Host Access Management and Security Server

Installation Guide

12.5

Legal Notice

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/about/legal/.

The only warranties for this product and any associated updates or services are those that may be described in express warranty statements accompanying the product or in an applicable license agreement you have entered into. Nothing in this document should be construed as creating any warranty for a product, updates, or services. The information contained in this document is subject to change without notice and is provided “AS IS” without any express or implied warranties or conditions. Micro Focus shall not be liable for any technical or other errors or omissions in this document. Please see the product’s applicable end user license agreement for details regarding the license terms and conditions, warranties, and limitations of liability.

Any links to third-party websites take you outside Micro Focus websites, and Micro Focus has no control over and is not responsible for information on third party sites.

Contents

Host Access Management and Security Server Installation Guide 7

1 Introduction 9

How Management and Security Server works . . . 9
What Management and Security Server installs . . . 10
Installed and Enabled Components . . . 10
Add-On Products . . . 10
Overview of Components and Add-On Products . . . 11
Administrative Server . . . 11
Metering Server . . . 12
Configuration Utilities . . . 12
Security Proxy Add-On . . . 12
Terminal ID Manager Add-On . . . 12
Automated Sign-On for Mainframe Add-On . . . 13
Micro Focus Advanced Authentication Add-On . . . 13

2 Preparing to Install 15

Prerequisite Actions . . . 15
Shut down any currently running components. . . . 15
Obtain the required user privileges. . . . 15
Obtain the required account permissions. . . . 15
On Linux, verify fonts are installed. . . . 16
System Requirements . . . 16
Administrative Server Requirements . . . 16
Browser Requirements . . . 16
Metering Server Requirements . . . 17
Requirements for Add-On Products . . . 17

3 Automated Installation 19

About Automated Installation . . . 19
Automated Installation Procedure . . . 19
Step 1: Run the automated installer. . . . 19
Step 2: Enter configuration information. . . . 21
Step 3: Start services . . . 22
Installation Variations . . . 22
Installing on UNIX with no JRE . . . 23
Servlet Runner Launcher JVM Options . . . 23
Servlet runner other than Apache Tomcat . . . 23
Integrating SiteMinder with MSS . . . 23
Using the automated installer in console mode . . . 25
Unattended installation . . . 25
Manual installation . . . 26

4 Manual Installation 27

About Manual Installation . . . 27
Manual Installation Procedure . . . 27
Step 1: Extract the manual installation .zip file. . . . 27

Step 2: Run a configuration utility. 28
Step 3: Start the server components.. 29
Manual Installation Variations 30
Installing on UNIX with no JRE 30
Servlet Runner Launcher JVM Options 30

5 Starting the Administrative Console 31

Log in to the Administrative Console. 31
Using **Administrative Server (HTML login)**. 31
Using Administrative Server login 32
Configure the Administrative Server 32
Initial Settings. 33
Next Steps 33

6 Setting Up Metering 35

How Metering Works. 35
Overview of Metering Setup 35
Metering: Prerequisites and System Requirements 36
Configuring the Metering Server. 36

7 Installing Add-On Products 37

Installing Activation Files. 37
Use the automated installer to install activation files 37
Use the Administrative Console to install activation files 38

8 Setting Up the Security Proxy 39

Overview of Security Proxy Server 39
Security Proxy: Prerequisites and System Requirements. 41
Performance and Scaling Requirements 41
Speed of Processors 42
Number of Processors (or Cores) 42
System RAM 42
Java Heap Size 42
Java Runtime Environment (JRE) 43
Number of Available Ports and Descriptors 43
Number of Concurrent Connections. 44
Operating System 44
Server Dedication. 44
Key Lengths and Cipher Suites 44
Install the Security Proxy Server. 44
Run the automated installer 45
Install the activation file, and activate the Security Proxy 46
Manually install the Security Proxy 46
Configuring the Security Proxy Server 47

9 Setting Up Terminal ID Manager 49

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

10 Setting Up Automated Sign-On for Mainframe 53

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

11 Setting Up Micro Focus Advanced Authentication Add-On 55

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

12 After you install 57

Issue: Applications hang on UNIX or Linux 57
The Problem. 57
The Fix: `/dev/urandom`. 57
Alternative Solutions 57
Resources. 58

13 Upgrading to Version 12.5 59

Download Product Files 59
Upgrading the Security Proxy Server 60
Match the version. 60
Synchronize an upgraded Security Proxy 60
Upgrading Replicated Servers 62
Upgrading Add-On Products. 62
Using the Automated Installer. 62
Upgrading a Manual Installation 63
Step 1. Extract the manual installation.zip file. 63
Step 2. Install the new product version into a different folder. 63
Step 3. Run the Configuration Upgrade Utility 63
Step 4. Install and start services 64
If you are upgrading Reflection for the Web 65
Directory Names and Installation Paths 65
If you use LDAP with TLS (LDAPS) 65

14 Uninstalling 67

Removing Components 67

15 Appendices 69

Appendix A. Configuration Utilities 69
Initial Configuration Utility. 69
Configuration Upgrade Utility 70
HTTPS Certificate Utility 70
IIS Integration Utility (on Windows) 71
Appendix B. Specifying a non-default location for MSSData 72

Host Access Management and Security Server Installation Guide

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

At a Glance:

About Management and Security Server 12.5
About Automated Installation
About Add-On Products
If you are evaluating...

About Management and Security Server 12.5

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

See the **Release Notes** for a list of new features, resolved issues, and known issues in this release.

About Automated Installation

When possible, we recommend using the automated installer to install Management and Security Server and your entitled Add-On products. Check the Installation Variations if your system requirements differ from an automated installation.

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

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

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

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

About Add-On Products

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

Add-on products include:

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

If you are evaluating...

If you are running an evaluation copy, the product will be fully functional for 120 days. During that time you can install, configure, and test Host Access Management and Security Server.

Please contact Micro Focus or your authorized reseller to obtain the full-use version of the software.

1 Introduction

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

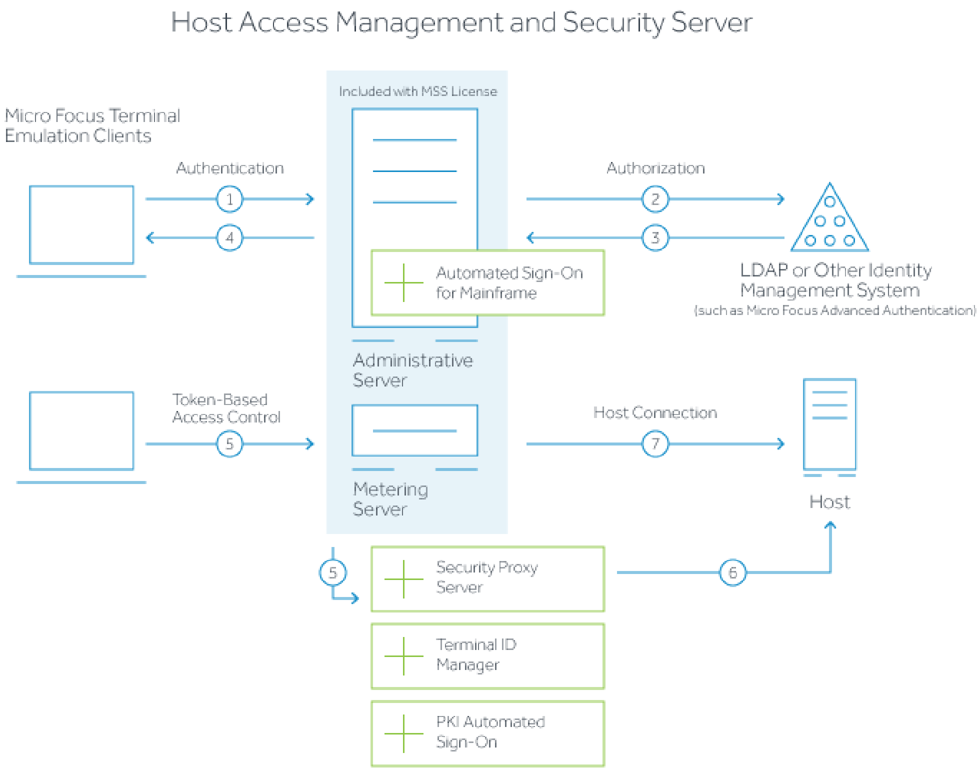
Secure access is delivered to applications on IBM, HP, Linux, UNIX, Unisys, and OpenVMS hosts.

In this section:

- How Management and Security Server works
- What Management and Security Server installs
- Overview of Components and Add-On Products

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.


Host Access Management and Security Server
Included with MSS License
Micro Focus Terminal Emulation Clients
Authentication
1
4
Authorization
2
3
Automated Sign-On for Mainframe
LDAP or Other Identity Management System
(such as Micro Focus Advanced Authentication)
Administrative Server
Token-Based Access Control
5
Host Connection
7
Metering Server
Host
5
Security Proxy Server
6
Terminal ID Manager
PKI Automated Sign-On

1. User connects to the Administrative Server.

2. User authenticates to a directory server (LDAP/Active Directory) or other identity management system (optional).
3. The directory server provides user and group identity (optional).
4. The Administrative Server sends an emulation session to the 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.

Related Topics

- What Management and Security Server installs
- Add-On Products

What Management and Security Server installs

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

Installed and Enabled Components

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

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

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

Add-On Products

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

Add-On Products include

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

Related Topics

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

Overview of Components and Add-On Products

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

- Administrative Server
- Metering Server
- Configuration Utilities
- Security Proxy Add-On
- Terminal ID Manager Add-On
- Automated Sign-On for Mainframe Add-On
- Micro Focus Advanced Authentication Add-On

Administrative Server

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

The user interface for the Administrative Server is the **Administrative Console**, where an administrator can configure and save settings.

Administrative Console

The Administrative Console user interface was introduced in Management and Security Server 12.4 SP1. Use the Administrative Console to:

- Manage Sessions
- Manage Packages
- Assign Access
- Configure Settings

  - General Settings
  - General Security
  - Secure Shell
  - Certificates
  - Trusted Certificates
  - Credential Store
  - Security Proxy
  - Authentication & Authorization
  - Product Activation
  - Automated Sign-on for Mainframe
  - Metering
  - Terminal ID Manager

  - Replication
  - Logging
- Run Reports

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 can be installed either on the same server as the Management and Security Server or on another system.

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.

Configuration Utilities

While the automated installer handles most of the configuration, one or more utilities may be required after you complete the installation and configuration steps.

See Appendix A: Configuration Utilities for more information.

Security Proxy Add-On

The Security Proxy 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), which can be installed by an automated installer.

NOTE: The Security Proxy must be the same `<major>.<minor>.<update>` version as Management and Security Server.

For example, when you upgrade Management and Security Server to version 12.5, be sure to upgrade the Security Proxy to version 12.5.

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

Terminal ID Manager Add-On

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

See Setting Up Terminal ID Manager.

Automated Sign-On for Mainframe Add-On

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

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

See Setting Up Automated Sign-On for Mainframe.

Micro Focus Advanced Authentication Add-On

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

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

See Setting Up Micro Focus Advanced Authentication Add-On.

Related Topics

- How Management and Security Server works
- Preparing to Install

2 Preparing to Install

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

- Prerequisite Actions
- System Requirements

Prerequisite Actions

Before you run the automated installer, be sure to:

- Shut down any currently running components.
- Obtain the required user privileges.
- Obtain the required account permissions.
- On Linux, verify fonts are installed.

Shut down any currently running components.

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

Obtain the required user privileges.

- **On Windows.** If you install servers on a Windows workstation, the installer must be launched by a user who is an Administrator with administrative privileges. Note that applications run by administrators are run with standard user permissions unless the user specifically authorizes the application to use more elevated privileges.
- **On Linux or UNIX.** If you are installing on a Linux or UNIX platform, the installer must be launched by a user with root privileges. If you cannot obtain elevated privileges, you may need to use a manual installation process.
- If the MSSData directory (which stores site-specific content) must be installed to a non-default location, see Appendix B: Specifying a non-default location for MSSData.

Obtain the required account permissions.

Make sure that you have the necessary account permissions to install components on the target server.

If you plan to use X.509 client certificates or secure LDAP access control, the account used to run the Administrative Server must have permission to write to the Java certificate authority certificates file (cacerts).

The default Windows location is

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

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.

Related topics

- System Requirements

System Requirements

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

- Administrative Server Requirements
- Browser Requirements
- Metering Server Requirements
- Requirements for Add-On Products

Administrative Server Requirements

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

- **Enterprise Class Server operating system**, with:

  – 3.40 GHz (4 cores) and 8GB of RAM
  – Sufficient drive space, typically 250GB when used on a drive with fast read/write capabilities. Space requirements vary depending on how Management and Security Server is used.
  – a 64-bit server-class system for production. For initial testing or evaluation, a workstation could be used.

- **Server running JRE 8**, with JCE Unlimited Strength Policy Files applied

  An Open JDK (Azul Zulu) is installed by the automated installer (or multi-component manual installation).

Browser Requirements

The browser requirements vary according to the users' workflow.

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

- support JavaScript and cookies

When using the **Administrative Server** (Java-based) login, the browser must:

- use JRE 8
- run trusted applets
- support JavaScript and cookies

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

Metering Server Requirements

The Metering Server requires a server running JRE 8.

Requirements for Add-On Products

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

Security Proxy Add-On

Terminal ID Manager Add-On

Automated Sign-On for Mainframe Add-On

Micro Focus Advanced Authentication Add-On

Related Topics

- Prerequisite Actions

3 Automated Installation

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

In this section:

- About Automated Installation
- Automated Installation Procedure
- Installation Variations

About Automated Installation

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

The automated installer for 64-bit systems:

- can be run on Linux 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 for initial testing.

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

Related Topics

- Automated Installation Procedure
- Installation Variations

Automated Installation Procedure

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

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

Step 1: Run the automated installer.

To run the automated installer.

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

   Note: Version 12.5 is denoted as version `12.5.0.<nnn>`.

Operating System	Automated Installer
Linux 64-bit	mss-12.5.<nnn>-prod-linuxx64.sh
z Linux	mss-12.5.<nnn>-prod-unix-nojre.sh
Windows 64-bit	mss-12.5.<nnn>-prod-wx64.exe

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

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

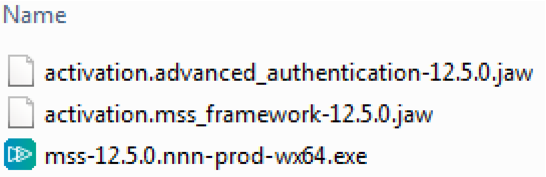
To install the activation files now:

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

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

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

On Windows, for example: to install the Advanced Authentication Add-On, place the activation file in the same folder as the installer, `mss-12.5.0.<nnn>-prod-wx64.exe`.



Name

activation.advanced_authentication-12.5.0.jaw

activation.mss_framework-12.5.0.jaw

mss-12.5.0.nnn-prod-wx64.exe

3 Run the MSS installer.

4 Select a **language** to use during installation.

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

6 Read and accept the license agreement.

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

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

Host Access Management and Security Server. Select this check box to install the Administrative Server, which includes the Administrative 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.

9 **Start Menu** directory: On Windows, select the directory where you want to create the program shortcuts. You also have the option to create shortcuts for all users, or to suppress the creation of a Start Menu directory. Click **Next**.

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

Continue with Step 2: Enter configuration information.

(During an **upgrade**, the installer retains your settings, and you will not be prompted to run a configuration utility. For more information, see Upgrading to Version 12.5.)

Step 2: Enter configuration information.

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

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

Enter or verify your configuration information.

1. **Installation Directory:** Confirm or browse to the location where the Administrative Server was installed.
2. **MSS Server Services:** Select the services you want to enable. You must have an MSS Server service running on one machine at your site. If entitled, you can optionally choose to install the Security Proxy server.
3. **Volume Purchase Agreement number:** Optional. Enter the Volume Purchase Agreement (VPA) number. You can modify the VPA number later in the Administrative Console.
4. **Servlet runner ports:** Accept the default entries or enter the port numbers that the servlet runner will use for HTTP and HTTPS connections. The default port number for HTTP is 80, and the default for HTTPS is 443.
5. **Security Proxy server ports:** If you are installing the Security Proxy, specify the port numbers for the Security Proxy. The default listening port is 3000. The default monitor port is 8080. You can change Security Proxy settings after installation using the Security Proxy Wizard.
6. **Administration password:** Enter a password. Use this password to open the Administrative Console and to administer Metering and Terminal ID management (if installed). You can create different passwords for each server later.
7. **Server Names for URLs and Certificates:** The information that you enter on this and the following panel enable you to create self-signed certificates that will be used to make secure TLS connections to the Administrative Server and Security Proxy after installation. Enter a DNS name or IP address. The current DNS name is provided if available. If you want to change the servlet runner certificate later, use the HTTPS Certificate Utility.
8. **Server certificates: organization and locality** (optional)

   This panel includes additional information for creating certificates.

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

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

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

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

   Country: Provide a two-letter ISO country code, such as `US`.
9. **Confirm Configuration:** Click **Next** to apply the specified configuration changes.
10. **Configuration summary:** A summary of the configuration changes is created in `InitalConfigurationUtility.log` in the `<installation>\utilities\logs` directory.

    Click **Done** to continue with Step 3: Start Services.

Step 3: Start services

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

The MSS Server must be started before you can run the Administrative 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 To start the service after an automated installation.
2. **Installation Complete.** The components are installed and the services are started.
3. Continue with Starting the Administrative Server.

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

To start the service after an automated installation

On Windows:

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

On Linux or UNIX:

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

Related Topics

- Installation Variations

Installation Variations

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

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

Installing on UNIX with no JRE

Use this option if your UNIX platform (such as z/OS, 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-12.5.<nnn>-prod-unix-nojre.sh`, where <nnn> is the build number.
2. Proceed with the installation, using your existing JRE.

   Note: Your JRE must be Java version 8.
3. Be sure that the JCE Unlimited Strength Jurisdiction Policy Files are applied, and apply them each time you upgrade your JRE.

NOTE: If you plan to use **Replication**, be sure to see the **Caution** in the Master Server Role help. You may need to edit a file.

Servlet Runner Launcher JVM Options

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

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

Servlet runner other than Apache Tomcat

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

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

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.

If you used a manual installation, run the **IIS integration utility** (in `\MSS\utilities\bin`) before configuring access control for SiteMinder.

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:

     Copy these files:

     `<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\bin`.

   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, “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. Add the SiteMinder libraries to MSS.

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:

1. Locate the file, `smjavaagentapi.jar`, in your SiteMinder Web Agent installation.
2. 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`.
3. Restart the MSS server.

Note: 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 memeory, which authenticates them only for that browser session.

Using the automated installer in console mode

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

All screens present their information on the console and allow you to enter the same information as in the automated installer. This option is useful if you want to run the automated installer on a headless or remote server.

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

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

Unattended installation

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

NOTE: The Configuration Utilities do not support an unattended mode. These utilities run with a graphical user interface (or in an attended console mode). For more information, see Appendix A. Configuration Utilities, which are optional for many upgrade scenarios.

To use unattended installation:

1. Install Management and Security Server on a machine using the automated installer. You can use the graphical interface or console mode (`-c`) to install the product.

   The installation process creates a text file, `response.varfile`, that contains the selected installation options. The file is located in `[MssServerInstall]\.install4j\response.varfile`

2. Copy `response.varfile` to another machine where you would like to install Management and Security Server.
3. Locate the appropriate executable (listed in Step 1: Run the automated installer) to install the product. Launch the installation program using the `-q` argument and a `-varfile` argument that specifies the location of `response.varfile`.

For example, to install Management and Security Server on a 64-bit Linux platform with a `response.varfile` located in the same directory, use this command, where <`12.5.0.nnn`> is the product version and build number:

```
mss-<12.5.0.nnn>-prod-linuxx64.sh  –q –varfile response.varfile
```

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

Manual installation

If you are unable to use an automated installer, see the Manual Installation section.

Related Topics

- Automated Installation Procedure

4 Manual Installation

If you cannot run the automated installer -- or if `root` privileges are not available -- use this manual installation process.

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

About Manual Installation

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

The manual installation:

- can be run on numerous platforms, including Linux, UNIX (all flavors), and Windows.
- installs a default servlet runner.
- installs an Open JDK (unless you run the no-jre installer).
- installs the Administrative Server, the Metering Server, the Security Proxy*, and the Terminal ID Manager*.

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

Related Topics

- Manual Installation Procedure
- Manual Installation Variations

Manual Installation Procedure

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

Note: `root` privileges are *not* required.

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

Step 1: Extract the manual installation .zip file.

To install the components:

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

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

```
jar xvf mss-12.5.0.<nnn>-prod-linuxx64.zip
```

2 Change to the `install_manual` directory.

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

An `mss` directory is created. For example:

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

Step 2: Run a configuration utility.

For a new installation, use the **Initial Configuration Utility** to configure the Administrative Server. The Initial Configuration Utility:

- enables the services you select for the Administrative Server.
- creates an `MSSData` directory under which site-specific content is stored.
- generates cryptographic keys and self-signed certificates for the servlet runner and Administrative Server.
- sets the administrative password.
- sets a port value for the Administrative Server in configuration files.

Run the Initial Configuration Utility

1 Before you run the **Initial Configuration Utility**, these conditions must be in place:

1a Make sure the earlier version of the software is not running.

Doing so will avoid potential port conflicts and allow you to accept default port assignments.

1b If you are upgrading a Linux or UNIX system, make sure that no startup scripts are running.

1c Verify that you have administrator privileges. If not, you will be prompted for credentials.

1d Uninstall the services, such as the MSS Server and MSS SecurityProxy.

1e Be sure the scripts are executable by running this command:

```
chmod +x  InitialConfigurationUtility
```

2 In the `mss/server/conf/container.properties` file, change the `dataFolder` property to a folder where the current user has `write` access.

3 Go to the `mss/utilities/bin` directory, and run the **Initial Configuration Utility** in console mode with the `–c` parameter.

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

Enter or verify your configuration information.

Proceed through the prompts, noting the following:

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

2 **MSS Server Services:** Select the services you want to enable. You must have an MSS Server service running on one machine at your site. If entitled, you can optionally choose to install the Security Proxy server.

3. **Volume Purchase Agreement number:** Optional. Enter the Volume Purchase Agreement (VPA) number. You can modify the VPA number later in the Administrative Console.
4. **Servlet runner ports:** Accept the default entries or enter the port numbers that the servlet runner will use for HTTP and HTTPS connections. The default port number for HTTP is 80, and the default for HTTPS is 443.
5. **Security Proxy server ports:** If you are entitled and installing the Security Proxy, specify the port numbers for the Security Proxy. The default listening port is 3000. The default monitor port is 8080. You can change Security Proxy settings after installation using the Security Proxy Wizard.
6. **Administration password:** Enter a password. Use this password to open the Administrative Console and to administer Metering and Terminal ID management (if installed). You can create different passwords for each server later.
7. **Server Names for URLs and Certificates:** The information that you enter on this and the following panel enables you to create self-signed certificates that will be used to make secure TLS connections to the Administrative Server and Security Proxy after installation. Enter a DNS name or IP address. The current DNS name is provided, if available. If you want to change the servlet runner certificate later, use the HTTPS Certificate Utility.
8. **Server certificates: organization and locality** (optional)

   This panel includes additional information for creating certificates.

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

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

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

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

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

Step 3: Start the server components.

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

To start the servlet runner after a manual installation

On Windows:

Either

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

   -- or --

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

   (To uninstall the Windows service: `uninstall-server-service.bat`)
2. Open **Windows Services**.

3. Right-click **Micro Focus MSS Server**.
4. Click **Start**.

On Linux or UNIX:

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

Next step

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

Continue with Starting the Administrative Console.

Related Topics

- Manual Installation Variations

Manual Installation Variations

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

Installing on UNIX with no JRE

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

No JRE is installed with this installer.

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

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

   Note: Your JRE must be Java version 8, and have the JCE Unlimited Strength Policy Files applied.

Servlet Runner Launcher JVM Options

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

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

Related Topics

- Manual Installation Procedure

5 Starting the Administrative Console

The Administrative Console is the user interface for the Administrative Server -- the central component of Management and Security Server. Use the 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 Console
- Configure the Administrative Server

Log in to the Administrative Console

You can open the 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. If you ran the automated installer, the servlet runner is automatically started.

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

To start the service after an automated installation

To start the servlet runner after a manual installation

2 Choose a login option:

- **Administrative Server (HTML login)**

  This non-Java login directly opens the Administrative Console (in English).

  See Using Administrative Server (HTML login).

- **Administrative Server**

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

  See Using Administrative Server login.

Using Administrative Server (HTML login)

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

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

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

2 In the **User** field, enter either `admin` (the default) or your site-specific user name.

3 Enter the administrator password specified during installation and configuration.

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

4 Click **Login**. The Administrative Console opens to the **Manage Sessions** panel.

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

5 To see the list of sessions, open **Manage Sessions**.

6 Continue with Configuring the Administrative Server.

Using Administrative Server login

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

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

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

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

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

4 Enter the administrator password specified during installation.

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

5 Click **Submit**.

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

6 Click the **Administrative Console** button.

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

7 Continue with Configuring the Administrative Server.

Configure the Administrative Server

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

Initial Settings

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

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**.

Next Steps

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

As a next step, you might:

Set up Metering
Set up Security Proxy Add-On
Set up Terminal ID Manager Add-On
Set up Automated Sign-On for Mainframe Add-On

Set up Micro Focus Advanced Authentication Add-On

6 Setting Up Metering

Use the Metering Server to audit session activity and to control concurrent access to specific hosts. The Metering Server is included with Management and Security Server and is installed using the automated installer on the same machine as the Management and Security Server.

Once installed, the Metering Server requires some additional setup before you can deploy metered terminal sessions. Refer to these topics:

- How Metering Works
- Overview of Metering Setup
- Metering: Prerequisites and System Requirements
- Configuring the Metering Server

How Metering Works

At a glance, 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 log 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

Related Topics

- Overview of Metering Setup
- Metering: Prerequisites and System Requirements
- Configuring the Metering Server

Overview of Metering Setup

To set up metering, you must configure the Metering Server in the Administrative Console and then enable client to be metered.

1. In the Administrative Console, use **Manage Sessions** to create session that you want to meter.
2. Open **Configure Settings - Metering** to configure the server.

   Follow the prompts and click **Help** for more information.

3. Enable each client to be metered. Refer to the product documentation for details.
   - For **Reflection ZFE**, see How to Set Up Metering.
   - For **Reflection Desktop**, see Enable Usage Metering.
4. After the clients begin to meter, you can view Metering Reports.

   In the Administrative Console, click **Run Reports - Usage Metering**.

Related Topics

- Metering: Prerequisites and System Requirements
- Configuring the Metering Server
- How Metering Works

Metering: Prerequisites and System Requirements

Before you can create metered sessions, verify that:

- Metering Server is installed and added to the Administrative Console. (To see the list of current metering servers, go to **Configure Settings - Metering**.)
- Server running JRE 8 (An Open JDK is installed by the automated installer.)

NOTE:

- In most deployments, only one metering server is needed to support all clients. If more than one metering server is run, the metering report numbers must be manually combined.
- The metering service does not support load balancing. Each emulation client must report directly to a single metering server.

Related Topics

- Overview of Metering Setup
- Configuring the Metering Server
- How Metering Works

Configuring the Metering Server

In the Administrative Console, use **Configure Setting - Metering** to configure the Metering Server and restrict concurrent sessions.

See the Metering Help for details.

Related Topics

- How Metering Works
- Overview of Metering Setup
- Metering: Prerequisites and System Requirements

7 Installing Add-On Products

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

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

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

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

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

Related Topics

- Installing Activation Files

Installing Activation Files

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

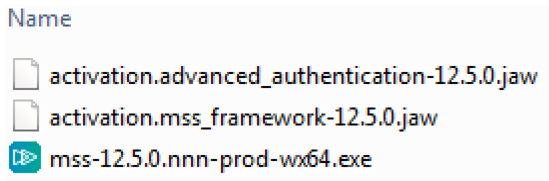
- Use the automated installer to install activation files
- Use the Administrative Console to install activation files

Use the automated installer to install activation files

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

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

   On Windows, for example: to install the Advanced Authentication Add-On, place the activation file in the same folder as the installer, `mss-12.5.0.<build>-prod-wx64.exe`.

   Name

   activation.advanced_authentication-12.5.0.jaw
   activation.mss_framework-12.5.0.jaw
   mss-12.5.0.nnn-prod-wx64.exe

   NOTE: The `activation.mss_framework-12.5.0.jaw` activation file is automatically installed to enable the Host Access Management and Security Server framework.

3. Run the MSS installer.

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

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

Use the 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 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 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 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
   - Micro Focus Advanced Authentication

8 Setting Up the Security Proxy

The Security Proxy Add-On requires a separate license. This Installation Guide provides the steps to install and activate the Security Proxy.

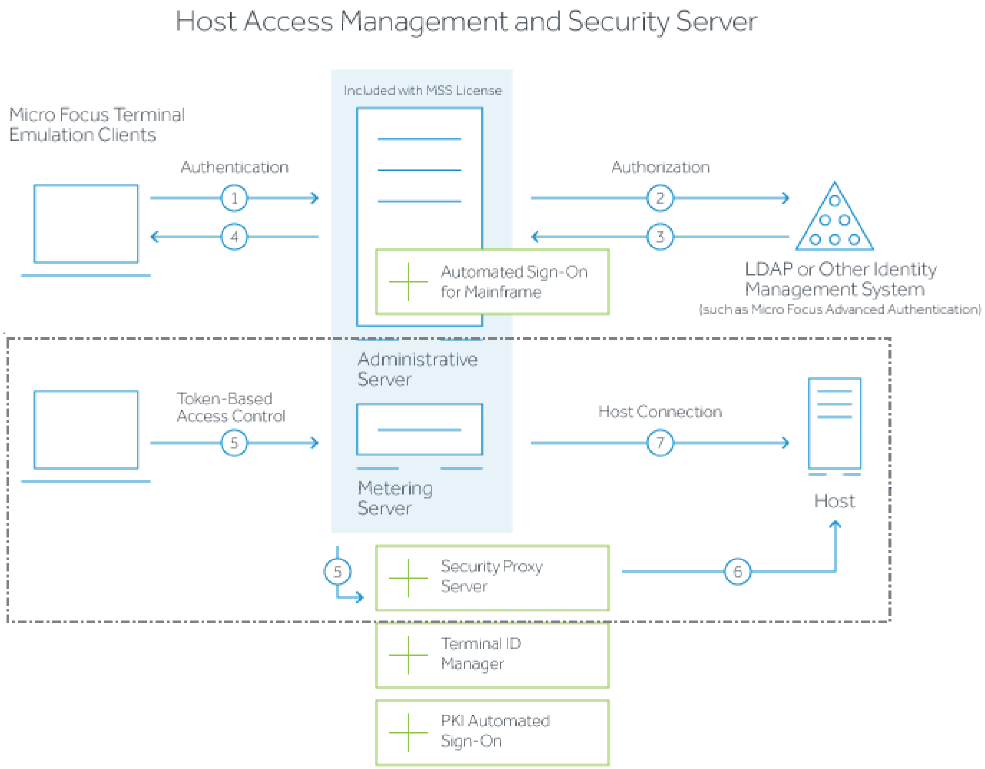
For the configuration steps, see Using the Security Proxy Server in the Management and Security Server Administrator Guide for the next steps.

- Overview of Security Proxy Server
- Security Proxy: Prerequisites and System Requirements
- Performance and Scaling Requirements
- Install the Security Proxy Server
- Configuring the Security Proxy Server

Overview of Security Proxy Server

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

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


Host Access Management and Security Server
Included with MSS License
Micro Focus Terminal Emulation Clients
Authentication
1
4
Authorization
2
3
Automated Sign-On for Mainframe
LDAP or Other Identity Management System
(such as Micro Focus Advanced Authentication)
Administrative Server
Token-Based Access Control
5
Host Connection
7
Metering Server
Host
5
Security Proxy Server
6
Terminal ID Manager
PKI Automated Sign-On

1 User connects to the Administrative Server.

2 User authenticates to a directory server (LDAP/Active Directory) or other identity management system (optional).

3 The directory server provides user and group identity (optional).

4 The Administrative Server sends an emulation session to the authorized client.

5 When the **Security Proxy Server** is configured for use by a session, the emulation client makes a TLS connection to Security Proxy and sends it a signed session token.

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

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

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

Related Topics

- Security Proxy: Prerequisites and System Requirements
- Performance and Scaling Requirements

Security Proxy: Prerequisites and System Requirements

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

- Management and Security Server (the Administrative Server) is installed.
- The Security Proxy activation file is available.

NOTE: The Security Proxy must be the same `<major>.<minor>.<update>` version as Management and Security Server. For example, when you upgrade Management and Security Server to version 12.5 be sure to upgrade the Security Proxy to version 12.5.

- The server is running JRE 8 (An Open JDK is installed by the automated installer.)
- The Performance and Scaling Requirements are addressed.

Related Topics

- Performance and Scaling Requirements
- Install the Security Proxy Server

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.

***Table 8-1** Recommended Specifications for Security Proxy servers*

System Specification	up to 6000 connections (concurrent and active)	up to 2000 connections (concurrent and active)
Speed of processors	2.7 GHz or faster	2.33 GHz or faster
Number of processors (or cores)	4 or more	2 or more
System RAM	4 GB or more	3 GB
Java Virtual Machine (JVM) heap size	3072 MB	2048 MB
Java Runtime Environment (JRE)	Use a current 64-bit JRE	Use a current 64-bit JRE
File descriptors (Linux/UNIX)	21,000	7,000

Additional specifications:

- Number of Available Ports and Descriptors
- Number of Concurrent Connections
- Operating System
- Server Dedication
- Key Lengths and Cipher Suites

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 3072 MB 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:

```
-Xms3072m

-Xmx3072m
```

Java Runtime Environment (JRE)

Use a current JRE. In general, performance is better with newer JREs -- better memory handling, HotSpot technology, improved speed, and the ability to support an increased number of sessions. Several companies provide JREs, and performance varies from one product to another.

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 an SSL/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.

Install the Security Proxy Server

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

If you cannot use the automated installer, other installation options are available that require additional configuration.

NOTE: About secure connections

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

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

With any installation method, you can increase the security of terminal session connections by ensuring that there is only one known, secure link between the Security Proxy server and the host computer. If you select End to end encryption when configuring a session, the connection between the Security Proxy and the host will use TLS.

Installation Methods

- Run the automated installer
- Install the activation file, and activate the Security Proxy
- Manually install the Security Proxy

Run the automated installer

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

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

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

   After the automated installer runs, the **Initial Configuration Utility** generates cryptographic keys and self-signed certificates, automates configuration, and sets a port value for the Security Proxy.
4. Start the Security Proxy server -- done by the automated installer.

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

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

   -- or --

   Use the steps below to Install the activation file, and activate the Security Proxy.
2. Activate the Security Proxy Server:

   Copy the security proxy activation file into the `/securityproxy/lib/modules` directory on the machine where Security Proxy Server is installed.
3. Start the Security Proxy server -- done by the automated installer.

Install the activation file, and activate the Security Proxy

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

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

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

   ```
   activation.security_proxy-12.5.0.jaw
   ```

   Note the download location.
2. In the Administrative Console, click **Configure Settings - Product Activation**.
3. Click **Activate New** and browse to `activation.security_proxy-12.5.0.jaw`
4. Click the file. The **Security Proxy Add-On** is installed and added to the **Product** list.
5. Restart your browser to ensure that the Administrative Console is fully updated with the new set of activation files. You do not need to restart the administrative server (MSS Server) service.
6. Activate Security Proxy Server:

   Copy the security proxy activation file, into the `/securityproxy/lib/modules` directory on the machine where Security Proxy Server is installed.
7. Continue with the steps to Configure and Start the Security Proxy Server (in the Management and Security Server Administrator Guide).

Manually install the Security Proxy

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

To manually install and configure the Security Proxy:

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

Operating System	Manual Installation File
Linux 64-bit	securityproxy-prod-linuxx64-manual.tar.gz
UNIX	securityproxy-prod-unix-nojre-manual.tar.gz
Windows 64-bit	securityproxy-prod-wx64-manual.zip

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

   ```
   [MssServerInstall]\securityproxy
   ```

   NOTE: The `<nojre>` option requires an existing JRE, version 8.
3. After the Security Proxy Add-On is installed, some setup is required before you can deploy encrypted sessions.
4. Continue with the steps to Configure and Start the Security Proxy Server in the Management and Security Server Administrator Guide.

Configuring the Security Proxy Server

Refer to Using the Security Proxy Server in the Management and Security Server Administrator Guide for the steps to configure secure sessions using the Security Proxy.

Steps include:

- 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

The Terminal ID Manager lets you centrally manage and assign terminal and device IDs to emulator sessions. You can pool terminal IDs, track ID usage, and manage inactivity timeout values for specific users, thus conserving terminal ID resources and significantly reducing operating expenses.

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

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

Terminal ID Manager: Prerequisites and System Requirements

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

- Management and Security Server is installed.
- Terminal ID Manager Add-On activation file is available.
- Server running JRE 8 (An Open JDK is installed by the automated installer.)

Related topic

- Step 1: Install Terminal ID Manager.

Step 1: Install Terminal ID Manager.

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

Install the Terminal ID Manager activation file.

You can install Terminal ID Manager either by running the automated installer or by using the Administrative Console (**Configure Settings - Product Activation**).

Using the automated installer

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

1. Copy the activation file into the same directory as the automated installer (that was used to install Management and Security Server).
2. Run the automated installer on that same machine to install only Terminal ID Manager.

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

3 Continue with Step 2: Activate the server.

Using the Administrative Console

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

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

```
activation.terminal_id_manager-12.5.0.jaw
```

2 Download the file and note the location.

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

4 Click **Activate New** and browse to `activation.terminal_id_manager-12.5.0.jaw`.

5 Click the file. The **Terminal ID Management Add-On** is installed and added to the **Product** list.

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

7 Continue with Step 2: Activate the server.

Step 2: Activate the server.

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

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

2 Restart the MSS Server.

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

3a On the **About > Product Information** panel, find the **MSS Data Path**.

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

```
idmanagement.enabled=false
```

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

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

Continue with Step 3: Configure Terminal ID Manager.

Step 3: Configure Terminal ID Manager.

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

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

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

To configure the Terminal ID Manager:

1 In Administrative Console, go to **Configure Settings - Terminal ID Manager**.

   Check **Enable Terminal ID Manager**, and enter the required information.

2 Open the Terminal ID Manager console, in one of two ways:

   2a Click the Server URL for the Terminal ID Manager.

   2b From the **Start** menu, click **Terminal ID Management Administration**.

3 Populate the server with IDs, pools and association sets.

   Refer to **Help** for assistance.

4 After completing the steps to populate the Terminal ID management database, start the Terminal ID Manager console.

5 On the **Server Settings** tab, confirm that

   - the database input is valid.
   - the Terminal ID Manager is available for sessions configured to use the **ID Manager** as the connection method.

6 Configure sessions for your users with **Terminal ID Manager** as the connection method.

   If available, click **Test selected attributes** to test the connection and confirm that the configuration successfully assigns an ID for the session.

Use the **Monitor IDs** tab in the Terminal ID Manager console to review ID usage and release, reclaim, and hold IDs.

10 Setting Up Automated Sign-On for Mainframe

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

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

Overview of Automated Sign-On for Mainframe

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

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

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

Related Topics

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

Automated Sign-On for Mainframe: Prerequisites and System Requirements

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

- Management and Security Server (the Administrative Server) is installed.
- Terminal emulation software, such as Reflection Desktop, is installed on the client and administrator's workstations.
- The Automated Sign-On for Mainframe Add-On activation file is available (after purchase).
- z/OS with DCAS is installed on the mainframe.
- LDAP directory is used for user authorization.
- A browser using JRE 8 that can run trusted applets and supports JavaScript,

  cookies, and cascading style sheets.

Related Topics

- Steps to Set Up Automated Sign-On for Mainframe

Steps to Set Up Automated Sign-On for Mainframe

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

- Step 1. Install Automated Sign-On for Mainframe.
- Step 2. Configure the mainframe.
- Step 3. Configure settings in Administrative Console.

Step 1. Install Automated Sign-On for Mainframe.

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

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

   `activation.automated_signon_for_mainframe-12.5.0.jaw`
2. Download the activation file and note the location.
3. In the Management and Security Server, open the Administrative Console and click **Configure Settings - Product Activation**.
4. Click **Activate New** and browse to `activation.automated_signon_for_mainframe-12.5.0.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 Administrative Console is fully updated with the new set of activation files. You do not need to restart the Administrative Server (MSS Server) service.
7. Continue with Step 2. Configure the mainframe.

Step 2. Configure the mainframe.

Detailed steps are provided in the Automated Sign-On for Mainframe Administrator Guide.

(If you prefer a PDF version, click the 📄 icon at the top of the guide.)

Step 3. Configure settings in Administrative Console.

In the Administrative Console, open **Configure Settings - Automated Sign-on**.

Follow the steps for the Configuration Tasks presented in the Automated Sign-On for Mainframe Administrator Guide.

11 Setting Up Micro Focus Advanced Authentication Add-On

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

As an add-on product, this access control method provides user authentication to Management and Security Server using Micro Focus Advanced Authentication.

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

Advanced Authentication Add-On: Prerequisites and System Requirements

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

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

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

Related Topics

- Setting Up Micro Focus Advanced Authentication Add-On
- Step 1: Installing Micro Focus Advanced Authentication Add-On

Step 1: Installing Micro Focus Advanced Authentication Add-On

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

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

   ```
   activation.advanced_authentication-12.5.0.jaw
   ```

2. Download the activation file and note the location.
3. In the Management and Security Server, open the Administrative Console and click **Configure Settings - Product Activation**.
4. Click **Activate New** and browse to activation.advanced_authentication-12.5.0.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 Administrative Console is fully updated with the new set of activation files. You do not need to restart the Administrative Server (MSS Server) service.
7. Continue with Step 2: Setting up Advanced Authentication in the Administrative Console.

Step 2: Setting up Advanced Authentication in the Administrative Console

In the 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.

Continue with Step 3: Configuring authentication methods.

Step 3: Configuring authentication methods

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

12 After you install

Check this section if you encounter issues after you install and begin using Management and Security Server. For further assistance, contact Support.

- Issue: Applications hang on UNIX or Linux
- Resources

Issue: Applications hang on UNIX or Linux

The Problem

The Management and Security Server installer, server, and configuration utilities may hang on UNIX or Linux systems, particularly headless ones. The hang or stall is caused by an insufficient amount of entropy in the system, typically due to a lack of interaction with the operating system's UI (or lack of UI).

The Fix: `/dev/urandom`

In Management and Security Server (12.4.2 and higher), the Entropy Gathering Device (EGD) for UNIX/Linux is explicitly set to `/dev/urandom`, which is a non-blocking EGD. Although the use of `/dev/urandom` may be controversial, it was decided that using a non-blocking EGD would provide a more favorable user experience.

Alternative Solutions

If use of `/dev/urandom` is not acceptable or permitted in your environment, you can configure the applications to use `/dev/random`, as follows.

1. For security and responsiveness, consider installing a software package that obtains secure random data from the machine's hardware. These packages require systems equipped with newer chipsets or cryptographic hardware. Refer to the package documentation for specific requirements. Example packages include:
   - `rng-tools`
   - `haveged`
2. Explicitly change the EGD by setting a property for each Management and Security Server application, as listed in Table 1.

Table 12-1 Example: changing the EGD to `/dev/random`

Application	How to set the Entropy Gathering Device (EGD)
Installer	On the installer's **command line**, prepend `-J` to the Java System property: `mss-12.5.0.<nnn>-prod-linuxx64.sh -J-Djava.security.egd=file:///dev/random` For each of the applications below, either edit the property's value or comment-out the property to use the system's default EGD value of `/dev/random`.
MSS Server	In **container.conf**, modify the service wrapper's `additional` JVM property by incrementing the highest number (X) by one integer: `wrapper.java.additional.X=-Djava.security.egd=file:///dev/random`
Initial Configuration Utility	In the `*.vmoptions` file for each utility and the Security Proxy, add the property or set the value. `-Djava.security.egd=file:///dev/random`
Configuration Upgrade Utility	
HTTPS Certificate Utility	
Keychain Utility	
MSS Security Proxy	

Related Topics

- Appendix A. Configuration Utilities
- Resources

Resources

For assistance with technical issues:

- See Host Access Management and Security Server - Technical Resources
- Contact Support

13 Upgrading to Version 12.5

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

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

CAUTION: Check the versions of the products that use Management and Security Server to be sure that connections work as expected.

- **Reflection ZFE.** Reflection ZFE version 2.3 is compatible with Management and Security Server 12.5.
- **Reflection for the Web.** Reflection for the Web must be upgraded to 12.3 SP1 (or higher) to be compatible with the updated crypto modules in Management and Security Server (since version 12.4 SP1).

Note: The **Security Proxy Server** must be the same `<major>.<minor>.<update>` version as Management and Security Server.

Upgrading topics:

- Download Product Files
- Upgrading the Security Proxy Server
- Upgrading Replicated Servers
- Upgrading Add-On Products
- Using the Automated Installer
- Upgrading a Manual Installation
- Directory Names and Installation Paths
- If you use LDAP with TLS (LDAPS)

Download Product Files

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

1. Download the automated installer or the manual.zip file 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`.

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

Related Topics

- Upgrading the Security Proxy Server

- Upgrading Replicated Servers
- Upgrading Add-On Products
- Using the Automated Installer
- Upgrading a Manual Installation

Upgrading the Security Proxy Server

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

- Match the version
- Synchronize an upgraded Security Proxy

Match the version

The <major>.<minor>.<update> version of the Security Proxy must be the same as Management and Security Server.

Be sure to download the upgraded Security Proxy activation file and run it with the automated installer. Or, install the activation file and activate the server.

Synchronize an upgraded Security Proxy

If the Security Proxy is installed when you upgrade Management and Security Server from version 12.4.<nn> to a later version (including updates and service packs), be sure to synchronize the Security Proxy with the MSS Administrative Server.

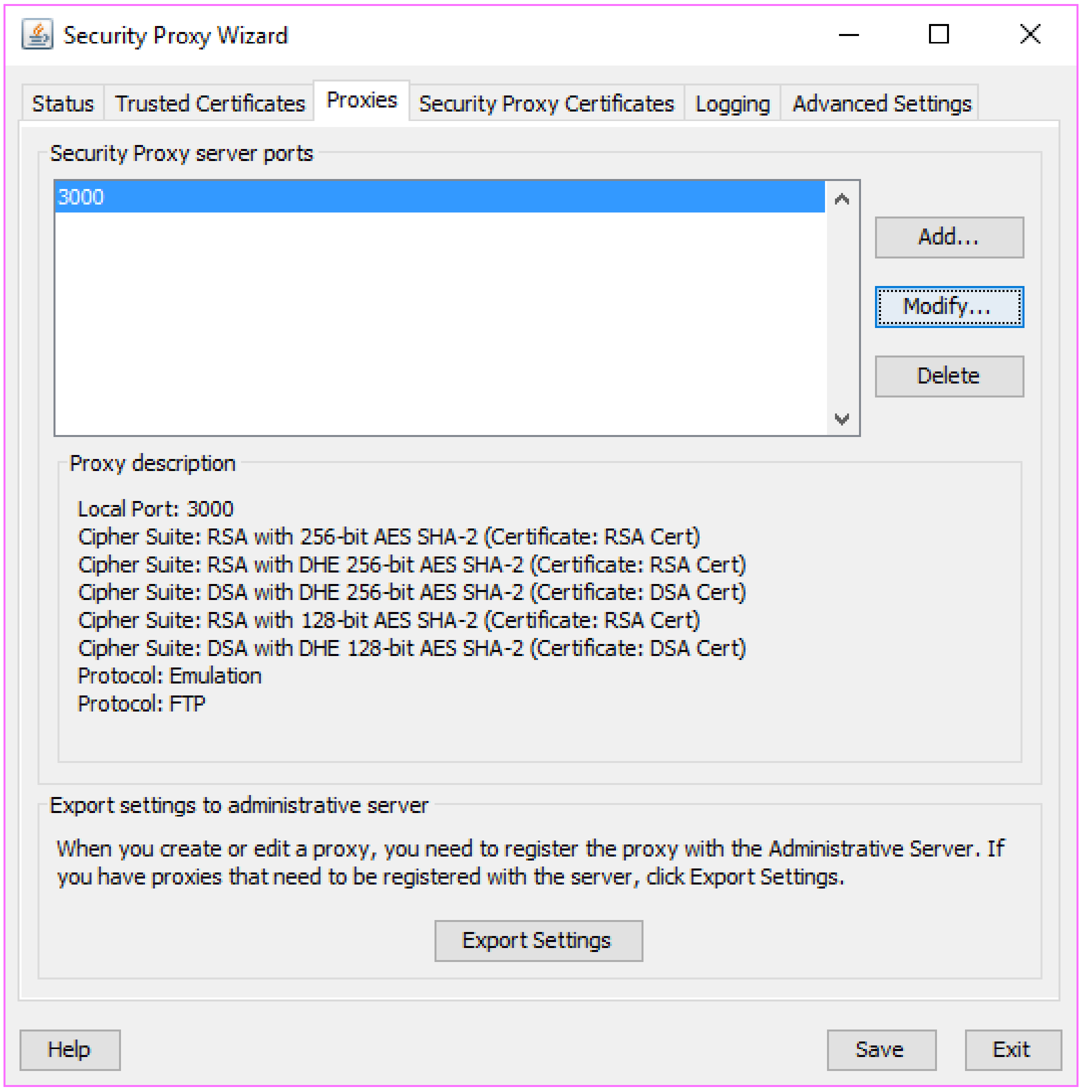
To synchronize the Security Proxy:

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



Local Port: 3000
Cipher Suite: RSA with 256-bit AES SHA-2 (Certificate: RSA Cert)
Cipher Suite: RSA with DHE 256-bit AES SHA-2 (Certificate: RSA Cert)
Cipher Suite: DSA with DHE 256-bit AES SHA-2 (Certificate: DSA Cert)
Cipher Suite: RSA with 128-bit AES SHA-2 (Certificate: RSA Cert)
Cipher Suite: DSA with DHE 128-bit AES SHA-2 (Certificate: DSA Cert)
Protocol: Emulation
Protocol: FTP

When you create or edit a proxy, you need to register the proxy with the Administrative Server. If you have proxies that need to be registered with the server, click Export Settings.

3 To select a different certificate for a particular port:

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

3b Note (or change) the selected cipher suites.

3c Select an RSA certificate or DSA certificate for that type of cipher suite. Click **OK**.

3d On the **Proxies** tab, click **Save**.

3e Click **Export** to send the settings to the MSS Administrative Server.

Related Topics

- Upgrading Replicated Servers
- Upgrading Add-On Products
- Using the Automated Installer
- Upgrading a Manual Installation

Upgrading Replicated Servers

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

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

1 In the Administrative 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 the **Master** server.

4 When all of the servers are set to **Standalone**, upgrade each server.

5 When all of the servers are upgraded, re-enable **Replication**:

   5a Configure the **Master** server from **Standalone** back to the **Master** server role, and add the **Slave** servers.

   5b Configure the **Slave** servers from **Standalone** back to the **Slave** server role, and add the **Master** server.

   For more information, see **Replication** in the *Management and Security Server Administrator Guide*.

Related Topics

- Upgrading Add-On Products
- Using the Automated Installer
- Upgrading a Manual Installation

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.

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

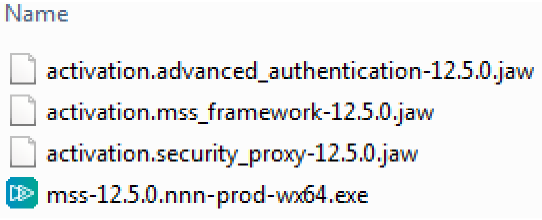
Related Topics

- Using the Automated Installer
- Upgrading a Manual Installation

Using the Automated Installer

To upgrade using the automated installer:

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



Name

activation.advanced_authentication-12.5.0.jaw

activation.mss_framework-12.5.0.jaw

activation.security_proxy-12.5.0.jaw

mss-12.5.0.nnn-prod-wx64.exe

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.

Upgrading a Manual Installation

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

To upgrade a manual installation:

- Step 1. Extract the manual installation.zip file.
- Step 2. Install the new product version into a different folder.
- Step 3. Run the Configuration Upgrade Utility
- Step 4. Install and start services
- If you are upgrading Reflection for the Web

Step 1. Extract the manual installation.zip file.

After you download and extract the.zip file for your platform, make each tar file executable.

Step 2. Install the new product version into a different folder.

Plan to install the new product version into a different folder than the earlier installation; that is, side by side.

Step 3. Run the Configuration Upgrade Utility

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

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

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

Run the configuration utility

1 Before you run the Configuration Upgrade Utility, these conditions must be in place:

1a Make sure the earlier version of the software is not running when you run the Configuration Upgrade Utility.

Doing so will avoid potential port conflicts and allow you to accept default port assignments.

1b If you are upgrading a Linux or UNIX system, make sure that no startup scripts are running.

1c Verify that you have administrator privileges. If not, you will be prompted for credentials.

1d Uninstall the services, such as the MSS Server and MSS Security Proxy.

1e In the `mss/server/conf/container.properties` file, change the `dataFolder` property to the new (custom) location where the current user has `write` access.

2 Run the **Configuration Upgrade Utility**.

- For Linux or UNIX, the utility must be made executable using the `chmod +x` command.
- To run it in console mode, use the `–c` parameter.

Proceed through the prompts.

3 **Select your language.**

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

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

5 **Services:** Select the services you want to enable. You must have an Administrative Server service running, but the Metering Server, Terminal ID Manager Add-On, and the Security Proxy Add-On can be installed and run on separate machines.

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

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

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

9 **Configuration Summary:** A summary of the configuration changes, `configutil.log` in the installation directory, is created. Click **Done** to continue to Step 4. Install and start services.

Step 4. Install and start services

After you run the **Configuration Upgrade Utility**, install and start the 12.5.0.<nnn> services that you uninstalled before you began (such as MSS Server and MSS Security Proxy).

Note: If you are upgrading Reflection for the Web, be sure to see If you are upgrading Reflection for the Web

If you are upgrading Reflection for the Web

The `rweb-client` web application context must be installed to complete the upgrade.

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

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

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

Directory Names and Installation Paths

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

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

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

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

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

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

Related Topics

- Upgrading to Version 12.5

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 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.”

14 Uninstalling

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

To uninstall Management and Security Server:

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

Removing Components

To remove a component:

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

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

     ```
     [MssServerInstall]/uninstall
     ```

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

NOTES:

- If you plan to remove either the **Administrative Server**, the **Terminal ID Manager**, or the **Metering Server** using the automated installer, be aware that you must uninstall web applications and the servlet runner at the same time.
- If you installed a component **manually**, simply delete the directory where you extracted it. If you want to save the settings that you configured, be sure to retain the MSSData directory. For more information about retaining settings, see Upgrading to Version 12.5.

15 Appendices

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

Appendix A. Configuration Utilities

During and after you install Management and Security Server, you may be directed to run one or more utility. To run these utilities, Management and Security Server must have been installed using either the automated installer or the multi-component manual installation.

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

Initial Configuration Utility

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

The Initial Configuration Utility:

- enables the services you select for the Administrative Server.
- creates an MSSData directory under which site-specific content is stored.
- generates cryptographic keys and self-signed certificates for the servlet runner and the Administrative Server.
- sets the administrative password.
- sets a port value for the Administrative Server in configuration and HTML files.
- (if installed) configures the Security Proxy Add-On: generates cryptographic keys and self-signed certificates, automates configuration, and sets a port value for the Security Proxy.

Running the utility:

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

   Windows systems:

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

   Linux or UNIX systems:

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

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

Configuration Upgrade Utility

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

The Configuration Upgrade Utility (CUU):

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

Run the utility

1 Before you begin:

1a Make sure the earlier version of the software is not running when you run the Configuration Upgrade Utility.

This step will avoid potential port conflicts and allow you to accept default port assignments.

1b Verify that you have administrator privileges. If not, you will be prompted for credentials.

1c **For manual installation:** First uninstall any services, such as MSS Server and MSS SecurityProxy.

2 Launch the Configuration Upgrade Utility from its installed location. To launch in console mode, use `-c`.

Windows systems:

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

Linux or UNIX systems:

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

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

4 **For manual installation:** After running the CUU, install and start the 12.5 services (such as MSS Server and MSS SecurityProxy).

HTTPS Certificate Utility

The HTTPS Certificate Utility manages the default servlet runner certificate. Use this utility to install or update a certificate for the HTTP server functionality that is included with the Management and Security Server. This certificate enables clients to establish secure connections (HTTPS) to the services provided by the Management and Security Server. (Other certificates are managed differently.)

Beginning in version 12.4.2, 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. To run this utility, Management and Security Server must have been installed using an automated installer or multi-component manual installation file.

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

   Windows systems:

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

   Linux or UNIX systems:

   ```
   [MssServerInstall]/utilities/bin/HTTPSCertificateUtility
   ```
3. Follow the prompts in the utility, and select a certificate action:
   - Generate a new key pair and self-signed certificate.
   - 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. Use of either utility will overwrite any existing keys.
- You can configure Management and Security Server to use either a self-signed certificate, or a CA-signed SSL server certificate. For details regarding CA-signed certificates, see Technical Note 1702.

Requiring HTTPS in the Administrative Server

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

1. In the Administrative Console, click **Configure Settings** > **General Security**.
2. Check **Require HTTPS for connections to the Management and Security Server**.
3. Click **Apply**.

IIS Integration Utility (on Windows)

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

Reasons to Integrate Management and Security Server with IIS

By default, a web server is installed, and you do not need to integrate the product with IIS. However, you may choose to integrate Management and Security Server with IIS to

- take advantage of the IIS Single Sign-on (SSO) functionality.
- use your existing web server certificates on IIS.

NOTE: When integrated with the IIS web server, Management and Security Server uses IIS and the IIS-configured server certificate for HTTPS communication; the servlet runner certificate is ignored. Although the servlet runner certificate is not used after IIS integration, it is recommended that you do not delete that certificate. Once integrated with IIS, the expiration status of the servlet runner certificate does not affect the Management and Security Server installation.

When to integrate:

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

Running the IIS Integration Utility:

1. Run the IIS Integration Utility (`IISIntegrationUtility.exe`) located in the `[MssServerInstall]\utilities\bin` directory.
2. To integrate IIS with Management and Security Server, select a site and click **Integrate**.
3. If you are prompted, confirm the installation directory (for example, `C:\Program Files\Micro Focus\MSS`) and click **Yes.**
4. If you are prompted to install required IIS role services, click **Yes**. Installation of role services can take a few minutes.
5. If you are prompted to restart the Administrative Server service, click **Yes**.
6. On the Integration Completed message box, click **Yes** to exit.
7. Restart the Administrative Server. This step is necessary only if you did not select the option to restart the MSS service.
    - If you installed the product as a Windows service, go to Control Panel > Administrative Tools > Services > Micro Focus MSS Server. Stop and restart the service.
    - You can also use the -stop and -start commands with MssServer.exe.
8. Confirm that integration was successful by browsing to

    ```
    http://<serverName>[:port]/mss/AdminStart.html
    ```

    where <serverName> is the IP address or alias of your Microsoft Windows machine running the Administrative Server, for example: http://myserver.mycompany.com/mss/AdminStart.html.

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

Appendix B. Specifying a non-default location for MSSData

MSSData is the root directory under which site-specific content is stored, including server configuration files, keystores, and emulator session information. This directory is created automatically; there are no additional steps required for installation.

The default location for MSSData:

- **On Windows**:

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

- **On Linux or UNIX:**

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

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 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 UNIX: `dataFolder=/var/data/mssdata`
3. Save your changes and restart the MSS Server.