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

Host Access Management and Security Server Installation Guide

1 Introduction

1.1 How Management and Security Server works .................................................. 9
1.2 What Management and Security Server installs ............................................. 10
  1.2.1 Installed and Enabled Components ....................................................... 10
  1.2.2 Add-On Products ..................................................................................... 10
1.3 Overview of Components and Add-On Products ............................................. 11
  1.3.1 Administrative Server ............................................................................ 11
  1.3.2 Metering Server ..................................................................................... 11
  1.3.3 Configuration Utilities ........................................................................... 11
  1.3.4 Security Proxy Add-On .......................................................................... 11
  1.3.5 Terminal ID Manager Add-On ................................................................. 12
  1.3.6 Automated Sign-On for Mainframe Add-On ........................................... 12
  1.3.7 Micro Focus Advanced Authentication Add-On ..................................... 12

2 Preparing to Install

2.1 Prerequisite Actions ....................................................................................... 13
  2.1.1 Shut down any currently running components ....................................... 13
  2.1.2 Obtain the required user privileges ....................................................... 13
  2.1.3 Obtain the required account permissions ............................................. 13
  2.1.4 On Linux, verify fonts are installed ...................................................... 14
2.2 System Requirements ..................................................................................... 14
  2.2.1 Administrative Server requirements .................................................... 14
  2.2.2 Browser requirements .......................................................................... 15
  2.2.3 Metering Server requirements .............................................................. 15
  2.2.4 Requirements for Add-On Products ..................................................... 15

3 Automated Installation

3.1 Automated Installation Procedure ................................................................. 17
  3.1.1 Step 1: Run the automated installer ....................................................... 17
  3.1.2 Step 2: Enter configuration information ............................................. 18
  3.1.3 Step 3: Start services ............................................................................ 20
3.2 Ports used by Management and Security Server ......................................... 20
3.3 Installation Variations .................................................................................... 21
  3.3.1 Installing on UNIX with no JRE ............................................................. 21
  3.3.2 Servlet Runner Launcher JVM Options .............................................. 22
  3.3.3 Servlet runner other than Apache Tomcat ........................................... 22
  3.3.4 Integrating SiteMinder with MSS ......................................................... 22
  3.3.5 Using the automated installer in console mode .................................... 24
  3.3.6 Unattended installation ....................................................................... 24

4 Open the Administrative Console

4.1 Log in to the Administrative Server ............................................................ 27
  4.1.1 Using the Administrative Server HTML login ................................... 27
  4.1.2 Using the Administrative Server Java-based login ............................... 28
## Contents

Configure the Administrative Server ................................................................. 28  
  Initial Settings ................................................................................................. 29  
  Next Steps ....................................................................................................... 29  

5 Setting Up Metering 31  
  Metering Setup at a glance .............................................................................. 31  
  Metering: Prerequisites and System Requirements ........................................ 31  
  How Metering Works. ....................................................................................... 31

6 Installing Add-On Products 33  
  Installing Activation Files .................................................................................. 33  
    Use the automated installer to install activation files ..................................... 33  
    Use the Administrative Console to install activation files .............................. 34

7 Setting Up the Security Proxy 35  
  Before you install the Security Proxy ............................................................... 35  
    How the Security Proxy Server works ............................................................ 35  
    Security Proxy: Prerequisites and System Requirements ............................. 37  
  Install the Security Proxy Server .................................................................... 40  
    To install the Security Proxy WHEN you install the MSS Administrative Server  41  
    To install the Security Proxy AFTER you install the MSS Administrative Server 42

8 Setting Up Terminal ID Manager 45  
  Terminal ID Manager: Prerequisites and System Requirements ....................... 45  
    Supported emulator and session types .......................................................... 45  
  Run the MSS automated installer .................................................................... 46  
    To install Terminal ID Manager on a separate machine .............................. 46  
    To install Terminal ID Manager on the same machine ................................. 46  
  Configure Terminal ID Manager ...................................................................... 47

9 Setting Up Automated Sign-On for Mainframe 49  
  Automated Sign-On for Mainframe: Prerequisites and System Requirements ... 49  
  Installing Automated Sign-On for Mainframe .................................................. 49  
    Next step ....................................................................................................... 50

10 Setting Up Micro Focus Advanced Authentication Add-On 51  
  Advanced Authentication Add-On: Prerequisites and System Requirements .......... 51  
  Step 1: Installing Micro Focus Advanced Authentication Add-On ................... 51  
  Step 2: Setting up Advanced Authentication in the Administrative Console .......... 52  
  Step 3: Configuring authentication methods .................................................... 52

11 After you install 53  
  Issue: Applications hang on UNIX or Linux ..................................................... 53  
    The Problem. ................................................................................................. 53  
    The Fix: /dev/urandom ................................................................................. 53  
    Alternative Solutions ................................................................................... 53  
  Resources ....................................................................................................... 54
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 12.6
About Automated Installation
About Add-On Products
If you are evaluating...

About Management and Security Server 12.6

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

Management and Security Server version 12.6 released with Host Access for the Cloud* 2.4

* Beginning with version 2.4, Reflection ZFE is called Host Access for the Cloud.

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

About Automated Installation

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

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

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

- The manual installation files are no longer available.
- Check the Installation Variations if your system requirements differ from an automated installation.

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

About Add-On Products

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

Add-on products include:

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

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.
Introduction

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

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 *
  * if entitled. 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 and security can be augmented with add-on products. Each add-on product requires a separate license and may require separate installation and activation.

See Installing Add-On Products for details.

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.

Administrative Console

The Administrative Console is the user interface for Management and Security Server’s Administrative Server. Use the Administrative Console to manage sessions, assign access to sessions, configure security settings, configure metering and add-on functionality, and to 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 is automatically installed with the Management and Security Server.

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

See Setting Up Metering.

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 12.6, be sure to upgrade the Security Proxy to version 12.6.

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.


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
Preparing to Install

Check these requirements before you install Management and Security Server.

- 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 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.

- Supported Platforms
- Administrative Server requirements
- Browser requirements
- Metering Server requirements
- Requirements for Add-On Products

Supported Platforms

Automated installers are available for 64-bit systems running on Linux, UNIX, and Windows.

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

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.
**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, installed with the Administrative Server, also 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**

- A server running JRE 8. (An Open JDK is installed by the automated installer.)
- See also Setting Up the Security Proxy

**Terminal ID Manager**

- A server running JRE 8. (An Open JDK is installed by the automated installer.)
- See also Setting Up Terminal ID Manager

**Automated Sign-On for Mainframe**

- 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.
- See also Setting Up Automated Sign-On for Mainframe

**Micro Focus Advanced Authentication**

- See Setting Up Micro Focus Advanced Authentication Add-On
Related topics

- Prerequisite Actions
Automated Installation

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

**NOTE:** If you are not able to use an automated installer, contact Support for guidance.

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
- Ports used by Management and Security Server
- Installation Variations

Automated Installation Procedure

*Reminder:* 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.

Consider installing your entitled activation files along with the automated installer.

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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Automated Installer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux 64-bit</td>
<td>mss-12.6.0.&lt;nnn&gt;-prod-linuxx64.sh</td>
</tr>
<tr>
<td>z Linux</td>
<td>mss-12.6.0.&lt;nnn&gt;-prod-unix-nojre.sh</td>
</tr>
<tr>
<td>Windows 64-bit</td>
<td>mss-12.6.0.&lt;nnn&gt;-prod-wx64.exe</td>
</tr>
</tbody>
</table>
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 Automated Sign-On for Mainframe Add-On, place the activation file in the same folder as the installer, mss-12.6.0.<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. Check this 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 12.6.)

**Step 2: Enter configuration information.**

If you are installing Management and Security Server for the first time on this machine, the automated installer starts the Initial Configuration Utility. For a description, see Initial Configuration Utility.
NOTE: Do not close the installer when the configuration utility is launched. You must complete additional steps in the installer after completing configuration.

Enter or verify your configuration information. Refer to Ports used by Management and Security Server as needed.

1 **Installation Directory**: Confirm or browse to the location where the Administrative Server was installed.

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

3 **Volume Purchase Agreement number**: Optional. Enter the Volume Purchase Agreement (VPA) number. You can modify the VPA number later in the 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.
   **Note**: To change the administrative password later, use either the Administrative Console (Configure Settings - General Security) or run the Password Change Utility, (documented in the Management and Security Server Administrator Guide).

7 **Server Names for URLs and Certificates**: The information that you enter on this and the following panel enable you to create self-signed certificates that will be used to make secure TLS connections to the Administrative Server and Security Proxy after installation.
   Enter a **DNS name** or **IP address**. The current DNS name is provided, when available. To change the servlet runner certificate later, use the HTTPS Certificate Utility.

8 **Server certificates: organization and locality** (optional)
   This panel includes additional information for creating certificates.
   **Organizational Unit**: Enter the name of your organizational unit, typically the name of your department or division.
   **Organization**: Enter the name of your organization, typically the legal name of your company or organization.
   **City or Locality**: Enter the full formal name (no abbreviations).
   **State**: Enter the full formal name (no abbreviations).
   **Country**: Provide a two-letter ISO country code, such as US.

9 **Confirm Configuration**: Click Next to apply the specified configuration changes.

10 **Configuration summary**: A summary of the configuration changes is created in InitialConfigurationUtility.log in the <installation>\utilities\logs directory.
   Click Done. You are ready for Step 3: Start Services.
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 **Open the Administrative Console**.

**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

- Ports used by Management and Security Server
- Installation Variations
- Open the Administrative Console

Ports used by Management and Security Server

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

<table>
<thead>
<tr>
<th>Port used for ...</th>
<th>Default port number</th>
<th>How to change the port number</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td></td>
</tr>
</tbody>
</table>
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

### 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-12.6.<u>.<nnn>-prod-unix-nojre.sh, where <u> is the update number and <nnn> is the build number.
2. Proceed with the installation, using your existing JRE.

### Port used for ... | Default port number | How to change the port number
---|---|---
HTTPS | 443 | 1. Start the MSS server. This action creates the default PropertyDS.xml file in the MSSData directory. 2. Open PropertyDS.xml. 3. In the string shown below, change the value from 443 to the preferred port number: `<CORE_PROPERTY NAME="sslport"> <STRING>443</STRING> ` 4. Restart Management and Security Server.
Security Proxy listening port | 3000 |  
Security Proxy monitoring port | 8080 |  
Database replication | 7000 |  
Database replication TLS | 7001 |  
X.509 Trusted subsystem | 8003 |  
Service registry | 8761 |  

### HTTPS 443

1. Start the MSS server. This action creates the default PropertyDS.xml file in the MSSData directory.
2. Open PropertyDS.xml.
3. In the string shown below, change the value from 443 to the preferred port number: `<CORE_PROPERTY NAME="sslport"> <STRING>443</STRING> ` 4. Restart Management and Security Server.
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

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.

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 to “See Help to enable,” then the SiteMinder Java Agent library has not been detected in the classpath for the MSS Server.

To resolve: Be sure to complete step 4: **Add the SiteMinder libraries to MSS.**

---

**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 memory, 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 `<12.6.0.nnn>` is the product version and build number:

   ```bash
   mss-<12.6.0.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."
Related topics

- Open the Administrative Console
- Automated Installation Procedure
Open the Administrative Console

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

After you log in to the Administrative 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 Server
- Configure the Administrative Server

Log in to the Administrative Server

You can log in to the Administrative Server (which opens 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. (The servlet runner is automatically started by the MSS installer.)
2. Choose a login option:
   - **Administrative Server**
     This HTML login directly opens the Administrative Console (in English).
     See Using Administrative Server (HTML login).
   - **Administrative Server** (via Java-based links list)
     This login opens the list of session links, with a link to the Administrative Console. (Java is required on the client.)
     See Using the Administrative Server Java-based login.

Using the 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 the Administrative Server Java-based 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 (via Java-based links list)
   - 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 Configure the Administrative Server.

Configure the Administrative Server

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

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

1. Open **Configure Settings - General Settings**. Enter your initial settings and preferences. Open Help for more information. Click **Apply**.

2. Open **Configure Settings - General Security**. Scroll to the **Require new login** field. Change the default to a higher number to avoid a session timeout while you are configuring settings. Click **Apply**.

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

---

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

---

**Next Steps**

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

For details, see:

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

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

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

- Metering Setup at a glance
- Metering: Prerequisites and System Requirements
- How Metering Works

Metering Setup at a glance

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

2. On the Configure Settings - Metering panel, click the link to a Metering Server to open the separate Metering Console (after you log in as a Metering administrator).
   Use the Metering Console to configure license pools and server settings and to run reports. Open Help for assistance.
3. Enable the clients that are to be metered.
   Refer to your emulator’s product documentation to enable metering for that client.

Metering: Prerequisites and System Requirements

Before you can create metered sessions, verify that:

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

How Metering Works

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

1. A user starts a client session and initiates a host connection.
2. The session requests a license from the Metering Server, and once granted, the host connection proceeds, and the Metering Server begins to record product usage.
3. The session sends updates to the Metering Server at regular intervals until the user closes the session.
4. The metering data is available for the administrator to generate reports.
   You can filter Metering Reports to show
   • activity by user, machine, IP address, and other attributes
   • concurrent usage (to comply with your license)
   • host connections
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 Automated Sign-on for Mainframe Add-On, place the activation file in the same folder as the installer, `mss-12.6.0.<nnn>-prod-wx64.exe`.

   ![Image of file selection](image)

   **NOTE:** The `activation.mss_framework-12.6.0.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
Setting Up the Security Proxy

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

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

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

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

If you choose to install it separately, follow the steps in this guide to **install** and **activate** the Security Proxy.

Then, see *Using the Security Proxy Server* (in the MSS *Administrator Guide*) to **configure** the Security Proxy.

- **Before you install the Security Proxy**
- **Install the Security Proxy Server**

### Before you install the Security Proxy

Learn how the Security Proxy Server works, and check the System Requirements before you install and configure the Security Proxy.

- **How the Security Proxy Server works**
- **Security Proxy: Prerequisites and System Requirements**

### How the Security Proxy Server works

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

The following diagram highlights the Security Proxy (steps 5 and 6) in the context of the overall Management and Security Server set up.
1 User connects to the Administrative Server.
2 User authenticates to a directory server (LDAP/Active Directory) or other identity management system (optional).
3 The directory server provides user and group identity (optional).
4 The Administrative Server sends an emulation session to the authorized client.

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

6 The Security Proxy Server validates the session token and establishes a connection to the specified host:port. The security proxy encrypts the data before forwarding it back to the user.

   Note: The connection between the Security Proxy and the host is not encrypted — unless End to end encryption is selected in the session configuration.

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

The Security Proxy Add-On requires a separate license. Before installing the Security Proxy, verify that:

- the Management and Security Server automated installer is available. (The Security Proxy can be installed along with MSS or by itself later.)
- the Security Proxy activation file (activation.security_proxy-12.6.<n>.jaw) 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 12.6.0 be sure to upgrade the Security Proxy to version 12.6.0.

- 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 7-1  Recommended Specifications for Security Proxy servers

<table>
<thead>
<tr>
<th>System Specification</th>
<th>up to 6000 connections (concurrent and active)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed of processors</td>
<td>2.7 GHz or faster</td>
</tr>
<tr>
<td>Number of processors (or cores)</td>
<td>4 or more</td>
</tr>
<tr>
<td>System RAM</td>
<td>4 GB or more</td>
</tr>
<tr>
<td>Java Virtual Machine (JVM) heap size</td>
<td>3072 MB</td>
</tr>
<tr>
<td>Java Runtime Environment (JRE)</td>
<td>Use a current 64-bit JRE</td>
</tr>
<tr>
<td>File descriptors (Linux/UNIX)</td>
<td>21,000</td>
</tr>
</tbody>
</table>

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>in`.

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:

```shell
-Xms3072m
-Xmx3072m
```

**Java Runtime Environment (JRE)**

Use a current JRE. In general, newer JREs provide better performance with more efficient 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:

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

To change the number of available ports:
Setting Up the Security Proxy

```
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:

\[
\text{number of descriptors} = 20 + (\text{<connections>} \times 2)
\]

where \(<\text{connections}>\) 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: \(20 + (6000 \text{ connections} \times 2) = 12020\) 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 \(<\text{descriptors}>\) 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.

Related topics
- Install the Security Proxy Server

Install the Security Proxy Server

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

NOTE: About secure connections

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

If you install and run the Security Proxy server directly on the host, connections will be highly secure but CPU-intensive because additional processing is required to encrypt and decrypt the data stream.
You can increase the security of terminal session connections by ensuring that there is only one known, secure link between the Security Proxy server and the host. If you select **End to end encryption** when configuring a session, the connection between the Security Proxy and the host will use TLS.

### Installation options

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

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

**NOTE:** If you are not able to use the automated installer — contact Support for guidance.

### To install the Security Proxy **WHEN** you install the MSS Administrative Server

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

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

1. Download the Security Proxy Add-On activation file, `activation.security_proxy-12.6.0.jaw`, and note the location.
2. Place the security proxy activation file in the same folder as the MSS automated installer. *In this example, the Host Access for the Cloud activation file is also installed.*

3. Run the MSS installer for your platform. During installation, be sure BOTH boxes are checked:
   - [ ] Host Access Management and Security Server
   - [ ] Security Proxy Server

4. When prompted, run the **Initial Configuration Utility**.
   This utility generates cryptographic keys and self-signed certificates, automates configuration, and sets a port value for the Security Proxy.
   The automated installer also places the activation file in the installation directory:

```
/MSS/securityproxy/lib/modules
```
The Security Proxy is now installed, activated, and configured.

5 To view or change the configuration, open the Security Proxy Wizard from the Start menu. For details, see Using the Security Proxy Server - Configure and Start the Security Proxy Server (in the MSS Administrator Guide).

To install the Security Proxy AFTER you install the MSS Administrative Server

You can add the Security Proxy to MSS after the MSS Administrative Server is already installed. Keep in mind that the Security Proxy needs to be installed, activated, and configured, which can be done either automatically or as separate actions. Choose a method:

- Automatically install, activate, and configure the Security Proxy
- Separately install, activate, and configure the Security Proxy

Automatically install, activate, and configure the Security Proxy

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

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

Separately install, activate, and configure the Security Proxy

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

1 Install.
   [ ] Host Access Management and Security Server
   [ ] Security Proxy Server
   NOTE: if only the Security Proxy Server is checked, the MSS files are removed.

2 Activate.
   Download the activation file for the Security Proxy Add-On, and note the download location.
   activation.security_proxy-12.6.0.jaw

3 In the MSS Administrative Console, click Configure Settings - Product Activation.
4 Click Activate New and browse to activation.security_proxy-12.6.0.jaw
5 Click the file. The Security Proxy Add-On is installed and added to the Product list.
6 Copy the security proxy activation file, into the /securityproxy/lib/modules directory on the machine where Security Proxy Server is installed.
   The Security Proxy is now installed and activated.

7 Configure.
   Use the Security Proxy Wizard to configure settings and manage certificates. Then, you can configure sessions to use the Security Proxy.
   Follow the steps in Using the Security Proxy Server in the MSS Administrator Guide.
In brief, you will:

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

Reference:

*MSS Administrator Guide: Using the Security Proxy Server*
Setting Up Terminal ID Manager

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

The Terminal ID Manager Add-On requires a separate license and an activation file.

Follow these steps to install Terminal ID Manager — either on the same machine or a different machine from where Management and Security Server is installed.

Then, use the Terminal ID Manager Guide to complete the configuration.

- Terminal ID Manager: Prerequisites and System Requirements
- Run the MSS automated installer
- 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 (on the same or a different machine).
- Terminal ID Manager Add-On activation file is available.
- Your emulator is supported. See Supported emulators and session types.

Supported emulator and session types

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

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

Some Windows-based sessions also support Terminal ID Manager. Refer to your product’s documentation.

Next:

- Run the MSS automated installer
- Configure Terminal ID Manager
Run the MSS automated installer

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

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

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

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

- To install Terminal ID Manager on a separate machine
- To install Terminal ID Manager on the same machine

**To install Terminal ID Manager on a separate machine**

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

   **NOTE:** The Terminal ID Manager activation file must also be on the separate machine. For ease of installation, place the activation file, `activation.terminal_id_manager-12.6.<n>.jaw`, in the same directory as the automated installer. When you run the installer, the activation file will be placed in the required location.

2. In the early installation panel, select only the Administrative Server. (Leave the Security Proxy unchecked on the separate machine.)

3. When the *Initial Configuration Utility* panel displays, enable only the Terminal ID Manager service.

4. Check to be sure that the Terminal ID Manager activation file (activation.terminal_id_manager-12.6.<n>.jaw) is installed on the separate machine in this location:
   
   ```
   C:\Program Files\Micro Focus\MSS\server\web\webapps\tidm\WEB-INF\lib\modules
   ```
   
   If the activation file is not present, copy it from your download location to the `...\tidm\WEB-INF\lib\modules` directory on the separate machine.

5. When you return to the automated installer, select the option to Start the server components now.

Next: Configure Terminal ID Manager

**To install Terminal ID Manager on the same machine**

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

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

   **NOTE:** The Terminal ID Manager activation file must also be on this machine.
For ease of installation, place the activation file, `activation.terminal_id_manager-12.6.<n>.jaw`, in the same directory as the automated installer.

When you run the installer, the activation file will be placed in the required location.

2 On the early installation panel, check that the **Terminal ID Manager** will be enabled.

3 When the automated installer completes, select the option to **Start the server components** now.

4 Verify that the Terminal ID Manager **activation file** is installed:
   4a In the **Administrative Console**, open **About > Activated Products**.
   4b In the **Product** column, look for **Terminal ID Management Add-On**.
      • If **present**, the activation file is installed on this machine.
      • If **not present**, click **Activate New**, and upload the activation file from your download location.

Next: **Configure Terminal ID Manager**

**Configure Terminal ID Manager**

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

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

Refer to the **Terminal ID Manager Guide** to complete the configuration.
Automated Sign-On for Mainframe is an add-on product that enables you to configure user access to z/OS mainframe applications using a single login. This add-on product requires a separate license.

- Automated Sign-On for Mainframe: Prerequisites and System Requirements
- Installing 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.

### Installing Automated Sign-On for Mainframe

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

1. After purchasing Automated Sign-On for Mainframe Add-On, you will receive information about downloading the product activation file: `activation.automated_signon_for_mainframe-12.6.0.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-12.6.0.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.
Next step

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

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

Refer to the Automated Sign-on for Mainframe Administrator Guide for details.
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
- 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-12.6.0.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-12.6.0.jaw.
5. Click the file. The Advanced Authentication Add-On is installed and added to the Product list.
6 Restart your browser to ensure that the 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:

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.
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 11-1  Example: changing the EGD to /dev/random

<table>
<thead>
<tr>
<th>Application</th>
<th>How to set the Entropy Gathering Device (EGD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installer</td>
<td>On the installer’s command line, prepend -J to the Java System property:</td>
</tr>
<tr>
<td></td>
<td>mss-12.6.&lt;n&gt;.&lt;nnn&gt;-prod-linuxx64.sh -J-Djava.security.egd=file:///dev/random</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>MSS Server</td>
<td>In <em>container.conf</em>, modify the service wrapper’s additional JVM property by incrementing the highest number (X) by one integer:</td>
</tr>
<tr>
<td></td>
<td>wrapper.java.additional.X=-Djava.security.egd=file:///dev/random</td>
</tr>
<tr>
<td>Initial Configuration Utility</td>
<td>In the *.vmoptions file for each utility and the Security Proxy, add the property or set the value.</td>
</tr>
<tr>
<td>Configuration Upgrade Utility</td>
<td></td>
</tr>
<tr>
<td>HTTPS Certificate Utility</td>
<td></td>
</tr>
<tr>
<td>Keychain Utility</td>
<td></td>
</tr>
<tr>
<td>MSS Security Proxy</td>
<td></td>
</tr>
</tbody>
</table>

Related topics

- Appendix A. Configuration Utilities
- Resources

Resources

For assistance with technical issues:

- See Host Access Management and Security Server - Technical Resources
- Contact Support
Upgrading to Version 12.6

Use the automated installer to upgrade to Management and Security Server.

If your current version was installed using manual installation files -- and you cannot use an automated installer -- contact Support for guidance.

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

- **Host Access for the Cloud** *version 2.4 is compatible with Management and Security Server 12.6.
- **Reflection for the Web** version 13.0 is compatible with Management and Security Server 12.6.

* formerly called Reflection ZFE

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
- 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 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`.
   Check to be sure the version matches the one for Management and Security Server.
3. Place the activation files in the same location as the automated installer.

Related topics

- Upgrading the Security Proxy Server
- Upgrading Replicated Servers
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:

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
- Running the automated installer
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
- Running the automated installer

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.

Upgrade your add-on products by either
- running the automated installer
- using the Administrative Console

Running 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.
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.

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.”
Uninstalling

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:

   When the automated installer is used 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:**
   - Run the uninstaller:
     
     \[
     \text{[MssServerInstall]/uninstall}
     \]

     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 12.6.
Appendix A. Configuration Utilities

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

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

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 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.

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.

**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 MSS 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 after Management and Security Server is installed.

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

2 Run the utility.

   **On Windows:**
On Linux or UNIX:

3 Follow the prompts in the utility, and select a certificate action:
   - Generate a new key pair and self-signed certificate.
   - Generate a new private key and Certificate Signing Request.
   - Import a certificate and private key.
   - Import the Management and Security Server certificate and private key.

**NOTE:** When needed, the HTTPS Certificate Utility can be run in console mode by using the `-console` application argument.

**Alternative approaches**

- Instead of running the HTTPS Certificate Utility, you can run the Initial Configuration Utility to generate cryptographic keys and self-signed certificates for the provided servlet runner. Any existing keys will be overwritten by either utility.
- You can configure Management and Security Server to use either a self-signed certificate, or a CA-signed SSL server certificate.

**Requiring HTTPS in the Administrative Server**

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.