Host Access Management and Security Server

Installation Guide

version 12.3

MICRO
FOCUS

Contents

Host Access Management and Security Server Installation Guide

The Host Access Management and Security Server Installation Guide is also available in Français and Deutsch.

The most up-to-date version of this guide is available online in English.

NOTE

- ***Update 1*** is now available. See the Release Notes for more information.
- After version 12.3, the PDF version of the Management and Security Server Installation Guide will no longer be included in the download package. Links will be provided to the guide online (for both HTML and PDF)

At a Glance:

About Management and Security Server

Host Access Management and Security Server provides an administrator the means to centrally secure, manage, and monitor users' access to host applications.

Management and Security Server can create host sessions for Micro Focus products including Reflection Desktop, InfoConnect, Reflection ZFE, Reflection for the Web, and Rumba.

This guide leads you through the steps to get up and running:

I. Basic Automated Installation
II. Add-On Products

Check the Installation Variations if your system requirements differ from the basic installation.

About Basic Automated Installation

Use the automated installer to install the basic components of Management and Security Server: **Administrative Server** and the **Metering Server**, which you can install at the same time or later.

You can create sessions and set secure connections right away. Then you can augment security and add other features by activating and configuring your licensed **Add-On Products**.

About Add-On Products

Use one or more Add-On Products to enhance Management and Security Server's functionality. The add-on products require separate licenses and additional installation or activation procedures. Add-on products include:

- Security Proxy Server
- Terminal ID Manager
- Automated Sign-On for Mainframe
- Micro Focus Advanced Authentication

If you are evaluating...

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 Introduction

From one central location, an administrator uses Host Access Management and Security Server to create, secure, configure, and monitor Windows terminal client sessions, Java-based browser sessions, and HTML5 sessions (that do not require Java).

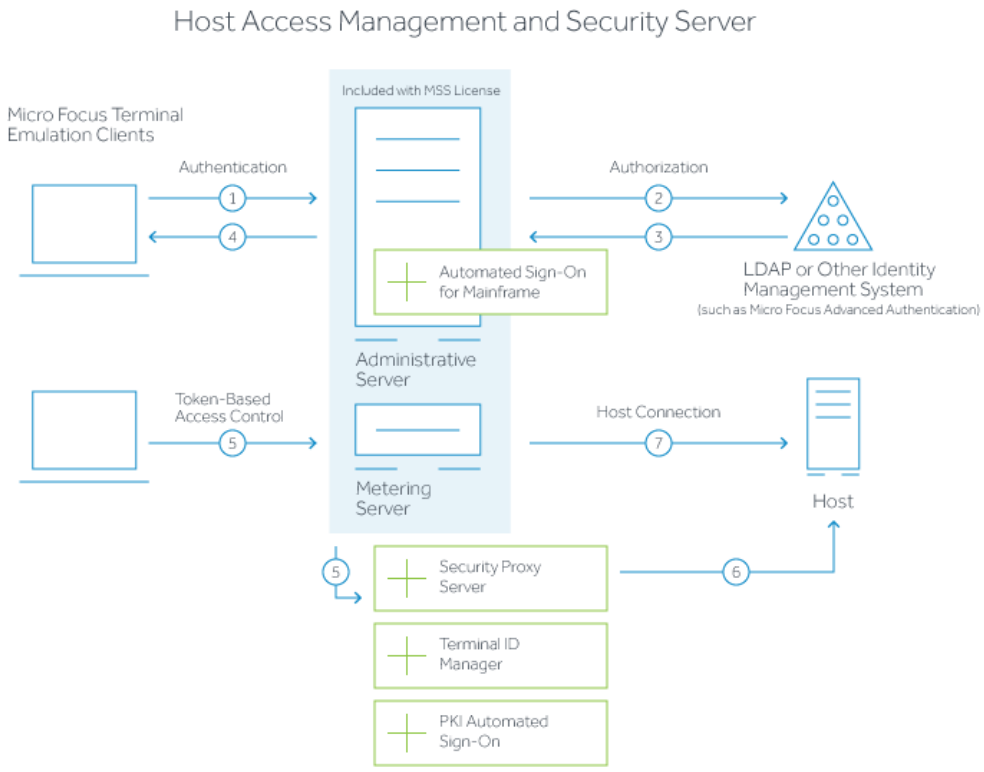
Secure access is delivered to applications on IBM, HP, Linux, UNIX, Unisys, and OpenVMS hosts.

In this chapter:

Overview of Management and Security Server

The overview diagram depicts the flow of secure interactions between a client and the host in a typical host session, including the option to use the Security Proxy Add-On (steps 5-6).

Other add-on products are also identified.



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 authorized 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 authorized user connects directly to the host.

Basic components

A basic installation of Management and Security Server includes the following components:

- Administrative Server
- Metering Server
- Configuration Utilities

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 configure and manage secure settings for those sessions.

The interface for the Administrative Server is the **Administrative WebStation**, where you configure and save settings.

Metering Server

Use the Metering Server to monitor the use of terminal sessions, including the ability to track the number of connections and total connection time per user. The Metering Server is included with Management and Security Server without needing a separate license.

You have the option to install the Metering Server either during or after the initial installation.

The Metering Server can be installed either on the same server as the Administrative Server or on another system. Before you can meter the use of terminal sessions, you must set up the metering server.

Configuration Utilities

While the automated installer handles most of the configuration, one or more utilities may be required after you complete the basic installation and configuration steps. See Appendix A: Configuration Utilities for more information.

Add-On Products

Management and Security Server's functionality can be augmented with add-on products. Each add-on product requires a separate license and may require separate installation and activation procedures. Add-on products include

- Security Proxy
- Terminal ID Manager
- Automated Sign-On for Mainframe
- Micro Focus Advanced Authentication

The add-on products are described briefly here. Installation and configuration steps are presented for each product separately.

Security Proxy

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. For details, see Setting up the Security Proxy.

Terminal ID Manager

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. For details, see Setting Up Terminal ID Manager.

Automated Sign-On for Mainframe

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. For details, see Setting Up Automated Sign-On for Mainframe.

Micro Focus Advanced Authentication Add-On

Advanced Authentication is a Micro Focus product that enables strong multi-factor authentication using a variety of authentication methods. This Add-On Product provides user authentication to Management and Security Server using Micro Focus Advanced Authentication.

For details, see Setting Up Micro Focus Advanced Authentication Add-On.

2 Preparing to Install

To get up and running with Management and Security Server, follow this two-part approach:

I. Basic Automated Installation. First, use the automated installer to install the basic components of Management and Security Server:

- Administrative Server (and its Administrative WebStation)
- Metering Server (could be installed later)
- Configuration Utilities

II. Add-On Products. Then, install (or activate) your licensed Add-On Products.

The system requirements and installation procedures for each add-on product are presented in the product-specific sections.

To prepare for installation, note the Prerequisite actions and the System Requirements.

NOTE: If the automated installer does not meet your needs, you can install Management and Security Server manually using multi-component manual installation files. See Manual Installation.

In this chapter:

Prerequisite Actions

Before you begin the automated installer, be sure to:

Shut down any currently running components.
Obtain the required user privileges.
Obtain the required account permissions.

Shut down any currently running components.

Before installing or upgrading, shut down any Management and Security Server (or its predecessor, Reflection Security Gateway) component that is currently running. (If you installed an earlier version with an automated installer, the automated installer will close components for you.)

Obtain the required user privileges

- **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 and click **Properties**. On the **Compatibility** tab, select the **Run this program as an administrator** check box, and then click **OK**.

- **On Linux or UNIX.** If you are installing on a Linux or UNIX 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. If you also require installation of the MSSData directory, which stores site-specific content, to a non-default location (/var/opt/microfocus/mss/mssdata), see Appendix B: Specifying the location of Configuration Information.

Obtain the required account permissions.

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, the account used to run the Administrative Server must have permission to write to the Java certificate authority certificates file (cacerts).

The default Windows location is

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

Note: If you are upgrading from version 12.1 or earlier, the location is

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

System Requirements

Check the requirements for the Administrative Server and the Browser before installing Management and Security Server.

Also check the requirements for the Metering Server and your Add-On Products.

Administrative Server Requirements

As the central component of Management and Security Server, the Administrative Server requires:

- **Server-class operating system**

  For production, a server-class system is required.
  For initial testing or evaluation, a workstation could be used.

- **Server running JRE 8 or later**

  JRE 8 is installed by the automated installer (or multi-component manual installation).

- **Servlet engine with Java servlet 2.3 and JSP 1.2**

  The automated installer installs a servlet engine by default.
  An application server, such as WebSphere, also meets the requirement.

- **Updated JCE Unlimited Strength Policy Files**

  These files are installed by the automated installer. No further action required.
  Apply these files when you manually install Management and Security Server.

These files must be applied *each time* you update your JRE.

For more information, see JCE Unlimited Strength Jurisdiction Policy Files.

Browser Requirements

A browser is required for the **Administrative WebStation**, and for users or administrators who use the Java-based login/links list applet to launch **client sessions**.

The browser must:

- use JRE 8 or later.
- run trusted applets.
- support JavaScript and cookies.

NOTE: No browser is required for users or administrators who launch Windows-based sessions from the desktop (such as Reflection Desktop v16 or Rumba).

Metering Server Requirements

The Metering Server requires:

- a server running JRE 8 or later.
- a servlet engine with Java Servlet 2.3 and JSP 1.2.

For descriptions, see the Administrative Server requirements.

Requirements for Add-On Products

System requirements for each add-on product are included in the specific sections:

Security Proxy Add-On

Terminal ID Manager Add-On

Automated Sign-On for Mainframe Add-On

Micro Focus Advanced Authentication Add-On

JCE Unlimited Strength Jurisdiction Policy Files

Each component that requires JRE also requires **Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files**.

If you use an automated installer or a multi-component manual installation 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.

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 Linux or 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.

3 Installing Management and Security Server: Basic Automated Installation

In this chapter:

If your system has other installation requirements, refer to the Installation Variations.

Basic steps

Begin with a basic installation of Management and Security Server. Using the automated installer is the simplest way to get up and running on Linux, UNIX, or Windows.

After the Administrative Server is installed and configured, you can start creating secure host sessions. Then, you can install and configure other components and add-on products.

A basic automated installation requires three steps:

1. Run the automated installer.
2. Enter configuration information.
3. Start services.

A basic automated installation assumes:

- The operating system is Linux, Solaris SPARC64, or Windows.
- A default servlet runner is installed.
- All components will be installed on the same machine.

  For initial testing, you can install on a workstation; however, we recommend installing on a server operating system for production.
- The Prerequisite actions have been performed.

Basic Automated Installation Procedures

The automated installer guides you through a series of questions to completely install, configure, and start the Administrative Server. Your Management and Security Server license includes the Metering Server, which you can install later, if preferred.

- Step 3: Start services
- Next steps

Step 1: Run the automated installer.

Automated installers are available for Linux, Solaris SPARC64, and Windows.

NOTE: After version 12.3, Management and Security Server will no longer provide installers for 32-bit systems.

To run the automated installer:

1 From your product download location, locate and run the automated installer for the operating system you are installing on. (In the file name, <nnn> is the build number.

Operating System	Automated Installer
Linux 64-bit	mss-12.3.<nnn>-prod-linuxx64.sh
Linux 32-bit	mss-12.3.<nnn>-prod-linuxia32.sh
Solaris SPARC64	mss-12.3.<nnn>-prod-solsparc64.sh
Windows 64-bit	mss-12.3.<nnn>-prod-wx64.exe
Window 32-bit	mss-12.3.<nnn>-prod-w32.exe

NOTE: The automated installer executable and activation jaw file MUST be in the same directory when the installer is run.

---

2 Select a **language** to be used only during installation.

No matter which language is chosen for the installation process, the installed product supports English, French, and German. Click Next to continue.

3 Read and accept the license agreement.

4 If upgrading, you are prompted to run the uninstaller. Click **OK**.

5 **Destination directory**: Accept the default installation directory, browse to a new directory, or enter the directory where you want to install.

NOTE: When upgrading from version 12.2, the MSSData directory is preserved you do not need to re-create your sessions. If upgrading from version 12.1 or earlier, the ReflectionData directory is copied from the previous location to MSSData, and session data is preserved.

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 and the Metering Server. A default servlet runner is automatically installed.

7 **Start Menu** directory: On Windows, select the directory where you want 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 directory.

8 The automated installer copies files to the designated directory and launches a configuration utility. Continue with Step 2: Enter configuration information.

Step 2: Enter configuration information.

If you are installing Management and Security Server for the first time on this machine, the automated installer starts the Initial Configuration Utility. For a description, see Initial Configuration Utility.

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

Enter or verify your configuration information.

1. **Installation Directory:** Confirm the location where the Administrative Server was installed. If the default value is not correct, browse to the correct location.
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. If entitled, you can optionally choose to install the Security Proxy server.
3. **Volume Purchase Agreement number:** Optional. Enter the Volume Purchase Agreement (VPA) number. You can modify the VPA number later in the Administrative WebStation.
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. **Security 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 and to administer Metering and Terminal ID management (if installed). You can create different passwords for each server later.
7. **Server Names for URLs and Certificates:** The 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.
8. **Server certificates: organization and locality** (optional)

   This panel includes additional information for creating certificates.

   Organizational Unit: Enter the name of your organizational unit, typically the name of your department or division.

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

   City or Locality: Enter the full formal name (no abbreviations).

   State: Enter the full formal name (no abbreviations).

   Country: Provide a two-letter ISO country code, such as US.
9. **Confirm Configuration:** Click **Next** to apply the specified configuration changes.
10. **Configuration summary:** A summary of the configuration changes is created in InitalConfigurationUtility.log in the logs directory under the installation directory. Click **Done** to continue with Step 3: Start Services.

Step 3: Start services

After completing the configuration, you are returned to the installer to select startup options.

NOTE: About IIS. If you installed Management and Security Server on Windows, the automated installer detects whether IIS is installed on your machine and offers to integrate IIS with Management and Security Server. You can run the IIS Integration Utility later, if preferred. For more information, see IIS Integration Utility.

---

1. **Start Services:** Start the server components.

   If you used the automated installer, the servlet runner is installed as a service and started automatically. If you need to manually start or stop the service, see Starting Services.

2. **Installation Complete.**

   After installing the Administrative Server, you can run the Administrative WebStation from any computer with a web browser. For example, go to the URL specified on the automated installer panel:

   `http://[server name][:port]/mss/AdminStart.html`

   Specify the port number if different from 80, the default.

   (On Windows, you can open the Administrative WebStation from the Start menu.)

Next steps

At this point, the installation is complete. You can begin using the Administrative WebStation to create and configure sessions. Your next steps:

1. Starting the Administrative WebStation.
2. Configuring the Administrative Server.

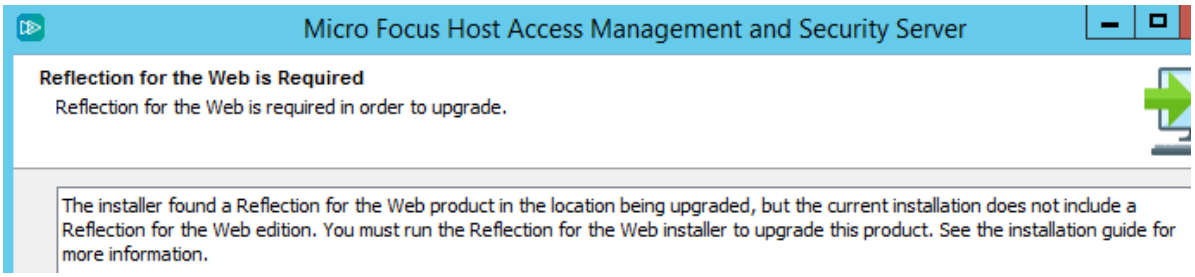
When ready, you can configure the Metering Server, or install and configure your Add-On Products. As a next step, you might:

- Set up Metering
- Set up Security Proxy Add-On
- Set up Terminal ID Manager Add-On
- Set up Automated Sign-On for Mainframe Add-On
- Set up Micro Focus Advanced Authentication Add-On

Troubleshooting

If you encounter this error while running the MSS installer, choose an option to resolve the issue.

Error: Reflection for the Web is Required.



Reason: Reflection for the Web is installed on this machine, and you are attempting to upgrade to a product other than Reflection for the Web. As a result, you will lose the ability to create and use Reflection for the Web Java-based sessions.

Resolution options:

- To *keep* the Reflection for the Web functionality, first *install* (or *upgrade*) Reflection for the Web, and then install the other product.
- To *remove* the Reflection for the Web functionality, first *uninstall* Reflection for the Web, and then install the other product.

Installation Variations

If the basic automated installation approach needs to be modified for your system, consider these variations:

- Installing on UNIX with no JRE
- Servlet runner other than Apache Tomcat
- Using SiteMinder
- Using the automated installer in console mode
- Unattended installation
- Manual installation

Installing on UNIX with no JRE

Use this option if your UNIX platform (such as z/OS, Mac, HP-UX, non-SPARC Solaris, and other Linux systems) requires a version of a Java Runtime Environment (JRE) other than the one provided by the installer.

No JRE is installed with these installer files.

1. Look in your download location for an installer with `nojre` in the filename. For example:

   Automated installer: `mss-12.3.<nnn>-prod-unix-nojre.sh`, where `<nnn>` is the build number.

   Manual installer: mss-prod-unix-nojre-manual.tar.gz
2. Proceed with the installation, using your existing JRE.

Servlet runner other than Apache Tomcat

If you use a servlet runner other than the default Tomcat servlet runner, such as IBM WebSphere, you must manually install the Management and Security Server components. For details, see Manual Installation.

Configure Management and Security Server as a web application, following the instructions provided by your servlet runner

Using SiteMinder

If you are using SiteMinder, you may need to update the server's path reference to the SiteMinder native libraries.

In MSS/server/conf, inspect the property named `wrapper.java.library.path.2` in the `container.conf` file. Verify that its value matches the path to the SiteMinder native libraries on your system. For example:

```
wrapper.java.library.path.2=C:/Program Files/CA/webagent/win64
```

If a change to this property is required, you must restart the server for those changes to take effect.

Using the automated installer in console mode

You can also run the installation tool in console mode for non-Windows systems. Console mode enables you to use a command line for input and output rather than a graphical user interface (such as X Windows).

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.

To use Console Mode: Run the automated installer executable for your platform with a `-c` parameter.

You can also run the Initial Configuration Utility and the Configuration Upgrade Utility in console mode.

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 “Appendix A. Configuration Utilities” on page 65, which are optional for many upgrade scenarios.

To use Unattended Installation:

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. The file is located in `[MssServerInstall]\.install4j\response.varfile`

2. Copy `response.varfile` to another machine where you would like to install Management and Security Server.
3. Locate the appropriate executable (listed in Step 1: Run the automated installer) 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 `<12.3.nnn>` is the product version and build number:

```
mss-<12.3.nnn>-prod-linuxx64.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."

Manual installation

If you are unable to use an automated installer, you can use multi-component installation files to manually install Management and Security Server. See the Manual Installation section.

4 Starting the Administrative WebStation

The Administrative WebStation is the interface for the Administrative Server, the central component of Management and Security Server. Use the Administrative WebStation to create, configure, and manage secure terminal emulation sessions for your users.

To start the Administrative WebStation:

1. If necessary, start the servlet runner. You can skip this step 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]/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.

Starting Services

Before you can run the Administrative WebStation, the Metering Server, or the Terminal ID Manager, the MSS Server must be started. **If you used the automated installer**, a servlet runner was installed and started by default. (You can skip this step.)

If you are using a servlet runner other than the default, refer to its documentation to start and stop the servlet runner.

Options for starting the servlet runner:

- “For an automated installation” on page 26
- “For a manual installation” on page 26
- “Servlet Runner Launcher JVM Options” on page 26

For an automated installation

If you used an automated installer, follow these steps to start or stop the service.

- **On Windows:** Open Windows Services. Right-click **Micro Focus MSS Server** and select **Start** (or Stop).
- **On Linux and UNIX:** The administrator must configure init scripts to start the MSS Server on startup.

For a manual installation

If you installed manually, start the servlet runner by using the following files, located in the Management and Security Server install directory.

On Windows

1. `server\bin\server.bat`
2. To install the Windows service: `install-server-service.bat`
3. To uninstall the Windows server: `uninstall-server-service.bat`

On Linux or UNIX

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

   `server/bin/server`

Servlet Runner Launcher JVM Options

If you need additional customization when you start the servlet runner, you can adjust the JVM options. To do so, edit the `container.conf` file, which is in the `server\conf` directory.

For example, `C:\Program Files\Micro Focus\MSS\server\conf`

5 Configuring the Administrative Server

Use the Administrative WebStation to configure settings for the Administrative Server. Begin with these basic settings:

1. Open the Administrative WebStation, either from the Windows Start menu, or the URL provided at the end of installation. The Home page displays.
2. Open **Settings** (from the left nav). On the **General** tab, enter your preferences. Open **Help** for more information. Then, click **Save Settings**.
3. Open **Security Setup**. On the **Security** tab, find the **Require new login** field. Change the default to a higher number to avoid a session timeout while you are configuring settings.

As you begin to work with the product features, refer to the Overviews, the References, and the individual Help files for assistance.

Next Steps

When ready, you can configure the Metering Server, or install and configure your Add-On Products. As a next step, you might:

Set up Metering
Set up Security Proxy Add-On
Set up Terminal ID Manager Add-On
Set up Automated Sign-On for Mainframe Add-On
Set up Micro Focus Advanced Authentication Add-On

6 Upgrading to Version 12.3

To upgrade to Host Access Management and Security Server version 12.3, consider whether your previous version was installed with an automated installer or by manual installation.

Note: Version 12.3 Update 1 is available. See the Release Notes for more information.

Product Download Files

Your list of entitlements on the Micro Focus | Attachmate download site includes **Product files** and **Activation** files.

Product files. The Host Access Management and Security Server product files are available for download. Find the automated installer or multi-component installation files for the platform where Management and Security Server will be installed. Note that version 12.3 Update 1 is available.

Activation files. Add-On products are installed and enabled by using activation files, which are in this format: `activation.<product_name>.jaw`. Your entitled Add-On Product activation files are available from the same download location as your product files.

Be sure to check the Version Compatibility Requirements.

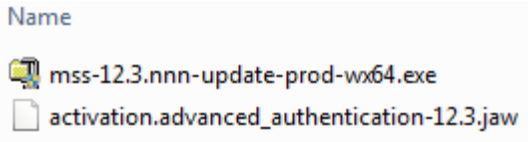
Version Compatibility Requirements

During installation, the Management and Security Server (MSS) installer detects your previously installed Add-On products, such as Advanced Authentication. The activation files for those products must be version-compatible with the version of Management and Security Server being installed.

To ensure the add-on products will be enabled, you may need to install version-compatible activation files. The easiest way to install the activation files is by running the MSS installer. Follow these steps:

1. Download the activation file for the version of your add-on products from the Micro Focus | Attachmate download site (where you downloaded Host Access Management and Security Server).
2. Place each activation file in the directory with the MSS installer.

   For example, if your machine is Windows 64-bit, place the activation file in the same folder as the installer: `mss-12.3.<build>-update-prod-wx64.exe`.



3 Run the MSS installer.

If you run the MSS installer and incompatible versions are detected, you will be prompted to **Cancel** the installation and install the activation files (as above) before resuming.

Automated Installation

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

To upgrade using the automated installer:

1 Run the automated installer to upgrade the Administrative Server.

The automated installer retains your current settings. You do not need to run a configuration upgrade utility or re-create your sessions.

2 Upgrade your Add-On Products, as needed.

Manual Installation

If you installed the predecessor product using a multi-component manual installer, you can use the same approach again. To upgrade a manual installation:

1 If you used the servlet runner included with the product, extract the multi-component manual installation file appropriate for your platform.

2 Plan to install the new manual multi-component product version into a different folder than the earlier installation (that is, side by side).

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

NOTE: If you are manually upgrading Reflection for the Web, see To complete a Reflection for the Web upgrade.

Configuration Upgrade Utility

When manually upgrading Management and Security Server, use this utility to:

- enable the services for this Administrative Server.
- copy the Administrative Server keystore from the previous location to the new location if necessary.
- copy the MSSData (or ReflectionData) directory from the previous default location to the new default location (if a custom location was not configured).
- copy Security Proxy Server configuration files (if enabled) from the old install directory to the new install directory.,
- update port values in configuration and HTML files.

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

Before you begin:

1. Make sure the earlier version of the software is not running when you run the Configuration Upgrade Utility. Doing so will avoid potential port conflicts and allow you to accept default port assignments.
2. If you are upgrading a Linux or UNIX system, make sure that no startup scripts are running.
3. Verify that you have administrator privileges. If not, you will be prompted for credentials.
4. Uninstall the services, such as the MSS Server and MSS SecurityProxy.

Run the utility:

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 66).
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.

After you run the CUU:

1. Install and start the 12.3 services that you uninstalled before you began (such as MSS Server and MSS SecurityProxy).

To complete a Reflection for the Web upgrade:

If you are manually upgrading Reflection for the Web, you must install `rweb-client.war` to create a web application context.

To install `rweb-client.war`:

1. In your Reflection for the Web download location, open the `install_manual\components` directory.
2. 2 Locate and copy `rweb-client.war` to this MSS `webapps` folder:

   `<MSS install directory>\server\web\webapps`

   The servlet runner will expand the war file and an rweb-client context will be created.
3. Start (or restart) the MSS Server.

Upgrading Add-On Products

The version number of each Add-On Product needs to match the version number of Management and Security Server. That is, when you upgrade to Management and Server version 12.3, you must download and install version 12.3 of your Add-On Product(s).

BEFORE YOU UPGRADE Management and Security Server, see the Version Compatibility Requirements.

NOTE: Your entitled Add-On Product activation files are available from the same download location as the product files.

Directory Names and Installation Paths

If you are upgrading from version 12.1 or earlier, a new installation of Micro Focus Host Access Management and Security Server creates different directory names than the predecessor product.

When upgrading from Reflection Security Gateway, the automated installer uses the existing paths and directory names. Compare the current path to the new default installation path (on Windows):

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 directory names remain the same when upgrading, many files within the directories have been renamed. For example,

- `ReflectionServer.exe` was changed to `server\bin\server.bat`
- `ProgramData\Attachmate\ReflectionServer\ReflectionData` was changed to `ProgramData\Micro Focus\MSS\MSSData`

7 Setting Up Metering

The Metering Server enables you to audit and control access to host sessions. The Metering Server is included with Management and Security Server and is installed using the automated installer on the same machine as the Administrative Server.

Once installed, the Metering Server requires some additional setup before you can deploy metered terminal sessions.

In this chapter:

Metering: Prerequisites and System Requirements

Before you can create metered sessions, verify that:

- Metering Server is installed and added to the Administrative WebStation. (The automated installer adds the Current Metering Server by default. See Settings > Metering tab.)
- Server running JRE 8 or later (installed by the automated installer).
- Servlet engine with Java servlet 2.3 and JSP 1.2 (installed by the automated installer).

  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.

Creating Metered Terminal Sessions

Follow these steps to create metered sessions.

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.
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.

To enable metering

- For Windows-based sessions

  Refer to Technical Note 2392 (http://support.attachmate.com/techdocs/2392.html) for steps to enable metering for Windows-based sessions.

- For Web-based sessions

  1. In the Administrative WebStation table of contents, click Session Manager.
  2. Click the Add button after selecting a session type or click an existing session name to edit. it
  3. On the Configure a Session page, click Launch.
  4. In the emulation window, open Administration > Metering Setup.
  5. Select the **Enable usage metering** check box, and make sure the correct metering server is selected in the **Metering web server** box.

     The **Require metering host** check box is cleared by default so that connections are made even if the metering server is unavailable. Select this check box if you want connections to be made only when the metering server is available.
  6. Click OK, close the emulation window, and save your changes.

Using 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 if it is not already running.
2. Open the Metering Administration tool:

   On Windows, go to 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** (that you set during installation), and click **Submit**.

   If you installed manually, type in the default password, `admin`. You can change this password later.

4. Continue with Configuring License Pools.

Configuring License Pools and Server Settings

A license pool comprises the licenses for a given product name, type, and VPA number.

After you install the Metering Server and configure metered sessions, the first time a client requests a license from a pool, it is automatically added to the metering server list of License Pools.

1. Open the Metering Administration tool, if it is not already open, and log in.

   When you ran your metered product, the Product, Product type, and VPA number were specified, and appear here as static text, along with the number and type of licenses and the type of enforcement, if any.

2. Click **Configure** if you wish to change the **Server Settings**, including your password, logs, and email notifications. Open **Help** for details.
3. To change a product's metering settings, click that product link, and edit the **License Pool** settings. Click **Help** for details.
4. 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.

Viewing Metering Reports

To view reports about metering activity:

1. Start the servlet runner, if it is not already running.
2. Reports can be viewed from the Administrative WebStation or from the metering reports tool.
   - In the Administrative WebStation, click **Reports** > **Metering**. Verify or select your metering server, and click **Show Report**.

     -- or --
   - Open the Metering Reports tool. From the Windows Start menu, go to **Metering Reports**.
   - On other platforms (or from a different machine), go to

     `http://[metering server name]/meter/ReportsLogin.do`.
3. If prompted, enter your password you specified during installation.
4. Several different reports can be configured from this page. For detailed information about each report, click **Help**.

NOTE: If more than one metering server is run, the metering report numbers must be manually added together.

8 Installing Add-On Products

Management and Security Server's functionality can be augmented with one or more Add-On Products. Each add-on product requires a separate license and separate installation or activation.

Refer to the specific chapters for instructions about installing and activating your Add-On Product(s):

- Setting up Security Proxy
- Setting up Terminal ID Manager
- Setting up Automated Sign-On for Mainframe
- Setting up Micro Focus Advanced Authentication

Installing a Product using an Activation File

After purchasing an add-on product, you will receive information about downloading the product as an activation file, which has this format:

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

General procedure

Activation files can be installed using the *About Management and Security Server* page in the Administrative WebStation. The Help topic on that page provides detailed instructions.

To install an Add-On Product:

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.

Further configuration:

Each Add-On Product requires further activation or configuration. For details, refer to the appropriate chapter for your add-on product(s).

9 Setting Up the Security Proxy

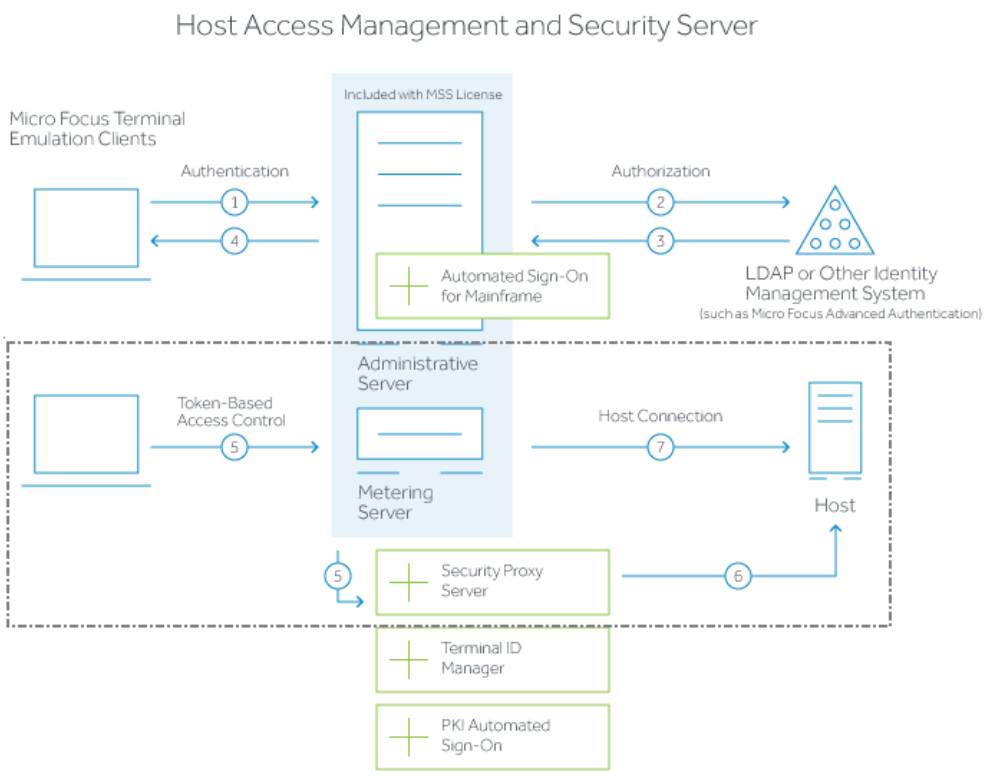
The Security Proxy Add-On requires a separate license. To use the Security Proxy, follow the steps to install, activate, and configure the product.

In this chapter:

Brief Overview

The Security Proxy provides token-based access control and encrypted network traffic to and from user workstations.

The following diagram highlights the Security Proxy (steps 5 and 6) in the context of the overall Management and Security Server set up.



When the Security Proxy Server is configured for use by a session, steps 5 and 6 apply:

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 authorized client.

   .....

5. When the **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 session token.
6. The **Security Proxy Server** validates the session token and establishes a connection to the specified host:port.

   The security proxy encrypts the data before forwarding it back to the user.

   .....

7. When no Security Proxy is present or a session is not configured to use it, the authorized user connects directly to the host.

Security Proxy Server: Prerequisites and System Requirements

Before installing the Security Proxy Add-On, verify that:

- Management and Security Server (the Administrative Server) is installed.

- Security Proxy Add-On activation file is available.
- Server running JRE 8 or later (installed by the automated installer).
- Servlet engine with Java servlet 2.3 and JSP 1.2 (installed by the automated installer).

Deploying a Secure Session

To deploy a secure session through the Security Proxy, the administrator must:

1. Install the Security Proxy server files on your server.
2. Start the Security Proxy server.
3. Create an encrypted terminal emulation session using the Session Manager in the Administrative WebStation. Then, map the secure session(s) to your authorized users.
4. Once the sessions are deployed, you can run reports to monitor the Security Proxy server activity.

Step 1: Install the Security Proxy Server.

Use the automated installer to install and configure the Security Proxy Server and generate the required trusted certificates so you can begin creating secure sessions.

The steps guide you through using the automated installer. However, if you cannot use the automated installer, manual installation is available, which requires several configuration steps.

NOTE: If you install the proxy server directly on the host computer, connections will be highly secure but CPU-intensive because additional processing is required to encrypt and decrypt the data stream.

Use the automated installer.

You can use the automated installer to install the Security Proxy either *when* or *after* you install the Administrative Server. The automated installer both installs and configures the Security Proxy.

To install the Security Proxy ***when*** you install the Administrative Server:

1. Verify that the Security Proxy Add-On license is available.
2. Start the automated installer for your platform.
3. During installation, select the check box for the Security Proxy.

   After the automated installer runs, the Initial Configuration Utility generates cryptographic keys and self-signed certificates, automates configuration, and sets a port value for the Security Proxy.
4. Continue with Step 2: Run the Security Proxy.

To install the Security Proxy ***after*** you install the Administrative Server:

1. Re-run the automated installer (as above), and select ***only*** the Security Proxy. When prompted, run the Initial Configuration Utility.

   -- or --

   use the steps below to install the activation file and then activate the server.
2. Activate the Security Proxy Server:

Copy the security proxy activation file into the `/securityproxy/lib/modules` directory on the machine where Security Proxy Server is installed.

3. Start the Security Proxy Server.
4. Continue with Step 2: Start the Security Proxy.

Install the activation file and then activate the server.

To add install the Security Proxy Add-On ***after*** you install the Administrative Server, use the Administrative WebStation to install the Security Proxy activation file on the designated server.

Then, you must activate that server. Follow these steps:

1. After purchasing the Security Proxy Add-On, download the activation file:

   ```
   activation.security_proxy-12.3.jaw
   ```

   Note the download location.
2. In the Administrative WebStation, click **Resources** > **About Management and Security Server**.
3. Beneath the box on the About Management and Security Server page, 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 **Security Proxy Add-On** is included in the list of Installed products, and can be configured in the Administrative WebStation: **Security Setup** > **Security Proxy** tab.
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 (MSS Server) service.
7. Activate Security Proxy Server:

   Copy the security proxy activation file into the `/securityproxy/lib/modules` directory on the machine where Security Proxy Server is installed.
8. Start the Security Proxy Server.
9. Continue with Step 2: Start the Security Proxy.

Step 2: Start the Security Proxy.

If the automated installer was used to install the Security Proxy on the same machine as the Administrative Server, the automated installer already

- configured the Security Proxy.
- generated the certificates to establish trust between the Security Proxy and the Administrative Server.
- started the Security Proxy service.

Continue with Step 3: Create Secure Sessions.

If you need to start or stop the Security Proxy service later, follow these steps.

- **On Windows.** Open Windows Services, and select **Micro Focus MSS Security Proxy**.
- **On Linux or UNIX platforms.** The administrator must configure init scripts to start the Security Proxy server on startup.

Step 3: Create and Map Secure Sessions.

You are ready to configure emulation sessions to connect to the host through the Security Proxy.

1. In the Administrative WebStation, open **Session Manager**. Click **Add**.
2. Select a **Session type** and enter a **Session name**. Click **Continue**.

   Or, click an existing session name to add security.
3. **Launch** the session.
4. Open the **Connection Setup** dialog. (You may need to Disconnect first.)
5. In the Connection Setup dialog:
   - **5a** Click the TLS/SSL button (or tab).
   - **5b** Select the Encryption level, such as *TLS 1.2, TLS 1.0, SSL 3.0.*
   - **5c** In the TLS/SSL settings dialog, check the **Use security proxy** box.
   - **5d** Select a Security proxy.
   - **5e** Enter the **Destination host** (and port, if not the default). Click **OK** to close the dialog.
   - **5f** Close the session window. Click **Save/Exit** to save your changes and return to the Administrative WebStation.

   The new (or existing) secure session is listed in the Session Manager. Repeat as needed to create more secure sessions.
6. Map the secure session(s) to your authorized users. Refer to the **Access Mapper** Help for details.

You can view reports to monitor the usage of the security proxy server.

Step 4: View Security Proxy Reports.

To monitor Security Proxy Server activity:

1. Check to be sure that the Security Proxy is running.
2. In the Administrative WebStation, open **Reports** > **Security Proxy Server**.
3. Select the **Security proxy server** that is currently running.
4. Select the **Report type** to show activity for the selected server. The results display on this page. Click Help for details about each report type.

- **Current activity**

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

  Shows details about security proxy server events, such as when the proxy server was started and stopped, any connection attempts, and the IP addresses that made them.
- **Current activity from all proxy servers**

  Shows the total current connections for all configured security proxy servers.

If you experience problems with the Security Proxy server, Technical Support may ask for information from the activity log file to aid in troubleshooting. By default, Error, Warning, and Info messages are logged. To change the types of information logged, use the Security Proxy Wizard.

Manual Installation: Security Proxy

If you are licensed for the Security Proxy Add-On, and unable to use the automated installer, you can install the Security Proxy Server using the multi-component manual installation file for the appropriate platform.

The multi-component file can be used whether you are using the default or another servlet runner for the Administrative Server.

To manually install and configure the Security Proxy, follow these steps:

A. Install the Security Proxy file.

1 From your download directory, locate the `securityproxy` installation file for your platform.

Operating System	Manual Installation File
Linux 32-bit	securityproxy-prod-linuxx64-manual.tar.gz
Linux 64-bit	securityproxy-prod-linuxia32-manual.tar.gz
Solaris SPARC64	securityproxy-prod-solsparc64-manual.tar.gz
UNIX	securityproxy-prod-unix-nojre-manual.tar.gz
Windows 64-bit	securityproxy-prod-wx64-manual.zip
Windows 32-bit	securityproxy-prod-w32-manual.zip

2 Extract the file into any directory. The default path for an automated installation is:

`[MssServerInstall]\securityproxy`

NOTE: To use the `-nojre-` installation package, verify that:

- JRE 8 or higher is already installed.
- the JCE Unlimited Strength Jurisdiction Policy Files are applied.

3 After the Security Proxy Add-On is installed, some setup is required before you can deploy encrypted sessions.

Next step: Generate or import an Administrative Server certificate.

B. Configure the Security Proxy.

The Security Proxy Server uses files generated by the Security Proxy Wizard or the automated installer to manage the encrypted connections that pass through the Security Proxy.

The Security Proxy cannot be run until the server is configured.

Use the Security Proxy Wizard to configure the Security Proxy server. (When available, the automated installer will configure the Security Proxy Server.)

About the Security Proxy Wizard

If you installed Management and Security Server and the Security Proxy manually, you must run the Security Proxy Wizard before you can run the security proxy server or create encrypted sessions. After the initial configuration, use the Security Proxy Wizard to manage your security proxy settings and certificates.

The Security Proxy Wizard:

- generates or imports the certificate used to authenticate the Security Proxy Server.
- sets up a `server.properties` file that contains information about each security proxy connection.
- imports the certificate from the Administrative Server -- if you are using authorization to determine access levels.

NOTE: When using the **automated installer**, the Security Proxy Server is configured, and you can skip this step. You can run the Security Proxy Wizard later to change settings or manage certificates.

Using the Security Proxy Wizard

1. Start the Security Proxy Wizard based on where you installed the product.

   On Windows: run `[MssServerInstall]\securityproxy\bin\SecurityProxyServerWizard.exe`

   On Linux or UNIX:

   - The Security Proxy Wizard requires an X11 window to display its graphical interface. Use the console of an X window or an X session, and open a terminal window.
   - Run the executable:

     `[MssServerInstall]/securityproxy/bin/SecurityProxyServerWizard`
2. The wizard opens with the **Status** tab in focus. Choose whether to open an existing `server.properties` file or to create a new one for this Security Proxy server.
3. Continue with the **Trusted Certificates** and **Proxies** tabs. Confirm or enter the required information.

   Refer to the **Help** on each tab for more information.
4. On the **Proxies** tab, click **Export Settings** to export the settings to the Administrative Server. Specify or accept the default Administrative Server, Port, and Context. Click **Export**.
5. When `server.properties` is configured, click **Exit** to close the wizard and save your settings. You may need to restart the Security Proxy service.

To make changes to the security proxy server settings later, simply re-run the Security Proxy Wizard.

C. Start the Security Proxy

After a `server.properties` file is configured for the Security Proxy server (by using the automated installer or the Security Proxy Wizard), start the Security Proxy Server:

On Windows: `[MssServerInstall]\securityproxy\bin\MssSecurityProxy.exe`

On Linux or UNIX: `[MssServerInstall]/securityproxy/bin/MssSecurityProxy`

To install as a service:

1. Change to your MSS install directory.
2. Then use a parameter.
   - **On Windows:**

     ```
     MssSecurityProxy.exe install
     MssSecurityProxy.exe start
     ```

   - **On Linux or UNIX:**

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

     ```
     MssSecurityProxy start
     ```

At this point, the installation and configuration are complete. You are ready to create secure sessions.

D. Next steps

After you manually install, configure, and start the Security Proxy, you are ready to create and map secure sessions. Then, you can monitor the security proxy activity with the Administrative Server.

The steps are the same whether you use an automated installer or manual installation. See:

- Step 3: Create secure sessions.
- Step 4: View Security Proxy Reports

Optional: Increased security

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 Security Proxy server is encrypted, data between the Security Proxy server and the host computer is typically not encrypted.

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 Security Proxy server and the host computer.

You may want to consider a dedicated connection between the Security Proxy server and the host computer, so that the Security 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 Security Proxy server directly on the host computer. A variety of platform-specific multi-component installation files 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 Security 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)

10 Setting Up Terminal ID Manager

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 Add-On requires a separate license. To use Terminal ID Manager, follow the steps to install, activate, and configure the product.

In this chapter:

Terminal ID Manager: Prerequisites and System Requirements

Before installing the Terminal ID Manager Add-On, verify that:

- Management and Security Server is installed.
- Terminal ID Manager Add-On activation file is available.
- Server running JRE 8 or later (installed by the automated installer).
- Servlet engine with Java servlet 2.3 and JSP 1.2 (installed by the automated installer).

Step 1: Install Terminal ID Manager.

The Terminal ID Manager Add-On requires an activation file to be installed on the same server as the Administrative Server.

Install the Terminal ID Manager activation file.

To install Terminal ID Manager *after* you install Management and Security Server:

1. After purchasing Terminal ID Manager Add-On, you will receive information about downloading the product activation file:

   `activation.terminal_id_manager-12.3.jaw`
2. Download the activation file and note the location.
3. In the Management and Security Server, open the Administrative WebStation and click **Resources** > **About Management and Security Server**.
4. Beneath the box on the About Management and Security Server page, click **Browse** or **Choose File** (depending on your browser).
5. Locate and select the activation file. Click **Open**.

6 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 Terminal ID Manager tab in the Administrative WebStation (Step 3).

7 Restart your browser to ensure that the Administrative WebStation is fully updated with the new activation file. You do not need to restart the administrative server.

8 Continue with Step 2: Activate the server.

Or, re-run the automated installer.

You can use the automated installer to install Terminal ID Manager either *when* or *after* you install the Administrative Server.

1 Copy the activation file into the same directory as the automated installer (that was used to install Management and Security Server).

2 Run the automated installer on that same machine to install only Terminal ID Manager.

   The automated installer places the activation file in the correct location.

3 Continue with Step 2: Activate the server.

Step 2: Activate the server.

Next, you need to activate the server the Terminal ID Manager will run on.

1 Copy the Terminal ID Manager activation file to the `msstidm/WEB-INF/lib/modules` directory on each machine where Terminal ID Manager is installed.

2 Restart the Terminal ID Manager servlet.

   If the Terminal ID Manager servlet is running under the default servlet runner, then restart the Administrative 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:

   3a On the **About** page, look under System information to find the **MSSData path**.

   3b In the `rweb.properties` file, look for this line:

   idmanagement.`enabled=false`

   3c If the enabled value is `false`, change the value to **`true`**.

   3d Save the file, and then restart the Terminal ID Manager servlet as described above.

Step 3: Configure Terminal ID Manager.

Before you can deploy terminal sessions that use a **Terminal ID Manager** connection ID, the Terminal ID Manager must be set up.

After installation, first configure the Terminal ID Manager settings in the Administrative WebStation, Then, use the Terminal ID Manager console options for Administration and Monitoring.

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

To configure the Terminal ID Manager:

1. In Administrative WebStation, go to **Settings** > **Terminal ID Manager** tab. Enter the required information.
2. Open the Terminal ID Manager by either
   - **2a** Clicking the name of the Terminal ID Manager
   - **2b** From the Start menu, click **Terminal ID Management Administration**.
3. Populate the server with IDs, pools and association sets.

   Refer to the Help files for assistance.
4. After completing the steps to populate the Terminal ID management database, start the Terminal ID Manager console
5. On the **Server Settings** tab, confirm that
   - the database input is valid.
   - the Terminal ID Manager is available for sessions configured to use the **ID Manager** as the connection method.
6. 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.

11 Setting Up Automated Sign-On for Mainframe

Automated Sign-On for Mainframe enables you to configure user access to z/OS mainframe applications using a single login, such as a smartcard.

In this chapter:

Brief Overview

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.

The configuration for Automated Sign-On for Mainframe requires an administrator to:

- Activate Automated Sign-On for Mainframe.
- Configure the z/OS mainframe.
- Create and configure an IBM 3270 mainframe session.
- Set up and store mainframe user mappings.
- Configure settings in the Administrative WebStation.

Automated Sign-On for Mainframe: Prerequisites and System Requirements

Before installing or configuring Automated Sign-On for Mainframe, the following requirements must be met:

- Management and Security Server (the Administrative Server) is installed.
- Terminal emulation software, such as Reflection Desktop, is installed on the client and administrator's workstations.
- The Automate Sign-On for Mainframe Add-On activation file is available (after purchase).
- z/OS with DCAS is installed on the mainframe.
- LDAP directory is used for user authorization.
- A browser using JRE 8 or later that can run trusted applets and supports JavaScript, cookies, and cascading style sheets.
- JCE Unlimited Strength Jurisdiction Policy Files are required on the Administrative Server.

Steps to Set Up Automated Sign-On for Mainframe

Settings must be configured on the mainframe as well as in Management and Security Server.

- “Step 1. Install Automated Sign-On for Mainframe.” on page 52
- “Step 2. Configure the mainframe.” on page 52
- “Step 3. Configure settings in Administrative WebStation.” on page 52

Step 1. Install Automated Sign-On for Mainframe.

Automated Sign-On for Mainframe is installed with an activation file. Follow these steps.

1. After purchasing Automated Sign-On for Mainframe Add-On, you will receive information about downloading the product activation file:

   ```
   activation.automated_signon_for_mainframe-12.3.jaw
   ```

2. Download the activation file and note the location.
3. In the Management and Security Server, open the Administrative WebStation and click **Resources** > **About Management and Security Server**.
4. Beneath the box on the About Management and Security Server page, click **Browse** or **Choose File** (depending on your browser).
5. Locate and select the activation file. Click **Open**.
6. 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 (Step 3).
7. Restart your browser to ensure that the Administrative WebStation is fully updated with the new activation file. You do not need to restart the administrative server.
8. Continue with Step 2: Configure the mainframe.

Step 2. Configure the mainframe.

Detailed steps are provided in the Automated Sign-On for Mainframe Administrator Guide (http://docs.attachmate.com/mss/12.2/asm-admin.pdf).

Step 3. Configure settings in Administrative WebStation.

In the Administrative WebStation, open Settings > Automated Sign-On tab.

Follow the steps for the Configuration Tasks presented in the Administrator Guide (http://docs.attachmate.com/mss/12.2/asm-admin.pdf).

12 Setting Up Micro Focus Advanced Authentication Add-On

Advanced Authentication is a Micro Focus product that enables strong multi-factor authentication using a variety of authentication methods, including biometrics, one-time passwords, smartphone authentication.

As an Add-On Product, this access control method provides user authentication to Management and Security Server using Micro Focus Advanced Authentication.

In this chapter:

Advanced Authentication Add-On: Prerequisites and System Requirements

Before installing and configuring Micro Focus Advanced Authentication Add-On, verify that:

- Management and Security Server is installed.
- Micro Focus Advanced Authentication Add-On is licensed.
- The Micro Focus Advanced Authentication server is installed on a separate machine.

  Note the server name (or IP address) and the server's port number.

Step 1: Installing Micro Focus Advanced Authentication Add-On

The Advanced Authentication Add-On is installed with an activation file, as follows.

1. After purchasing Micro Focus Advanced Authentication Add-On, you will receive information about downloading the product activation file:

   `activation.advanced_authentication-12.3.jaw`
2. Download the activation file and note the location.
3. In the Management and Security Server, open the Administrative WebStation and click **Resources** > **About Management and Security Server**.
4. Beneath the box on the About Management and Security Server page, click **Browse** or **Choose File** (depending on your browser).
5. Locate and select the activation file. Click **Open**.
6. Click **Install** to add the product.

The new product is included in the list of Installed products, and the configuration settings are available in the Administrative WebStation.

7 Restart your browser to ensure that the Administrative WebStation is fully updated with the new activation file. You do not need to restart the administrative server.

8 Continue with Step 2: Setting up Advanced Authentication in the Administrative WebStation.

Step 2: Setting up Advanced Authentication in the Administrative WebStation

In the Administrative WebStation:

1 Open **Access Control Setup**, and click **Micro Focus Advanced Authentication**. Click **Next**.

If you see Current Settings listed, click **Configure** to view the list of methods.

2 Enter the Advanced Authentication **server name** (or IP address), noted earlier.

3 Enter the **port number** of the Advanced Authentication server, if different from the default of 443.

4 Note the default **LDAP credentials** for scheme.

By default, LDAP credentials are required for the Advanced Authentication scheme call. When unchecked, only a username is required.

5 Open **Help** to see the notes for the administrator.

6 Click **Next**. Confirm LDAP as your authorization method, and click **Next**.

7 Then, configure your LDAP server. See **Help** for assistance.

Step 3: Configuring authentication methods

To configure Advanced Authentication methods, such as Voice, refer to your Advanced Authentication (https://www.netiq.com/documentation/advanced-authentication-framework-52/) server documentation.

13 Installing Management and Security Server: Manual Installation

Use the multi-component installation files to manually install the needed components for your platform if any of the following is true:

- You want to use a servlet runner other than the default, which is automatically installed.
- You are installing on a platform for which an automated installer is not supported.
- You cannot run the automated installer for any other reason.

In this chapter:

Basic Manual Installation

Begin with a basic installation of Management and Security Server. Using the multi-component installation files is the simplest way to manually install the Administrative Server on Linux, UNIX, or Windows.

After the Administrative Server is installed and configured, you can started creating secure host sessions. Then, you can install and configure other components and your licensed Add-On Products.

A basic manual installation requires three steps:

1. Extract the multi-component manual installation file.
2. Enter configuration information.
3. Start services.

A basic manual installation assumes:

- The operating system is Linux, Solaris SPARC64, or Windows.
- A default servlet runner will be installed.
- All components will be installed on the same machine.

  For initial testing, you can install on a workstation; however, we recommend installing on a server operating system for production.
- The Prerequisite actions have been performed.
- The JCE Unlimited Strength Jurisdiction Policy Files have been applied. These policy files must be applied each time you update your JRE. For details, see Applying the JCE Unlimited Strength Jurisdiction Policy Files.

Basic Manual Installation Procedures

Use the multi-component installation file to manually install Management and Security Server. This file installs the following components on one server:

- Administrative Server
- A default servlet runner
- The JRE for the appropriate platform
- Metering Server
- Terminal ID Manager (if entitled)
- Security Proxy Server (if entitled)

Follow these steps.

Step 1: Extract the multi-component manual installation file.

Multi-component manual installation files are available for Linux, Solaris SPARC64, and Windows.

NOTE: After version 12.3, Management and Security Server will no longer provide installers for 32-bit systems.

To install the components:

1. From your download location, unzip the mss product file that you downloaded for your platform.

   This will create an install directory structure that contains an install_manual folder. For example:

   ```
   jar xvf mss-12.3.<nnn>-prod-linuxx64.zip
   ```
2. Change to the `install_manual` folder.
3. In the install_manual folder, unzip the mss archive file.

   This will create an `mss` folder. For example:

   ```
   tar xvf mss-beta-linuxx64-manual.tar.gz
   ```

Step 2: Enter configuration information.

Use the **Initial Configuration Utility** to configure the Administrative Server.

The Initial Configuration Utility (ICU) configures the following:

- 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 the servlet runner and Administrative Server.
- sets the administrative password.
- sets a port value for the Administrative Server in configuration files.

Run the ICU.

In the mss folder, go to the utilities/bin folder. Run the Initial Configuration Utility.

- On Windows, the ICU is named `InitialConfigurationUtililty.exe`.
- On Linux, the ICU is named `InitialConfigurationUtililty`.

Enter or verify your configuration information.

1. **Installation Directory:** Confirm the location where the Administrative Server was installed. If the default value is not correct, browse to the correct location.
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. If entitled, you can optionally choose to install the Security Proxy server.
3. **Volume Purchase Agreement number:** Optional. Enter the Volume Purchase Agreement (VPA) number. You can modify the VPA number later in the Administrative WebStation.
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. **Security 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 and to administer Metering and Terminal ID management (if installed). You can create different passwords for each server later.
7. **Server Names for URLs and Certificates:** The 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.
8. **Server certificates: organization and locality** (optional)

   This panel includes additional information for creating certificates.

   Organizational Unit: Enter the name of your organizational unit, typically the name of your department or division.

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

   City or Locality: Enter the full formal name (no abbreviations).

   State: Enter the full formal name (no abbreviations).

   Country: Provide a two-letter ISO country code, such as `US`.
9. **Confirm Configuration:** Click **Next** to apply the specified configuration changes.
10. **Configuration summary:** A summary of the configuration changes is created in InitalConfigurationUtility.log in the logs directory under the installation directory. Click **Done** to continue with Step 3: Start Services.

Step 3: Start services

After completing the configuration, you are ready to start the servlet runner and run the Administrative WebStation.

NOTE: If you installed Management and Security Server on Windows, the automated installer detects whether IIS is installed on your machine and offers to integrate IIS with the product. You can run the IIS Integration Utility later, if preferred. For more information, see Running the IIS Integration Utility.

---

1. **Start Services:** Start the server components.

   If you do not start the server components now, you can manually start them later.

   (See Starting the servlet runner.)

2. **Installation Complete.**

   After installing the Administrative Server, you can run the Administrative WebStation from any computer with a web browser. For example:

   `http://[server name][:port]/mss/AdminStart.html`

   Specify the port number if different from 80, the default.

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.

If you are using a servlet runner other than the one provided, refer to its documentation to start and stop the servlet runner.

To start the servlet runner:

1. In your mss/server/bin folder, locate either `server.bat` (Windows) or `server` (Linux or UNIX).
2. Start the server.
   - **On Windows:**

     `server.bat`
   - **On Linux or UNIX:**

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

     `server start`

Next steps

At this point, the installation is complete. You can begin using the Administrative WebStation to create and configure sessions. When ready, you can configure the Metering Server, or install and configure your Add-On Products.

As a next step, you might:

Start using the Administrative WebStation
Configure the Administrative Server
Set up Metering
Set up Security Proxy Add-On
Set up Terminal ID Manager Add-On

Set up Automated Sign-On for Mainframe Add-On
Set up Micro Focus Advanced Authentication Add-On

Manual Installation Variations

If the basic manual installation approach needs to be modified for your system, consider this option:

- **Installing on other UNIX platforms** (no JRE)

  Use this option if your UNIX platform requires a version of the Java runtime environment (JRE) other than the one provided by the installer.For details, see Installing on UNIX with no JRE.

“No JRE” Manual Installation

Procedure for Installing with no JRE

1. To use any of the `-nojre-` installation packages, confirm that a JRE 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 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 8 or higher.
3. Be sure that the JCE Unlimited Strength Jurisdiction Policy Files are applied, and apply them each time you upgrade your JRE. For details, see Applying the JCE Unlimited Strength Jurisdiction Policy Files.

14 Uninstalling

If you are using an automated installer to upgrade, you do not need to uninstall Management and Security Server first. The automated installer will uninstall the previous installation.

To uninstall Management and Security Server:

- On Windows, open Control Panel > Programs and Features, and click Micro Focus Host Access Management and Security Server.
- On Linux or UNIX, use the Uninstall utility.

Removing Components

To remove a component:

1. Stop all of the Management and Security Server components 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 used the automated installer to install the servlet runner and the Security Proxy as Windows services, the uninstaller will stop them automatically.
2. **On Windows:**
   - Verify that no Management and Security Server directories are open in your browser.
   - Use **Control Panel** > **Programs and Features** to remove a product or component.

   On Linux or UNIX:
   - If you used an automated installer for Linux or 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.

NOTES:

- 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.
- 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 to Version 12.3” on page 29.

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.

Java Server 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.

15 Appendices

Appendix A. Configuration Utilities

During and after you install Management and Security Server, you may be directed to run one or more utility. These utilities require that Management and Security Server was installed using either the automated installer or the multi-component manual installation.

- Initial Configuration Utility
- Configuration Upgrade Utility
- HTTPS Certificate Utility
- IIS Integration Utility (on Windows)

Initial Configuration Utility

You can run this utility independently if you did not enter the configuration information when you installed Management and Security Server.

The Initial Configuration 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 the servlet runner and the Administrative Server.
- sets the administrative password.
- sets a port value for the Administrative Server in configuration and HTML files.
- (if installed) configures the Security Proxy Add-On: generates cryptographic keys and self-signed certificates, automates configuration, and sets a port value for the Security Proxy.

Running the utility:

1. Be sure you have administrator privileges. If not, you will be prompted for credentials.
2. Launch the Initial Configuration Utility from its installed location. You can use `-c` to launch in console mode.

   Windows systems:

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

   Linux or UNIX systems:

   ```
   [MssServerInstall]/utilities/bin/InitialConfigurationUtility
   ```
3. Enter (or verify) your configuration information, as prompted.

Configuration Upgrade Utility

You can run this utility independently if you did not enter the configuration information when you upgraded Management and Security Server.

The Configuration Upgrade Utility (CUU):

- enables the services for this Administrative Server.
- copies the servlet runner's keystore from the previous location to the new location, if necessary.
- copies the MSSData (or ReflectionData) directory from the previous default location to the new default MSSData location (unless a custom location was configured).
- updates port values in configuration and HTML file.
- (if installed) copies Security Proxy Server configuration files from the old install directory to the new install directory.

Run the utility

1. Before you begin:
   - **1a** Make sure the earlier version of the software is not running when you run the Configuration Upgrade Utility.

     This step will avoid potential port conflicts and allow you to accept default port assignments.
   - **1b** Verify that you have administrator privileges. If not, you will be prompted for credentials.
   - **1c** **For manual installation:** First uninstall the services, such as the MSS Server and MSS SecurityProxy.
2. Launch the Configuration Upgrade Utility from its installed location. To launch in console mode, use `-c`.

   Windows systems:

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

   Linux or UNIX systems:

   ```
   [MssServerInstall]/utilities/bin/ConfigurationUpgradeUtility
   ```
3. Enter (or verify) your configuration information, as prompted.
4. **For manual installation:** After running the CUU, install and start the 12.3 services (MSS Server and MSS SecurityProxy).

HTTPS Certificate Utility

The HTTPS Certificate Utility manages the default servlet runner certificate. Use this utility to install or update a certificate for the HTTP server functionality that is included with the Management and Security Server.

This certificate enables clients to establish secure connections (HTTPS) to the services provided by the Management and Security Server. (Other certificates are managed differently.)

Running the HTTPS Certificate Utility

The HTTPS Certificate Utility can be run at any time to manage the servlet runner certificate. The utility requires that Management and Security Server was installed with an automated installer or multi-component manual installation file.

1. Verify that you used the HTTP Server functionality that was provided during installation.
2. Run the utility (`HttpsCertificateUtility.exe` or `HttpsCertificateUtility`).

   Windows systems:

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

   Linux or UNIX systems:

   `[MssServerInstall]/utilities/bin/HTTPSCertificateUtility`
3. Follow the prompts in the utility, and select a certificate action:
   - generate a new key pair and self-signed certificate.
   - import a CA-signed certificate and private key.
   - 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.

Alternative approaches

- Instead of running the HTTPS Certificate Utility, you can 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 CA-signed certificates, see Technical Note 1702 (http://support.attachmate.com/techdocs/1702.html).

Requiring HTTPS in the Administrative Server

Once your server supports HTTPS, use the Administrative WebStation to restrict the Administrative Server to the HTTPS protocol.

1. In the Administrative WebStation, click **Security Setup** > **Security** tab.
2. In the **Administrative server access protocol** section, select the **Require HTTPS - recommended** check box.
3. Click **Save Settings**.

IIS Integration Utility (on Windows)

If Microsoft Internet Information Services (IIS) is installed on your Windows 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.

Reasons to Integrate Management and Security Server with IIS

By default, a web server is installed, and you do not need to integrate the product with IIS. However, you may choose to integrate Management and Security Server with IIS 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 servlet runner certificate is ignored. Although the servlet runner certificate is not used after IIS integration, it is recommended that you do not delete that certificate. Once integrated with IIS, the expiration status of the servlet runner certificate does not affect the Management and Security Server installation.

When to integrate:

- You can run the IIS Integration Utility independently, even if you chose to not integrate while installing Management and Security Server.
- If a previous IIS integration existed when you ran the Initial or Upgrade configuration utility, the integration may be affected. Use the IIS Integration Utility to remove the existing integration and perform IIS integration again.

Running the IIS Integration Utility:

1. Run the IIS Integration Utility (`IISIntegrationUtility.exe`) located in the `[MssServerInstall]\utilities\bin` directory.
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 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.

Appendix B. Specifying a non-default location of MSSData

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

This directory 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:

- **On Windows Server 2012** and Windows Server 2008:

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

- **On Linux or UNIX:**

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

To change the location of MSSData, edit the `web.xml` file as follows:

1. Locate and open the `web.xml` file in a text editor, such as Notepad. For example, `web.xml` is within the MSS directory for each component:

   `mss/server/web/webapps/mss/WEB-INF/web.xml`

   `mss/server/web/webapps/meter/WEB-INF/web.xml`

   `mss/server/web/webapps/tidm/WEB-INF/web.xml` (if licensed)

2. In `web.xml`, 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.