# Installation Guide

Host Access Management and Security Server

Micro Focus®

MICRO FOCUS®

# Installation Guide

## Host Access Management and Security Server

12.2

Attachmate Corporation

705 5th Avenue South

Seattle, WA 98104

USA

+1.206.217.7100

http://www.attachmate.com (http://www.attachmate.com)

# Contents

# Installation Guide: Host Access Management and Security Server

Management and Security Server provides an administrator the means to centrally manage, secure, and monitor users' access to host connections. Management and Security Server can be used to manage several products including Reflection Desktop, Reflection ZFE, Reflection for the Web, and Rumba.

This guide provides a product overview and detailed steps for installing and configuring Host Access Management and Security Server.

The installation of Management and Security Server includes the Administrative Server with the option to install the Metering Server at the same time or later. You have the option to augment Management and Security Server's functionality with other products, including

- Security Proxy Server
- Terminal ID Manager
- Automated Sign-On for Mainframe

The add-on products require separate licenses and may require additional installation or activation procedures.

If you are running an evaluation copy, the product will be fully functional for 120 days. During that time you can install, configure, and test Host Access Management and Security Server. Please contact Micro Focus or your authorized reseller to obtain the full-use version of the software.

# 1 Preparing to Install

For each component, you can use either the automated installer (page 17) or the archive files to manually install (page 21) 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 Administrative Server must be installed. The Security Proxy, when available, is optional.
- Any Management and Security Server (or its predecessor, Reflection Security Gateway) component currently running must be shut down before installing or upgrading. (The automated installer will close components for you if you installed the earlier version with an automated installer.)
- Make sure that you have the necessary account 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 Administrative Server has permission to write to the Java SDK certificate authority certificates file (cacerts). The default location in Windows is:

  `C:\Program Files\Micro Focus\MSS\jre\lib\security`

  **Note:** If you are upgrading from Reflection Security Gateway, the Windows location remains

  `C:\Program Files\Attachmate\ReflectionServer\jre\lib\security`

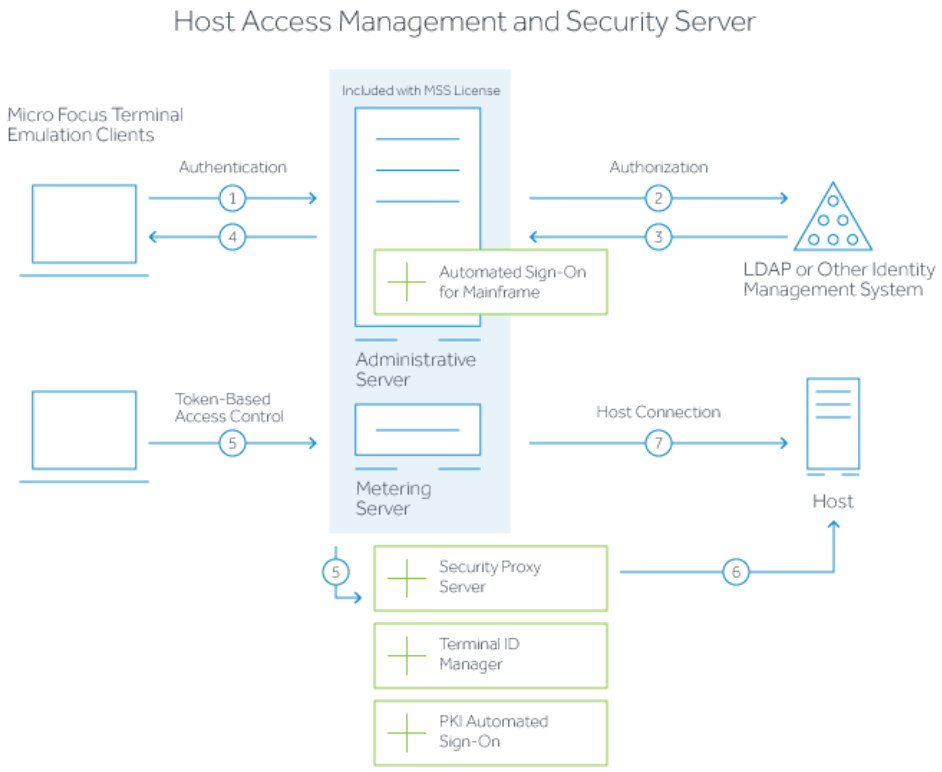
## 1.1 Management and Security Server Overview

Management and Security Server provides authentication, authorization, and secure access to enterprise resources. Secure access is delivered to applications on IBM, HP, UNIX, Linux, Unisys, and OpenVMS hosts.

In addition to providing access to terminal sessions, Management and Security Server provides the ability to secure your system with directory-based authorization, strong authentication, and centrally managed sessions and macros.

The overview diagram depicts the secure interactions between the client and the host, including the option to use the Security Proxy Add-On.

.




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

## 1.2 Components and Add-On Products

The following components and add-on products are available with Management and Security Server. Each add-on product requires a separate license to be activated. Some add-on products can be installed using the automated installer, while others require a separate installation.

See Chapter 3, “Configuring Components and Add-Ons,” on page 31 for configuration details.

### 1.2.1 Administrative Server

The Administrative Server is the central component of Host Access Management and Security Server that enables you to define terminal emulation sessions, and then manage and configure secure settings for those sessions. The Administrative WebStation is the interface for the Administrative Server, where you configure and save settings.

The Administrative Server can be installed using the automated installer or a manual installation.

### 1.2.2 Metering Server

Use the Metering Server component to monitor the use of terminal sessions including the ability to track the number of connections and total connection time per user.

The optional Metering Server is included with Management and Security Server and can be installed onto the same server as the Administrative Server or on another system — either during the initial installation or later. Before you can meter the use of terminal sessions, you must set up the metering server (page 36).

### 1.2.3 Security Proxy Add-On

The Security Proxy acts as a proxy for terminal sessions and provides token-based access control, routing encrypted network traffic to and from user workstations. The Security Proxy Server can be installed on the same server as the Administrative Server or on another system using either the automated installer or a manual installation

If Security Proxy is added after you install the Administrative Server, you can either run the automated installer or install the activation file using the Administrative WebStation and then activate the server. See “Security Proxy Server” on page 31 for details.

### 1.2.4 Terminal ID Manager Add-On

The Terminal ID Manager enables 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.

The Terminal ID Manager can be installed on the same server as the Administrative Server or on another system using either the automated installer or a manual installation.

### 1.2.5 Automated Sign-On for Mainframe Add-On

Automated Sign-On for Mainframe enables an administrator to configure a connection to the Digital Certificate Access Server (DCAS) on an IBM z/OS mainframe, and then configure their mainframe sessions so that users can access their entitled sessions using a single login, such as with a smartcard.

To add Automated Sign-On for Mainframe, you need to install the activation file and configure settings using the Administrative WebStation. Some configuration is also needed on the mainframe.

### 1.2.6 Utilities

A variety of utilities may be required after you complete the basic installation and configuration steps. See “Configuration Tools” on page 28 for a summary.

# 1.3 System Requirements

Check the requirements for each component, which vary slightly.

## Administrative Server Requirements

The Administrative Server is the central component of Management and Security Server and is platform-independent. For production, the Administrative Server should be installed on a server-class operating system. To run the Administrative Server, you need:

- A servlet engine or application server compliant with Java Servlet 2.3 specification and JSP (page 49) 1.2 such as Apache Tomcat.
- A server running JRE 7 or later. The required JRE is installed automatically when you use an automated installer or a multi-component archive file to install Management and Security Server.

  (See JCE Unlimited Strength Jurisdiction Policy Files.)

## Administrative WebStation Requirements

- Any web browser using a JRE 7 or later that can run trusted applets and supports JavaScript and cookies.

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

## Metering Server Requirements

- Servlet engine or application server compliant with Java Servlet 2.3 specification and JSP 1.2 such as Tomcat.
- A server running JRE 7 or later. The required JRE is installed automatically when you use an automated installer or a multi-component archive file to install Management and Security Server.

## Security Proxy Server Requirements

- A server running JRE 7 or later. The required JRE is installed automatically when you use an automated installer or a multi-component archive file to install Management and Security Server.

## Terminal ID Manager Requirements

- Servlet engine or application server compliant with Java Servlet 2.3 specification and JSP 1.2 such as Tomcat.
- A server running JRE 7 or later. The required JRE is installed automatically when you use an automated installer or a multi-component archive file to install Management and Security Server.

## Terminal Emulation Session Requirements

- Users or administrators who launch Windows-based or Web-based sessions from the Java-based login/links list applet must have 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 browsers.

### 1.3.1 JCE Unlimited Strength Jurisdiction Policy Files

Each component that requires JRE also requires **JCE Unlimited Strength Jurisdiction Policy Files**.

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

---

**NOTE: JCE Unlimited Strength Jurisdiction Policy Files must be applied**

- when you manually install Management and Security Server.
- each time you upgrade your JRE.

See Applying the JCE Unlimited Strength Jurisdiction Policy Files.

---

# 2 Installing Management and Security Server

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

- Will you be upgrading from the predecessor product, Reflection Security Gateway 2014?

  If yes, first review the Upgrading section. “Upgrading from Reflection Security Gateway” on page 43.
- What operating systems are running on the machines where you want to install?

  See Installation Options.
- 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 Administrative Server. Other components such as the Metering Server, Security Proxy Server, and Terminal 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 20) 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 23) 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 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

| Operating System | Web Server or Servlet Runner | Recommended Installation Procedure |
|---|---|---|
| Linux | Tomcat (default) | Use the automated installer:<br>mss-<version>-prod-linuxx64.sh<br>or<br>mss<version>-prod-linuxia32.sh |
| Windows | Tomcat (default) | Use the automated installer:<br>mss-<version>-prod-wx64.exe<br>or<br>mss-<version>-prod-w32.exe |
| Windows with IIS (Internet Information Services) | Tomcat (default) | Use the automated installer:<br>mss-<version>-prod-wx64.exe<br>or<br>mss-<version>-prod-w32.exe |
| Windows, Unix, Linux, or Macintosh | IBM WebSphere | Use the manual installation procedure for individual components and configure as a web application following the steps supplied with your servlet runner. |

# 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 Management and Security Server for your site, you can install in a test environment.

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

## Privilege Requirements

**On Windows.** 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 servers to run with administrative privileges, right-click the Start Menu shortcut and click **Properties**. On the **Compatibility** tab, select the **Run this program as an administrator** check box, and then click **OK**.

**On UNIX/Linux.** 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 21). If you also require installation of the MSSData folder, which stores site-specific content, to a non-default location (/var/opt/microfocus/mss/mssdata), see “Specifying the Location of Configuration Information” on page 27.

## 2.1.1 Automated Installation and Configuration: Checklist and Defaults

Use this checklist to identify the defaults and the data that you must specify when running the installer and configuration utilities. Then refer to this list to keep track of your choices as you install Management and Security Server.

**If you are upgrading from Reflection Security Gateway:** It is not necessary to uninstall the product before running the automated installer. The automated installer will uninstall the earlier product and migrate user data when it is detected. The installation path and folder names do not change.

### Step 1: Initial Installation (not upgrading)

| Installation Option | Default | Your Installation Entry |
|---|---|---|
| Component Selection | Administrative Server, Security Proxy Add-On | |
| Destination Directory | Windows:<br>C:\Program Files\Micro Focus\MSS<br>Linux (dynamically determined)<br>SUSE Linux:<br>`/opt/microfocus/mss`<br>RedHat:<br>`/usr/local/bin/microfocus/mss` | |
| Start Menu Folder | Micro Focus Host Access Management and Security Server | |
| Create shortcuts for all users | No (Windows only) | |
| Suppress creation of Start Menu folder | No (Windows only) | |

### Step 2: Configuration

**Configuration of Initial Installation**

| Installation Option | Default | Your Installation Entry |
|---|---|---|
| Installation directory | Confirm the installation directory<br>Windows:<br>`C:\Program Files\Micro Focus\MSS`<br>SUSE Linux:<br>`/opt/microfocus/mss`<br>RedHat:<br>`/usr/local/bin/microfocus/mss` | |

| Installation Option | Default | Your Installation Entry |
|---|---|---|
| Services | Administrative Server, Metering Server, Terminal ID Manager | |
| VPA number | no default given | |
| Servlet runner HTTP port | 80 | |
| Servlet runner HTTPS port | 443 | |
| Security Proxy port | 3000 | |
| Security Proxy monitor port | 8080 | |
| Password | none provided | |
| Server name for URLs and Certificates | DNS name of computer on which the Administrative Server is installed | |
| Organizational Unit | your department name | |
| Organization | your company name | |
| City or locality | your city without abbreviation | |
| State | your state or province without abbreviation | |
| Country | two-letter country code | |

### Configuration Upgrade from Reflection Security Gateway

| Installation Option | Default | Your Installation Entry |
|---|---|---|
| Installation directory | The location where the current version is or will be installed. For example, C:\Program Files\Micro Focus\MSS or /opt/microfocus/mss or /usr/local/bin/microfocus/mss | |
| Previous Installation directory | The location where the earlier version of the product was installed. For example, C:\Program Files\ReflectionServer | |
| Services | Administrative Server, Metering Server, Terminal ID Manager | |
| Servlet runner HTTP port | 80 | |
| Servlet runner HTTPS port | 443 | |
| Server name | DNS name of computer on which the administrative server is installed | |

### Step 3: Starting Services

Before selecting startup options on a Windows machine, the automated installer detects if Windows Internet Information Services (IIS) is installed on your machine and offers to integrate IIS with Management and Security Server. The default is **Yes**.

| Installation Option | Default | Your Installation Entry |
|---|---|---|
| Start server components now | yes | |
| URL for Administrative WebStation | `http://[administrative server DNS name] /mss/AdminStart.html`<br>An IP address can be used instead of a DNS name. | |
| URL for Metering Administration | `http://[administrative server DNS name] /meter/AdminStart.html`<br>An IP address can be used instead of a DNS name. | |
| URL for Metering Reports | `http://[adinistrative server DNS name] /meter/MeteringReports.html`<br>An IP address can be used instead of a DNS name. | |
| URL for Terminal ID Manager Administration and Monitoring | `http://[administrative server DNS name]/tidm`<br>An IP address can be used instead of a DNS name. | |

## 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:

`mss-<version>-prod-linuxx64.sh`

or

`mss-<version>-prod-linuxia32.sh`

**On Windows**

In the \install-automated directory, double-click the product file for your operating system.:

`mss-<version>-prod-wx64.exe`

or

`mss-<version>-prod-w32.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.

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

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

**MSS Server**

Select this check box to install the Administrative Server, which includes the Administrative WebStation. The default servlet runner (Tomcat) and the Metering Server are automatically installed.

If the **Security Proxy Add-On** and the **Terminal ID Manager Add-On** are licensed, they can be installed with the automated installer. For installation options, see Chapter 3, “Configuring Components and Add-Ons,” on page 31

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 Management and Security Server 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 28).

---

**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 Administrative Server; creates an MSSData directory under which site-specific content is stored; generates cryptographic keys and self-signed certificates for Tomcat and Administrative Servers; sets the administrative password; and sets a port value for Tomcat in configuration and HTML files. If the Security Proxy Add-On is installed, the utility generates cryptographic keys and self-signed certificates, automates configuration, and sets a port value for the Security Proxy.

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

2 **MSS Server Services:** Select the services you want to enable. You must have an MSS Server service running on one machine at your site. The Metering and Terminal ID Manager Add-On components are optional and can be installed and run on separate machines. To enable the optional components later, use the Configuration Upgrade Utility. (page 28)

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 are entitled and 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 Terminal 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 TLS connections to the Administrative 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 29).
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 Administrative 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, MSSData (if a custom location was not configured), copies Security Proxy Server configuration files (if enabled) from the old install directory to the new install directory, and updates port values in configuration and HTML files.

---

**NOTE:** When upgrading only the Proxy Server, the panels described below are not all displayed.

---

1. **Select your language.**
2. **Installation Directory:** Confirm the location where the new version of the Administrative 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 an Administrative Server service running, but the Metering Server, Terminal ID Manager Add-On, and the Security Proxy Add-On 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 Management and Security Server. 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 29).

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.

### Step 3: Start Services

After completing configuration, you are returned 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 30) 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 45 and “Running the Security Proxy” on page 35.

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

   After installing the Administrative 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]/mss/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 > Micro Focus Host Access Management and Security Server > Administrative Server.

## 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 28) in console mode.

## 2.1.4 Unattended Installation

Management and Security Server installation is 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 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 28, which are optional for many upgrade scenarios.

1. Install Management and Security Server 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 Management and Security Server. On the original machine, `response.varfile` is located here:

   `[MssServerInstall]\.install4j`
3. Locate the appropriate executable (see “Installing and Configuring with Automated Utilities” on page 17) 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 Management and Security Server on a 64-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:

```
mss-<nn.n.nnn>-prod-linuxx-64.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 Tomcat, which is automatically installed with the product.
- 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, Management and Security Server components may not function correctly.

## 2.2.1 Applying the JCE Unlimited Strength Jurisdiction Policy Files

Management and Security Server requires 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 Management and Security Server, the JCE Unlimited Strength Policy Files are applied for you.

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

- manually install Management and Security Server.
- 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 (http://www.oracle.com/technetwork/java/javase/downloads/index.html)

   IBM: https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk (https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk)
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, use the multi-component archive file that contains all necessary components. The archive file includes the following:

- Management and Security Server
- Metering Server
- Terminal ID Manager (if licensed)
- Security Proxy Server (if licensed)
- Tomcat servlet runner
- The JRE for the appropriate platform

| Archive File | Description |
|---|---|
| mss-prod-wx64-manual.zip | Multi-component zip file for Windows 64- bit systems |
| mss-prod-w32-manual.zip | Multi-component zip file for Windows 32- bit systems |
| mss-prod-linuxx64-manual.tar.gz | Multi-component archive file for Linux 64-bit systems |
| mss-prod-linuxia32-manual.tar.gz | Multi-component archive file for Linux 32-bit systems |

Extract the files; then run the appropriate automated configuration utility (page 28). If you are upgrading (page 43), 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 Terminal ID Manager by simply deleting the folders for those components.

After you have installed the Administrative Server and completed this part of the configuration, you can start the servlet runner and run the Administrative WebStation (page 45). To configure the Security Proxy Server, generate or import an Administrative Server security certificate.

## 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 (JRE) other than the one provided by the installer. No JRE is installed with these files.

Platforms that may use these files include z/OS, Mac, HP-UX, Solaris, and other Linux systems.

### Automated installer

For example:

```
mss-12.2.<build number>-prod-unix-nojre.sh
```

### Manual installer

For example:

`mss-prod-unix-nojre-manual.tar.gz`

### Manual Installer for Security Proxy only

`securityproxy-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 Management and Security Server 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 23) 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 49) 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 Administrative Server, Metering Server, and Terminal 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:

| Archive File | Component |
|---|---|
| `mss.war` | Administrative Server (page 25) (Emulation & Administration) |
| `meter.war` | Metering Server (page 26) |

| Archive File | Component |
|---|---|
| `tidm.war` | Terminal ID Manager (page 26) |
| `idmutils.zip` | A zip file containing sample database script templates with examples of ID attributes and pool types for the "Terminal ID Manager" on page 39 |

There is an additional set of archive files for installing the Security Proxy Server (page 25) on a separate machine.

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: Administrative Server

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

### Installing mss.war

Create an mss directory and extract mss.war into the mss 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 Administrative Server

It is recommended that you use the default location for the MSSData directory. If you need to use a different location, see "Specifying the Location of Configuration Information" on page 27.

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

1. Start the Administrative Server (with defaults) to generate the PropertyDS.xml file. **Note:** If there is a port conflict, the administrative server may fail to start or function correctly.
2. Open PropertyDS.xml in the MSSData 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 Administrative Server, with the correct port.

## 2.2.6 Manual Installation: Security Proxy

If you are licensed for the Security Proxy Add-On, 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 Administrative Server. The archive files are located in the `\install_manual` directory.

**Installing the securityproxy archive file**

1. Locate the securityproxy archive file in the `\install_manual` directory.

| | |
|---|---|
| `securityproxy-prod-linuxx64-manual.tar.gz` | Archive file for the security proxy server for a Linux 64-bit system |
| `securityproxy-prod-linuxia32-manual.tar.gz` | Archive file for the security proxy server for a Linux 32-bit system |
| `securityproxy-prod-wx64-manual.zip` | Archive file for the security proxy server for a Windows 64-bit system |
| `securityproxy-prod-w32-manual.zip` | Archive file for the security proxy server for a Linux 32-bit system |

2 Extract the file into any directory. The default path in automated installations is as follows:

`[MssServerInstall]\securityproxy`

After you install the Security Proxy Server, generate or import a Administrative Server security certificate (page 32) and start the Security Proxy Server (page 35).

## 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 meter.war for your platform (located in the `install_manual\components` directory) to install the metering server.

### Installing meter.war

Create an meter directory within the appropriate directory, and extract meter.war into the meter 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 36).

You can edit the web.xml file to specify the location of the MSSData directory, but it is not necessary if the MSSData directory is in the default location. See “Specifying the Location of Configuration Information” on page 27 for instructions.

## 2.2.8 Manual Installation: Terminal ID Manager

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

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

### Installing tidm.war

Create a tidm directory within the appropriate directory, and extract tidm.war into the tidm 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 Terminal ID Manager, confirm that the servlet runner has started. See “Setting Up Terminal ID Manager” on page 40.

You can edit the web.xml file to specify the location of the MSSData directory, but it is not necessary if the MSSData directory is in the default location. See “Specifying the Location of Configuration Information” on page 27 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 `[MssServerInstall]\utilities\idmutils.`

After completing these steps, see “Setting Up Terminal ID Manager” on page 40.

## 2.2.9 Specifying the Location of Configuration Information

MSSData is the root directory under which site-specific 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 MSSData, you can edit the web.xml file (instructions below) to specify the location of the MSSData directory.

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

- On Windows Server 2012 and Windows Server 2008:

  ```
  C:\ProgramData\Micro Focus\MSS\MSSData
  ```

- On Windows Server 2003:

  ```
  C:\Documents and Settings\All Users\Application Data\Micro Focus\MSS\MSSData
  ```

- On UNIX and Linux:

  ```
  /var/opt/microfocus/mss/mssdata
  ```

If you need to specify the location of MSSData, 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 MSS directory for each component:

   ```
   mss/apache-tomcat/webapps/mss/WEB-INF/web.xml
   ```

   ```
   mss/apache-tomcat/webapps/tidm/WEB-INF/web.xml
   ```

   ```
   mss/apache-tomcat/webapps/meter/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>MSSData</param-name>
     <param-value>/var/opt/microfocus/mss/mssdata</param-value>
   </context-param>
   ```

3. Save your changes and restart the servlet runner (page 45).

# 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 how you installed the product.

- Initial Configuration and Configuration and Upgrade Utilities (page 28)
- Set up certificates using the HTTPS Certificate Utility (page 29)
- Integrate with IIS on a Windows machine (page 30)

## 2.3.1 Initial Configuration and Configuration Upgrade Utilities

These utilities require that Management and Security Server was installed using either the automated installer or the multi-component archive file (page 23).

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 17.

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

**Windows systems**

```
[MssServerInstall]\utilities\bin\InitialConfigurationUtility.exe
```

and

```
[MssServerInstall]\utilities\bin\ConfigurationUpgradeUtility.exe
```

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**

```
[MssServerInstall]/utilities/bin/InitialConfigurationUtility
```

and

```
[MssServerInstall]/utilities/bin/ConfigurationUpgradeUtility
```

### Initial Configuration Utility

This utility enables the services you select for the Administrative Server; creates an MSSData directory under which site-specific content is stored; generates cryptographic keys and self-signed certificates for Tomcat and the Administrative Servers; sets the administrative password; and sets a port value for Tomcat in configuration and HTML files. If the Security Proxy Add-On is installed, the utility generates cryptographic keys and self-signed certificates, automates configuration, and sets a port value for the Security Proxy.

### Configuration Upgrade Utility

This utility enables the services for this Administrative 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, MSSData (if a custom location was not configured), copies Security Proxy Server configuration files (if enabled) 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 Reflection Security Gateway" on page 43 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 administrative 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 Management and Security Server 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**: Start > All Programs > Micro Focus Host Access Management and Security Server > HTTPS Certificate Utility
- **Linux/UNIX:** [MssServerInstall]/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 Administrative 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 45) to restrict the Administrative Server to the HTTPS protocol.

1. Choose **Security Setup** on the navigation bar or home page.
2. Choose the **Security** tab.
3. In the **Administrative 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 Services (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 Management and Security Server 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 Management and Security Server 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 integrated with the IIS web server, Management and Security Server 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 Management and Security Server installation.

---

**To integrate with IIS:**

1. Run the IIS Integration Utility (`IISIntegrationUtility.exe`) located in the `[MssServerInstall]\utilities\bin` folder.
2. To integrate IIS with Management and Security Server, select a site and click **Integrate**.
3. If you are prompted, confirm the installation directory (for example, C:\Program Files\Micro Focus\MSS) 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 Administrative Server service, click **Yes**.
6. On the Integration Completed message box, click **Yes** to exit.
7. Restart the Administrative Server. This step is necessary only if you did not select the option to restart the MSS service.
   - If you installed the product as a Windows service, go to Control Panel > Administrative Tools > Services > Micro Focus MSS Server. Stop and restart the service.
   - You can also use the -stop and -start commands (page 45) with MssServer.exe.
8. Confirm that integration was successful by browsing to http://<serverName>[:port]/mss/AdminStart.html where <serverName> is the IP address or alias of your Microsoft Windows machine running the Administrative Server, for example: http://myserver.mycompany.com/mss/AdminStart.html

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

# 3 Configuring Components and Add-Ons

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.

## 3.1 Administrative Server

The Administrative Server includes the Administrative WebStation — a web site used to configure and secure terminal emulation sessions for 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 Administrative Server in your network environment, you may need to complete some additional configuration before connections can be made.

Start the Administrative WebStation (page 45) and browse through the information using the table of contents (on the left) and the links embedded in each page.

If you are upgrading from a previous version, refer to the upgrade (page 43) sections for information about retaining session settings from your previous installation.

## 3.2 Security Proxy Server

After the Security Proxy Add-On is installed, some setup is required before you can deploy encrypted sessions. The Security Proxy Add-On consists of two Java applications: the Security Proxy Wizard and the Security Proxy Server.

- The Security Proxy Wizard (page 33) 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 Security Proxy Server on the same machine as the Administrative 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 35) 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 can be installed on the same computer as the Administrative Server or on a different computer. Although data between the terminal session and the proxy server is encrypted, data between the proxy server and the host computer is typically not encrypted, so no

matter which installation method you choose, you can increase the security of terminal session connections 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 25) 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.

For more information see these technical notes:

- 1557: Security Proxy Server Performance Factors (http://support.attachmate.com/techdocs/1557.html)
- 1883: End-to-End Encryption through the Security Proxy (http://support.attachmate.com/techdocs/1883.html)

### 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 35).
3. Create an encrypted terminal emulation session (page 35) 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.

## 3.2.1 Generating an Administrative Server Certificate

Before you run the Security Proxy Wizard, you must generate or import a certificate for the Adminsitrative 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 Management and Security Server manually, generate a certificate using Security Setup:

1. Start your servlet runner (page 45) and log onto the Administrative WebStation (page 45).
2. In Security Setup, click the **Certificates** tab.
3. Generate or import a certificate using the links in the Administer Management and Security 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 33.

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 Administrative Server.

## 3.2.2 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 Administrative 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 > Micro Focus Host Access Management and Security Server > Security Proxy Wizard. Alternatively, run the SecurityProxyServerWizard.exe file in the `[MssServerInstall]\securityproxy\bin\` folder.
- If you installed manually and completed the initial configuration (page 25), run the `[MssServerInstall]\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 `[MssServerInstall]/securityproxy/bin/securityproxyserverwizard` 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:

| Parameter | Description |
|---|---|
| `-locale [en\|fr\|de]` | Specify the language in which the wizard opens. For example, navigate to the Security Proxy Wizard folder (the default on Windows is `\securityproxy\bin`) and enter this command to start the wizard in French.<br><br>`SecurityProxyServerWizard -locale fr` |
| `-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.<br><br>`SecurityProxyServerWizard -serverproperties "C:\Program Files\Micro Focus\MSS\securityproxy\conf\server.properties"` |

## 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 Administrative 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 Administrative Server over the network.

   For evaluation purposes, import a trusted certificate from the Administrative 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 Administrative Server address, the Administrative Server (not the Proxy Server) port number, the servlet context, and the friendly name of the Administrative Server. The context name is used in the URL that accesses the Administrative Server, and it is often, although not always, the same as the folder within which the Administrative Server is installed. The default context name is `mss`. 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.

11 Export the settings to the Administrative Server. Click **Export Settings** on the **Proxies** tab. In the **Export Proxies** dialog box, specify or accept the default Administrative 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.

## 3.2.3 Running the Security Proxy

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

### Automated install

If you use the Windows automated installer, the Windows service for the Security Proxy Server starts automatically when installation is complete. You can start or stop the service by going to Windows Control Panel > Administrative Tools > Services, and selecting Micro Focus MSS Security Proxy.

For UNIX and Linux platforms, you can start and stop the service using the method that is appropriate to your platform. Use -start and -stop parameters (page 45) 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 MssSecurityProxy.exe (Windows) or MssSecurityProxy (UNIX and Linux) to start the servlet runner. It is located in [MssServerInstall]\securityproxy\bin (Windows) or [MssServerInstall]/securityproxy/bin (Linux).

**Windows**

1 `MssSecurityProxy -install.` This command installs MSS Server as a Windows service.

2 `MssSecurityProxy -start`

**UNIX/Linux**

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

2 `msssecurityproxy -start`

All the available parameters (page 45) for MssSecurityProxy.exe and securityproxy are identical to the Administrative Server's servlet runner.

## 3.2.4 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 Windows-Based Session** page, click the **Launch** button.

4 In the session window, on the **Connection** menu, click **Connection Setup**.

- 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.

### 3.2.5 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.

## 3.3 Metering Server

The Metering Server requires some additional setup before you can deploy metered terminal sessions. This optional component is included with Management and Security Server and can be installed using the automated installer.

Before you begin setting up metering, the Metering Server must be enabled (the default).

Metering can run on any supported web server with a servlet runner using Java 7 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.

---

**NOTE:** In most deployments, only one metering server is needed to support all clients. If more than one metering server is run, the metering report numbers must be manually combined.

The metering service does not support load balancing. Each emulation client must report directly to a single metering server.

---

## 3.3.1 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:

To enable metering for Windows-based sessions, you must configure client workstations to report to the metering server. You can either use the Installation Customization Tool to create a customized terminal emulation installation that includes metering configuration information, or if you are using Reflection, you can use Reflection's Group Policy settings to configure metering after installation.

### 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 45).
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 `meter`.
6. Select the **Use HTTPS** check box to enable a secure connection using HTTPS.
7. Click the **Add to Table** button.

## 3.3.2 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 45).
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 > Micro Focus Host Access Management and Security Server > 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/meter/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 38).

## 3.3.3 Configuring License Pools

1 Create (page 37) and then run your metered sessions. This automatically creates the product license pools.

2 Open (page 37) 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, for Management and Security Server version 12.2, 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 Management and Security Server topic.

7 Select the **Limit number of concurrent users to number of licenses** check box if you want to block users from running a client session or making connections when the number of concurrent users exceeds the number of licenses.

8 If license limits have been exceeded, the Administrative 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 39).) Enter e-mail addresses separated by commas. E-mail notifications can be sent if **Concurrent** is selected as the license type.

9 Select the **Limit connections** check box to prevent users from logging on to more than the number of hosts you specify in the field. This feature is available only for Reflection for the Web emulation sessions.

10 Click **Submit**. Repeat these steps for each Micro Focus 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.

## 3.3.4 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 45). 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 > Micro Focus Host Access Management and Security Server > Metering Reports.
- On other platforms or from a different machine, open a web browser and go to http://[metering server name]/meter/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 39).

### 3.3.5 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 37).

2 On the 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. The Administrative Server 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, Reflection for the Web 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.

## 3.4 Terminal ID Manager

After you purchase the add-on license for Terminal ID Manager, you have several installation options:

- Run the automated installer with the Terminal ID Manager Add-On file located in the same directory as the installer.
- Copy the Terminal ID Manager activation file to the Terminal ID Manager server, “[tidm context name]\WEB-INF\lib\modules”, and then restart the Terminal ID Manager application.

If. you use Management and Security Server’s automated installer to add Terminal ID Manager, a self-contained JRE and servlet runner are installed for you

Configure the Terminal ID Manager settings in the Terminal ID Manager console and in the Administrative WebStation. See “Setting Up Terminal ID Manager” on page 40 for more information.

**NOTE:** After installation, two Terminal ID Manager console options appear from the Start menu installation path:

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

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

Terminal ID Manager can run on any supported web server with a servlet runner using Java 7 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.

### 3.4.1 Setting Up Terminal ID Manager

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

If you installed the Terminal ID Manager using the automated installer, use the configuration steps below. For a manually installed version, first install the Terminal ID Manager (page 26) [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 Terminal ID Manager" in the Terminal ID Manager console. (On the Server Settings tab, click Help; then click the **Setup Instructions** link.)

1. Open the Administrative WebStation and configure the Terminal ID Manager settings. On the **Settings** tab, click **Terminal ID Manager** and provide the necessary information.
2. Populate the server with IDs, pools and association sets. Open the Terminal ID Manager console.
3. After completing the step to populate the Terminal ID management database, start the Terminal 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 **Terminal ID Manager** as the connection method.

   If available, 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 Terminal ID Manager console to review ID usage and release, reclaim, and hold IDs.

## 3.5 Removing Components

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

- All of the Management and Security Server components must be stopped to complete uninstallation. If you installed the product manually, stop the servlet runner and the Security Proxy (if added) 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 Management and Security Server directories are open in Windows Explorer (or other browser).
- If you plan to remove either the Administrative Server, the Terminal 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:

  ```
  [MssServerInstall]/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 MSSData directory. For more information about retaining settings, see “Upgrading from Reflection Security Gateway” on page 43.

# 4 Upgrading from Reflection Security Gateway

Host Access Management and Security Server version 12.2 is the upgrade from the predecessor product, Reflection Security Gateway 2014 R2.

(If you are upgrading from Reflection for the Web, refer to the Reflection for the Web Installation Guide (http://support.attachmate.com/product/?prod=RWEB).)

## 4.1 Directory Names and Installation Paths

A new installation of Micro Focus Host Access Management and Security Server applies different directory names than the predecessor product. When you upgrade from Reflection Security Gateway 2014, however, the automated installer will use the existing paths and folder names.

For example, the default installation path (on Windows) is

**the current path for an upgrade:** `C:\Program Files\Attachmate\ReflectionServer`

**the new path for a new installation:** `C:\Program Files\Micro Focus\MSS`

Although the installation folder names remain the same when upgrading, many files within the folders have been renamed. For example,

- Program Files\...\ ReflectionServer.exe was renamed MssServer.exe
- ProgramData\Attachmate\ReflectionServer\ReflectionData was renamed ProgramData\Micro Focus\MSS\MSSData

## 4.2 Automated Installation

When available, use an automated installer to upgrade to Management and Security Server.

The automated setup program will install the latest software and retain your current settings. You do not need to run a configuration upgrade utility or re-create your sessions.

## 4.3 Manual Installation

If you installed the predecessor 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 23) appropriate for your platform.

Then, run the Configuration Upgrade Utility to handle the upgrade of your settings.

Before you begin, make sure that:

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

# 5 Starting the Administrative WebStation

To start the Administrative WebStation:

1. If necessary, start the servlet runner (page 45). 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 > Micro Focus Host Access Management and Security Server > Administrative Server.) The URL uses this format:

   ```
   http://[host name]:[port number]/mss/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/mss/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 browser 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 list of links opens, which is empty until you configure sessions. (When you upgrade, your previously-configured sessions appear in the list.) Click the **Administrative WebStation** button at the bottom of the page.

## 5.1 Starting the Servlet Runner

Before you can run the Administrative WebStation, the Metering Server, or the Terminal 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 installation

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 Micro Focus MSS 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 installation

If you installed manually, run MssServer.exe (Windows) or mssserver (UNIX and Linux) to start the servlet runner. It is located in the Management and Security Server install directory.

**Windows**

1. `MssServer.exe -install.` This command installs Administrative Server as a Windows service.
2. `MssServer.exe -start`

**UNIX/Linux**

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

### Parameters

The parameters for the Administrative Server (MssServer) and the Security Proxy (an optional add-on) are identical. The available parameters are as follows:

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

You can also use JVM options to customize the servlet runner launcher (page 46).

## 5.2 Servlet Runner Launcher JVM Options

If you need additional customization when you start the servlet runner (page 45), you can adjust the JVM options. You can also use these options to start the proxy server (page 35).

To accomplish this, edit the MssServer.vmoptions file, which is found in the same directory as the launcher (for example, C:\Program Files\Micro Focus\MSS).

# 6 Installing Add-On Products

Management and Security Server can be used to manage Reflection ZFE and Reflection for the Web, and the functionality can be augmented with several add-on products, including

- Security Proxy
- Terminal ID Manager
- Automated Sign-On for Mainframe

These products require a separate installation. Based on your entitlements, continue with the steps to install and activate your product(s).

## 6.1 Installing a Product with an Activation File

After purchasing an add-on product, you will receive information about downloading the product. Security Proxy, Terminal ID Manager, and Automated Sign-On for Mainframe are downloaded as activation files, which have this format:

```
activation.<product_name>.jaw
```

1. Download the activation file and note the download destination.
2. In the Administrative WebStation, click Resources > About Management and Security Server.
3. On the About Management and Security Server page, beneath the box, click Browse or Choose File (depending on your browser).
4. Locate and select the activation file. Click Open.
5. Click Install to add the product.

   The new product is included in the list of Installed products, and the configuration settings are available on the add-on product's tab in the Administrative WebStation.
6. Restart your browser to ensure that the Administrative WebStation is fully updated with the new set of activation files. You do not need to restart the administrative server.
7. If you installed either Security Proxy Add-On or Terminal ID Manager Add-On, continue with these steps to activate the server installation.

### 6.1.1 To activate the Security Proxy Server:

1. Copy the activation file into the /securityproxy/lib/modules folder onto each machine where Security Proxy Server is installed.
2. Start the Security Proxy Server.

### 6.1.2 To activate the Terminal ID Manager:

1. Copy the activation file into the tidm/WEB-INF/lib/modules folder onto each machine where Terminal ID Manager is installed.
2. Restart the Terminal ID Manager servlet.

If the Terminal ID Manager servlet is running under Tomcat, then restart the Tomcat server. If the Terminal ID Manager is running under a different application server, follow the procedures for that application server to restart the Terminal ID Manager servlet.

3 If the Terminal ID Manager does not start, you may need to edit the rweb.properties file in the MSSData directory.

- To find the location of **MSSData**, go to the Administrative WebStation > Resources > About Management and Security Server. On the About page, look under **System information** for **MSSData path**.
- In the `rweb.properties` file, look for this line: `idmanagement.enabled=false`
- If the enabled value is `false`, change the value to `true`.
- Save the file, and then restart the Terminal ID Manager servlet as described above.

### 6.1.3 To activate Automated Sign-On for Mainframe:

In the Administrative WebStation, go to Settings > Automated Sign-On and open the Help file for guidance through the settings.

Note that your mainframe administrator needs to configure the DCAS server. An Administrator Guide is available with detailed procedures.

# Terms

**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.

**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.

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

**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 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.