

Management and Security Server Installation Guide

12.8.3

Table of contents

Management and Security Server Installation Guide	4
At a Glance:	4
About Management and Security Server	4
Installation Notes	4
If you are evaluating...	5
Introduction	6
Introduction	6
What Management and Security Server installs	7
Overview of Components and Add-On Products	8
Preparing to Install MSS	11
Preparing to Install	11
Prerequisite Actions	12
Minimum System Requirements	14
Installing MSS	15
Installing MSS	15
Installation Steps	16
Ports	23
Installation Variations	26
Opening the MSS Administrative Console	32
Opening the MSS Administrative Console	32
Log in to the Administrative Server	33
Configure the Administrative Server	34
Setting Up Metering	35
Setting Up Metering	35
How Metering Works	36
Installing Add-On Products	37
Installing Add-On Products	37
Installing Activation Files	38
Setting Up the Security Proxy	40
Setting Up the Security Proxy	40

Security Proxy: Prerequisites and System Requirements	41
Install and Activate the Security Proxy Server	45
Setting Up Terminal ID Manager	49
Setting Up Terminal ID Manager	49
Terminal ID Manager: Prerequisites and System Requirements	50
Run the MSS Automated Installer	51
Configure Terminal ID Manager	53
Setting Up Automated Sign-On for Mainframe	54
Setting Up Automated Sign-On for Mainframe	54
Installing Automated Sign-On for Mainframe	55
Setting Up MSS Automated Sign-On for Host Access	56
Setting Up MSS Automated Sign-On for Host Access	56
Installing MSS Automated Sign-On for Host Access	57
Setting Up Advanced Authentication Add-On	58
Setting Up Micro Focus Advanced Authentication Add-On	58
Installing and Configuring Advanced Authentication Add-On	59
Troubleshooting the Installation	60
Installation does not complete on UNIX or Linux platforms	60
Upgrading	61
Upgrading MSS	61
Upgrading the Security Proxy Server	63
Upgrade Replicated Servers	67
Upgrading Add-On Products	68
If You Use LDAP with TLS (LDAPS)	69
Uninstalling	70
Technical References	71
Technical References	71
How Management and Security Server works	72
Configuration Utilities	73
Specifying a non-default location for MSSdata	78
Installing and Running MSS on a Locked-down System	79
Run services as a dedicated user	82
Legal Notice	84

1. Management and Security Server Installation Guide

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

1.1 At a Glance:

- [About Management and Security Server](#)
- [Installation Notes](#)
- [About Add-On Products](#)
- [If you are evaluating...](#)

1.2 About Management and Security Server

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

Management and Security Server 12.8.3 released with Host Access for the Cloud 2.7.3.

See the [MSS Release Notes](#) for a list of new features, resolved issues, and known issues.

1.3 Installation Notes

When you install or upgrade Management and Security Server, use the automated installer to install these components.

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

*The Security Proxy Server and Terminal ID Manager are optional Add-On Products that can be installed along with the other components. A license entitlement is required to enable and activate these products.

 **Note**

The manual installation files are no longer available. Check the [Installation Variations](#) if your system requirements differ from an automated installation.

1.3.1 Chained Installation

Because Management and Security Server (MSS) provides the MSS Administrative Console to manage Host Access for the Cloud and Reflection for the Web, MSS is installed automatically as a chained installation when you install either of those products.

After you install, 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.

1.3.2 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 additional configuration is required.

Add-on products include:

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

1.4 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.

2. Introduction

2.1 Introduction

From one central location, an administrator uses Host Access Management and Security Server (MSS) to create, secure, configure, and monitor Windows terminal client sessions, Reflection for the Web sessions, and browser-based Host Access for the Cloud sessions.

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

 **Note**

A compatible version of MSS is installed automatically during an installation of Host Access for the Cloud or Reflection for the Web.

2.1.1 In this section

- [What Management and Security Server installs](#)
- [Overview of Components and Add-On Products](#)

2.2 What Management and Security Server installs

Management and Security Server consists of servers, applications, and add-on products.

2.2.1 Installed and Enabled Components

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

- Host Access Management and Security Server
- Administrative Server (and its MSS Administrative Console)
- Metering Server
- Configuration Utilities
- Security Proxy *
- Terminal ID Manager *

* if entitled. The Security Proxy and Terminal ID Manager are add-on products, which must be appropriately licensed before they are enabled.

2.2.2 Add-On Products

Management and Security Server's functionality and security can be augmented with add-on products. Each add-on product requires a separate license and may require separate installation and activation. A unique activation file is provided for each add-on product.

See [Installing Add-On Products](#) for details.

More information

- [Overview of Components and Add-on Products](#)
- [How Management and Security Server works](#)

2.3 Overview of Components and Add-On Products

Management and Security Server (MSS) includes these components and add-on products:

- [Administrative Server](#)
- [Metering Server](#)
- [Configuration Utilities](#)
- [Activation Files](#)
- [Security Proxy Add-On](#)
- [Terminal ID Manager Add-On](#)
- [Automated Sign-On for Mainframe Add-On](#)
- [Automated Sign-On for Host Access Add-On](#)
- [Micro Focus Advanced Authentication Add-On](#)

2.3.1 Administrative Server

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

The user interface for the Administrative Server is the **MSS Administrative Console** .

MSS ADMINISTRATIVE CONSOLE

The MSS Administrative Console is the user interface for Management and Security Server's Administrative Server. Use the MSS Administrative Console to manage sessions, assign access to sessions, configure security settings, configure metering and add-on functionality, and to run reports.

2.3.2 Metering Server

Use the Metering Server to monitor the use of terminal sessions, including the number of connections and total connection time per user. The Metering Server does not require a separate license and is automatically installed with the Management and Security Server.

Before you can meter the use of terminal sessions, you must set up the Metering Server and enable the clients to be metered.

See [Setting Up Metering](#).

2.3.3 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 list items.

See [Configuration Utilities](#) for more information.

2.3.4 Activation Files

Activation files are used to enable product functionality. Each emulator client and add-on product that is managed by MSS has its own activation file, which enables communication with MSS. The activation file has this format:

```
activation.<product_name-version>.jaw
```

Notes about Activation Files

- **Compatibility.** We recommend installing the latest activation files to ensure that all product features are correctly enabled.
- **Installation.** The MSS automated installer typically installs the needed activation files, and the products are activated as part of the installation process. However, if activation was not part of the installation, you can complete the activation process in the **MSS Administrative Console** ([Configure Settings - Product Activation](#)).
- **Upgrading.** After adding new activation files, be sure to remove the older ones.
- **Clustering.** If you cluster servers for high availability, you must install or update the activation files on *each* clustered node. Activation files *are not replicated*.
- **Add-on products.** Check the "Setting up" sections in this guide to be sure your add-on products are installed *and* activated.

2.3.5 Security Proxy Add-On

The Security Proxy Server 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). The Security Proxy can be installed by the automated installer.

Note

It is best to install the latest activation files to ensure that all product features are correctly enabled. For example, when you upgrade MSS to version 12.8.3, also upgrade the Security Proxy to 12.8.3.

After you install the Security Proxy, refer to [Using the Security Proxy Server](#) (in the *MSS Administrator Guide*) to set certificates and configure secure sessions.

2.3.6 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). Terminal ID Manager can be installed by the automated installer.

See [Setting Up Terminal ID Manager](#).

2.3.7 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 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 MSS Administrative Console. Additional configuration is needed on the client emulator and the mainframe.

See [Setting Up Automated Sign-On for Mainframe](#).

2.3.8 Automated Sign-On for Host Access Add-On

MSS Automated Sign-On for Host Access enables an administrator to provide users with access to their assigned sessions using a single login.

To add Automated Sign-On for Host Access, you need to install the activation file and configure settings using the MSS Administrative Console. Additional configuration is needed on the client emulator and the host.

See [Setting Up MSS Automated Sign-On for Host Access](#).

2.3.9 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 the Micro Focus Advanced Authentication appliance.

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

See [Setting Up Micro Focus Advanced Authentication Add-On](#).

3. Preparing to Install MSS

3.1 Preparing to Install

Check these requirements before you install Management and Security Server.

- [Prerequisite Actions](#)
- [Minimum System Requirements](#)

3.2 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
- On Linux, verify fonts are installed
- Consider configuring an alternate temp directory

3.2.1 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.)

3.2.2 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 the MSSData directory (which stores site-specific content) must be installed to a non-default location, see the Technical Reference, [Specifying a non-default location for MSSData](#).

3.2.3 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`

3.2.4 On Linux, verify fonts are installed

If you are installing on a headless Linux system and no fonts are installed, you may encounter this error: `java.lang.Error: Probable fatal error: No fonts found`.

To resolve, ensure that `fontconfig` or at least one font is installed on the system.

3.2.5 Consider configuring an alternate temp directory

If you are installing Management and Security Server in a highly secure environment, where the `/tmp` directory may be restricted, we recommend configuring an alternate temp directory to enable a successful installation.

The installation of MSS requires a writable system temp directory, and if one is not available, the installer may fail to run.

Note

During operation, MSS uses an internal temp directory that should be suitable in all cases.

To configure a temp directory, see Technical Reference, [Installing and Running MSS on a Locked-down System](#).

More information

- [Minimum System Requirements](#)

3.3 Minimum System Requirements

Management and Security Server 12.8.3 supports these platforms and higher. The requirements do not take into account other applications and resources that may be installed on your system.

3.3.1 Administrative Server

Hardware:

- 3.40 GHz (4 cores) and 8 GB of RAM
- Sufficient drive space, typically 250GB when used on a drive with fast read/write capabilities
- 64-bit server-class system for production. For initial testing, a workstation could be used

Operating System

- Windows Server 2012
- SUSE Linux Enterprise Server (SLES) v12 SP4
- Red Hat Enterprise Linux 7.6
- Linux on z Systems:
 - SUSE Linux Enterprise Server (SLES) v12 SP4
 - Red Hat Enterprise Linux 7.6

3.3.2 Web browser

- Web browser
- JavaScript and cookies (always true)
- Other requirements vary according to the administrator's workstation and the users' workflow.

3.3.3 Additional system requirements

- Java 11 when using the "no JRE" installer (OpenJDK is provided in other cases)
- Prerequisites and requirements for Add-on Products:
 - [Security Proxy](#)
 - [Terminal ID Manager](#)
 - [Automated Sign-on for Mainframe](#)
 - [Micro Focus Advanced Authentication](#)

More information

- [Prerequisite Actions](#)

4. Installing MSS

4.1 Installing MSS

Use the **automated installer** to install the Management and Security Server components on Linux, UNIX, or Windows.

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 or Windows.
- can be run on UNIX (or z Linux) using the “no JRE” version of the automated installer.
- can install all components on the same machine (a workstation) for initial testing. However, for production, we recommend installing on a server operating system.

If you are not able to use an automated installer, [contact Customer Support](#) for guidance.

Note

For security purposes, it is advantageous to run services as a dedicated user with a minimal set of privileges. To perform this task, see the Technical Reference: [Run services as a dedicated user](#).

Continue with the [Installation Steps](#).

More information

- [Installation Steps](#)
- [Ports](#)
- [Installation Variations](#)

4.2 Installation Steps

Use the automated installer to install MSS.

Reminder

Be sure the [Prerequisite Actions](#) have been performed. Then, follow these steps.

4.2.1 Step 1: Run the automated installer

Consider installing your entitled activation files along with 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
Windows 64-bit	<code>mss-12.8.<n>.<nnn>-prod-wx64.exe</code>
Linux 64-bit	<code>mss-12.8.<n>.<nnn>-prod-linuxx64.sh</code>
z Linux	<code>mss-12.8.<n>.<nnn>-prod-unix-nojre.sh</code>

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 Products at a later time, see [Installing Activation Files](#).

To install the activation files now:

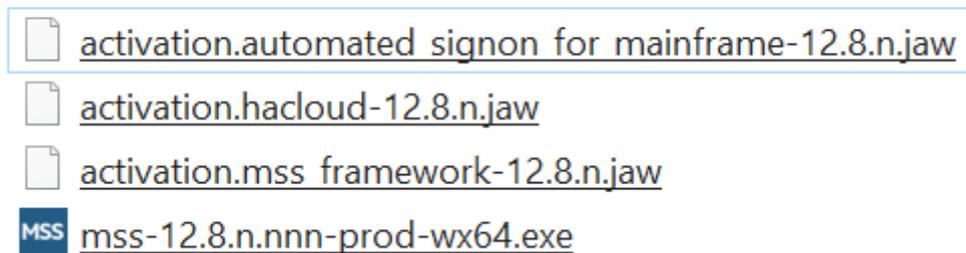
- a. Download the current version of the activation file for each of your Add-On Products from the Micro Focus download site (where you downloaded Host Access Management and Security Server).

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

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

On Windows, for example: to install the Automated Sign-On for Mainframe Add-On, place the activation file in the same folder as the installer, `mss-12.8.<n>.<nnn>-prod-wx64.exe`.

Name



3. Run the MSS installer.
4. Click **Next** to continue. The installer lists the products that will be enabled.
5. Read and accept the license agreement.
6. **Destination directory:** Accept the default installation directory, browse to a new directory, or enter the directory where you want to install.
7. Select the components to install, and then click **Next**.

Host Access Management and Security Server. Check this box to install the Administrative Server, which includes the MSS Administrative Console and Metering Server, and the default servlet runner.

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

8. Start Menu directory: On Windows, select the directory where you want to create the program shortcuts.

You have the option to create shortcuts for all users, or to suppress the creation of a Start Menu directory.

Click **Next**.

9. 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 MSS](#).)

4.2.2 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. Refer to [Ports used by MSS](#) as needed.

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 MSS Administrative Console.
4. **Servlet runner ports:** Accept the default entries or enter the port number that the servlet runner will use for HTTPS connections. The default port 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 MSS Administrative Console and to administer Metering and Terminal ID management (if installed). You can create different passwords for each server later.

 **Note**

To change the administrative password later, use the MSS Administrative Console (Configure Settings - General Security).

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, when available. 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 `InitialConfigurationUtility.log` in the `<installation>\utilities\logs` directory.

Click **Done**. You are ready for [Step 3: Start services](#).

4.2.3 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 MSS Administrative Console, 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 [Start services after installation](#).

2. Installation Complete. The components are installed and the services are started.

3. Continue with [Open the MSS Administrative Console](#).

Note

About IIS. If you installed MSS 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 \(on Windows\)](#).

Start services after installation

You can start the Micro Focus MSS Server after MSS is installed.

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.

4.3 Ports

Refer to this chart to identify the default ports and how to change them, if necessary.

Port used for...	Default port number	Comments
HTTPS - Administrative Console, Terminal ID Management, Metering, Metering Management	443	To change the port number: <ol style="list-style-type: none"> 1. Start the MSS server. This action creates the default <code>PropertyDS.xml</code> file in the MSSData directory 2. Open <code>PropertyDS.xml</code>. 3. In the string shown below, change the value from <code>443</code> to the preferred port number. <code>443</code> 4. Restart Management and Security Server.
Security Proxy listening	3000	
Security Proxy monitoring	8080	
Cassandra TLS inter-node communication	7001	
Cassandra JMX monitoring	7199	
X.509 authentication to MSS via Centralized Management	8000	Used by Desktop products when Centralized Management is enabled and by Reflection for the Web/MSS applets for X.509 authentication by end users.
Tomcat AJP ports used for IIS integration	8001, 8002	
X.509 Trusted subsystem (multiple servers)	8003	Used by MSS and HACloud to perform privileged administrative operations. NOTE: The X.509 port 8000 and the trusted subsystem port 8003 behave similarly. Both require X.509 client authentication. However, they use different trust stores and the operations that can be executed via those ports differ.
Metering server	8089	

Service registry	8761	
Cassandra client port	9042	
Cassandra sidecar	9043	
Service wrapper monitoring	32000-32001	If 32000 is not available, then 32001 is attempted
MSS JMX monitoring	44000	
Random port required by MSS JMX/RMI	Random	
Random port required by Cassandra JMX/RMI	Random	

4.4 Installation Variations

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

- [Installing on Unix with no JRE](#)
- [Integrating SiteMinder with MSS](#)
- [Using the automated installer in console mode](#)
- [Unattended installation](#)

4.4.1 Installing on Unix with no JRE

Use this option if your Unix platform (such as z/OS, z Linux, Mac, HP-UX, 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-12.8.<u>.<nnn>-prod-unix-nojre.sh
```

, where `<u>` is the update number and `<nnn>` is the build number.

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

Note: Your JRE must be Java version 11.

3. Be sure that the JCE Unlimited Strength Jurisdiction Policy Files are applied, and apply them each time you upgrade your JRE.

4.4.2 Integrating SiteMinder with MSS

When you integrate SiteMinder with Management and Security Server (MSS), you can leverage SiteMinder's single sign-on capabilities to authenticate your users. You can also configure additional authorization in MSS to restrict access to sessions.

Follow these steps to integrate MSS and SiteMinder.

1. Install or enable IIS v7 or higher.

IIS must be installed on the same machine where MSS is installed. Refer to your Windows help documentation for instructions on how to install or enable IIS.

2. Install a SiteMinder Web Agent.

Install a SiteMinder Web Agent on the same machine as the MSS server. The Web Agent can be configured to provide security for IIS. Refer to the SiteMinder documentation for detailed information about Web Agent installation and configuration.

3. Install MSS and integrate with IIS.

When you install or upgrade Management and Security Server, the MSS automated installer detects whether IIS is installed on your machine and offers to integrate it. Select the option to integrate Management and Security Server with IIS.

4. Add the SiteMinder libraries to MSS.

SiteMinder provides two different Agent libraries that are compatible with MSS. Choose one to add to your MSS installation:

- **Java JNI Agent.** This option is composed of a JAR file and several native modules, which are available on a Web Agent installation.

Copy the file from the SiteMinder Web Agent installation to the MSS Server installation:

Copy: `<Web Agent dir>\java\smjavaagentapi.jar`

To: `<MSS install dir>\server\services\shared\lib`

Make sure that the SiteMinder Web Agent bin directory is findable through the PATH variable for the Operating System.

- **Pure Java Agent.** This option is composed only of JAR files, which are available on the SiteMinder SDK.

Copy the JAR files from the SiteMinder SDK to the MSS Server installation:

`<SDK dir>\java[64]\smagentapi.jar`

`<SDK dir>\java\crypto.jar`

To: `<MSS install dir>\server\services\shared\lib`

Restart the MSS server.

5. Configure SiteMinder.

You must create a new security realm for MSS content. Add or edit a rule for the realm so that the effective resource is accessible to clients:

MSS: `<agent name>/mss*`

SiteMinder users must be authorized for `GET` and `POST` actions against the resource.

6. Configure a path to SiteMinder libraries in MSS.

By default, the path value in MSS for the native SiteMinder Web Agent libraries resolves to: `C:`

`\Program Files\CA\webagent\win64\binI`

If the path value for the SiteMinder libraries is different for your system, then update this value in the property named `wrapper.java.library.path.2` located in `MSS\server\conf\container.conf`.

When updating this value, note that the path separator character is a **forward slash (/)**, such as `wrapper.java.library.path.2=C:/Program Files/CA/webagent/win64/bin`

After the value is modified, restart the MSS server for the changes to take effect.

7. Configure SiteMinder Authentication in MSS.

In the MSS Administrative Console, open **Configure Settings - Authentication & Authorization**.

Select **SiteMinder** and click **Help** for details.

Note

If the SiteMinder option is **disabled** with the message to “See Help to enable,” then the SiteMinder Java Agent library has not been detected in the classpath for the MSS Server. *To resolve:* Be sure to complete step 4: Add the SiteMinder libraries to MSS (above).

Troubleshooting SiteMinder

- *Error: Failed to initialize SiteMinder libraries*

If you see this error message while configuring authentication, there may be a version conflict between SiteMinder binaries.

To resolve this issue:

- Locate the file, `smjavaagentapi.jar`, in your SiteMinder Web Agent installation.
- Copy the jar file to the web application’s lib directory.

The location can vary based on product and version. For MSS 12.4 and higher, the path is `<installation directory>\server\services\shared\lib`

In earlier versions, look for `\webapps\mss\WEB-INF\lib`.

- Restart the MSS server.

- *Error: “CA SiteMinder authentication required”*

When using SiteMinder with **Host Access for the Cloud**, SiteMinder does not recognize successful CA authentication and displays the error.

To resolve this issue:

- Open Windows Services > Micro Focus MSS Server.
- On the **Log On** tab, check the box to **Allow service to interact with desktop**.

When **Allow service to interact with desktop** is enabled, the PATH environment variable is available to the MSS service. When disabled, the PATH environment variable is empty, and the dependent jar files cannot be found.

- *Reflection for the Web users* must first authenticate using SiteMinder before they can access sessions. The SiteMinder Web Agent downloads a cookie to each user's browser memory, which authenticates them only for that browser session

4.4.3 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.

4.4.4 Unattended installation

Management and Security Server installation is based on install4j technology, which supports unattended mode. Unattended installation enables you to install the product the same way on a series of computers.

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.
4. 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 `<12.8.n.nnn>` is the product version and build number:

```
mss-<12.8.n.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."

More information

- [Open the Administrative Console](#)
- [Installation steps](#)

5. Opening the MSS Administrative Console

5.1 Opening the MSS Administrative Console

The **MSS Administrative Console** is the user interface for the **Administrative Server** -- the central component of Management and Security Server (MSS).

After you log in to the Administrative Server, use the MSS Administrative Console 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 Server](#)
- [Configure the Administrative Server](#)

5.2 Log in to the Administrative Server

You can log in to the Administrative Server (which opens the MSS Administrative Console) 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. (The servlet runner is automatically started by the MSS installer.)
2. Open the Administrative Server login page either from the Windows Start menu or from the URL:
 - Start > All Programs > Host Access Management and Security Server > **Administrative Server**
 - `https://<hostname>[:port]/adminconsole/`

Note

If the port number is `443` (the default for HTTPS), it is not needed in the URL. For example, `https://myserver.mycompany.com/adminconsole/`

This login directly opens the MSS Administrative Console.

3. In the **User** field, enter either `admin` (the default) or your site-specific user name.
4. Enter the administrator password specified during installation and configuration.
5. Click **Login**. The MSS Administrative Console opens to the **Manage Sessions** panel.

Note

The default password is `admin`. We recommend that you change this password as soon as possible. In the MSS Administrative Console, go to the **Configure Settings - General Settings** panel.

Next: [Configure the Administrative Server](#)

5.3 Configure the Administrative Server

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

5.3.1 Initial Settings

After you log in to the Administrative Server, set your initial preferences.

1. Open **Configure Settings - General Settings**. Enter your initial settings and preferences. Open **Help** for more information. Click **APPLY**.
2. Open **Configure Settings - General Security**. Scroll to the **Require new login** field.

Change the default to a higher number to avoid a session timeout while you are configuring settings. Click **APPLY**.

As you begin to work with the product features, open **Help** [?] and expand the Contents for more information.

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**.

5.3.2 Next Steps

When ready, you can configure the Metering Server, or install and configure your Add-On Products.

For details, see:

- [Setting Up Metering](#)
- [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](#)

6. Setting Up Metering

6.1 Setting Up Metering

Use the Metering Server to monitor session activity and to control concurrent access to specific hosts. Metering Reports are available as clients use the metered sessions.

The Metering Server is included with Management and Security Server (no separate license is required). When using the automated installer, the Metering Server is installed on the same machine as the Management and Security Server.

6.1.1 At a glance

Once installed, the Metering Server requires some additional setup. You must:

1. Configure the Metering Server in the MSS Administrative Console: **Configure Settings - Metering**.

Open **Help** for assistance.

2. On the Configure Settings - Metering panel, click the link to a Metering Server to open the separate **Metering Console** (after you log in as a Metering administrator).

Use the Metering Console to configure license pools and server settings and to run reports.

Open **Help** for assistance.

3. Enable the **clients** that are to be metered.

Refer to your emulator's product documentation to enable metering for that client.

6.1.2 Prerequisites and System Requirements

The Metering server, which is installed with Management and Security Server, is compatible with the [MSS Minimum System Requirements](#).

More information

- [How Metering Works](#)

6.2 How Metering Works

When the configuration is complete, here's how the Metering Server communicates with the metered client.

1. A user starts a client session and initiates a host connection.
2. The session requests a license from the Metering Server, and once granted, the host connection proceeds, and the Metering Server begins to record product usage.
3. The session sends updates to the Metering Server at regular intervals until the user closes the session.
4. The metering data is available for the administrator to generate reports.

You can filter **Metering Reports** to show

- activity by user, machine, IP address, and other attributes
- concurrent usage (to comply with your license)
- host connections

More information

- [Setting up Metering](#)

7. Installing Add-On Products

7.1 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
- Automated Sign-On for Host Access
- 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-version>.jaw
```

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

More information

- [Installing Activation Files](#)
- [Upgrading Add-On Products](#)

7.2 Installing Activation Files

Add-On Products and other products can be installed in two ways:

- Use the automated installer to install activation files
- Use the MSS Administrative Console to install activation files

7.2.1 Use the automated installer to install activation files

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

Note

The `activation.mss_framework-12.8.n.jaw` activation file is automatically installed to enable the Host Access Management and Security Server framework.

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 Automated Sign-on for Mainframe Add-On, place the activation file in the same folder as the installer, `mss-12.8.n.<nnn>-prod-wx64.exe`.

Name

	<u>activation.automated signon for mainframe-12.8.n.jaw</u>
	<u>activation.hacloud-12.8.n.jaw</u>
	<u>activation.mss framework-12.8.n.jaw</u>
	<u>mss-12.8.n.nnn-prod-wx64.exe</u>

3. Run the MSS installer.

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

To see which Add-On products are installed, see the **Product** list on the **Configure Settings - Activate Products** panel.

7.2.2 Use the MSS Administrative Console to install activation files

The activation files for add-on products can be installed or upgraded using the **Configure Settings - Activate Products** panel in the MSS Administrative Console. 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 MSS Administrative Console, click **Configure Settings - Product Activation**.
3. Click **ACTIVATE NEW** and browse to the activation file for the product you want to install:

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

4. Click the file. The new product is installed and added to the Product list.
5. After the add-on product is installed, be sure to configure settings to activate and use the product.
6. Restart your browser to ensure that the MSS Administrative Console 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 detailed steps, open the product Help to [Configure Settings - Product Activation](#), and click **Complete the Activation**.

Steps are available for

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

8. Setting Up the Security Proxy

8.1 Setting Up the Security Proxy

When you use the Security Proxy Server, data sent between the client session and the Security Proxy is TLS-encrypted, and the host is protected from direct user contact.

The Security Proxy is an add-on product that must be

- **installed** on the desired server
- **activated** so it can be managed by Management and Security Server
- **configured** to trust Management and Security Server (using the Security Proxy Wizard)

 **Note**

The Security Proxy is *automatically* installed, activated, and configured when you install it along with Management and Security Server (using the automated installer).

If you choose to install it separately, continue with the steps in this section to **install** and **activate** the Security Proxy.

After you verify that the system and performance requirements are met, see [Using the Security Proxy Server](#) (in the *MSS Administrator Guide*) to **configure** the Security Proxy.

More information

- [Security Proxy: Prerequisites and System Requirements](#)
- [Install and Activate the Security Proxy Server](#)

8.2 Security Proxy: Prerequisites and System Requirements

The Security Proxy Add-On requires a separate license. The Security Proxy requirements are in addition to the [MSS Minimum System Requirements](#).

Before installing the Security Proxy, verify that:

- the Management and Security Server automated installer is available. (The Security Proxy can be installed along with MSS or by itself later.)
- the Security Proxy activation file (`activation.security_proxy-12.8.<n>.jaw`) is available.

Note

We recommend installing the latest activation files to ensure that all product features are correctly enabled. For example, when you upgrade Management and Security Server to 12.8.3, be sure to upgrade the Security Proxy to 12.8.3.

- the [Performance and Scaling Requirements](#) are addressed.

8.2.1 Performance and Scaling Requirements

The Security Proxy Server's performance is affected by the hardware, software, and environmental factors. Follow these guidelines for best performance.

We recommend these specifications for up to 6000 concurrent and active connections.

System Specification	up to 6000 connections (concurrent and active)
Speed of processors	2.7 GHz or faster
Number of processors (or cores)	4 or more
System RAM	4 GB or more
Java Virtual Machine (JVM) heap size	3 GB
File descriptors (Linux/UNIX)	21,000

Additional specifications

- [Number of Available Ports and Descriptors](#)
- [Number of Concurrent Connections](#)
- [Operating System](#)
- [Server Dedication](#)
- [Key Lengths and Cipher Suites](#)

8.2.2 System Specification - Details

Speed of Processors

As a general rule, a faster processor performs operations more quickly. The two most processor-intensive operations performed by the Security Proxy server are establishing new connections and encrypting and decrypting data.

Number of Processors (or Cores)

The Security Proxy server is a thread-intensive application. Each connection to the Security Proxy spawns two threads. A system with more processors (or cores) will perform better than one with fewer processors.

System RAM

Each connection requires memory, and more connections can be made with more memory. More RAM installed on the machine means less paging to disk and better overall performance. A minimum of four gigabytes (4 GB) RAM is recommended.

Java Heap Size

A 64-bit JRE with a heap size of 3 GB can support 6000 concurrent connections.

The installer will install and configure the Security Proxy server to use a server JVM. By default, the server JVM will allocate a heap space that is equal to one quarter the size of physical memory. For example, if a computer has 8 GB of physical memory, then the server JVM will allocate a maximum heap size of 2 GB. To increase the heap allocation, use the JVM command-line options `-Xms` and `-Xmx`, which can be set in the `MssSecurityProxy.vmoptions` file, located in `<Security Proxy installation directory>\bin`.

For example, to support 6,000 connections, use a text editor to open the file named `...` `\MSS\securityproxy\bin\SecurityProxy.vmoptions` and add (or edit) the following lines to this file:

```
-Xms3g
-Xmx3g
```

8.2.3 Additional Specifications - Details

Number of Available Ports and Descriptors

You may need to increase the number of ports or file descriptors made available by the operating system.

WINDOWS SERVER - PORTS

The default number of ephemeral ports is 5000. Use these commands to show or change the number of ports.

- To print the number of ports available:

```
netsh int ipv4 show dynamicportrange tcp
```

- To change the number of available ports:

```
netsh int ipv4 set dynamicport tcp start=10000 num=6000
```

LINUX OR UNIX - DESCRIPTORS

The default number of file descriptors (and thus ports) available to a process can be low (in the hundreds).

Each security proxy server needs approximately 20 file descriptors, and each connection uses two file descriptors. To determine the number of file descriptors required, use this formula:

```
number of descriptors = 20 + (<connections> * 2)
```

where `<connections>` represents the maximum number of concurrent connections the Security Proxy server may receive. Note: The permitted number of concurrent sessions is governed by your product license.

For example: `20 + (6000 connections * 2) = 12020 descriptors`

To increase the number of descriptors:

1. As a user with root privileges, open the command shell that launches the Security Proxy server. This shell should be the same one used to configure the Security Proxy server.
2. At the command line, enter:

```
ulimit -n <descriptors>
```

where `<descriptors>` represents the integer number of descriptors needed to support the Security Proxy connections.

 **Note**

- The `ulimit` command syntax may vary depending on your shell. For more information about using the command, refer to your OS documentation or man pages.
- The shell inherits the default limit from the kernel variable `rlim_fd_cur` value set in the `/etc/` system file. The maximum number of descriptors that can be set (“hard limit”) is governed by the kernel variable `rlim_fd_max`.

Number of Concurrent Connections

Through considerable stress testing, it has been demonstrated that the Security Proxy server can maintain 6,000 concurrent and active connections with heavy payloads, as long as the Security Proxy: Prerequisites and System Requirements are met and a 64-bit JRE is used.

Operating System

Slightly better performance was observed on a Linux-based system with respect to time taken to establish connections and data transmission rates.

Server Dedication

A dedicated Security Proxy server will perform better than a server that performs multiple functions. For example, if the server acts as a web server, a mail server, or as a host, in addition to acting as a Security Proxy server, performance for all concurrent functions will be affected.

Key Lengths and Cipher Suites

The Security Proxy server uses two distinct cipher algorithms to establish and secure a TLS connection. A public key algorithm (DSA or RSA) is used during the connection process to authenticate the server and exchange shared-secret (symmetric) keys for the secure connection.

KEY LENGTHS USED FOR AUTHENTICATION

A longer DSA or RSA public key will slow the initial connection speed but may be suitable when security is a primary concern. Open the Security Proxy Wizard to view or modify the key length.

CIPHER SUITES USED FOR DATA ENCRYPTION/DECRYPTION

The cipher suites used in session data encryption/decryption can dramatically affect the connection speed once the connection is established. The default cipher suite is RSA with 128-bit AES SHA-1.

Use the Security Proxy Wizard (Proxies > Modify) to select different cipher suites.

More information

- [Install and Activate the Security Proxy Server](#)

8.3 Install and Activate the Security Proxy Server

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

Note

About secure connections. The Security Proxy Server can be installed on the same machine as the Administrative Server or on a different machine. Although data between the terminal session and the Security Proxy server is encrypted, data between the Security Proxy server and the host is typically not encrypted.

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

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. If you select **End to end encryption** when configuring a session, the connection between the Security Proxy and the host will use TLS.

8.3.1 Installation options

You can install the Security Proxy either at the same time or after you install Management and Security Server (the Administrative Server). Choose an option.

- To install the Security Proxy **WHEN** you install the MSS Administrative Server
- To install the Security Proxy **AFTER** you install the MSS Administrative Server

Note

If you are not able to use the automated installer, contact [Support](#) for guidance.

8.3.2 Installing the Security Proxy *WHEN* you install the MSS Administrative Server

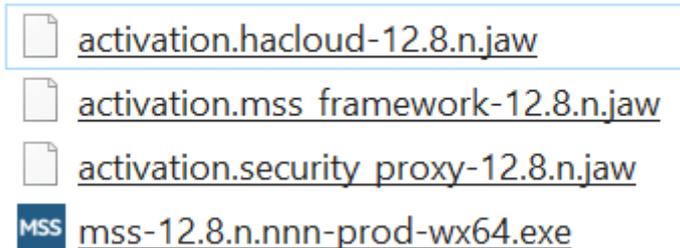
Using this option, the MSS automated installer (and Configuration Utility) automatically installs, configures, and activates the Security Proxy. This approach saves time and reduces the risk of errors.

Be sure the Security Proxy Add-On activation file is available for download. (A separate license is required.)

1. Download the Security Proxy Add-On activation file, `activation.security_proxy-12.8.n.jaw`, and note the location.
2. Place the security proxy activation file in the same folder as the MSS automated installer.

In this example, the Host Access for the Cloud activation file is also installed.

Name



3. Run the MSS installer for your platform. During installation, be sure BOTH boxes are checked:

- Host Access Management and Security Server
- Security Proxy Server

4. When prompted, run the **Initial Configuration Utility**.

This utility generates cryptographic keys and self-signed certificates, automates configuration, and sets a port value for the Security Proxy.

The automated installer also places the activation file in the installation directory:

```
/MSS/securityproxy/lib/modules
```

The Security Proxy is now installed, activated, and configured.

5. To view or change the configuration, open the **Security Proxy Wizard** from the **Start** menu.

For details, see [Using the Security Proxy Server - Configure and Start the Security Proxy Server](#) (in the MSS Administrator Guide).

8.3.3 Installing the Security Proxy AFTER you install the MSS Administrative Server

You can add the Security Proxy to MSS after the MSS Administrative Server is already installed.

Keep in mind that the Security Proxy needs to be installed, activated, and configured, which can be done either automatically or as separate actions. Choose a method:

- [Automatically install](#)
- [Separately install](#)

Automatically install, activate, and configure the Security Proxy

To install the Security Proxy when the compatible version of the Administrative Server is already installed, you can re-run the automated installer.

Use the same steps: To install the Security Proxy WHEN you install the MSS Administrative Server.

Separately install, activate, and configure the Security Proxy

Or, you can install the Security Proxy server without the activation file, and later upload the security proxy activation file using the MSS Administrative Console. Then, use the Security Proxy Wizard to configure the Security Proxy server.

1. Install.

Run the MSS automated installer and check BOTH boxes – for Host Access Management and Security Server and the Security Proxy Server.

- Host Access Management and Security Server
- Security Proxy Server

 **Note**

If only the Security Proxy Server is checked, the MSS files are removed.

2. Activate.

Download the activation file for the Security Proxy Add-On, and note the download location.

`activation.security_proxy-12.8.n.jar`

3. In the MSS Administrative Console, click **Configure Settings - Product Activation**.

4. Click **Activate New** and browse to `activation.security_proxy-12.8.n.jar`

5. Click the file. The **Security Proxy Add-On** is installed and added to the **Product** list.

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

The Security Proxy is now installed and activated.

7. Configure.

Use the **Security Proxy Wizard** to configure settings and manage certificates. Then, you can configure sessions to use the Security Proxy.

Follow the steps in [Using the Security Proxy Server](#) (in the *MSS Administrator Guide*).

In brief, you will:

- Configure and Start the Security Proxy Server
- Import the Security Proxy certificates
- Create Secure Sessions
- Assign Secure Sessions
- Run Reports

9. Setting Up Terminal ID Manager

9.1 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 and an activation file.

Follow these steps to install Terminal ID Manager by running the MSS automated installer – either on the same machine or a different machine from where MSS is installed.

Then, use the [Terminal ID Manager Guide](#) to complete the configuration.

More information

- [Prerequisites and System Requirements](#)
- [Run the MSS automated installer](#)
- [Configure Terminal ID Manager](#)

9.2 Terminal ID Manager: Prerequisites and System Requirements

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

- Management and Security Server is installed (on the same or a different machine).
- Terminal ID Manager Add-On **activation file** is available.
- Your emulator and session types are supported:

Web-based session types

Support for Terminal ID Manager is available in **Host Access for the Cloud and Reflection for the Web** for these session types:

- IBM 3270, IBM 3270 Printer
- IBM 5250, IBM 5250 Printer
- ALC, Airlines Printer
- T27, T27 Printer
- UTS

Windows-based Desktop sessions

Refer to your product documentation to check whether your emulator session type supports Terminal ID Manager.

Next steps:

- [Run the MSS automated installer](#)
- [Configure Terminal ID Manager](#)

9.3 Run the MSS Automated Installer

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

For maximum flexibility and performance, you may want to install the Terminal ID Manager Add-On on a separate machine from the one used by the Administrative Server (where Management and Security Server is installed).

Use the MSS automated installer to place the activation file in the required location.

Follow the steps for installing Terminal ID Manager either on a separate or the same machine:

- [To install Terminal ID Manager on a separate machine](#)
- [To install Terminal ID Manager on the same machine](#)

9.3.1 Installing Terminal ID Manager on a *separate* machine

1. Run the Management and Security Server (MSS) automated installer on a different machine from where MSS was initially installed.

Note

The Terminal ID Manager **activation file** must also be on the separate machine.

For ease of installation, place the activation file, `activation_terminal_id_manager-12.8.n.jaw`, in the same directory as the automated installer. When you run the installer, the activation file will be placed in the required location.

2. In the early installation panel, select *only* the **Administrative Server**. (Leave the Security Proxy unchecked on the separate machine.)
3. When the **Initial Configuration Utility** panel displays, enable *only* the **Terminal ID Manager** service.
4. Check to be sure that the Terminal ID Manager activation file (`activation_terminal_id_manager-12.8.n.jaw`) is installed on the separate machine in this location:

```
C:\Program Files\Micro Focus\MSS\server\web\webapps\tidm\WEB-INF\lib\modules
```

 If the activation file is *not present*, copy it from your download location to the ... `\tidm\WEB-INF\lib\modules` directory on the separate machine.
5. When you return to the automated installer, select the option to **Start the server components now**.

Next: [Configure Terminal ID Manager](#)

9.3.2 Installing Terminal ID Manager on the same machine

If you installed Management and Security Server without selecting Terminal ID Manager, you can run the automated installer again to update the installation to include Terminal ID Manager on the same machine.

1. Run the MSS automated installer to install Terminal ID Manager.

 **Note**

The Terminal ID Manager **activation file** must also be on this machine.

For ease of installation, place the activation file, `activation_terminal_id_manager-12.8.n.jaw`, in the same directory as the automated installer. When you run the installer, the activation file will be placed in the required location.

2. On the early installation panel, check that the **Terminal ID Manager** will be enabled.
3. When the automated installer completes, select the option to **Start the server components now**.
4. Verify that the Terminal ID Manager **activation file** is installed:
 - a. In the MSS Administrative Console, open **About > Activated Products**.
 - b. In the **Product** column, look for **Terminal ID Management Add-On**.
 - If *present*, the activation file is installed on this machine.
 - If *not present*, click **ACTIVATE NEW**, and upload the activation file from your download location.

Next: [Configure Terminal ID Manager](#)

9.4 Configure Terminal ID Manager

After installation, Terminal ID Manager must be enabled in the **MSS Administrative Console**.

Then, you can configure server settings and monitor terminal IDs in the **Terminal ID Manager Console**.

Refer to the [Terminal ID Manager Guide](#) to complete the configuration.

10. Setting Up Automated Sign-On for Mainframe

10.1 Setting Up Automated Sign-On for Mainframe

Automated Sign-On for Mainframe is an add-on product that enables you to configure user access to z/OS mainframe applications using a single login. This add-on product requires a separate license.

10.1.1 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.

More information

- [Installing Automated Sign-on for Mainframe](#)

10.2 Installing Automated Sign-On for Mainframe

The Automated Sign-On for Mainframe Add-on product 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-12.8.n.jaw
```

2. Download the activation file and note the location.
3. In the Management and Security Server, open the MSS Administrative Console and click **Configure Settings - Product Activation**.
4. Click **ACTIVATE NEW** and browse to

```
activation.automated_signon_for_mainframe-12.8.n.jaw
```

.
5. Click the file. The **Automated Sign-On for Mainframe Add-On** is installed and added to the **Product** list.
6. Restart your browser to ensure that the MSS Administrative Console is fully updated with the new set of activation files. You do not need to restart the Administrative Server (MSS Server) service.

10.2.1 Next step

After Automated Sign-on for Mainframe Add-On is activated, settings must be configured on different systems:

- z/OS
- Management and Security Server
- your emulator

Refer to the [Automated Sign-on for Mainframe - Administrator Guide](#) for details.

11. Setting Up MSS Automated Sign-On for Host Access

11.1 Setting Up MSS Automated Sign-On for Host Access

MSS Automated Sign-On for Host Access is an add-on product that enables you to configure user access to host applications using a single login. This add-on product requires a separate license.

 **Note**

If you are using a z/OS system, see [Setting Up Automated Sign-On for Mainframe](#).

11.1.1 Prerequisites and System Requirements

Before installing or configuring MSS Automated Sign-On for Host Access, 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 MSS Automated Sign-On for Host Access Add-On activation file is available (after purchase).
- LDAP directory is used for user authorization.

More information

- [Installing Automated Sign-on for Host Access](#)

11.2 Installing MSS Automated Sign-On for Host Access

The MSS Automated Sign-On for Host Access Add-on product is installed with an activation file. Follow these steps.

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

```
activation.automated_signon_for_hostaccess-12.8.n.jaw
```

2. Download the activation file and note the location.

3. In the Management and Security Server, open the MSS Administrative Console and click **Configure Settings - Product Activation**.

4. Click **ACTIVATE NEW** and browse to

```
activation.automated_signon_for_hostaccess-12.8.n.jaw.
```

5. Click the file. The **MSS Automated Sign-On for Host Access Add-On** is installed and added to the **Product** list.

6. Restart your browser to ensure that the MSS Administrative Console is fully updated with the new set of activation files. You do not need to restart the Administrative Server (MSS Server) service.

11.2.1 Next step

After Automated Sign-on for Host Access Add-On is activated, settings must be configured on different systems:

- your host
- Management and Security Server (MSS)
- your emulator

Refer to the technical reference, **Configuring MSS Automated Sign-on for Host Access**, in the [MSS Administrator Guide](#) for details.

12. Setting Up Advanced Authentication Add-On

12.1 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 the Micro Focus Advanced Authentication product.

12.1.1 Prerequisites and System Requirements

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

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

Tip

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

More information

- [Installing and Configuring Micro Focus Advanced Authentication Add-On](#)

12.2 Installing and Configuring Advanced Authentication Add-On

Three basic steps are required to install and configure the Micro Focus Advanced Authentication Add-On. Before starting, make sure you've met the [system requirements](#).

12.2.1 Step 1: Install 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-12.8.n.jaw`

2. Download the activation file and note the location.
3. In the Management and Security Server, open the MSS Administrative Console and click **Configure Settings - Product Activation**.
4. Click **ACTIVATE NEW** and browse to `activation.advanced_authentication-12.8.n.jaw`.
5. Click the file. The **Advanced Authentication Add-On** is installed and added to the **Product** list.
6. Restart your browser to ensure that the MSS Administrative Console is fully updated with the new set of activation files. You do not need to restart the Administrative Server (MSS Server) service.

12.2.2 Step 2: Set up Advanced Authentication in the MSS Administrative Console

In the MSS Administrative Console:

1. Open **Configure Settings - Authentication & Authorization**, and click **Micro Focus Advanced Authentication**.
2. Open **Help [?]** and follow the steps to configure Advanced Authentication.

12.2.3 Step 3: Configure authentication methods

To configure Advanced Authentication methods, such as Voice, refer to your [Micro Focus Advanced Authentication server documentation](#).

13. Troubleshooting the Installation

Check this section if you encounter issues after running the Management and Security Server installer.

13.1 Installation does not complete on UNIX or Linux platforms

The MSS installer, server, or configuration utilities may stall on UNIX or Linux systems, particularly headless ones. This delay is caused by an insufficient amount of entropy in the system. In some environments, cryptographic operations can strain the Java Virtual Machine's entropy source. An insufficient pool of entropy can result in long delays during server startup and at other times while additional entropy is collected.

To remedy the issue: Install either a hardware-based random number generator or a software-based entropy daemon, such as [Haveged](#) or [Rng-tools](#).

Note

Some platforms already install and enable an entropy service by default.

More information

- See Knowledge base article, [Ensuring Sufficient Entropy](#).
- For further assistance, contact [Customer Support](#).

14. Upgrading

14.1 Upgrading MSS

Use the automated installer to upgrade to Management and Security Server (MSS) 12.8.3.

14.1.1 Before you begin

Caution

Check this list before you begin upgrading.

- Back up system data before upgrading.
- **Compatibility.** Check the versions of the products that use MSS to be sure that connections work as expected.
- **Activation files.** We recommend installing the latest activation files to ensure that all product features are correctly enabled. Be sure to remove the activation files associated with previous versions.
- **Clustering.** When upgrading clustered MSS servers, you need to install the upgraded activation files to each clustered node. The activation files are not replicated.
- If you used **Replication** in a previous version, you can use the simplified [Clustering](#) workflow in MSS. See [Upgrading Replicated Servers](#).
- **Manual installation is no longer supported.** If your current version was installed using manual installation files -- *and you cannot use an automated installer* -- contact [Customer Support](#) for guidance.

14.1.2 Downloading 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 (MSS), your purchased Add-On Products are also listed.

1. Download the automated installer 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-version>.jaw.`

We recommend installing the latest activation files to ensure that all product features are correctly enabled.

3. Place the activation files in the same location as the automated installer.
-

More information

- [Upgrading the Security Proxy Server](#)
- [Upgrading Replicated Servers](#)
- [Upgrading Add-On Products](#)

14.2 Upgrading the Security Proxy Server

When you upgrade Management and Security Server, note these requirements for the Security Proxy.

14.2.1 Check the version

We recommend installing the latest activation file to ensure that all product features are correctly enabled. For instance, when you upgrade to MSS 12.8.3, also upgrade the Security Proxy to version 12.8.3.

Download the upgraded Security Proxy activation file and run it with the automated installer. Or, install the activation file and activate the server. See [Install and Activate the Security Proxy Server](#).

14.2.2 Synchronize an upgraded Security Proxy

If the Security Proxy is installed when you upgrade Management and Security Server, be sure to synchronize the Security Proxy with the MSS Administrative Server.

To synchronize the Security Proxy:

1. Open the **Security Proxy Wizard** (from the Start menu).

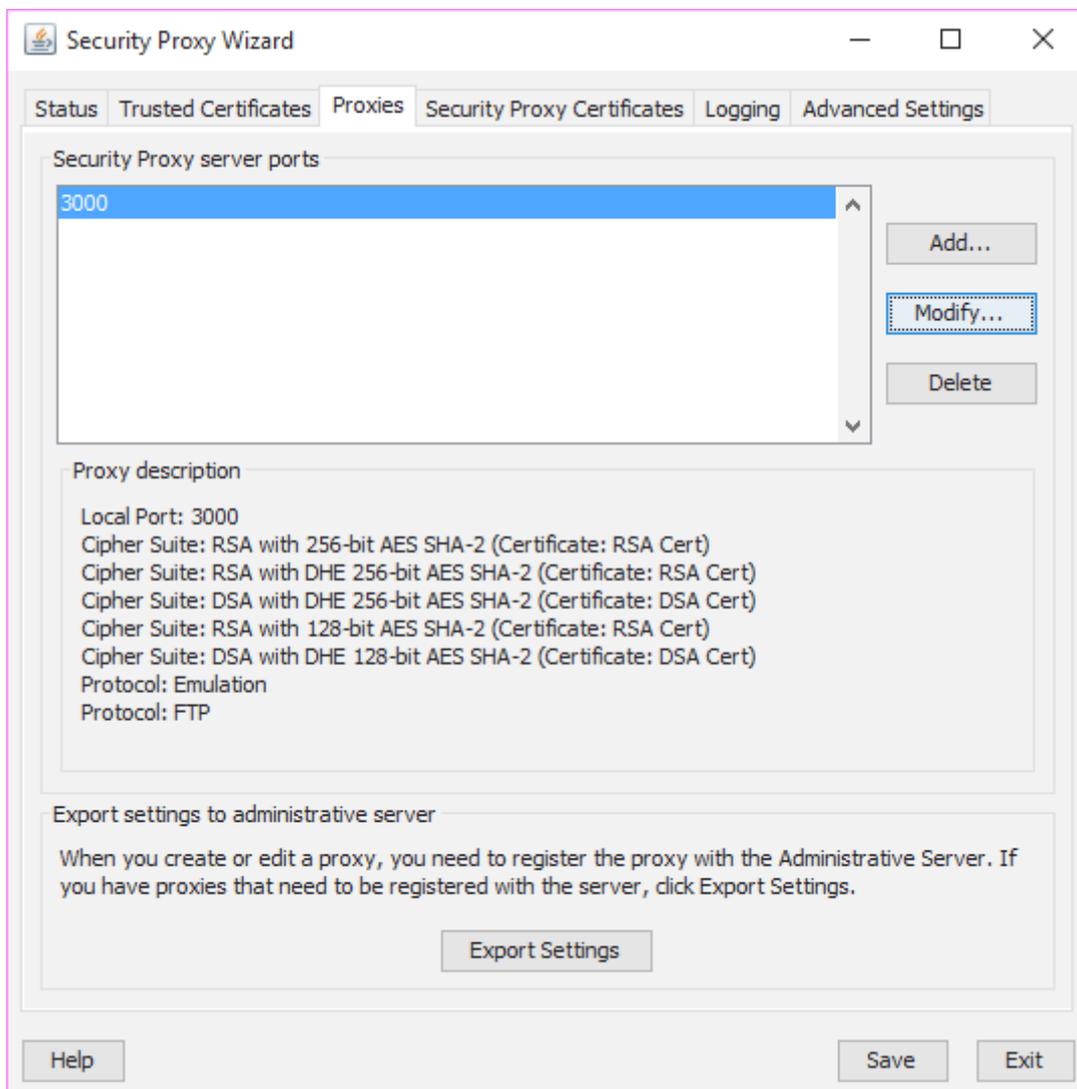
Caution

TLSv1.1, TLSv1, and SSL 3.0 are no longer supported. If you see a warning, review your selected Protocols on the **Advanced Settings** tab.

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:
 - a. Click the **Proxies** tab > **Modify**.
 - b. Note (or change) the selected cipher suites.

- c. Select an RSA certificate or DSA certificate for that type of cipher suite. Click **OK**.
- d. On the **Proxies** tab, click **Save**.
- e. Click **Export** to send the settings to the MSS Administrative Server.

14.3 Upgrade Replicated Servers

Replication, in earlier versions of MSS, has been replaced with *Clustering*. To upgrade the servers that are replicated, you must first disable Replication and then configure Clustering.

Caution

Before you upgrade and begin to configure Clustering, all servers previously configured for Replication must be set to **Standalone** – no Master or Slaves.

To disable Replication on every server configured for replication, begin with the **Slave** servers. Then, disable Replication on the **Master**.

1. In the MSS Administrative Console, click **Configure Settings - Replication**.
2. Select the **Standalone** Server Role. Click **Apply**.
3. Repeat steps 1 and 2 for all of the Slave servers and then for the Master server.
4. When all of the servers are set to Standalone, upgrade each server.
5. When all of the servers are upgraded, configure a **cluster** of at least three MSS servers.

Follow the *Clustering* steps in the MSS Administrator Guide.

14.4 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 Management and Security Server product files.

We recommend installing the latest activation files to ensure that all product features are correctly enabled.

To upgrade your add-on products, either:

- [Use the MSS automated installer](#)
- or
- [Use the MSS Administrative Console to install activation files.](#)

14.4.1 Use the MSS automated installer

To upgrade using the automated installer:

1. If you are upgrading **Add-On Products**, place the downloaded activation files in the same directory as the automated installer.

In this example, the Automated Sign-on for Mainframe and the Security Proxy Add-on products will be installed.

Name

	<u>activation.automated signon for mainframe-12.8.n.jaw</u>
	<u>activation.mss framework-12.8.n.jaw</u>
	<u>activation.security proxy-12.8.n.jaw</u>
	<u>mss-12.8.n.nnn-prod-wx64.exe</u>

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 the Configuration Upgrade Utility or re-create your sessions.

14.4.2 Use the MSS Administrative Console to install activation files

You can install upgraded activation files using the same procedure as installing the initial files.

See [MSS Administrative Console to install activation files](#).

14.5 If You Use LDAP with TLS (LDAPS)



Note

When you upgrade Management and Security Server, you must re-establish trust of your LDAP server when using TLS (LDAPS).

Background

When LDAP authentication or authorization is configured to use LDAPS, the LDAP server is secured with a certificate. The cacerts file containing the trusted CA certificate is overwritten when Management and Security Server is upgraded, and LDAPS connections fail.

Workaround

To re-establish trust of the LDAP server, use the **IMPORT CERTIFICATE** function.

1. In the MSS Administrative Console, open **Configure Settings – Authentication & Authorization**.
2. Scroll to and check the affected LDAP server. Click **EDIT**.
3. Scroll to and click the **IMPORT CERTIFICATE** button. A dialog presents the certificate for this server.

If this button is not present, then TLS is not used for authentication of the LDAP server, and the issue documented here does not apply.

4. Click **IMPORT**. A message confirms “The server is trusted.”

15. Uninstalling

 **Note**

When upgrading, the MSS automated installer will uninstall the previous installation and preserve some customized data, such as MSSData. You do not need to run a separate uninstall.

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.

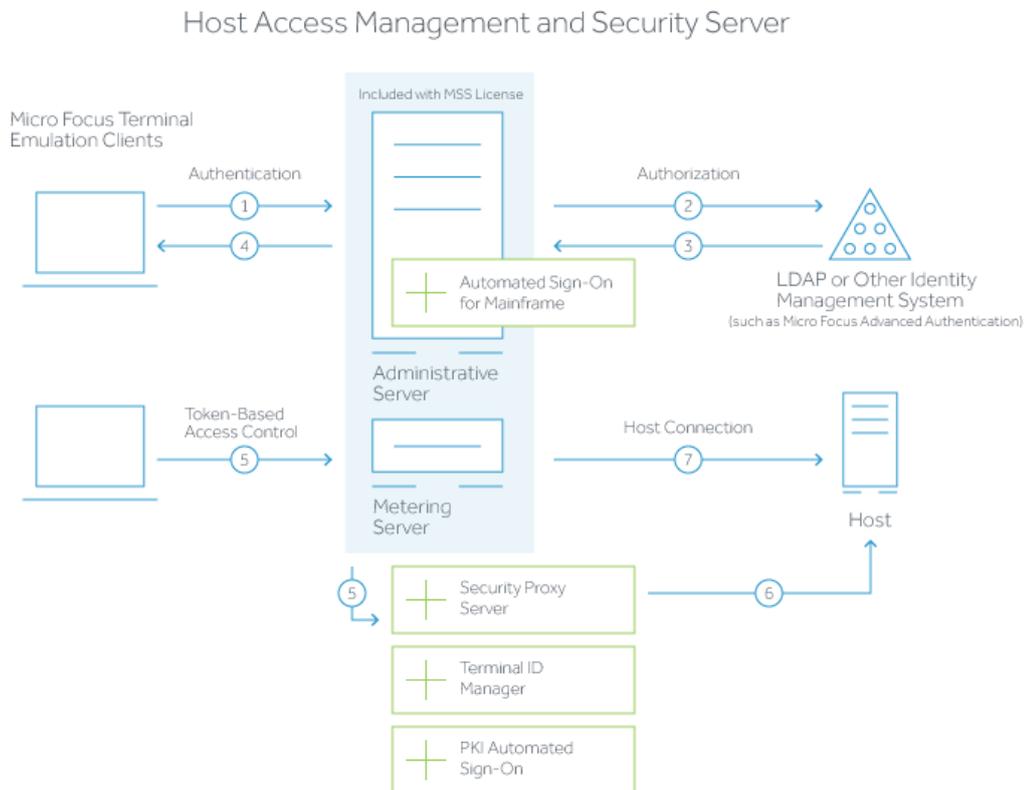
16. Technical References

16.1 Technical References

- [How Management and Security Server Works](#)
- [Configuration Utilities](#)
- [Specifying a non-default location for MSSData](#)
- [Installing and Running MSS on a Locked-down System](#)
- [Run services as a dedicated user](#)

16.2 How Management and Security Server works

This diagram depicts the flow of secure interactions between a client and the host in a typical host session, using Management and Security Server. Note the option to use the Security Proxy Server and other Add-On products.



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 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.

16.3 Configuration Utilities

During and after the installation of Management and Security Server, you may be directed to run one or more of these utilities.

- [Initial Configuration Utility](#)
- [Configuration Upgrade Utility](#)
- [HTTPS Certificate Utility](#)
- [IIS Integration Utility \(on Windows\)](#)

16.3.1 Initial Configuration Utility

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

- 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.

16.3.2 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 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

Before you begin:

1. 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.

2. Verify that you have administrator privileges. If not, you will be prompted for credentials.
3. 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
```

4. Enter (or verify) your configuration information, as prompted.

16.3.3 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.)

The HTTPS Certificate Utility can be used to create a private key and generate a Certificate Signing Request (CSR). You can then import the signed certificate and the private key.

Running the HTTPS Certificate Utility

The HTTPS Certificate Utility can be run at any time after Management and Security Server is installed.

1. Verify that you used the HTTP Server functionality that was provided during installation.
2. Run the utility.

On Windows:

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

On Linux or UNIX:

```
[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.
- Generate a new private key and Certificate Signing Request.
- Import a certificate and private key.
- Import the Management and Security Server certificate and private key.



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. Any existing keys will be overwritten by either utility.
- You can configure Management and Security Server to use either a self-signed certificate, or a CA-signed SSL server certificate.

REQUIRING HTTPS IN THE ADMINISTRATIVE SERVER

Beginning in version 12.8, Management and Security Server requires HTTPS. No additional setting is needed in the MSS Administrative Console to restrict the Administrative Server to the HTTPS protocol.

16.3.4 IIS Integration Utility

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. This

question appears 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, such as authentication to the Administrative Console and to the HTML Assigned Sessions list.
- 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\Microsoft 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.

16.4 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.

The default location for MSSData:

- **On Windows:**

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

- *On Linux or UNIX:*

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

16.4.1 Changing the location

If you have a special circumstance that requires a non-default location for MSSData, edit the `container.properties` file to specify the location of the MSSData directory.

This single setting is used by the MSS, Metering, and Terminal ID Manager servers.

1. Locate and open the `container.properties` file in a text editor.

- **On Windows**, open `C:\Program Files\Micro Focus\MSS\server\conf`.
- **On Linux or UNIX**, open `/opt/microfocus/mss/conf`.

2. Replace `dataFolder=rwebdata_location_placeholder` with the location and name of the directory you define. Follow these examples.

- **On Windows:** `dataFolder=c:\\data\\MSSData`
- **On Linux or UNIX:** `dataFolder=/var/data/mssdata`

3. Save your changes and restart the MSS Server.

16.5 Installing and Running MSS on a Locked-down System

During operation, MSS uses an internal temp directory that should be suitable in all cases.

However, the *installation* of MSS requires a writable system temp directory, and if one is not available, the installer may fail to run.

The MSS product is delivered as a single zip file that includes all installers for all platforms. The MSS zip file contains install4j installers for Windows, Linux, and UNIX.

- [Setting a TEMP directory for install4j](#)
- [When installing both MSS and Host Access for the Cloud \(HACloud\)](#)
- [Troubleshooting: Setting an alternate temp directory](#)

16.5.1 Setting a TEMP directory for install4j

The installer (Windows or Linux/UNIX) requires a writable temp folder. If the default temp directory is not suitable, the installer can be run with an alternate temp directory.

 **Note**

The installer must be run with administrative permissions.

- **Windows**

If the default temp directory is not writable, set the environment variables TMP or TEMP to an alternate location temporarily while running the installer.

Restore the variables when the installation is complete.

- **Linux/UNIX**

The environment variable INSTALL4J_TEMP determines the base directory that the MSS installer uses for self-extraction. As the installer extracts files and launches Java to perform other tasks, the Java temp location (/tmp) is used.

To run the Linux installers with an alternate temp directory:

- Define the variable INSTALL4J_TEMP, specifying the value as the desired temp location.
- Create the temp directory specified for the installer. The installer requires a directory that already exists.
- Add the command line switch `-J-Djava.io.tmpdir={tmpdir}` when launching the installer. For example:

```
abcd@linux:~$ INSTALL4J_TEMP=/home/abcd/i4jtemp
abcd@linux:~$ export INSTALL4J_TEMP
abcd@linux:~$ sudo ./mss-12.8.0.12345-linuxx64.sh -J-Djava.io.tmpdir=/home/abcd/i4jtemp
```

16.5.2 When installing both MSS and Host Access for the Cloud

If you use HACloud, note the installation requirements, based on your environment.

For a chained installation of MSS and HACloud

- **On Windows.** If you temporarily set the TMP or TEMP environment variables as described above (Setting a TEMP directory for install4j), a chained installation of HACloud and MSS needs no other adjustments.

- **On Linux/UNIX.** You cannot run a chained installation.

Run the `INSTALL4J_TEMP` var set and the `-J-Djava.io.tmpdir` switch separately, each with administrative permissions.

If you plan to install MSS and HACloud separately, install MSS first.

16.5.3 Troubleshooting: Setting an alternate temp directory

MSS uses an internal temp directory that should be suitable in all cases. However, if necessary, this directory location can be changed by editing the `container.conf` file and the `Cassandra jvm.options` file.

Changing the internal temp location

1. Open `<installation folder>/mss/server/conf/container.conf` in a text editor.
2. Edit the `wrapper.java.additional` property to specify the new location. If the path contains spaces:
 - **On Windows**, enclose it in quotes.
 - **On Linux/UNIX**, use the appropriate syntax. For example, `wrapper.java.additional.9=-Djava.io.tmpdir=../tmp`
3. If needed, you can set an additional property to delete the temp directory when the server shuts down.
4. Edit the `Cassandra jvm.options` file, and modify the two properties that control the location of temp files: `-Djava.io.tmpdir` and `-Djna.tmpdir`.
5. Restart the server

16.6 Run services as a dedicated user

From a security perspective, it is advantageous to run services as a dedicated user with a minimal set of privileges.

You must first install the product, and then adjust the MSS service as described below.

Note

You must repeat these steps after any product upgrades.

16.6.1 To run the Micro Focus MSS Server service as a dedicated user on Windows:

1. Create a standard user.
2. **Stop the Micro Focus MSS Server service.**
3. Open the **Properties** of the Micro Focus MSS Server service.
4. Go to the **Log On** tab.
5. Select **This account**.
6. Enter the username and password of the user who is going to run the service.
7. Give the user **full control** to the following directories:
 - `<install_dir>\server\conf`
 - `<install_dir>\server\etc`
 - `<install_dir>\server\logs`
 - `<install_dir>\server\tmp`
 - `<install_dir>\server\microservices\auth-service`
 - `<install_dir>\server\microservices\cassandra`
 - `<install_dir>\server\web\work`
 - `<install_dir>\server\webapps\mss\ex\modules`
 - `<install_dir>\server\webapps\mss\WEB-INF\lib\modules`
 - MSSData directory (for example, `C:\ProgramData\Micro Focus\MSS\MSSData`)
 - `<mssdata_dir>\db`
 - `<mssdata_dir>\deploy`

8. Change ownership and give full control to the user for following files:

- <mssdata_dir>\keychain.bcfks
- <mssdata_dir>\keychain.bcfks.bak
- <mssdata_dir>\keychain.pwd
- <mssdata_dir>\AccessDS.xml
- <mssdata_dir>\PropertyDS.xml
- <mssdata_dir>\SessionDS.xml
- <mssdata_dir>\idm\IDManager.config

9. Start the Micro Focus MSS Server service.

To give full control of a file or folder:

1. Right click on the file or folder.
2. Select **Properties**.
3. Go to the **Security** tab.
4. Click **Edit**.
5. Click **Add**.
6. Enter the user name and click **OK**.
7. Check **Full control** under the Allow column and click **Apply**.

To change ownership of a file or folder:

1. Right-click the file or folder.
2. Select **Properties**.
3. Go to the **Security** tab.
4. Click **Advanced**.
5. Click **Change** beside the current Owner.
6. Enter the new owner name and click **OK**.
7. Click **Apply**.

16.6.2 To run the Micro Focus MSS Server service as a dedicated user on UNIX / Linux:

Follow the steps above but adjust them accordingly for your environment and distribution.

17. Legal Notice

© Copyright 2022 Micro Focus or one of its affiliates

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contains Confidential Information. Except as specifically indicated otherwise, a valid license is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/legal>.