 Upgrading from Automatically Installed Versions: Reflection for the Web 2008 or Earlier

If Reflection for the Web 2008 or an earlier version is installed on your local computers and servers, use these instructions to upgrade to the current version of Reflection for the Web or Reflection Security Gateway. This upgrade procedure applies to all editions; in the case of the Limited Edition of Reflection for the Web, the security proxy component is not supported.

To upgrade from Reflection for the Web 2008 or Reflection for the Web 9.x:

Step 1. Back up customized files

- Copy and save the cacerts file located here:
  
  [MgmtServerInstall]/_jvm/lib/security/

- Copy and save any files that you customized in the
  
  [MgmtServerInstall]/jakarta-tomcat/webapps/rweb/
  or
  [MgmtServerInstall]/jakarta-tomcat/webapps/rwebmeter/
  or
  [MgmtServerInstall]/jakarta-tomcat/webapps/rweb/gm/ directory.

- If you have replicated servers in your environment, see the information in "Additional Upgrade Modifications" on page 40 before proceeding.

Step 2. Install Reflection for the Web or Reflection Security Gateway Components

Install the product components in a non-web-servable space. This must be a directory that is inaccessible to your web server. Before you begin, review options for installation procedures (page 13).

When you upgrade from a previous version, you do not need to uninstall the product if you are using the automated installer to upgrade from an earlier version. The installation program will prompt you for uninstallation.

Step 3. Upgrade Files from the Previous Version

Run the configuration upgrade utility to configure your new installation. There are additional steps you should do after running the utility:

- Follow the steps in "Upgrading Static Sessions" on page 41 to upgrade sessions that were not saved using the Session Manager or that were manually edited.

- To ensure that your secure sessions were saved correctly, open the Administrative WebStation, and click Security Proxy under Security Setup.

- To ensure that your metering settings were saved correctly, open the Metering Configuration tool. For detailed configuration information, see Setting Up the Metering Component (page 50).

- See "Additional Upgrade Modifications" on page 40 for other changes you may need to make after upgrading.
3.3.2 Upgrading from Manually Installed Versions: Reflection for the Web 2008 or Earlier

The automated installer associated with Reflection for the Web and Reflection Security Gateway is available on a wider variety of platforms than Reflection for the Web 2008 or earlier. Also, more upgrade options are available for earlier versions of the product that were manually installed.

NOTE: Before installing, check the path to your Tomcat directory. If the previous version has a format similar to the ones below, modify the directory to remove the version number and to change "jakarta" to "apache."

Change \[MgmtServerInstall\]/jakarta-tomcat-[version number]/webapps/rweb/ to \[MgmtServerInstall\]/apache-tomcat/webapps/rweb/

- or -

cchange[MgmtServerInstall]/jakarta-tomcat-[version number]/webapps/rweb/gm/ to \[MgmtServerInstall\]/apache-tomcat/webapps/rweb/gm/

Upgrade Options

Automated install - recommended. It is strongly recommended that you install using the automated installer and the configuration upgrade utility.

If you need to perform a manual installation, use the Tomcat servlet runner included with the product. Extract the multi-component archive file (page 24) appropriate for your platform, and then run the configuration upgrade utility to handle the upgrade of your settings.

For either option:

- Install the new version in a different target directory than the previous version. (For an automated install, the default is different than the previous default, so you will be installing in a different target directory if you accept it.)
- It is not necessary to uninstall the previous version.
- When you run the configuration upgrade utility, browse to the location of the previous version so that settings can be migrated.
- Make sure the earlier version of the software is not running when you run the configuration utility. This avoids potential port conflicts and allows you to accept default port assignments. If you are upgrading a Linux or UNIX system, make sure no startup scripts are running.

If you cannot follow one of these options, use the instructions below to upgrade the individual components. If possible, use the directory defaults established by the automated install, such as the location of ReflectionData (page 28), in order to limit the number of files you need to customize.

Component upgrade from Reflection for the Web 2008 or Reflection for the Web 9.x:

Step 1: Back up customized files

- Copy and save cacerts in the

  \[MgmtServerInstall\]/_jvm/lib/security/ directory.
You may have the cacerts in a location associated with a JDK install. Other locations may be the /jvm/lib/security or /jre/lib/security directory of the JDK installation used by Reflection for the Web. In any case, locate this file and make a separate copy of it.

- Copy and save any files that you customized in these directories:
  
  [MgmtServerInstall]/jakarta-tomcat-[version number]/webapps/rweb/
  
  or
  
  [MgmtServerInstall]/jakarta-tomcat-[version number]/webapps/rweb/gm/
  
  If you have replicated servers in your environment, see the information in "Additional Upgrade Modifications" on page 40 before proceeding.

Step 2: Uninstall Reflection for the Web 2008 or Reflection for the Web 9.x Components

Retain these files and directories (in addition to those listed above for all installation methods):

1 Reflection Management Server

- Copy and save the earlier version of the web.xml file located here:
  
  [MgmtServerInstall]/jakarta-tomcat-[version number]/webapps/rweb/WEB-INF/
  
- Copy and save the earlier version of the ReflectionData directory.
  
  For example, the default location of ReflectionData in Reflection for the Web 2008 is as follows:

  On Windows 2003, the default location for ReflectionData is
  C:\Documents and Settings\All Users\Application Data\ReflectionServer\ReflectionData

  On other supported Windows systems, the default location for ReflectionData is
  C:\ProgramData\Attachmate\ReflectionServer\ReflectionData

  On UNIX and Linux, the default location for ReflectionData is
  /var/opt/attachmate/reflectionserver/reflectiondata

  **NOTE:** These defaults are not directly specified in the web.xml file; instead, a value of rwebdata_location_placeholder for the ReflectionData parameter in web.xml generates the appropriate defaults for the platforms listed above.

  If you specified a custom location for ReflectionData or are upgrading from a version previous to Reflection for the Web 2008, open web.xml and locate the ReflectionData parameter to identify the path.

  This folder must be backed up in a location that is not referenced by any upgrade or configuration procedure. This will assure that you have an independent validation of these settings.

- Copy and save the earlier version of any unprotected, static sessions located here:

  [MgmtServerInstall]/jakarta-tomcat-[version number]/webapps/rweb/session/

  These sessions may also be saved in other directories within the webapps directory. See "Upgrading Static Sessions" on page 41 for more information.

2 Security Proxy server

Copy and save the earlier version of these directories:

[security proxy installation]/conf/
[security proxy installation]/keystores/

This saves your server.properties file and your certificates.

3 Metering server
Copy and save the earlier version of the web.xml file located here:

[metering server installation]/jakarta-tomcat-[version number]/rwebmeter/WEB-INF/

4 Servlet runner
Copy and save the earlier version of the Tomcat keystore located here:

[tomcat installation]/jakarta-tomcat-[version number]/conf/

5 Delete the directories in which you installed the previous version of the Reflection for the Web components.

Step 3: Install Reflection for the Web or Reflection Security Gateway Components

See Manually Installing Individual Components (page 26) for a summary of the individual archive files that you can use. Install in a non-web-servable space and in a directory that is inaccessible to your web server.

Step 4: Upgrade Files from the Previous Version

If you installed manually, ensure that these files are copied or edited correctly.

Reflection Management Server

- Copy the old ReflectionData directory into the appropriate location for your site (page 28). If you are copying this directory into the default location, you do not need to edit the web.xml file.

  To specify a non-default location for ReflectionData in the web.xml file, open the file in a text editor. Copy the path to the ReflectionData directory from the web.xml file that you saved into the new web.xml file in this location:

  [MgmtServerInstall]/apache-tomcat/webapps/rweb/WEB-INF

- The SSL port Reflection uses to make an HTTPS connection is set at 443 by default. If you need to change the port number, start the Management Server. This creates the default PropertyDS.xml file. Then, open PropertyDS.xml in the ReflectionData directory. Change the value from 443 to the appropriate port number in the section below, and then restart the Management Server.

  <CORE_PROPERTY NAME="sslport">
  <STRING>443</STRING>

Security Proxy Server

Copy the /conf/ and /keystores/ directories that you saved in step 2 into the new security proxy installation.

To ensure that you can edit your existing secure sessions and create new secure sessions in the Session Manager, export the security proxy server settings to the Administrative WebStation. Run the Security Proxy Wizard. Go to the Proxies tab and click Export Settings, which will export the settings to the Management Server.

Metering Server

If you copied the ReflectionData directory into the default location, you do not need to edit the web.xml file.
If a non-default location for ReflectionData is necessary, edit the web.xml file. Copy the path to the ReflectionData directory from the web.xml file you saved into the new web.xml file in this directory:

[metering server installation]
/apache-tomcat/webapps/rwebmeter/WEB-INF

**Servlet runner**

1. Copy the Tomcat keystore you saved into this location:

   [tomcat installation]/apache-tomcat/conf/

2. In a text editor, open this file;

   [tomcat installation]/apache-tomcat/conf/server.xml

3. Make necessary modifications to the HTTP port or HTTPS port.

See "Additional Upgrade Modifications" for other changes you may need to make after upgrading.

### 3.4 Additional Upgrade Modifications

These upgrade modifications may be necessary after any upgrade method.

**All upgrades**

- **Customized static session files**

  To retain any unprotected static sessions, see “Upgrading Static Sessions” on page 41.

- **IIS Integration**

  The automated installation program detects IIS and allows you to integrate Reflection for the Web or Reflection Security Gateway as part of the installation process. If you need to make modifications later, see “Running the IIS Integration Utility” on page 31.

- **Upgrading replicated servers**

  If server replication is enabled for 9.x versions and above, you must disable it on every server with replication before you upgrade. Follow these steps:

   1. In the Administrative WebStation, under Activities > Settings, click the Replication tab and select the Standalone option. Click Save Settings.
   2. Repeat this step for the Master server and all the Slave servers.
   3. Upgrade all the servers.
   4. Configure the Master server from Standalone back to Master role and define the Slave servers.
   5. Configure the Slave servers from Standalone back to Slave role and point them to the Master server.

- **Importing an activation file**

  After installing Reflection for the Web or Reflection Security Gateway 2014, you can add modules for other terminal types or for expanded functionality, which require activation files to be imported. The automated installation procedure provides a warning when this step is required after you finish installing. See “Adding a Module to your Reflection Product” on page 55 for details.
If you're upgrading from Reflection for the Web 2008 or earlier:

- **Customized login and links lists**
  
  Reflection for the Web 2008 R2 introduced a new method for customizing the login/links list page, and this is the location where customized page templates are stored. If you are upgrading from this version, no other changes are necessary.

  If you are upgrading from a version previous to Reflection for the Web 2008 R2, and you customized the login and links list pages, copy the LauncherHTML.jsp file from the backup of this directory:

  ```
  [MgmtServerInstall]/jakarta-tomcat-[version number]/webapps/rweb/gm/
  ```

  into this directory:

  ```
  [MgmtServerInstall]/apache-tomcat/webapps/rweb/templates
  ```

  You will then need to edit your customized page to incorporate the elements that generate the Reflection applet tags. To see how the new Reflection applet tag elements are inserted into your custom content, use this file as a guide:

  ```
  webapps/rweb/templates/samples/customloginpage.jsp
  ```

  Once your custom page is complete, use the **General Settings** page of the Administrative WebStation to specify the name of your customized login/links list page.

- **Trusted certificates**

  You may need to modify information in the cacerts file. If necessary, you can use a JDK keytool to compare the oldcacerts file that you backed up from here:

  ```
  [MgmtServerInstall]/_jvm/lib/security/ (or the JDK location where cacerts is located)
  ```

  with the new one here:

  ```
  [MgmtServerInstall]/jre/lib/security/
  ```

- **SSL client certificates or SSH user keys**

  If you enabled client authentication in previous versions of the product, a client computer had a client certificate client.pfx file in its user.home directories. This directory contains required files for host-based authentication. The certificates should now be stored in the `RWEB_PREFS` folder on the user's computer. To find the folder, click **About Reflection** on the Help menu of a terminal session, then click the **System Information** tab.

  If you used the Secure Shell transport in HP, VT, or SFTP sessions and you authenticated using user keys in previous versions of Reflection for the Web, the public/private key pairs were installed in the clients' user.home\.ssh\ directories. The key pairs should now be stored in the `RWEB_PREFS\.ssh` folder on the user's computer. To confirm the location of this folder, click **About Reflection** on the Help menu of a terminal session, then click the **System Information** tab.

### 3.5 Upgrading Static Sessions

When terminal sessions are created or modified using the Session Manager, the protected sessions are upgraded during the upgrade procedures when using an automated installer or during startup (when the Tomcat server is started) after a manual installation.

Follow the steps below if any of these conditions exist:

- The sessions were not saved using Session Manager.
The HTML in your sessions was manually modified.

You want to upgrade the static sessions for any reason.

If you have keyboard map files that are not contained within a configuration file, then you must upgrade these files before you upgrade the sessions.

1. Open a Command Prompt, and change directories to find the location below. For Windows, the location is:

   [installation path]\ReflectionServer\apache-tomcat\webapps\rweb\WEB-INF\lib

2. On the same command line, on one continuous line, enter the appropriate syntax (displayed below) to upgrade your specified configuration files. You must specify the items displayed in **bold**:

   - **Language.** On the command line, include the language you want to use: German (de), English (en), or French (fr).
   - **Name of relative or absolute directory or file that contains the configuration files.** (You must be able to access this file or directory from the machine where you are upgrading.)
   - **Enter this command as one continuous line:**

      ```
      java -classpath RWebServlet.jar com.wrq.util.upgrade.ConfigUpgrade -locale <de | en | fr> <file name | directory>
      ```

**Example**

For example, to upgrade the configuration files in the session directory for use with the English version, enter this information:

1. In the Command Prompt, change directories to arrive at this location in Windows:

   C:\Program Files\Attachmate\ReflectionServer\apache-tomcat\webapps\rweb\WEB-INF\lib

2. On the same continuous line, enter the command, language, and location of the session directory:

   ```
   java -classpath RWebServlet.jar com.wrq.util.upgrade.ConfigUpgrade -locale en "C:\Program Files\Attachmate\ReflectionServer\apache-tomcat\webapps\rweb\session"
   ```
Starting the Administrative WebStation

To start the Administrative WebStation:

1. If necessary, start the servlet runner (page 43). You do not need to do this step manually if you ran the automated installer and chose to start the services as the final step.

2. Open the URL for the administrator login page in your web browser. (On Windows with an automated installation, go to Start > All Programs > Attachmate Reflection for the Web 2014 or Attachmate Reflection Security Gateway 2014 > Administrative WebStation.) The URL uses this format:

   http://[host name]:[port number]/rweb/AdminStart.html

   If the port number is the default of 80 for HTTP, you need not include it in the URL. For example, the URL to open the Administrative WebStation might be:

   http://myserver.mycompany.com/rweb/AdminStart.html

3. If you connect using HTTPS and your server has a self-signed certificate, your browser will warn you about the certificate you created. This is expected behavior. When the warning message is displayed, accept the self-signed certificate or choose to proceed, and the product's administrator login page will open. These warning messages will not appear after you purchase a CA-signed certificate or if you import the self-signed certificate into your certificate store.

4. Log on as an administrator by entering the password that you specified during installation. If you installed the product manually, the default password is admin. It is recommended that you change this password as soon as possible. (In the Administrative WebStation, go to Security Setup > Security tab to change the administrator password.)

5. Click Submit. A links list opens; click the Administrative WebStation button at the bottom of the page. (When you upgrade, your previously-configured sessions appear in the list.)

4.1 Starting the Servlet Runner

Before you can run the Administrative WebStation, the metering server, or the ID Manager, you must start the servlet runner. The Tomcat servlet runner is installed by default when you install the product with the automated installer. If you are using a servlet runner other than the one provided, refer to its documentation to start and stop the servlet runner.

Automated install

If you used the automated installer, the servlet runner is installed as a service and you do not need to start it manually.

On Windows, you can start or stop the service by going to the Windows Services list and selecting Attachmate Reflection Server.

For UNIX and Linux platforms, you can start and stop the service at run level changes using the method that is appropriate to your platform. Use the -start and -stop parameters described below. If you used the automated installer, a link to the services is created in this location:

/etc/init.d
Manual install

If you installed manually, run ReflectionServer (Windows) or reflectionserver (UNIX and Linux) to start the servlet runner. It is located in the ReflectionServer directory.

**Windows**

1. `ReflectionServer -install`. This command installs Reflection Server as a Windows service.
2. `ReflectionServer -start`

**UNIX/Linux**

1. Use the daemon appropriate to your platform for installing or uninstalling the servlet runner as a service.
2. `reflectionserver -start`

**Parameters**

The parameters for ReflectionServer and for SecurityProxy are identical. The available parameters are as follows:

- `-start` Start the Reflection Server or Security Proxy Server
- `-stop` Stop the Reflection Server or Security Proxy Server
- `-status` Display the status of the Reflection Server or Security Proxy Server
- `-install` Install the Reflection Server or Security Proxy Server as a service (Windows only)
- `-uninstall` Uninstall the Reflection Server or Security Proxy Server as a service (Windows only)

You can also use JVM options to customize the servlet runner launcher (page 44).

### 4.2 Servlet Runner Launcher JVM Options

If you need additional customization when you start the servlet runner (page 43), you can adjust the JVM options. You can also use these options to start the proxy server (page 49).

To accomplish this, edit the ReflectionServer.vmoptions file, which is found in the same directory as the launcher (for example, ReflectionServer).
5 Configuring Components

The product components can be installed on the same computer or on separate computers. Once each component is installed, it must be configured to meet the needs of your networking environment.

5.1 Management Server

The Reflection Management Server includes the Administrative WebStation -- a web site used to configure Reflection sessions for your users -- and the Java applets used to deploy Reflection terminal sessions to your users.

The Administrative WebStation includes detailed information and options for configuring sessions. Use the information in the WebStation itself, as well as the online help, to get started. If you have a web proxy between client machines and the Reflection Management Server in your network environment, you may need to complete some additional configuration before connections can be made.

Start the Administrative WebStation (page 43) and browse through the information using the table of contents (on the left) and the links embedded in each page.

If you cannot open the WebStation, refer to the information about possible password problems (page 32).

If you are upgrading from a previous version, refer to the upgrade (page 33) sections for information about retaining session settings from your previous installation.

5.2 Security Proxy Server

The security proxy server component requires some setup before you can deploy encrypted sessions. The Reflection security proxy server software consists of two Java applications: the Security Proxy Wizard and the Security Proxy Server.

- The Security Proxy Wizard (page 47) guides you through the steps of setting up the proxy server properties file and importing or generating a security certificate for the proxy server.

  If you used an automated installation procedure to install the product and installed the proxy server on the same machine as the Management Server, you do not need to use the wizard before you start the proxy server. Self-signed certificates are created and the management certificate is added to the proxy server trusted certificates list during the installation.

  If you installed the product manually, you must run the wizard before you can create encrypted terminal sessions that pass through the proxy server and before you can run the security proxy server.

  After initial configuration, use the wizard to manage your security proxy settings and certificates.

- The Security Proxy Server (page 49) manages encrypted connections that pass through the proxy server for secure sessions. The security proxy server uses files generated by the wizard or the automated installer and cannot be run until the server is set up.
The security proxy server component can be installed to the same server as the Reflection Management Server. If you install the security component on a different computer, however, increase the security of each Reflection terminal session by ensuring that there is only one known, secure link between the proxy server and the host computer. You may want to consider a dedicated connection between the proxy server and the host computer, so that the proxy server does not communicate with the host computer over a connection accessible by other computers on the network.

Another approach is to run the proxy server directly on the host computer. A variety of platform-specific archive files (page 27) for installing the security proxy are available that may be appropriate for your host. Replace the JRE with one that is appropriate for your host if necessary. If you run the proxy server directly on the host computer, secure connections will be CPU intensive because additional processing is required to encrypt and decrypt the data stream.

Overview of Deploying a Secure Session

Deploying a secure session through the security proxy can be divided into several general tasks:

1. Install the security proxy server files on your server.
2. Run the security proxy server (page 49).
3. Create an encrypted terminal emulation session (page 49) using the Session Manager in the Administrative WebStation.
4. Map the session to your users. For more information, refer to the overview information and the online help in the Session Manager.

5.2.1 Generating a Management Server Certificate

Before you run the Security Proxy Wizard, you must generate or import a certificate for the Management Server.

NOTE: If you used an automated installer or the multi-component archive file and then ran a configuration utility, an initial self-signed certificate is generated and you can skip these steps.

If you installed Reflection manually, generate a certificate using Security Setup:

1. Start your servlet runner (page 43) and log onto the Administrative WebStation (page 43).
2. In Security Setup, click the Certificates tab.
3. Generate or import a certificate using the links in the Administer Reflection Management Server Certificate section.
   - For evaluation purposes or if you are waiting for your CA-signed certificate, generate a self-signed certificate by clicking the Generate a self-signed certificate link.
   - To use an existing CA-signed certificate, click the Import a signed certificate and private key link.
   - To request a certificate from a Certificate Authority, click the Generate a certificate signing request to a certificate authority link.
4. Enter the requested information, and then click Submit. For more information about each entry, click Help.
5. Verify the information. Click Submit to generate the certificate, to generate the certificate signing request (CSR), or to import the key pair. If you generated a self-signed certificate or imported a key pair, proceed to the instructions for “Using the Security Proxy Wizard” on page 47.
6 If you generated a CSR, you now have a private key. The private key is kept on your server that
is physically and electronically secure. Submit the CSR to a commercial certificate authority (CA)
or a private CA within your organization. Popular commercial CAs include VeriSign, Thawte, and
Entrust. Follow the CA's instructions for submitting your request and obtaining a server
certificate. The CA will verify your company information and issue a certificate. This process may
take several days.

7 When you receive the certificate from the CA, restart the Administrative WebStation, go to
Security Setup > Certificates, and click the View and process pending certificate signing
requests link. Click Process the signed certificate. Specify the requested information and
select Install certificate. Click Submit to package the signed public key with your stored private
key and install your CA-signed certificate on the Management Server.

5.2.2 Using the Security Proxy Wizard

The wizard imports or generates the security certificate used to authenticate the security proxy server
and sets up a properties file that contains information about each security proxy connection. If you are
using authorization to determine access levels, the security proxy also imports the certificate from the
Reflection Management Server.

If you used an automated installer, the security proxy server has been configured and you can skip
this step; you can run the wizard later to manage your proxy settings.

If you installed manually, you must first run the Security Proxy Wizard on the computer where you
installed the software before you can run the security proxy server.

Starting the Security Proxy Wizard

Windows

- If you used the automated installer, go to Start > All Programs > Attachmate Reflection for the
  Web or Reflection Security Gateway > Security Proxy Wizard. Alternatively, run the
  SecurityProxyServerWizard.exe file in the [MgmtServerInstall]\securityproxy\bin\ folder.
- If you installed manually and completed the initial configuration (page 27), run the
  [MgmtServerInstall]\securityproxy\bin\SecurityProxyServerWizard.exe file.

UNIX or Linux

- The Security Proxy Wizard requires an X11 window to display its graphical interface. Use the
  console of an X window, or an X session, as provided with Reflection X, and open a terminal
  window.
- Run the [MgmtServerInstall]/securityproxy/bin/securityproxyservewizard file.

Security Proxy Wizard Options

If you run the Security Proxy Wizard from the command line or from a command prompt, these
command line options are available:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-locale [en</td>
<td>fr</td>
</tr>
</tbody>
</table>

    SecurityProxyServerWizard -locale fr
Configuring the Security Proxy Using the Security Proxy Wizard

If you manually installed the security proxy, run the wizard to complete the configuration of a security proxy port.

1 Start the Security Proxy Wizard.

2 Create a server.properties file by clicking New on the Status tab. It is recommended that you install the file in the \securityproxy\conf\ folder within your installation of the security proxy server. For example, in the Select Data Root dialog box, select the securityproxy folder, and then click the Create button. The conf folder and the server.properties file are automatically created. Verify that you do not have two conf directories in the path. Click Yes to continue. Enter a host name for the security proxy server, and then click OK.

3 Add the Management Server certificate to the security proxy trusted certificates list. On the Trusted Certificates tab, you can import a trusted certificate from a file or directly from the Management Server over the network.

   For evaluation purposes, import a trusted certificate from the Reflection Management Server over the network. Click Import, then click the Server button. In a production environment, or in an environment where greater security is required, it is recommended that importing the trusted certificates be performed by copying the certificates from one machine to the other and then importing them from a local file.

4 Specify (or accept the defaults for) the Reflection Management Server address, the Management Server (not the Proxy Server) port number, the servlet context, and the friendly name of the Reflection Management Server. The context name is used in the URL that accesses the Management Server, and it is often, although not always, the same as the folder within which the Management Server is installed. The default context name is rweb. Click OK.

5 Create the proxy. On the Proxies tab, click Add. Enter the local port number. This is the port on which the proxy listens for connections. It can be any unused port number; it should not be the standard port for the host connection. Click Add to change the default cipher suite.

6 In the Add Cipher Suite dialog box, select a Cipher suite or accept the default. Click the Generate button.

7 In the Generate Security Proxy Certificate dialog box, enter the certificate information. Click the Generate button.

8 In the Add Cipher Suite dialog box, click OK to add the cipher suite.

9 Modify the Proxy Type as necessary. For evaluation purposes, retain the default settings.

10 In the Add Proxy dialog box, click OK to add the proxy.

Parameter | Description
--- | ---
-serverproperties [path and file name of your server properties file] | Specify the server.properties file to open. For example, navigate to the Security Proxy Wizard folder (the default on Windows is \securityproxy\bin\) and enter this command to start the wizard with the specified file.

SecurityProxyServerWizard -serverproperties "C:\Program Files\Attachmate\ReflectionServer\securityproxy\conf\server.properties"

-Parameter Description
11 Export the settings to the Management Server. Click Export Settings on the Proxies tab. In the Export Proxies dialog box, specify or accept the default Management Server, Port, and Context, and then click Export.

12 When you have set up the security proxy server component, click Exit to close the wizard and save your settings. To make changes to the proxy server settings later, simply rerun the wizard.

5.2.3 Running the Security Proxy

The security proxy server enables encrypted connections from Reflection terminal sessions.

Automated install

If you use the Windows automated installer, the servlet runner starts automatically. You can start or stop the service by going to Windows Control Panel > Administrative Tools > Services, and selecting Attachmate Security Proxy Server.

For UNIX and Linux platforms, you can start and stop the service at run level changes using the method that is appropriate to your platform. Use -start and -stop parameters (page 43) for the security proxy.

If you used the automated installer, a link to the services is created in this location.

/etc/init.d

Manual install

After you create a server.properties file for the proxy server computer (which can be created by using the Security Proxy Server Wizard), run SecurityProxy.exe (Windows) or securityproxy (UNIX and Linux) to start the servlet runner. It is located in the ReflectionServer (or reflectionserver) directory.

Windows

1 SecurityProxy -install. This command installs Reflection Server as a Windows service.

2 SecurityProxy -start

UNIX/Linux

1 Use the daemon appropriate to your platform for installing or uninstalling the servlet runner as a service.

2 securityproxy -start

All the available parameters (page 43) for SecurityProxy.exe and securityproxy are identical to the Reflection Management Server’s servlet runner.

5.2.4 Creating Secure Sessions

1 Open the Session Manager in the Administrative WebStation to create configuration files that launch secure terminal sessions.

2 Click the Add button, or click a session name to add security to an existing session.

3 Name and select the session type (both web-based and Windows-based sessions can be configured to use the security proxy). On the Configure a Reflection Session page, click the Launch button.

4 In the session window, on the Connection menu, click Connection Setup.
Reflection for the Web

- Click the SSL/TLS button, and select the appropriate level for your SSL/TLS security.
- Select the Use Reflection security proxy check box, and then specify the default destination host.
- Click OK to close the SSL/TLS Settings dialog box. Click OK to close the Connection Setup dialog box.
- Continue to configure your session by specifying options using the menus in the session window.
- Close the session window, and click the Save/Exit button to save your changes and return to the Administrative WebStation.

Reflection Security Gateway

- Use the security configuration options as described for your Windows-based session.
- Close the session window, and click the Save/Exit button to save your changes and return to the Administrative WebStation.

The new secure session is listed in the Session Manager.

5.2.5 Viewing Security Proxy Reports

To monitor security proxy server activity, check to be sure that the security proxy is running. Open the Security Proxy Server Report page in the Reports section of the Administrative WebStation. Select the security proxy that is currently running from the Security Proxy server list. Use the report to monitor two types of activity for the selected server:

- **Current activity**
  Shows the current connections to the security proxy server, including the IP addresses of the computers connected.

- **History of activity**
  Shows details about security proxy server events, such as when the proxy server was started and stopped, and connection attempts and the IP addresses that made them. If you experience any problems with the security proxy server, technical support may ask for information from the activity log file to aid in troubleshooting. Error, warning, and info messages are logged by default. You can change the types of information logged to include more or less information by using the Security Proxy Wizard.

5.3 Metering Server

The metering server component requires some additional setup before you can deploy metered terminal sessions. Before you begin setting up metering, the Reflection metering server component must be enabled (the default).

Metering can run on any supported web server with a servlet runner using Java 1.6 or later JRE. It is recommended, however, that you use the servlet runner that is installed when you use the automated installer, or is available in the multi-component file for manual installation.

If you have a different servlet runner already installed, follow your servlet runner's instructions for installing new Java servlets.
5.3.1 Creating Metered Sessions

Before you can create a metered terminal session, the metering server must be added using the Administrative WebStation. If you used an automated installer, the metering server was automatically added to the list, and you can create a metered session now.

Follow these steps to create metered sessions:

Reflection for the Web

1. In the Administrative WebStation table of contents, click Session Manager.
2. Click the Add button or click a session name to edit it.
3. On the Configure a Session page, click the Launch button.
4. In the emulation window on the Administration menu, click Metering Setup.
5. Select the Enable metering check box, and make sure the correct metering server is selected in the Metering web server box. The Require metering host check box is cleared by default so that connections are made even if the metering server is unavailable. Select this check box if you want connections to be made only when the metering server is available.
6. Click OK, close the emulation window, and save your changes.

Reflection Security Gateway

To enable metering for Reflection version 12.0 or later Windows-based sessions, you must configure Reflection workstations to report to the metering server. You can either use the Reflection Customization Manager to create a customized Reflection installation that includes metering configuration information, or you can use Reflection's Group Policy settings to configure metering information after installation of Reflection.

Configuring Server Settings in the Administrative WebStation

Use the Settings option in the Administrative WebStation if you installed manually, or if you want to use HTTPS to view metering reports or add an additional metering server to the list.

1. Open the Administrative WebStation (page 43).
2. Click Settings, then click the Metering tab.
3. Enter the Metering web server name. This is the full name or IP address of the server on which the metering component is installed.
4. Enter the Metering web server port. The default is 80 for HTTP, 443 for HTTPS.
5. Enter the Metering servlet context. This is the name of the directory in which you installed the metering component. The default is rwebmeter.
6. Select the Use HTTPS check box to enable a secure connection using HTTPS.
7. Click the Add to Table button.
5.3.2 Opening the Metering Administration Tool

Use the Metering Administration tool to configure settings for the metering server and for license pools.

1. Start the servlet runner (page 43).
2. Open the Metering Administration tool:
   - If you installed on Windows and want to open the Metering Administration tool on the machine where you installed it, use the Start menu: Start > All Programs > Attachmate Reflection for the Web or Attachmate Reflection Security Gateway > Metering Administration.
   - If you installed on another platform or want to access the metering server from a different machine, open a browser to go to the metering server's URL, which will be in this form:

         http://[server name]:[port number]/[metering server context name]/AdminStart.html

   For example, if you used the default settings, the URL might be:

         http://MeteringServer/rwebmeter/AdminStart.html

3. A logon page opens. Enter the Metering administrator password, and click Submit.
   - If you used an automated installer, you entered a password during installation. Type your password here.
   - If you installed manually, type in the default password, admin. You can change this password later.
4. Configure license pools (page 52).

5.3.3 Configuring License Pools

1. Create (page 51) and then run your metered sessions. This automatically creates the product license pools.
2. Open (page 52) the metering administration tool.
3. After logging in, click a link for the product to configure. Your licenses and products and the type of enforcement, if any, are specified here.
4. When you ran your metered product, the Product, Product type, and VPA number were specified, and appear here as static text.
5. Select the type of license (either nonconcurrent or concurrent). Enter the number of licenses covered by the agreement.
6. Enter the Major version number of the product. For example, if you are using Reflection Security Gateway 2014, enter 12. To find version information, select the Resources topic from the Administrative WebStation's navigation panel on the left, and then select the About Reflection topic.
7. Select the Limit number of concurrent users to number of licenses check box if you want to block users from running Reflection or making connections when the number of concurrent users exceeds the number of licenses.
8. If license limits have been exceeded, the Management Server can notify administrators you list here. (You must first configure the global SMTP and e-mail account name fields when you configure metering options (page 53).) Enter e-mail addresses separated by commas. E-mail notifications can be sent if Concurrent is selected as the license type.
9 Select the **Enable Reflection for the Web connection limit** check box to prevent users from logging on to more than the number of hosts you specify in the field. This feature is available for Web-based sessions only.

10 Click **Submit**. Repeat these steps for each Attachmate product you want to meter. These settings appear in the **License Pool Settings** list. Click the product name in the list to edit these settings later.

### 5.3.4 Viewing Metering Reports

To view reports about metering activity:

1 Start the servlet runner.

2 Reports can be viewed from the Administrative WebStation or from the metering reports tool.
   - Start the **Administrative WebStation** (page 43). In the table of contents, under Reports, click **Metering Reports**. Ensure that your metering server is selected in the Metering web server box. Click **Show Report**.
   - To open the Metering Reports on the Windows machine where the metering server is installed, go to Start > All Programs > Attachmate Reflection for the Web or Reflection Security Gateway Metering Reports.
   - On other platforms or from a different machine, open a web browser and go to http://[metering server name]/rwebmeter/ReportsLogin.do.

3 Either a login prompt or the main reports page opens. If you specified a password during installation or metering configuration, enter it and click **Submit**. If you installed manually, the default password is admin. You can change this password when you configure metering options (page 53).

### 5.3.5 Configuring Metering Options

After you install the metering server, you can configure the server for your environment. You can run the server without performing this step.

1 Open the **Metering Administration tool** (page 52).

2 On the Reflection Metering Server configuration page, next to **Change server settings**, click **Configure**.

3 **Passwords**: These are optional settings. The Administrator password provides access to these configuration pages and to the metering reports. The Reports password provides access to the metering reports, but does not provide access to the metering configuration. If you used an automated installer, the password you entered during installation is the default for both passwords here. If you installed manually, the default for both passwords is admin.

4 **Metering logs**: Specify the number of days to save log files. Reflection automatically deletes log files that are older than the value specified here. The default is 365. It is recommended that you keep backup copies of your old log files in long term storage. They will then be available, if needed, for auditing purposes. Specify the number of minutes between metering log entries or checkpoints. The default is 60 minutes, in other words, entries are logged once per hour.

5 **Metered client**: Specify how often the client sends a heartbeat signal to the server to communicate that it is running. Select the check box if you want to include the hosts that users connect to in the metering log. Host connection tracking is not available for Reflection X, Web-based AS/400 data transfer, and FTP sessions.
6 E-mail notification options: These are optional settings. To send e-mail notifications when the number of concurrent licenses is exceeded, enter the SMTP server to use and the e-mail account name that will be shown as the sender of the e-mail.

7 Click Submit to save your settings and return to the main configuration page.

5.4 ID Manager

The ID Manager component requires some additional setup before you can deploy terminal sessions that use an ID Manager connection ID. Before you begin setting up ID management for client sessions, the Reflection ID Manager component must be installed as described in “Installing Reflection for the Web and Reflection Security Gateway” on page 13.

ID Manager can run on any supported web server with a servlet runner using Java 1.6 or later JRE. It is recommended, however, that you use the servlet runner that is installed when you use the automated installer or that is available in the multi-component file for manual installation.

If you have a different servlet runner already installed, follow your servlet runner's instructions for installing new Java servlets.

5.4.1 Setting Up ID Manager

Before you can deploy a terminal session that uses an ID Manager connection ID, the ID Manager must be configured.

If you installed the ID Manager using the automated installer, use the configuration steps below. For a manually installed version, first install the ID Manager (page 28) [manually], and then follow these steps.

The overview below gives a high-level summary of the procedure. For detailed instructions, see the topic “Setting Up ID Manager” in the ID Manager console. (On the Server Settings tab, click Help; then click the Setup Instructions link.)

1 Open the Administrative WebStation and configure the ID Manager settings. On the Settings tab, click ID Manager and provide the necessary information.

2 Populate the server with IDs, pools and association sets. Open the ID Manager console.

3 After completing the step to populate the ID management database, start the Reflection ID Manager console and use the display on the Server Settings tab to confirm that the database input is valid, and that the ID Manager is available for sessions configured to use the ID Manager as the connection method.

4 Configure sessions for your users with ID Manager as the connection method. As part of the session configuration procedure, click Test selected attributes to test the connection and confirm that the configuration successfully assigns an ID for the session.

Use the Monitor IDs tab in the ID Manager console to review ID usage and release, reclaim, and hold IDs.
5.5 Adding a Module to your Reflection Product

Reflection for the Web includes editions that provide Web-based terminal support for a variety of host types. Reflection Security Gateway provides Windows-based terminal support for a variety of Attachmate terminal emulation products.

You can install either of these products and then later import an activation file to add the functionality of the other without needing to reconfigure or restart your Management Server. Activation files are also available to add other modules, such as Reflection Automated Sign-on for Mainframe.

Importing Activation Files

Additional modules, such as Reflection Automated Sign-on for Mainframe, can be installed by importing activation files, which are made available at an Attachmate download location after purchasing the module. Activation file names have this format:

activation.<module_name>.jaw

For example, this procedure adds Reflection Security Gateway functionality to an existing Reflection for the Web installation.

1. In the Administrative WebStation, click Resources in the Reference section.
2. Click About Reflection. This page shows the current product (including version number) you are running, and provides the option to install your other entitled module(s).
3. From the Attachmate download location, download the module for Reflection for the Web (activation.<module_name>.jaw) to a location on your local computer.
4. On the About Reflection page, click Browse beneath the list of installed modules. Locate and select the module you downloaded.
5. Click Open.
6. Click Install. The new module is included in the list of installed modules.
7. Close all instances of the browser. Start the Administrative WebStation again. In the Session Manager, click Add to see the new column of Windows-based session options.

NOTE: If you have Reflection Security Gateway Limited Edition, which provides support for a set of Windows-based sessions, you can add support for a limited set of Web-based sessions as part of the product. To set up Reflection Security Gateway to manage the supported Web-based sessions, install the activation file using the above procedure.

Product Rename Utility:

If you add a Reflection for the Web activation file to an existing Reflection Security Gateway installation, the product name changes to Reflection for the Web. However, some Windows-based utilities (the Start menu program group and the Add/Remove programs list) will not reflect this change. To synchronize these names after adding the Reflection for the Web module, use the Product Rename Utility, located here:

[installation directory]\utilities\bin\ProductRenameUtility.exe
5.6 Removing Components

To remove a product component from your computer, follow these steps:

- All of the Reflection for the Web or Reflection Security Gateway components must be stopped to complete uninstallation. If you installed Reflection manually, stop the servlet runner and the security proxy and close the command windows before you begin uninstallation. If you installed the servlet runner and the security proxy as Windows services using the automated installer, the uninstaller will stop them automatically.

- On Windows platforms, verify that no Reflection Management Server directories are open in a browser window.

- If you plan to remove either the Management Server, the ID Manager, or the Metering Server using the automated installer, be aware that you must uninstall web applications and the servlet runner at the same time.

- To uninstall on Windows, use Programs and Features from the Control Panel.

- If you used an automated installer for UNIX, run the uninstaller:

  [installation directory]/uninstall

  Files not installed by the automated installer will not be removed. Static session pages that may be configured, or other customized content, will still be available following an automated uninstall.

- If you installed a component manually, simply delete the directory where you extracted it. If you want to save the settings that you configured, be sure to retain the ReflectionData directory. For more information about retaining settings, see “Upgrading from a Previous Version” on page 33.
Terms

Java Software Development Kit (JDK). The JDK (previously called the Java SDK) is the software development environment for writing Java applets or applications; it is a superset of the Java Runtime Environment and the Java Virtual Machine.

Java Runtime Environment (JRE). The JRE is a subset of the JDK for end-users. It includes a Java Virtual Machine and a Java interpreter and provides a unified interface to Java programs, regardless of the underlying operating system.

Java Virtual Machine (JVM or VM). The JVM is the part of Java that interprets Java bytecode. Because the JVM is part of the JDK, it has the same version number. When a browser supports a specific version of the JDK, this includes the JVM.

JavaServer Pages (JSP). A Java technology that helps software developers serve dynamically generated web pages based on HTML, XML, or other document types.

Java Cryptography Extension (JCE). The Java Cryptography Extension (JCE) provides a framework and implementations for encryption, key generation and key agreement, and Message Authentication Code (MAC) algorithms.