Host Access Management and Security Server

Administrator Guide

12.8

Contents

4

Host Access Management and Security Server

Management and Security Server (MSS) provides a browser-based central point of administration so you can quickly configure and deploy secure terminal sessions.

An administrator uses Management and Security Server to create host sessions for Micro Focus products: Reflection Desktop, InfoConnect Desktop, Host Access for the Cloud, Reflection for the Web, and Rumba+ Desktop. The administrator can leverage the existing user and group directories to control access to the sessions.

MSS at a glance

Scan through these topics to become familiar with the MSS Administrative Console interface and the functonality of the components and add-on products.

- About Management and Security Server 12.8
- Release Notes
- About the MSS Administrative Console
- About Add-On Products

About the MSS Administrative Console

Use the MSS ADMINISTRATIVE CONSOLE to centrally secure, manage, and monitor users' access to configured sessions.

In this guide:

- Manage Sessions
- Manage Packages
- Assign Access
- Configure Settings
- Run Reports
- Technical References

About Add-On Products

Add-on products can be used to enhance Management and Security Server's functionality with supplemental means of security. These products require separate licenses and can be installed along with Management and Security Server. Additional activation or configuration is required.

Add-on products include:

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

1 About Management and Security Server 12.8

Host Access Management and Security Server version 12.8 released along with Host Access for the Cloud 2.7 in September 2021. See the Release Notes for details.

In the **MSS ADMINISTRATIVE CONSOLE**, open the **About** menu to view

- Product Information
- Activated Products
- Legal Information

Click ⊙ on the upper-right of any panel to open the **MSS Administrative Console Help**.

Product Information

View the installed **Version** and **System Information** for Host Access Management and Security Server.

Support Diagnostics

Use this option to download an archive of logs and diagnostic data from all servers. The data is packaged into a single zip file that can be sent to Micro Focus Support, when requested.

NOTE: When the server is configured for **LDAP** (specifically **Active Directory**), the MSS administrator may need to include a domain name when prompted for credentials. The format for the username is `domain\user`, such as `mycompany\joesmith`.

Activated Products

Click the link to go to the **Configure Settings - Product Activation** panel to see the list of currently installed activation files for add-on or other products.

Legal Information

View the license agreement and legal notices.

2 Manage Sessions

Use the **Manage Sessions** panel to add and configure terminal sessions. Sessions can be modified later, as needed.

Begin with the steps to **Add and Launch a session**, and then follow the steps for your product or session type. The interface varies to accommodate the different configuration settings.

- ◆ Add and Launch a session
- ◆ After the session is launched
- ◆ Manage saved sessions

Add and Launch a session

1 On the **Manage Sessions** panel, click **+ADD**.

2 Under **Configure Session**, select your **Product**. The interface changes to accommodate the settings needed for the selected product (or session type).

   Follow the steps for your product or session type.
   - ◆ Host Access for the Cloud
   - ◆ Reflection/InfoConnect Desktop
   - ◆ Reflection/InfoConnect Desktop - Workspace Automated Sign-on
   - ◆ Reflection for the Web
   - ◆ Rumba+ Desktop

Host Access for the Cloud

To add, configure, and launch a Host Access for the Cloud session:

1 On the **Manage Sessions** panel, click **+ ADD** and select **Host Access for the Cloud**.

2 Be sure Host Access for the Cloud is installed and an active session server is available. Otherwise, you will either see a message or the **LAUNCH** button will be disabled.

3 Enter a **Session name**.

4 Note the Session Server Address (session server URL), and click **LAUNCH**.

5 A browser automatically opens the session to the **CONNECTION** panel. Configure the initial settings, and click **Save**.

6 Continue editing the session configuration. When finished, click **Exit** to save the session to the Management and Security Server.

7 As a next step, you can
   - ◆ Use Assign Access to make the session available to end users.
   - ◆ Return to Manage Sessions to add or edit a session.

Related Topics

- Assign Access
- Manage Sessions
- Authentication & Authorization

Reflection/InfoConnect Desktop

NOTE: *MSS no longer supports centralized management for Reflection 14, Reflection for Secure IT, Extra! X-treme, or Verastream Host Integrator*.

To add, configure, and launch a session:

1 On the **Manage Sessions** panel, click **+ADD**.

2 Under **Configure Session**, select your **Product**.

3 Enter a unique **Session name** that does not exceed 64 characters.

   Session names **cannot include** any of these characters: \ / : * ? " < > ¦

4 Open the **Comments** option to enter a comment about this session. Comments are internal notes for the administrator that can be displayed in the **Manage Sessions** summary list.

5 Configure your **File Storage** preferences.

   - **Overwrite setting files**

     When selected, Management and Security Server compares the user's local settings with the web server version of the settings files. When they are different, the local file is overwritten.

     By overwriting existing settings files, you can easily distribute updates; however, the users' changes will be lost.

   - **Save settings files as read-only**

     The settings files can be saved as **Read-only** or **Hidden**. Users cannot change **Read-only** settings unless they have permissions to do so.

   - **Save settings files as hidden**

     Hidden files do not appear in the user's Windows Explorer unless the user configures Windows to show hidden files. You may need to clear **Enable Protected Mode** in the workstation's browser settings.

   - **For sessions to be launched from an end user's Assigned Sessions list**, choose where you want the settings files to be stored on the user's workstation.

     — **My Documents\<product folder>**

     — **Temp**

     — your specified **<User profile folder>**

6 Click **LAUNCH** to open the session and configure your preferences and other settings. If you see a **Launch Application** dialog asking to use **Zulu Platform x64 Architecture**, your client is already configured with **MSS Client Launcher**. If you don't see anything or are asked to select an application, MSS Client Launcher is probably missing and subsequent steps should be followed. See Using the MSS Client Launcher.

NOTE: *If the* **LAUNCH** *button is disabled:*

1. Be sure the product (for the session you want to launch) is activated.
   Open **Configure Settings - Product Activation** in the Administrative Console.
2. If your product is not in the list, click **ACTIVATE NEW**.
3. Browse to the activation file for the product for which you are creating a session. The file is in this format: `activation.<product_name-version>.jaw`.
4. Click the file, and the product is added to the Product list.
5. Restart your browser to ensure that the Administrative Console is fully updated with the new set of activation files. You do not need to restart the MSS server.
6. Continue to **ADD** and then **LAUNCH** your session.

Using the MSS Client Launcher

Administrators can use the **MSS Client Launcher** with *any browser* to launch and configure **Reflection/InfoConnect Desktop** sessions. When **Centralized Management** is enabled in the Reflection or InfoConnect Desktop client, end users' sessions may be launched from the Assigned Sessions list.

The administrator can install the MSS Client Launcher either *before* launching a session or *when* the first session is launched.

- "About the MSS Client Launcher" on page 13
- "Installing the MSS Client Launcher" on page 14
- "Launching sessions with the MSS Client Launcher" on page 15

About the MSS Client Launcher

The MSS Client Launcher is a standalone application used to configure **Reflection/InfoConnect Desktop sessions** from the **MSS Administrative Console**. The Launcher replaces the Java applet-based tool used in previous versions of MSS.

The MSS Client Launcher must be installed on the administrator's workstation. The MSS administrator can use *any supported browser*, such as Mozilla Firefox, Google Chrome, or Microsoft Edge, to configure Reflection/InfoConnect Desktop sessions.

Note: Administrator permissions are required to install the MSS Client Launcher on the desktop machine because the MSS Client Launcher installs to the `C:\Program Files` directory by default. Once installed, the MSS Client Launcher can be used by all users of that machine. (Log files are created in a per-user writable location.)

Installing the MSS Client Launcher

The MSS Client Launcher must be installed on the administrator's workstation before you can launch and configure a Reflection or InfoConnect Desktop session.

To install the MSS Client Launcher, you need administrative permissions. You can either:

◆ Install the MSS Client Launcher *before launching a session*

or

◆ Follow the MSS Administrative Console prompts *when you launch a session*

Install the MSS Client Launcher before launching a session

You can prepare your local administrator machine with the MSS Client Launcher before you begin configuring a Desktop session.

Keep in mind: You, the administrator, will first need to know where to find the MSS Client Launcher installer (`.msi`) file. Then, after the Launcher is installed, you can immediately begin to configure a session after launching it.

On the administrator machine:

1 Copy the `client-launcher-installer.msi` from the MSS server installation, `<install_dir>/Micro Focus/MSS/server/installers` to a location on your local administrator machine.

2 Run the installer with administrative permissions to install the MSS Client Launcher.

3 After the MSS Client Launcher is installed, proceed as you would to launch and configure a new or existing Desktop session.

Follow the MSS Administrative Console prompts when you launch a session

Or, you can download and install the MSS Client Launcher *when* you launch a new or existing **Reflection** or **InfoConnect Desktop** session, provided you have sufficient Windows administrator permissions.

Keep in mind: Until the MSS Client Launcher is installed, the flow of launching a Desktop session is interrupted by the dialog prompts to download and run the MSS Client Launcher installer (`.msi`) file. Then, after the Launcher is installed, you need to re-launch the session you want to configure.

NOTE: The dialog buttons and text vary, depending on the browser being used. The dialog text from *Mozilla Firefox* is included as an example.

In the MSS Administrative Console:

1 In **Manage Sessions**, either click **+ADD** or click an existing **Reflection/InfoConnect Desktop** session.

2 Click **LAUNCH**.

When the MSS Client Launcher *is not installed*, a dialog may ask you to identify an application to use to launch the session. In some browsers, no dialog appears at all.

3 If a dialog asks you to select an application because the MSS Client Launcher *is not installed*, click **CANCEL**.

4 On the **Launching Session** panel, click **DOWNLOAD**.

5 Then, click **Save File** to save `client-launcher-installer.msi`, which contains the MSS Client Launcher.

6 Click **Run** and proceed through the **MSS Client Launcher Installer Setup Wizard**, accepting or modifying the defaults.

Note: You must have administrative permissions to install the Launcher locally.

7 After the MSS Client Launcher is installed, return to **Manage Sessions**.

Launching sessions with the MSS Client Launcher

When the MSS Client Launcher is installed, the flow of launching and then configuring a Desktop session is continuous.

Note: The dialog buttons and text vary, depending on the browser being used.

1 On the Manage Sessions panel, either click **+ADD** or click an existing Reflection/InfoConnect Desktop session.

A dialog asks if you want to open the link using **Zulu Platform x64 Architecture**.

2 Click **Open link** or **Allow** (or other label), depending on your browser.

3 The Desktop session launches in a separate window and is ready to be configured.

4 See After the session is launched.

Related topics

- After the session is launched
- Assign Access
- Authentication & Authorization

Reflection/InfoConnect Desktop - Workspace Automated Sign-on

Use this session type to enable automated logons to a mainframe from managed desktop sessions running **Reflection or InfoConnect Workspace**.

Note: Automated Sign-on for Mainframe is an add-on product to Management and Security Server and requires a separate license. It may take some time to perform the prerequisite steps.

To add and configure a Workspace Automated Sign-on (ASM) session:

- Complete the prerequisites
- Add and Configure the Workspace Automated Sign-on (ASM) session
- Assign Access to a Workspace Automated Sign-on session

Complete the prerequisites

The prerequisite actions require configuration in Management and Security Server, in the terminal client, and on your z/OS.

End-user tasks:

- Configure their Desktop client for **Centralized Management**.
- Check the **Enable automated sign-on for mainframes** option.

See Step 6 in Automated Sign-on for Mainframe - Administrator Guide.

Administrator tasks:

See the Configuration Workflow in the *Automated Sign-on for Mainframe - Administrator Guide* to see the list of tasks and to get an idea of how much time to allot.

1 Configure the Automated Sign-On for Mainframe settings to secure the server connections and manage user access. And, the mainframe needs to be configured to support PassTickets.

2 In **Reflection/InfoConnect Workspace**, create a 3270 session that includes an **ASM login macro**. Detailed steps are included in your Reflection/InfoConnect documentation.

IMPORTANT: Note the *exact host name* to which the client is connecting. This name will become the Workspace Automated Sign-on session name.

---

3 Save the session in a location that can be accessed by Management and Security Server.

4 Proceed with the Add and Configure the Workspace Automated Sign-on (ASM) session settings in Management and Security Server.

Add and Configure the Workspace Automated Sign-on (ASM) session

Open or return to Management and Security Server - Administrative Console.

1 Open **Manage Sessions**, and click **+ ADD**.

2 Under **Product**, select **Reflection/InfoConnect Desktop**.

3 Under **Session type**, select **Workspace Automated Sign-on**.

4 In the **Session name** field, enter the *exact name* of the host to which the client will connect.

The session name *must exactly match* the host name (mentioned in the prerequisites). Proper naming of the Workspace Automated Sign-on session is critical.

If you are not sure, enter any session name now, and edit it before testing the connection.

NOTE: Host name variations. If clients connect to different variations of the host name, or if they connect to the host by its IP address, *each of those variations* needs its own *Workspace ASM session with a matching name*.

For example, if the session is being configured to automatically log on to `blue.mycompany.com`, then the session name must be `blue.mycompany.com` — not `blue`, or `123.456.78.90`, or another variation.

To enable sessions to automatically log on to a different host name, you must create separate sessions for EACH name.

---

5 Scroll to the **Workspace Automated Sign-on Settings File** section.

Click **BROWSE.**

6 Browse to and select the Reflection/InfoConnect Workspace session (`*.rd3x`) that contains the **ASM login macro**, created earlier (Complete the prerequisites - step 2).

7 Click **SAVE** to upload the settings file and save the session.

Workspace Automated Sign-on sessions are configured manually in the Administrative Console by uploading an appropriate settings file to the MSS server.

The Workspace Automated Sign-on session ⚸🌐 is available to be assigned.

Assign Access to a Workspace Automated Sign-on session

When you are ready to assign users to be able to log on automatically to the mainframe session, refer to **Assign Access** - Search & Assign.

In particular, note the required **EDIT** option used to select a method to obtain the mainframe user name.

When a Workspace Automated Sign-on session is assigned to that user, the session's macro is loaded and run automatically based on a specific naming convention required by the Workspace Automated Sign-on session.

REMINDER: To use a Workspace Automated Sign-on session, the end user must have their Desktop client configured for **Centralized Management** and the **Enable automated sign-on for mainframes** option checked.

Related topics

- Assign Access
- Automated Sign-On for Mainframe

Reflection for the Web

To add, configure, launch, and deploy a Reflection for the Web session:

- Add a session and configure settings in MSS
- Launch Reflection for the Web
- Configure the launched session
- Assign the session in MSS
- Distribute the Reflection for the Web Launcher to client workstations

Add a session and configure settings in MSS

Add your Reflection for the Web session and configure these settings in MSS before you launch the session and configure your preferences.

To add and configure a Reflection for the Web session:

1 Open **Manage Sessions**, and click **+ ADD**.

2 Under **Product**, select **Reflection for the Web**.

3 Select a **Session type**, such as IBM 3270.

4 Enter a unique **Session name** that does not exceed 64 characters.

   Session names **cannot include** any of these characters: \ / : * ? " < > ¦

5 Open the **Comments** option to enter a comment about this session. Comments are internal notes for the administrator that can be displayed in the **Manage Sessions** summary list.

6 Use the additional settings to customize the display and behavior of your Reflection for the Web session:

   Appearance | FTP | Advanced Settings | Applet Parameters

7 When you are finished with these initial settings, Launch Reflection for the Web to configure further session details.

Appearance

 ◆ **Window title**. You can change the title bar for the session with special characters.

   The title can include these special characters.

Character	Value
&&	a single ampersand
&c	Connection Status (whether you are connected and over what transport)
&d	Date
&h	Host name
&s	Session type
&t	Transport
&v	Terminal session identifier that uniquely identifies this terminal session from others. See specific types:
&v for IBM 3270 and IMB 3270 Printer sessions	LU name
&v for IBM 5250 and IBM 5250 Printer sessions	Device name
&v for ALC. UTS Terminal, T27, T27 Printer, and Airlines Printer sessions	Terminal ID

FTP

Select **Enable FTP within this session** when you want to include FTP as an option on the **File** menu for IBM 3270, IBM 5250, HP, VT, or UTS terminal emulation sessions. When enabled, users can open a window that allows them to easily transfer files using FTP.

Show FTP Window as

When you configure a standalone FTP session, use these options to specify the appearance of the FTP window.

- Select **Local/remote lists and console** to display lists of files and directories (local and server) are displayed in the top of the FTP window, and an FTP console with a command line is displayed in the bottom.

- Users can change the FTP window appearance after the session is started by using buttons on the FTP button bar. However, when either **Lists only** or **Console only** is selected, users cannot change the FTP window appearance.

Advanced Settings

See: Advanced—More Settings | Applet Parameters

Advanced—More Settings

Click **Advanced**, and use these settings to customize how the session is displayed, launched, and delivered.

- Window Size and Status Bar
- View Session HTML

Window Size and Status Bar

- **Use best dimensions for each user**

  Based upon the client machine's screen resolution, Management and Security Server is able to determine the best width and height for each user's session window. This setting applies only when the session is displayed in its own window.

- **Use maximized dimensions**

  The session will be in a full screen display. This setting applies only when the session is displayed in its own window.

- **Use these window dimensions**

  The **Width** and **Height** options determine the dimensions of the applet (in pixels).

- **Display status bar**

  This option controls whether the status bar appears in the terminal window. The status bar appears at the bottom of the window and includes information such as the cursor position, whether the connection is encrypted, and the type and status of the connection.

View Session HTML

The session HTML is automatically generated by the Management and Security Server. The Reflection for the Web session HTML is displayed for the special case where the static HTML must be saved in a file.

Copy the HTML into a text editor. Save the file in `MSSData/deploy` as an `HTML` file. After you make changes to the session settings, click **REFRESH HTML** and re-save the file. As noted in `MSSData/deploy/deploy.txt`, you can also save the session's configuration file.

When the `<session>.html` is saved, the session can be assigned to users via **Assign Access**. The session will appear in the user's list of entitled sessions with a different icon, but it *does not appear* in the administrator's **Manage Sessions** list (in the Administrative Console).

See Knowledge Base article 7022329 for more information.

Applet Parameters

You can customize the properties of a Reflection for the Web session by adding applet parameters. (You may need to scroll to the **Applet Parameters** button.)

Applet parameters modify the behavior of the basic session. When you launch a session and change its settings, the new settings are saved in a configuration file. Applet parameters allow you to extend functionality beyond the configuration file.

Refer to Applet Attributes and Parameters in the *Reflection for the Web Reference Guide* for descriptions and valid values of the standard applet parameters

To add a parameter

1 Click **+ADD**.

2 From the **Parameter** drop-down list, select a standard parameter, or click **<Custom>** to add a new one.

3 Enter a **Value**, if required.

4 Click **ADD**. The parameter is added to the table.

NOTE: Not all parameters are valid for all session types. To check whether a parameter applies to your session, refer to Applet Attributes and Parameters in the *Reflection for the Web Reference Guide*.

List of current parameters

The applet parameters that are currently assigned to this session are listed in the table. To remove a parameter, check it, and click **REMOVE**.

Launch Reflection for the Web

The **Reflection for the Web Launcher** must be installed on the administrator's workstation before you can launch and configure a Reflection for the Web session.

For more information about the Reflection for the Web Launcher, see Reflection for the Web Installation Guide.

- **When RWeb Launcher is *not* installed**, the session does not launch.

  Click **DOWNLOAD** to download `RWebLauncher.msi` and install the Reflection for the Web Launcher.

- **When RWebLauncher *is* installed**, you see the option to open the session using **Zulu Platform x32 Architecture**. This OpenJDK option requires no Java plug-in.

  Click **Open link** to launch the session.

Next step: Configure the launched session

Configure the launched session

After you launch your Reflection for the Web session, configure your session settings, such as Profiling. Open the Reflection for the Web product Help for assistance.

When you click **Save** or **Exit/Save,** the settings are exported to Management and Security Server, and the session is added to the **Manage Sessions** list.

NOTE: To set up **Metering**, you need to configure both the server and the client. See Metering for details.

Next step: Assign the session in MSS

Assign the session in MSS

In the **MSS Administrative Console**, click **Assign Access**.

If LDAP authorization is enabled, you can search for a particular user or group. Select a user or group and check the session(s) you want to assign.

For assistance, see Assign Access.

Next step: Distribute the Reflection for the Web Launcher to client workstations

Distribute the Reflection for the Web Launcher to client workstations

Now that the Reflection for the Web Launcher is installed on the administrator's workstation, and at least one session is configured and assigned, the Reflection for the Web Launcher Installer needs to be distributed to users' workstations.

The users need the Launcher to launch their list of assigned Reflection for the Web sessions.

See the Reflection for the Web Installation Guide for deployment options.

Related topics

- Assign Access
- Authentication & Authorization
- Manage saved sessions
- Export a Reflection for the Web session

Rumba+ Desktop

To add and configure a Rumba+ Desktop session:

- Complete the prerequisites
- Upload the Rumba+ Session Profile
- Edit a configured Rumba+ session

Complete the prerequisites

These tasks must be completed in your Rumba+ application before the session can be managed by Management and Security Server.

- configure a session in your Rumba+ application
- save the session profile
- enable **Centralized Management** in **Rumba+ Options**.

Next, you must upload and attach your Rumba+ session profile to the session you are configuring in Management and Security Server.

Upload the Rumba+ Session Profile

1 Open **Manage Sessions**, and click **+ ADD**.

2 Under **Product**, select **Rumba+ Desktop**.

3 In Management and Security Server (after you add a session and enter a **Session name**), click **BROWSE.**

4 Navigate to and select the Rumba+ session profile (saved by your Rumba+ application).

   The profile name displays below the **BROWSE** button.

5 **Overwrite settings files** is not checked by default, which means that users can set local preferences in their launched sessions and open sessions using their local settings file. These sessions are **not updated** from the Management and Security Server settings file.

   However, if you want Management and Security Server to compare the local and web server versions of the settings file and **overwrite the user's file**, then check **Overwrite settings files**.

   Note: This setting allows you to easily distribute updates to existing settings files, but changes that users made to their settings will be lost.

6 If entitled to the **Security Proxy Add-On**, you can configure the Rumba+ session to connect through a Security Proxy server that has client authorization enabled.

The **Security Proxy Settings** require one setting in the Rumba+ session (configured separately using the Rumba+ client), and one setting on this Configure Session panel.

   6a In the Rumba+ session, set the host name and port to the address of the Security Proxy server.

   6b On this **Configure Session** panel, check the **Use security proxy server** box.

      Enter the host name and port to which the Security Proxy will forward the connection.

7 Click **SAVE**. The profile is then uploaded and attached to the session.

After the Rumba+ session profile is uploaded, users can open their assigned Rumba+ sessions from the Windows **Start** menu, as usual. The first time the session is launched, the settings file is downloaded from Management and Security Server to the client computer.

Next step: Use Assign Access to make the session available to end users.

NOTE: Rumba+ sessions are not available as direct URLs. Instead, Rumba+ sessions are launched from the Windows **Start** menu, and the session profiles are obtained from MSS when **Centralized Management** is configured in Rumba+.

Edit a configured Rumba+ session

1 Using your Rumba+ application, open the appropriate session profile, and make the changes. Save the profile.

2 In Management and Security Server, open **Manage Sessions**, and click the session name.

3 Click **BROWSE** and select the Rumba+ session profile that you just edited and saved.

4 Click **SAVE** to upload and attach the updated profile.

Related topics

- Assign Access
- Using the Security Proxy Server

After the session is launched

1 Configure your settings and **Save** the session.

The settings are sent to Management and Security Server, and the saved session is added to the list on the **Manage Sessions** home panel.

In the list of sessions, use the column chooser ▥ to show or hide the session properties: Type, Name, Description, Direct Link, your Comments, and Security Status.

2 *Optional.* If you are entitled, the launched session can be configured to connect through the Security Proxy. For details, see Using the Security Proxy Server.

3 As a next step, you can

- Use Assign Access to make the session available to end users.
- Return to Manage Sessions to add or edit a session.

Manage saved sessions

You can edit, copy, or delete any session in the **Manage Sessions** list. The export option is exclusive to exporting a Reflection for the Web session to Host Access for the Cloud.

Edit a session | Copy a session | Delete a session | Export a Reflection for the Web session

Edit a session

1 In **Manage Sessions**, click the session you want to edit. Or, check the box, and then click **EDIT**.

2 Note the **Properties**, which are not editable.

3 Change the settings you wish to edit. (Details are described in Add and Launch a session.)

4 Click **SAVE**, or **LAUNCH** the session.

NOTE: If an administrator is editing a session, and a second administrator attempts to open the same session, a message displays to notify the second admin that the session is locked and changes cannot be saved.

Copy a session

To add a new session with the same properties:

1. In **Manage Sessions**, right-click the session you want to copy. (Or, check the box and click **COPY**.)

2. Enter a **Name** for the copied session. Click **OK**.

The session is saved with identical properties and added to the **Manage Sessions** list.

Delete a session

Right-click the session or session you want to delete. To delete multiple sessions, check the boxes and click **DELETE**.

The deleted sessions are removed from the list.

Export a Reflection for the Web session

The **Manage Sessions** list provides the **EXPORT** option to save a Reflection for the Web session as a Host Access for the Cloud session type. After the Host Access for the Cloud session is created, the original Reflection for the Web session remains unchanged in the **Manage Sessions** list.

On the **Manage Sessions** panel:

1 Locate the Reflection for the Web session you want to save as a Host Access for the Cloud session type.

   TIP: Reflection for the Web session types are identified by a globe icon (denoting a web-based session), followed by the terminal type, such as 3270: 🌐 `3270`.

2 Right-click the session (or check the box) and click **EXPORT**.

3 On the **Export session** panel, enter the name for the new Host Access for the Cloud session, and the address of the Session Server that will host the session.

4 Click **CREATE**. The new session is added to the **Manage Sessions** list and can be assigned to users or groups. Note that the icon changed to the Host Access for the Cloud session type: ☁

The original Reflection for the Web session is unchanged and remains available in the session list.

Related Topics

- Authentication & Authorization
- Assign Access
- Add and Launch a session

3 Manage Packages

The **Manage Packages** feature is available with Micro Focus Windows-based emulator clients, such as Reflection Desktop or InfoConnect Desktop.

Use **Manage Packages** to deploy configuration data to specified users. You can manage the macros and settings installed on each user's machine by uploading .msi files. Packages are available only with Windows-based clients.

The available packages are listed on this panel.

 ◆ "Configure a Package" on page 27
 ◆ "Upload or Update a Package" on page 27

Configure a Package

To use this feature, you must first create an `.msi` file that packages the files you want to deploy.

For example: with Reflection Desktop, use the **Installation Customization Tool** to package the files. Refer to the product documentation for information about which files you can include and how to use the tool.

Related Topics

 ◆ Upload or Update a Package

Upload or Update a Package

You can add a new package or update an existing one.

To upload a new package:

1 Click **+ ADD**, and then **BROWSE** to the `.msi` file you want to upload.

2 Add a **Description** for your reference.

NOTE: If you cluster an MSS server that contains packages for Windows-based sessions, the assignments and settings are replicated automatically. However, the **package data must be manually copied** to each server. See Clustering.

To update an existing package:

1 Check the package you want to update and click **EDIT**.

2 **BROWSE** to the newer version of the file. The file name must be the same.

 The new configuration information is deployed to a user workstation when the user logs on.

To delete a package:

Check the package, and click DELETE.

Next steps:

After you upload a package, use **Assign Access** to associate the package with a user.

When a user logs on or launches a session from a direct URL, the `.msi` file contents will be installed on the user's machine.

Related Topics

- Search & Assign
- Manage Sessions

4 Assign Access

Use **Assign Access** to provide user access to one or more sessions or packages.

The ability to assign sessions or packages to a specific user or group of users is dependent on whether LDAP authorization is enabled. To enable and configure your LDAP server, open Authentication & Authorization, and click **Use LDAP to restrict access to sessions**.

- ◆ "Search & Assign" on page 29
- ◆ "Currently Assigned" on page 32
- ◆ "Providing Access to Assigned Sessions" on page 32

Search & Assign

With LDAP authorization enabled, you can assign sessions and packages to an individual user, a group of users, or a specific folder in your LDAP directory.

When multiple LDAP servers are configured, search for users or groups within a domain.

- ◆ "Search for Users or Groups/Folders" on page 29
- ◆ "Assign Sessions or Packages" on page 30

Search for Users or Groups/Folders

Determine who should have access.

1 Verify or select the **Domain**.

   To assign sessions or packages to **All users within the selected domain**, keep that Search result selected, and skip to step 5.

2 When LDAP authorization is enabled, you can search for and assign access to specific **Users**, **Groups**, or **Folders** in that domain. When LDAP authorization is *not* enabled, access to sessions or packages can be assigned only to **All Users**.

   > **NOTE:** The **Search by** options are based on the LDAP server configuration (Search Base and Groups/Folders). You will see either **Users | Groups** OR **Users | Folders**.

   To search, select a **Search by** option, enter a name, or enter the asterisk (*) wildcard or a combination of * and letters in the text box.

3 Click **SELECT ATTRIBUTES** or add **CUSTOM ATTRIBUTES** to narrow your search using the available filters. Click **SEARCH**.

4 In the **Search Results** find and click the name of the user, group, or folder.

   Click **Details** to see this user or group's attributes and the groups from which they can inherit access. A group's Details also includes the members of that group.

Or, click **SEARCH AGAIN** to change the search attributes or to search for another user.

5 For the selected user or group of users, continue with Assign Sessions or Packages.

Related Topics

- Assign Sessions or Packages

Assign Sessions or Packages

Determine which sessions or packages this user or group is entitled to access.

1 Check the Sessions or Packages you want to make available to the selected user or group.

NOTE: You can assign access by inheritance. See these examples.

- An asterisk (*****) next to the Session name denotes that a user has inherited access to that session by being a member in a group.

  For example: JohnUser is a member of Group A. If you assign Session1 to Group A, then JohnUser inherits access to Session1. When viewing JohnUser's assigned sessions, an asterisk appears next to Session1.

  To remove a user's access to an inherited session, click the User, and clear the **Allow user to inherit (*) access to sessions** check box (below the list of sessions).

- Granting access to **All users** means granting access to the search base, and every user inherits that access. Such access is extended to individual users only when the **Allow user to inherit (*) access to sessions** option is checked.

- Sessions cannot be assigned to Active Directory primary groups (such as Domain users).

---

2 Select or clear the option to **Allow access to Administrative Console**.

When checked, the selected user or group has access to the MSS Administrative Console.

3 The **EDIT** option is used for **Automated Sign-on to a Mainframe**, including Reflection/ InfoConnect Desktop - **Workspace Automated Sign-on** sessions.

4 To assign an automated sign-on session, click **EDIT**. Then continue with Select the source of the mainframe user name.

5 Click **APPLY** to save your assigned sessions.

6 Repeat the steps to Search & Assign sessions to a different user or group.

Related Topics

- Search for Users or Groups/Folders
- Select the source of the mainframe user name

Select the source of the mainframe user name

In the list of available sessions to assign, the **EDIT** option displays when **Automated Sign-On for Mainframe** is activated.

NOTE: To recap, the configuration of **Automated Sign-On for the Mainframe** requires:

- The Automated Sign-On for Mainframe Add-On product is installed and configured on the Host Access Management and Security Server.
- A session to the mainframe was created with a log-in macro detailed in the Automated Sign-on for Mainframe - Administrator Guide.
- The session is assigned to the appropriate user or group. (The session cannot be inherited.)
- The method for obtaining the mainframe user name is selected (after you click **EDIT**).

When you click EDIT to assign a session

(continuing from Assign Sessions step 3)

1 When you click **EDIT**, the **Source of mainframe user name** panel opens, which identifies the selected user and the session that you want them to automatically log on to.

2 Choose the method to **derive the mainframe user name**:

- **Not set**

  This default must be changed for automated sign-on.

- **UPN**

  Select this option to request a PassTicket from DCAS by deriving the mainframe user name from the User Principal Name (UPN) of the user. The UPN is typically available from a smart card or client certificate, and is a standard attribute in Active Directory servers.

  A UPN is formatted as an internet-style email address, such as `userid@domain.com`, and Management and Security Server derives the mainframe user name as the short name preceding the '@' symbol.

- **LDAP attribute value in the authenticating directory**

  Select this option to perform a lookup in the LDAP directory (defined in Authentication & Authorization) and return the value of the entered attribute as the mainframe user name.

  Enter the LDAP attribute. *Note:* All LDAP attributes must meet these criteria:

  — must begin with an alpha character

  — no more than 50 characters

  — any alphanumeric character or a hyphen is permitted

- **LDAP attribute value in a secondary directory**

  When using a secondary LDAP directory, you can use this search filter to find the user object in the secondary LDAP directory. The value is returned as the mainframe user name.

  Note the criteria for LDAP attributes, listed above.

- **Literal value**

  This option is available for sessions assigned to users, but not groups. This method is typically used for testing, not for production.

Enter a value that meets these criteria:

— up to eight alphanumeric characters

— no spaces

— no other characters

3 If you configured multiple DCAS servers, select the one to use for this automated sign-on session.

An asterisk (*) appears next to your preferred DCAS server; however, you can select a different one.

4 Click **OK**.

Related Topics

◆ Search & Assign

◆ Assign Sessions or Packages

◆ Currently Assigned

Currently Assigned

The **Currently Assigned** view lists all of the users and groups who have been assigned one or more sessions or packages.

Click a user or group in the Search Results. Their assigned sessions are checked.

Providing Access to Assigned Sessions

The **Assigned Sessions** list is an HTML portal that provides users with the ability to launch the sessions that have been assigned to them.

After a user authenticates to the MSS server, they see their list of entitled sessions. The list is available at

```
https://<mssserver>/sessions/
```

Requirements: Sessions from the following products may be launched from the **Assigned Sessions** list:

◆ **Host Access for the Cloud** (2.6 or higher)

HACloud users can also access their assigned sessions by logging in to the HACloud session server directly.

◆ **Reflection Desktop** (17.0 or higher)

Reflection Desktop users can access their assigned sessions when Desktop is configured for centralized management.

◆ **InfoConnect Desktop** (17.0 or higher)

InfoConnect Desktop users can access their assigned sessions when Desktop is configured for centralized management.

◆ **Reflection for the Web** (13.2 or higher)

Note: Please see important notes regarding load balancer configuration when using a load balancer in front of the Assigned Session list. See Using a Load Balancer.

Related Topics

- Search & Assign
- Manage Sessions
- Authentication & Authorization

5 Configure Settings

Use these settings to enable features in Management and Security Server.

- General Settings
- General Security
- Secure Shell
- Certificates
- Trusted Certificates
- Credential Store (Reflection for the Web)
- Security Proxy Server
- Authentication & Authorization
- Product Activation
- Automated Sign-On for Mainframe
- Metering
- Terminal ID Manager
- Clustering
- Logging

General Settings

Configure these settings for using Management and Security Server.

- Set VPA number
- Set server name

Set VPA number

The volume purchase agreement (VPA) number appears in the client's **About** box and is used by the Metering server. If the VPA is unspecified, it is reported as 00000 in the emulator and in metering reports.

If you did not enter your number during installation, you can add it here.

Set server name

You can enter up to 45 characters to identify this MSS Administrative Server. This name is helpful for debugging in larger environments where more than one MSS Administrative Server is in a cluster or behind a load balancer. In these cases, it can be difficult for the client to determine which MSS Administrative Server is being accessed.

This string is printed in the console.

General Security

The General Security panel prompts you to set (or change) passwords, configure smart card settings, and set other security options.

- Server access protocol
- Restrict administrator account
- Change administrator password
- Require new login
- Smart card settings
- Certificate chooser prompt
- Enable identity verification
- Change keystore password
- PKI Server
- Keychain

Server access protocol

By default, Management and Security Server allows browsers to use the HTTPS protocol to communicate between the client computer and the Management and Security Server.

Use the **HTTPS Certificate Utility** to manage the Administrative Server certificate. The HTTPS Certificate Utility installs with Management and Security Server, and is available from the Start menu.

Related Topics

- Smart card settings
- General Security

Restrict administrator account

Use these settings to limit access to the Management and Security Server administrator account.

IP range

Enter a range of IP addresses -- either IPv4 or IPv6 -- for devices that are allowed to log in as administrator. IP addresses outside this range will be rejected even if the correct password is entered.

Note: If the designated machines have multiple IP addresses, enter all of the possible IP addresses that the client might send.

You can use an asterisk (*) as a wild card in any part of the IP address. Use a single * (the default) to allow anyone with the password to log in as administrator. To restrict access, you must include * or a number in each section of the address.

Use a hyphen (-) to indicate an inclusive range of addresses and a comma (,) to list individual addresses. Examples:

This entry...	allows access from...
*	all IP addresses
123.*.*.*	all IP addresses that begin with 123
123.123.4.5 - 123.123.4.7	only 123.123.4.5, 123.123.4.6, and 123.123.4.7
123.*.*.*, 246.246.0.1	all IP addresses that begin with 123 and from 246.246.0.1
123.123.4.5	only the given IP address

Maximum allowed attempts before lockout

After a user has attempted to log into the administrator account the specified number of times without providing the correct password, the user is locked out. This feature helps to guard against brute force attacks.

A zero (0) here or in the following field disables the lockout feature. This is the default.

Lockout duration (seconds)

This field specifies the length of time a user remains locked out after the specified number of failed login attempts. This feature helps to guard against brute force attacks.

A zero (0) here or in the preceding field disables the lockout feature. This is the default.

Related topics

- General Security

Change administrator password

Each time you log on to Management and Security Server as an administrator, you enter a password, which opens the **Administrative Console**:

`<hostname>/adminconsole`

To change the administrative password, you can either

- use the Administrative Console (**Configure Settings - General Security**).
- run the **Password Change Utility**.

Running the Password Change Utility

The password change utility allows you to re-set the administrative password without needing to log in to the Administrative Server.

To change the password:

1 Choose an option to run the installed `PasswordChangeUtility`.
- **On Windows:** Run the utility from the install location:

  `[MssServerInstall] ...\MSS\utilities\bin\PasswordChangeUtility.exe`
- **On UNIX or Linux:** Run the utility from

  `… /mss/utilities/bin/PasswordChangeUtility`
- **On a command line:** run the utility in command line mode `(-c)`.

2 Follow the prompts to change and save the password.
3 Restart the MSS Server.

Related topics

- General Security

Require new login

Set the time when the administrator must log in (again).

Require a new login to the server after an inactive period (minutes)

Management and Security Server times out when a user has not launched a session or otherwise interacted with the Administrative Server during the specified time. The user must log in again to open a new host session or access the Administrative Console. Host sessions that are already open are not affected.

NOTE: When you are configuring sessions and settings, you may want to lengthen the timeout period to avoid disruption. Then, reset the time when you're done.

Require new login for each host session launched by a user

When LDAP authentication is in effect, you can require users to log in to the Administrative Server each time they launch a session. This option does not apply when the user is logged in as administrator.

Related topics

◆ General Security

Smart card settings

Smart cards store digital certificates that can be used to validate (authenticate) a user's identity to the network. Digital certificates are used in X.509 systems, and are part of an organization's public key infrastructure (PKI). Smart card support is available only on Windows platforms.

The default setting

Management and Security Server's default smart card parameter specifies the provider, sunpkcs11, and the associated certificate attributes.

If you use a different provider, enter the smart card provider along with certificate attributes to identify valid certificates on the user's smart card. For details and examples, see About smart card parameters.

Smart card libraries

Applies to: Reflection for the Web.

Smart card libraries are required when using `sunpkcs11` to access smart cards. (MSCAPI uses DLLs that ship with Windows, and the provider DLLs do not need to be specified in this field.)

SunPKCS11 requires one or more libraries, such as ActivClient. Noting the library examples provided in Management and Security Server, you could use `acpkcs211` instead of `acpkcs`, and `acpkcs211.dll` instead of `acpkcs201.dll`. Separate the library names with commas.

Note: When using ActivClient7 with Management and Security Server, you must include the full Windows short (MS-DOS) path to the dll. For example, the short path on a Windows x64 system would be `C:\PROGRA~2\ActivIdentity\ActivClient\acpkcs211.dll`

Paths on a Windows machine can use either forward slash (`/`) or backward slash (`\`) file designations.

About smart card parameters

Applies to: Reflection Desktop (for Centralized Management) and Reflection for the Web

Smart card parameters can be used as filters to identify valid certificates on a user's smart card.

The smart card setting in Management and Security Server includes the smart card provider and certificate attributes as a filter to select a valid identity certificate.

Smart Card Provider

The first part of the parameter identifies the software provider that Management and Security Server should use to access the smart card certificate reader on the client machine.

In the default parameter, sunpkcs11 (Public-Key Cryptography Standard) is the intended software provider. Another valid provider is MSCAPI (Microsoft CryptoAPI, native to Windows).

If you use a smart card provider other than sunpkcs11, enter the provider followed by the desired certificate attributes. A colon (:) is required to separate the provider from the filter when multiple masks are used (See Certificate Attributes).

Certificate Attributes

The next part of the default parameter is made up of two filters, separated by a semi-colon (;). Each filter consists of Object-ID (OID) masks that specify certificate attributes. The masks specify which certificate attributes (encoded tokens) MUST (+) or MUST NOT (-) be on the certificate before it can be used for login or client authentication.

The default parameter specifies these attributes:

```
KU+DIGSIG,KU-NONREP,EKU+CLIAUTH,EKU+SCLOGIN,EKU-EMLPROT;
KU+DIGSIG,KU+NONREP,EKU-NONE.
```

The first filter uses the following logic for each attribute to be TRUE. When all attributes are TRUE, the certificate is valid and can be used for authentication.

- `KU+DIGSIG`: Key Usage of Digital Signature OID MUST be present in the certificate.
- `KU-NONREP`: Key Usage of Nonrepudiation OID MUST NOT be present in the certificate.
- `EKU+CLIAUTH`: Extended Key Usage of Client Authentication OID MUST be present in the certificate.
- `EKU+SCLOGIN`: Extended Key Usage of Smart Card Login OID MUST be present in the certificate.
- `EKU-EMLPROT`: Extended Key Usage of Email Protection (called Secure Email) OID MUST NOT be present in the certificate.

If any attribute in the first filter is FALSE, the second filter is used. The second filter in the default parameter uses this logic for each attribute to be TRUE:

- `KU+DIGSIG`: Key Usage of Digital Signature OID MUST be present in the certificate.
- `KU+NONREP`: Key Usage of Nonrepudiation OID MUST be present in the certificate.
- `EKU-NONE`: Extended Key Usage MUST NOT be present in the certificate.

Certificate chooser prompt

After a user inserts a smart card and enters the Personal Identification Number (PIN), a list of certificates displays. Use this setting to select how the user is prompted to choose a certificate.

Show certificate prompt

This default option requires the user to choose the correct certificate each time they log on. In the displayed list, the **Type** column can help to identify the proper certificate.

Show certificate prompt and allow user to save selection

This option allows the user to save the certificate selection. When the user chooses to save the selection, the cached certificate is used for this connection and the user will not be prompted to choose the certificate on subsequent logons.

Enable identity verification

When a Reflection for the Web session is set to use TLS to connect to the host or the Security Proxy Server, the emulator applet authenticates the server to which it is connecting using the host or security proxy certificate.

When **Enable server identity verification** is selected, the applet checks the common name on the certificate against the name of the host or server. You must ensure that the common name on the server certificate is the *same* as the name of the host or proxy server to which it has been issued.

When the client verification option is cleared, the applet verifies that the server has a trusted certificate, but does not check that the server presenting the certificate is actually the one to which the certificate was issued.

If the connection uses TLS, the common name on the server certificate must always match the host or security proxy server name, regardless of whether server identity verification is selected.

You can override this setting on a per session basis with the `serverIdentityOverride` applet parameter.

Related topics

◆ General Security

Change keystore password

You can set a password to protect keystores and private keys that are stored on the Management and Security Server. The password set here protects the keystores in the `MSSData/trustedcerts` folder, which includes:

◆ the Management and Security Server certificate and private key

◆ the client certificate and private key

◆ the imported certificates on the Terminal Emulator Client trusted certificate list, which are listed on the **Configure Settings - Trusted Certificates** panel

For details about the `trustedcerts` keystores and other credential stores in MSS, see the Technical Reference, **Credential stores used in MSS**.

To change the password for this keystore, enter the existing password and the new password. Click **APPLY**. If a keystore password has not been previously set, leave the **Existing password** field blank.

NOTE: This password does **not** protect:

◆ the trusted certificates from certificate authorities (CA) for the **Terminal Emulator Client** that are listed in the **Trusted Root Certificate Authorities** table on the **Configure Settings - Trusted Certificates** panel.

◆ the Management and Security Server Trusted Certificate list.

To change the password that protects these certificates, see Keystore Password for the Trusted Certificates List.

Keystore Password for the Trusted Certificates List

The Administrative Server uses the JVM (java virtual machine) default password, `changeit`, to protect the Administrative Server's trusted certificate list. The keystore for the Administrative Server trusted certificate list is stored within the `java.home` directory for the JVM that is installed with the Administrative Server.

The default location on a Windows platform is `C:\Program Files\Micro Focus\MSS\jre\jre\lib\security`. The keystore is stored in the `cacerts` file.

To change the password that protects the Administrative Server's trusted certificate list:

1 Open a **Command Prompt**. Change to the installation directory. On a Windows platform using the default installation, change to `C:\Program Files\Micro Focus\MSS\jre\jre\lib\security`. The `cacerts` file is in this directory.

2 Enter the following command:

```
..\..\keytool.exe -storepasswd -v -new new_pass -keystore cacerts
```

Where `new_pass` is your new password, and `cacerts` is the file in which the keystore is stored.

3 In the **Enter keystore password** prompt, type the current password, which by default is `changeit`, and press **Enter**.

The new password is saved to `cacerts`.

4 Use your new password (`new_pass` in this example) to import an untrusted certificate when configuring LDAP or to view and modify trusted certificates on the **Configure Settings - Trusted Certificates** panel.

Related topics

◆ General Security

PKI Server

You can use PKI Services Manager to validate client certificates used to authenticate to Management and Security Server.

NOTE: **PKI Services Manager** is available as a separate download from the same product download page as Host Access Management and Security Server.

Two options can be set on this panel to use PKI Server:

◆ **when the authentication method is X.509 with Fallback to LDAP authentication**

Check this box if you want PKI Services Manager to validate the certificates used to authenticate to Management and Security Server.

◆ **by the terminal emulation and file transfer clients**

Check this box if you want PKI Services Manager to validate the certificates used to authenticate the clients.

After the PKI Services Manager is installed and configured, enter:

◆ **PKI Server address**: the name or IP address of the computer running PKI Services Manager.

◆ **PKI Server port**: the PKI Services Manager port. (The default is 18081.)

Related topics

◆ General Security

Keychain

The passwords and passphrases (such as LDAP server passwords) used by the Management and Security Server are stored in an encrypted **keychain**. The keychain file is located in `MSSData/keychain.bcfks`.

At server startup, the keychain file is unlocked for use by the Management and Security Server.

If you wish to change the default keychain settings, be sure to read the CAUTIONS before you proceed.

◆ ☑ **Use a keychain password file to allow unattended server startup**.

Checked by default, this setting enables unattended startup of the Management and Security Server. The keychain password is written to the keychain password file, `MSSData/keychain.pwd`.

On subsequent server startup or restart, the keychain password is read from the keychain password file, and the keychain is unlocked without needing additional action by the administrator.

NOTE: The system administrator MUST restrict the file system permissions for the `keychain.bcfks` and `keychain.pwd` files to only Read/Write access by root and the process that runs the Management and Security Server. All other access to these files must be denied.

CAUTION: When this option is *not* checked, the keychain must be manually unlocked. The system administrator must run the **Keychain Utility** application, available from the **Start** menu, and enter the keychain password. (The **Keychain Utility** is installed with Management and Security Server.)

◆ **Keychain port for submitting the unlock password**

This setting defines the port number that the keychain service listens on. To change the default port (12797), enter a local port number from 1 to 65535. Or, enter `0` to allow a random port assignment.

When the keychain must be manually unlocked, this port is accessed by the **Keychain Utility.**

◆ To change the keychain password:

    1. Enter the **Existing password for unlocking the keychain file**.

       The default password is `changeit`.

    2. **Enter** and **Confirm** your new keychain password.

       The keychain password is case-sensitive.

CAUTION: When using *Clustering*, the keychain is replicated, but the **keychain password** is *not replicated*.

Each server in a cluster has its own password to encrypt/decrypt the keychain. Changing the keychain password on the MASTER server will *not change* the password on the other nodes in the cluster. As a result, the system administrator will need to keep track of each server's password.

If the administrator chooses to run in *attended* mode, where the **Keychain Utility** is used to specify the keychain password for the server during startup, the administrator will need to enter the unique password for *each server* on the cluster.

Secure Shell

Use the **Secure Shell** panel to manage the public and private keys needed for secure shell (SSH) connections.

Known Hosts List

The known hosts list contains the public keys of hosts that the terminal emulator can connect to using secure shell. When an SSH connection is negotiated, the client authenticates the host against a list of known hosts.

The known hosts list on the Management and Security Server can be used by all clients, similar to the default user key pair. The table displays the hosts that are known.

To add a host to the list of known hosts, import a file that contains the host's public key.

1 In the `/etc/ssh` directory, locate the file that contains the public key, such as `ssh_host_<algorithm>_key.pub`.

   The format of the file can be OpenSSH, Base64 encoded.DER, or .PFX.

2 Add hostname,ip if the file does not already contain that information.

   That is, be sure the file contains `hostname,ip algorithm key`. For example:

   ```
   mySSHhost,10.10.1.1 ssh-rsa
   AAAAB3NzaB1yc2EAAAABIwAAAIEA0WR3aIRtilXquUmXtxw5oi3rMkhY9jw/
   lV03WvUNvSb/xQnIfoMeserY5DfU8+eqUPzLX0efJMik22VFAzFo+ZCOnlHbj39yNi2a1/
   7dAJYECaHo7pxhILHAZxXbwOpWSms3aaccWOOEA+Fyzv8DpppQ9WrpD/fWVvXWNGR22sU=
   ```

3 Copy the key file into this directory on Management and Security Server:

   Unix: `/var/opt/microfocus/mss/mssdata/certificates`

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

4 On the **Secure Shell** panel, under **Known Hosts List**, click **+ IMPORT**.

5 Enter the required information:

   - **File name**: the name of the file with the host's public key that you copied (step 2).

   - **Public key file password**: if required.

   - **Host name**: as specified in the public key file. The name you enter must *exactly match* the hostname in the public key. For example, if the hostname in the key is `hostname.example.com`, and you enter `hostname`, the import will not work.

   - **Host IP address**: as specified in the public key file, if present. If there is no IP address in the public key file, leave this field blank.

6 Click **IMPORT**.

   This host now displays in the Known Hosts List.

Shared User Key Pair

A user key pair is a public and private key used to authenticate a web-based client to a secure shell host. Although each typically has unique keys, a key pair can be shared among users.

To share a user key pair, choose one of these methods:

+ GENERATE

The generated user key pair will be stored on the Management and Security Server and automatically deployed to Reflection for the Web clients.

To generate a key pair, enter the required information:

- **Key algorithm**: RSA (the default) or DSA
- **Encryption key length**: the size of the public and private keys. Longer keys are more secure but may take more time to generate.

When you click **APPLY**, the key pair is created in the `MSSData/trustedcerts` folder as `sshclient.bcfks`, and the details are displayed in this panel.

+ IMPORT

A public key and its associated private key pair can be imported from a local workstation.

To import a key pair to the Management and Security Server:

1 Copy the key pair file or files to the `certificates` directory on the Management and Security Server:

   UNIX: `/var/opt/microfocus/mss/mssdata/certificates`

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

2 Enter the **File name**.

   - If the keys are in **OpenSSH** format files, enter the name of the private key file. The public key must be in a file with the same name and a `.pub` extension.
   - If the keys are in a **.PFX** format file, enter the file name.

3 Enter the **Password** that protects the private key. If the file is not protected, leave this field blank.

4 If the file contains multiple certificates, enter the **Friendly name** of the one associated with the desired key pair. Otherwise, leave this field blank.

5 Click **IMPORT**. The key pair file is created in the `MSSData/trustedcerts` folder, and the details are displayed on this panel,

EXPORT

You can export the shared user public key or key pair to an OpenSSH or secssh format file.

Specify a file name for export; for example, `id_rsa`. The public key is written to a file with this name and a `.pub` extension. When selected for export, the private key is written to this file.

The file or files are written to this folder on the Management and Security Server:

UNIX: `/var/opt/microfocus/mss/mssdata/certificates`

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

Check or enter the required information.

- **Export the private key with the public key** - otherwise, only the public key is exported.
- **Overwrite existing file(s)** - if other key files exist with the name.
- **Key file name** - a name for the file that will be created by the export operation.

  Enter the name for the private key (the file name with no extension) even if you are exporting only the public key.

- **Private key passphrase (optional)** - if you are exporting the private key, you can protect it with a password you enter here.

  Note: The password does not apply to the public key.

Shared User Key Pair Details

- **Public Key Algorithm** - the algorithm used to generate the host's key pair.
- **Public Key Fingerprint (SHA-1)** - A message digest of the public key made using the SHA-1 algorithm. The fingerprint can be used by a client to validate the public key.
- **Public Key Fingerprint (MD5)** - A message digest of the public key made using the MD-5 algorithm.

Related Topics

- Configure Settings

Certificates

Certificates in Management and Security Server generally identify a client or server. (Client certificates can identify individuals.)

During authentication, Entity A presents a certificate to Entity B, which checks the signature against its store of trusted certificates. If the certificate or its root is trusted, the transaction proceeds. If not, Entity B may either reject the transaction or present Entity A's user with a warning.

Server certificates. The need for server certificates depends on the security settings that are used for your terminal sessions:

- If you use **TLS** security, the Host needs server certificates.
- If you use the **Security Proxy Server**, both the **Management and Security Server** and the **Security Proxy** need server certificates.

Use the Certificates panel to generate and apply a self-signed certificate for Management and Security Server or to import a signed client certificate to share.

- "Administer the Management and Security Server Certificate" on page 48
- "Administer Shared Client Certificate" on page 49
- "Other certificates" on page 49

Administer the Management and Security Server Certificate

Management and Security Server requires a certificate to connect to the Security Proxy. You can generate a self-signed certificate or import a CA-signed certificate and private key.

Generate a self-signed certificate

This form generates a self-signed Management and Security Server certificate that can be used to connect to the Security Proxy. If a self-signed server certificate already exists, the certificate generated here will replace it.

To generate the certificate:

1 Enter the Common name of the site on which the certificate will be installed, such as `hostname.company.com` (for an external site) or hostname (for an internal site).

2 Enter the required information.

3 Open Advanced Settings, and confirm or change the settings, as desired.

4 Click +GENERATE and VIEW DETAILS to verify your entries.

Import a key pair

If a server certificate and private key already exist, the imported key pair will overwrite them.

To import the key pair:

1 Copy the file containing the certificate and the private key into this folder on the Management and Security Server:

   UNIX: `/var/opt/microfocus/mss/mssdata/certificates`

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

2 Enter the required information.

   Keystore file name: the file that contains the certificate

   Keystore password: that protects the file that contains the certificate

   Friendly name: so you can easily identify the certificate

3 Click IMPORT.

Administer Shared Client Certificate

A client certificate is used to identify users connecting to the Security Proxy or to a TLS host when client authentication is required. If all users share the same client certificate, the Administrative Server can automatically distribute it to the Reflection for the Web emulator clients when needed.

If a server certificate and private key already exist, the imported key pair will overwrite them.

To import the key pair:

1 Copy the file containing the certificate and the private key into this folder on the Management and Security Server:

   UNIX: `/var/opt/microfocus/mss/mssdata/certificates`

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

2 Enter the required information.

   Keystore file name: the file that contains the certificate

   Keystore password: that protects the file that contains the certificate

   Friendly name: so you can easily identify the certificate

3 Click **IMPORT**.

Related topics

 ◆ Other certificates

 ◆ Administer the Management and Security Server Certificate

Other certificates

Certificates that are needed for other functions are managed differently.

 ◆ Use the **Security Proxy Wizard** to manage the Security Proxy certificate.

 ◆ To generate other self-signed certificates or to import signed certificates to the Security Proxy, clients, or host systems, use the certificate features in those components.

 ◆ Use the **HTTPS Certificate Utility** to administer web certificates (for use with Tomcat) or to generate a Certificate Signing Request (CSR)

HTTPS Certificate Utility

This utility installs or updates a certificate for the HTTP server functionality that is included with Management and Security Server (from the Start menu). This certificate enables clients to establish secure connections (HTTPS) to the services provided by the Management and Security Server.

The HTTPS Certificate Utility also provides the option to create a private key and a Certificate Signing Request (CSR).

How to Generate a Certificate Signing Request (CSR)

A Certificate Signing Request or CSR is a block of encoded text that is given to a Certificate Authority (CA) when applying for an SSL Certificate. The CSR includes identity information and a public key. A CA verifies the identity of the server's domain name and its owner and then adds a signature to the certificate to verify the server's authenticity to other computers.

The Certificate Authority uses a CSR to create your SSL certificate, but it does not need your private key. Keep your private key secret.

Choose a method to generate a CSR and obtain a CA-signed certificate:

- "Use the HTTPS Certificate Utility" on page 50
- "Use a Certificate Authority's Instructions" on page 51
- "Use Commands for Keytool or Openssl Tool" on page 51

Use the HTTPS Certificate Utility

To generate a CSR and a new private key:

1 Open the **HTTPS Certificate Utility** from the **Start** menu. (It installs with Management and Security Server.)

2 Proceed through the utility, and review your previous actions, if pertinent.

3 On the **Select a certificate action** screen, select **Generate a new key pair and Certificate Signing Request**.

4 Proceed through the screens to specify information for the certificate:

- a Friendly Name
- a Common Name
- the certificate's organization and locality
- the certificate's validity and key length
- the directory that will store the private key and the CSR
- the certificate store's File name, File type, and Password that will be used to store the private key and the CSR

5 Note the **Next steps** and Quit the HTTPS Certificate Utility.

....

6 Send the `*.csr` file from the directory you specified to the Certificate Authority (CA) of your choice. Do not send your private key.

....

7 When the signed SSL certificate is received from the CA (response time varies), return to the **HTTPS Certificate Utility** to import the certificate together with the private key that was generated in the previous steps.

8 Proceed to the **Select a certificate action screen**, and select **Import a certificate and private key**.

9 Enter the certificate store file name that you previously specified.

10 Enter the keystore's password.

11 Click **Next** to apply the configuration changes. Click **Done** to close the utility.

Use a Certificate Authority's Instructions

To generate a CSR and obtain a CA-signed certificate, choose a CA, follow their instructions, and use the tools they provide. Here are some examples:

- DigiCert
- GeoTrust
- Thawte

CAs provide detailed instructions for common tools such as keytool and openssl. Some have their own tools that you can download. Creating a CSR can also be done completely online. For example, see SSL Tools

Use Commands for Keytool or Openssl Tool

If you are unable to use the HTTPS Certificate Utility or follow the instructions from a CA, you can use the manual keytool commands for CSR to perform the three steps: generate a key, generate a CSR, and import the response from the CA.

From the mss/server folder, run the following commands.

1 Generate a key:

```
../jre/bin/keytool -genkey -alias server -keyalg RSA -keysize 2048 -
keystore keystore.bcfks \
-storetype bcfks -providername BCFIPS -providerpath ./lib/bc-fips-*.jar
\
-providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

2 Generate a CSR:

```
../jre/bin/keytool -certreq -alias server -keyalg RSA -file server.csr
-keystore keystore.bcfks \
-storetype bcfks -providername BCFIPS -providerpath ./lib/bc-fips-*.jar
\
-providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

3 Import the response from the CA:

```
../jre/bin/keytool -importcert -trustcacerts -file careply -keystore
keystore.bcfks \
-storetype bcfks -providername BCFIPS -providerpath ./lib/bc-fips-*.jar
\
-providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

Or, you can use the openssl tool to generate CSRs and keys in two steps: generate a key and a CSR, and import the response from the CA.

1 `openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr`

2 `openssl pkcs12 -export -out keystore.p12 -in careply -inkey server.key`

Related topics

- Administer the Management and Security Server Certificate
- Administer Shared Client Certificate

Trusted Certificates

The Certificate Store contains the certificates that are trusted by the terminal emulator client and the Management and Security Server.

NOTE: When using **Clustering**, any changes made to the certificate stores (**+ IMPORT** or **DELETE** certificates) **will be replicated** to the other MSS servers in the cluster. You do not need to repeat the process on each MSS server.

Select **Terminal Emulator Clients** or **Management and Security Server** to filter the view of trusted certificates.

- Certificate Store - Terminal Emulator Clients
- Certificate Store - Management and Security Server
- Certificate Store - Trusted Sub-System
- Trusted Root Certificate Authorities

Certificate Store - Terminal Emulator Clients

Clients that make a TLS connection to a host or Security Proxy must trust the host or proxy certificate. This panel presents a list of root certificates trusted by the terminal emulator applet.

The table lists the certificates that have been imported to the terminal emulator applet's trusted list. To view details about the certificate, click the certificate's Friendly name.

To add a client certificate to the MSS trust store:

1. With **Terminal Emulator Clients** selected, click **+ IMPORT**.

2. Click **UPLOAD**. Select the file containing the certificate to upload to the MSS Administrative Server.

3. Enter the **Keystore file name**, **Keystore password**, and **Friendly name**.

4. Click **IMPORT** to add the certificate.

5. Restart the MSS Administrative Server.

See Trusted Root Certificate Authorities (collapsed by default).

Certificate Store - Management and Security Server

This collection of certificates includes CA certificates used to authenticate X.509 clients and to establish other servers as known and trusted to the Management and Security Server. To view details, click the certificate's Friendly name.

This collection is used for the following features:

- **X.509 with Fallback to LDAP authentication:** Add CA certificate(s) needed to authenticate end-user certificates, such as a certificate stored on a smart card.

  For these features, certificates are added to establish the other server as known and trusted.
- **Automated Sign-On for Mainframe:** Add a certificate(s) to establish trust of a Mainframe host.
- **Micro Focus Advanced Authentication (MFAA):** Add certificate(s) to trust the MFAA host.

Server certificates from other servers should be included in this certificate collection.

To add a server certificate to the MSS trust store:

1. With **Management and Security Server** selected, click **+ IMPORT**.

2. Click **UPLOAD**. Select the file containing the certificate to upload to the MSS Administrative Server.

3. Enter the **Keystore file name**, **Keystore password**, and **Friendly name**.

4. Click **IMPORT** to add the certificate.

5. Restart the MSS Administrative Server.

IMPORTANT: When **X.509** with **Fallback to LDAP authentication** is used in conjunction with other Management and Security Server features that also use the certificates in this collection (such as Automated Sign-On for Mainframe), **use caution** to ensure that trust is not inadvertently broadened and granted to unintended end-user clients.

See Trusted Root Certificate Authorities (collapsed by default).

Certificate Store - Trusted Sub-System

This collection of certificates includes certificates used to establish other servers as known and trusted to the Management and Security Server. To view details, click the certificate's Friendly name.

This collection is used for these features:

- **Clustering:** Add certificate(s) to trust other MSS servers in a cluster.
- **X.509 authentication for Host Access for the Cloud** (HA Cloud): Add session server certificate(s) to establish trust between MSS and HA Cloud.

To add a server certificate to the MSS trust store:

1. With **Trusted Sub-System** selected, click **+ IMPORT**.

2. Click **UPLOAD** to select the file containing the certificate to upload to MSS Administrative Server.

3. Enter the **Keystore file name**, **Keystore password**, and **Friendly name**.

4. Click **IMPORT** to add the certificate.

5. Restart the MSS Administrative Server.

See Trusted Root Certificate Authorities (collapsed by default).

Trusted Root Certificate Authorities

This table is collapsed by default on the **Trusted Certificates** panel. The table lists the set of commonly used root certificates in Management and Security Server. To view details about a root certificate, click its **Friendly Name**.

If a trusted CA root certificate expires or is compromised, you may need an update.

NOTE: If certificate changes are needed by Windows-based clients to perform **X.509 authentication**, you must restart the Management and Security Server for the changes to take effect.

Credential Store (Reflection for the Web)

The credential store is a database of usernames and passwords that have been used to log on to a host. Reflection for the Web uses these credentials in conjunction with login macros to automatically log on to host sessions. The Credential Store requires Windows on the client machine.

- ◆ "Enable credential store" on page 54
- ◆ "Select form of identity" on page 54
- ◆ "Regenerate encryption key" on page 55
- ◆ "Delete selected credentials" on page 55

Enable credential store

Check **Enable credential store** to save new credentials or read existing ones.

Select form of identity

By default, users are represented in the credential store depending on how they authenticate, such as with a Windows domain and username.

Check **Use LDAP distinguished name** to represent users by their LDAP Distinguished Name. This option requires LDAP authorization to be enabled in **Configure Authentication**.

Regenerate encryption key

When you enable the credential store, you should back up the key used to encrypt usernames and passwords in the credential store.

To back up the key, copy `[MSSData]/PropertyDS.xml` to a secure location. Make a new backup of `PropertyDS.xml` whenever you change settings in the Administrative Console so that these settings will not be overwritten when you restore the file. **Note:** You need administrator privileges to open or edit `PropertyDS.xml`.

When you click REGENERATE KEY:

A new key is generated to either replace an existing key or to add a key when the credential store is empty. When replacing an existing key, the data is decrypted using the old key and re-encrypted using the new key. Subsequent encryption uses the new key.

NOTE: Re-encrypting the credential store with a new key could take quite a bit of time. During the re-encryption, nothing can be written to or read from the credential store.

You *cannot* regenerate a key if the existing key is corrupted or maliciously altered. You must first recover the old key from a backup or delete all credentials before generating a new key.

Recovering an encryption key

To recover the old encryption key from the backup, edit `PropertyDS.xml` (requires administrator privileges):

1. Open the current `PropertyDS.xml` file and the backup copy in an editor.
2. Copy the values for the following properties from the backup to the current version of `PropertyDS.xml`:

   `CS.EncKey`
   `CS.EncAlgorithm`
   `CS.EncKeyLength`
   `CS.EncIV`
3. Save `PropertyDS.xml`.
4. Restart the Management and Security Server.

Delete selected credentials

When the credential store is enabled, new credentials are added when users run sessions configured with single sign-on macros. As time goes by, you may wish to remove older credentials. Use this option to delete stored user credentials based on the last-used date.

Note: Once credentials are deleted, they cannot be recovered.

To delete credentials:

1 Select one or more USERS.

2 Sort by CREDENTIAL LAST USED.

3 Check the credentials you want to delete, and click DELETE.

Security Proxy Server

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

After the Preliminary steps are completed, use this panel to import the settings from the Security Proxy Server to the Management and Security Server

- "Preliminary steps - Install and Configure" on page 56
- "Import Security Proxy settings" on page 56
- "Create and assign secure sessions" on page 58

Preliminary steps - Install and Configure

Before you can import the settings, you must install the Security Proxy and configure some initial settings.

Refer to the Technical Reference, Using the Security Proxy Server, for details.

Next Step: Import Security Proxy settings

Import Security Proxy settings

After the Security Proxy is installed, configured, and started, import the Security Proxy settings to the Administrative Server.

1 In the Administrative Console, open **Configure Settings** > **Security Proxy**.

2 Click **+ IMPORT**.

3 Enter the **Server name** of the computer on which you installed the Security Proxy Server.

   NOTE:

   - The Security Proxy Server must be running when you import the settings.

   - The name you enter must match the common name on the security proxy certificate if client verification of server identity is enabled (the default setting).

     The Administrative Server verifies the security proxy server identity by comparing the common name on the proxy certificate to the name of the server itself. If the names do not match—for instance, you enter `servername` and the server certificate common name is `servername.example.com`—you may be able to import the certificate, but session connections through the proxy will fail when the client attempts to verify the server identity.

   - The Security Proxy server must trust the Administrative Server certificate. (See Preliminary Steps.)

---

4 Enter the **Monitor port**. You can check the Security Proxy Monitor port number in the Security Proxy Wizard (**Advanced Settings**).

5 Enter a name that clients would recognize. If a single proxy server name is always used, leave this field blank.

In some cases, clients may need to access the security proxy using a different name than the one used to import the security proxy settings. For example, as administrator, your computer may access the Security Proxy through an internal network, but your end users may access the Security Proxy from outside the firewall and use a different proxy name. In this case, enter the name that the clients use in this field.

When both names are entered, the Administrative Server uses the first name to contact the Security Proxy and import its settings and certificate, and then displays the second name in the table on the **Security Proxy** panel and in the Terminal Session tool. Emulator sessions use the second name to contact the proxy. If any end users contact the Security Proxy using both proxy names, import the Security Proxy settings twice, and define separate sessions for each proxy name.

6 Click **IMPORT**. After the Security Proxy settings are imported, the Security Proxy server is listed in the table with its details:

Server name: The name of the server on which the security proxy is installed.

Authorization: The status of client authorization on this server. Authorization is enabled by default.

Monitor Port: The port on which the Security Proxy listens for incoming communication. Used when the Administrative Server contacts the proxy to get report information or to import the security settings. Usually 8080.

Proxy Port: The port the emulator uses to open a secure connection to the Security Proxy.

Supported Protocols: The protocols that are available on the Security Proxy. Each proxy can support emulation and/or FTP. or the Passthrough proxy (no TLS handshake, client/server authentication, or encryption).

Destination: When client authorization is turned off, each Security Proxy port connects to one host. Set the destination host for this proxy port in the Security Proxy Wizard. When client authorization is on, one port can connect to multiple hosts.

Friendly Name: The name of the server certificate used for this Security Proxy setting.

Cipher Suite: The encryption algorithm used for this proxy port.

7 **Accept settings exported from Security Proxy Servers.**

When you use the **Security Proxy Wizard** to set up or change a Security Proxy, you can export information and certificates directly to the Administrative Server over an HTTP connection. This information is not encrypted.

CAUTION: By default, the administrative server supports only HTTPS. To export information and certificates to the administrative server, you need to first enable HTTP connection on the server. Contact Support for assistance.

To use the automatic export in the Security Proxy Wizard, you must check this box.

IMPORTANT

- **If you change settings on the Security Proxy**, you must re-import them to the Management and Security Server.

- **When you upgrade**, open the **Security Proxy Wizard**, review the status of your Security Proxy servers, and click **Save**. This action synchronizes the Security Proxy server with the Management and Security Server.

Next step: Create and assign secure sessions

Create and assign secure sessions

After the trust between the Administrative Server and the Security Proxy is set, use **Manage Sessions** and **Assign Access** to create and assign secure sessions to authorized users.

For detailed steps, refer to Using the Security Proxy Server:

 - Create Secure Sessions
 - Assign Secure Sessions

Related Topics

 - Preliminary steps - Install and Configure
 - Import Security Proxy settings

Authentication & Authorization

Choose a method to validate a user's identity (authentication). Then you can assign sessions to specific users or groups (authorization).

 - Choose Authentication Method
 - Choose Authorization Method
 - LDAP Server Configuration
 - Single Sign-on through IIS
 - Windows Authentication - Kerberos
 - Windows Authentication - NTLMv2 (deprecated)
 - X.509 Configuration
 - SiteMinder Configuration
 - Micro Focus Advanced Authentication
 - SAML Authentication

Choose Authentication Method

Authentication validates the user's identity based on some credentials, such as a username/password combination or a client certificate. Select a method to authenticate users:

 - **None** — Management and Security Server does not present a login screen. Any user can access their assigned sessions without being prompted for credentials. Session authorization is not available.
 - **LDAP** — Management and Security Server makes a read-only connection to your existing LDAP (Lightweight Directory Access Protocol) server to verify usernames and passwords. You can also use LDAP to authorize session access. LDAP is an industry standard application protocol for accessing and maintaining distributed directory information services over a network.

   NOTE: You can enable more than one LDAP server.

- **Single sign-on through IIS** — This method uses Microsoft IIS web server. This option requires no additional setup as long as you used the automated installer and chose to integrate with IIS during the installation process. You can find more information on install configurations in the MSS Installation Guide.

- **Windows Authentication - Kerberos** — Kerberos is an authentication protocol that uses cryptographic tickets to avoid transmitting plain text passwords. Client services obtain ticket-granting tickets from the Kerberos Key Distribution Center (KDC) and present those tickets as their network credentials to gain access to services.

  NOTE: If Kerberos is enabled and you wish to use a different authentication method, you must first disable Kerberos. See Disabling Kerberos.

- **Windows Authentication - NTLMv2 (deprecated)** —*For security reasons*, this option, which uses the NT LAN Manager version 2 (NTLM v2) protocol to authenticate users, is *not recommended*.

  For details, see *Knowledge Base article 7024851*.

- **X.509** — X.509 is a standard for managing digital certificates and public key encryption. When you use certificate-based authentication, you can specify the certificate source and setting for LDAP failover if certificate-based authentication fails.

- **SiteMinder** — To enable this option on a Windows system, install both MSS and a SiteMinder web agent on the same machine as IIS, and set up the server to use your IIS web server.

- **Micro Focus Advanced Authentication** — MSS provides an optional Add-on to use Advanced Authentication™, a separate Micro Focus product that provides a multi-factor authentication solution that uses a chain of authentication methods.

- **SAML** — SAML (Security Assertion Markup Language) is an xml-based open standard format that exchanges authentication and authorization data between an identity provider and a service provider.

The setup options vary based on your selection.

Related Topics

- LDAP Server Configuration
- Enabling Multiple LDAP Servers
- Single Sign-on through IIS
- Windows Authentication - Kerberos
- Windows Authentication - NTLMv2 (deprecated)
- X.509 Configuration
- SiteMinder Configuration
- Micro Focus Advanced Authentication
- SAML Authentication

Choose Authorization Method

The authorization method determines who can access your terminal emulation sessions.

- **Allow authenticated users to access all published sessions**

When this option is selected, the **Assign Users & Groups** panel presents the list of sessions that you can to publish to *all* end users. Users see the list of sessions when they log in.

 ◆ **Use LDAP to restrict access to sessions**

When this option is selected, the **Assign Users& Groups** panel allows you to assign specific sessions to specific LDAP users or groups. Logon userids must match those in the LDAP directory. After the sessions are assigned, the authorized users see their list of sessions when they log in.

Related Topics

 ◆ LDAP Server Configuration

 ◆ Enabling Multiple LDAP Servers

 ◆ Choose Authentication Method

 ◆ Assign Access

LDAP Server Configuration

When you use LDAP to authenticate or authorize users, Management and Security Server makes a read-only connection to the LDAP server. Use these settings to configure that connection.

 ◆ "LDAP Servers" on page 61

 ◆ "Enabling Multiple LDAP Servers" on page 61

 ◆ "LDAP Configuration" on page 61

 ◆ "Search Base and Groups/Folders" on page 63

 ◆ "Certificate" on page 64

 ◆ "Authentication of End Users" on page 64

 ◆ "Validate LDAP Connection" on page 64

 ◆ "Advanced Settings" on page 64

LDAP Servers

You can **ADD**, **EDIT**, **TEST**, or **DELETE** the connection for each LDAP server. Check with your organization's LDAP administrator for more information, if needed to configure these options.

To use more than one LDAP server to authenticate or authorize users, you must first set a property. See Enabling Multiple LDAP Servers, and then proceed with the LDAP configuration for each server.

Enabling Multiple LDAP Servers

More than one LDAP server can be configured to authenticate and authorize users. A property must be set, and then the servers can be added and configured.

To enable multiple LDAP servers:

1 Open `PropertyDS.xml.` (Administrative privileges are required.)

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

2 Locate this property, and set the value to `true`:

```
<CORE_PROPERTY NAME="AC.DirAllowMultiLdap">

<BOOLEAN>true</BOOLEAN>

</CORE_PROPERTY>
```

3 Save the file.

4 Restart the MSS server.

5 Return to the **Administrative Console** and enter the LDAP Configuration information for each LDAP Server.

Or, if you are configuring **Single sign-on through Windows authentication**, return to Adding Another Server for Windows Authentication NTLMv2.

NOTE: To revert to a single LDAP server, set the property in step 2 to `false`, save the file, and restart the MSS server.

LDAP Configuration

Click **+ADD** to open the LDAP Configuration panel, or select a server and click **EDIT**.

Enter or edit the **LDAP Server** information.

- **Server type**

  Select the type of LDAP server you are using. The options on this panel change depending on the LDAP server type you select. If you do not see your specific LDAP server in the list, select **Generic LDAP Compliant Directory Server (RFC 2256)**.

- **Security options**

  Data can be passed between the MSS Administrative Server and the LDAP server as clear text or encrypted. The type of encryption used depends on your LDAP server. TLS is available for all server types, and Kerberos v5 is available for Windows Active Directory.

  - **Plain Text.** By default, Management and Security Server transmits data between the MSS Administrative Server and the LDAP server in clear text. If you choose this option, you should prevent users from accessing the network link between these two servers.

  - **TLS.** When using TLS as the security option for an LDAP server, you must import the server's trusted certificate. Use the **IMPORT CERTIFICATE** button (below). If you are presented with multiple certificates, it is best to import the CA certificate.

  - **Kerberos v5.** When you select Windows Active Directory with Kerberos, you must enter the name of the Kerberos key distribution centers. Multiple key distribution centers, delimited by commas or spaces, can be used. If you do not know the name of the Kerberos key distribution center, enter the fully-qualified DNS name of the Active Directory server.

    The option under the key distribution center name field allows you to encrypt all data transmitted over the Kerberos connection. By default, only user names and passwords are passed securely between the Administrative Server and LDAP servers using Kerberos. Encrypting all data is more secure, but may increase performance overhead.

- **Server name**

  Enter the LDAP server name as either a name or a full IP address. If you selected **TLS**, this LDAP server name must exactly match the Common Name on the LDAP server's certificate.

Multiple server names, delimited by commas or spaces, can be used for failover support. If an LDAP server is down, the next server on the list will be contacted. In this case, all fields specified on this panel that are used for LDAP connections should be available on all the LDAP servers, and should have identical configurations.

Windows Active Directory - DNS domain. When Windows Active Directory is selected (without Kerberos), you have the option to use a DNS domain instead of a specific domain controller. No further configuration is required. When selected, you do not need to specify a domain controller address or the corresponding NetBIOS name because Management and Security Server provides the Domain Controller Locator Service. This service can be used *only* when the Administrative Server is running on Windows.

For example, when you enter a domain name, such as `mycompany.com`, Management and Security Server automatically finds an available **domain server** and the **domain name**, which can be different from the DNS domain.

◆ **Server port**

Enter the port used by your LDAP server. The default is 389 for plain text or 636 for TLS.

If you are using Windows Active Directory, you may wish to set the server port to the global catalog port, which is 3268 (or 3269 over TLS). Global catalog searches can be faster than referral-based cross-domain searches.

◆ **Username** and **Password**

Provide the username and password for an LDAP server account that can be used to access the directory in Read-only mode. Generally, the account does not require any special directory privileges but must be able to search the directory based on the most common directory attributes (such as `cn`, `ou`, `member` and `memberOf`). Re-enter the password in the **Password confirmation** box.

NOTE: The username must uniquely identify the user in the directory. The syntax depends on the type of LDAP server you are using.

◆ For **Windows Active Directory** with **Plain Text**, enter

NetBIOS domain\sAMAccountName (such as `exampledomain\username`)
userPrincipalName (such as `username@exampledomain.com`)
or
distinguished name (such as `uid=examplename,DC=examplecorp,DC=com`).

◆ For any **other LDAP** server type, enter the **distinguished name** (such as `uid=examplename,DC=examplecorp,DC=com`).

If this account password changes, be sure to update the account password here and apply the new settings. To avoid this problem, you may wish to set up an account that is not subject to automatic password aging policies, or that cannot be changed by other administrators without notice.

Search Base and Groups/Folders

◆ **Directory search base**

Enter the distinguished name of the node in the directory tree you want to use as the base for Administrative Server search operations. Examples: `DC=my_corp,DC=com` or `o=my_corp.com`.

For more information about how to describe the search base, see the LDAP administrator for your organization.

◆ **Groups or folders**

While you can assign sessions to specific users in the directory, you can also assign sessions to either **Logical groups** or **Folders**. Choose the option that reflects the way the data is organized in your directory -- and the way you want to Assign Access. For instance if you want to assign access to a folder, then **Folders** must be selected here.

In Management and Security Server, the term **folder** is used to describe both organizational units and containers. Most directories have an organizational structure that uses logical groups; for example, `groupOfNames` and `groupOfUniqueNames`.

Certificate

Click **IMPORT CERTIFICATE** to import the LDAP server's trusted certificate into the JRE's default trusted keystore. This button displays when **TLS** is selected.

Authentication of End Users

LDAP attribute for identifier. The default LDAP attribute to use as an identifier is available when you select an LDAP server type.

Default LDAP identifiers:

Server type	Default user identifier
OpenLDAP Directory Server	cn
Generic LDAP Compliant Directory Server (RFC 2256)	cn
RACF Directory Server	racfid
Oracle LDAP Directory Server	uid
IBM Tivoli Directory Server	cn
Windows Active Directory	List of domains*
NetIQ eDirectory	cn
Windows Active Directory with LDAP login form	cn

* When you select **Windows Active Directory** with **Kerberos**, you must enter a Kerberos realm (such as `domain@example.com`). If you are using **Windows Active Directory** with **Plain text**, enter a NetBIOS domain name with a maximum of 15 characters (such as `MYCOMPANY, SALES`). If you have more than one domain or realm, separate the entries with commas (for example, `1stDomain, 2ndDomain, 3rdDomain`). When an end user requests the list of sessions, the login panel prompts for a username and password and displays available domains or realms in a drop-down list.

Validate LDAP Connection

Click **TEST CONNECTION** to verify that this LDAP server can connect to the Administrative Server (Management and Security Server). If the test fails, check the logs and resolve the issue before continuing.

Advanced Settings

Maximum nested level for groups

This number determines how assigned sessions are inherited. If Group A contains Group B of which JohnUser is a member, and you assign a session to Group A, JohnUser will also have access to that assigned session. If users do not inherit sessions as you expect, increase this number. Do not raise this level more than necessary because too high a number can impair performance if you have a large number of users. The default is 5.

After the LDAP servers are configured, use **Assign Users & Groups** to authorize users' access to sessions.

Related Topics

- Manage Sessions
- Assign Access

Single Sign-on through IIS

This method assumes that Management and Security Server is set up to use Microsoft IIS web server (Windows only).

If you installed using the automated installer and integrated with IIS during installation, setup is complete. If you used an alternative installation method, see the MSS Installation Guide for more information.

Users who have logged in to Windows do not need to log in again to access sessions. You must administer usernames and passwords through the identity system used by IIS, typically Active Directory.

This authentication method can be used for the Sessions list as well as the Administrative Console.

To enable Single Sign-on through IIS:

1 Open `mss/server/conf/container.properties`

2 Insert this line: `management.server.iis.url=<url>`

where `<url>` is the IIS web server address and port along with the /MSS path.

For example:

`https://<iisserver>/mss` (when TLS is configured on your IIS server).

If authentication fails, you may need to remove the domain name in order for the domain credentials to be passed to IIS: https://server/mss.

3 If you want to access the **Host Access for the Cloud** web client, then you'll need to set that in the Session Server container.properties as well. See Configure Single Sign-on through IIS in the HACloud documentation.

NOTE: If you use an **MSS load balancer** with Single Sign-on through IIS, additional persistence configuration is required. See Using a Load Balancer.

Troubleshooting IIS Integration

If you encounter these errors, add or change the following settings.

- *Error:* "Login failed. Invalid username or password."

  Resolution:

    1. Change the authentication method to **Anonymous**.

    2. Set the Anonymous Authentication to use **Application pool identity**.

- *Error:* "Request Entity Too Large"

  Resolution:

    1. Add the following line to both `MSS\server\web\conf\ntiis\worker.properties` and `\...\ntiis\worker_sec.properties`:

       `worker.ajp13_worker.max_packet_size=65536`

    2. Add the following setting to `MSS\server\conf\container.properties`:

       `servletengine.ajpMaxPacketSize=65536`

Circumstantial Credential Prompts When Using Single Sign-on

When Management and Security Server is configured to use Single Sign-On through IIS or through Windows, a user will be prompted for credentials under certain circumstances:

- The browser's process owner is **not a valid Windows user or a member of the Active Directory** domain. Typically the browser's process owner performs the interactive login to the operating system. However, an exception to this occurs when the Run As command launches the browser as a different user.

- The browser does not support single sign-on using **Kerberos**.

  - In Internet Explorer, this option is enabled by selecting Enable Integrated Windows Authentication. While this option is enabled by default, it can be overridden through Group Policies and practices.

  - In Mozilla Firefox, you must configure support for Kerberos authentication. Refer to Firefox documentation for instructions.

- When using **Internet Explorer,** if the `management.server.iis.url` property contains periods (such as http://www.microsoft.com or https://10.0.0.1), the requested address is assumed to exist on the Internet. Credentials are not passed automatically, and a credentials prompt will appear. However, Internet Explorer can be configured to automatically pass

credentials for such an address by adding it to the Trusted Sites list. Alternatively, you can configure a Custom security level in Internet Explorer to perform an **Automatic logon with current username and password**.

Related Topics

- Assign Access

Windows Authentication - Kerberos

Kerberos is an authentication protocol that uses cryptographic tickets to avoid transmitting plain text passwords. Client services obtain ticket-granting tickets from the Kerberos Key Distribution Center (KDC) and present those tickets as their network credentials to gain access to services.

In this configuration, a Windows machine on the associated domain can authenticate automatically to MSS to either launch sessions from the HACloud session server or to use Reflection Desktop sessions configured for centralized management.

- Limitations, Requirements, Terminology
- Enabling Kerberos
- Configuring Kerberos
- Configuring Kerberos for Clustered Servers
- Troubleshooting Kerberos Configuration
- Upgrading MSS: Considerations for Kerberos
- Disabling Kerberos

Limitations, Requirements, Terminology

Before you begin to configure Windows Authentication - Kerberos, check these details.

Limitations

- Current implementation is limited to the HACloud and Reflection Desktop clients
- Sessions cannot be launched from a user's Assigned Sessions list

Requirements

To experience full Kerberos authentication, users must

- access the client (HACloud or Reflection Desktop) from a Windows machine that is part of a **Kerberos protected domain**.
- be logged into that machine with a user account that is part of the **Kerberos Active Directory.**

If these requirements are not met, the users will be prompted for credentials.

Kerberos Terminology

You may want to become familiar with these terms when configuring Kerberos.

Term	Definition
Delegated Authentication	When a user authenticates to a service, Kerberos supports a delegation mechanism that enables the service to act on behalf of the user when connecting to back-end hosts.
Fully Qualified Domain Name (FQDN)	The FQDN consists of two parts: the hostname and the domain name. For example, an FQDN for a hypothetical mail server might be mymail.mycompany.com
Key Distribution Center (KDC)	A server that provides authentication and ticket-granting services. In an Active Directory domain, the Windows domain controller acts as the KDC.
Keytab file	The keytab file contains the Service Principal Name's encryption keys used when communicating with the KDC.
Realm	A realm is the domain over which a KDC has the authority to authenticate a user. The realm name is an upper-case version of the DNS domain. For example, MYCOMPANY.COM.
Service Principal Name (SPN)	The Service Principal Name uniquely identifies a service instance. SPNs are used to associate a service instance with a domain logon account.

Related topics

- Enabling Kerberos
- Configuring Kerberos

Enabling Kerberos

Note: The **Windows Authentication - Kerberos** option in the MSS Administrative Console is not available until these steps are completed.

To enable **Windows Authentication - Kerberos**, follow these steps:

1 Edit `<install-dir>/mss/server/conf/container.properties` and add this property:

    `mss.oauth=true`

2 Edit `<install-dir>/mss/server/microservices/auth-service/service.yml` and set the `enabled` property to `true`.

3 Restart the server.

4 Continue with Configuring Kerberos.

Configuring Kerberos

Kerberos requires configuration in Windows (KDC and Active Directory), the MSS Administrative Console, and your browser.

- Configure KDC and Active Directory
- Settings in the MSS Administrative Console
- Verify your Kerberos Configuration

Configure KDC and Active Directory

To configure Windows Authentication - Kerberos support, certain steps must first be done on the KDC: create a service account, assign an SPN, and create a keytab.

Create a Service Account for your MSS deployment

1 Open **Active Directory Users and Computers** by clicking **Start | Administrative Tools | Active Directory Users and Computers**.

2 Select the **Active Directory** domain in the menu on the left.

3 Select the **New User** action to display the **New User** wizard.

4 In the **Full name** field, type the name of your MSS deployment service account (such as `my-mss-deployment`).

5 In the **User logon name** field, type the name of your MSS deployment used in step 4.

6 Click **Next**.

7 Assign a **password** to this service account. Be sure to take note of this password because it will be needed later.

8 Uncheck **User must change password at next logon**.

9 Check **Password never expires**.

10 Click **Next**.

11 Click **Finish**.

Assign an SPN for the MSS server to the Service Account

1 Open a command prompt with Administrator rights.

2 To verify no duplicate SPN entries exist, type the command `setspn -X`.

3 Type the command `setspn -A HTTP/<fully-qualified-name-of-mss-server> <service-account-name>`

   Example: `setspn -A HTTP/my-mss-server.my-company.com my-mss-deployment`

4 To verify the SPN was successfully added, type the command `setspn -L <service-account-name>`

For further help on the `spn` command, use the `setspn /help` command.

Create a Keytab for the Service Account to be used by MSS

1 Open a command prompt with Administrator rights.

2 Type the command:

```
ktpass -princ HTTP/<fully-qualified-name-of-mss-server>@<active-
directory-domain> -mapuser <service-account-name> -pass <service-
account-password> -ptype KRB5_NT_PRINCIPAL -crypto ALL -out <service-
account-name>.keytab
```

Example:

```
ktpass -princ HTTP/my-mss-server.my-company.com@MYDOMAIN.COM -mapuser
my-mss-deployment@MYDOMAIN.COM -pass password -ptype KRB5_NT_PRINCIPAL
-crypto ALL -out my-mss-deployment.keytab
```

3 Make sure the keytab file that is created is available when configuring **Windows Authentication - Kerberos** in the MSS Administrative Console.

Notes:

- The keytab file contains sensitive data, so be sure to protect it accordingly.
- You can use any name for the keytab file.
- If setting up a cluster of MSS servers, this keytab file with a single SPN is all that is needed.
  See Configuring Kerberos for Clustered Servers for further details.

Settings in the MSS Administrative Console

After enabling Kerberos and configuring the KDC and Active Directory to generate the keytab file, you must configure Kerberos in the MSS Administrative Console. Following these steps:

1 Navigate to Configure Settings - Authentication & Authorization and click **Windows Authentication - Kerberos**.

2 Select the desired **Authorization** method.

3 In the Kerberos Configuration section, enter the following:

   3a **Realm** - The name of your realm or domain name. For example, `MYCOMPANY.COM`.

   3b **Service Principal Name (SPN)** - The SPN created for your MSS instance. Enter the SPN using the indicated format: `HTTP/<fully-qualified-domain-name>@<REALM-NAME>`.

   3c **Key Distribution Center (KDC)** - Specify the KDC or domain controller host name

   3d **Port** - Enter the KDC port if different from the default of 88.

   3e Click **IMPORT** to upload the keytab file generated on the KDC. This file must be available on the system used to access the MSS Administrative Console.

   3f Click **TEST CONNECTION** to test that the KDC can be accessed.

4 In the **LDAP Servers** section, click **ADD** to configure the Active Directory used by the KDC.

(See LDAP Configuration for further details).

5 Click **Apply**.

Notes:

- The SPN must be the SPN used when configuring the KDC.
- The SPN must be in the keytab file that is uploaded.
- You must configure an **LDAP server** with **Windows Active Directory** as the **Server type**.
  Active Directory is the only supported LDAP Server type for Windows Authentication - Kerberos.

Verify your Kerberos Configuration

Now that your single MSS server is configured for Windows Authentication - Kerberos, it is a good idea to verify that the configuration is working correctly.

Steps to verify:

1 Use a client system that is a member of the Active Directory domain.

2 Log onto the client system using the credentials of a user that is a member of the Active Directory.

3 If not already done, configure your browser for Kerberos. Refer to your browser's help for instructions on how to enable Kerberos.

4 Once configured for Kerberos, use that browser to access the url:

   `https://<fully-qualified-mss-server>:9443/osp/a/hc/auth/app`

5 To verify your Kerberos configuration:

   When configured correctly, you should see that the user logged into the client machine is logged into the web application without being prompted for any credentials.

   When not configured correctly, you may see a prompt for credentials indicating that LDAP fallback has occurred, or you may encounter an error message. If this happens, see Troubleshooting Kerberos Configuration for assistance.

Notes:

* When using Kerberos authentication for **Reflection Desktop** clients, the browser on the client system needs to be configured, as mentioned in step 3 above.

Related topics

* Configuring Kerberos for Clustered Servers
* Troubleshooting Kerberos Configuration

Configuring Kerberos for Clustered Servers

If you enabled clustering for your MSS deployment, some additional steps are required for configuring Windows Authentication - Kerberos.

The following steps can be done either before clustering the MSS server or after the cluster has already been established. For more information, see Clustering.

* Step 1. Configure each server to be clustered
* Step 2. Configure Load Balancer/Proxies
* Step 3. Set Certificates
* Step 4. Add the SPN of the load balancer to the KDC

Step 1. Configure each server to be clustered

1 Enable Kerberos on each server in the cluster by following the steps in Enabling Kerberos.

2 After successfully completing all of the Configure KDC and Active Directory steps **for a single server**, you need to add an SPN for each additional server in the cluster.

The SPN must be added to the Active Directory service account that was already created for your MSS deployment.

3 For each additional server in the cluster:

Follow the steps described in .

Notes:

◆ The keytab file generated for the single server deployment does not need to be—and **should not be**—modified for a clustered deployment.

◆ The addition of the SPNs to the service account is all that is required.

Step 2. Configure Load Balancer/Proxies

If you are putting a load balancer in front of your MSS cluster, some additional steps are required when using Windows Authentication - Kerberos. These steps must be done **on each server** in the cluster.

1 Edit `<install-dir>/mss/conf/container.properties` and add this property:

```
oauthadapter.management.server.url=https://<load-balancer-
address:port>/mss
```

2 Configure the auth-service to accept connections from the load balancer by editing the `<install-dir>/mss/server/microservices/auth-service/service.yml` file and adding these properties to the `env` section:

```
- name: authsvc.http-interfaces
  value: {name}
- name: authsvc.http-interfaces.{name}.anyLocalInterface
  value: true
- name: authsvc.http-interfaces.{name}.proxyDomain
  value: {domainName-of-proxy-interface}
- name: authsvc.http-interfaces.{name}.proxyPort
  value: {port-of-proxy-interface}
- name: authsvc.http-interfaces.{name}.port
  value: 9443
- name: authsvc.http-interfaces.{name}.tls
  value: true
```

Notes:

◆ `{name}` - any name you wish for the proxy interface

◆ `{domainName-of-proxy-interface}` - the fully qualified address of the load balancer

◆ `{port-of-proxy-interface}` - the port used by the load balancer

◆ If additional interfaces are necessary, you can define a comma-delimited list of names in the `authsvc.http-interfaces` property and then define the complete set of properties for each name.

3 Restart the server.

Step 3. Set Certificates

In order for the load balancer to allow HTTPS connections to the MSS server, the load balancer public certificate needs to be uploaded to the MSS cluster. Follow these steps:

1 Log into the MSS Administrative Console on one machine in the cluster.

2 Navigate to **Configure Settings - Trusted Certificates**.

3 Select the **Trusted Sub-System** certificate store.

4 Click **+IMPORT**.

5 Click **UPLOAD** and locate the load balancer's public certificate.

6 Enter a **Friendly name** for the certificate entry.

7 Click **IMPORT**.

Step 4. Add the SPN of the load balancer to the KDC

For the load balancer to forward Kerberos login requests from users, the load balancer must be registered as an additional Service Principal Name (SPN) with the service account on the KDC.

Follow the steps in Step 1. Configure each server to be clustered, above, to add the SPN of the load balancer machine to the service account on the KDC used to authenticate users.

For example:

```
setspn –A HTTP/load-balancer.my-company.com my-mss-deployment
```

As with other MSS servers in a cluster:

◆ You do not need to—*and should not*—generate a new keytab file.

◆ The addition of the load balancer as an SPN to the service account is all that is required.

Related topics

◆ Troubleshooting Kerberos Configuration

◆ Configuring Kerberos

Troubleshooting Kerberos Configuration

The first step in troubleshooting issues with Windows Authentication – Kerberos is to increase the logging level for the MSS authentication service. Follow these steps:

1 Edit the <install-dir>/mss/server/microservices/auth-service/service.yml file and add this to the env section:

```
- name: authsvc.logging.level
  value: DEBUG
```

2 Restart the server

If you are troubleshooting a cluster of MSS servers, we recommend that you increase the logging level on all servers in the cluster.

Once debug logging is enabled, you can find the log output for Kerberos and OAuth operations in `<install-directory>/mss/server/logs/auth-service/auth-service-osp.*.log`.

Other general information for the MSS authentication service is logged to the `auth-service.log` file in the same location.

Issue	Possible cause
User is prompted for credentials	◆ The client machine is not a member of the Active Directory domain ◆ The user has not logged onto the client machine with the credentials of a user in the Active Directory domain ◆ The browser (Internet Options) has not been configured for Kerberos ◆ The necessary SPN has not been added to the KDC service account
User encounters the error message: "Unable to complete request at this time"	◆ LDAP is misconfigured ◆ The keytab file created for the service account on the KDC is not valid
User encounters the error message: `XDAS_OUT_POLICY_VIOLATION`	◆ The proxy interface properties are not properly configured when the MSS server is behind a reverse proxy or load balancer
User encounters the error message: "This site cannot be reached"	◆ The auth service is not running or has not been enabled ◆ Check the `service.yml` to verify that the `enabled` setting is set to `true`
Authentication takes a long time	◆ LDAP is configured with the standard LDAP port. Instead, configure LDAP with the global catalog port (such as 3268)
Reflection Desktop displays a "connection failed" error when trying to open a session	◆ Reflection Desktop must have Centralized Management configured to access the MSS server using HTTPS ◆ And, the certificate of the MSS server must be trusted by the Windows Trusted Root Certification Authorities store

Upgrading MSS: Considerations for Kerberos

Before you upgrade MSS, back up the properties defined in these files:

- ◆ `<install-dir>/mss/server/conf/container.properties`
- ◆ `<install-dir>/mss/server/microservices/auth-service/service.yml`

After upgrading your MSS servers, you need to redefine the properties in those files.

Related topics

- ◆ Enabling Kerberos
- ◆ Configuring Kerberos for Clustered Servers

Disabling Kerberos

When switching to another method of authentication, you must first disable Kerberos.

To disable Kerberos:

1 Edit `<install-dir>/mss/server/conf/container.properties` and set this property to false:

   `mss.oauth=false`

2 Edit `<install-dir>/mss/server/microservices/auth-service/service.yml` and set the enabled property to `false`.

3 Restart the server.

4 Choose another Authentication method in the MSS Administrative Console.

Windows Authentication - NTLMv2 (deprecated)

This authentication method, which uses NTLMv2, is *not recommended* for security reasons.

CAUTION: Customers using Single Sign-on through Windows to authenticate to Host Access Management and Security Server (MSS) are subject to the Netlogon Elevation of Privilege Vulnerability (CVE 2020-1472).

For details, see *Knowledge Base article 7024851*.

To use Windows Authentication - NTLMv2:

1 In **Configure Settings - Authentication & Authorization**, click **Windows Authentication - NTLMv2 (deprecated)**.

2 Select your authorization method:

   ◆ **Allow authenticated users to access all published sessions**

   ◆ **Use LDAP to restrict access to session**

      NOTE: The same server will be used for Windows (Active Directory) authentication and LDAP authorization.

3 Click **+ADD** and proceed according to your selected authorization method.

   ◆ If you are **not using LDAP**, continue with the steps to Configure Windows Authentication - NTLMv2 (without LDAP) Configure Windows Single Sign-on (without LDAP)

   ◆ If you **are using LDAP** to restrict access, continue with Use LDAP to restrict access to Single Sign-on sessions.

Related topics

   ◆ Configure Windows Authentication - NTLMv2 (without LDAP)

   ◆ Use LDAP to restrict access to Window Authentication - NTLMv2 sessions

   ◆ Adding Another Server for Windows Authentication NTLMv2

Configure Windows Authentication - NTLMv2 (without LDAP)

Use these settings to configure Windows Authentication - NTMLv2 *without using LDAP* authorization.

(If instead you want to use LDAP, click **CANCEL**. Click **Use LDAP to restrict access to sessions**, click **+ADD** and proceed with Use LDAP to restrict access to Window Authentication - NTLMv2 sessions.)

1 Enter the settings to **ADD** or **EDIT** an NTLM server for Single Sign-on through Windows Authentication:

   1a Choose and enter either

   - **Domain Controller DNS name or IP address**

     IP address or DNS name of the Active Directory Domain Controller.

     NetBIOS hostname of domain controller

     The first 15 characters of the domain controller's host name, for example, `myComputer`.

     Note: The term **NetBIOS** is called *pre-Windows 2000* in some Windows utilities.

     — or —

   - **DNS domain**

   1b **NetBIOS domain name**

   The first 15 characters of the left-most label in the DNS domain name.

   Example: For the DNS domain name `mydomain.mycompany.com`, enter the NetBIOS domain value `mydomain`.

   TIP: To obtain the NetBIOS name for a domain on **Windows Server 2000 or higher**:

   1. Open the Active Directory **Domains and Trusts** snap-in (`domain.msc`).
   2. In the console tree, right-click the domain and select **Properties**.
   3. The **Domain name** (pre-Windows 2000) field displays the `NetBIOS name`.

   On Windows Server 2008 or higher, you can also use the Active Directory module for Windows PowerShell to find the NetBIOS name of a domain in Active Directory Domain Services.

   On **Windows Server 2008 only**, if the Active Directory module is not available, you may need to install it first, using this PowerShell command:

   ```
   import-module activedirectory
   ```

   This example demonstrates how to find the NetBIOS name of the domain called `mydomain.com`:

   ```
   Get-ADDomain -Identity mydomain.com | findstr /I NetBIOSName
   ```

   1c **Computer account (for servicing)**

   A computer account in the Active Directory domain. A computer account is different than a user account. The computer account should not be associated with an actual physical or virtual computer.

To specify the Computer account for servicing

A computer account's syntax is the pre-Windows 2000 computer name, followed by a `$` sign, followed by the `@` symbol, and then the DNS domain name.

Syntax: `<Computer name (pre-Windows 2000)>$@<DNS domain name>`

For example, if the Computer name is `ReflServiceAccount`, the pre-Windows 2000 Computer name is `REFLSERVICEACCO` and the **computer account** is: `REFLSERVICEACCO$@mydomain.com`

    1d **Computer account password**

If the password of the computer account is not already known, it must be explicitly reset in Active Directory. You can reset a computer account's password using a simple VBScript, or the ADSI Edit tool.

2 Click **TEST CONNECTION**.

This action checks the NTLMv2 connection to be sure the server is listening and is in fact a domain controller. The test attempts to authenticate to the server using the IP address or alias for the domain controller, the NetBIOS hostname, computer account, and password.

Note: The Domain is not tested and could still be a cause for error later in the authentication process.

If the result is **Success**, click **OK**.

If **TEST CONNECTION** fails, check the logs and resolve the issue before continuing.

3 To add another server, see Adding Another Server for Windows Authentication NTLMv2.

Related Topics

- Use LDAP to restrict access to Window Authentication - NTLMv2 sessions
- Adding Another Server for Windows Authentication NTLMv2

Use LDAP to restrict access to Window Authentication - NTLMv2 sessions

To configure *Windows Authentication - NTLMv2* with LDAP authorization, first enter the LDAP settings and then the authentication settings for Single Sign-on through Windows.

1 Enter the **LDAP Server** information:

- **Server type** and **Security options**
- **Server name** and **Server port** — or — **DNS domain** and **Server port**
- **Username**
- **Password**.

2 Enter the **Directory search base**, and choose **Logical groups** or **Folders**.

3 Enter the **Domain** used to authenticate end users.

4 If desired, click **Password expiration** to set a reminder.

5 Continue with the **Single Sign-on through Windows Authentication Configuration**. Enter the required settings:

    5a **NetBIOS hostname of domain controller**

TIP: To obtain the NetBIOS name for a domain on **Windows Server 2000 or higher**:

1. Open the Active Directory **Domains and Trusts** snap-in (`domain.msc`).

2. In the console tree, right-click the domain and select **Properties**.

3. The **Domain name** (pre-Windows 2000) field displays the `NetBIOS name`.

On Windows Server 2008 or higher, you can also use the Active Directory module for Windows PowerShell to find the NetBIOS name of a domain in Active Directory Domain Services.

On **Windows Server 2008 only**, if the Active Directory module is not available, you may need to install it first, using this PowerShell command:

```
import-module activedirectory
```

This example demonstrates how to find the NetBIOS name of the domain called `mydomain.com`:

```
Get-ADDomain -Identity mydomain.com | findstr /I NetBIOSName
```

5b Computer account (for servicing)

A computer account in the Active Directory domain. A computer account is different than a user account. The computer account should not be associated with an actual physical or virtual computer.

To specify the Computer account for servicing

A computer account's syntax is the pre-Windows 2000 computer name, followed by a `$` sign, followed by the `@` symbol, and then the DNS domain name.

Syntax: `<Computer name (pre-Windows 2000)>$@<DNS domain name>`

For example, if the Computer name is `ReflServiceAccount`, the pre-Windows 2000 Computer name is `REFLSERVICEACCO` and the **computer account** is: `REFLSERVICEACCO$@mydomain.com`

5c Computer account password

If the password of the computer account is not already known, it must be explicitly reset in Active Directory. You can reset a computer account's password using a simple VBScript, or the ADSI Edit tool.

6 Click **TEST CONNECTION**.

This action checks the NTLMv2 connection to be sure the server is listening and is in fact a domain controller. The test attempts to authenticate to the server using the IP address or alias for the domain controller, the NetBIOS hostname, computer account, and password.

Then, the LDAP connection is tested.

Note: The Domain is *not* tested and could still cause an error later in the authentication process. If the result is **Success**, click OK and continue with your setup.

If **TEST CONNECTION** fails, the message specifies whether check the NTLM or the LDAP server connection failed. Check the logs and resolve the issue before continuing.

7 **Advanced Settings**: For the **Maximum nested level for groups**, accept the default (5), or change the number.

8 Click **OK**.

9 To add another server, see Adding Another Server for Windows Authentication NTLMv2.

- Configure Windows Authentication - NTLMv2 (without LDAP)
- Adding Another Server for Windows Authentication NTLMv2

Adding Another Server for Windows Authentication NTLMv2

You can add one or more Active Directory servers to use Windows authentication with or without LDAP authorization.

1. **Prerequisite:** The property must be set to enable multiple LDAP servers—*even if you do not use LDAP to restrict sessions*. See Enabling Multiple LDAP Servers.

2. On the **Configure Authentication** panel, verify that this method is selected:
   - Single sign-on through Windows authentication

3. Select the Authorization method for this server:
   - **Allow all authenticated users to access all sessions**
   - **Use LDAP to restrict access**

4. Click **+ADD** under **Servers** (or **NTLM Servers**).

5. Continue with the steps for the selected type of authorization:
   - Configure Windows Authentication - NTLMv2 (without LDAP)
   - Use LDAP to restrict access to Window Authentication - NTLMv2 sessions

Related Topics

- Manage Sessions
- Assign Access
- LDAP Configuration

X.509 Configuration

Use this configuration to enable users to authenticate with X.509 client certificates, and then automatically connect to a host session. Optionally, you can specify settings to fall back to LDAP authentication if certificate-based authentication fails.

- "Pre-requisites" on page 80
- "Authentication Settings" on page 80
- "Certificate Revocation Checking" on page 81

Pre-requisites

See X.509 Certificates - Setup Requirements to be sure the requirements for this authentication scheme are met.

Authentication Settings

LDAP options for authentication

- **Fallback to LDAP authentication**

Use this option to prompt the user for LDAP credentials when certificate-based authentication fails.

- **Validate LDAP User Account**

Account validation is always enabled and causes authentication to fail when an LDAP search fails to resolve a Distinguished Name (DN) for the name value obtained from the user's certificate. If you are using Microsoft Active Directory as your LDAP server type, additional validation is performed. User authentication will fail when the user's Active Directory account is either disabled or expired.

- **Distinguished Name Resolution Order**

The values in this property can be re-ordered, added, or removed. Items are listed in order of preference. For example, to locate the **User Principal Name** of the certificate before checking other values, enter `upn, email, cn_val, cn`.

- **UPN Attribute Name**

This property is used only when `upn` is present in the **Distinguished Name Resolution Order** field; otherwise this property is ignored. The User Principal Name (UPN) is an Internet -style login name and generally takes the form `auser@domain.com`.

The **UPN** value is retrieved from the **Subject Alternative Name** field in the user's certificate. The Administrative Server then performs a search for an LDAP user object, based on the UPN attribute name and value, to validate that the user object exists in the LDAP database. The LDAP search filter takes the form of (`upn-attribute-name=upn-value-from-certificate`). For example: `userPrincipalName=auser@domain.com`.

Enter the name of the **LDAP attribute** used in the LDAP directory where the UPN-style name is stored. If the LDAP Server type is Microsoft Active Directory, use the default UPN attribute name: `userPrincipalName`. Other LDAP implementations may use a different attribute name, such as `email` or a custom name.

Client options

- **Login Timeout (optional)**

This setting logs the date and time of the user's logon to the specified LDAP attribute.

Enter any available single value LDAP attribute, such as `wWWHome` (if using Microsoft Active Directory), or enter a custom single value LDAP attribute created by the LDAP administrator.

- **Custom Message when Authentication Fails (optional)**

When authentication fails, the user sees the default message, "The attempt to authenticate using a certificate or smart card has failed."

You can append the general message with customized text. To do so, use \n to begin a new line. For example, to add a Help Desk number, enter

```
\n\nFor further assistance:\n 1. Click OK to log on with User name and
Password.\n 2. Call the Help Desk at 411-555-1212.
```

 ◆ **Custom PIN Prompt (optional)**

Use this field to add custom text to the **Enter PIN** dialog prompt. For example, `Enter your smart card PIN`.

Allowed source of certificates for Reflection for the Web clients

Applies to: Reflection for the Web

 ◆ Select **Hard certificates** to use smart cards as an alternative to permanently installing client certificates on local hard drives. This option simplifies user authentication and prevents the unauthorized capture of passwords over networks. For more information, see Smart card settings

 ◆ Select **Soft certificates** to use certificates stored on the client's computer for X.509 authentication. The user's certificate must be included in a keystore named `usercert.pfx`.

The admin must copy `usercert.pfx` to the preference files directory on a client workstation, typically in `C:\Users\<username>\AppData\Roaming\mfmss`.

When soft certificates are enabled, X.509 authentication proceeds as follows:

1. The browser on the client is used to browse to the Administrative Server (`https://<servername>:<port>/rweb`).

2. During X.509 authentication, the launcher checks for the `usercert.pfx` file before checking for a smart card.

3. When the `usercert.pfx` file is found in the preference files location on the client, either

   X.509 authentication completes and the user's list of links displays

   – or –

   an **Enter Passphrase** dialog box opens, if required for `usercert.pfx`. Once the user enters the correct passphrase, X.509 authentication completes and the list of links displays.

Certificate Revocation Checking

Changes to the certificate revocation checking settings below do not take effect until the server is restarted.

NOTE: If you enable both OCSP and CRL checking, then OCSP will always be tried first. If the revocation status cannot be determined using OCSP, the validation will fall back to using CRL.

Enable Online Certificate Status Protocol (OCSP)

The **Online Certificate Status Protocol (OCSP)** is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

Use this option to specify Online Certificate Status Protocol (OCSP) settings that verify the TLS client certificate chain. OCSP is an alternative to Certificate Revocation Lists (CRLs), and is often implemented in a Public Key Infrastructure (PKI).

An OCSP server, also called a responder, may return a signed response signifying that the certificate specified in the request is good, revoked, or unknown. If it cannot process the request, it may return an error code.

Enable OCSP

Check this box to enable and configure OCSP options. The OCSP responder's signing certificate is checked using the same settings as the rest of the certificate validation.

Use Authority Information Access (AIA) Extension

The Authority Information Access (AIA) extension indicates how to access Certificate Authority information and services for the issuer of the certificate in which the extension appears. When enabled, the OCSP server URL specified in the Authority Information Access extension of a certificate is used to check the certificate revocation status using the Online Certificate Status Protocol.

Additional OCSP Responders

In addition to the URLs from the AIA extension, you can specify the URLs (separated by a space) of other OCSP responders. If you clear the Use AIA Extension check box, or if the certificate does not contain an AIA extension, only the URLs in this text box will be used. HTTP URLs are supported.

Example: `http://ocsp.example.com`

Enable Certificate Revocation List (CRL)

Use this option when the revocation status cannot be determined using OCSP.

Enable CRL

Check this box and enter the URLs of Certificate Revocation List issuers to be used for certificate verification. These are the URLs that your Security Proxy server is set to use when checking the user's client certificate. Enter each URL, separated by a space. LDAP and HTTP URLs are supported.

Use CRL Distribution Point (CRLDP) Extension

The CRL Distribution Point (CRLDP) extension indicates how to access Certificate Authority information and services for the issuer of the certificate in which the extension appears. When enabled, the CLR server URL (specified in the CRLDP extension of a certificate) is used to retrieve the Certificate Revocation List.

Additional CRL Issuers

In addition to the URLs from the CRLDP extension, you can specify the URLs (separated by a space) of other CRL issuers. If you clear the Use CRL Distribution Point checkbox, or if the certificate does not contain a CRLDP extension, only the URLs in this text box will be used.

Examples:

`ldap://myCAServer.example.com/CA/certificaterevocationlist`

`http://server1.example.com/CertEnroll/server1.example.com.crl`

SiteMinder Configuration

Management and Security Server uses Microsoft IIS to integrate with SiteMinder. For instructions on how to integrate IIS with MSS and if needed, Host Access for the Cloud, see Configure Single Sign-on through IIS .

If you selected SiteMinder as your authentication method, complete the configuration:

 ◆ **Agent version**

   Some configurations vary depending on the version you select.

 ◆ **Agent name**

   The name of the SiteMinder agent that is used by IIS. This is the **Name** of the agent configured to work with IIS that is integrated with the Management and Security Server.

 ◆ **Configuration file (version 5+)**

   Provide a full path to the SiteMinder host configuration file. This is typically `SmHost.conf` and resides in the `config` directory in the SiteMinder web agent installation directory.

 ◆ **Shared secret (version 4)**

   The secret used by the policy server to verify the agent. This is the Shared secret that was created in the SiteMinder Administration tool under System Configuration > Agents.

 ◆ **Policy server host (version 4)**

   The IP address (preferred) or DNS name of the host on which the SiteMinder policy server is installed.

 ◆ **Authentication port (version 4)**

   The SiteMinder policy server's authentication port. The default for this port is 44442. To check the port number, open the SiteMinder Policy Server Management Console, click the Settings tab, and look for the Authentication port number under Access Control. If other SiteMinder port numbers were changed from their defaults, you must reset the corresponding port numbers in the Management and Security Server PropertyDS.xml file, located in the MSSData folder.

 ◆ **User identity**

   Determines which SiteMinder user attribute is displayed in the list of sessions and used for LDAP authorization.

 ◆ **User identity LDAP search attribute (optional)**

   When the Administrative Server is configured to use authorization, use this field to specify the LDAP attribute used by the Administrative Server to perform an LDAP search request for the user's distinguished name (DN). During authorization, the Administrative Server issues an LDAP search request to obtain the user's LDAP DN. The LDAP search request's filter uses the attribute specified in this field.

   For example, if you enter the value "uid" into this field, then the LDAP search filter will look like: (uid=<SiteMinder username>) where <SiteMinder username> is the value of the SiteMinder user's name, obtained from the SiteMinder session token, using the ATTR_USERNAME key. Example: (uid=johns)

   NOTE: When the Administrative Server is not configured for authorization, any value entered in this field is ignored.

SiteMinder and 64-bit systems

If you're using a 64-bit operating system, check to be sure that the `PATH` variable places the path to the 64-bit libraries before the path to the 32-bit libraries. To confirm the order, open a command window and type: `echo %PATH%`.

If the 64-bit libraries are not first in the path, then edit the `PATH` variable so that the path to the 64-bit libraries comes before the path to the 32-bit libraries.

Related Topics

- Assign Access
- Add and Launch a session

Micro Focus Advanced Authentication

Advanced Authentication™ is a separate Micro Focus product that provides a multi-factor authentication solution to protect your sensitive data by using a chain of authentication methods.

Management and Security Server provides an optional Add-on to use the multi-factor capability. To enable the Advanced Authentication option, you must have both products installed and configured.

In brief, you must

- "Step 1. Install and configure the Micro Focus Advanced Authentication product" on page 85
- "Step 2. Download the Advanced Authentication Add-on activation file." on page 85
- "Step 3. Configure Management and Security Server to use Advanced Authentication" on page 85

Follow the detailed steps.

Step 1. Install and configure the Micro Focus Advanced Authentication product

You can configure a chain of multiple authentication methods by using Micro Focus Advanced Authentication.

Refer to the **Advanced Authentication Documentation** to install and configure the product.

When configuring the Advanced Authentication product to work with Management and Security Server, these steps are required.

1 **Install** Micro Focus Advanced Authentication Server, noting the server name (or IP address).

2 Configure the authentication **Methods** you wish to use for MSS authentication.

   Options include LDAP password, Email one-time password (OTP), Time-limited one-time password (TOTP), Smartphone, and more.

3 Create a **Chain**.

   Add your preferred methods in the order you want the user to encounter them as they log in.

4 Configure a **customized Event** and name it **MSS**.

The event name must match the hard-coded setting in Management and Security Server; thus, the name must be `MSS`.

A different name will not work.

Step 2. Download the Advanced Authentication Add-on activation file.

After you obtain the separate license for **Host Access Management and Security Server - Advanced Authentication Add-On**, go to the **Micro Focus download page** (where you downloaded Management and Security Server).

Download the **activation file**, named `activation.advanced_authentication-<version>.jaw`.

Step 3. Configure Management and Security Server to use Advanced Authentication

In the MSS **Administrative Console**, first upload the activation file, and then establish trust between the Advanced Authentication server and the Management and Security Server.

Upload the activation file:

1 Log in to **Management and Security Server**.

2 Open the Administrative Console to **Configure Settings - Product Activation**.

3 Click **ACTIVATE NEW**.

4 Browse to and click the activation file you downloaded earlier: `activation.advanced_authentication-<version>.jaw`.

The file is installed and added to the list of **Currently Installed** products.

Establish trust between the **Advanced Authentication** server and the **Management and Security Server**:

1 In Management and Security Server, open **Configure Settings - Authentication & Authorization**.

2 Select **Micro Focus Advanced Authentication** as the authentication method.

If desired, select **LDAP** as the authorization method.

3 Import the Advanced Authentication server's certificate:

3a Enter the **Server** name or IP address of the Advanced Authentication server, noted earlier, **without** a protocol. (That is, omit `https://`.)

For example, enter `myserver.mycompany.com`.

Note: The Advanced Authentication server uses **Port 443**, the default.

3b Click **IMPORT CERTIFICATE**. A message displays to confirm whether the server is trusted.

NOTE: If you are presented with multiple certificates to import, it is best to choose the CA certificate.

If you see, "**Failed to retrieve the certificate chain for the server**," be sure the server name is entered correctly. The host name must match the name in the server certificate.

4 By default, the **Verify server identity** option checks to make sure the host name is matched with the certificate from the Advanced Authentication server.

Note: When present, the SAN (Subject Alternative Name) in the Advanced Authentication server certificate is used, not the common name.

CAUTION: Clearing the **Verify server identity** check box is a security risk. Do not disable this feature unless you understand the risk.

---

5 With **Verify server identity** checked, click **TEST CONNECTION**.

The test is successful when the entry for the Advanced Authentication server is valid, and the server address is in the certificate.

If the test connection fails, troubleshoot as follows:

- If you see, **Advanced Authentication Failure - The hostname you entered does not match the server certificate**, check the certificate in the **Configure Settings - Trusted Certificates** list.

  Then, return to **Configure Settings - Authentication & Authorization** and correct the server name to match the SAN in the certificate.

  For instance, a mismatch occurs when you enter the IP address, and the IP address is not in the certificate.

- For more information, see `trace.0.log`. By default, `trace.0.log` is located in `\ProgramData\Micro Focus\MSS\MSSData\log`.

  Use the **LogViewer** utility to view the trace log file. See Using Log Viewer.

6 When **TEST CONNECTION** succeeds, you are ready to use Advanced Authentication.

NOTE: If the first authentication request from MSS to the Advanced Authentication server fails, restart the MSS server to enable subsequent requests to succeed.

SAML Authentication

SAML (Security Assertion Markup Language) is an XML-based open standard format that exchanges authentication and authorization data between an **identity provider*** and a **service provider****.

This release supports **SAML v2.0 Web Browser SSO Profile** for Host Access for the Cloud 2.4 or higher.

Configuring Management and Security Server (MSS) to use SAML is a multi-step process.

In general, you must

- ❒ Configure MSS as a SAML service provider.
- ❒ Download or access the service provider's metadata from MSS.
- ❒ Export the service provider's metadata into the identity provider.
- ❒ Map the identifier source.
- ❒ Configure the SAML whitelist.
- ❒ Configure LDAP, when used for authorization.

* identity provider:	the server that issues SAML assertions and performs authentication on behalf of the service provider.
** service provider:	the web server from which you access information or services. MSS acts as the service provider.

Follow the **SAML Configuration steps**.

SAML Configuration steps

Be sure to read the Important information, Cautions, and Notes as you configure MSS to use SAML.

IMPORTANT: The SAML authentication scheme in MSS relies on HTTP session cookies for proper operation. Consistent use of fully-qualified DNS names across all SAML entities is strongly recommended. In particular, any clients of MSS should be configured to access MSS using the same DNS name that is used for the Assertion Consumer Service prefix URL.

Follow these steps:

- Configure MSS as a SAML Service Provider
- Advanced SAML Service Provider Settings
- Identity Mapping
- SAML whitelist
- LDAP Servers
- Troubleshooting SAML setup

Configure MSS as a SAML Service Provider

These steps are required before you can download the service provider's metadata.

1 Import the **identity provider's metadata** to MSS (the service provider).

Click **IMPORT** and enter the file name or the HTTP endpoint (a URL). You may need to consult with your SAML administrator to locate the metadata.

After importing, click **APPLY** to store the metadata.

Note: The colored box under the IMPORT button displays the status of the identity provider (IdP) metadata: not stored, imported, or stored.

2 Enter the service provider SAML **Entity ID**. The entry can be either a **URL** (preferred) or a **URN** for your installed Management and Security Server.

URN examples: `com:company:hostname:sp`, `com:microfocus:mssprod:sp`

3 Enter the **SAML Assertion Consumer Service prefix URL**.

This entry is the prefix URL for the MSS endpoint that handles SAML assertions. At runtime, this prefix is used to build the web endpoint for the SAML assertion consumer service (SACS) and will resolve to `<prefix URL>/callback`.

For example, if your prefix is `https://hostname.domain.com/mss`, then at runtime, the assertion consumer service will be `https://hostname.domain.com/mss/callback`

CAUTION: The value specified for the prefix URL must meet this requirement. If you encounter an error message, be sure this requirement is met.

- The prefix URL value **must end** with the MSS server's **web application context**.

  For example, the default context is `/mss`.

---

4 Click **APPLY**.

The **Download** button is enabled when these values have been specified and applied:

- Identity Provider metadata
- Service Provider SAML Entity ID
- SAML Assertion Consumer Service prefix URL

5 **Sign Requests**. Check this box to sign the SAML service provider requests made by MSS.

NOTE: If needed, a different private key and/or certificate may be specified in the keystore named `saml.bcfks`, located in the `MSSData` directory. You can manage this keystore with Java's KeyTool.

When the `saml.bcfks` keystore is changed, restart MSS, and then repeat the steps to **Download** the service provider (MSS) metadata and **EXPORT** it to the identity provider.

---

6 Download or access the service provider (MSS) metadata.

Use the **Download** button or the HTTP endpoint defined in the **Export service provider's metadata** field.

7 Export the service provider's metadata to the identity provider.

Refer to your identity provider's documentation to complete these steps:

7a Upload the service provider metadata to the identity provider.

7b Configure the identity provider to trust MSS (the service provider).

Advanced SAML Service Provider Settings

Set these values in `MSS/server/conf/container.properties`:

- `saml.max.authentication.lifetime`

Default is **86400** (seconds), which equals 24 hours. By default, the SAML client will accept assertions based on a previous authentication for 24 hours.

Note: There are two types of timeouts on the identity provider (IdP) side:
— session timeout, based on the last login timestamp
— idle timeout, based on the last user's action timestamp

To prevent user sessions from timing out unexpectedly, use one of the recommended values for `saml.max.authentication.lifetime`.

Recommended Values

Platform	saml.max.authentication.lifetime (seconds)
ADFS	28800
Okta	2592000
Azure	2592000

- ◆ `saml.wants.assertions.signed`

  Default is **true**. By default, assertions are signed, but this property can be disabled by setting it to false.

- ◆ `saml.path.parameter.callback.url.enabled`

  Default is **true**. Set to false to use query parameter in the callback url.

Identity Mapping

The SAML assertion provides values that can be used as the source for the user identifier. When LDAP authorization is enabled, you could use the LDAP user identifier.

Choose your preferred sources to identify and authorize each user.

User identifier source

Choose a value from the SAML assertion. *Note*: The user identifier appears in the user interface.

- ◆ **Assertion subject**. Use the SAML assertion's Subject name identifier as the user identifier.
- ◆ **Assertion attribute**. Enter a SAML assertion attribute name to use as the source for the user identifier.

Distinguished name source (for LDAP authorization)

Choose whether to use the LDAP source or a value from the SAML assertion.

- ◆ **LDAP**. Use LDAP when the user's identifier is unique within LDAP.
- ◆ **Assertion subject**. Use the SAML assertion's Subject name identifier as the user's distinguished name for LDAP authorization.
- ◆ **Assertion attribute**. Enter a SAML assertion attribute name to use as the source for the user's **distinguished name** for LDAP authorization.

SAML whitelist

MSS uses a whitelist composed of trusted host names to mitigate a potential security vulnerability when using SAML authentication. By default, the SAML whitelist is enabled and contains the registered Host Access for the Cloud session servers and the MSS host itself.

NOTE: The SAML whitelist is restrictive by default. That is, if a user specifies a valid host name in the URL — but that host name is not in the whitelist — the end-user browser application will not be able to use SAML.

For example, the user may specify a numeric IP address in the browser, but by default, numeric IPs are not whitelisted. When an untrusted host name is specified in the browser URL, an HTTP 403 error is returned, and the browser content indicates that a technical error has occurred. The Trace log file will also contain a Warning message indicating that a request was received that is "not from a host in the SAML whitelist."

To configure the SAML whitelist:

1 Check **Enable SAML whitelist** (the default).

   For troubleshooting purposes, the SAML whitelist can be disabled.

2 Enter **alternative host names** to include in the SAML whitelist.

   Specify any alternate host names for the SAML client application hosts, such as a short host name, a fully-qualified DNS name, or a numeric IP address. Separate the host names with a space.

LDAP Servers

Verify or edit the configuration of your **LDAP Servers**.

Troubleshooting SAML setup

If you encounter this issue, follow the steps to resolve it.

   ◆ **Unable to log in or authenticate**

   Look for error messages in the MSS trace log: `\MSS\MSSData\log\trace.<n>.log`.

   If you see, "*Authentication issue instant is too old or in the future*," the saml token has expired.

   Resolution:

   ◆ Close all the browser instances and try to log in again. This action creates a new saml token.

   ◆ Update the `saml.max.authentication.lifetime`, according to the recommended values in the Advanced SAML Service Provider Settings.

Related Topics

   ◆ LDAP Server Configuration

   ◆ Authentication & Authorization

Product Activation

View the list of activation files for currently installed MSS add-on products and emulator clients that are centrally managed by Management and Security Server.

The activation files enable communication with MSS. For more information, see the Activation Files topic in the MSS Installation Guide.

Use this panel to upload the activation files for MSS add-on products or other emulators.

- ◆ "Install an additional product" on page 91
- ◆ "Complete the activation" on page 92

NOTE: If you see this message, "`Activation files installed on the Management and Security Server do not match those available to emulator client sessions,`" resolve the conflict either by

- ◆ manually copying the activation files installed in the `WEB-INF/lib/modules` folder of the Administrative Server to the `ex/modules` folder of the emulator client so the contents of both locations match
- ◆ or, by reinstalling the file using **ACTIVATE NEW** on the **Configure Settings - Product Activation** panel.

Install an additional product

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

   `activation.<product_name-version>.jaw`

2 Download the activation file and note the download destination.

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

4 Click **ACTIVATE NEW** and browse to the activation file for the product you want to install:
   `activation.<product_name-version>.jaw`

5 Click the file. The new product is added to the Product list.

   If you uploaded a product evaluation file, open the column chooser ⊞ to view the Expiration date.

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 MSS server.

   Management and Security Server displays the required configuration settings.

7 Be sure to Complete the activation.

CAUTION: Check this list to avoid issues when upgrading or using Clustering.

- ◆ When upgrading an add-on product or emulator, add the new activation file(s) and be sure to remove the older ones.
- ◆ If you cluster servers for high availability, you must install or update the activation files on *each* clustered node. Activation files *are not replicated*.

Complete the activation

After the activation files are uploaded, further configuration may be required to complete the installation.

Click your product and follow the steps to complete the activation.

- "Security Proxy Server" on page 92
- "Terminal ID Manager" on page 92
- "Automated Sign-On for Mainframe" on page 93
- "Micro Focus Advanced Authentication" on page 93

Security Proxy Server

1 Copy the activation file, `activation.security_proxy-12.8.<n>.jaw`, into the `/securityproxy/lib/modules` folder on each machine where Security Proxy Server is installed.

2 Start the **Security Proxy Server**.

3 To configure the Security Proxy Server, refer to Using the Security Proxy Server (a technical reference in the MSS Help).

Terminal ID Manager

1 Copy the activation file, `activation.terminal_id_manager-12.8<n>.jaw`, into the `Micro Focus/MSS/server/web/webapps/tidm/WEB-INF/lib/modules` folder on each machine where Terminal ID Manager is installed.

2 Restart the Terminal ID Manager servlet.
   - If the Terminal ID Manager servlet is running under Tomcat, then restart the Tomcat server.
   - If the Terminal ID Manager is running under a different application server, follow the procedures for that application server to restart the Terminal ID Manager servlet.

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

   2a Open **About** > **Product Information**. Find the **MSS Data Path**.

   2b In the `MSSData` directory, open `rweb.properties`, and look for this line:
   `idmanagement.enabled=false`

   2c If the enabled value is `false`, change the value to `true`.

   2d Save the file, and then restart the Terminal ID Manager servlet as described above.

Automated Sign-On for Mainframe

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

2 Check **Enable automated sign-on to mainframe sessions**, and enter the required information. See Help for assistance.

3 See the Automated Sign-on for Mainframe - Administrator Guide for the required mainframe configuration.

Micro Focus Advanced Authentication

1 In the **Administrative Console**, open Authentication & Authorization.

2 Click **Micro Focus Advanced Authentication**, and enter the required information. See Help for assistance.

Automated Sign-On for Mainframe

Automated Sign-On for Mainframe enables an end user to automatically log on to a mainframe host application using a terminal emulation client.

Note: An LDAP directory is required for user authorization.

Settings must be configured on:

* Management and Security Server — to secure the server connections and manage user access
* the terminal emulation client — to create the login macro and configure the client
* z/OS — to support the use of PassTickets

Refer to the Automated Sign-on for Mainframe - Administrator Guide for the configuration needed in the client and on z/OS.

Continue with **Configure Settings - Automated Sign-on** in Management and Security Server.

- Automated Sign-on for mainframe sessions
- DCAS Servers
- Secondary LDAP directory
- User Principal Name (UPN)
- Search filter used with secondary LDAP directory
- Check the client settings

Automated Sign-on for mainframe sessions

Check **Enable automated sign-on to mainframe sessions** to display the required configuration fields.

Then enter the required settings:

- DCAS Servers
- Secondary LDAP directory
- User Principal Name (UPN)

DCAS Servers

The DCAS (Digital Certificate Access Server) configuration is used to obtain a PassTicket from the mainframe.

The configured DCAS servers are listed. From here you can:

- "Add a DCAS server" on page 94
- "Edit an existing DCAS server" on page 96
- "Test the Connection" on page 96
- "Set a Preferred DCAS server" on page 96
- "Delete a DCAS server" on page 96

Add a DCAS server

Click **+ADD** and enter the details for the **DCAS Server Configuration**.

NOTE: Check with your mainframe host administrator regarding the required DCAS settings.

- Each DCAS server must be configured to accept client connections from the Administrative Server,
- Several keystores must be correctly configured for client authentication. For details, see Configuring DCAS and RACF on z/OS in the *Automated Sign-On for Mainframe - Administrator Guide*.

To configure MSS for automated sign-on, you need the DCAS server name, port, and the source where the mainframe user names are stored.

Server name

Enter the name of the DCAS server.

Server port

The default port is 8990; however, the DCAS server can be configured to use any port.

Client certificate used to authenticate to DCAS server

Choose which certificate to use for client authentication of the MSS Administrative Server to the DCAS server.

- **Use Management and Security Server certificate**

  This option uses the Administrative Server's certificate and private key (configured on the **Configure Settings - Certificates** panel).

♦ **Use custom keystore**

This option uses a separate keystore that contains a certificate and private key.

1. Enter the **Keystore filename** with the correct extension. The keystore can be one of these formats:

   ♦ Java keystore: `.jks`

   ♦ PKCS#12 keystore: `.p12` or `.pfx`

   ♦ Bouncy Castle BCFKS keystore: `.bcfks`

2. Enter the (case-sensitive) **Keystore password** used to read the keystore.

   The password for the keystore and the private key **must be the same**.

3. The keystore must be placed in the `MSSData\trustedcerts` folder.

   The default Windows location is

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

Verify server identity

Check this box to verify the hostname entered in the **Server name** field against the certificate received from the DCAS server when a secure connection is made from the Administrative Server to DCAS.

Test Connection

Click this button to test the connection between the MSS Administrative Server and the DCAS server.

Using multiple DCAS Servers

You can configure more than one DCAS server for automated sign-on. Repeat the steps to Add a DCAS server. Then, you can Set a Preferred DCAS server.

Edit an existing DCAS server

Select a server, click **EDIT**, and adjust the settings as needed. Click **APPLY**.

Test the Connection

Select a server click **TEST CONNECTION** to test the connection between the MSS Administrative Server and the DCAS server.

Set a Preferred DCAS server

When multiple DCAS servers are configured, you can select a preferred one that will be used most often when assigning sessions. Select your preferred DCAS server, and click **SET PREFERRED**. A star

★ appears next to the name of the preferred DCAS server.

When you assign access to an automated sign-on session, the preferred server will be highlighted; however, you can choose any of your configured DCAS servers.

Related topics

- Secondary LDAP directory
- User Principal Name (UPN)

Delete a DCAS server

Select the DCAS server, and click **DELETE**. When sessions are assigned to use this DCAS server, a dialog lists the assigned sessions.

If only one DCAS server is configured, all of the session assignments will be removed. You can cancel this action in the confirmation message.

If multiple DCAS servers are configured, you have the option to either remove or re-assign the sessions. To change the session assignments, select a different DCAS server from the drop-down list.

Secondary LDAP directory

Mainframe usernames may be stored in a secondary LDAP directory, which can be different from the directory used for authentication.

Check **Enable secondary LDAP server** to display the configuration fields for a separate LDAP server.

When enabled, the search filter on the secondary LDAP directory can be used in **Assign Access** to authorize users or groups to access specific sessions. When this check box is cleared, the search filter option in the Assign Access is unavailable.

Enter the settings for your secondary LDAP server.

- "Server type" on page 97
- "Security options" on page 97
- "Server name" on page 97
- "Server port" on page 98
- "Username and Password" on page 98
- "Search Base" on page 98
- "Certificate" on page 99
- "Validate LDAP Connection" on page 99

Server type

Select the type of LDAP server that is used to store your mainframe usernames. The options on this panel change depending on the LDAP server type you select. If you do not see your specific LDAP server in the list, select **Generic LDAP Compliant Directory Server (RFC 2256)**.

Security options

Data can be passed between the Administrative Server and the LDAP server as clear text or encrypted. The type of encryption used depends on your LDAP server. TLS is available for all server types, and Kerberos v5 is available for Windows Active Directory.

- **Plain Text.** By default, Management and Security Server transmits data between the Administrative Server and the LDAP server in clear text. If you choose this option, you should prevent users from accessing the network link between these two servers.

- **TLS.** When using TLS as the security option for an LDAP server, you must import the server's trusted certificate. Use the IMPORT CERTIFICATE button (below). If you are presented with multiple certificates, it is best to import the CA certificate.

- **Kerberos v5.** When you select Windows Active Directory with Kerberos, you must enter the name of the Kerberos key distribution centers. Multiple key distribution centers, delimited by commas or spaces, can be used. If you do not know the name of the Kerberos key distribution center, enter the fully-qualified DNS name of the Active Directory server.

  The option under the key distribution center name field allows you to encrypt all data transmitted over the Kerberos connection. By default, only user names and passwords are passed securely between the Administrative and LDAP servers using Kerberos. Encrypting all data is more secure, but may increase performance overhead.

Server name

Enter the LDAP server name as either a name or a full IP address. If you selected TLS, this LDAP server name must exactly match the Common Name on the LDAP server's certificate.

Multiple server names, delimited by commas or spaces, can be used for failover support. If an LDAP server is down, the next server on the list will be contacted. In this case, all fields specified on this panel that are used for LDAP connections should be available on all the LDAP servers, and should have identical configurations.

Windows Active Directory - DNS domain. When Windows Active Directory is selected (without Kerberos), you have the option to use a DNS domain instead of a specific domain controller. No further configuration is required. For more information, see LDAP Configuration.

Server port

Enter the port used by your LDAP server. The default is **389** for plain text or **636** for TLS.

If you are using Active Directory, you may wish to set the server port to the global catalog port, which is **3268** (or **3269** over TLS). Global catalog searches can be faster than referral-based cross-domain searches.

Username and Password

Provide the username and password for an LDAP server account that can be used to access the directory in Read-only mode. Generally, the account does not require any special directory privileges but must be able to search the directory based on the most common directory attributes (such as `cn`, `ou`, `member` and `memberOf`). Re-enter the password in the **Password confirmation** box.

NOTE: The **username** must uniquely identify the user in the directory. The syntax depends on the type of LDAP server you are using.

- For **Windows Active Directory** with **Plain Text**, enter

  NetBIOS domain\sAMAccountName (such as `exampledomain\username`)
  userPrincipalName (such as `username@exampledomain.com`)
  or
  distinguished name (such as `uid=examplename,DC=examplecorp,DC=com`).

- For any **other LDAP** server type, enter the **distinguished name** (such as `uid=examplename,DC=examplecorp,DC=com`).

If this account password changes, be sure to update the account password here and apply the new settings. To avoid this problem, you may wish to set up an account that is not subject to automatic password aging policies, or that cannot be changed by other administrators without notice.

Search Base

Directory search base. Enter the distinguished name of the node in the directory tree you want to use as the base for Administrative Server search operations.

Examples: `DC=my_corp,DC=com` or `o=my_corp.com`.

For more information about how to describe the search base, see the LDAP administrator for your organization.

Certificate

Click **IMPORT CERTIFICATE** to import the LDAP server's trusted certificate into the JRE's default trusted keystore. This button displays when **TLS** is selected.

Validate LDAP Connection

Click **TEST CONNECTION** to verify that the secondary LDAP server can connect to the Administrative Server (Management and Security Server).

It the test fails, consult the logs to resolve the issue.

Related topics

- User Principal Name (UPN)
- Search filter used with secondary LDAP directory

User Principal Name (UPN)

An LDAP attribute value in the form of a User Principal Name (UPN) may be used as a direct source for a mainframe username or as an element in a search filter for a secondary LDAP directory.

Enter the name of the **LDAP attribute** in the *authenticating* directory that contains the UPN value. The UPN generally has the form `auser@domain.com`.

Management and Security Server identifies the UPN value used to authenticate, then the portion before the **@** sign is used either

- as the mainframe username itself (when the UPN is selected for mapping directly without the use of a secondary LDAP directory).

    For example, a UPN of `auser@domain.com` would result in the mainframe username of "`auser`" (the portion before the @).

    or

- as an element in a search filter for a secondary LDAP directory.

Related topics

- Search filter used with secondary LDAP directory
- Secondary LDAP directory

Search filter used with secondary LDAP directory

Choose the method for obtaining mainframe usernames from your secondary LDAP directory.

- **Use value derived from the UPN**.

    When using a secondary LDAP directory, "`auser`" is used as the derived value to look up another value in the secondary directory that contains the mainframe username.

    For instance, a search filter could be created for a secondary lookup, where "(`some attribute in 2ndary=auser`)"

    Enter the attribute from the *secondary* directory

- Alternatively, Automated Sign for Mainframe can use a value of another **attribute in the authenticating directory** can be used as the value in the search filter to find the object in the secondary LDAP directory containing the user's mainframe username.

    Enter the attributes for both the *authenticating* and the *secondary* LDAP servers.

Check the client settings

After Automated Sign-on for Mainframe is configured in MSS, be sure the client is configured to use a session with an automated sign-on macro. Then, you can assign access to those sessions.

For details, see the Configuration Workflow in the *Automated Sign-on for Mainframe - Administrator Guide*.

Related topics

- User Principal Name (UPN)
- Reflection/InfoConnect Desktop - Workspace Automated Sign-on
- Search & Assign
- Select the source of the mainframe user name

Metering

Use the options on the **Configure Settings - Metering** panel to set the location of the usage metering server. The options set here are used as defaults for displaying connection activity in the usage reports.

- High Availability
- Add a Metering Server
- Reset Password
- Metering Server Setup
- Client Setup
- Metering Reports

High Availability

The Metering server can be installed on multiple machines and clustered to provide high availability.

A minimum of three MSS servers is recommended for high availability. To configure a cluster, see Clustering.

When multiple metering servers are installed and clustered, emulation clients can continue to function even if a metering server becomes unavailable. Clustering and replication of metering license data is backed by a database.

Add a Metering Server

1 Click **+ADD SERVER** to identify your Metering Server and add it to the table as a direct link.

- **Metering web server name**: Identifies the web server on which the metering server resides. Enter a full server name or the full IP address.
- **Port**: Specifies the port on which the metering server resides. The default is 443 for HTTPS.

- **Metering servlet context**: Specifies the web application context for the metering server.

  This entry is used in the URL for this metering server, and is specified when the metering component is installed. The default, `meter`, is the correct value if you used the automated installer and have only one metering server.

2 Click **ADD** to add the server to the Metering Server Setup table.

The Metering Server is listed as a URL. For example, if the web application context name for your metering server is `meter`, the URL added to the list is

```
https://<servername:port>/meter/AdminStart.html
```

Reset Password

Use this button to reset the Metering administrator password to the MSS Administrative Console password.

1 Check the box for the metering server.

2 Click **RESET PASSWORD**.

If you want to *change* the metering administrator password, open the Metering Console.

1 Click the metering server to open the **Metering Console**.

2 Log in with your current password.

3 Click **Server Settings**.

4 Change the metering administrator password or the Reports Viewer password, as desired.

5 Click **APPLY**.

Metering Server Setup

The default display lists the direct URL for each metering server.

Note: Deleting a server from the list does not uninstall the metering server, but prevents it from appearing in the list of available metering servers when you launch a session from **Manage Sessions**.

1 Check **Use LDAP ID** if you want metering to be based on the LDAP IDs at your site.

2 Click the link to open the **Metering Console** for that metering server.

   You will be prompted for your Metering administrator login.

3 Use the Metering Console to configure settings and license pools for that metering server. Open the Metering Console **Help** for more information.

Client Setup

After the Metering server is configured, the administrator must configure the client software to enable sessions to be metered. Each client is a little different.

For instance,

- In **Host Access for the Cloud**, metering is set globally for all emulation sessions created by the session server.

- In **Reflection for the Web**, the administrator launches the session that is to be metered and enables usage metering on the Administration > Metering Setup dialog.
- In **Reflection Desktop**, the administrator must configure client workstations to report to the Metering server.

Check your client's product documentation to set up Metering.

Metering Reports

After the client sessions are enabled for metering, you can view metering activity in various reports.

From the MSS Administrative Console, click **Run Reports** > **Usage Metering**. Click **SHOW REPORT MENU**, which opens the Metering Console for that metering server.

Or, you can click **Run Reports** directly from the Metering Console. Choose from these reports:

Current Activity
Concurrent Usage
Usage by Attribute
Usage by User or Machine
All Usage Activity
Host Connections

Terminal ID Manager

Terminal ID Manager is a Management and Security Server Add-on product that enables you to conserve terminal ID resources by providing IDs to client applications at runtime.

In addition to setting up Terminal ID Manager in the MSS Administrative Console, further configuration must be done in the **Terminal ID Manager Console** to set up and manage terminal IDs.

Refer to the Terminal ID Manager Guide for the complete set of configuration steps.

Use the options on this panel to set the location of the Terminal ID Manager server.

Enable Terminal ID Manager

On the machine *where Management and Security Server is installed*, open the Administrative Console to **Configure Settings - Terminal ID Manager**.

NOTE: To access the Terminal ID Manager configuration panel in the Administrative Console, you must install the Terminal ID Manager **activation file** on the *same* machine -- even if you installed Terminal ID Manager on a separate machine.

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

If you do not see the **Enable** *check box*, the Terminal ID Manager activation file is not installed. To install:.

    1a In the **Administrative Console**, open **About > Activated Products**.

    1b Click **ACTIVATE NEW**, and upload `activation.terminal_id_manager-12.7.<n>.jaw` from your download location.

2 Enter the **Web server name**.

You can use a full server name or the full IP address.

3 Enter the **Web server port** of the server where Terminal ID Manager was installed.

During an automated installation, the default port is **443** for HTTPS.

4 Note the **Servlet context**. The default is `tidm`.

This entry is used in the URL that accesses the Terminal ID Manager server.

Open the Terminal ID Manager Console

Click the **Server URL** to open the **Terminal ID Manager Console**. You will be prompted for the administrator login.

Note: You can also open the Terminal ID Manager from the **Start** menu.

Use the **Terminal ID Manager Console** to define the server settings and to configure pools to manage terminal IDs. Open Help for assistance.

At first, you may notice a red server status: `Server database not yet configured`. If so, you need to set up the database. Follow the steps in the Terminal ID Manager Console Help.

Once the database is configured, the status changes to green: `Server database available`, and you can continue configuring your Terminal ID Manager.

To complete the configuration, use the Terminal ID Manager Guide.

Clustering

Management and Security Server (MSS) can be configured to provide high availability with a cluster of MSS servers.

NOTE: ***Before you upgrade***— If your environment uses **Replication** in Management and Security Server, all servers must be set to **Standalone** (no Master or Slaves) *before you upgrade to* MSS 12.7 or higher. See Upgrading Replicated Servers in the *MSS Installation Guide* for detailed steps. The upgraded servers can then join a cluster.

    ◆ Configuring Clustering
    ◆ Using a Load Balancer
    ◆ Upgrading Servers in a Cluster
    ◆ Troubleshooting Clustering

Why create a cluster of MSS servers?

The MSS server is installed as a standalone server. While this type of deployment provides full functionality and access to all services, it lacks the attributes to provide high availability and redundancy that remove single points of failure.

By creating a cluster of at least three MSS servers, the data is replicated to each server. If one of the clustered servers goes down, another server can seamlessly provide the data.

What data does *not* get replicated?

All configuration elements of the clustered servers are replicated ***except***:

- Log files
- Activation files. You must install or update the activation files on each clustered node.
- Credential Store settings
- Some Certificates settings (See X.509 Certificates - Setup Requirements)
- The password that unlocks the keychain (See Keychain for details.)
- Package data. If you cluster an MSS server that contains **packages for Windows-based sessions**, the assignments and settings are automatically replicated. However, the ***package data must be manually copied*** to each server.
- The Web Agent name, when **SiteMinder** is used for authentication. The Web Agent name must be set separately for each replicated machine.

Related topics

- "Configuring Clustering" on page 105
- "Using a Load Balancer" on page 110
- "Upgrading Servers in a Cluster" on page 110
- "When using a Security Proxy" on page 111
- "Troubleshooting Clustering" on page 111

Configuring Clustering

To configure your system for high availability, and minimal downtime, we recommend that you create a cluster of at least three MSS server installations. If one of the clustered servers goes down, another server can seamlessly provide the replicated data and reduce the chance of downtime.

NOTE: Check that all ports for each system that will join the cluster are not being blocked by any firewall configuration.

To create, configure, and adjust a cluster:

- Establish the cluster
- Add an MSS server to the cluster
- Monitor Cluster Servers' Status

- Remove an MSS server from a cluster
- Promote an MSS server to MASTER
- Change the database network adapter

Establish the cluster

After installation, an MSS server is not aware of any other MSS servers. Use **Clustering** to create a cluster of connected MSS servers that replicate data to all of the clustered servers.

First decide which MSS servers you want to include in the cluster.

1 Identify the MSS server that contains the configuration settings that you want all of the clustered servers to inherit. Consider this server to be the primary one.

CAUTION: The selection is important because when another server joins the cluster, it loses all of its current configuration settings before acquiring the cluster's settings (replicated from the primary server).

2 Log on to the MSS server you identified as the primary one.

3 Open **About > Activated Products** and note which activation files are present on the primary server. The activation files do not get replicated and must be added to each node.

4 From the Administrative Console, click **Configure Settings - Clustering**.

   In the list of nodes, this MSS server is designated as MASTER in the cluster (MASTER = `true`).

5 Select (or confirm) the **Database Network Adapter**.

   The drop-down list shows each network adapter and its associated IP address. All other database nodes in the cluster must be able to connect to the selected IP address.

   If your system has a single network adapter, that adapter is automatically selected.

6 To add other MSS servers, you need to log on to each of those servers and JOIN them to the cluster. They are *not added* from the MASTER server interface.

NOTE: *This approach is different from configuring* **Replication** *in earlier releases of MSS.*

Add an MSS server to the cluster

Now that a cluster is established, other MSS servers can be added one at a time.

1 Log in to one of the MSS servers that you want to include in the cluster.

2 From the Administrative Console, click **Configure Settings - Clustering.**

3 Click **JOIN CLUSTER** to add this server to the cluster.

4 Enter the address (including port if necessary) of the remote server you want to cluster with.

   If this server is joining a collection of servers that are already clustered, you can enter the address of any of those clustered servers. Click **Next**.

NOTE: When you add a server to a cluster, the server being added will lose all of its current configuration settings. After the **JOIN** process, the added server inherits the configuration settings of the specified server, which is the same for all servers that are already in the cluster.

5 Verify that the certificate presented matches the server you just entered. Click **Next**.

6 Enter the username and password of a user with administrative rights on the server entered in step 5. Click **Next**.

7 The Clustering Progress dialog displays updates as each step is completed.

The full clustering process can take some time to complete. During this time, you will not be able to interact with the Administrative Console. See About the Clustering Process.

8 Once the clustering process is complete, click **OK** to dismiss the dialog.

All servers in the cluster are displayed in the **Management Server Nodes** table, and the one you are logged in to is listed first (at the top).

NOTE: Each server in the cluster is added as a node. Data is replicated to all of the nodes.

- One server is designated as the MASTER (`true`) in the Management Server Nodes table. The MASTER ensures that all nodes in the cluster receive all configuration changes, regardless of which node the change was initiated on.

- Any changes made to the certificate stores (**+ IMPORT** or **DELETE** certificates) will be replicated to the other MSS servers in the cluster. You do not need to repeat the process on each MSS server.

---

9 Open **About > Activated Products** to compare the list of activation files with those on the primary server. To add the activation files, follow the Product Activation steps to "Install an additional product."

10 To add another server to this cluster, repeat steps 1 - 10.

About the Clustering Process

- During the clustering process, certain services provided by the servers in the cluster are automatically restarted. As a result, some MSS functionality is temporarily interrupted during the clustering process.

- Clustered MSS servers and services communicate over a secure TLS channel, which requires server certificates to be exchanged among all the servers in the cluster. This certificate exchange is handled automatically during the clustering process.

- If an error occurs during the clustering process, the progress dialog will note the error. Refer to Troubleshooting Clustering for assistance.

When the cluster is configured, you can adjust the settings to monitor, promote, or remove a server in the cluster.

Once the cluster is established, the servers will synchronize with replicated data.

Monitor Cluster Servers' Status

For troubleshooting and general information, you may want to monitor the status of the clustered servers. To view the servers' status:

1 Log in to the Administrative Console for any server in the existing cluster.

2 Click **Configure Settings - Clustering**.

3 The **Management Server Nodes** table displays all of the servers in the cluster. Note that the server you are logged in to is listed first.

The current status for each server is specified in three columns:

- ◆ **Server Status**

  UP indicates that the management server instance itself is running and pingable. The UP link opens the Administrative Console login screen for that server in a new browser tab. (The server you are currently logged into does not provide an UP link).

  DOWN indicates the server is not currently running.

- ◆ **Service Registry Status**

  UP indicates that the service registry process for that server is running and pingable. The UP link opens the dashboard screen for that service registry instance in a new browser tab.

  DOWN indicates the service process for that server is not currently running.

- ◆ **Database Status**

  UP indicates that the database node associated with that server is currently running. The UP link opens the database cluster information in JSON format in a new browser tab. The database cluster information includes some general information about each database node as well as more specific information about that particular database node.

  DOWN indicates that the database node is not currently running.

NOTE: If the database node for a certain server is not currently running, you will not be able to view the Clustering panel in the Administrative Console on that server.

If you are viewing the Clustering panel, and the database node associated with that server goes DOWN, you will no longer be able to interact with the Clustering UI, but monitoring will continue. In either case, refer to Troubleshooting Clustering for assistance.

Remove an MSS server from a cluster

At times, you may need or want to remove an MSS server instance from a cluster, such as when a server is DOWN.

Note: You cannot remove the designated MASTER server from the cluster. If you need to remove the current MASTER server, you must first promote a different server to MASTER, and then remove the previous MASTER server. (See Promote an MSS server to MASTER.)

To remove an MSS server from a cluster:

1 Log into the Administrative Console for any server in the existing cluster.

2 Click **Configure Settings - Clustering**.

3 In the **Management Server Nodes** table, select the server to be removed.

4 Click **REMOVE** (above the Management Server Nodes table).

5 Click **OK** in the confirmation dialog.

6 A progress screen displays updates as each step of the removal process is completed.

The removal process can take some time to complete. During this time, you will not be able to interaction with the Administrative Console.

When a node is removed, its certificates are removed from the cluster.

7 Once the removal process is complete, click **OK** to dismiss the dialog.

The **Management Server Nodes** table reflects the server removal. If you are currently logged into the Administrative Console of the server that was removed, the Management Server Nodes table shows only a single entry of that server.

If you are logged into the Administrative Console of a different server in the cluster, the Management Server Nodes table no longer shows the server that was removed.

NOTE:

- During the removal process, certain services provided by servers in the cluster are automatically restarted. As a result, some aspects of MSS functionality is temporarily interrupted during the removal process.

- A server designated as MASTER in the Management Server Nodes table cannot be removed from a cluster. You must first promote another server in the cluster to be the MASTER server. See Promote an MSS server to MASTER.

- Server certificate cleanup is handled automatically during the removal process, which breaks the trust relationship between the removed server and the rest of the servers in the cluster.

- ⚠ A server with a Server Status of **DOWN** in the Management Server Nodes table can be removed from a cluster, but be aware that this server is **NO LONGER EXPECTED TO BE USED** after removal.

  For best results ALL servers in the cluster should be in the **UP** state when performing a server removal.

Promote an MSS server to MASTER

The MSS cluster configuration requires that one server in the cluster be designated as MASTER. The designated server appears in the **Management Server Nodes** table with a `true` entry in the MASTER column.

The role of the MASTER is to ensure all of the clustered nodes receive all configuration changes, no matter which node initiated the change. Any of the clustered servers could be the MASTER.

One reason to promote a server to MASTER is to be able to remove the currently-designated MASTER. For instance, if the current MASTER server goes **DOWN** and you choose to remove it from the cluster, you must first promote a different server to MASTER to enable the **REMOVE** button.

To change which server is designated as MASTER in an MSS cluster:

1 Log into the Administrative Console for any server in the existing cluster.

2 Click **Configure Settings - Clustering**.

3 In the **Management Server Nodes** table, select the server you wish to promote to MASTER.

4 Click **PROMOTE** (above the table).

5 Click **OK** in the confirmation dialog.

6 The selected server becomes the MASTER, identified with the `true` entry in the Management Server Nodes table. The previous master server simply becomes a node in the cluster, and could be removed, if needed.

NOTE: A **DOWN** server cannot be promoted to MASTER. Either start the server before promoting it, or select a different server in the cluster to promote to MASTER.

Change the database network adapter

At times, you may need to change the database network adapter used by a given server in an MSS cluster.

To change the database network adapter:

1 Log into the Administrative Console of the server whose database network adapter you want to change.

2 Select **Configure Settings - Clustering**.

3 Select the desired **Database Network Adapter** (with its associated IP address) from the drop-down list.

4 Click **APPLY** (at the bottom of the screen).

The database node is restarted with the desired network adapter.

NOTE: If the database node is not currently running, you will not be able to change the database network adapter in the Administrative Console's Clustering view. Refer to Troubleshooting Clustering for assistance.

Related topics

- Using a Load Balancer
- Upgrading Servers in a Cluster
- When using a Security Proxy
- Troubleshooting Clustering

Using a Load Balancer

Once the servers are clustered, you can configure a load balancer in front of your MSS instances for high availability. Use these values:

- **Load balancing algorithm:** Least Connections (or something similar)
- **Session persistence:** To enable session persistence, configure the MSS load balancer to stick on existing cookies and URL parameters *in the order specified below*:
  — Stick on cookie **SESSIONID**
  — Stick on URL parameter **sessid** (only necessary when Single sign-on through IIS is configured as the authentication method)
  — Stick on cookie **JSESSIONID**
  — Stick on URL parameter **jsessionid**
- **Health check endpoint:** `https://<mss-server>/mss/actuator/health`
- **TLS:** Configure TLS and install certificates as needed.

If you are using Host Access for the Cloud, see the Host Access for the Cloud Documentation for additional information about deploying MSS for high availability.

Upgrading Servers in a Cluster

The upgrade process does not preserve the MSS cluster configuration. To upgrade:

1 Remove each MSS server from the cluster.

2 Upgrade each MSS server individually.

3 Log in to each upgraded server and repeat the steps to Add an MSS server to the cluster.

See Configuring Clustering for more information.

When using a Security Proxy

If you are using a Security Proxy server, you must also import the certificates for all of the remote Administrative Servers to *each* Security Proxy server. Use the **Security Proxy Wizard** to import these certificates.

When you create a secure session that connects to a Security Proxy server, the session is thereafter linked to this specific Security Proxy. When this session is replicated to other servers in the cluster, the session is then initiated from a different MSS Administrative Server, but the session itself will still connect to the original Security Proxy for which it was configured.

If client authorization is enabled on the Security Proxy Server, then the Security Proxy Server will only accept connections from sessions initiated from the MSS Administrative Servers it trusts. That is, their certificates are in the Security Proxy Trusted Certificate list.

In order for connections from replicated servers to succeed in this environment, the certificates from every MSS Server in the cluster need to be imported to the Security Proxy server. If there are multiple Security Proxy Servers in the cluster, then this operation needs to be done on each of these Security Proxy Servers.

Related topics

* Configuring Clustering
* Upgrading Servers in a Cluster
* Troubleshooting Clustering

Troubleshooting Clustering

The clustering of MSS server installations requires secure communication among the server nodes and well as the configuration and initialization of sub-services provided by MSS.

If you encounter issues while setting up or using Clustering, try these troubleshooting tips.

* Ports - Ensure that all ports for each system in the cluster are not being blocked by any firewall configuration.
* Logs related to clustering - First, consult the logs on each system in the cluster to help further identify the nature of the issue encountered.
* Common issues - Then, check the common issues for specific errors or problems.

After you make a change, retry the **Join Cluster** process.

Ports

Check the table of Default Port Numbers used by MSS in the *MSS Installation Guide* to look for conflicts.

Logs related to clustering

When trying to diagnose and troubleshoot clustering problems, refer to the logging output on each system involved in the MSS cluster — including systems that already exist in the cluster as well as a system being added or removed.

On each system, look in the `<mss-install>/server/logs` folder for the following log files.

* `container.log` - contains logging out from the MSS server container itself, including the output for each step in the clustering process.
* `cassandra.log` - contains logging output from the cassandra database node included with each MSS server.
* `cassandra-sidecar.log` - contains logging output for the configuration and initialization of the cassandra service that occurs during the clustering process.
* `service-registry.log` - contains logging output from the service-registry service that is included with each MSS server.

For diagnostic purposes, the logging output on each system can be increased. In a working production environment, however, we recommend that you restore the default logging output for performance and resource considerations.

To increase the logging output prior to making clustering configurations:

1 Insert the following lines into `<mss-install>/server/conf/log4j.xml`.

```
<Logger
name="com.microfocus.mss.mgmt.console.viewcomponents.clustering"
level="debug"/>

<Logger
name="com.microfocus.centralmgmt.configuration.controller.clustering"
level="debug"/>

<Logger
name="com.microfocus.centralmgmt.configuration.services.clustering"
level="debug"/>
```

2 Restart the system.

3 After clustering is configured and working properly, remember to restore the default logging output.

Common issues

Try these troubleshooting tips for specific error messages or problems.

- The **database network adapter must be set** before you can join the cluster

  1. Log into the Administrative Console of the specified server.

  2. Click **Configure Settings - Clustering**.

  3. Select the desired **Database Network Adapter** and click **APPLY**

- **Unable to retrieve the server certificate** when running the join cluster wizard

  1. Ensure that the correct server name and secure port are entered in the wizard.

  2. If using a non-default configuration, be sure that the proper servlet context is entered in the wizard.

- **Invalid user name or password**

  Ensure that the credentials entered for the specified server in the **Join cluster** wizard match the credentials of a user with admin rights on that server.

- Failure encountered during the **testing connection step**

  1. Take note of the systems specified in the error message.

  2. Ensure the server address for all systems can be resolved from all other systems.

  3. Ensure that the HTTPS port (default of 443) and system port (default of 8003) is accessible from all systems.

- Failure encountered when **updating the cluster truststore**

  1. Take note of the systems specified in the error message.

  2. Ensure that the `<mss-install>/server/etc` directory is writable.

  3. Ensure that `<mss-install>/server/etc/system-trustcerts.bcfks` can be opened with KeyStore Explorer.

  4. If a non-default configuration is being used, ensure that these properties are set correctly in `<mss-install>/server/conf/container.properties`:

     ```
     servletengine.system.ssl.trustStoreFileName
     servletengine.system.ssl.trustStorePassword
     ```

- Failure encountered when **initializing system ports**

  1. Take note of the systems specified in the error message.

  2. Refer to `servletengine.log` and `container.log` for further diagnostics.

- Failure encountered when **configuring the replication role**

  1. Ensure that the cassandra database is running properly on the system being added or removed from the cluster.

  2. Refer to `cassandra.log` and `container.log` for further diagnostics.

- Failure encountered when **updating the service registry**

  1. Take note of the systems specified in the error message.

  2. Ensure that the file `<mss-install>/server/microservices/service-registry/service.yml` exists and is writable.

- Failure encountered in **any of the database-related steps**

  1. Take note of the systems specified in the error message.

  2. Refer to these log files for further diagnostics:

     `<mss-install>/server/logs/cassandra.log`

     `<mss-install>/server/logs/cassandra-sidecar.log`

     `<mss-install>/server/microservices/cassandra/logs/debug.log`

  3. Ensure that the `<mss-install/server/microservices/cassandra/conf/cassandra.yaml` file exists and is writable.

  4. In `<mss-install>/server/microservices/cassandra/conf/cassandra.yaml`, ensure that:

     — the `listen_interface` property is set to the correct interface name.

     — the `storage_port` (defaults to 7000) and `ssl_storage_port` (defaults to 7001) property files are accessible from all other systems in the cluster.

- **Cannot enter the Clustering view** in the MSS Administrative Console because the **local database node is not running**

  Refer to these log files for further diagnostics:

  `<mss-install>/server/logs/cassandra.log`

  `<mss-install>/server/microservices/cassandra/logs/debug.log`

- The **cassandra database node will not start** because an **invalid `listen_interface`** is configured

  1. In `<mss-install>/server/microservices/cassandra/conf/cassandra.yaml`, be sure that the `listen_interface` property is set to the correct interface name.

  2. If the correct interface name cannot be determined:

     a. Comment out the `listen_interface` property line and uncomment the `listen_address` property line, which should be set to `localhost`.

     b. Search for `-seeds:` and be sure the value is set to "`127.0.0.1`"

  3. Save the file and restart the MSS server. The Clustering view should now be accessible.

4. In the Clustering view, select the **Database Network Adapter** with the IP address that is accessible to all systems in the cluster.

5. Click **APPLY**.

◆ The **SERVER STATUS is DOWN** for one or more nodes displayed in the **Management Server Nodes** table

1. Take note of the server address.

2. Refer to the appropriate log on that system for further diagnostics.

◆ The **DATABASE STATUS is displaying DOWN** for a system where you verified that the database node is running.

Ensure that the system port, configured via the `servletengine.system.ports` property in `container.properties` (default = 8003), is not being blocked by any firewall configurations on that system.

Related topics

◆ What data does *not get replicated?*
◆ Configuring Clustering
◆ Upgrading Servers in a Cluster
◆ When using a Security Proxy

Logging

Management and Security Server stores logs for the MSS microservices, webapps, and other components. The log files are saved in different locations and the properties are set using different configuration files.

Locate the logs of interest and follow the instructions for configuring the properties, as needed.

◆ Locating MSS log files
◆ Configuring the MSS log files

Locating MSS log files

The MSS log files are saved in these sub-directories of your installation location.

◆ \MSS\server\logs\
◆ \MSS\server\microservices\cassandra\logs\
◆ \MSS\MSSData\

\MSS\server\logs\

This location contains log files for MSS microservices and several shared server components.

To configure one of these logs, use its specific **service.yml** file. See Edit service.yml.

cassandra-sidecar\cassandra-sidecar.log
metering\metering.log
service-registry\service-registry.log
cassandra.log
container.log
servletengine.log

NOTE: Some of these logs are helpful when troubleshooting Clustering issues. See Logs related to clustering.

\MSS\server\microservices\cassandra\logs\

debug.log
gc.log
system.log

\MSS\MSSData\

The logs in these directories show information about users' session activity, system configuration activity, and basic trace logging.

idm\log\   for Terminal ID Manager
                 See the Terminal ID Manager Guide to set logging and tracing.
log\   for the MSS Administrative Server
                 See Configure Settings - Logging (below) to set log levels for these files.

NOTE: The **LogViewer** can be used to view the legacy log files under `mssdata\log\`. The LogViewer enables you to set filters, search message text, and change defaults. On Windows, the Log Viewer is available from the Start menu. Click File > Load and select a specific log file, or drag-and-drop the desired log file into the LogViewer and it will load. For more information, see Using Log Viewer.

Configuring the MSS log files

Different configuration files are used to set log levels and other properties in the MSS log files. Follow the instructions for the files of interest.

- Edit service.yml
- Edit log4j2.xml
- Edit logging.properties
- Configure Settings - Logging

Edit service.yml

Each microservice has its own **service.yml** file, which is used to configure logging and other properties for only that microservice. For instance, the service.yml for cassandra is in `<install-dir>\MSS\server\microservices\cassandra\service.yml`.

Use these guidelines for editing a `service.yml` file.

NOTE: When editing *any* **service.yml** file:

  ◆ Lines in service.yml must be indented using spaces.
  ◆ You must restart the server after any changes to service.yml.

Configure log rotation

Verify or edit the default values in **service.yml**. Note: `name` and `value` must be vertically aligned.

```
– name: LOGGING_FILE_MAXSIZE
  value: 10MB
– name: LOGGING_FILE_MAXHISTORY
  value: 10
```

Set logging levels

You can set the logging levels in **service.yml** to produce different types of information. Use the following format, being sure that `name` and `value` are vertically aligned.

```
– name: logging.level.<logger>
  value: "<log level>"
```

Where `<logger>` is the name of the logger to adjust and `<log level>` is one of the following:

  ◆ **Trace** - designates finer-grained informational events than Debug
  ◆ **Debug** - designates fine-grained informational events that are most useful to debug an application.
  ◆ **Info** - designates informational messages that highlight the progress of the application at coarse-grained level.
  ◆ **Warn** - designates potentially harmful situations.
  ◆ **Error** - designates error events that might still allow the application to continue running.
  ◆ **Fatal** - designates very severe error events that will presumably lead the application to terminate.

Remember to restart the server after making changes to service.yml.

Edit log4j2.xml

Located in `<install-dir>\mss\server\conf\`

Use **log4j2.xml** to configure the logging level for the overall service container and services shared among MSS components. You can set the logging level for each <logger>. See the list of values in Set logging levels.

For example, `<Logger name="prefix" level="debug"/>`

Edit logging.properties

Located in `<install-dir>\mss\server\conf\`

Use **logging.properties** to configure `servletengine0.log`, the servlet-engine component of MSS.

Configure Settings - Logging

In the MSS Administrative Console, open Configure Settings – Logging to set logging for users' session activity, system configuration activity, and basic trace logging.

Select logging levels for the log files located in \MSS\MSSData\logs.

- Administrative Server
- Credential store (Reflection for the Web)
- trace.log
- Write client debug output to console

Administrative Server

Set the level of logging for users' session activity and system configuration activity. You can configure the logs to

- log errors and informational messages
- log only errors
- or, disable the log altogether

Location of logs: `\MSS\MSSData\logs\awsaudit.0.log`

Credential store (Reflection for the Web)

Set the level of logging for Credential Store activity. You can configure the logs to

- log errors and informational messages
- log only errors
- or, disable the log altogether

Location of logs: `\MSS\MSSData\logs\credentialaudit.0.log`. You can also open **Run Reports - Credential Store** in the Administrative Console.

trace.log

When analyzing server problems, Customer Support may request that this setting be changed to include debug information. You cannot disable this logging option.

Set the level of logging for the trace log:

- log errors, warnings, and informational messages (the default)
- log errors, warnings, informational, and debug messages
- log errors and warnings

Location of logs: `\MSS\MSSData\logs\trace.0.log`

NOTE: About Log Filenames. The log filename uses the naming convention **logfile.<number>.log**, where **logfile.0.log** is the current file, and previous log files are rolled over to names with numbers greater than zero, such as **logfile.1.log**.

To specify where the sequence number appears in the filename, edit the **log.properties** file by adding the `%g` token in the filename, such as **logfile.%g.log**.

Customizing the logging properties

You can customize the properties logged in trace.log by editing the **log.properties** file in `MSSData\properties`.

For example, use **template_log.properties** to customize logging properties.

1 In the `MSSData\properties` directory, open the **template_log.properties** file.

   The template shows examples of the options that can be changed in log.properties.

2 Use the template file as a reference. (See the commented section.) Or, copy and paste its contents into the log.properties file and modify as needed.

3 When the changes are complete, save the file as **log.properties**.

4 Restart the MSS Server service for the changes to take effect.

Similarly the you can customize the log files for the **Terminal ID Manager**. Go to `mssdata\idm\properties\` and edit **template_log.properties**.

See the technical reference, Using Log Viewer, for more information about customizing and view the log data.

Write client debug output to console

Do not enable this setting unless requested to do so by Customer Support.

When enabled, all subsequent launches of Management and Security Server will send debug information to the console.

6 Run Reports

Reports provide information about Management and Security Server components and products. View the activity for the features you are using.

- "Log File Viewer Reports" on page 121
- "Usage Metering Reports" on page 122
- "Security Proxy Server Reports" on page 122
- "Assigned Access Reports" on page 124
- "Credential Store Reports (Reflection for the Web)" on page 125

Log File Viewer Reports

To view a Log File Viewer Report, make your selections, and click **SHOW REPORT**. The Log File Viewer Report includes information about users' session activity and administrators' configuration activity.

You can change the level of information to be logged on the Logging tab in the Settings tool.

Filters

Choose the type of report and the type of information you want to view.

Report type

- **Management server - User activity:** information about all users' session activities.
- **Management server - System configuration activity:** information about administrators' configuration activities.
- **Credential store activity:** information on the credential store, including who has attempted to access the credential store.

Message type

At least one of these options must be selected for a report to appear.

- **Info:** includes Informational messages
- **Error:** includes all Error messages

Sort field

Select **Date** or **User** to determine how the information in the report will be sorted.

Show Report

Click **SHOW REPORT** to view the activity for the criteria you specified.

In the Log File Viewer Report:

- **Date:** The date of the activity
- **Type:** Informational or Error
- **User:** The login ID of the user or administrator
- **Message:** A detailed description of the event.

   Events described in these reports include logging on and off, logon failure messages, terminal session requests, terminal sessions created, settings changed, and reports requested.

Usage Metering Reports

When you click **Run Reports - Usage Metering** > **SHOW REPORT MENU**, you will first be prompted for your Metering administrator password.

The **Metering Console** opens to **Run Reports**. You can view usage activity in reports when Metering is configured *and* users begin to access metered sessions.

Open **Help** for details about each report.

Security Proxy Server Reports

To view a Security Proxy Server Report, you must first install and configure at least one Security Proxy server -- and be sure the activation file is installed (as described in the MSS Installation Guide).

After you install the Security Proxy server, refer to Using the Security Proxy Server to configure sessions to use the Security Proxy.

To view a report of the Security Proxy server activity, select a **Report Type**, a **Security proxy server**, and click **SHOW REPORT.** *Note:* To add servers to the drop-down list, use the **Configure Settings - Security Proxy** panel to import a Security Proxy server.

Report types:

- "Current user activity" on page 122
- "Security Proxy server logs" on page 123
- "Connections per proxy server" on page 124

Current user activity

This report shows the date and time the report was created and the total number of current connections. The default view shows these results:

- **Start Time:** The time the session connected.
- **Accepted At:** The proxy IP address and port number on which the connection was accepted.

- **Source:** If **Resolve client machine DNS name** is off (the default), this column shows the client's IP address and port number. If client name resolution is on, the client's DNS name and port are displayed.

- **Destination:** If **Resolve remote host DNS name** is on (the default), this column shows the destination host's DNS name and port number. If **host name resolution** is off, the host's IP address and port are displayed.

- **Authorization:** The user or group ID under which the connection was authorized and the web server which authorized the user or group. The format is `<distinguished name>/<web server name>`.

  For example, if the access control model is **None** (end users log on as guest) and the server name is "hostname.example," the Authorization column displays `rwebgroup=guest/hostname.example.com`.

Use the Column Chooser ⊞ to view more results:

- **ID:** The connection identification code. A code is assigned to each active connection at the time the connection is made. The code is constructed from the proxy instance number (p), the thread number (t), the connection number (c), and for FTP connections the session number (s). For example, a code for an FTP connection might be p1t52c8s8: proxy instance 1, thread 52, connection 8, session 8.

- **Client In:** The total number of bytes read from the host during this connection.

- **Server Out:** The total number of bytes written to the host during this connection.

- **Security:** The TLS version and the cipher suite.

- **Protocol:** The protocol (Emulation, FTP, or Pass Through) used in the connection. For FTP connections, the column also shows whether the control channel or active data transfer was involved.

Security Proxy server logs

For the selected Security Proxy server, this report shows each event that occurred from the time the first entry was written in the active log file to the time the report was requested.

Note that by default, the log file has a maximum size of 500 KB; when that size is reached, a new active log is started and this report shows activity from that time. You can change the maximum file size in the **Security Proxy Wizard** > **Logging** tab.

- **Time:** The time at which the log entry was written.

- **Accepted At:** The proxy IP address and port number on which the connection was accepted.

- **Source:** If **Resolve client machine DNS name** is off (the default), this column shows the client's IP address and port number. If client name resolution is on, the client's DNS name and port are displayed.

- **Destination:** If **Resolve remote host DNS name** is on (the default), this column shows the destination host's DNS name and port number. If **host name resolution** is off, the host's IP address and port are displayed.
- **Authorization:** The user or group ID under which the connection was authorized and the web server which authorized the user or group. The format is <distinguished name>/<web server name>. For example, if the access control model is None (end users log on as guest) and the server name is "hostname.example," the Authorization column displays rwebgroup=guest/hostname.example.com.

Use the Column Chooser ⊞ to view more results:

- **Priority:** The priority of the log entry: Info (information), Error, Debug, Audit, or Warn.
- **Protocol:** The protocol (Emulation, FTP, or Pass Through) used in the connection.
- **Security:** The TLS version and the cipher suite.
- **Message:** A short description of the event. The code in brackets at the beginning of each message identifies the action taking place on the proxy server and uses the same format as the ID shown in the Current Activity report.

Connections per proxy server

This report shows the total current connections of all security proxy servers.

- **Security proxy address:** The security proxy server and its associated port.
- **Security proxy current connections:** Tthe count of current connections for that server.

Note: A single FTP session connecting through a security proxy server produces a count of three separate connections.

Assigned Access Reports

Use this report to view your assigned sessions. You can filter by **Users and Groups** or by **Sessions**.

Users and Groups

This report lists all users and groups and the sessions that are assigned to them. The report also indicates whether a user or group has access to the Administrative Console.

Enter a **Search field** string to limit the report to all users and groups that include the search string. The search is not case-sensitive.

Click **SHOW REPORT**.

Sessions

This report lists the sessions and the users and groups that are assigned to that session. Individual members of a group are not listed.

Enter a **Search field** string to limit the report to all sessions that include the search string. The search is not case-sensitive.

Click **SHOW REPORT**.

Credential Store Reports (Reflection for the Web)

- ◆ "Credential Store Users" on page 125
- ◆ "Credential Store Usage History" on page 125

Credential Store Reports are available only for Reflection for the Web. You can filter by User, date, and host.

Credential Store Users

Click **Users** to see a count of credential store users. You can also request a list of credential store users. In this case, the report output includes both the number of users and a list of every user who has credentials stored in the credential store.

When you request the Users report, the resulting report displays the count of Credential Store users. If you select **Show list of users**, the report will include the identity of every user in the credential store.

Credential Store Usage History

Select a date and time range for the usage history report. You can specify day, month, year, and hour for both the From and To portion of the range. Credential store usage can be based on **Access by user** or **Access by host**.

NOTE: Credential store usage reports will be empty when credential store logging is disabled. To enable logging for the **Credential store**, go to **Configure Settings** > **Logging**.

Usage History

In the **Filter string** box, provide a user or host name for the query; then click **Access by user** or **Access by host**. All appropriate names containing that string will be included in the report.

Access by user

When you request the **Access by user** Usage History report, the resulting report displays access by users that match the string specified. The resulting report includes the date of access, the user's identity, the message, and the access category.

If the report is empty, be sure to enable logging for **Credential store** on the **Configure Settings** > **Logging** panel.

Access by Host

When you request a Usage History report for a **host name**, you can also filter by any other string that appears in the message field of the credential store log.

The resulting report displays access to hosts that match the specified string. The resulting report includes the date of access, the user's identity, the message, and the access category.

If the report is empty, be sure to enable logging for **Credential store** on the **Configure Settings** > **Logging** panel.

7 Technical References

Technical References supplement the product Help with overviews and detailed articles.

- ◆ "Using the Security Proxy Server" on page 127
- ◆ "Security Overview" on page 135
- ◆ "Credential stores used in MSS" on page 137
- ◆ "X.509 Certificates - Setup Requirements" on page 141
- ◆ "Using Log Viewer" on page 143

Using the Security Proxy Server

The Security Proxy Server provides token-based access control and encrypted network traffic to and from user workstations. See How the Security Proxy Works.

This article walks through the steps configure and deploy secure sessions using the Security Proxy.

Steps at a glance:

1. Install the Security Proxy Server
2. Configure and Start the Security Proxy Server
3. Import the Security Proxy certificates
4. Create Secure Sessions
5. Assign Secure Sessions
6. Run Reports

Notes about Upgrading

How the Security Proxy Server works

Resources

1. Install the Security Proxy Server

Use the automated installer to install and configure the Security Proxy Server. The Security Proxy can be installed on a different machine. Refer to the MSS Installation Guide for detailed steps.

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

Be sure to check the Security Proxy Server's System Requirements and the Performance and Scaling Requirements.

Next step: Configure and Start the Security Proxy Server.

2. Configure and Start the Security Proxy Server

The Security Proxy Server must be configured to establish trust with the Management and Security Server (MSS). Use the **Security Proxy Wizard** to manage your Security Proxy settings and certificates.

Specifically, the Security Proxy Wizard:

 ⬥ generates or imports the certificate used to authenticate the Security Proxy Server.

 ⬥ sets up a `server.properties` file that contains information about each security proxy connection.

 ⬥ imports the certificate from the Administrative Server -- if you are using authorization to determine access levels.

NOTE: If you installed the Security Proxy using the **automated installer**, the Security Proxy Server is configured and started, and you can skip to Import the Security Proxy certificates.

Run the Security Proxy Wizard later to change settings or manage certificates.

Using the Security Proxy Wizard

1 Start the Security Proxy Wizard, according to where you installed the product.

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

   On Linux or UNIX:

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

    ⬥ Run the executable:

      `[MssServerInstall]/securityproxy/bin/SecurityProxyServerWizard`

2 The wizard opens with the **Status** tab in focus. Choose whether to open an existing `server.properties` file or to create a new one for this Security Proxy server.

   Refer to the **Help** on each tab for more information.

3 On the **Trusted Certificates** tab, **Import** the Management and Security Server certificate.

4 On the **Proxies** tab, **Add** or **Modify** a proxy.

5 On the **Security Proxy Certificates)** tab, **Generate** or **Import** a security proxy certificate.

6 Return to the **Proxies** tab and click **Export Settings** to export the settings to the Administrative Server.

   Specify or accept the default Administrative Server, Port, and Context. Click **Export**.

7 To verify that the `server.properties` is configured, return to the **Status** tab.

8 Click **Exit** to close the wizard and save your settings. You may need to restart the Security Proxy service.

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

Next step: .

Start the Security Proxy Server

If the automated installer was used to install the Security Proxy on the same machine as the Administrative Server, the Security Proxy Server has been started. Continue with 3. Import the Security Proxy certificates.

If a non-automated installation method was used, you must start the Security Proxy Server.

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

- **On Windows**

  Or, run: `[MssServerInstall]\securityproxy\bin\MssSecurityProxy.exe`

  To start or stop the service, open Windows Control Panel > Administrative Tools > Services, and select **Security Proxy**.

  Note: When the automated installter is used, you can choose to install the servlet runner as a Windows service, in which case the servlet runner starts automatically.

- **On UNIX and Linux**

  For UNIX and Linux platforms, you can start and stop the service at run level changes using the method that is appropriate to your platform. Use `-start` and `-stop` parameters for the security proxy.

  Or, run: `[MssServerInstall]/securityproxy/bin/MssSecurityProxy`

  Note: When the automated installer is used, a link to the services is created in

  `/etc/init.d`

- **Command line options**

  You can use these commands on all platforms to start and stop the Security Proxy:

  ```
  securityproxy -start
  securityproxy -stop
  securityproxy -status
  ```

To install as a service:

1 Change to your MSS install directory.

2 Then use a parameter.

   - **On Windows:**

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

   - **On Linux or UNIX:**

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

```
MssSecurityProxy start
```

> **Note:** The administrator must configure `init` scripts to start the Security Proxy server on startup.

Next step: Import the Security Proxy certificates.

Using FIPS-Approved Mode

When the Security Proxy and terminal sessions are configured to run in FIPS-approved mode, all connections are made using security protocols and algorithms that meet FIPS 140-2 standards.

The current cryptomodules require a manual edit to the Security Proxy properties file to run in FIPS-approved mode.

If you are upgrading from a version that used `fipsMode=approved`, the new property is *not* automatically enabled and must be manually configured.

To configure the Security Proxy to run in FIPS-approved mode:

1 Open `mss\securityproxy\conf\server.properties`.

2 In the `FIPS 140-2 Mode` section, add or set the `fipsApprovedMode=` setting to `on`:

   `fipsApprovedMode=on`

3 Restart the Security Proxy server.

3. Import the Security Proxy certificates

Once the Security Proxy is installed and configured, open Management and Security Server to import the Security Proxy settings.

1 Open the **Administrative Console** > **Configure Settings - Security Proxy** panel.

2 Click **+IMPORT** and enter the required information. See **Help** for assistance.

3 To delete a Security Proxy server, check its box, and click **DELETE**.

Next step: Create Secure Sessions.

4. Create Secure Sessions

After the trust relationship is set between the Management and Security Server and Security Proxy, you can create secure sessions for your users.

1 In the MSS Administrative Console, open **Manage Sessions**, and click **+ ADD**.

2 Select your **Product** (and **Session type**, if needed), and enter a **Session name**.

3 **LAUNCH** the session.

4 As administrator, open the **Connection Setup (or Connection Settings)** dialog. You may need to Disconnect first.

NOTE: The dialog labels vary, depending on your emulator product. Refer to the product documentation for details.

4a Click the option to **Use TLS security**.

4b Select a range or an individual TLS version: **TLSv1.3** or **TLSv1.2**.

A new configuration of the Security Proxy server, created by the MSS installer, enables both TLSv1.3 and TLSv1.2. The default settings allows a TLS connection, depending on the capabilities of the host or server to which you are connecting.

Note: Saved settings for TLSv1.1 and TLSv1 are honored but cannot be set for new installations.

4c Check **Use Security proxy**.

4d Select a **Security proxy server** and a **Proxy port** for this session.

4e Enter the **Destination host** and the **Destination port**.

4f If you check **End-to-end encryption**, the connection between the Security Proxy and the host will use TLS. Otherwise, that connection is not encrypted.

4g Click **OK**. Close the session, and click **Save/Exit** to send the settings to the Management and Security Server.

Next step: Assign Secure Sessions.

5. Assign Secure Sessions

Now you can enable user access to the secure sessions.

1 In the Administrative Console, open **Assign Access**.

2 **Search** for and click the user or group who should have access to the secure session.

3 Check the **Session** that is configured to use the Security Proxy.

4 Click **APPLY**.

5 Deploy sessions to users.

Next step: After the sessions have been opened and used, you can Run Reports to view the activity.

6. Run Reports

In the Administrative Console, open **Run Reports - Security Proxy** to view the activity from your Security Proxy servers. See the Run Reports - Security Proxy Server Reports **Help** for more information.

Related topics

- Notes about Upgrading
- How the Security Proxy Server works
- Resources

Notes about Upgrading

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

- Match the version
- Synchronize the upgrade

Match the version

The `<major>.<minor>` 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. Refer to the MSS Installation Guide.

Synchronize the upgrade

If Security Proxy is installed when you upgrade Management and Security Server, (including updates and service packs), complete these steps to be sure the Security Proxy server is synchronized with the MSS Administrative Server.

After you upgrade:

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

2 On the **Proxies** tab, review the configuration for each port, and click **Save**.

   Note the **Cipher Suites and Certificates**:

   - Multiple cipher suites of the same key type can use the same certificate.

◆ Management and Security Server automatically selects the certificate to use with the associated cipher suite. The selection is based on longest expiration date and other properties. For example:
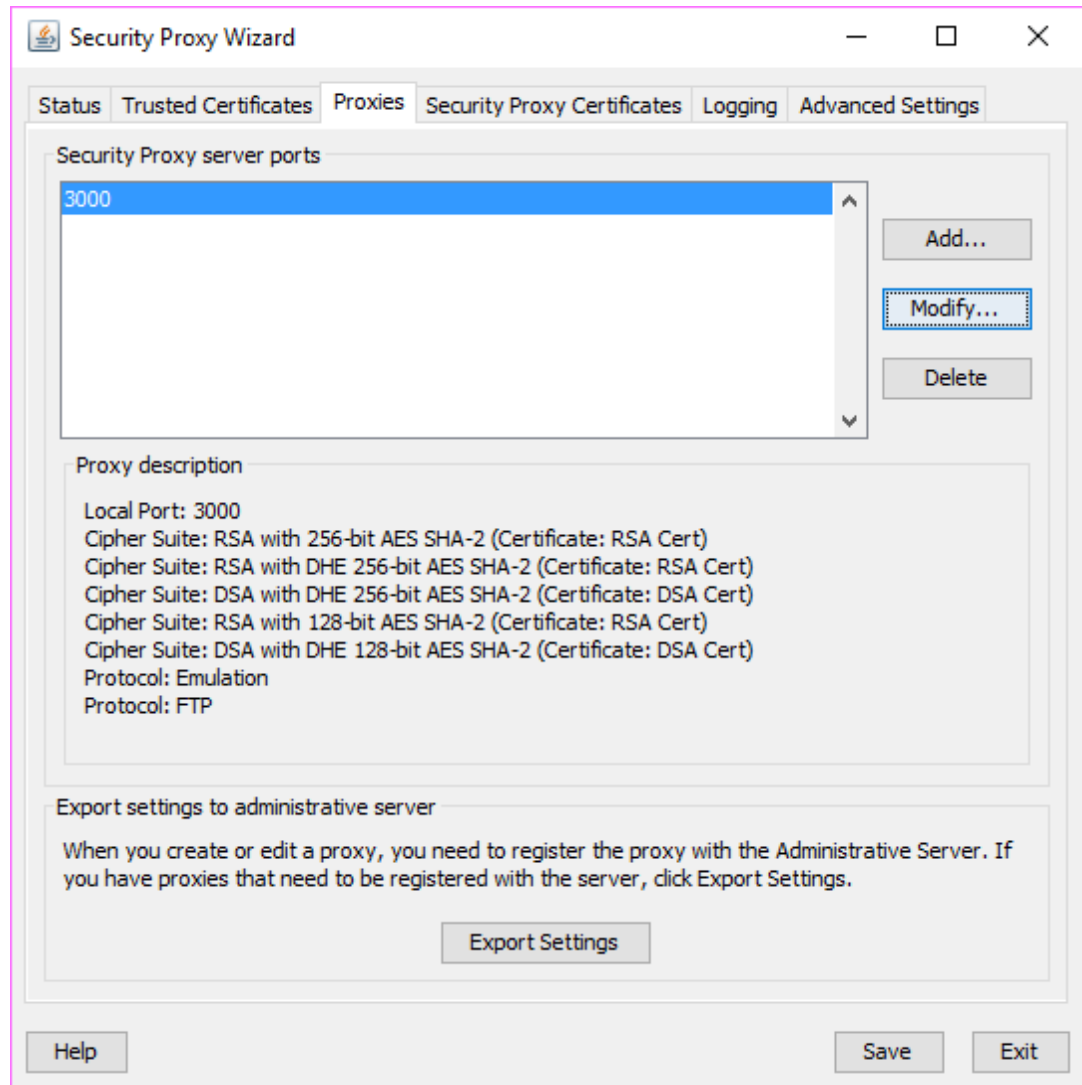
3 To select a different certificate for a particular port:

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

   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 > Settings > Export** to send the settings to the MSS Administrative Server.

Resources

Support Resources

MSS Installation Guide

Security Proxy Wizard (Open from the Start menu)

Management and Security Server Administrative Console - Help:

- Security Proxy
- Manage Sessions
- Assign Access

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.
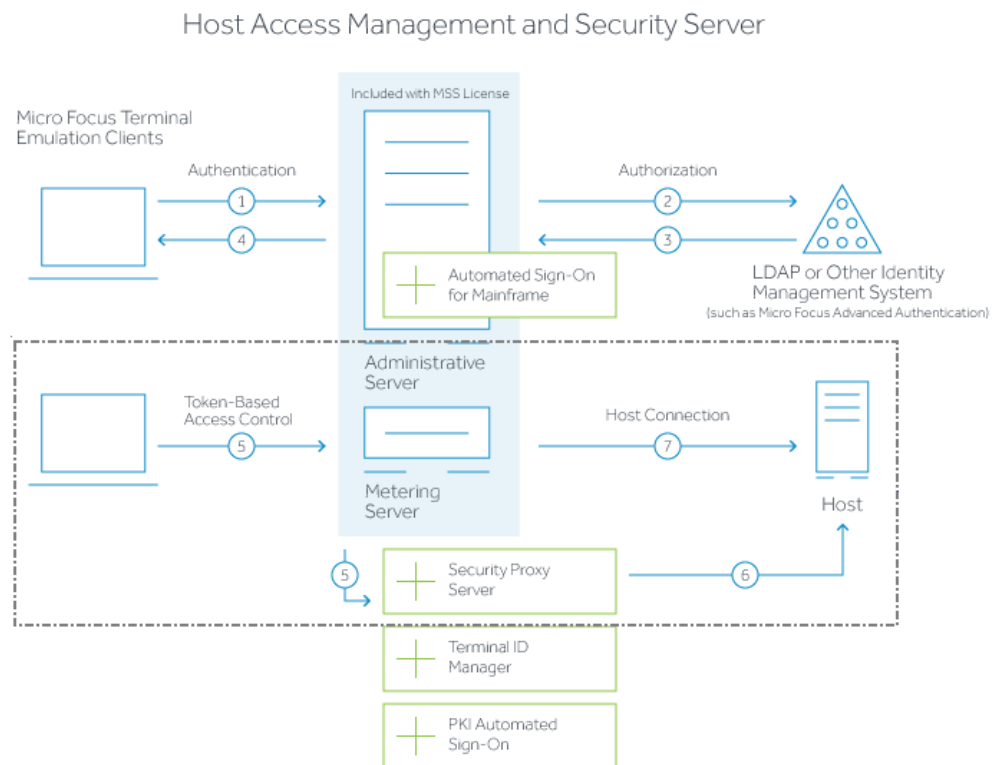
1 User connects to the Administrative Server.

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.

Security Overview

With Management and Security Server, you can provide secure host access to all your users, whether they are around the corner or around the world.

In addition to using HTTPS connections and a variety of authentication and authorization methods, you can configure specific sessions to use the Security Proxy Server to shield the host from direct access by clients. (A separate license is required for the Security Proxy Add-On product.)

TLS Data Encryption

Use the TLS data encryption options to secure the client-server data exchanges.

TLS Encryption between the Client Browser and the Management and Security Server

By default, Management and Security Server allows browsers to use the HTTPS protocol to communicate between the client computer and the Management and Security Server.

When an HTTPS connection is made to the web server, the web server authenticates itself to the client browser using a server certificate. The client checks the server certificate against its trusted certificate store. If the certificate or its root is in the trusted store, the connection proceeds. If the certificate is not trusted, the browser warns the user and requires the user to agree to the connection.

If you use a self-signed certificate or one from a certificate authority (CA) that is not trusted by a user's browser, the browser will present a warning each time the user attempts to access the Management and Security Server. Many browsers permit the user to add the unknown certificate to a trusted certificate list, eliminating the warning. Another option is to use a Management and Security Server certificate from a CA whose root certificate is already trusted by the browser.

TLS Encryption between Client Session and Host

You can provide a level of security by using the TLS protocol to protect data sent between the client terminal (or printer) session and the host. (The host must be TLS-enabled.)

The option to require a TLS connection between the client and the host is available when you launch the session from **Manage Sessions**. In the launched session, go to the Connection Setup or Security Properties options to set a TLS connection.

TLS Encryption and Authorization between the Client Session and the Security Proxy Server

Greater security is provided by adding the Security Proxy Server, which requires a separate license. 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 no longer support SSL encryption.)

In addition, when Security Proxy authorization is enabled, only users who have been authenticated and authorized by the Administrative Server are able to access the host. Others are denied access.

NOTE: To use the Security Proxy Server, the Administrative Server certificate must be trusted by the Security Proxy. The automated installer generates a self-signed certificate that must be imported to the Security Proxy's list of trusted certificates. If you installed a CA-signed certificate on the Administrative Server, you do not need to import the certificate to the Security Proxy.

End to end Encryption: Tunneled TLS Direct Connection to the Host

When you use the Security Proxy, data sent between the emulator and the proxy is TLS-encrypted. You can also tunnel a TLS direct connection to the host through the Security Proxy Server. This form of end-to-end encryption can be set up for a host that supports TLS connections.

To set up this type of connection, open the session's Security (TLS Settings) dialog to configure a session to use the Security Proxy. Check the optionfor **End to end encryption**.

As part of the TLS protocol, the client checks the server or host name against the name on the server certificate. Therefore, TLS connections require the common name on the server certificate to match the host or Security Proxy server name. When end-to-end encryption through the Security Proxy is enabled, the client will receive a server certificate from both the Security Proxy and the host. It is recommended that the host certificate have the Security Proxy server name identified as a subject alternate name (SAN).

FIPS-Approved Mode

The United States government's Federal Information Processing Standards (FIPS) are sets of standards developed by the National Institute of Standards and Technology (NIST) that describe the handling and processing of information within governmental agencies.

Specifically, FIPS 140-2 sets standards for cryptographic modules. The cryptographic modules are validated against the specific set of requirements and tested in 11 categories by independent US government-certified testing laboratories. NIST and Canada's Communications Security Establishment (CSE) jointly administer the process by which modules are validated against FIPS 140-2.

When you configure the Security Proxy Server and secure terminal sessions to run in FIPS-approved mode, all connections are made using security protocols and algorithms that meet FIPS 140-2 standards.

Related Topic:

 * Using the Security Proxy Server

Credential stores used in MSS

Management and Security Server (MSS) stores certificates and keys in several locations. Here's how the stores are used during a TLS transaction.

Keystores contain a party's own certificate and a private key. The party's keystore is used to authenticate itself when presented to another party (server or client).

Trust stores contain the certificates from other parties (servers or clients). The trust store may contain certificates from trusted Certificate Authorities (CAs) as well as other parties' self-signed certificates. Trust stores are used to verify the certificates received during a TLS transaction.

During a TLS transaction, the keystore is used to authenticate the sender to the receiver. The receiver verifies the certificate presented by checking its list of trusted certificates in the trust store.

MSS uses Bouncy Castle as the provider for keystore operations, and the `.bcfks` (Bouncy Castle FIPS keystore) extension is used for cryptographic files.

The tables that follow identify and describe the credentials stored in each location.

Stores used by MSS in *MSSData/trustedcerts*

The keystores in this location include the Management and Security Server certificate + private key, the client certificate + private key, and the imported certificates on the Trusted Certificates list for the terminal emulator client.

The keystores in `MSSData/trustedcerts` are described in the following table.

- **Keystore location:** `%ProgramData%/Micro Focus/MSS/MSSData/trustedcerts/`
- **Password location:** This keystore password is encrypted in the KeyChain (in `MSSData/keychain.bcfks`).
- **To change this password:** Administrative Console > **Configure Settings – General Security** > **Change keystore password**

Stores used by MSS

Keystore	Function
`client.bcfks`	◆ for Reflection for the Web's shared private key ◆ A client certificate is used to identify users connecting to the Security Proxy or an SSL/TLS host when either requires client authentication. If all users share the same client certificate, then the Administrative Server can automatically distribute it to Reflection for the Web clients when needed.
`rweb.bcfks`	◆ for the Management and Security Server certificate ◆ signs the Security Proxy token ◆ for client authentication to DCAS when using Automated Sign-on for Mainframe
`saml.bcfks`	◆ for SAML authentication
`sshclient.bcfks`	◆ for Reflection for the Web SSH ◆ not used by MSS itself
`trustedascj.bcfks`	◆ for outbound HTTPS: Micro Focus Advanced Authentication and Automated Sign-on for Mainframe ◆ used for LDAPS
`trustedps.bcfks`	◆ trust store for Host Access for the Cloud and Reflection for the Web using SSL to host ◆ not used by MSS itself ◆ When settings are exported from the Security Proxy Wizard, certificates are added to this store.
`trustedws.bcfks`	◆ contains only the public key and certificate from the `rweb.bcfks` store ◆ Certificates from this store are imported by the Security Proxy server into its `trustedws.bcfks` store.

Keychain in *MSSData*

The Keychain contains a SecretKeyEntry with assorted encrypted secrets, including the keystore password for files in `trustedcerts`.

- ◆ *Keystore location:* `%ProgramData%/Micro Focus/MSS/MSSData/keychain.bcfks`
- ◆ *Password location:* Either base64 in `%ProgramData%/Micro Focus/MSS/MSSData/keychain.pwd`, or in the Keychain Utility.
- ◆ *To change the password for the keychain:* Administrative Console > **Configure Settings – General Security** > **Keychain**

Stores located in *server/etc*

The keystores in `%ProgramFiles%/Micro Focus/MSS/server/etc` are described in the table below.

To change the password for the keystore:

1. Open `/MSS/server/conf/container.properties`.
2. Update the keystore's password property, listed in the table.

Stores in server/etc

Keystore	Function, Configuration location, Password property
`servletcontainer.bcfks`	◆ Credential store for Tomcat HTTPS, all three ports ◆ Created at startup ◆ Used for the embedded web servers (Tomcat) ◆ **Configuration location:** `/MSS/server/services/servletengine-tomcat/META-INF/service.ctx.xml` ◆ **Property to change password:** `servletengine.system.ssl.keyStorePassword`
`system-trustcerts.bcfks`	◆ Trust store for Tomcat HTTPS trusted subsystem port ◆ Created at startup ◆ Used for the Trusted Subsystem (X.509 authentication and Clustering) ◆ **Configuration location:** `/MSS/server/services/servletengine-tomcat/META-INF/service.ctx.xml` ◆ **Property to change password:** `management.server.client.ssl.trustStorePassword`
`mss-cluster.bcfks`	◆ Used internally for signing and encryption ◆ Created at startup ◆ NOTE: If this store is modified or deleted, certain properties may need to be manually re-encrypted by re-entering them in the Administrative Console ◆ **Configuration location:** `/MSS/server/conf/product-core-ctx.xml` ◆ **Property to change password:** `cluster.key-store-password`

Stores used by Security Proxy in *proxyserver/keystores*

The keystores in `proxyserver/keystores` are described in the table below.

- ◆ *Keystore location:* `%ProgramFiles%/Micro Focus/MSS/securityproxy/keystores/`
- ◆ *Password location:* hard-coded
- ◆ *To change this password:* This password cannot be changed.

Stores used by Security Proxy

Keystore	Function
`rwebps.bcfks`	◆ Credential store for proxy, inbound TLS ◆ The public key and certificate from this store are exported to the Administrative Server and stored in its `trustedps.bcfks` store.
`trustedps.bcfks`	◆ Stores the public key and certificate from `rwebps.bcfks`, noted above.
`trustedws.bcfks`	◆ Trust store for proxy, both for TLS client authentication and proxy token signature verification ◆ Contains public keys and certificates imported into the proxy from trusted MSS Administrative Servers
`trustedmss.bcfks`	◆ Stores the public key and certificate for MSS servers that the user has chosen to trust when exporting settings or importing servers in the Security Proxy Wizard

cacerts in *jre/lib/security/cacerts*

The **cacerts** trust store contains a set of commonly used root certificates that comes by default with Management and Security Server.

- ◆ *Keystore location:* `%ProgramFiles%/Micro Focus/MSS/jre/jre/lib/security/cacerts`
- ◆ *Password location:* System property `javax.net.ssl.trustStorePassword`
- ◆ *To change this password:* Set a property in `container.conf` and change the password of the file using a utility such as `keytool`, `portecle`, or `keystore explorer`.

To view the certificates, go to **Configure Settings – Trusted Certificates**. Select **Management and Security Server** as the Certificate Store, and then open the list under **Trusted Root Certificate Authorities**.

The **cacerts** trust store is:

- ◆ the trust store for outbound TLS
- ◆ combined with `trustedascj` for Automated Sign-on for Mainframe and Micro Focus Advanced Authentication
- ◆ not a `.bcfks` file

X.509 Certificates - Setup Requirements

To authenticate users with X.509 client certificates, such as a certificate stored on a smart card, be sure these requirements are met. Some settings are client-specific.

In addition, you can use X.509 authentication to access the Administrative Console and the HTML Session list.

- Client requirements
- Servers in a Cluster
- Configure Access to the Administrative Console or Sessions List

Client requirements

These settings are required for any client using X.509 certificates.

- [ ] **X.509** must be enabled in the **Administrative Console**: **Configure Settings** - **Authentication & Authorization** > **X.509**.

- [ ] Each client that is authorized to use MSS resources must have a client certificate, such as a certificate stored on a smart card.

- [ ] The issuer of the client certificates must be trusted by MSS. For more information, refer to Trusted Certificates.

- [ ] If using **Clustering**, be sure to configure the servers that will be replicated. See Servers in a Cluster.

Check the requirements for your client:

- "Host Access for the Cloud clients" on page 141
- "Windows-based clients" on page 142

Host Access for the Cloud clients

These additional settings must be in place for Host Access for the Cloud.

- [ ] A port configured for TLS client authentication must be enabled on MSS.

  This secure port listens for and authenticates communications between MSS and the Host Access for the Cloud Session Server. This port is automatically configured when using the MSS automated installer or an MSS configuration utility.

- [ ] *Note:* A certificate to trust the Host Access for the Cloud Session Sever is configured by the automated installer.

  No further action is needed, unless you want to add a CA-signed certificate to the MSS trust store.

- [ ] If using **Clustering**, be sure to configure the servers that will be replicated. See Servers in a Cluster.

To add a CA-signed or other certificate to the MSS trust store:

1. In the Administrative Console, open **Configure Settings - Trusted Certificates**.

2. Click **Trusted Sub-System**, and click **+IMPORT**.

3. Click **UPLOAD** and select the file containing the certificate to upload to the MSS Administrative Server.

4. Enter the **Keystore file name**, **Keystore password**, and **Friendly name**.

5. Click **IMPORT** to add the certificate.

6. Restart the MSS Administrative Server.

Windows-based clients

These additional settings must be in place for Windows-based clients.

☐ A port configured for TLS client authentication must be enabled on MSS. This secure port authenticates end-user certificates presented by Windows-based clients (such as Reflection Desktop or Rumba+).

   Note: When using the MSS automated installer or an MSS configuration utility, this port is automatically configured.

☐ The MSS Administrative Server must be restarted after adding a CA-signed certificate.

☐ If using **Clustering**, be sure to configure the servers that will be replicated. See Servers in a Cluster.

Servers in a Cluster

If you are using **X.509 authentication** and **Clustering**, the changes you make to a certificate store are automatically replicated to the other MSS Administrative Servers in the cluster.

You *do not need to repeat* the process on each MSS server in the cluster.

Configure Access to the Administrative Console or Sessions List

Administrators can use X.509 authentication to log in to the MSS Administrative Console, and users can use X.509 authentication to access their list of assigned sessions.

To enable X.509 authentication, you must perform the following setup in addition to configuring the X.509 authentication settings in the Administrative Console.

1 Add the root CA certificate to the MSS servletcontainer truststore using either the **Keystore Explorer** utility or the **Java keytool**.

   ◆ **Keystore Explorer**

      a. Open `servletcontainer.bcfks` in the `etc` folder of the MSS installation. The default password is `changeit`.
      b. From the **Tools** menu, choose **Import Trusted Certificate**.

c. Select the root CA certificate that was used to issue the end-user certificates for X.509 authentication.

d. Enter an alias to identify the certificate in the truststore.

e. After the certificate is imported, choose **File** > **Save**; then exit Keystore Explorer.

   ◆ **Java keytool**

a. Open a command prompt in the `etc` folder of the MSS installation.

b. Issue the following keytool command. Specify the full path to the root CA certificate if it's not in the current directory. In this example, `daso_rootca.crt` is the certificate being imported, and `daso_rootca` is the alias being assigned.

```
keytool -importcert -no-prompt -file daso_rootca.crt -keystore
   servletcontainer.bcfks -providername BCFIPS -storetype bcfks -
   providerclass
   org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -
   providerpath ../lib/bc-fips-*.jar -storepass changeit -alias
   daso_rootca
```

2 Configure the MSS Administrative Console to use HTTPS to access MSS web services.

Open `<installpath>\MSS\server\conf\container.properties` and edit this setting to use HTTPS:

`management.server.url=https://<servername>:<HTTPS port>/mss`

Note: *Enter the* `<servername>` *and* `<HTTPS port>` *that were set during the initial installation*.

3 Restart the server for the changes to take effect.

4 Navigate to the server URL using HTTPS. The browser will prompt for your certificate credentials.

Assuming that the user certificate is configured in the browser (details vary by browser), you can navigate to the adminconsole url:

`https://<servername>:<HTTPS port>/adminconsole`

Using Log Viewer

The Log Viewer application works with the XML log files written by all Host Access Management and Security Servers, including the Security Proxy Server.

Using the Log Viewer, you can:

◆ Filter log messages by severity.

◆ Search for message text to quickly find the records you need.

◆ Filter logs at view time, which enables you to find an interesting record, and then expand your view to see the context from all log sources without having to correlate multiple logs manually.

Notes about viewing information

◆ Log message details are displayed in a separate split window below the log message summary window and update automatically as messages are scrolled through.

◆ Open log files are listed in the vertical pane on the left side of the Log Viewer with the fully-qualified path and filename of the currently open log file displayed in the status line at the bottom of the Log Viewer window.

◆ Records in the XML logs contain rich information, including millisecond-accurate event times and sequence numbers that guarantee that messages are seen as atomic units in the order they were logged.

◆ Records in the XML logs are language-independent and can be viewed in any supported language, regardless of where they were originally written. Two different users can view the exact same log file in two different languages, with no loss of information.
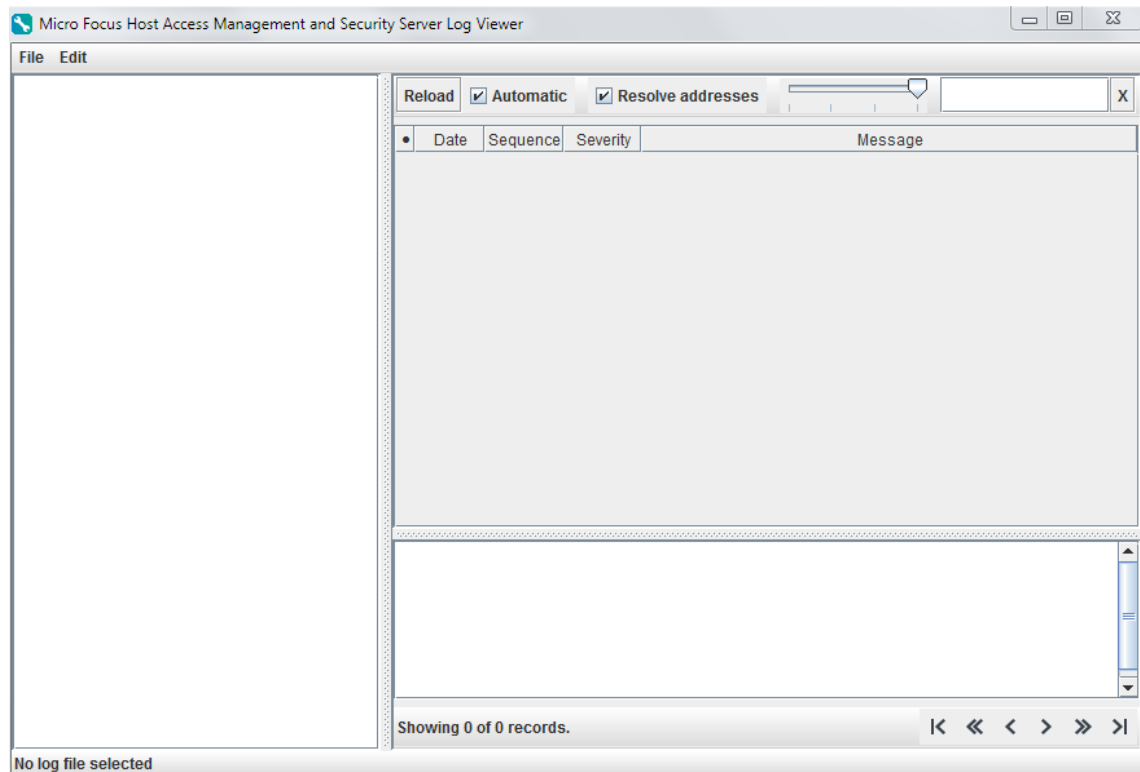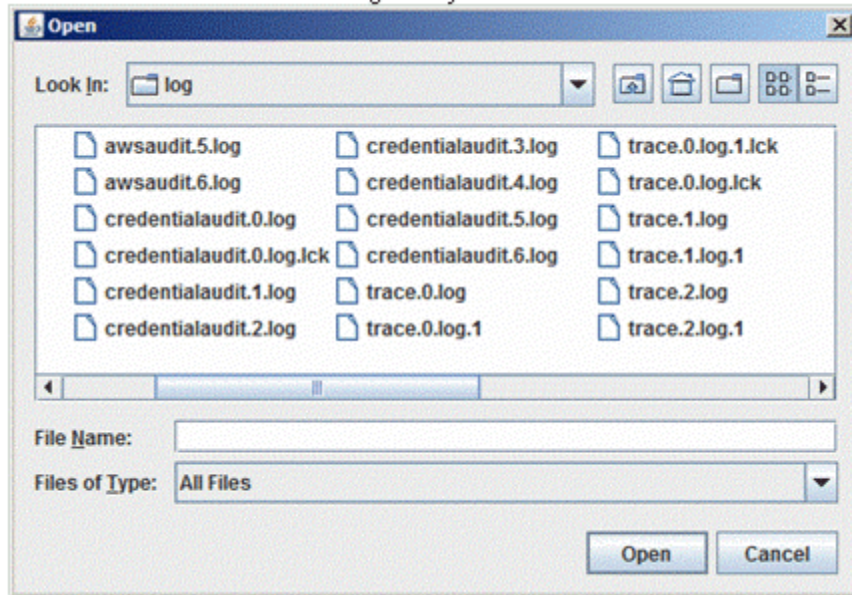
To use the Log Viewer

1 Open the Log Viewer.

On Windows: Open from the **Start** menu, or double-click the executable:

`C:\Program Files\Micro Focus\MSS\utilities\bin\LogViewer.exe`

**On Linux:** `/usr/local/microfocus/mss/utilities/bin/LogViewer`

2 In the Log Viewer, click **File** > **Load**. (Shortcuts: **Ctrl+L** to Load, and **Ctrl+O** to Close.)

2a Browse to the directory containing the log files you want to view.

2b Select a log file and click **Open.**

Server log files are located in the **MSSData** directory. To locate the MSSData path, click **About** > **Product Information** in the Administrative Console.

3 Click the file in the left pane of the Log Viewer to view the details.
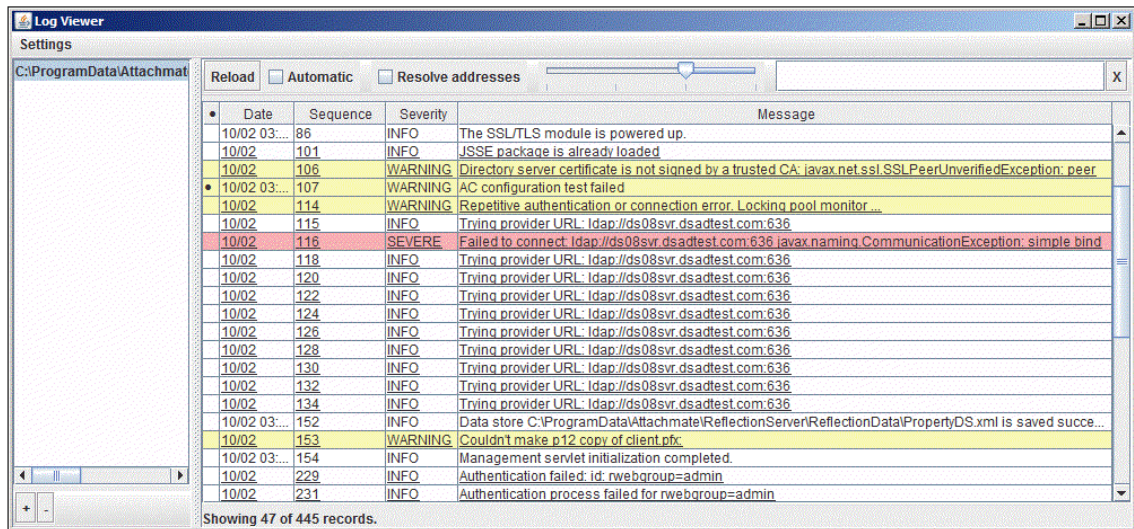
Other Features

Log Viewer provides these options from the top of the right pane.

- **Reload**—Refreshes the log. You can view logs while they are open for writing.
- **Automatic**—Refreshes the log about every 6 seconds, automatically.
- **Resolve addresses**—Displays DNS names instead of numeric IP addresses.

Note: Address resolution may be slow, since it can require multiple DNS requests per address. Results are cached until you close the Log Viewer.

 ◆ **Slider** for Message Level Control—Filters the messages by Severity level.

   Severe messages are highlighted in red. Warnings are highlighted in yellow.

 ◆ **Search**—Type a partial search string into the text box to search the message field for matching strings. Log Viewer displays only the results with that string.

Changing Logging Options

You can change certain default logging options for the product you have installed by editing the `log.properties` file.

Enable debug messages.
Change the default log file size.
Change the number of saved log files.
Change default log file directory.

The `log.properties` file is located in the `MSSData\properties` directory.

An example using `template_log.properties`

To customize logging properties:

 1 In the `MSSData\properties` directory, open the `template_log.properties` file.

    The template shows examples of the options that can be changed in `log.properties`.

 2 Use the template file as a reference. (See the commented section.) Or, copy and paste its contents into the `log.properties` file and modify as needed.

 3 When the changes are complete, save the file as `log.properties`.

 4 Restart the MSS Server service for the changes to take effect.

Gathering Log Files to View on another Server or to Send to Technical Support

Log files can be collected in a couple of ways.

 ◆ Use the **COLLECT LOGS** button on the **Configure Settings - Logging** page to initate a local download of the MSS logs, MSS data, and configuration files.

   The resulting zip file contains captured logs and configuration data and can be sent to Micro Focus Customer Support for troubleshooting purposes.

 ◆ Copy the following files from the `MSSData\log` directory. You do not need to stop the MSS server.

   ```
   trace.<n>.log
   awsaudit.<n>.log
   credentialaudit.<n>.log
   useraudit.<n>.log
   ```
   After you gather the files, copy them to another server for viewing or if requested, and send them to Micro Focus Customer Support for troubleshooting purposes.

NOTE: The log files are generated such that the lowest generation number (.0) is the current one, and higher numbers are successively older. For example, `trace.0.log` is more recent than `trace.5.log`.
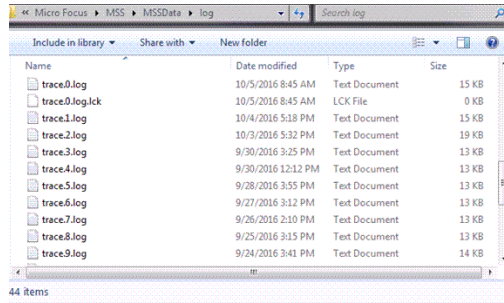
If the (.0) log file covers the period where the event occurred, then gathering (.0) is sufficient. Otherwise, gather additional log files. The file count limit for each log file is 10. The files with `.lck` extensions are not needed for viewing.