Host Access Management and Security Server

Installation Guide

version 12.4.1

MICRO
FOCUS

Contents

Host Access Management and Security Server Installation Guide 7

1 Introduction 9

Overview of Management and Security Server . . . 9
Management and Security Server Components . . . 10
Installed and Enabled Components . . . 10
Add-On Products . . . 10
Overview of Components and Add-On Products . . . 11
Administrative Server . . . 11
Metering Server . . . 11
Configuration Utilities . . . 11
Security Proxy Add-On . . . 11
Terminal ID Manager Add-On . . . 11
Automated Sign-On for Mainframe Add-On . . . 12
Micro Focus Advanced Authentication Add-On . . . 12

2 Preparing to Install 13

Prerequisite Actions . . . 13
Shut down any currently running components . . . 13
Obtain the required user privileges . . . 13
Obtain the required account permissions . . . 13
System Requirements . . . 14
Administrative Server Requirements . . . 14
Browser Requirements . . . 15
Metering Server Requirements . . . 15
Requirements for Add-On Products . . . 15

3 Automated Installation 17

About Automated Installation . . . 17
Automated Installation Procedure . . . 17
Step 1: Run the automated installer . . . 17
Step 2: Enter configuration information . . . 19
Step 3: Start services . . . 20
Troubleshooting . . . 20
Installation Variations . . . 21
Installing on UNIX with no JRE . . . 21
Servlet Runner Launcher JVM Options . . . 21
Servlet runner other than Apache Tomcat . . . 22
Using SiteMinder . . . 22
Using the automated installer in console mode . . . 22
Unattended installation . . . 22
Manual installation . . . 23

4 Manual Installation 25

About Manual Installation . . . 25
Manual Installation Procedure . . . 25
Step 1: Extract the manual.zip file . . . 25

Step 2: Run a configuration utility. . . . 26
Step 3: Start the server components. . . . 27
Manual Installation Variations. . . . 27
Installing on UNIX with no JRE 28
Servlet Runner Launcher JVM Options 28

5 Starting the Administrative WebStation 29

Log in to the Administrative WebStation. . . . 29
Using **Administrative Server (HTML login)** 29
Using Administrative Server login 30
Configure the Administrative Server 30
Initial Settings 31
Next Steps 31

6 Setting Up Metering 33

Metering: Prerequisites and System Requirements 33
Creating Metered Terminal Sessions 33
Configuring Server Settings in the Administrative WebStation 33
To enable metering 34
Using the Metering Administration Tool 34
Configuring License Pools and Server Settings 35
Viewing Metering Reports 35

7 Installing Add-On Products 37

Installing Activation Files for Add-On Products 37
Use the automated installer to install activation files 37
Use the ***About*** page to install activation files 38

8 Setting Up the Security Proxy 39

Overview of Security Proxy Server 39
Security Proxy Server: Prerequisites and System Requirements 40
Deploying a Secure Session 41
Step 1: Install the Security Proxy Server. . . . 41
Use the automated installer. . . . 41
Install the activation file and then activate the server. . . . 42
Step 2: Start the Security Proxy. . . . 42
Step 3: Create and Map Secure Sessions. . . . 43
Step 4: View Security Proxy Reports. . . . 43
Manual Installation: Security Proxy 44
Step 1. Manually Install the Security Proxy file. . . . 44
Step 2. Configure and Start the Security Proxy Server. . . . 44
Next steps 46
Synchronize an Upgraded Security Proxy 47

9 Setting Up Terminal ID Manager 49

Terminal ID Manager: Prerequisites and System Requirements 49
Step 1: Install Terminal ID Manager. . . . 49
Install the Terminal ID Manager activation file. . . . 49
Step 2: Activate the server. . . . 50
Step 3: Configure Terminal ID Manager. . . . 51

10 Setting Up Automated Sign-On for Mainframe **53**

Overview of Automated Sign-On for Mainframe . . . 53
Automated Sign-On for Mainframe: Prerequisites and System Requirements . . . 53
Steps to Set Up Automated Sign-On for Mainframe. . . . 54
Step 1. Install Automated Sign-On for Mainframe.. . . . 54
Step 2. Configure the mainframe. . . . 54
Step 3. Configure settings in Administrative WebStation. . . . 54

11 Setting Up Micro Focus Advanced Authentication Add-On **55**

Advanced Authentication Add-On: Prerequisites and System Requirements . . . 55
Step 1: Installing Micro Focus Advanced Authentication Add-On . . . 55
Step 2: Setting up Advanced Authentication in the Administrative WebStation . . . 56
Step 3: Configuring authentication methods . . . 56

12 Upgrading to Version 12.4 Update 1 **57**

Download Product Files . . . 57
Upgrading the Security Proxy Server . . . 57
Upgrading Replicated Servers . . . 58
Upgrading Add-On Products . . . 58
Run the automated installer . . . 58
Upgrading a Manual Installation. . . . 58
Run the Configuration Upgrade Utility . . . 59
To complete a Reflection for the Web upgrade . . . 60
Directory Names and Installation Paths . . . 60

13 Uninstalling **61**

Removing Components . . . 61

14 Appendices **63**

Appendix A. Configuration Utilities . . . 63
Initial Configuration Utility . . . 63
Configuration Upgrade Utility . . . 64
HTTPS Certificate Utility . . . 64
IIS Integration Utility (on Windows) . . . 65
Appendix B. Specifying a non-default location for MSSData . . . 66

Host Access Management and Security Server Installation Guide

Host Access Management and Security Server provides an administrator the means to centrally secure, manage, and monitor users' access to host applications. Use this Installation Guide to install and configure the server components and add-on products.

At a Glance:

About Management and Security Server
About Automated Installation
About Add-On Products
If you are evaluating...

About Management and Security Server

Using Management and Security Server, an administrator can create host sessions for Micro Focus products including Reflection Desktop, InfoConnect, Reflection ZFE, Reflection for the Web, and Rumba. Then, the administrator can centrally secure, manage, and monitor users' access to those sessions.

This guide provides the steps to get up and running. When possible, we recommend installing Management and Security Server using the automated installer. Add-On products are available and can also be installed by the automated installer.

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

About Automated Installation

Use the automated installer to install the Management and Security Server components:

- Administrative Server
- Metering Server
- Configuration Utilities
- Security Proxy Server *
- Terminal ID Manager *

* The Security Proxy Server and Terminal ID Manager are Add-On Products that are installed with the other components. However, a license entitlement is required to enable and activate these products.

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

Add-On Products, which require separate licenses, enhance Management and Security Server's functionality with supplemental means of security. These products can be installed along with Management and Security Server, although addition activation or configuration is required.

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 browser-based Reflection ZFE sessions that do not require Java.

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

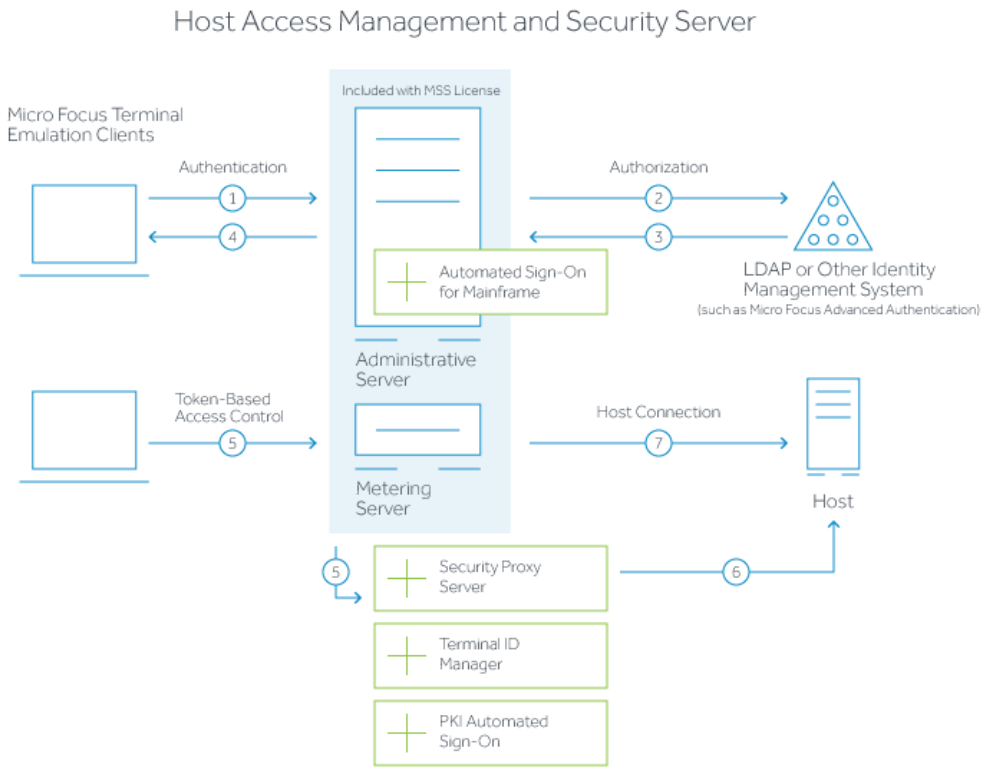
In this section:

- Overview of Management and Security Server
- Management and Security Server Components
- Overview of Components and Add-On Products

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 Server (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.

Management and Security Server Components

Management and Security Server consists of servers, applications, and Add-On Products.

Installed and Enabled Components

An automated installation of Management and Security Server installs and enables:

- Host Access Management and Security Server
- Administrative Server
- Metering Server
- Configuration Utilities
- Security Proxy *
- Terminal ID Manager *

  * The Security Proxy and Terminal ID Manager are Add-On products, which must be appropriately licensed before they are enabled.

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.

Add-On Products include

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

Overview of Components and Add-On Products

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 user interface for the Administrative Server is the **Administrative WebStation**, where an administrator can 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 and does not require a separate license.

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.

For details, see Setting Up Metering.

Configuration Utilities

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

Security Proxy Add-On

The Security Proxy acts as a proxy for terminal sessions and provides token-based access control, routing encrypted network traffic to and from user workstations. A separate license is required for the Security Proxy (as an add-on product), which can be installed by an automated installer.

For details, see Setting up the Security Proxy.

Terminal ID Manager Add-On

The Terminal ID Manager lets you centrally manage and assign terminal and device IDs to emulator sessions. You can pool terminal IDs, track ID usage, and manage inactivity timeout values for specific users, thus conserving terminal ID resources and significantly reducing operating expenses. A separate license is required for the Terminal ID Manager (as an add-on product), which can be installed by an automated installer.

For details, see Setting Up Terminal ID Manager.

Automated Sign-On for Mainframe Add-On

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

To add Micro Focus Advanced Authentication, you need to install the activation file and configure settings using the Administrative WebStation.

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

2 Preparing to Install

Before you begin to install Management and Security Server, check:

- Prerequisite Actions
- System Requirements

Prerequisite Actions

Before you run 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 component that is currently running. (If you installed an earlier version with an automated installer, the automated installer will close the 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 with administrative privileges. Note that applications run by administrators are run with standard user permissions unless the user specifically authorizes the application to use more elevated privileges.
- **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 the MSSData directory (which stores site-specific content) must be installed to a non-default location, see Appendix B: Specifying a non-default location for MSSData.

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
```

System Requirements

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

In this section:

- Administrative Server Requirements
- Browser Requirements
- Metering Server Requirements
- Requirements for 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 64-bit 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).

- **Updated JCE Unlimited Strength Policy Files**

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

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

  - manually install Management and Security Server.
  - upgrade your JRE (each time).

NOTE: 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.

If you choose the “No JRE” installer for UNIX, the files are *not* installed.

To Apply the JCE Unlimited Strength Jurisdiction 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 8: (http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.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.

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.

When using the non-Java **Administrative Server (HTML login)** option, the browser must:

- support JavaScript and cookies

When using the **Administrative Server** login, 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). Some exceptions may apply.

Metering Server Requirements

The Metering Server requires a server running JRE 8 or later.

Requirements for Add-On Products

The prerequisites and system requirements for each add-on product are included in the specific product sections:

Security Proxy Add-On

Terminal ID Manager Add-On

Automated Sign-On for Mainframe Add-On

Micro Focus Advanced Authentication Add-On

3 Automated Installation

When possible, use the automated installer to install the Management and Security Server components on Linux, UNIX, or Windows.

In this section:

- About Automated Installation
- Automated Installation Procedure
- Troubleshooting
- Installation Variations

About Automated Installation

In addition to installing all of the Management and Security Server components, the automated installer can install the activation files for your entitled add-on products.

The automated installer for 64-bit systems:

- can be run on Linux, Solaris SPARC-64, or Windows.
- can be run on AIX using the “no JRE” version of the automated installer.
- can install all components on the same machine for initial testing.

Management and Security Server can be installed on a workstation; however, we recommend installing on a server operating system for production.

Automated Installation Procedure

Before you begin, be sure the Prerequisite Actions have been performed. Then, follow these steps.

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

Step 1: Run the automated installer.

To run the automated installer:

1. From your product download location, locate the automated installer for your system’s platform. (In the file name, <nnn> is the build number.)

Operating System	Automated Installer
Linux 64-bit	mss-12.4.<nnn>-prod-linuxx64.sh
Solaris SPARC 64-bit	mss-12.4.<nnn>-prod-solsparc64.sh
IBM AIX	mss-12.4<nnn>-prod-unix-nojre.sh
Windows 64-bit	mss-12.4.<nnn>-prod-wx64.exe

2 (Optional.) **If you are entitled to Add-On products,** we recommend installing the current activation file(s) when you run the automated installer.

To install or update your Add-On Product(s) at a later time, see Installing Activation Files for Add-On Products.

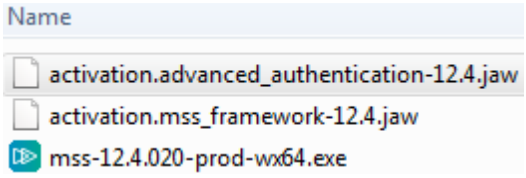
To install the activation file(s) now:

2a Download the current version of the activation file for each of your Add-On Products from the Micro Focus download site (where you downloaded Host Access Management and Security Server).

Activation files are in this format: `activation.<product_name>.jaw`

2b Place each activation file in the directory with the MSS installer.

On Windows, for example: to install the Advanced Authentication Add-On, place the activation file in the same folder as the installer, `mss-12.4.<build>-prod-wx64.exe`.



3 Run the MSS installer.

4 Select a **language** to be used during installation.

5 Click **Next** to continue. The installer lists the products that will be enabled.

6 Read and accept the license agreement.

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

8 Select the components to install, and then click **Next**.

Host Access Management and Security Server. Select this check box to install the Administrative Server, which includes the Administrative WebStation, Metering Server, and Terminal ID Manager. A default servlet runner is automatically installed.

- **Terminal ID Manager** is enabled only when entitled.
- **Security Proxy Server**, when entitled, can be installed now or later.

9 **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. Click **Next**.

10 During a **new installation**, the automated installer copies files to the designated directory and launches a configuration utility.

Continue with Step 2: Enter configuration information.

(During an **upgrade**, the installer retains your settings, and you will not be prompted to run a configuration utility. For more information, see Upgrading to Version 12.4.)

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 or browse to the location where the Administrative Server was installed.
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 installing 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 `<installation>\utilities\logs` 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.

The MSS Server must be started before you can run the Administrative WebStation, the Metering Server, or the Terminal ID Manager.

1. **Start Services** is selected by default.

   If you chose to *not* start services now, you can do so later. See To start the service after an automated installation.
2. **Installation Complete.** The components are installed and the services are started.
3. Continue with Starting the Administrative Server.

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.

To start the service after an automated installation

On Windows:

1. Open **Windows Services**.
2. Right-click **Micro Focus MSS Server**.
3. Click **Start**.

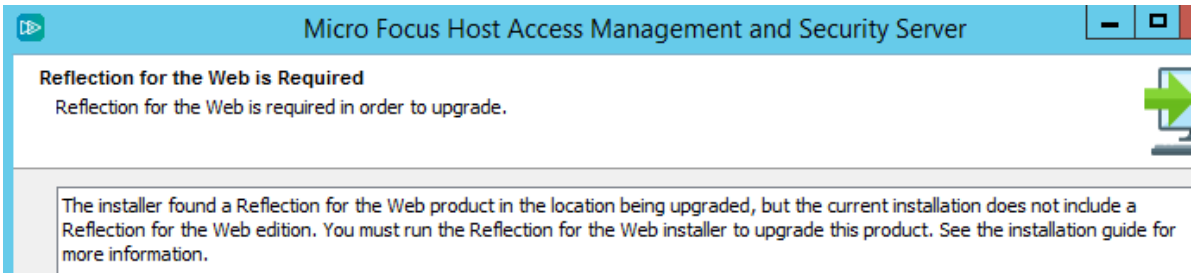
On Linux or UNIX:

1. In the `server/bin` directory, execute the script named `server`.
2. Additionally, the administrator may create `init` scripts to start the MSS Server on startup.

Troubleshooting

If you encounter this error while running the Management and Security Server automated 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 automated installation approach needs to be modified for your system, consider these variations:

- Installing on UNIX with no JRE
- Servlet Runner Launcher JVM Options
- 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, AIX, 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 this installer.

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

   `mss-12.4.<nnn>-prod-unix-nojre.sh`, where `<nnn>` is the build number.
2. Proceed with the installation, using your existing JRE.

   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 steps, see To Apply the JCE Unlimited Strength Jurisdiction Policy Files.

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`, in the `server\conf` directory.

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

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

Using the automated installer in console mode

If preferred, you can 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, 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 `<12.4.nnn>` is the product version and build number:

```
mss-<12.4.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, see the Manual Installation section.

4 Manual Installation

If you cannot run the automated installer, use this manual installation process.

In this section:

- About Manual Installation
- Manual Installation Procedure
- Manual Installation Variations

About Manual Installation

A manual installation contains all of the files needed to install the Management and Security Server components. The manual installation:

- can be run on numerous platforms, including Linux, UNIX (all flavors), Solaris SPARC64, and Windows.
- installs a default servlet runner.
- installs a JRE and applies the JCE Unlimited Strength Jurisdiction Policy files (unless you run the no-jre installer).
- installs the Administrative Server, the Metering Server, the Security Proxy*, and the Terminal ID Manager*.

  * The Security Proxy and Terminal ID Manager require separate entitlements.

Manual Installation Procedure

Before you begin, be sure the Prerequisite actions have been performed. Then follow these steps.

- Step 1: Extract the manual.zip file.
- Step 2: Run a configuration utility.
- Step 3: Start the server components.

Step 1: Extract the manual.zip file.

To install the components:

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

   An install directory structure is created that contains an `install_manual` directory. For example:

   ```
   jar xvf mss-12.4.<nnn>-prod-linuxx64.zip
   ```

2. Change to the `install_manual` directory.
3. In the `install_manual` directory, unzip the `mss archive` file.

An `mss` directory is created. For example:

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

Step 2: Run a configuration utility.

For a new installation, use the **Initial Configuration Utility** (ICU) to configure the Administrative 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 Administrative Server.
- sets the administrative password.
- sets a port value for the Administrative Server in configuration files.

Run the Initial Configuration Utility.

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

- On Windows: `InitialConfigurationUtililty.exe`
- On Linux or UNIX: `InitialConfigurationUtililty`

Enter or verify your configuration information.

Complete the online form, noting the following:

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 installing 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 enables 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 the server components.

Step 3: Start the server components.

The MSS Server must be started before you can access and manage the Administrative WebStation, the Metering Server, or the Terminal ID Manager.

To start the servlet runner after a manual installation

On Windows:

Either

1 In the installation directory, locate and run: `server\bin\server.bat`

-- or --

1 Install the Windows service: `install-server-service.bat`

(To uninstall the Windows service: `uninstall-server-service.bat`)

2 Open **Windows Services**.

3 Right-click **Micro Focus MSS Server**.

4 Click **Start**.

On Linux or UNIX:

1 In the `server/bin/server directory`, execute the script named `server`.

2 Additionally. the administrator may create `init` scripts to start the MSS Server on startup.

Next step

At this point, the installation is complete. The components are installed and the services are started.

Continue with Starting the Administrative WebStation.

Manual Installation Variations

If you need to modify the manual installation approach to fit your system, consider these options:

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.

No JRE is installed with this installer.

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

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

2. Proceed with the installation, using your existing JRE.

   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 To Apply the JCE Unlimited Strength Jurisdiction Policy Files.

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, in the `server\conf` directory.

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

5 Starting the Administrative WebStation

The Administrative WebStation is the user 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.

Choose a login option, and then configure your initial settings.

- Log in to the Administrative WebStation
- Configure the Administrative Server

Log in to the Administrative WebStation

You can open the Administrative WebStation from the Windows **Start** menu or from a URL on any computer with a web browser.

1. First, be sure the servlet runner is started. If you ran the automated installer, the servlet runner is automatically started.

   If you need to manually start the servlet runner, refer to the appropriate steps:

   To start the service after an automated installation

   To start the servlet runner after a manual installation
2. Choose a login option:
   - **Administrative Server (HTML login)**

     This non-Java login directly opens the Administrative WebStation (and is English-only).

     See Using Administrative Server (HTML login).
   - **Administrative Server**

     This login opens the list of session links, with a link to the Administrative WebStation. (Java is required on the client.)

     See Using Administrative Server login.

Using Administrative Server (HTML login)

1. Open the login page either from the Windows **Start** menu or from the URL:
   - Start > All Programs > Host Access Management and Security Server > Administrative Server (HTML login)
   - `http://<hostname>[:port]/mss/Admin.html`

     Note: If the port number is 80 (the default for HTTP), it is not needed in the URL. For example, `http://myserver.mycompany.com/mss/Admin.html`
2. In the **User** field, enter either `admin` (the default) or your site-specific user name.
3. Enter the administrator password specified during installation and configuration.

   Note: The default password is `admin`. We recommend that you change this password as soon as possible. In the Administrative WebStation, go to **Security Setup** > **Security** tab.
4. Click **Login**. The Administrative WebStation opens to the **Home** page.

NOTE: 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 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.

5 To see the list of sessions, open **Session Manager**.

6 Continue with Configuring the Administrative Server.

Using Administrative Server login

1 Open the login page either from the Windows **Start** menu, or from the URL:

- Start > All Programs > Host Access Management and Security Server > Administrative Server
- `http://<hostname>[:port]/mss/AdminStart.html`

  Note: If the port number is 80 (the default for HTTP), it is not needed in the URL. For example, `http://myserver.mycompany.com/mss/AdminStart.html`

2 If prompted to run the launcher application, click **Run**.

3 Keep the box checked to log in as administrator (and use the defaults), or clear the check box and enter a site-specific **User name**.

4 Enter the administrator password specified during installation.

Note: The default password is `admin`. We recommend that you change this password as soon as possible. In the Administrative WebStation, go to S**ecurity Setup** > **Security** tab.

5 Click **Submit**.

The list of Session links opens. (This list will be populated with sessions you create.)

6 Click the **Administrative WebStation** button.

NOTE: 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 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.

7 Continue with Configuring the Administrative Server.

Configure the Administrative Server

Before you begin creating and configuring sessions, set your preferences for using the Administrative WebStation.

Initial Settings

Log in to the Administrative WebStation, and set your initial preferences, which can be changed later.

1. Open **Settings** (from the left nav). On the **General** tab, enter your initial settings and preferences. Open `Help` for more information. Click **Save Settings**.
2. 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. Click **Save Settings**.

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

NOTE: To configure the servers to run with administrative privileges, right-click the **Start** menu and click **Properties**. On the **Compatibility** tab, select **Run this program as an administrator**, and then click **OK**.

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 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 section:

- Metering: Prerequisites and System Requirements
- Creating Metered Terminal Sessions
- Using the Metering Administration Tool
- Configuring License Pools and Server Settings
- Viewing Metering Reports

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).

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
- To enable metering

Configuring Server Settings in the Administrative WebStation

Use the Administrative WebStation to add a metering server and to enable metering.

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 **Add to Table**.

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, click **Session Manager**.
  2. Click **Add** after selecting a session type or click an existing session name to edit.
  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 Metering Administration 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: 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 is 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** (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 and log in to the **Metering Administration** tool, if it is not already open.

   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. See **Help** for details.
3. To change a product's metering settings, click that product link, and edit the **License Pool** settings. See **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 opened in several ways:
   - In the **Administrative WebStation**, click **Reports** > **Metering**. Verify or select your metering server, and click **Show Report**.
   - From the Windows **Start** menu, open **Metering Reports**.
   - On other platforms (or from a different machine), go to

     `http://[metering server name]/meter/ReportsLogin.do`.
3. If prompted, enter the 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 you are running more than one metering server, you must add the metering report numbers together for an accurate report.

---

7 Installing Add-On Products

Management and Security Server's functionality can be augmented with one or more Add-On Products:

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

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`

Each add-on product requires a separate license and separate installation or activation.

Installing Activation Files for Add-On Products

Add-On Products can be installed in two ways:

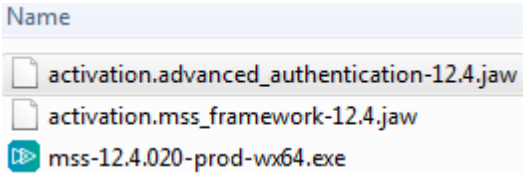
- Use the automated installer to install activation files
- Use the About page to install activation files

Use the automated installer to install activation files

The easiest way to install or upgrade activation files is by running the MSS automated installer.

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

   On Windows, for example: to install the Advanced Authentication Add-On, place the activation file in the same folder as the installer, `mss-12.4.<build>-prod-wx64.exe`.



   NOTE: The `activation.mss_framework-12.4.jaw` activation file is automatically installed to enable the Host Access Management and Security Server framework.

3. Run the MSS installer.

The activation files are placed in the appropriate directories, and you can begin configuring the add-on features.

The add-on products are also included on the *About Management and Security Server* page under **Installed products**.

Use the *About* page to install activation files

The activation files for add-on products can be installed or upgraded using the **About Management and Security Server** page. Further action is required to configure the add-on features.

1. Download the current version of 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.

   NOTE: The list of installed products includes the **Host Access Management and Security Server Framework** activation file, which is automatically installed to enable the server framework.

   ---
6. Restart your browser to ensure that the Administrative WebStation is fully updated with the new set of activation files. You do not need to restart the administrative server.
7. Each add-on product requires further configuration and/or activation.

   For details, refer to the appropriate section for setting up your add-on product(s).

   NOTE: The activation files for the **Security Proxy** and **Terminal ID Manager** must be copied to specific locations to activate the features.

   See the **Help** topic on the **About** page for detailed instructions.

Refer to the specific section for instructions about installing and activating your add-on product(s):

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

8 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.

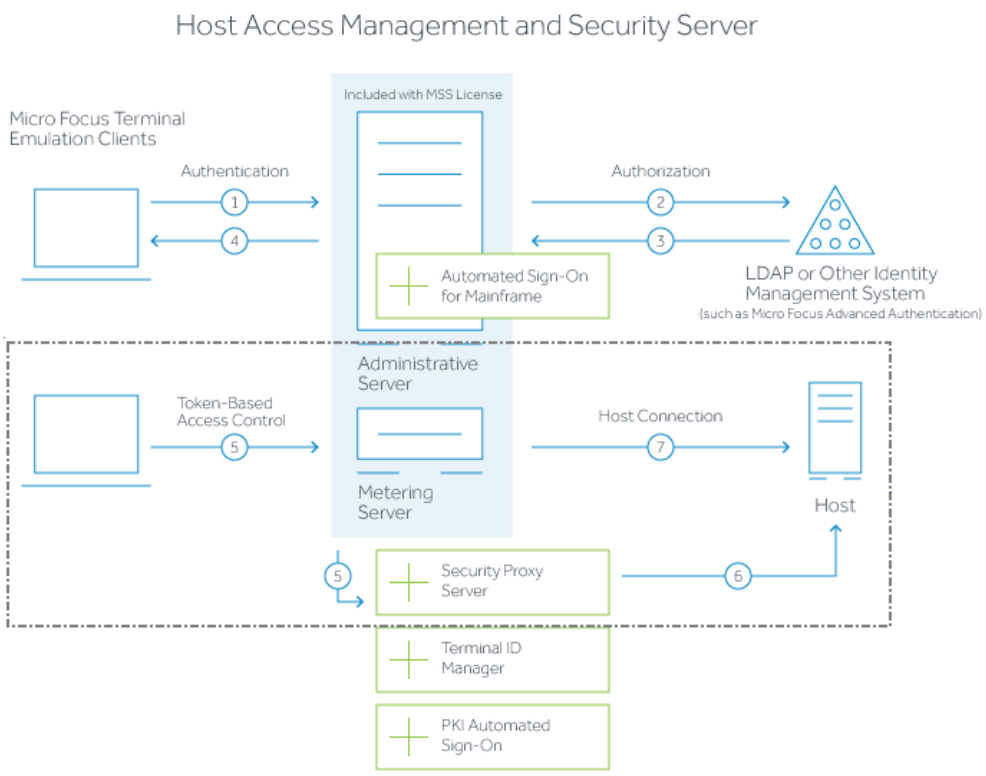
In this section:

- Overview of Security Proxy Server
- Security Proxy Server: Prerequisites and System Requirements
- Deploying a Secure Session
- Step 1: Install the Security Proxy Server.
- Step 2: Start the Security Proxy.
- Step 3: Create and Map Secure Sessions.
- Step 4: View Security Proxy Reports.
- Manual Installation: Security Proxy
- Synchronize an Upgraded Security Proxy

Overview of Security Proxy Server

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.



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).

Deploying a Secure Session

Follow these steps to deploy a secure session through the Security Proxy, and then run reports to monitor the Security Proxy server activity.

- Step 1: Install the Security Proxy Server.
- Step 2: Start the Security Proxy.
- Step 3: Create and Map Secure Sessions.
- Step 4: View Security Proxy Reports.

Step 1: Install the Security Proxy Server.

Use the automated installer to install and configure the Security Proxy Server and to 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: Start 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-12.4.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 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 has 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 encrypted terminal emulation sessions to connect to the host through the Security Proxy. Then, you can map the secure session(s) to the authorized users.

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 **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. Use the **Access Mapper** to map the secure session(s) to your authorized users. See **Help** for details.

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

See Step 4: View Security Proxy Reports.

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, and click **Show Report.**

   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.

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

- Step 1. Manually Install the Security Proxy file.
- Step 2. Configure and Start the Security Proxy Server.
- Next steps

Step 1. Manually Install the Security Proxy file.

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

Operating System	Manual Installation File
Linux 64-bit	securityproxy-prod-linuxx64-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

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.

Step 2. Configure and Start the Security Proxy Server.

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.

Use the Security Proxy Wizard to 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.

Start the Security Proxy Server,

After a `server.properties` file is configured for the Security Proxy Server, 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.

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.

Continue with these steps, which are the same whether you use manual installation or an automated installer.

- Step 3: Create and Map 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

1883: End-to-End Encryption through the Security Proxy

Synchronize an Upgraded Security Proxy

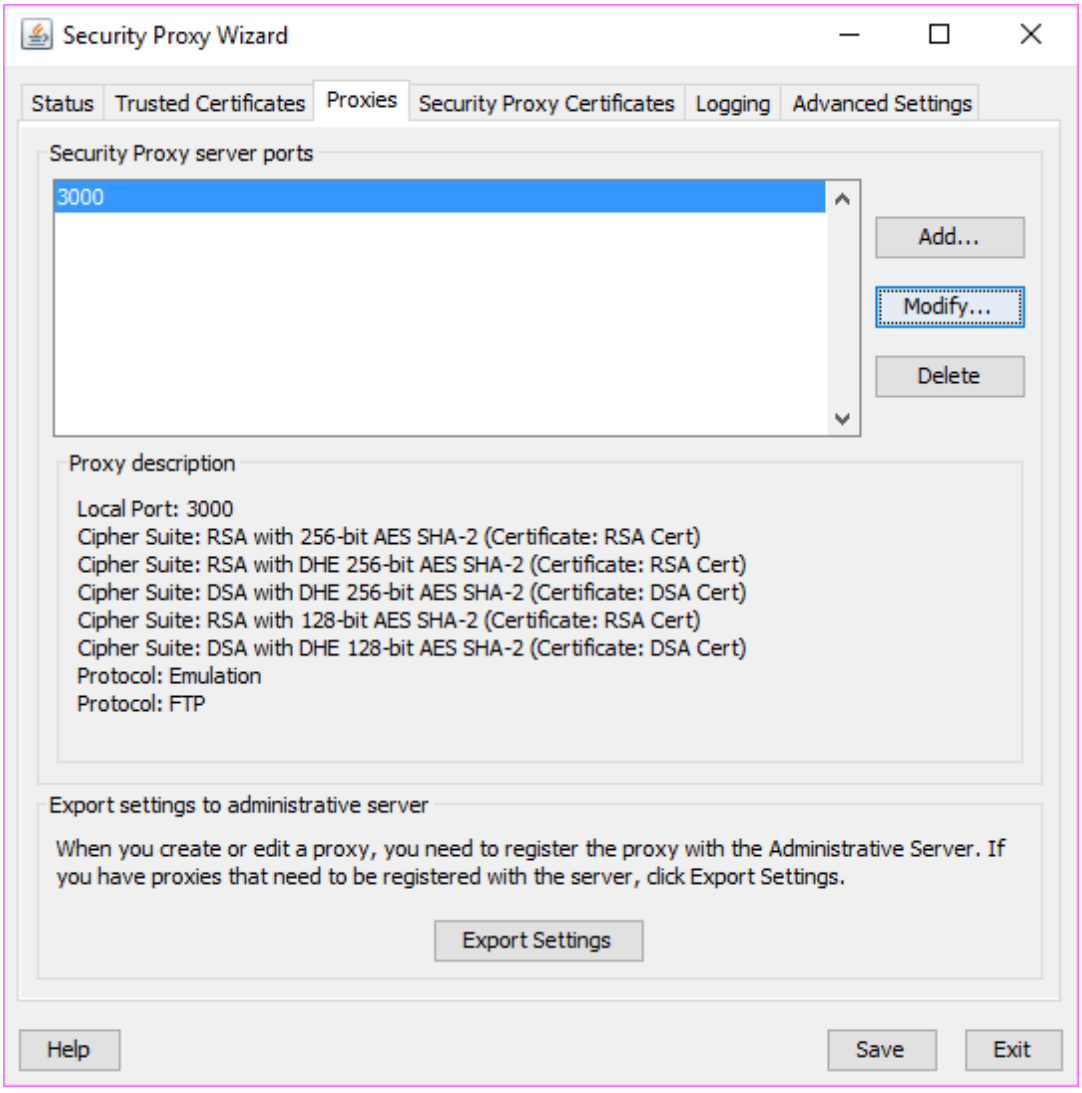
If Security Proxy is installed when you upgrade from Management and Security Server 12.4 to a later version (including updates and service packs), complete these steps to be sure the security proxy server is synchronized with the MSS administrative server.

After you upgrade:

1. Open the **Security Proxy Wizard** (from the Start menu).
2. On the **Proxies** tab, review the configuration for each port, and click **Save**.

   Note the **Cipher Suites and Certificates**:

   - Multiple cipher suites of the same key type can use the same certificate.
   - Management and Security Server automatically selects the certificate to use with the associated cipher suite. The selection is based on longest expiration date and other properties. For example:



3 To select a different certificate for a particular port:

3a Click the **Proxies** tab > **Modify**.

Note (or change) the selected cipher suites.

Select an RSA certificate or DSA certificate for that type of cipher suite. Click **OK**.

On the **Proxies** tab, click **Save**.

Click **Export** to send the settings to the MSS administrative server.

9 Setting Up Terminal ID Manager

The Terminal ID Manager lets you centrally manage and assign terminal and device IDs to emulator sessions. You can 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 section:

- Terminal ID Manager: Prerequisites and System Requirements
- Step 1: Install Terminal ID Manager.
- Step 2: Activate the server.
- Step 3: Configure Terminal ID Manager.

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).

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.

You can install Terminal ID Manager either by running the automated installer or by using the Administrative WebStation *About* box.

Using the automated installer

You can run 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.

Using the Administrative WebStation *About* box

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-12.4.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.

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 `/tidm/WEB-INF/lib/modules` directory on ***each*** machine where Terminal ID Manager is installed.

2 Restart the MSS Server.

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.

Continue with Step 3: Configure Terminal ID Manager.

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 **Help** 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.

10 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 section:

- Overview of Automated Sign-On for Mainframe
- Automated Sign-On for Mainframe: Prerequisites and System Requirements
- Steps to Set Up Automated Sign-On for Mainframe

Overview of Automated Sign-On for Mainframe

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

To configure Automated Sign-On for Mainframe, you must:

- 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 Automated 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. For details, see the Administrative Server Requirements.

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.
- Step 2. Configure the mainframe.
- Step 3. Configure settings in Administrative WebStation.

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-12.4.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.
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.

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.

11 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, and 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 section:

- Advanced Authentication Add-On: Prerequisites and System Requirements
- Step 1: Installing Micro Focus Advanced Authentication Add-On
- Step 2: Setting up Advanced Authentication in the Administrative WebStation
- Step 3: Configuring authentication methods

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-12.4.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 If the **port number** of the Advanced Authentication server differs from the default (443), enter the port number.

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.

Continue with Step 3: Configuring authentication methods.

Step 3: Configuring authentication methods

To configure Advanced Authentication methods, such as Voice, refer to your Advanced Authentication server documentation.

12 Upgrading to Version 12.4 Update 1

Management and Security Server can be upgraded using the same procedure that was used to install your current version -- the automated installer or manual installation.

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

In this section:

- Download Product Files
- Upgrading the Security Proxy Server
- Upgrading Replicated Servers
- Upgrading Add-On Products
- Run the automated installer
- Upgrading a Manual Installation
- Directory Names and Installation Paths

Download Product Files

When you are ready to upgrade, log in to the Micro Focus download site to find your list of entitlements. In addition to Host Access Management and Security Server, your purchased Add-On Products are also listed.

1. Download the automated installer or multi-component installation files for the platform where **Management and Security Server** will be installed.
2. Download the activation files for your entitled **Add-On Products**, which are in this format: `activation.<product_name>.jaw`.

   If using the automated installer, place the activation files in the same location as the installer.

Upgrading the Security Proxy Server

If the Security Proxy is installed when you upgrade Management and Security Server from version 12.4 to a later version, including 12.4 Update 1, be sure to synchronize the Security Proxy with the MSS administrative Server.

For details, see Synchronize an Upgraded Security Proxy.

Upgrading Replicated Servers

If enabled, Replication must be *disabled* on every server before you upgrade Management and Security Server.

Before you upgrade: Disable Replication on every server configured for replication, beginning with the **Slave** servers. Then, disable Replication on the **Master**.

1. In the Administrative WebStation, click **Settings** > **Replication** tab.
2. Select the **Standalone** Server Role. Click S**ave Settings**.
3. Repeat steps 1 and 2 for all of the Slave servers and then the Master server.
4. When all of the servers are set to **Standalone**, upgrade each server.
5. When all of the servers are upgraded, re-enable **Replication**. See Technical Note 2174 for detailed steps.

Upgrading Add-On Products

The procedure for upgrading Add-On Products is similar to the initial installation.Your entitled add-on product activation files are available from the same download location as the product files.

If you are using the automated installer, continue with the steps in this section. If the automated installer is not an option see the steps to Use the *About* page to install activation files.

Run the automated installer

To upgrade using the automated installer:

1. If you are upgrading **Add-On Products**, be sure the downloaded activation files are in the same directory as the automated installer.
2. Run the automated installer to upgrade the Administrative Server.

   The automated installer retains your current settings and removes files from the previous installation. You do not need to run a configuration upgrade utility or re-create your sessions.

Upgrading a 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. 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 upgrade your settings.

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

Run the 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 64).
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.

Install and start services

After you run the Configuration Upgrade Utility, install and start the 12.4 services that you uninstalled before you began (such as MSS Server and MSS SecurityProxy).

To complete a Reflection for the Web upgrade

The `rweb-client` web application context must be installed.

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

   `<MSS install directory>\server\web\webapps`
3. Start (or restart) the MSS Server.

The servlet runner will expand the war file and an `rweb-client` context will be created.

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`

13 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:** click **Control Panel** > **Programs and Features** > **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.
   - If you installed the product manually, stop the servlet runner and the Security Proxy (if added) and close the command windows before you begin to remove the components.
   - 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 12.4 Update 1.

14 Appendices

Appendix A. Configuration Utilities
Appendix B. Specifying a non-default location for MSSData

Appendix A. Configuration Utilities

During and after you install Management and Security Server, you may be directed to run one or more utility. To run these utilities, Management and Security Server must have been 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 any services, such as 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 12.4 services (such as 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. To run this utility, Management and Security Server must have been installed using 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**.
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 even if you did not integrate IIS when you installed 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 for 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.

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. 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 MSS Server.