

Host Access Management and Security Server Administrator Guide

12.6

© Copyright 2019 Micro Focus or one of its affiliates

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

Contents

| | |
|--|-----------|
| Host Access Management and Security Server | 7 |
| 1 About Management and Security Server 12.6 | 9 |
| About Management and Security Server | 9 |
| About Add-On Products | 9 |
| 2 Manage Sessions | 11 |
| Add a session | 11 |
| Product- or Session-specific settings | 12 |
| Configure a Host Access for the Cloud session | 13 |
| Configure a Reflection/InfoConnect Desktop - Workspace Automated Sign-on session | 13 |
| Configure a Rumba+ Desktop session | 14 |
| Configure a Reflection for the Web session | 15 |
| Edit a session | 19 |
| Copy a session | 19 |
| Delete a session | 19 |
| 3 Manage Packages | 21 |
| Configure a Package | 21 |
| Upload or Update a Package | 21 |
| 4 Assign Access | 23 |
| Search & Assign | 23 |
| Search for Users or Groups/Folders | 23 |
| Assign Sessions or Packages | 24 |
| Currently Assigned | 26 |
| 5 Configure Settings | 27 |
| General Settings | 27 |
| Set VPA number | 27 |
| Set server name | 28 |
| Custom login page | 28 |
| Reflection for the Web Launcher | 28 |
| Applet tag | 29 |
| Links List | 30 |
| General Security | 30 |
| Server access protocol | 31 |
| Change administrator password | 31 |
| Restrict administrator account | 32 |
| Require new login | 33 |
| Smart card settings | 33 |
| Certificate chooser prompt | 35 |
| Enable identity verification | 35 |
| Change keystore password | 36 |
| PKI Server | 37 |
| Keychain | 37 |

| | |
|---|----|
| Secure Shell | 38 |
| Known Hosts List | 38 |
| Shared User Key Pair | 39 |
| Certificates | 41 |
| Administer the Management and Security Server Certificate | 41 |
| Administer Shared Client Certificate | 42 |
| Other certificates | 43 |
| Trusted Certificates | 45 |
| Certificate Store - Terminal Emulator Clients | 45 |
| Certificate Store - Management and Security Server | 45 |
| Trusted Root Certificate Authorities (collapsed by default) | 46 |
| Credential Store (Reflection for the Web) | 46 |
| Enable credential store | 46 |
| Select form of identity | 46 |
| Regenerate encryption key | 47 |
| Delete selected credentials | 47 |
| Security Proxy | 48 |
| Preliminary steps - Install and Configure | 48 |
| Import Security Proxy settings | 48 |
| Create and assign secure sessions | 49 |
| Authentication & Authorization | 50 |
| Choose Authentication Method | 50 |
| Choose Authorization Method | 51 |
| LDAP Server Configuration | 52 |
| Single Sign-on through IIS | 56 |
| Single Sign-on through Windows Authentication | 56 |
| X.509 Configuration | 60 |
| SiteMinder Configuration | 64 |
| Micro Focus Advanced Authentication | 65 |
| SAML Authentication | 67 |
| Product Activation | 70 |
| Install an additional product | 70 |
| Complete the activation | 71 |
| Automated Sign-On for Mainframe | 72 |
| Automated Sign-on for mainframe sessions | 72 |
| DCAS Servers | 72 |
| Secondary LDAP directory | 75 |
| User Principal Name (UPN) | 77 |
| Search filter used with secondary LDAP directory | 78 |
| Next step | 78 |
| Metering | 79 |
| High Availability | 79 |
| Add a Metering Server | 79 |
| Metering Server Setup | 79 |
| Terminal ID Manager | 80 |
| Enable Terminal ID Manager | 80 |
| Open the Terminal ID Manager Console | 81 |
| Replication | 81 |
| Replication Database | 81 |
| How to Configure Replication | 82 |
| Importing Server Certificates | 83 |
| Securing Replication Connections | 83 |
| Standalone Server Role | 84 |
| Master Server Role | 84 |
| Slave Server Role | 85 |
| Copying Package Data | 88 |
| Upgrading Replication Servers | 89 |
| Troubleshooting Replication | 89 |
| Logging | 90 |

| | |
|---|-----------|
| Administrative Server | 91 |
| trace.log | 91 |
| Write client debug output to Java console | 91 |
| Mark Log | 91 |
| Credential store | 91 |
| 6 Run Reports | 93 |
| Log File Viewer Reports | 93 |
| Filters | 93 |
| Show Report | 94 |
| Usage Metering Reports | 94 |
| Credential Store Reports | 94 |
| Credential Store Users | 94 |
| Credential Store Usage History | 94 |
| Security Proxy Server Reports | 95 |
| Current user activity | 95 |
| Security Proxy server logs | 96 |
| Connections per proxy server | 97 |
| Assigned Access Reports | 97 |
| Users and Groups | 97 |
| Sessions | 97 |
| 7 Technical References | 99 |
| Using the Security Proxy Server | 99 |
| 1. Install the Security Proxy Server | 99 |
| 2. Configure and Start the Security Proxy Server | 100 |
| 3. Import the Security Proxy certificates | 102 |
| 4. Create Secure Sessions | 102 |
| 5. Assign Secure Sessions | 103 |
| 6. Run Reports | 103 |
| Notes about Upgrading | 103 |
| Resources | 105 |
| Security Overview | 105 |
| TLS/SSL Data Encryption | 105 |
| FIPS-Approved Mode | 108 |
| Credential stores used in Management and Security Server | 108 |
| Stores used by MSS in <i>MSSData/trustedcerts</i> | 109 |
| Keychain in <i>MSSData</i> | 109 |
| Stores used by Tomcat in <i>server/etc</i> | 110 |
| Stores used by Security Proxy in <i>proxyserver/keystores</i> | 110 |
| cacerts in <i>jre/lib/security/cacerts</i> | 111 |
| X.509 Certificates - Setup Requirements | 111 |
| Client requirements | 111 |
| Replicated servers | 113 |
| Optional: Administrative Console login | 113 |
| Updated Cryptographic Modules | 114 |
| Why were the cryptographic modules changed? | 114 |
| What changed in Management and Security Server? | 114 |
| What do I need to do? | 115 |
| Using Log Viewer | 116 |
| To use the Log Viewer | 116 |

Host Access Management and Security Server

Host Access Management and Security Server 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 including Reflection Desktop, InfoConnect, Host Access for the Cloud, Reflection for the Web, and Rumba+. Then, the existing user and group directories can be leveraged to control access to the sessions.

[About Management and Security Server 12.6](#)
[Release Notes](#)

1 About Management and Security Server 12.6

Host Access Management and Security Server version 12.6 released with Host Access for the Cloud 2.4 in June 2019. See the [Release Notes](#) for details.

Open the **About** menu to view

- ♦ **Product Information:** the installed **Version** and **System Information** for Host Access Management and Security Server.
- ♦ **Activated Products:** the currently installed activation files (for [add-on](#) or other products), displayed on the **Configure Settings - Product Activation** panel.
- ♦ **Legal Information:** the license agreement and legal notices.

About Management and Security Server

Use the **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

2 Manage Sessions

Use **Manage Sessions** (known as *Session Manager* in previous versions) to create and configure terminal sessions. Use the column chooser to modify the summary view of your sessions.

- ◆ [“Add a session” on page 11](#)
- ◆ [“Product- or Session-specific settings” on page 12](#)
- ◆ [“Edit a session” on page 19](#)
- ◆ [“Copy a session” on page 19](#)
- ◆ [“Delete a session” on page 19](#)
- ◆ [Export a Reflection for the Web session](#)

Add a session

- 1 Click **Manage Sessions > Add**.
- 2 Under Configure Session, select your **Product**.
Select the **Session type** for **Host Access for the Cloud**, **Reflection/InfoConnect Desktop**, **Reflection for Windows**, or **Reflection for the Web**.
- 3 Enter a unique **Session name** that does not exceed 64 characters.
Session names cannot include any of these characters: \ / : * ? " < > |

NOTE: The **Workspace Automated Sign-on** session type has [session name requirements](#). You can enter a name now and edit it later.

- 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 If you are adding one of these session types, continue with the product-specific steps:
 - ◆ [Host Access for the Cloud](#)
 - ◆ [Reflection/InfoConnect Desktop - Workspace Automated Sign-on](#)
 - ◆ [Rumba+ Desktop](#)
 - ◆ [Reflection for the Web](#)

For all other products or session types, continue with step 6.

- 6 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.

NOTE: If a user runs Windows 7 with Internet Explorer in protected mode, file virtualization may prevent Management and Security Server from finding a folder. To turn off protected mode on the machine, go to Tools > Internet Options > Security tab. Clear the **Enable Protected Mode** check box. Click OK and restart Internet Explorer.

- ◆ **For sessions to be launched from an end user's list of links**, 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>

7 Click **Launch** to start the session in administrator mode in a separate window.

NOTE: To configure this session to connect through the Security Proxy (if you are entitled), see [Setting Up the Security Proxy Server](#).

8 Configure 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.

Note: Use the column chooser to show or hide session properties: Type, Name, Description, Direct Link, Comments, Security Status.

9 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

- ◆ [Authentication & Authorization](#)
- ◆ [Assign Access](#)
- ◆ [Edit a session](#)

Product- or Session-specific settings

If you are using one of these products, follow the steps to configure a session or session type.

[Host Access for the Cloud](#)

[Reflection/InfoConnect Desktop - Workspace Automated Sign-on](#)

[Rumba+ Desktop](#)

[Reflection for the Web](#)

Configure a Host Access for the Cloud session

- 1 Note the session properties and the Session Server URL. Click **Launch**.
- 2 A browser opens to the web client **Settings > Connections** panel. Configure the settings for this session, and click **Save**.
- 3 When finished configuring, click **Exit** to save the session to the Management and Security Server.
- 4 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](#)

Configure a Reflection/InfoConnect Desktop - Workspace Automated Sign-on session

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

In addition to adding the session, you must [Configure Settings for Automated Sign-On](#) to secure the server connections and manage user access. And the mainframe needs to be configured to support PassTickets. See the [Automated Sign-on for Mainframe Administrator Guide](#) for details.

Prerequisites

To add a **Workspace Automated Sign-on (ASM)** session, these preliminary tasks must be completed outside of Management and Security Server.

- 1 In **Reflection/InfoConnect Workspace**, create a 3270 session that includes an ASM login macro. Detailed steps are included in your Reflection/InfoConnect documentation.
- 2 Save the session in a location that can be accessed by Management and Security Server.

Proceed with the [Workspace Automated Sign-on \(ASM\) Settings File](#) configuration in Management and Security Server.

Workspace Automated Sign-on (ASM) Settings File

Continue on the **Manage Sessions - Add New Session** panel in Management and Security Server (where you selected the Product name and Session type).

- 1 **Session name requirements.** The Workspace ASM session name *must exactly match* the host name to which the client is connecting.

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 this session is being configured to automatically log on to `blue.mycompany.com`, then the session name must be `blue.mycompany.com`, not `blue` or another variation.

If you want to enable sessions to automatically log on to `blue.mycompany.com`, `blue`, or `123.456.78.90` (`blue.mycompany.com`'s IP address), you must create separate sessions with all of these names.

Proper naming of the Workspace ASM session is critical.

If necessary, edit the session name or create additional sessions.

- 2 Click **Browse**. Select the Reflection/InfoConnect session that contains the Workspace ASM login macro.
- 3 Click **Save** to upload the settings file and save the session.

The session is added to the **Manage Sessions** list and is available to be assigned.

Assigning 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 [Search & Assign](#).

In particular, note the required **Edit** option used to [select a method to obtain the mainframe user name](#).

Related topics

- ◆ [Assign Access](#)
- ◆ [Automated Sign-On for Mainframe](#)

Configure a Rumba+ Desktop session

You are able to add a Rumba+ session to be managed by Management and Security Server because you already

- ◆ configured a session in your Rumba+ application.
- ◆ saved the session profile.

Now, you must upload and attach your Rumba+ session profile to the session you are adding to Management and Security Server.

Rumba+ Session Profile

- 1 After you enter a Session name, click **Browse**. Select the Rumba+ session profile (saved by your Rumba+ application). The profile name displays on this panel.
- 2 By default, **Overwrite settings files** is not selected, and users can set local preferences in their launched sessions.

Check this option 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 if there are differences.

NOTE: After a Rumba+ session is created in the Administrative Console, users can open their Rumba+ sessions from the Windows Start menu, as usual. The settings file is downloaded from Management and Security Server to the client computer the first time the session is launched.

Users can then launch the session using the local settings file. Sessions launched from the local settings file are not updated from the Management and Security Server settings file.

Overwrite settings files allows you to easily distribute updates to existing settings files; however, changes that users made to their settings will be lost.

- 3 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.

3a In the Rumba+ session, set the host name and port to the address of the Security Proxy server.

3b 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.

- 4 Click **Save**. The profile is then uploaded and attached to the session.

To 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.

Configure a Reflection for the Web session

You can use additional settings to customize the display and behavior of your Reflection for the Web session.

Options on this panel: [Appearance](#) | [FTP](#) | [Advanced Settings](#) | [Applet Parameters](#)

Appearance

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

Table 2-1 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 IBM 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 |

- ◆ **Display session in its own window.** Select to launch a session in a frame outside of the browser page.
- ◆ **Display session embedded in a web browser window.** Select to launch the session in a new browser window.

Use this option to specify a custom page template, which allows you to format the HTML to add custom text, graphics, or JavaScript for the session. The template jsp must be stored in the /mss/server/web/webapps/mss/templates folder on the MSS server. You can copy one of the sample templates as a starting point for your own template.

Templates must be stored in the templates folder directly or in a subfolder. If you leave the page template field empty, the embedded session will appear in a new browser window with a simple heading that shows the name of the session. When the specified template is not present, the default embedded page is used. For more information, see the Knowledgebase article: [Using Templates in Reflection for the Web](#).

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.

FTP Window

When you configure a standalone FTP session, use these options to specify the appearance of the FTP window. When **Local/remote lists and console** is selected, lists of local and server files and directories are displayed in the top portion of the FTP window, and an FTP console with a command line is displayed in the bottom portion.

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

Advanced Settings

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

- ◆ [“Window Size and Status Bar” on page 17](#)
- ◆ [“Session Auto Launch” on page 17](#)

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.

Session Auto Launch

Check **Auto Launch** to automatically launch the session when the session list is displayed. Users cannot override this Auto Launch mechanism.

When this setting is not enabled, users can choose to open a session automatically by configuring Session Attributes, available from the **Action** button on the session list.

Applet Parameters

You can customize the properties of a Reflection for the Web session by adding applet parameters.

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 be sure a parameter applies to your session, refer to the **Applet Attributes and Parameters**.

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

Click **Launch**, and then configure the session. When you **Save/Exit** the session, the settings are sent to the Management and Security Server.

Next steps

As a next step, you can


- ◆ Use [Assign Access](#) to make the session available to end users.
- ◆ [Configure Authentication](#) and LDAP authorization.
- ◆ Return to [Manage Sessions](#) to add or edit a session.
- ◆ [Export a Reflection for the Web session](#)

Export a Reflection for the Web session

Use 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 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

- ◆ [Assign Access](#)
- ◆ [Authentication & Authorization](#)
- ◆ [Manage Sessions](#)

Edit a session

- 1 In **Manage Sessions**, click the session you want to edit. Or, check the box, and then click **Actions > Edit**.
- 2 Note the **Properties**, which are not editable.
- 3 Change the settings you wish to edit. (Details are described in either [Add a session](#) or [Product- or Session-specific settings](#).)
 - ◆ Session Name
 - ◆ Window title
 - ◆ Display option -- in a separate window or embedded in a browser window
 - ◆ FTP option for this session
 - ◆ Advanced settings
- 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.

Related Topics

- ◆ [Authentication & Authorization](#)
- ◆ [Assign Access](#)
- ◆ [Add a session](#)

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 the click **Actions > 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 **Actions > Delete**.

The deleted sessions are removed from the list.

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 21](#)
- ◆ [“Upload or Update a Package” on page 21](#)

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.

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**.

NOTE: Package management requires additional configuration on replicated Administrative Servers. See [Replication > Copying Package Data](#).

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 23
- ♦ “[Currently Assigned](#)” on page 26

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 23
- ♦ “[Assign Sessions or Packages](#)” on page 24

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 Administrative Console.

- 3 The **Edit** option is used for Automated Sign-On to a mainframe. To assign an automated sign-on session, click **Edit**. Then continue with [Select the source of the mainframe user name](#).
- 4 Click **Apply** to save your assigned sessions.
- 5 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

This 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.

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](#)
- ◆ [Authentication & Authorization](#)
- ◆ [Product Activation](#)
- ◆ [Automated Sign-On for Mainframe](#)
- ◆ [Metering](#)
- ◆ [Terminal ID Manager](#)
- ◆ [Replication](#)
- ◆ [Logging](#)

General Settings

Configure these settings for using Management and Security Server.

- ◆ [“Set VPA number” on page 27](#)
- ◆ [“Set server name” on page 28](#)
- ◆ [“Custom login page” on page 28](#)
- ◆ [“Reflection for the Web Launcher” on page 28](#)
- ◆ [“Applet tag” on page 29](#)
- ◆ [“Links List” on page 30](#)

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 Administrative Server. This name is helpful for debugging in larger environments where more than one Administrative Server is behind a load balancer. In these cases, it can be difficult for the client to determine which Administrative Server is being accessed.

This string is printed in the Java console.

Custom login page

You can create your own login/links list page and store it separately from the installed default page. The page can have any custom content desired, including graphics, links, or JavaScript.

If you specify a custom login page here, the custom page jsp must be stored on the server in the templates folder directly or in a subfolder. A sample custom login page is available in the `MSS/server/web/webapps/mss/templates/samples` folder, along with some other samples for dynamic embedded sessions.

If the custom login page is not found under the templates folder, the default login page is displayed. If you are developing a custom login page and have trouble getting it to display properly, you may not be able to access the Administrative Console to change the custom page specification. Rename the custom page in the templates folder, and the default page will be used.

Reflection for the Web Launcher

The **Reflection for the Web Launcher** is a private client-side application that eliminates the need for Oracle's JRE or the Java plug-in. This feature is available with Reflection for the Web 13.0 and higher.

NOTE: *The Reflection for the Web Launcher settings display only when Reflection for the Web is installed and activated.*

See [Using the Reflection for the Web Launcher](#) (in the [Reflection for the Web Installation Guide](#)) for details about the Launcher, the deployment options, and the expected user experience.

Deployment Options

Three deployment options are available to accommodate your environment's readiness to transition away from Oracle's JRE and/or the Java plug-in and begin using the Reflection for the Web Launcher.

- ◆ **Standard**

Select the **Standard** option until you are ready to move away from Oracle's JRE or the Java plug-in.

The user experience is the same as with previous versions of Reflection for the Web, which rely on the Java browser plug-in and its legacy JNLP (Java Network Launch Protocol) behavior to launch the links list and Reflection for the Web sessions (before version 13.0).

- ◆ **Hybrid**

Select the **Hybrid** option for a phased rollout. As you transition away from the Java browser plug-in and/or Oracle's JRE, you can roll out Reflection for the Web Launcher to subsets of users.

In the hybrid environment, the user's setup determines whether Reflection for the Web sessions are launched using either the **Standard** or the **Launcher** method.

- **Standard** is used if the user still has the Java browser plug-in. Sessions are launched as they were in previous versions of Reflection for the Web.
- **Launcher** is used when the Reflection for the Web Launcher is installed on a user's workstation. Sessions are launched using JNLP instead of the Java browser plug-in.

When **Hybrid** is selected, you have the option to show authenticated users a link to download the Reflection for the Web Launcher Installer.

◆ **Launcher**

Select the **Launcher** option when you are ready to completely transition away from the Java plug-in and/or Oracle's JRE.

The **Launcher** option exclusively uses the Reflection for the Web Launcher, which uses JNLP to launch sessions. Oracle's Java browser plug-in *cannot* be used to launch the links list or terminal sessions.

When **Launcher** is selected, you have the option to show authenticated users a link to download the Reflection for the Web Launcher Installer.

Distribution option: Show link...

Check this box to enable individuals to download the Reflection for the Web Launcher, when either **Hybrid** or **Launcher** is selected.

When **Show link to download the Windows-based installer for the Reflection for the Web Launcher** is checked, the user sees a link to manually download the `.msi` file for the Reflection for the Web Launcher Installer — after they authenticate to MSS.

This one-time option sets up the workstation with the Reflection for the Web Launcher. After the Reflection for the Web Launcher is installed, the user can ignore the download link.

For further distribution details and the expected user experience, see [Using the Reflection for the Web Launcher](#) (in the [Reflection for the Web Installation Guide](#)).

NOTE: JRE security updates will be provided via an updated `.msi` file in Reflection for the Web product updates.

Applet tag

For Standard (legacy) systems, the **APPLET tag** is a consistent way to deploy Java applets across browsers on all platforms.

NOTE: The `APPLET tag` option has *no effect* when using the **Launcher** deployment option. See [Reflection for the Web Launcher](#).

The **OBJECT/EMBED tag** may be used to resolve issues for specific browsers. More specifically:

- ◆ Use the **APPLET tag** to deploy applets to a mixed-browser environment.
- ◆ Use the **OBJECT tag** to deploy applets that are to be used only with **Internet Explorer**.
- ◆ Use the **EMBED tag** to deploy applets that are to be used only with the **Mozilla** family of browsers.

When using the **OBJECT/EMBED** tag, you can specify the URL for the **OBJECT codebase** attribute and the **EMBED pluginspage** attribute, which is used to download the latest JRE when no JRE is present on the machine.

You can specify the location if you want to distribute the JRE from an alternate location.

Links List

A direct link is a URL that opens the specified session after the user authenticates. Check **Show links list for direct sessions** if you want users to see a list of links to their entitled sessions when you provide a direct link to a session.

This setting applies only to sessions that are configured to launch in a frame outside of the browser page.

NOTE: Java version detection is disabled by default to provide faster startup of sessions on the client. When Java detection is enabled, users are informed when their Java version is unsupported by the product.

The specific version of Java detected is also used to configure applet parameters that help manage the behavior of sessions when navigating away from and back to the web page.

To enable Java version detection, edit this configuration file:

- 1 Open `/mssdata/propertyDS.xml`.
 - 2 Change the **enableJavaVersionDetection** value from `false` to `true`:

```
<CORE_PROPERTY NAME="enableJavaVersionDetection">
<BOOLEAN>true</BOOLEAN>
</CORE_PROPERTY>
```
 - 3 Save the file.
-

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” on page 31](#)
- ◆ [“Change administrator password” on page 31](#)
- ◆ [“Restrict administrator account” on page 32](#)
- ◆ [“Require new login” on page 33](#)
- ◆ [“Smart card settings” on page 33](#)
- ◆ [“Certificate chooser prompt” on page 35](#)
- ◆ [“Enable identity verification” on page 35](#)
- ◆ [“Change keystore password” on page 36](#)
- ◆ [“PKI Server” on page 37](#)
- ◆ [“Keychain” on page 37](#)

Server access protocol

By default, Management and Security Server allows browsers to use the HTTP protocol to communicate between the client computer and the Management and Security Server. Although HTTP is universally available, information exchanged using HTTP is sent in clear text and is vulnerable to unauthorized access.

To secure your passwords and other sensitive data, we recommend that you require browsers to connect to Management and Security Server using the HTTPS protocol, which provides TLS/SSL encryption. To require HTTPS:

- ◆ Check **Require HTTPS for connections to the Management and Security Server**.
- ◆ Make sure TLS/SSL is enabled on your web server.

If you installed Management and Security Server with the automated installer, TLS/SSL is enabled with a self-signed server certificate.

NOTE: When users first request a session, they may see a warning that the certificate is not trusted by their browser. Generally, users can choose to permanently accept the certificate.

If your web server uses a certificate signed by a popular Certificate Authority, most browsers are able to establish a TLS/SSL connection without going through the security warning.

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](#)

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](#)

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:

Table 5-1

| 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](#)

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.

From a user's smart card, only one certificate is used to authenticate to Management and Security Server. By default, smart card support is available for sessions using PKCS #11 (Public-Key Cryptography Standard) smart card readers, such as ActivCard.

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

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

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.

Related topics

- ◆ [General Security](#)

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.

Related topics

- ◆ [General Security](#)

Enable identity verification

When a 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 Management and Security Server](#).

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 keychain stores the passwords and passphrases (such as LDAP server passwords) used by the Management and Security Server. The keychain file is encrypted and is unlocked for use by the Management and Security Server at server startup. The keychain file is located in `MSSData/rweb.keychain`.

You can also set a password for the keychain, using these settings.

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

By default, this setting enables unattended startup of the Management and Security Server. The keychain password is written to the keychain password file `MSSData/rweb.pwd`. On subsequent server startup or restart, the keychain password is read from the keychain password file, and the keychain is unlocked without additional action by the administrator.

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

- ◆ **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.

This port is accessed by the KeychainUtility when the keychain must be manually unlocked.

- ◆ **Existing password for unlocking the keychain file**

The default password is `changeit`

- ◆ **New password and Confirm new password**

Enter a case-sensitive password.

Note: The system administrator MUST restrict the filesystem permissions for the `rweb.keychain` and `rweb.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.

Related topics

- ◆ [General Security](#)

Secure Shell

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

- ◆ [“Known Hosts List” on page 38](#)
- ◆ [“Shared User Key Pair” on page 39](#)

Known Hosts List

The known hosts list contains the public keys of hosts that the terminal emulator applet 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
AAAAB3NzaBlyc2EAAAABIAAAIEA0WR3aIRtilXquUmXtxw5oi3rMkhY9jw/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” on page 39](#)
- ◆ [“Import” on page 39](#)
- ◆ [“Export” on page 40](#)
- ◆ [“Shared User Key Pair Details” on page 40](#)

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/SSL** 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 41](#)
- ◆ [“Administer Shared Client Certificate” on page 42](#)
- ◆ [“Other certificates” on page 43](#)

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**.

Related topics

- ♦ [Administer Shared Client Certificate](#)
- ♦ [Other certificates](#)

Administer Shared Client Certificate

A client certificate is used to identify users connecting to the Security Proxy or to a TLS/SSL host when client authentication is required. If all users share the same client certificate, the Administrative Server can automatically distribute it to the 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.

- ♦ 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 **Security Proxy Wizard** to manage the Security Proxy certificate.
- ♦ 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 43](#)
- ♦ [“Use a Certificate Authority’s Instructions” on page 44](#)
- ♦ [“Use Commands for Keytool or Openssl Tool” on page 44](#)

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 a 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, with links to the CSR generation instructions:

- ♦ [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, import the response from the CA.

- 1 `keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore keystore.jks`
- 2 `keytool -certreq -alias server -keyalg RSA -file server.csr -keystore keystore.jks`
- 3 `keytool -importcert -trustcacerts -file careply -keystore keystore.jks`

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.

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

- ◆ [“Certificate Store - Terminal Emulator Clients” on page 45](#)
- ◆ [“Certificate Store - Management and Security Server” on page 45](#)
- ◆ [“Trusted Root Certificate Authorities \(collapsed by default\)” on page 46](#)

Certificate Store - Terminal Emulator Clients

Clients that make a TLS/SSL 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. Enter the keystore file name, password, and friendly name.

Note: Make sure the file containing the certificate is on the Administrative Server in this folder:

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

3. Click **Import** to add the certificate.
4. 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.
- ◆ **Replication:** Add certificate(s) to trust other MSS servers used in Replication.
- ◆ **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. Enter the keystore file name, password, and friendly name.

Note: Make sure the file containing the certificate is on the Administrative Server in this folder:

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

3. Click **Import** to add the certificate.

4. 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).

Trusted Root Certificate Authorities (collapsed by default)

This 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 46](#)
- ◆ [“Select form of identity” on page 46](#)
- ◆ [“Regenerate encryption key” on page 47](#)
- ◆ [“Delete selected credentials” on page 47](#)

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

Use this panel to import the settings from the Security Proxy Server to the Management and Security Server after the Preliminary steps are completed.

- ◆ [“Preliminary steps - Install and Configure” on page 48](#)
- ◆ [“Import Security Proxy settings” on page 48](#)
- ◆ [“Create and assign secure sessions” on page 49](#)

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.

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” on page 50](#)
- ◆ [“Choose Authorization Method” on page 51](#)
- ◆ [“LDAP Server Configuration” on page 52](#)
- ◆ [“Single Sign-on through IIS” on page 56](#)
- ◆ [“Single Sign-on through Windows Authentication” on page 56](#)
- ◆ [“X.509 Configuration” on page 60](#)
- ◆ [“SiteMinder Configuration” on page 64](#)
- ◆ [“Micro Focus Advanced Authentication” on page 65](#)
- ◆ [“SAML Authentication” on page 67](#)

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.

NOTE: If you set the authorization method to **None**, be aware that all users are logged in as Guest. During session configuration, it is best to *not allow* users to modify their session settings (User Preference Rules), because they can overwrite each other's choices.

- ◆ **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 option 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 [Management and Security Server Installation Guide](#).
- ◆ **Single sign-on through Windows authentication** - This option uses the NT LAN Manager version 2 (NTLM v2) protocol to authenticate users. When a user logs into the Windows domain and requests a session using a web browser that supports integrated authentication through NTLM v2, a secure hash of the user's credentials is sent to a domain controller for verification. Once verified, the Administrative Server establishes an authenticated HTTP session with the user's browser.

NOTE: NTLM v1 is no longer supported. Any settings saved for Single sign-on through Windows are exclusively for NTML v2 and will overwrite any existing NTLM v1 settings.

Microsoft Internet Explorer, as well as other web browsers, support integrated authentication through NTLM, but other browsers may require additional configuration to enable this functionality. The computer running the Administrative Server does not need to be a member of the Windows domain.

- ♦ **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 the Administrative Server and a SiteMinder web agent on the same machine as IIS, and set up the server to use your IIS web server.

The setup options vary based on your selection.

Related Topics

- ♦ [LDAP Server Configuration](#)
- ♦ [Enabling Multiple LDAP Servers](#)
- ♦ [Single Sign-on through IIS](#)
- ♦ [Single Sign-on through Windows Authentication](#)
- ♦ [X.509 Configuration](#)
- ♦ [SiteMinder Configuration](#)

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 52](#)
- ◆ [“Enabling Multiple LDAP Servers” on page 52](#)
- ◆ [“LDAP Configuration” on page 53](#)
- ◆ [“Search Base and Groups/Folders” on page 54](#)
- ◆ [“Certificate” on page 54](#)
- ◆ [“Authentication of End Users” on page 54](#)
- ◆ [“Validate LDAP Connection” on page 55](#)
- ◆ [“Advanced Settings” on page 55](#)

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 Single Sign-on Through Windows](#).

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 Administrative Server and the LDAP server as clear text or encrypted. The type of encryption used depends on your LDAP server. TLS/SSL 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/SSL.** When using TLS/SSL 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/SSL**, 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/SSL.

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/SSL). 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\AMAccountName (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/SSL** 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.

Table 5-2 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 your 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 [Management and Security Server 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.

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 `http://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](#)

Single Sign-on through Windows Authentication

Use this configuration to set up Management and Security Server in a Windows environment that uses Active Directory authentication (NTLM v2) with or without LDAP authorization.

NOTE: NTLM v1 is no longer supported. Any settings saved for **Single sign-on through Windows authentication** are exclusively for NTML v2 and will overwrite any existing NTLM v1 settings.

If you cannot upgrade to NTLM v2, you can manually edit your NTLM v1 settings. Contact Support for details.

- 1 In **Configure Settings - Authentication & Authorization**, click **Single sign-on through Windows authentication**.
- 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 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 Single Sign-on \(without LDAP\)](#)
- ◆ [Use LDAP to restrict access to Single Sign-on sessions](#)

Configure Windows Single Sign-on (without LDAP)

Use these settings to configure Windows Single Sign-on authentication *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 Single Sign-on 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 Single Sign-on Through Windows](#).

Related Topics

- ♦ [Use LDAP to restrict access to Single Sign-on sessions](#)
- ♦ [Adding Another Server for Single Sign-on Through Windows](#)

Use LDAP to restrict access to Single Sign-on sessions

To configure *Single Sign-on through Windows authentication* 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 Single Sign-on Through Windows](#).

Related topics

- ◆ [Configure Windows Single Sign-on \(without LDAP\)](#)
- ◆ [Adding Another Server for Single Sign-on Through Windows](#)

Adding Another Server for Single Sign-on Through Windows

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 Single Sign-on \(without LDAP\)](#)
 - ◆ [Use LDAP to restrict access to Single Sign-on 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.

NOTE: X.509 is supported through the HTTPS port. Users should disable HTTP ports when running X.509.

- ◆ [“Pre-requisites” on page 61](#)
- ◆ [“Authentication Settings” on page 61](#)
- ◆ [“Certificate Revocation Checking” on page 62](#)

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)**

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

Note: If you do not use Reflection for the Web, the Hard and Soft certificate settings do not apply.

- ◆ 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\mfms`.

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 (`http://<servername>:<port>/rweb`).
2. During X.509alt 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.509alt authentication completes and the links list displays

– or –

an **Enter Passphrase** dialog box opens, if required for `usercert.pfx`. Once the user enters the correct passphrase, X.509alt authentication completes and the links list 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/SSL 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** checkbox, 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 [Using the IIS Reverse Proxy with Host Access for the Cloud](#)

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 a session](#)

Micro Focus Advanced Authentication

Advanced Authentication is a separate Micro Focus product that offers biometric and multi-factor authentication for several Micro Focus products, including Management and Security Server.

A separate Add-On license is required to use **Micro Focus Advanced Authentication** with **Management and Security Server**. See the [Preliminary Tasks](#) for details.

Configuring Advanced Authentication

To activate and set up Advanced Authentication, complete the preliminary tasks prior to configuring the Advanced Authentication server to trust the Management and Security Server.

- ◆ [“Preliminary Tasks” on page 65](#)
- ◆ [“Configuring Advanced Authentication in the Administrative Console” on page 66](#)

Preliminary Tasks

- 1 Install Micro Focus Advanced Authentication Server, and note the
 - ◆ server name (or IP address)
 - ◆ server's port number
- 2 After you obtain the separate license for **Host Access Management and Security Server - Advanced Authentication Add-On**, download the activation file, named `activation.advanced_authentication-<version>.jaw`, from the product download page.
- 3 Upload the activation file.
 - 3a Log in to **Management and Security Server**.
 - 3b Open the Administrative Console to **Configure Settings - Product Activation**.
 - 3c Click **Activate New**.
 - 3d Browse to and click the activation file you downloaded in step 2.

The file is installed and added to the list of Currently Installed products.
- 4 Continue with the steps for [Configuring Advanced Authentication in the Administrative Console](#) to establish trust between the Advanced Authentication server and Management and Security Server.

Configuring Advanced Authentication in the Administrative Console

Follow these steps to 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.
Select LDAP as the **Authorization** method, if desired.
- 3 Import the Advanced Authentication server's certificate:
 - 3a Enter the **Server** name or IP address of the Advanced Authentication server (noted in [Preliminary Tasks](#) - step 1) **without** a prefix, such as `https://`.
For example, enter `<myserver>.<mycompany>.com`.
 - 3b Enter the server's **Port** number (also noted in [Preliminary Tasks](#) - step1).
 - 3c 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 this error appears, **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 SANs (Subject Alternative Names) 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 Click the **Test Connection**, with **Verify server identity** checked.

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 is *not* successful, troubleshoot the error as follows:

- ♦ **Advanced Authentication Failure - The hostname you entered does not match the server certificate.**

Check the certificate in the Configure Settings - Trusted Certificates list. Then, 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`. To view the trace log file, use the **LogViewer** utility. For more information, see [Using Log Viewer](#).

Configuring Advanced Authentication Methods

Refer to the [Advanced Authentication documentation](#) to configure Advanced Authentication methods, such as Fingerprint or Voice.

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 Reflection ZFE* 2.3 or higher.

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

Configuring Management and Security Server (MSS) to use SAML is a multi-step process.

In general, you must:

1. Configure MSS as a SAML service provider.
2. Download or access the service provider's metadata from MSS.
3. Export the service provider's metadata into the identity provider.
4. Map the identifier source.
5. Configure the SAML whitelist.
6. Configure LDAP, when used for authorization.

Follow the [SAML Configuration steps](#).

* **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.

SAML Configuration steps

Be sure to read the Important information, Cautions, and Notes as you configure Management and Security Server (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.

Detailed steps:

- ♦ [“Configure MSS as a SAML Service Provider” on page 67](#)
- ♦ [“Identity Mapping” on page 69](#)
- ♦ [“SAML whitelist” on page 69](#)
- ♦ [“LDAP Servers” on page 69](#)

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 these requirements. If you encounter an error message, be sure these requirements are met:

- ♦ The prefix URL value **must end** with the MSS server's **web application context**.

For example, the default context is `/mss`.

- ♦ The protocol **must match** the one used by MSS clients attempting to authenticate using SAML.

For example, when using SAML authentication in Host Access for the Cloud, the protocol specified in the `management.server.url` property in Host Access for the Cloud must match the protocol of the prefix URL defined in this field: `http` or `https`. A mix of protocols (`http` and `https`) is not supported.

-
- 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).

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:

- ◆ Check **Enable SAML whitelist** (the default).

For troubleshooting purposes, the SAML whitelist can be disabled.

- ◆ 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**.

Related Topics

- ◆ [LDAP Server Configuration](#)
- ◆ [Authentication & Authorization](#)

Product Activation

View the list of activation files for currently installed components, clients, and other products managed by Management and Security Server.

Use this panel to upload additional activation files.

- ◆ [“Install an additional product” on page 70](#)
- ◆ [“Complete the activation” on page 71](#)

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 by either

- ◆ 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, 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>.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>.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](#).

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 71](#)
- ◆ [“Terminal ID Manager” on page 71](#)
- ◆ [“Automated Sign-On for Mainframe” on page 71](#)
- ◆ [“Micro Focus Advanced Authentication” on page 72](#)

Security Proxy Server

- 1 Copy the activation file, `activation.security_proxy-<12.6.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-<12.6.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 Administrative 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.

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” on page 72](#)
- ♦ [“DCAS Servers” on page 72](#)
- ♦ [“Secondary LDAP directory” on page 75](#)
- ♦ [“User Principal Name \(UPN\)” on page 77](#)
- ♦ [“Search filter used with secondary LDAP directory” on page 78](#)
- ♦ [“Next step” on page 78](#)

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 73](#)
- ♦ [“Edit an existing DCAS server” on page 74](#)
- ♦ [“Test the Connection” on page 74](#)

- ◆ “Set a Preferred DCAS server” on page 74
- ◆ “Delete a DCAS server” on page 75

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 75](#)
- ◆ [“Security options” on page 76](#)
- ◆ [“Server name” on page 76](#)
- ◆ [“Server port” on page 76](#)
- ◆ [“Username and Password” on page 76](#)
- ◆ [“Search Base” on page 77](#)
- ◆ [“Certificate” on page 77](#)
- ◆ [“Validate LDAP Connection” on page 77](#)

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/SSL 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/SSL.** When using TLS/SSL 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/SSL, 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/SSL.

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/SSL). 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\AMAccountName (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/SSL** 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).

If 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.

Related topic

- ◆ [Next step](#)

Next step

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 \(UPN\)](#)
- ◆ [Configure a Reflection/InfoConnect Desktop - Workspace Automated Sign-on session](#)
- ◆ [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” on page 79
- ◆ “Add a Metering Server” on page 79
- ◆ “Metering Server Setup” on page 79

High Availability

The Metering server can be installed on multiple machines and clustered to provide high availability.

A minimum of three MSS servers is required for high availability. A master server and at least two slave servers must be configured in [Replication](#).

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.
 - ◆ **Use HTTPS:** Select this option to enable a secure connection using the HTTPS protocol.
 - ◆ **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 80 for HTTP, and 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

```
http://<servername:port>/meter/AdminStart.html.
```

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 In the Metering Console, you can configure settings and license pools for that metering server. Open the Metering Console [Help](#) for more information.

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 page 80](#)
- ◆ [“Open the Terminal ID Manager Console” on page 81](#)

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-12.6.<n>.jaw` from your download location.

- 2 Check [Use HTTPS](#) to encrypt the data between the Terminal ID Manager and the browser, as well as the connections between Terminal ID Manager and a client (Host Access for the Cloud or Reflection for the Web). You may see a warning if the certificate is not recognized.

- 3 Enter the [Web server name](#).

You can use a full server name or the full IP address.

- 4 Enter the [Web server port](#) of the server where Terminal ID Manager was installed.

During an automated installation, the default port is **80** for HTTP and **443** for HTTPS.

- 5 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](#).

Replication

Server replication makes it easier to configure and maintain multiple Administrative Servers, provide high availability, and have more flexibility when spanning geographically distant server installations.

Using replicated servers, you can synchronize multiple administrative servers by propagating configuration and session changes made on one server (the Master) to all of the servers in a replication group (the Slaves).

NOTE: To configure Metering for high availability, you must configure a master and at least two slaves.

Before you begin, review these topics:

- ♦ [Replication Database](#)
- ♦ [How to Configure Replication](#)
- ♦ [Securing Replication Connections](#)

Replication Database

Management and Security Server (MSS) uses a database to store information on replicated servers. This implementation introduces some terms to the Replication UI.

- ♦ **Database.** The database contains a **cluster** of MSS servers.
A **node** represents one server in the cluster.
- ♦ **Database Status.** The current status displays on the **Configure Settings-Replication** panel.
After you add or edit settings and click **Apply**, the MSS server initializes and implements the changed settings. The Database Status indicates the phase of the initialization process.
When the Database Status reaches the **Up** phase (indicating that the initialization is complete), you can make additional changes if needed.
- ♦ **Details.** Information about each node in the cluster. Replication is functioning properly when each node reports **Status: UP** and **Owns: 100%**. (That is, the server contains 100% of the replicated data.)

Related topics

- ♦ [How to Configure Replication](#)
- ♦ [Securing Replication Connections](#)

How to Configure Replication

Perform the configuration tasks *in this order* to set the trust relationships.

- 1 Identify which MSS server will be the **Master**, and which ones will be **Slave** servers.
As you decide, consider the [Server role: Master and Slave servers](#).
- 2 For each server to be clustered, import the certificates for the Master and all of the Slave servers to the Trusted Certificates store. See [Importing Server Certificates](#) for detailed steps.
- 3 Configure the Master server. See [Master Server Role](#) for detailed steps.
- 4 Configure each Slave server. See [Slave Server Role](#) for detailed steps.

Server role: Master and Slave servers

To implement server replication, you will configure one **Master** server and one or more **Slave** server

Before you begin, consider the roles of the **Master** and **Slave** servers and how to secure the connections

- ♦ **Slave** servers are configured according to the settings on this **Master** server. Any subsequent changes to the **Master** server will be automatically replicated to the **Slave** servers.
- ♦ Only one **Master** server can be configured, but multiple **Slave** servers can be associated with that **Master** server.
- ♦ You can modify the configuration on the **Master** server and push those updates to the **Slaves**.
- ♦ You can also modify the configuration on a **Slave** server and submit the changes, but they will not be applied until the requested change is implemented on the **Master** server.
- ♦ All configuration elements of the **Master** Administrative Server are replicated to a **Slave** server -- **except**:
 - log files
 - Credential Store settings
 - some Certificates settings
 - the Web Agent name, when *SiteMinder* is used for authentication. (The Web Agent name must be set separately for each replicated machine.)

Related Topics

- ♦ [Securing Replication Connections](#)
- ♦ [Standalone Server Role](#)
- ♦ [Master Server Role](#)
- ♦ [Slave Server Role](#)
- ♦ [Remove a down slave from a cluster](#)
- ♦ [Troubleshooting Replication](#)

Importing Server Certificates

Before you can configure replication, you must establish trust between the Master and the Slaves by entering all of the servers' certificates into the Trusted Certificate store. This is required regardless of your security settings.

The certificate of the current Administrative Server, along with the certificates of the remote Administrative Servers must be included in the list. This step is required for all servers, Master or Slave, in the management cluster. Self-signed, or other certificates that are not well known, must be imported to all Administrative Servers in the cluster.

Before you add the Master or Slave servers:

- 1 Open **Administrative Console > Configure Settings > Trusted Certificates**.
- 2 Under **Certificate Store**, click **Management and Security Server**.
- 3 In the list of certificates that are trusted by MSS, confirm that a trusted certificate is present. If not, continue importing the certificate.
- 4 Copy the remote server certificate, found here, `<install-dir>/MSS/server/etc/servletcontainer.cer`, to this location on the local server, `<mss-data-dir>/certificates`. You must provide a unique file name when you copy the file. Best practice is to name the file `<server-name>.cer` where `server-name` is the name of the remote server.
- 5 Click **+ Import** to add a certificate.
- 6 Enter the file name.
- 7 For the friendly name use the server name you provided in Step 4.
- 8 Click **Import**.

NOTE: If you installed MSS on z/Linux without a JRE (using the UNIX no-jre installer, see the Caution in the [Configure master server](#) section. You may need to edit a file.

Securing Replication Connections

You have the option to use HTTP or HTTPS as your server-to-server communication transport. HTTPS is recommended.

When using a Security Proxy

If you are using a **Security Proxy** server, you must also import the certificates for all 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 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 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 Administrative 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.

NOTE: The **Concurrency Lock Timeout**, included in the former *Administrative WebStation* interface, applies to managing sessions. See the Note in [Edit a session](#).

Related topics

- ♦ [Standalone Server Role](#)
- ♦ [Master Server Role](#)
- ♦ [Slave Server Role](#)

Standalone Server Role

This is the default role, and applies to Administrative Servers that are not configured for replication. The **Standalone** server role is used to reset Replication, such as when upgrading.

To set up Replication, configure a Master server, and add Slave servers.

- ♦ [Master Server Role](#)
- ♦ [Slave Server Role](#)

Master Server Role

Use the **Master server role** to set the configuration of this Administrative Server as the one that will be replicated to the specified Slave Administrative Servers.

- ♦ [“Configure master server” on page 84](#)

Configure master server

On the MASTER server that you want to replicate:

- 1 Click **Master**.
- 2 Check the **Database Status**. If **Up**, continue.
If **Down** or **Initializing**, wait until the changes take effect and the status is **Up**.
- 3 **Database Network Adapter**. Choose a network adapter associated with an IP address that the other MSS servers in the cluster can access.
- 4 **Global protocol**. Choose whether to **Use HTTPS for server to server communication** (between the Master and Slave servers). HTTPS is the default. If you choose to clear the HTTPS requirement, the [Importing Server Certificates](#) requirements still apply.

CAUTION: When **HTTPS is checked**:

- ♦ You cannot change the transport and retain previously configured Slave servers. You must delete existing Slave servers before changing the protocol from HTTP to HTTPS (or vice versa).
- ♦ If you installed MSS on **z Linux with no JRE** (using the UNIX no-jre installer), you **must edit** this file in the MSS installation directory:

```
mss/server/microservices/cassandra/conf/cassandra.yaml
```

```
Change # algorithm: SunX509
to      algorithm: IBMX509    (uncommented)
```

You do not need to restart the MSS server.

Without this change, the cassandra database fails to restart after replication is configured, and this exception is added to the `mss/server/logs/cassandra.log`:

```
"Caused by: java.security.NoSuchAlgorithmException: SunX509
TrustManagerFactory not available"
```

To resolve the exception, set the Replication server back to **Standalone**. Edit `cassandra.yaml`, as above, and proceed with Replication.

5 **Configure Master Server.** Change the default **Passphrase**, if desired.

The Master server and all associated Slave servers must share the same passphrase. Use these fields to change the default passphrase.

If you make no changes to the passphrase on any of the Administrative Servers in the cluster, the passphrase is automatically the same on all servers. A changed passphrase is in effect for all replication implementations, whether or not HTTPS is used.

6 Click Apply. To proceed, choose **Yes** on the Settings update confirmation. This confirmation causes the database to restart to allow for remote communication.

7 After the database has transitioned back to an **UP** status, click **Details** and confirm that the **Local Instance Address** is **Not** 127.0.0.1.

The next step is to proceed to the [Slave Server Role](#) section for information on adding slaves. You should complete all the steps for each slave before adding additional ones.

Related Topics

- ◆ [Slave Server Role](#)
- ◆ [Remove a down slave from a cluster](#)
- ◆ [Troubleshooting Replication](#)

Slave Server Role

Use the Slave server role to replicate the configuration of the Master Administrative Server.

- ◆ [Configure slave server](#)
- ◆ [Add the master server](#)
- ◆ [Add a slave to the master server](#)
- ◆ [Remove a running slave from a cluster](#)
- ◆ [Remove a down slave from a cluster](#)

Configure slave server

Before you add a replication server, remember:

- ◆ When you set up a Master server and then specify Slave servers, *any existing configuration* for the Slave server will be *overwritten*, and existing sessions on the Slave server will be deleted.
- ◆ It is important that you have followed the steps for importing trust certificates before you continue. This is a requirement regardless of your security settings.

On the SLAVE server that will replicate the Master:

- 1 Click **Slave**.
- 2 Check the **Database Status**. If **Up**, continue.
If **Down** or **Initializing**, wait until the changes take effect and the status is **Up**.
- 3 **Database Network Adapter**. Choose a network adapter associated with an IP address that the other MSS servers in the cluster can access.
- 4 **Global protocol**. Choose whether to **Use HTTPS for server to server communication** (between the Master and Slave servers). HTTPS is the default.

When you use HTTPS:

- ♦ You cannot change the transport and retain previously configured Slave servers. You must delete existing Slave servers before changing the protocol from HTTP to HTTPS (or vice versa).
 - ♦ If you installed MSS **on z Linux with no JRE**, be aware of the **Caution** stated in the [Configure master server](#) section.
- 5 Change the default **Passphrase**, if desired.
The Master server and all associated Slave servers must share the same passphrase. Use these fields to change the default passphrase. A changed passphrase is in effect for all replication implementations, whether or not HTTPS is used.
 - 6 Next step: [Add the master server](#).

Add the master server

A Slave server can be associated with only one Master Administrative Server. When configured, the Master is listed on this panel. To change the Master, delete the one in the list and click **+ Add**.

To add a **Master Server**:

- 1 Click **+ Add**, which expands the dialog.
- 2 Enter the **Master server host name**.
Add the fully qualified name of the Master server.
- 3 Enter the **Master port**.
The default host port is 443 for HTTPS and 80 for HTTP. Use the ports that you specified for HTTP and HTTPS during Management and Security Server setup.
- 4 Enter the **Servlet context**.
This entry specifies the web application context for the Master server. The servlet context is used in the URL that accesses the Master server, and is specified when the Administrative Server is installed.
The default, `mss`, is the correct value if you used the automated installer and did not change the default context as part of setup.
- 5 Click **Save**. to add the Master server to the list.
- 6 Select the server checkbox and click **Test Connection** to ensure the slave servers can communicate with the master.
- 7 Click **Apply** to save the configuration. To proceed, choose **Yes** on the Settings update confirmation. This confirmation causes the database to re-initialize to start the initial replication process with the master server.
This process can take some time. When the Database status transitions through, completing with an **Up** status, the initial replication is complete.

- 8 Click **Details** and ensure that all servers in the table show an 100% value in the **Owns** section.
- 9 The next step: Adding a slave to the master server.

Related Topics

- ♦ [Master Server Role](#)
- ♦ [Remove a running slave from a cluster](#)
- ♦ [Troubleshooting Replication](#)
- ♦ [Copying Package Data](#)
- ♦ [Upgrading Replication Servers](#)

Add a slave to the master server

- 1 From the **Configure Settings > Replication** panel on the master server, click **+Add** to add a slave server to the Slave Server table.
- 2 Enter the host name of the slave server you are adding.
- 3 Enter the port of the slave server. This will vary depending on what you entered in the **User HTTPS for server to server communication** setting. Click **Save**.
- 4 Select the newly added slave server and click **Test Connection** to ensure the master can now communicate with the slave.
- 5 Click **Apply** to save the newly added Slave. To proceed, choose **Yes** on the Settings update confirmation box. The Master will then contact all the slaves to let them know about the newly added slave. The database status will read *Status unavailable due to registry restart* while contact is being made, but will eventually transition back to the **Up** status when the process is complete.

Remove a running slave from a cluster

You can remove a running slave from a cluster and the slave will maintain all of its current data. However, after being removed from the cluster, the server will no longer receive replicated data.

To remove a running slave from a cluster:

- 1 From the **Configure Settings > Replication** panel on the slave server you want to remove.
- 2 Select the server from the Master server list and click **Delete**.
- 3 Set the **Server Role** to **Standalone** and click **Apply**.
- 4 To proceed, click **Yes** on the Settings update confirmation panel. The database status will cycle through Down, Initializing, and finally Up when the process is complete.
- 5 Click **Details** and verify that the address is **127.0.0.1**.
- 6 On the **Configure Settings > Replication** panel on the Master server, click **Details** and then **Remove** on the slave server you removed.
- 7 To proceed, click **Yes** on the Settings update confirmation panel. The database status will cycle through Down, Initializing, and finally Up when the process is complete.
- 8 Select the removed slave from the Slave Server table and click **Delete**.
- 9 Click **Apply** to save the removed Slave settings. To proceed, click **Yes** on the Settings update confirmation panel. The master contacts all the slaves to inform them about the removed slave. While this occurs, the Database status will be *Status unavailable due to registry restart*. The process completes with an **Up** status.

Remove a down slave from a cluster

When a slave server goes down and cannot be restarted, it must be removed from the cluster.

WARNING: If a down server is ever restarted, then the original cluster will be stuck in the Initializing status. To bring the server back into the cluster follow the first workaround in the [Troubleshooting Replication](#). To remove the server from the cluster follow the steps in [Remove a running slave from a cluster](#).

To remove a server from the database cluster:

- 1 From the **Configure Settings > Replication** panel on the Master server, open the **Database Status Details** dialog box and click **Remove** for the down server.
- 2 To proceed, click **Yes** on the Settings update confirmation panel. The database status cycles through **Initializing** and completes with an **Up** status once the server has been removed.
- 3 Select the down server from the Slave Server table and click **Delete**.
- 4 Click **Apply** to save the removed Slave settings. To proceed, click **Yes** on the Settings update confirmation panel. The master contacts all the slaves to inform them about the removed slave. While this occurs, the Database status will be *Status unavailable due to registry restart*. The process completes with an **Up** status.

Since the down server will not be able to be contacted you will receive an error message stating the it could not be updated. This is expected and you can safely dismiss it.

Related topics

- ♦ [Master Server Role](#)
- ♦ [Slave Server Role](#)
- ♦ [Troubleshooting Replication](#)

Copying Package Data

If you are replicating a 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 Slave server.

Package data needs to be manually copied from the Master server to each Slave server when:

- ♦ new packages are uploaded to the Master server.
- ♦ existing packages are updated or deleted from the Master server.

To copy the package data:

- 1 Upload, update, or delete packages on the Master server.
- 2 Delete all `.zip` files from the `/MSSData/deploy/packages/` directory from each Slave server.
- 3 Manually copy all of the `.zip` files from the `/MSSData/deploy/packages/` directory on the Master server to the analogous location on each Slave server.
- 4 To confirm success: Log in to Management and Security Server on a Slave server as a user who is authorized to receive the package. Verify that the package downloaded and installed successfully.

NOTE: If your client already has the package, first uninstall it from the client, and delete it from C:\Users\

Upgrading Replication Servers

If server replication is enabled, you must disable it on every server with replication before you upgrade. Follow these steps:

- 1 Set each Master server to **Standalone** and wait for the Database status to transition to **Up**.
- 2 Set each Slave server to **Standalone** and wait for the Database status to transition to **Up**.
- 3 Upgrade all the servers.
- 4 Follow the steps to:
 - ♦ [Configure master server](#)
 - ♦ [Add a slave to the master server](#)

Troubleshooting Replication

If you encounter any of these problems while configuring Replication, apply the appropriate workaround. For further assistance, contact Support.

- ♦ **Problem:** When setting an MSS server to a **Slave** role, the **Database Status** remains at **Initializing**, and in the **Details** view, the **Owns** value for all instances is less than 100%.

Workaround:

1. Set the server back to **Standalone** role and apply the change.
 2. From the **Configure Settings > Replication** panel on the Master server, open the **Database Status Details** dialog box and click **Remove** for the down server.
 3. To proceed, click **Yes** on the Settings update confirmation panel. The database status cycles through **Initializing** and completes with an **Up** status once the server has been removed.
 4. Add the server as a **Slave** again, and **Apply** the settings.
- ♦ **Problem:** When removing a database instance from a cluster using the **Details** view, the instance remains in the **Leaving** state.

(NOTE: The **Leaving** process for a database instance can take several minutes to complete.)

Workaround:

1. If the **Leaving** state does not change after a few minutes, open a command prompt in the <install-dir>/server/microservices/cassandra/bin directory.
 2. Enter the command: `nodetool removemode force`
- ♦ **Problem:** When setting a **Slave** to **Standalone** role, the **Database Status** remains at **Initializing**, and the **Details** view shows more than just the **Local Instance**.

(NOTE: The process for transitioning a server to **Standalone** role can take several minutes to complete.)

Workaround:

1. Open a command prompt in the <install-dir>/server/microservices/cassandra/bin directory.
2. Enter the command: `nodetool removemode force`

3. Open the **Details** view.
 - ♦ If only the **Local Instance** is showing, the status should change to **Up**.
 - ♦ If more than just the **Local Instance** displays, go back to the command prompt above, and enter the command: `nodetool removemode <host-id>`
where `<host-id>` is the Host Id shown in the **Details** view for the instance(s) to be removed.
 - ♦ **Problem:** When setting an MSS system to **Slave** role, and the **Database Status** remains **Down**.
Workaround:
 1. Change to the **Master** server role, and open **Details**.
 2. **Remove** the newly added slave, if present.
 3. Restart the **Slave** server.
 - ♦ **Problem:** When a server is on DHCP, either MSS fails to start, or the **Database Status** remains **Down**.
Workaround:
 1. As an administrator, open a command prompt in the `<install-dir>/server/microservices/cassandra/conf` directory.
 2. Open `cassandra.yaml` in a text editor.
 3. Note the value of "listen_interface", which should be similar to "eth0".
 4. Use a network utility such as **ifconfig** or **ipconfig** to determine the IP address of your network interface.
 5. Set the value of "seeds:" to your IP address that corresponds to the `listen_interface` value (step 3).
 6. Restart MSS.
-

Related topics

- ♦ [Master Server Role](#)
- ♦ [Slave Server Role](#)
- ♦ [Securing Replication Connections](#)

Logging

Use the options on this panel to configure the Management and Security Server logs. These logs show information about users' session activity, system configuration activity, and basic trace logging.

The **Log Viewer** utility provides detailed records and enables you to set filters, search message text, and change defaults. On Windows, the **Log Viewer** is available from the Start menu.

For more information, see [Using Log Viewer](#).

- ♦ ["Administrative Server" on page 91](#)
- ♦ ["trace.log" on page 91](#)
- ♦ ["Write client debug output to Java console" on page 91](#)

- ♦ [“Mark Log” on page 91](#)
- ♦ [“Credential store” on page 91](#)

Administrative Server

Set the level of logging for users' session activity and system configuration activity. You can configure the logs to keep a record of errors and informational messages or to log only errors; you can also disable the log altogether.

To view the information in the Administrative Server log, open [Run Reports - Log File Viewer](#) in the Administrative Console.

trace.log

Set the level of logging for the trace log. When analyzing server problems, Technical Support may request that this setting be changed to include debug information. You cannot disable this logging option.

The trace log file is located in the log folder within the MSSData folder.

NOTE: About 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`.

Upgrades from versions prior to 12.1 will retain the same log filename with the addition of version numbers appended to the end of the filename; for example, `logfile.txt.0`.

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`. For more information, see [Using Log Viewer](#).

Write client debug output to Java console

Do not enable this setting unless requested to do so by Technical Support.

When enabled, all subsequent launches of Management and Security Server will send debug information to the Java console.

Mark Log

Each time the **Mark Log** button is clicked, a searchable (LOG_MARK) message is written to the trace log files on all Administrative Servers. To locate the lines in the LogViewer, search for `LOG_MARK`.

Credential store

Set the level of logging for Credential Store activity. You can configure the logs to keep a record of errors and informational messages or to log only errors; you can also disable the log altogether.

To view the information in the credential store log, open [Run Reports - Credential Store](#) in the Administrative 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 93
- ◆ “Usage Metering Reports” on page 94
- ◆ “Credential Store Reports” on page 94
- ◆ “Security Proxy Server Reports” on page 95
- ◆ “Assigned Access Reports” on page 97

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.

Credential Store Reports

- ♦ [“Credential Store Users” on page 94](#)
- ♦ [“Credential Store Usage History” on page 94](#)

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.

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 Management and Security Server [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 95
- ◆ "Security Proxy server logs" on page 96
- ◆ "Connections per proxy server" on page 97

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:** The 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**.

7 Technical References

Technical References supplement the product Help with overviews and detailed articles.

- ♦ [“Using the Security Proxy Server” on page 99](#)
- ♦ [“Security Overview” on page 105](#)
- ♦ [“Credential stores used in Management and Security Server” on page 108](#)
- ♦ [“X.509 Certificates - Setup Requirements” on page 111](#)
- ♦ [“Updated Cryptographic Modules” on page 114](#)
- ♦ [“Using Log Viewer” on page 116](#)

Using the Security Proxy Server

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

[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” on page 100](#)
- ♦ [“Start the Security Proxy Server” on page 101](#)
- ♦ [“Using FIPS-Approved Mode” on page 102](#)

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](#).

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 installer 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 updated cryptomodules (since Management and Security Server 12.4 SP1) require a new setting for FIPS-approved mode. You must manually edit 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 **Action > 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 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/SSL security**.
- 4b Choose **TLS v1.2**, **TLSv1.1**, or **TLS v1**. (If you upgraded from a version that used TLS 1.0-1.2, all three are checked.)
(The versions may be listed as **TLS 1.2**, **TLS 1.0**.)
- 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.

Notes about Upgrading

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

- ♦ [“Match the version” on page 103](#)
- ♦ [“Synchronize the upgrade” on page 104](#)

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 [Management and Security Server Installation Guide](#).

Synchronize the upgrade

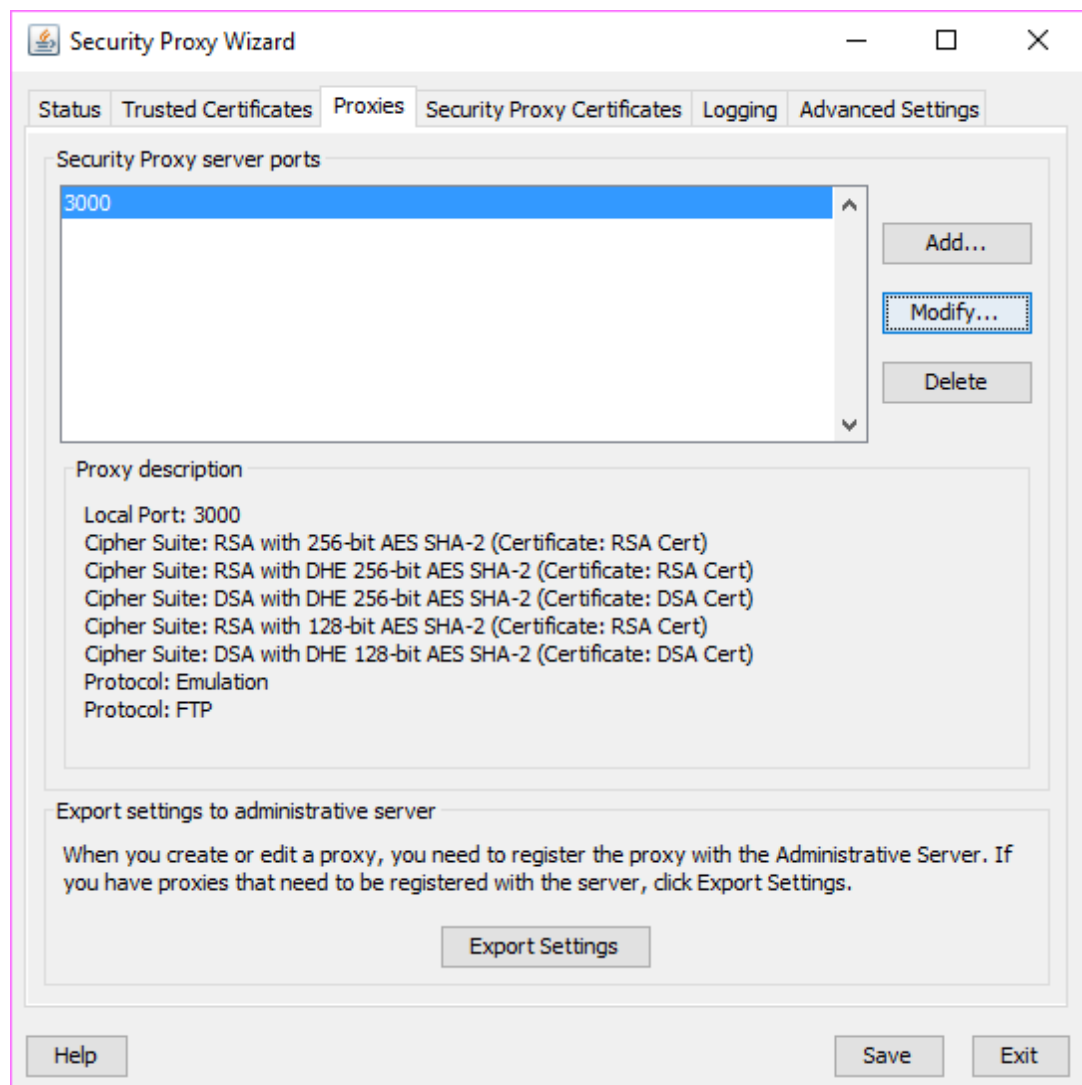
If Security Proxy is installed when you upgrade from Management and Security Server 12.4 to a later version (including updates and service packs), complete these steps to be sure the Security Proxy server is synchronized with the MSS Administrative Server.

After you upgrade:

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

Note the **Cipher Suites and Certificates**:

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



- 3 To select a different certificate for a particular port:
 - 3a Click the **Proxies** tab > **Modify**.
 - 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

[Management and Security Server Technical Resources](#)

[Management and Security Server Installation Guide](#)

Security Proxy Wizard (Open from the Start menu)

Management and Security Server Administrative Console - Help:

- ◆ [Security Proxy](#)
- ◆ [Manage Sessions](#)
- ◆ [Assign Access](#)

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/SSL Data Encryption” on page 105](#)
- ◆ [“FIPS-Approved Mode” on page 108](#)

TLS/SSL Data Encryption

Use the TLS/SSL data encryption options to secure the client-server data exchanges.

TLS/SSL Encryption between the Client Browser and the Management and Security Server

By default, Management and Security Server allows browsers to use the HTTP protocol to communicate between the client computer and the Management and Security Server. Although HTTP is universally available to web browsers, it is *not* a secure protocol. Information exchanged using HTTP is sent in clear text and is vulnerable to unauthorized access.

To secure your passwords and other sensitive data, you should require browsers to use the HTTPS protocol, which provides TLS/SSL encryption, when connecting to the Management and Security Server.

To require HTTPS:

1. Make sure TLS/SSL is enabled on your web server.

If you installed Management and Security Server with the automated installer, TLS/SSL is enabled by default.

2. Then, go to **Configure Settings - General Security** and check **Require HTTPS**.

NOTE: The **Require HTTPS** setting also forces any Java applets deployed by Management and Security Server to connect with the Management and Security Server using HTTPS. These applets are used when

- ♦ launching desktop sessions from the Java-based links list
 - ♦ launching Reflection for the Web sessions
 - ♦ configuring Reflection for the Web and desktop sessions from **Manage Sessions**.
-

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/SSL 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/SSL 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/SSLSettings) dialog to configure a session to use the Security Proxy. Check the option for **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 Management and Security Server

Management and Security Server (MSS) stores certificates and keys in several locations. Here's how the stores are used during a TLS/SSL 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/SSL 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 `.bckfs` (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`” on page 109](#)
- ♦ [“Keychain in `MSSData`” on page 109](#)
- ♦ [“Stores used by Tomcat in `server/etc`” on page 110](#)
- ♦ [“Stores used by Security Proxy in `proxyserver/keystores`” on page 110](#)
- ♦ [“cacerts in `jre/lib/security/cacerts`” on page 111](#)

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 [Table 7-1](#).

- ◆ **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**

Table 7-1 Stores used by MSS

| Keystore | Function |
|-------------------|--|
| client.bcfks | <ul style="list-style-type: none">◆ 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 | <ul style="list-style-type: none">◆ for the Management and Security Server certificate◆ signs the Security Proxy token |
| saml.bcfks | <ul style="list-style-type: none">◆ for SAML authentication |
| sshclient.bcfks | <ul style="list-style-type: none">◆ for Reflection for the Web SSH◆ not used by MSS itself |
| trustedascj.bcfks | <ul style="list-style-type: none">◆ for outbound HTTPS: Replication, Micro Focus Advanced Authentication, and Automated Sign-on for Mainframe◆ X.509 authentication client certificate validation and revocation checking◆ <i>not</i> used for LDAPS |
| trustedps.bcfks | <ul style="list-style-type: none">◆ 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 | <ul style="list-style-type: none">◆ contains only the public key and certificate from the <i>rweb.bcfks</i> store◆ Certificates from this store are imported by the Security Proxy server into its <i>trustedws.bcfks</i> 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/rweb.pwd, or in the KeychainUtility.
- ♦ **To change this password:** Administrative Console > **Configure Settings – General Security > Keychain**

Stores used by Tomcat in server/etc

The keystores in server/etc are described in [Table 7-2](#).

- ♦ **Keystore location:** %ProgramFiles%/Micro Focus/MSS/server/etc/
- ♦ **Password location:** Obfuscated in %ProgramFiles%/Micro Focus/MSS/server/services/servletengine-tomcat/META-INF/service.ctx.xml.
- ♦ **To change this password:** In /MSS/server/conf/container.properties, update these settings:

```
servletengine.system.ssl.keyStorePassword
management.server.client.ssl.trustStorePassword
```

Table 7-2 Stores used by Tomcat

| Keystore | Function |
|------------------------|--|
| servletcontainer.bcfks | <ul style="list-style-type: none"> ♦ Credential store for Tomcat HTTPS, all three ports ♦ Created at startup ♦ Used for the embedded web servers (Tomcat) |
| system.bcfks | <ul style="list-style-type: none"> ♦ Trust store for Tomcat HTTPS, trusted subsystem ♦ Created at startup ♦ Used for the Trusted Subsystem (X.509 authentication) |

Stores used by Security Proxy in proxyserver/keystores

The keystores in proxyserver/keystores are described in [Table 7-3](#)

- ♦ **Keystore location:** %ProgramFiles%/Micro Focus/MSS/securityproxy/keystores/
- ♦ **Password location:** hard-coded
- ♦ **To change this password:** This password cannot be changed.

Table 7-3 Stores used by Security Proxy

| Keystore | Function |
|-----------------|---|
| rwebps.bcfks | <ul style="list-style-type: none"> ♦ 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 | <ul style="list-style-type: none"> ♦ Stores the public key and certificate from rwebps.bcfks, noted above. |
| trustedws.bcfks | <ul style="list-style-type: none"> ♦ 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 |

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:

- ♦ used for LDAPS
- ♦ the trust store for outbound TLS
- ♦ combined with `trustedascj` for RASM, MFAA, replication, but not for LDAPS
- ♦ 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 log in to the Administrative Console. .

- ♦ [“Client requirements” on page 111](#)
- ♦ [“Replicated servers” on page 113](#)
- ♦ [“Optional: Administrative Console login” on page 113](#)

Client requirements

These settings are required for any client using X.509 certificates.

Table 7-4

| | |
|--------------------------|--|
| <input type="checkbox"/> | X.509 must be enabled in the Administrative Console: Configure Settings - Authentication & Authorization > X.509 . |
| <input type="checkbox"/> | Each client that is authorized to use Management and Security Server resources must have a client certificate, such as a certificate stored on a smart card, and a valid user account in LDAP. |
| <input type="checkbox"/> | The issuer of the client certificates must be trusted by Management and Security. For more information, refer to Trusted Certificates . |
| <input type="checkbox"/> | If using Replication, be sure to configure the Replicated servers . |

Check the requirements for your client:

- ◆ [“Host Access for the Cloud clients” on page 112](#)
- ◆ [“Windows-based clients” on page 113](#)

Host Access for the Cloud clients

These additional settings must be in place for Host Access for the Cloud.

Table 7-5

| | |
|--------------------------|---|
| <input type="checkbox"/> | A port configured for TLS client authentication must be enabled on the Management and Security Server. 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. |
| <input type="checkbox"/> | Note: A certificate to trust the Host Access for the Cloud Session Server is configured by the automated installer. No further action is needed, unless you want to manually add a CA-signed certificate to the MSS trust store . |
| <input type="checkbox"/> | If using Replication, be sure to configure the Replicated servers . |

To manually add a CA-signed or other certificate to the MSS trust store:

1. In the Administrative Console, open **Configure Settings - Trusted Certificates**.
2. Click **Management and Security Server**, and click **+Import**.
3. Enter the keystore file name, password, and friendly name.

Note: Make sure the file containing the certificate is on the Administrative Server in this folder:

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

4. Click **Import** to add the certificate.
 5. Restart the MSS Administrative Server.
-

Windows-based clients

These additional settings must be in place for Windows-based clients.

Table 7-6

| | |
|--------------------------|--|
| <input type="checkbox"/> | A port configured for TLS client authentication must be enabled on the Management and Security Server. This secure port authenticates end-user certificates presented by Windows-based clients (such as Reflection or Rumba+). |
| | <i>Note:</i> When using the MSS automated installer or an MSS configuration utility, this port is automatically configured. |
| <input type="checkbox"/> | The Administrative Server must be restarted after adding a CA-signed certificate. |
| <input type="checkbox"/> | If using Replication, be sure to configure the Replicated servers . |

Replicated servers

If you are using **X.509 authentication** and **Replication**, you must manually move your CA certificates for X.509 authentication, along with the `system.bcfks`, to the same location on *each* MSS Slave server in the replication cluster.

On *each* Slave server:

1. Locate the **MSSData** directory. This path is displayed in the Administrative Console: **About > Product Information**.
2. Copy the CA certificates to the `MSSData\certificates` directory.
3. Use the Administrative Console (**Configure Settings > Trusted Certificates**) to import the certificates into the Management and Security Server **Trusted Certificate List**. See **Help** for assistance.
4. Copy the `system.bcfks` from the Master to the same location on the MSS Slave:
`MSS\server\etc`
5. Restart the MSS Service on the Slave server (required for the changes to take effect).
6. Repeat these steps for *each* Slave server in the replication cluster.

Optional: Administrative Console login

You can use X.509 authentication to log in to the Administrative Console. In this instance, the Administrative Console acts as a client to the core MSS Administrative Server.

Use the Java keytool application to place the certificate in the expected location.

- 1 Add the root CA certificate to the MSS servletcontainer trust store.

```
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 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>:8443/mss
```

3 Navigate to the server URL using HTTPS.

Assuming that the user certificate is configured in the browser (details vary by browser), you can navigate to the adminconsole url:

```
https://<servername>:8443/adminconsole
```

Updated Cryptographic Modules

Beginning in version 12.4 Update 1 (12.4.1), Host Access Management and Security Server uses the **Bouncy Castle** provider for keystore operations. This article addresses some common questions.

- ♦ [“Why were the cryptographic modules changed?” on page 114](#)
- ♦ [“What changed in Management and Security Server?” on page 114](#)
- ♦ [“What do I need to do?” on page 115](#)

Why were the cryptographic modules changed?

Management and Security Server uses both internal and third-party FIPS-certified cryptographic libraries to perform various keystore and TLS operations.

In anticipation of the RSA BSAFE cryptography library reaching End of Primary Support (EOPS) in January 2017, Management and Security Server was re-configured to use the Bouncy Castle provider for keystore operations.

We also want to allow all customers to more easily use TLS 1.2 without requiring PKI Manager. The cryptographic changes support that ability.

What changed in Management and Security Server?

In brief, here's what changed:

- ♦ [“File extensions” on page 114](#)
- ♦ [“Certificate Signing Request” on page 115](#)
- ♦ [“Security Proxy Server” on page 115](#)

File extensions

Beginning in version 12.4 Update 1 (12.4.1), Management and Security Server generates keystores using the `.bcfks` (bouncy castle fips keystore) extension. The BCFKS store type was developed by Bouncy Castle to be FIPS Compliant.

MSS can still import `PKCS#12` keystores, including files with these extensions:

- ♦ `.p12` files, processed by the RSA BSAFE JCE provider `JsafeJCE`
- ♦ `.pfx` files, maintained by the Baltimore/ASCJ provider `ASCJ`

Certificate Signing Request

The Administrative Console does not provide the capability to generate a Certificate Signing Request (CSR). Instead, contact the CA directly. See [Generating a Certificate Signing Request \(CSR\)](#).

Security Proxy Server

An upgrade of the Security Proxy Server to version 12.4 Update 1 (12.4.1) may automatically select a certificate for use with the existing ciphers defined for a port.

Note: The ciphers previously configured for a given port will still be configured. Only the certificate will be auto-selected and associated with that port.

What do I need to do?

If either of these options apply to you, follow the steps below. If not, no further action is required.

- ♦ [“Using the Security Proxy Server” on page 115](#)
- ♦ [“Generating a Certificate Signing Request \(CSR\)” on page 115](#)

Using the Security Proxy Server

When you upgrade from Management and Security Server 12.4 to a later version or an update, you need to synchronize the Security Proxy as follows:

- 1 Open the **Security Proxy Wizard**.
- 2 On the **Proxies** tab, review the cipher suites and the auto-selected certificates for each security proxy server port.
- 3 Click **Save** and then **Export**.

This action synchronizes the Security Proxy with the MSS Administrative Server.

Generating a Certificate Signing Request (CSR)

To request a signed SSL certificate from a Certificate Authority (CA), choose a method:

- ♦ Use the **HTTPS Certificate Utility**, installed with Management and Security Server.

On the "Select a certificate action" screen, select **Generate a new private key and Certificate Signing Request** and proceed through the screens. Click **Help** for assistance.

After you receive the CA-signed certificate, return to this utility to import the certificate together with the private key that was generated by the utility.

- ♦ Work directly with a **CA** and follow their instructions. Here are some examples:

- Comodo
- DigiCert
- GeoTrust
- Thawte
- Symantec

For more details, see the Help for [Configure Settings - Certificates > Other certificates](#).

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.

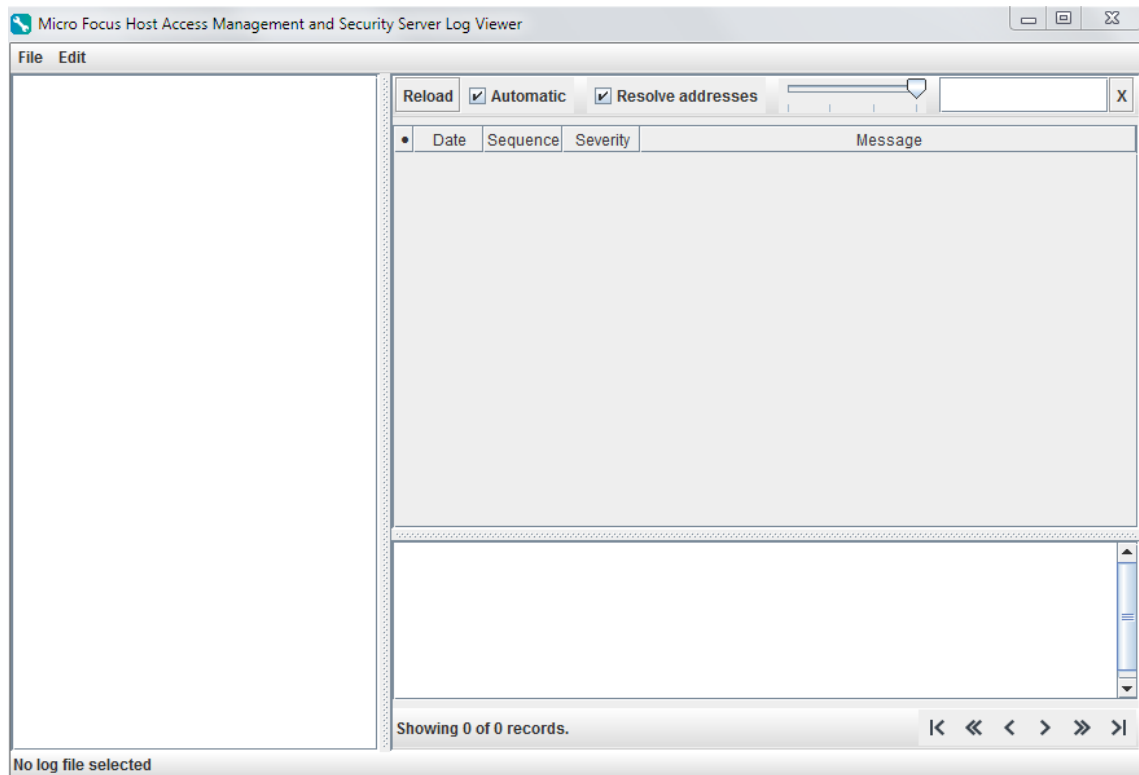
To use the Log Viewer

- 1 Open the Log Viewer.

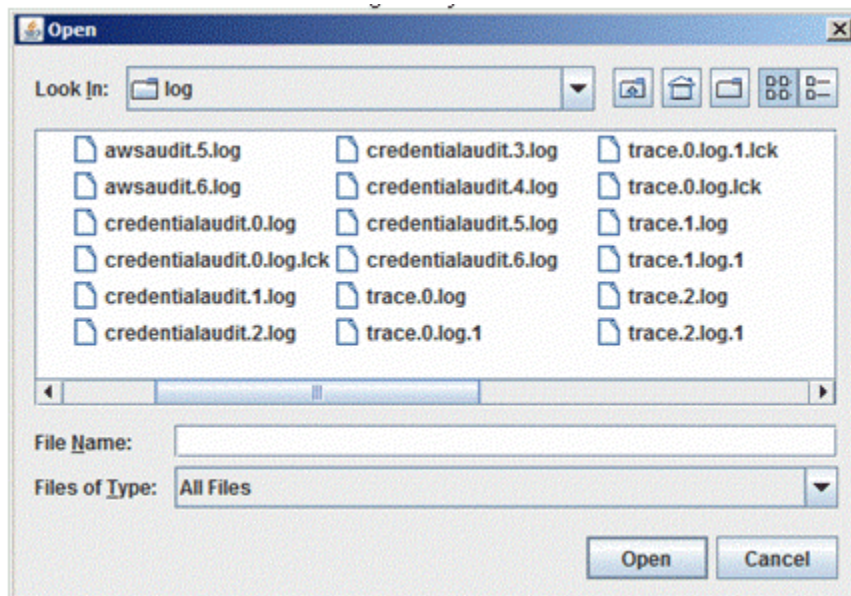
On Windows: Open from the **Start** menu, or double-click the executable:

`C:\Program Files\Micro Focus\MSS\utilities\bin\LogViewer.exe`

On Linux: `/usr/local/microfocus/mss/utilities/bin/LogViewer`

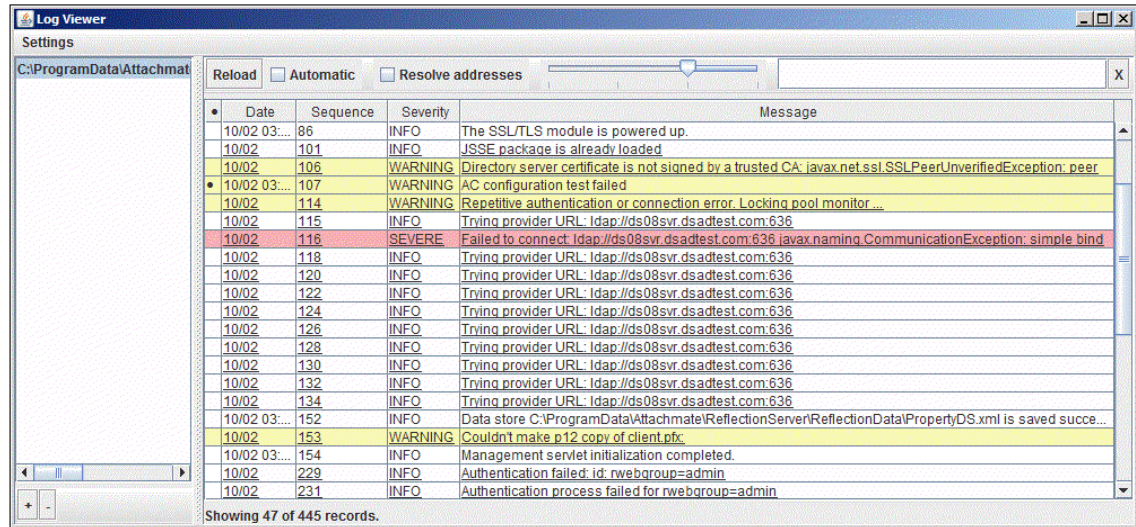


- 2 In the Log Viewer, click **File > Load**. (Shortcuts: **Ctrl+L** to Load, and **Ctrl+O** to Close.)
 - 2a Browse to the directory containing the log files you want to view.
 - 2b Select a log file and click **Open**.



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.
Click the **x** to clear the text field and view all messages for selected level control.

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.

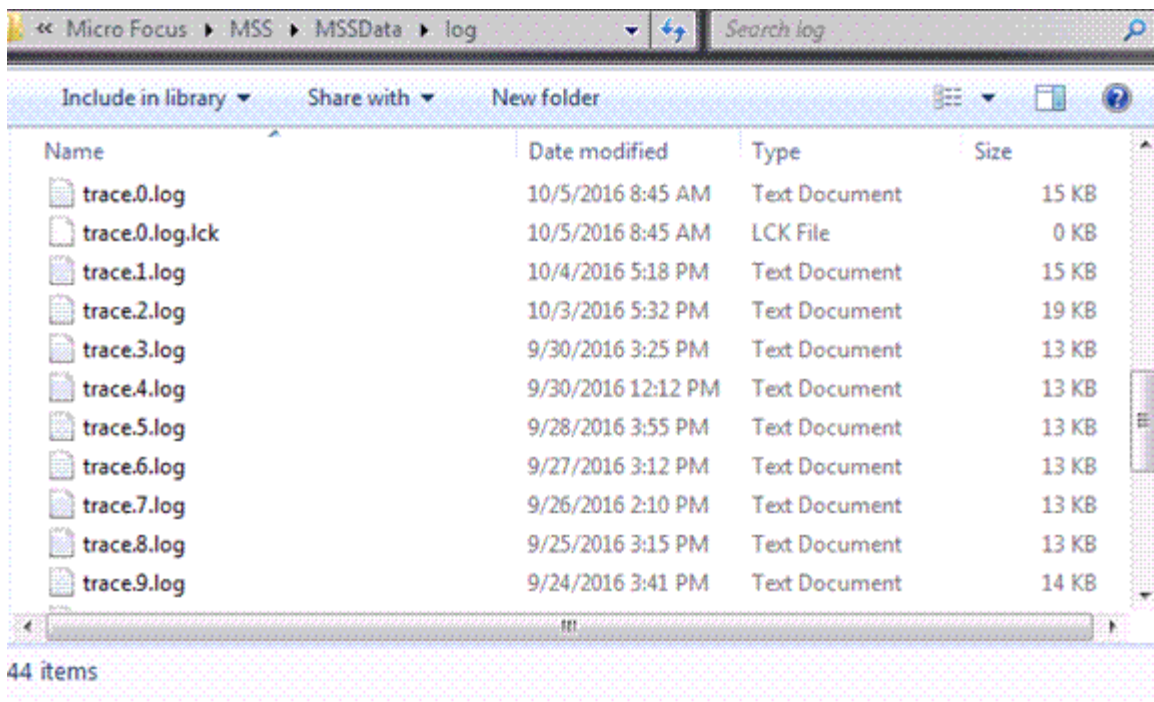
Gathering Log Files to View on another Server or to Send to Technical Support

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, send them to Technical Support.

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.7.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.

