MSS

Management and Security Server Administrator Guide

14.0.0

Table of contents

MSS Administrator Guide

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

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

MSS at a glance

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

About Management and Security Server

Release Notes

About the MSS Administrative Console

About Add-On Products

About MSS

About Management and Security Server

This Administrator Guide refers to Management and Security Server (MSS) 14.0.0. See the Release Notes for details.

In the MSS Administrative Console, open the **About** menu to view

Product Information

Support Diagnostics

Activated Products

Legal Information

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

Product Information

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

Support Diagnostics

When requested by Customer Support, use this option on the Product Information page to download an archive of logs and diagnostic data from all servers.

Click Download, enter your credentials, and click Download. The data is packaged into a single zip file that can be sent to Micro Focus Support.

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

Activated Products

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

Legal Information

View the license agreement and legal notices.

More information

- About the MSS Administrative Console
- About Add-On Products

About the MSS Administrative Console

Use the MSS Administrative (Admin) Console to centrally secure, manage, and monitor users' access to configured sessions.

The MSS Admin Console provides access to Cluster Management from the drop-down menu.
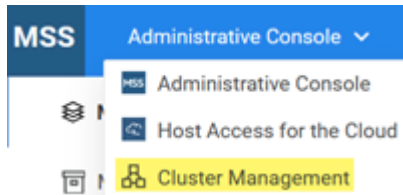
In this guide:

Manage Sessions

Manage Packages

Assign Access

Configure Settings

Run Reports

Technical References

More information

About Add-On Products

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:

Terminal ID Manager

Automated Sign-On

Micro Focus Advanced Authentication

More information

About the MSS Administrative Console

Manage Sessions

Manage Sessions

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

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

Add and launch a session

After the session is launched

Manage saved sessions

Add and launch a session

Add and Launch a Session

First, add a session for your product, and then configure specific settings.

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

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

3. Follow the steps for your product or session type.

Host Access for the Cloud

Reflection/InfoConnect Desktop

Reflection/InfoConnect Desktop - Workspace Automated Sign-on

Reflection for the Web

Rumba+ Desktop

Host Access for the Cloud

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

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

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

3. Enter a **Session name**.

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

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

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

7. As a next step, you can

Use Assign Access to make the session available to end users.

Return to Manage Sessions to add or edit a session.

Reflection/Infoconnect Desktop

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

To add, configure, and launch a session:

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

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

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

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

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

5. Configure your **File Storage** preferences.

   • **Overwrite setting files**

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

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

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

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

• **Save settings files as hidden**

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

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

My Documents `\<product folder>`

Temp

your specified `<User profile folder>\`

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

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

Using the MSS Client Launcher

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

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

> About the MSS Client Launcher
>
> Installing the MSS Client Launcher
>
> Launching sessions with the MSS Client Launcher

About the MSS Client Launcher

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

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

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

Installing the MSS Client Launcher

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

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

> Install the MSS Client Launcher before launching a session

or

> Follow the MSS Administrative Console prompts when you launch a session

Install the MSS Client Launcher *before launching* a session

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

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

On the administrator machine:

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

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

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

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

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

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

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

In the MSS Administrative Console:

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

2. Click **LAUNCH**.

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

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

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

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

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

> ⚲ **Note**
>
> You must have administrative permissions to install the Launcher locally.

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

Launching sessions with the MSS Client Launcher

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

> ⚲ **Note**
>
> The dialog buttons and text vary, depending on the browser being used.

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

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

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

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

4. See After the session is launched.

Reflection/InfoConnect Desktop - Workspace Automated Sign-on

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

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

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

Complete the prerequisites

Add and Configure the Workspace Automated Sign-on session

Assign Access to a Workspace Automated Sign-on session

Complete the prerequisites

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

End-user tasks:

Configure their Desktop client for Centralized Management.

Check the Enable automated sign-on for mainframes option.

See Step 6: Enable your emulator for automated sign-on in the *Automated Sign-on for Mainframe - Administrator Guide*.

Administrator tasks:

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

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

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

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

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

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

Add and Configure the Workspace Automated Sign-on session

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

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

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

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

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

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

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

> ## 💡 Note
>
> **Host name variations.** If clients connect to different variations of the host name, or if they connect to the host by its IP address, *each of those variations* needs its own *Workspace Automated Sign-on for Mainframe (ASM) session* with a matching name.
>
> For example, if the session is being configured to automatically log on to `blue.mycompany.com`, then the session name must be `blue.mycompany.com` — not `blue`, or `123.456.78.90`, or another variation.
>
> To enable sessions to automatically log on to a different host name, you must create separate sessions for EACH name.

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

    Click **BROWSE**.

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

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

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

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

Assign Access to a Workspace Automated Sign-on session

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

In particular, note the required **EDIT** option used to select the source of the user name on the host computer

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

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

Reflection for the Web

To add, configure, launch, and deploy a Reflection for the Web session, follow the instructions on this page.

Add a session and configure settings in MSS

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

To add and configure a Reflection for the Web session:

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

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

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

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

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

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

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

   Appearance | FTP | Advanced Settings | Applet Parameters

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

Appearance

Window title. You can change the title bar for the session with special characters. The title can include these special characters.

Character	Value
&&	a single ampersand
&c	Connection Status (whether you are connected and over what transport)
&d	Date
&h	Host name
&s	Session type
&t	Transport

Character	Value
`&v`	Terminal session identifier that uniquely identifies this terminal session from others. See specific types:
`&v for IBM 3270 and IMB 3270 Printer sessions	LU name`	
`&v for IBM 5250 and IBM 5250 Printer sessions	Device name`	
`&v for ALC. UTS Terminal, T27, T27 Printer, and Airlines Printer sessions`	Terminal ID

FTP

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

Show FTP Window as

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

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

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

Advanced Settings

Advanced > More Settings

Applet Parameters

Advanced > More Settings

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

Window Size and Status Bar

Window Size and Status Bar

- **Use best dimensions for each user**

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

- **Use maximized dimensions**

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

- **Use these window dimensions**

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

- **Display status bar**

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

View Session JNLP

The session JNLP (Java Network Launch Protocol) is automatically generated by the Management and Security Server. Except in special cases, there is no need to save the JNLP to a file.

If you do create a file with this JNLP content, use the `.mfjnlp` file extension to associate it with the Reflection for the Web Launcher. You must then distribute and maintain the `*.mfjnlp` files.

> 💡 **Note**
>
> Not all authentication schemes are supported when using JNLP saved to a file. Specifically, SAML and Windows Authentication - Kerberos are not supported.

Applet Parameters

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

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

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

To add a parameter

1. Click **+ADD**.

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

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

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

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

List of current parameters

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

Launch Reflection for the Web

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

For more information, see *Reflection for the Web Launcher* in the Reflection for the Web Deployment Guide.

When the Reflection for the Web Launcher is *not* **installed**, the session does not launch.

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

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

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

Next step: Configure the launched session

Configure the launched session

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

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

> **💡 Note**
>
> To set up **Metering**, you need to configure both the server and the client. See Metering for details.

Next step: Assign the session in MSS

Assign the session in MSS

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

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

For assistance, see Assign Access.

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

---

Distribute the Reflection for the Web Launcher to client workstations

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

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

For deployment options, see *Distribute the Reflection for the Web Launcher* in the Reflection for the Web Deployment Guide.

Rumba+ Desktop

To add and configure a Rumba+ Desktop session:

Complete the prerequisites

Upload the Rumba+ Session Profile

Edit a configured Rumba+ session

Complete the prerequisites

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

Configure a session in your Rumba+ application.

Save the session profile.

Enable **Centralized Management** in **Rumba+ Options**.

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

Upload the Rumba+ Session Profile

1. In the **MSS Administrative Console**, open **Manage Sessions**, and click **+ADD**.

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

3. Add a session, enter a Session name, and click **BROWSE**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Edit a configured Rumba+ session

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

2. In the MSS Administrative Console, 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.

After the session is launched

After the session is launched

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

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

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

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

3. As a next step, you can

   • Use Assign Access to make the session available to end users.

   • Return to Manage Sessions to add or edit a session.

Manage saved sessions

Manage saved sessions

You can modify your saved sessions that are listed in the Manage Sessions table. Follow the steps on this page to Delete, Import, Export, Edit, Copy, or Convert your sessions.

To **ADD** a session, see Add and Launch a Session

> ♀ **Note**
>
> Options are enabled for certain session types. For instance,
>
> only Host Access for the Cloud sessions can be exported and imported.
>
> only Reflection for the Web sessions can be converted (to Host Access for the Cloud).

Delete sessions

Check one or more sessions that you want to delete and click **DELETE**. The deleted sessions are removed from the list.

Import sessions

Applies to only Host Access for the Cloud sessions.

Click **IMPORT** and navigate to the zip file containing the Host Access for the Cloud sessions that you want to import to this MSS server. The zip file should have been generated when Exporting session data from another MSS.

Export sessions

Applies to only Host Access for the Cloud sessions.

Select one or more Host Access for the Cloud sessions to be exported and click EXPORT. A zip file containing the exported session data is generated and placed in the browser's download folder.

> ⚠️ **Caution**
>
> If the selected session contains sensitive information, that data will be included in the export package.

Edit a session

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

2. Use the scroll bar to see the available settings. Note that the **Properties** are not editable.

3. Change the settings you wish to edit. Configuration details for your session type are described in Add and Launch a session.

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

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

Copy a session

You can add a new session with the same properties.

1. In the **Manage Sessions** list, check or right-click the session that you want to copy, and click **COPY**.

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

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

> ♀ **Note**
>
> The copied session does not automatically have the same access rights. You need to assign access to the new session.

Convert a Reflection for the Web session

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

To convert a session:

1. In the **Manage Sessions** list, locate the Reflection for the Web session you want to save as a Host Access for the Cloud session type.

> 🔥 **Hint**
>
> Reflection for the Web session types are identified by a globe icon next to the terminal type, such as 3270: 🌐 3270 .

2. Check or right-click the session and click **CONVERT**.

3. On the **Convert session** panel, enter the name of 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.

More information

Add and Launch a session

Manage sessions

Manage Packages

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

First, you must 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.

Upload a new package

To add a package that can be centrally deployed:

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

2. Add a Description for your reference.

3. Click **SAVE**.

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

Update an existing package

You can replace an existing package with an updated version.

1. In the list of packages, check the one 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.

Delete a package

To delete a package, check it from the list and click **DELETE**.

Deploy a package

Use Assign Access to assign packages to users or groups.

Assign Access

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

Currently Assigned

Providing Access to Assigned Sessions

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

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](#).

Assign Sessions or Packages

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

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

> ♀ **Note**
>
> You can assign access by inheritance. See these examples.
>
> • An **asterisk (*)** next to the Session name denotes that a user has inherited access to that session by being a member in a group.
>
>   For example: JohnUser is a member of Group A. If you assign Session1 to Group A, then JohnUser inherits access to Session1. When viewing JohnUser's assigned sessions, an asterisk appears next to Session1.
>
>   *To remove a user's access to an inherited session*, click the User, and **clear** the **Allow user to inherit (*) access to sessions** check box (below the list of sessions).
>
> • Granting access to **All users** means granting access to the search base, and every user inherits that access. Such access is extended to individual users only when the **Allow user to inherit (*) access to sessions** option is **checked**.
>
> • Sessions cannot be assigned to Active Directory primary groups (such as Domain users).

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

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

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

   To assign an automated sign-on session, click **EDIT**. Then continue with Source of user name on host computer.

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

5. To assign sessions to a different user or group, repeat the steps to Search & Assign.

Source of user name on host computer

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

> 💡 **Note**
>
> To recap, the configuration of either **Automated Sign-On for Mainframe** or **Automated Sign-On for Host Access** requires:
>
> • The Automated Sign-On add-on product is installed and configured on MSS.
>
> • A session to the host was created with a log-in macro. See Automated Sign-on for Mainframe - Administrator Guide or Configuring MSS Automated Sign-On for Host Access.
>
> • The session is assigned to the appropriate user or group.
>
> • The method for obtaining the 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 user name on host computer** 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 user's name on the host computer**:

 • **Not set**

   This default must be changed for automated sign-on.

 • **UPN**

   Select this option to derive the user's name on the host system from the user's User Principal Name (UPN). 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 MSS derives the user name as the short name preceding the `@` symbol.

   In the drop-down, select your server for one-time password requests:

MSS Automated Sign-On for Host Access Service

DCAS server: `<hostname:port>`

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

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

1. Enter the LDAP attribute, using the specified criteria.

> 💡 **Note**
>
> All LDAP attributes must meet these *criteria*:
>
> must begin with an alpha character
>
> must be no more than 50 characters
>
> may be any alphanumeric character or a hyphen (-)

2. Select your server for one-time password requests:

MSS Automated Sign-On for Host Access Service

DCAS server: `<hostname:port>`

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

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

1. Select the LDAP attribute. Note the *criteria for LDAP attributes*, listed above.

2. Select your server for one-time password requests:

MSS Automated Sign-On for Host Access Service

DCAS server: `<hostname:port>`

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**.

Currently Assigned

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

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

Click Details to see the attributes and associated users or groups.

You can also run a report to see the currently assigned sessions or packages. See Run Reports - Assigned Access.

Providing Access to Assigned Sessions

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

After a user authenticates to the MSS server, they see their list of entitled sessions. The list is available at `https://<mssserver>/sessions/`

Requirements: Sessions from the following products may be launched from the **Assigned Sessions** list or other means, as noted:

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

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

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

  Users can also launch their sessions by saving the direct URL to the session. Centralized management does not need to be configured.

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

  Users can also launch their sessions by saving the direct URL to the session. Centralized management does not need to be configured.

- **Rumba+ Desktop** (10.1 SP1 or higher)

  Users can also launch their sessions by saving the direct URL to the session. Centralized management does not need to be configured.

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

  Users may need to first download and install the RWeb Launcher to open their assigned sessions.

Configure Settings

Configure Settings

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

General Security

Secure Shell

Certificates

Trusted Certificates

Credential Store

Authentication & Authorization

Product Activation

Automated Sign-On

Logging

Migration

General Security

General Security

The General Security panel prompts you to set (or change) passwords and set other security options.

Change administrator password

Require new login

Smart card settings

Certificate chooser prompt

Enable identity verification

Change the 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
```

> **Important**
>
> The MSS Administrative Console password is also used to log in to the Metering Console and Terminal ID Manager. One administrator password opens each of these MSS services.

Change administrator password

To change the administrative password, open **Configure Settings - General Security** in the MSS Administrative Console. Enter the current password; then enter and confirm the new password.

> **Note**
>
> This action also changes the administrator password for the Metering Console and Terminal ID Manager.

Reset the administrator password

In the case that the administrator password needs to be reset to access the **Administrative Console**, follow these steps.

To reset the administrator password:

1. Using ssh, make a terminal connection to any node in the cluster.
2. Execute the following commands:

```
/opt/opentext/csp/bin/kubectl delete secret mss-auth-service-admin -n mss
```

```
/opt/opentext/csp/bin/kubectl rollout restart statefulset mss-mss-server -n mss
```

3. Log into the Administrative Console using the now reset default password of `admin`.

If using the Appliance, you can access the command prompt in one of the following ways:

Use your virtualization console to access the command prompt

- Enable and use SSH

  a. Using a browser, log in into `https://clusternode:9443`

  b. Select System Services.

  c. Select SSH.

  d. Click Action and select Start.

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)

The MSS Server times out when a user has not launched a session or otherwise interacted with MSS during the specified time. The user must log in again to open a new host session or access the MSS 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.

Smart card settings

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

The default setting

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

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

Smart card libraries

Applies to: Reflection for the Web

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

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

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

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

About smart card parameters

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

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

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

Smart Card Provider

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

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

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

Certificate Attributes

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

The default parameter specifies these attributes:

```
KU+DIGSIG,KU-NONREP,EKU+CLIAUTH,EKU+SCLOGIN,EKU-EMLPROT;
```

```
KU+DIGSIG,KU+NONREP,EKU-NONE
```

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

- `KU+DIGSIG` : Key Usage of Digital Signature OID MUST be present in the certificate.

- `KU-NONREP` : Key Usage of Nonrepudiation OID MUST NOT be present in the certificate.

- `EKU+CLIAUTH` : Extended Key Usage of Client Authentication OID MUST be present in the certificate.

- `EKU+SCLOGIN` : Extended Key Usage of Smart Card Login OID MUST be present in the certificate.

- `EKU-EMLPROT` : Extended Key Usage of Email Protection (called Secure Email) OID MUST NOT be present in the certificate.

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

- `KU+DIGSIG` : Key Usage of Digital Signature OID MUST be present in the certificate.

- `KU+NONREP` : Key Usage of Nonrepudiation OID MUST be present in the certificate.

- `EKU-NONE` : Extended Key Usage MUST NOT be present in the certificate.

Certificate chooser prompt

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

Show certificate prompt

This default option requires the user to choose the correct certificate each time they log on.

In the displayed list, the **Type** column can help to identify the proper certificate.

Show certificate prompt and allow user to save selection

This option allows the user to save the certificate selection.

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

Enable identity verification

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

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

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

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

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

Secure Shell

Secure Shell

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

[Known Hosts List](#)

[Shared User Key Pair](#)

Known Hosts List

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

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

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

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

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

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

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

   ```
   mySSHhost,10.10.1.1 ssh-rsa AAAAB3NzaB1yc2EAAAABIwAAAIEA0WR3aIRtilXquUmXtxw5oi3rMkhY9jw/lV03WvUNvSb/
   xQnIfoMeserY5DfU8+eqUPzLX0efJMik22VFAzFo+ZCOnlHbj39yNi2a1/7dAJYECaHo7pxhILHAZxXbwOpWSms3aaccWOOEA+Fyzv8Dppp(
   fWVvXWNGR22sU=
   ```

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

4. Click **Upload**. Select the file containing the public key to upload to the MSS Server.

5. Enter the required information:

   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

+ IMPORT

EXPORT

Shared User Key Pair Details

+ 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. Click **UPLOAD**. Select the file containing the key pair to upload to the MSS Server.

2. If the keys are in **OpenSSH** format files, upload the public key first, followed by the private key. The public key must have the same name as the private key and a .pub extension.

3. If the keys are in a **.PFX** format file, upload that one file.

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

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

6. 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.

1. 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 packaged in a zip file and downloaded to your browser.

2. Check or enter the required information:

   - **Export the private key with the public key** - otherwise, only the public key is exported.

   - **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.

Certificates

Certificates

Use the Certificates panel to import a signed client certificate to share. This panel is only functional when Reflection for the Web is installed.

Administer Shared Client Certificate

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

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

To import the key pair:

1. Click **Upload**. Select the file containing the certificate and the private key to upload to the Management and Security Server.

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**.

Trusted Certificates

Trusted Certificates

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

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

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

Certificate Store - Terminal Emulator Clients

Certificate Store - Management and Security Server

Certificate Store - Terminal Emulator Clients

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

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

To add a client certificate to the MSS trust store:

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

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

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

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

5. Restart the MSS Server.

See (collapsed by default).

Certificate Store - Management and Security Server

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

This collection is used for the following features:

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

    For these features, certificates are added to establish the other server as known and trusted.

- **Automated Sign-On for Mainframe:** Add a certificate(s) to establish trust of a Mainframe host.

- **Micro Focus Advanced Authentication (MFAA):** Add certificate(s) to trust the MFAA host.

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

To add a server certificate to the MSS trust store:

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

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

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

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

5. Restart the MSS Server.

> **Important**
>
> When **X.509 with Fallback to LDAP authentication** is used in conjunction with other MSS 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

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

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

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

Credential Store - Reflection for the Web

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

Check **Enable credential store** to save new credentials or to 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 backup the key

1. First, shell into an application instance (pod) in Kubernetes:

   a. Log in to the Kubernetes Dashboard. See the *MSS Deployment Guide* for instructions to use the Kubernetes dashboard.

   b. Under Workloads, click Pods.

   c. Use the Name column to locate the pod named `mss-mss-server` . Use the dashboard's Filter button to narrow the list of pods with that name.

   d. Click ⋮ Exec, which opens a shell to access the pod's file system.

2. After you have shelled into an mss pod, then run this command, to backup PropertyDS.xml:

   `cp /mssdata/PropertyDS.xml /mssdata/PropertyDS.bak`

3. Exit the shell, and exit K8S Dashboard.

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**.

Authentication and Authorization

Authentication and Authorization

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

Choose Authentication Method

Choose Authorization Method

Enabling/Disabling OAuth

LDAP Server Configuration

Single Sign-on through IIS

Windows Authentication - Kerberos

OpenID Connect

X.509

SiteMinder

Micro Focus Advanced Authentication

SAML Authentication

Choose Authentication Method

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. The setup options vary based on your selection.

- **None** — Management and Security Server does not present a login screen. Any user can access their assigned sessions without being prompted for credentials. Session authorization is not available.

- **LDAP** — Management and Security Server makes a read-only connection to your existing LDAP (Lightweight Directory Access Protocol) server to verify usernames and passwords. You can also use LDAP to authorize session access. LDAP is an industry standard application protocol for accessing and maintaining distributed directory information services over a network.

> **Note**
>
> You can enable more than one LDAP server.

- **Single sign-on through IIS** — This method uses Microsoft's IIS web server. You can find more information in the MSS Deployment Guide.

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

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

- **OpenID Connect** — OpenID Connect (OIDC) is an open standard security protocol that delegates authentication to a third-party identity provider.

- **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. Be sure to check the setup requirements.

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

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

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

Choose Authorization Method

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.

Enabling/Disabling OAuth

Be sure OAuth is enabled when configuring these authentication methods:

Windows Authentication - Kerberos

OpenID Connect (OIDC)

X.509

Micro Focus Advanced Authentication

To enable OAuth

1. In the Administrative Console, open Cluster Management from the top left drop-down.

2. On the Services page, locate `mss-mss-server`. Click `···` Edit Properties.

3. Add a new Key/Value entry. Set the **Key** to `mss.oauth` and set the **Value** to `true`. Click OK.

4. Click ⋯ Redeploy All to redeploy the `mss-mss-server` service.

5. Wait until the redeployed services are in a ready state ✅.

> 💡 **Note**
>
> If the Cluster DNS changes, the `mss-auth-service` must be redeployed for the changes to take effect.
> Be aware that end users may be affected when a service is redeployed.

6. Remember to select your preferred authentication method in the MSS Administrative Console (Configure Settings - Authentication and Authorization > Choose Authentication Method). Then continue with your configuration.

Windows Authentication - Kerberos

OpenID Connect (OIDC)

X.509 Configuration

Micro Focus Advanced Authentication

To disable OAuth

1. In the Administrative Console, open Cluster Management.

2. On the Services page, locate `mss-mss-server`. Click ⋯ Edit Properties.

3. Locate the `mss.oauth` key and set the **Value** to `false`. Click OK.

4. Click ⋯ Redeploy All to redeploy the `mss-mss-server` service.

5. Wait until the redeployed services are in a ready state ✅.

6. Choose another Authentication method in the MSS Administrative Console.

LDAP Server Configuration

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

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 the Kubernetes dashboard:

   a. From the MSS Administrative Console drop-down menu, click Cluster Management.

   b. Click Advanced, and slide the button to enable the Kubernetes dashboard.

   c. Copy the authentication token, click the URL, and paste the token into the field provided.

   d. Click Sign in.

2. Shell into an application instance (pod) in Kubernetes:

   a. Under Workloads, click Pods.

   b. Use the Name column or the Filter to locate an `mss-mss-server` pod.

   c. On the far right, click ⋮ **Exec** to open a shell to access the pod's file system.

3. At the shell prompt:

   a. Make a backup copy of PropertyDS.xml:

   ```
   cp /mssdata/PropertyDS.xml /mssdata/PropertyDS.bak
   ```

   b. Then, use the built-in nano editor to open PropertyDS.xml for editing:

   ```
   nano /mssdata/PropertyDS.xml
   ```

   c. Press `Alt+C` to show the line numbers in nano

   d. Use the arrow keys to navigate to these XML elements, found around line 15

   ```
   <CORE_PROPERTY NAME="AC.DirAllowMultiLdap">
       <BOOLEAN>false</BOOLEAN>
   </CORE_PROPERTY>
   ```

   e. Change the Boolean value from `false` to `true`.

   f. Press `Ctrl+O` then ENTER to write the file.

   g. Press `Ctrl+X` to exit the editor.

4. Return to the MSS Admin Console's **Cluster Management** view.

   a. Click Services, and locate the `mss-mss-server` service.

   b. Click ⋯ Redeploy All.

> 🔥 **Important**
>
> Be aware that end users may be affected when a service is redeployed.

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

   Or, if you are configuring **Windows Authentication - Kerberos**, return to Configuring Kerberos.

> 💡 **Note**
>
> To revert to a single LDAP server, set the property value to `false`, save the file, and redeploy the MSS server.

LDAP Configuration

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

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

- **Server type**

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

- **Security options**

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

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

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

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

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

- **Server name**

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

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

  Windows Active Directory and **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 MSS running on **Windows**.

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

- **Server port**

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

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

- **Username and Password**

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

> **♀ Note**
>
> The username must uniquely identify the user in the directory. The syntax depends on the type of LDAP server you are using.
>
> - For **Windows Active Directory** with **Plain Text**, enter
>
>   **NetBIOS domain\sAMAccountName** (such as `exampledomain\username`) **userPrincipalName** (such as `username@exampledomain.com`) or **distinguished name** (such as `uid=examplename,DC=examplecorp,DC=com`).
>
> - For **any other LDAP** server type, enter the **distinguished name** (such as `uid=examplename,DC=examplecorp,DC=com`).
>
> If this account password changes, be sure to update the account password here and apply the new settings.
>
> To avoid this problem, you may wish to set up an account that is not subject to automatic password aging policies, or that cannot be changed by other administrators without notice.

Search Base and Groups/Folders

- **Directory search base**

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

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

> **ⓘ Info**
>
> If you are using LDAP authorization with OpenID Connect, return to Configuring OpenID Connect.

Groups or folders

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

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

Certificate

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

Authentication of End Users

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

Default LDAP identifiers:

Server type	Default user identifier
OpenLDAP Directory Server	cn
Generic LDAP Compliant Directory Server (RFC 2256)	cn
Oracle LDAP Directory Server	uid
Windows Active Directory	List of domains*
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 MSS 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. Be careful not to raise this level more than necessary because too high a number can impair performance when you have a large number of users. The default is `5` .

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

Single Sign-on through IIS

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

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

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

Configure MSS for Single Sign-on through IIS

First, integrate IIS with MSS using the detailed steps in the MSS Deployment Guide.

Then select the "Single sign-on through IIS" as the authentication method.

Troubleshooting IIS Integration

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

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

  Resolution:

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

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

- *Error*: "Request Entity Too Large"

  Resolution:

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

   `worker.ajp13_worker.max_packet_size=65536`

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

   `servletengine.ajpMaxPacketSize=65536`

Circumstantial Credential Prompts When Using Single Sign-on

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

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

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

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

- If the `management.server.iis.url` property contains periods (such as `http://www.microsoft.com` or `https://10.0.0.1`), the requested address is assumed to exist on the Internet for some browsers; credentials are not passed automatically, and a credentials prompt will appear.

  However, Edge can be configured to automatically pass credentials for such an address by adding it to the AuthServerAllowList. Refer to your browser's documentation for support of an equivalent setting.

Windows Authentication - Kerberos

Windows Authentication - Kerberos

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

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

✏️ **Support**

Kerberos is supported in

Reflection Desktop (configured for centralized management)

Host Access for the Cloud (HACloud)

the Assigned Sessions List, which can launch Reflection Desktop, HACloud, and Reflection for the Web

---

Enabling Kerberos

1. First, enable OAuth.

2. Then, in the MSS Administrative Console, click Configure Settings - Authentication & Authorization
   > **Windows Authentication - Kerberos**.

Requirements

To experience full Kerberos authentication, users must

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

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

Kerberos Terminology

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

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

Term	Definition
Service Principal Name (SPN)	The Service Principal Name uniquely identifies a service instance. SPNs are used to associate a service instance with a domain logon account.

Configuration Steps

Follow the detailed steps to set up **Windows Authentication - Kerberos**.

Configuring Kerberos

Troubleshooting Kerberos Configuration

Disabling Kerberos

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

Configuring Kerberos

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

> 💡 **Note**
>
> If using a load balancer, use its information for the Cluster DNS value and Service Account.

Configure KDC and Active Directory

To configure **Windows Authentication - Kerberos** authentication, these steps must first be done on the KDC:

Create a Service Account

Assign an SPN

Create a keytab

Create a Service Account for your MSS deployment

1. Open **Active Directory Users and Computers** (Start | Administrative Tools | Active Directory Users and Computers).

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

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

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

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

6. Click **Next**.

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

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

9. Check **Password never expires**.

10. Click **Next**.

11. Click **Finish**.

Assign an SPN for the Cluster DNS to the Service Account

1. Open a command prompt with Administrator rights.

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

3. Type the command

   `setspn -A HTTP/<fully-qualified-cluster-DNS> <service-account-name>`

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

4. To verify the SPN was successfully added, type the command

   `setspn -L <service-account-name>`

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

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

1. Open a command prompt with Administrator rights.

2. Type the command

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

   Example:

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

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

> **✏ Notes**
>
> The keytab file contains sensitive data, so be sure to protect it accordingly.
>
> You can use any name for the keytab file.
>
> When setting up a cluster of MSS servers, this keytab file with a single SPN is all that is needed.

Update supported encryption types and delegation rights in the SPN

1. Open Active Directory Users and Computers (Start | Administrative Tools | Active Directory Users and Computers).

2. In the left menu, click the Active Directory domain to expand the tree.

3. In the list of containers, click Users.

4. Find the user that was created in step 5 of the Configure KDC and Active Directory section.

5. Right-click that user and click Properties.

6. Open the Account tab.

7. In the Account options dialog, scroll to the bottom of the options list.

   Locate and CHECK these two items:

This account supports Kerberos AES 128 bit encryption

This account supports Kerberos AES 256 bit encryption

Account options:

☐ Use only Kerberos DES encryption types for this account
☑ This account supports Kerberos AES 128 bit encryption.
☑ This account supports Kerberos AES 256 bit encryption.
☐ Do not require Kerberos preauthentication
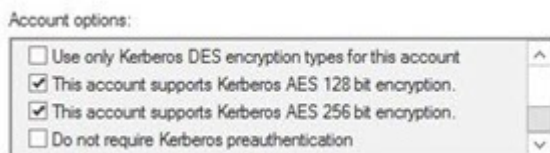
> **💡 Note**
>
> In the event a Kerberos Unsupported etype error is received, check "Do not require Kerberos preauthentication".
> For more information, see this Microsoft article.

8. Open the Delegation tab.

   Notice the default setting: Do not trust this user for delegation.

9. Click these two items:

Trust this user for delegation to specified services only

Use any authentication protocol

10. Add the service `ldap` for the LDAP server that will be used to assign users.

11. Click Apply and OK.

Settings in the MSS Administrative Console

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

1. Be sure to enable OAuth to enable the Kerberos settings.

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

3. Select the desired **Authorization** method.

4. In the Kerberos Configuration section, enter the following:

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

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

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

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

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

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

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

   (See LDAP Configuration for further details).

6. Click **Apply**.

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

Configure your browser for Kerberos

To sign in using Kerberos, your browser must be configured correctly for Windows Authentication via Kerberos and your machine must be a member of the proper domain (Kerberos realm).

Consult your browser's Help for instructions on how to enable Kerberos.

Verify your Kerberos configuration

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

Steps to verify:

1. Use a client system that is a member of the Active Directory domain.
2. Log on to the client system using the credentials of a user that is a member of the Active Directory.
3. Be sure to Configure your browser for Kerberos.
4. Once configured for Kerberos, use that browser to access the url:

   ```
   https://<fully-qualified-cluster-dns>/osp/a/hc/auth/app
   ```

5. To verify your Kerberos configuration:

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

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

> **Note**
>
> When using Kerberos authentication for **Reflection Desktop** clients, the browser on the client system must also be configured. See Configure your browser for Kerberos.

Troubleshooting Kerberos Configuration

Increase the logging level

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

1. Log in to the MSS Administrative Console at `https://hostname/adminconsole` .

2. Click Cluster Management from the drop-down menu.

3. On the Services page, locate `mss-auth-service` .

4. Click **...** Edit Properties and add this Key/Value pair:

Key: `authsvc.logging.level`

Value: `DEBUG`

5. Click OK.

6. On the `mss-auth-service` line, click **...** Redeploy All.

> 💡 **Note**
>
> Be aware that end users may be affected when a service is redeployed.

Locate log files

The log output for Kerberos and OAuth operations can be viewed in Cluster Management - Services.

1. Click `mss-auth-service` to see a more detailed view of the auth-service.

2. In the detailed view, click **...** and then either View Recent Logs or Download Logs.

Identify specific issues

Check the possible causes for issues you may encounter.

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

Issue	Possible cause
Kerberos authentication fails for users who belong to a large number of Active Directory groups	- The authentication string is too large. **Resolution:** Edit the properties of the `mss-auth-service` by adding this key/value pair: Key: `server.max-http-header-size`, Value: `10MB` For instructions, see Setting Advanced Properties.

OpenID Connect

OpenID Connect

OpenID Connect (OIDC) is an open standard security protocol that delegates authentication to a third-party identity provider.

To use OpenID Connect, configure the OpenID Connect provider, and then configure OpenID Connect in MSS.

> ✏️ **Support**
>
> OIDC is supported in
>
> Reflection Desktop (configured for centralized management)
>
> Host Access for the Cloud (HACloud)
>
> MSS Administrative Console
>
> the Assigned Sessions List, which can launch Reflection Desktop, HACloud, and Reflection for the Web

Configuring the OpenID Connect Provider

1. Create a new application.

2. Enter `https://<Cluster DNS value>/osp/a/hc/auth/app/contractcontinue` as the Callback URL.

3. Select the `openid`, `profile,` and `email` scopes.

4. Save the application.

Configuring OpenID Connect in MSS

1. First, enable OAuth.

2. Log into the MSS Administrative Console.

3. Click Configure Settings - **Trusted Certificates**.

4. Click **Management and Security Server** as the Certificate Store.

5. Import the OIDC Provider certificate.

6. Then, click Configure Settings - **Authentication & Authorization**.

7. Click **OpenID Connect** as the Authentication Method.

8. If you prefer to use LDAP for the Authorization method instead of allowing all authenticated uses to access all published sessions, see Using LDAP as the Authorization method.

9. Enter the **Provider URL**.

10. Enter the **Client ID**.

11. Enter the **Client Secret**.

12. The default **Source attribute** is `email`, but you can set it to `preferred_username` to identify the user by username instead of email address.

Using LDAP as the Authorization method

1. Under Authorization method, click **Use LDAP to restrict access to sessions**.

2. Add a LDAP server configuration. For descriptions of each setting, see LDAP Configuration.

Server Type:

Server name:

Server port:

Username:

Password:

Directory search base:

3. Enter a **Target attribute**. This attribute value must match the **Source attribute** entry (step 12 above).
   For instance, if `email` is used as source, then an LDAP attribute with email must be used here (Example: `email`). Or if `preferred_username` is used as the source, then an LDAP attribute with the username must be used here (Example: `uid`).

4. Click **Apply**, and wait for the auth service to restart.

5. Continue with configuring OpenID Connect, step 9 above.

X.509

X.509 Configuration

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

X.509 authentication can be used to access the Assigned Sessions list as well as the MSS Administrative Console.

Steps at a glance

1. Be sure the X.509 Certificate - Setup Requirements are met.

Add a CA-signed certificate as a Kubernetes secret.

Add a CA-signed certificate to the MSS trust store.

Enable X.509.

2. Configure X.509 Settings in the MSS Administrative Console.

Choose LDAP options.

See Certificate revocations checking.

Confirm or add LDAP server.

X.509 Certificate Prerequisites

Be sure the X.509 Certificate - Setup Requirements are met before configuring X.509 in the Administrative Console.

X.509 Settings in the MSS Administrative Console

After you click X.509 as the Authentication method, click *Use LDAP to restrict access to sessions* under Authorization method.

Choose your 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.

Certificate Revocation Checking

Changes to the certificate revocation checking settings below do not take effect until the server is restarted.

> 💡 **Note**
>
> If you enable both OCSP and CRL checking, then OCSP will always be tried first. If the revocation status cannot be determined using OCSP, the validation will fall back to using CRL.

`Enable Online Certificate Status Protocol (OCSP)`

The **Online Certificate Status Protocol (OCSP)** is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. Use this option to specify Online Certificate Status Protocol (OCSP) settings that verify the TLS client certificate chain. OCSP is an alternative to Certificate Revocation Lists (CRLs), and is often implemented in a Public Key Infrastructure (PKI).

An OCSP server, also called a responder, may return a signed response signifying that the certificate specified in the request is good, revoked, or unknown. If it cannot process the request, it may return an error code.

When you check **Enable Online Certificate Status Protocol (OCSP)**, the OCSP server URL (specified in the AIA extension of a certificate) is used to check the certificate revocation status using OCSP. 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.

`Enable Certificate Revocation List (CRL)`

Use this option when the revocation status cannot be determined using OCSP.

When you check **Enable Certificate Revocation List (CRL)**, the CRL server URL (specified in the CRLDP extension of a certificate) is used to retrieve the Certificate Revocation List. 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.

LDAP Servers

Confirm the listed server or add another LDAP server, which is used to authorize access to sessions.

X.509 Certificate - 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.

X.509 authentication can be used to access the Assigned Sessions list as well as the MSS Administrative Console.

Setup requirements

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

☐ Each client that is authorized to use MSS resources must have a client certificate, such as a certificate stored on a smart card.

☐ The client certificates cannot be signed with the SHA-1 hash algorithm.

☐ The Cluster DNS must be set to a non-IP address. See the Cluster Management - Settings help.

☐ The issuer of the client certificates must be installed as a Kubernetes secret.

☐ The issuer of the client certificates must be trusted by MSS.

☐ **X.509** must be enabled in the MSS Administrative Console.

Kubernetes secret

The issuer of the client certificates must be installed as a Kubernetes secret.

`To add a CA-signed certificate as a Kubernetes secret:`

1. Install the Kubernetes command line tool (kubectl).

2. In the Administrative Console, from the drop-down menu, select **Cluster Management**. Then click **Advanced** and the **Download KubeConfig File** button to save locally.

3. In a terminal run the following command:

```
kubectl --kubeconfig <kubeconfig-file> -n mss create secret generic mss-mss-server-x509-
signing-cert --from-file=ca.crt=<ca-cert.pem>
```

> 💡 **Note**
>
> The CA-signed certificate must be in PEM format.

MSS trust store

The issuer of the client certificates must be trusted by MSS.

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

1. In the Administrative Console, open **Configure Settings - Trusted Certificates**.

2. Click **Management and Security Server**, and click **+IMPORT**.

3. Click **UPLOAD** and select the file containing the certificate to upload to the MSS Server.

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

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

Enabling X.509

X.509 must be enabled in the MSS Administrative Console.

1. First, enable OAuth.

2. Then, after the CA-signed certificate is added as a Kubernetes secret, in the MSS Administrative Console, click Configure Settings - Authentication & Authorization > **X.509**.

Continue with the X.509 Settings in the MSS Administrative Console.

SiteMinder

SiteMinder

When you integrate SiteMinder with MSS, you can leverage SiteMinder's single sign-on capabilities to authenticate users. And, you can configure additional authorization in MSS to restrict access to sessions.

MSS uses **Microsoft IIS** to integrate with SiteMinder.

Prerequisites

Before you configure SiteMinder settings in MSS, be sure these prerequisites are met.

- **A SiteMinder Web Agent is installed on Microsoft IIS.**

  The Web Agent is installed on IIS and is configured to guard web resources. Refer to the SiteMinder documentation for more information.

- **Microsoft IIS is integrated with MSS.**

  See Integrate with the IIS Reverse Proxy in the *MSS Deployment Guide* for detailed instructions.

- **Required SiteMinder JARs and configuration files.**

  MSS offers support for the SiteMinder "pure Java" agent, which requires the following SiteMinder files:

  cryptoj.jar

  smagentapi.jar

  SmHost.conf

  Refer to the SiteMinder documentation for information about these files.

SiteMinder Configuration

- **Import SiteMinder File**

Import the following SiteMinder files into MSS:

cryptoj.jar

smagentapi.jar

SmHost.conf

- **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.

- **SSO zone name (optional)**

  The name of the SiteMinder SSO security zone.

- **Shared secret (version 4)**

  The secret used by the policy server to verify the agent. The Shared secret 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.

- **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 MSS Server is configured to use authorization, use this field to specify the LDAP attribute used by the Server to perform an LDAP search request for the user's distinguished name (DN). During authorization, the MSS 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 MSS Server is *not* configured for authorization, any value entered into this field is ignored.

Micro Focus Advanced Authentication

Micro Focus Advanced Authentication

Advanced Authentication™ is a separate Micro Focus product that provides a multi-factor authentication solution to protect your sensitive data by using a chain of authentication methods.

MSS provides an optional Add-on to use the multi-factor capability with Micro Focus Windows emulation products.

Prerequisites

To enable the Advanced Authentication option, these products must be installed:

- ☐ MSS

- ☐ the Micro Focus Advanced Authentication product

- ☐ the MSS Advanced Authentication *Add-on* product

> ♀ **Note**
>
> When using Micro Focus Windows emulation clients -- Reflection Desktop, InfoConnect Desktop, and Rumba+ Desktop -- **Centralized Management** *must* be enabled

In brief, you must

Step 1. Install and configure the Micro Focus Advanced Authentication product.

Step 2. Download the MSS Advanced Authentication Add-on activation file.

Step 3. Configure MSS to use Advanced Authentication.

Step 4. Trust the MSS endpoint on the Advanced Authentication server.

Detailed steps

Step 1. Install and configure the Micro Focus Advanced Authentication product

You can configure a chain of multiple authentication methods by using Micro Focus Advanced Authentication.

Refer to the Advanced Authentication Documentation to install and configure the product.

When configuring the Advanced Authentication product to work with Management and Security Server, these steps are required.

1. **Install** Micro Focus Advanced Authentication Server, noting the server name (or IP address).
2. Configure the authentication **Methods** you wish to use for MSS authentication.

   Options include LDAP password, Email one-time password (OTP), Time-limited one-time password (TOTP), Smartphone, and more.
3. Create a **Chain**.

   Add your preferred methods in the order you want the user to encounter them as they log in.
4. Configure a **customized Event** and name it **MSS**.

   The event name must match the hard-coded setting in Management and Security Server; thus, the name must be MSS.

   A different name will not work.

Step 2. Download the MSS Advanced Authentication Add-on activation file

After you obtain the separate license for **Host Access Management and Security Server - Advanced Authentication Add-On**, go to the **Micro Focus download page** (where you downloaded Management and Security Server).

Download the **activation file**, named `activation.advanced_authentication-<version>.jaw`.

Step 3. Configure MSS to use Advanced Authentication

```
Enable Advanced Authentication
```

1. Log in to **Management and Security Server** (MSS).
2. Enable OAuth.
3. Open the Administrative Console to **Configure Settings - Product Activation**.
4. Click **ACTIVATE NEW**.
5. Browse to and click the activation file you downloaded earlier:

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

The file is installed and added to the list of **Currently Installed** products.

```
Configure Micro Focus Advanced Authentication
```

1. In MSS, open **Configure Settings - Authentication & Authorization**.

2. Select **Micro Focus Advanced Authentication** as the authentication method.

   If desired, select **LDAP** as the authorization method.

3. Enter the **Server** name or IP address of the Advanced Authentication server *without* a protocol. (That is, omit `https://`.)

   For example, enter `myserver.mycompany.com`.

4. Enter the **Port** (443 by default).

5. Specify the **Search Repositories**, separated by commas, to use on the Advanced Authentication server.

   Users are defined in the search repositories.

6. Click **IMPORT CERTIFICATE**. A message displays to confirm whether the server is trusted.

> ♀ **Note**
>
> • If you are presented with multiple certificates to import, it is best to choose the CA certificate.
>
> • If you see, **"Failed to retrieve the certificate chain for the server,"** be sure the server name is entered correctly. The host name must match the name in the server certificate.

7. By default, the **Verify server identity** option checks to make sure the host name is matched with the certificate from the Advanced Authentication server.

> ♀ **Note**
>
> When present, the SAN (Subject Alternative Name) in the Advanced Authentication server certificate is used, not the common name.

> ⚠ **Caution**
>
> Clearing the **Verify server identity** check box is a security risk. Do not disable this feature unless you understand the risk.

8. With **Verify server identity** checked, click **TEST CONNECTION**.

   The test is successful when the entry for the Advanced Authentication server is valid, and the server address is in the certificate.

   • If the test connection fails, troubleshoot as follows:

If you see, **Advanced Authentication Failure The hostname you entered does not match the server certificate**, check the certificate in the **Configure Settings - Trusted Certificates** list.

Then, return to Configure Settings - Authentication & Authorization and correct the server name to *match the SAN* in the certificate.

For instance, a mismatch occurs when you enter the IP address, and the IP address is not in the certificate.

- For more information, see `trace.0.log`. By default, `trace.0.log` is located in `\ProgramData\Micro Focus\MSS\MSSData\log`.

9. When **TEST CONNECTION** succeeds, click **Apply** to save the changes.

> 💡 **Note**
>
> If the first authentication request from MSS to the Advanced Authentication server fails, restart the MSS server to enable subsequent requests to succeed.
>
> If Cluster DNS Name is updated after Micro Focus Advanced Authentication is configured, configuation will need to be re-applied.

Step 4. Trust the MSS endpoint on the Advanced Authentication server

1. Log into the Advanced Authentication server Admin Console.

2. Select **Endpoints** on the left menu.

3. Select the MSS endpoint created for your server.

4. Toggle "Is trusted" from **OFF** to **ON**.

5. Click **Save**.

6. Log in to the MSS Admin Console.

7. Go to **Cluster Management**.

8. Select **Services** and redeploy **mss-auth-service**.

SAML Authentication

SAML Authentication

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

This release supports **SAML v2.0 Web Browser SSO Profile** for Host Access for the Cloud 2.4 or higher.

Overview of steps

Configuring MSS to use SAML is a multi-step process. In general, you must:

☐ Configure MSS as a SAML service provider.

☐ Download or access the service provider's metadata from MSS.

☐ Export the service provider's metadata into the identity provider.

☐ Map the identifier source.

☐ Configure the SAML whitelist.

☐ Configure LDAP, when used for authorization.

* **identity provider:** the server that issues SAML assertions and performs authentication on behalf of the service provider.

** **service provider:** the web server from which you access information or services. MSS acts as the service provider.

Detailed steps

Follow the SAML Configuration steps.

SAML Configuration Steps

Be sure to read the **Important** information, **Caution**, and **Notes** as you configure MSS to use SAML.

> 🔥 **Important**
>
> The SAML authentication scheme in MSS relies on HTTP session cookies for proper operation. Consistent use of fully-qualified DNS names across all SAML entities is strongly recommended. In particular, any clients of MSS should be configured to access MSS using the same DNS name that is used for the Assertion Consumer Service prefix URL.

Follow the steps in these sections.

Configure MSS as a SAML Service Provider

These steps are required before you can access 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 prefix URL value *must* end with the MSS server's web application context. For example, the default context is `/mss` .
>
> If you encounter an error message, be sure this requirement is met.

4. Click **APPLY**.

   The **HTTP endpoint** 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**
>
> MSS uses the cluster certificate to sign the SAML requests. If the cluster certificate is changed, repeat the steps to **Access** the service provider (MSS) metadata and **EXPORT** it to the identity provider.

6. Access the service provider (MSS) metadata.

   Use 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:

a. Upload the service provider metadata to the identity provider.

b. Configure the identity provider to trust MSS (the service provider).

Advanced SAML Service Provider Settings

Set the values for the following properties in the Cluster Management > Services view. For instructions, see Setting Advanced Properties.

- `saml.max.authentication.lifetime`

  Default is **86400** (seconds), which equals 24 hours. By default, the SAML client will accept assertions based on a previous authentication for 24 hours.

  > 💡 **Note**
  >
  > There are two types of timeouts on the identity provider (IdP) side:
  >
  > • session timeout, based on the last login timestamp
  >
  > • idle timeout, based on the last user's action timestamp

  To prevent user sessions from timing out unexpectedly, use one of the recommended values for `saml.max.authentication.lifetime`.

  Recommended Values:

Platform	saml.max.authentication.lifetime (seconds)
ADFS	28800
Okta	2592000
Azure	2592000

- `saml.wants.assertions.signed`

  Default is **true**. By default, assertions are signed, but this property can be disabled by setting it to false.

- `saml.path.parameter.callback.url.enabled`

  Default is **true**. Set to false to use query parameter in the callback url.

Identity Mapping

The SAML assertion provides values that can be used as the source for the user identifier. When LDAP authorization is enabled, you could use the LDAP user identifier.

Choose your preferred sources to identify and authorize each user.

User identifier source

Choose a value from the SAML assertion. *Note:* The user identifier appears in the user interface.

- **Assertion subject**. Use the SAML assertion's **Subject name identifier** as the user identifier.
- **Assertion attribute**. Enter a SAML assertion **attribute name** to use as the source for the user identifier.

Distinguished name source (for LDAP authorization)

Choose whether to use the LDAP source or a value from the SAML assertion.

- **LDAP**. Use LDAP when the user's identifier is unique within LDAP.
- **Assertion subject**. Use the SAML assertion's **Subject name identifier** as the user's distinguished name for LDAP authorization.
- **Assertion attribute**. Enter a SAML assertion **attribute name** to use as the source for the user's distinguished name for LDAP authorization.

SAML whitelist

MSS uses a whitelist composed of trusted host names to mitigate a potential security vulnerability when using SAML authentication. By default, the SAML whitelist is enabled and contains the registered Host Access for the Cloud session servers and the MSS host itself.

> ♀ **Note**
>
> The SAML whitelist is restrictive by default. That is, if a user specifies a valid host name in the URL — but that host name is not in the whitelist — the end-user browser application will not be able to use SAML.
>
> For example, the user may specify a numeric IP address in the browser, but by default, numeric IPs are not whitelisted. When an untrusted host name is specified in the browser URL, an HTTP 403 error is returned, and the browser content indicates that a technical error has occurred. The Trace log file will also contain a Warning message indicating that a request was received that is "not from a host in the SAML whitelist."

To configure the SAML whitelist:

1. Check **Enable SAML whitelist** (the default).

   For troubleshooting purposes, the SAML whitelist can be disabled.

2. Enter **alternative host names** to include in the SAML whitelist.

   Specify any alternate host names for the SAML client application hosts, such as a short host name, a fully-qualified DNS name, or a numeric IP address. Separate the host names with a space.

LDAP Servers

Verify or edit the configuration of your LDAP Servers.

Troubleshooting SAML setup

Issue: **Unable to log in or authenticate**

Look for error messages in the MSS trace log: `\MSS\MSSData\log\trace.<n>.log`.

If you see, "*Authentication issue instant is too old or in the future*," the saml token has expired.

Resolution:

1. Close all the browser instances and try to log in again. This action creates a new saml token.

2. Update the `saml.max.authentication.lifetime`, according to the recommended values in the Advanced SAML Service Provider Settings.

Product Activation

Product Activation

View the list of activation files (license entitlement files) for currently installed MSS add-on products and emulator clients that are centrally managed by Management and Security Server.

The activation files enable communication with MSS. Use this panel to install the activation files for MSS add-on products or other emulators.

Install the activation file for an additional product

Complete the activation

> ♀ **Note**
>
> If you see this message,
> "`Activation files installed on the Management and Security Server do not match those available to emulator client sessions,`" resolve the conflict either by
>
> • manually copying the activation files installed in the `WEB-INF/lib/modules` folder of the MSS Server to the `ex/modules` folder of the emulator client so the contents of both locations match, or by
>
> • reinstalling the file using **ACTIVATE NEW** on the **Configure Settings - Product Activation** panel.

Install an Activation File for an Additional Product

1. After purchasing an add-on product or another emulator, you will receive information about downloading the product as an **activation file**, which has this format:

   `activation.<product_name-version>.jaw`

2. Download the activation file and note the download destination.

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

4. Click **ACTIVATE NEW** and browse to the activation file for the product you want to install:

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

5. Click the file. The new product is added to the Product list.

   If you uploaded a product evaluation file, open the column chooser ⊞ to view the Expiration date.

6. Restart your browser to ensure that the MSS 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. Continue with the configuration settings for the activated product.

   Be sure to Complete the activation.

> ⚠️ **Caution**
>
> When upgrading an add-on product or emulator, add the new activation file and be sure to remove the older one.

Complete the Activation

After the activation file is installed, further configuration may be required to activate your add-on product. Follow the steps for your product (listed on the right).

Security Proxy Server

1. Copy the activation file, `activation.security_proxy-14.0.0.<n>.jaw` , into the

   `/securityproxy/lib/modules` folder on *each* machine where Security Proxy Server is installed.

2. Start the **Security Proxy Server**.

Automated Sign-On for Mainframe

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

2. Check **Enable Automated Sign-On for Mainframe (for z/OS systems)**, and enter the required information. See the Automated Sign-On Help for assistance.

3. See the Automated Sign-on for Mainframe - Administrator Guide for the required mainframe configuration.

MSS Automated Sign-On for Host Access

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

2. Check **Enable MSS Automated Sign-On for Host Access**, and enter the required information. See the Automated Sign-On Help for assistance.

   When Automatic Sign-On is enabled via the Admin Console, it will be automatically scaled to one instance in a cluster.

Micro Focus Advanced Authentication

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

2. Click **Micro Focus Advanced Authentication**, and enter the required information. See Help for assistance.

Automated Sign-On

Automated Sign-On

Automated Sign-On enables an end user to automatically log on to a host application using a Micro Focus terminal emulation client. A separate license and additional configuration is required.

Settings must be configured in different locations:

Management and Security Server (MSS) — to enable the service, secure the server connections, and manage user access

the terminal emulation client — to create the login macro and configure the client

the host — to support the use of one-time passwords

Be sure to configure the settings for your host type. Others steps are required before enabling Automated Sign-On.

To enable Automated Sign-On

Check the box to enable the Automated Sign-On settings for your host type.

If the check box is not visible or is disabled, the activation file needs to be installed. See Install an Activation File for an Additional Product.

☐ **Enable Automated Sign-On for Mainframe** (for z/OS systems)

☐ **Enable MSS Automated Sign-On for Host Access**

> 💡 **Note**
>
> An LDAP directory is required to authorize Automated Sign-On capabilities for sessions.

Configure the settings for your host type

- *For z/OS*, refer to the Automated Sign-on for Mainframe - Administrator Guide for the client and z/OS configuration.

- *For other (non-zOS) host types*, refer to the technical reference, Configuring MSS Automated Sign-On for Host Access.

DCAS Servers (z/OS systems)

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, edit, or delete a DCAS server, test the connection, or set a preferred DCAS server.

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 MSS 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 Server to the DCAS server.

- **Use Management and Security Server certificate**

  This option uses the MSS 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. Click **Upload**. Select the keystore file to upload to the Management and Security Server. 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**.

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 MSS Server to DCAS.

Test Connection

Click this button to test the connection between the MSS 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 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.

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.

More information

Secondary LDAP directory

Search filter used with secondary LDAP directory

Check the client settings

Secondary LDAP directory

User names 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

Select the type of LDAP server that is used to store user names. The options on this panel change depending on the LDAP server type you select. If you do not see your specific LDAP server in the list, select **Generic LDAP Compliant Directory Server (RFC 2256)**.

Security options

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

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

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

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

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

Server name

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

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

Windows Active Directory - DNS domain. When Windows Active Directory is selected (without Kerberos), you have the option to use a DNS domain instead of a specific domain controller. No further configuration is required. For more information, see LDAP Configuration.

Server port

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

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

Username and Password

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

> 💡 **Note**
>
> The username must uniquely identify the user in the directory. The syntax depends on the type of LDAP server you are using.
>
> - For **Windows Active Directory** with **Plain Text**, enter
>
>   **NetBIOS domain\sAMAccountName** (such as `exampledomain\username`)
>
>   **userPrincipalName** (such as `username@exampledomain.com`)
>
>   or
>
>   **distinguished name** (such as `uid=examplename,DC=examplecorp,DC=com`).
> - For any **other LDAP** server type, enter the **distinguished name** (such as `uid=examplename,DC=examplecorp,DC=com`).
>
> If this account password changes, be sure to update the account password here and apply the new settings. To avoid this problem, you may wish to set up an account that is not subject to automatic password aging policies, or that cannot be changed by other administrators without notice.

Search Base

Directory search base. Enter the distinguished name of the node in the directory tree you want to use as the base for MSS Server search operations.

Examples: `DC=my_corp`,`DC=com`, or `o=my_corp.com`

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

Certificate

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

LDAP Connection

Click **TEST CONNECTION** to verify that the secondary LDAP server can connect to the MSS Server. If the test fails, consult the logs to resolve the issue.

Search filter used with secondary LDAP directory

Choose and configure a method for obtaining a user's name on the host computer from the secondary LDAP directory. See Search filter used with secondary LDAP directory.

More information

DCAS Servers (for z/OS systems)

User Principal Name (UPN)

Check the client and host settings

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 user's host name or as an element in a search filter for a secondary LDAP directory.

A UPN generally takes the form of an email address, such as `auser@domain.com`. Enter the name of the LDAP attribute in the authenticating directory that contains the UPN value.

To determine the user's name on the host computer, MSS looks at the user's UPN value in LDAP. Then the portion before the `@` sign is used either

- as the user's host name 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 user's name on the host of "`auser`" (the portion before the `@`).

  -- or --

- as an element in a search filter for a secondary LDAP directory.

More information

DCAS Servers (for z/OS systems)

Secondary LDAP directory

Search filter used with secondary LDAP directory

Check the client and host settings

Search filter used with secondary LDAP directory

Choose the method for obtaining user names 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 user's name.

  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-On can **use a value of another attribute in the authenticating directory** as the value in the search filter to find the object in the *secondary* LDAP directory containing the user's name.

  Enter the attributes for both the *authenticating* and the *secondary* LDAP directories.

More information

DCAS Servers (for z/OS systems)

User Principal Name (UPN)

Secondary LDAP directory

Check the client and host settings

Configure the Client and Host Settings

In addition to the settings in MSS, your emulation client and host must be configured for Automated Sign-On. Then, you can assign those sessions to users.

Configure the client

Your emulator client session needs:

Centralized Management

a recorded login macro

See your client's product documentation for details. See also the technical reference, Configuring MSS Automated Sign-On for Host Access.

Configure the host

Your host needs to be configured to support the use of one-time password requests.

- *For z/OS systems*, see the Configuration Workflow in the *Automated Sign-on for Mainframe - Administrator Guide*.

- *For other host systems*, work with your Micro Focus sales representative to get more information about the MSS Automated Sign-On for Host Access (ASO) protocol you must implement on your specific host system.

  The host must be adapted to

use `mutual TLS` to communicate with the ASO service

process one-time passwords issued by users during logon and validate them with the ASO service

More information

- Automated Sign-On for Mainframe - Administrator Guide
- Configuring MSS Automated Sign-On for Host Access

Logging

Logging

Management and Security Server stores logs for the MSS microservices, webapps, and other components.

Viewing log files

To view or download log files:

1. Log in to the MSS Admin Console at `https://hostname/adminconsole` .

2. From the drop-down menu, click Cluster Management.

3. Click Services, and find the service of interest.

4. Click that service to view the application instances (pods) across the cluster.

5. Click `...` and then click either

View Recent Logs - to view a "tail" of the logs' last 500 entries in a browser window

Download Logs - to download the entirety of all the log files

Setting log levels

The logging levels for the MSS server and for the Auth Service are set in different locations.

For the MSS server:

1. In the MSS Administrative Console, open Configure Settings - Logging.

2. For each service, set the level of logging for users' session activity and system configuration activity. You can configure the logs to

Log errors and informational messages

Log only errors

or, Disable the log altogether

For the Auth Service:

1. Open Cluster Management from the MSS Administrative Console drop-down.

2. Click Services and locate `mss-auth-service` .

3. Click `...` Edit Properties.

4. Enter this **Key**: `authsvc.logging.level`

5. Enter the **Value** for the level of logging you wish to track:

ERROR - designates error events that might still allow the application to continue running.

WARN - designates potentially harmful situations.

INFO - designates informational messages that highlight the progress of the application at coarse-grained level.

DEBUG - designates fine-grained informational events that are most useful to debug an application.

Migration

Migration

You can migrate your data from an existing install4j deployment to a new container-based deployment.

How can I migrate my data?

Use the provided migration tool to export data from your previous installation into a zip file. Then import the data into the new installation. See the detailed steps.

What data can I migrate?

Data that IS migrated by the tool	Data that is NOT migrated
session configurations	activation files
session assignments	kerberos settings
metering configuration	metering report data
authentication configuration	security proxy configuration
HACloud user preferences	passwords
keystores	
TIDM database	
session server extensions	

> 💡 **Note**
>
> Passwords are not migrated. For example the MSS Admin password will remain the same before and after migration.

What's required?

The existing data must be on a current major release of your product: MSS 12.8+, HACloud 2.7+, or RWeb 13.2+.

OS administrative privileges to run the migration tool.

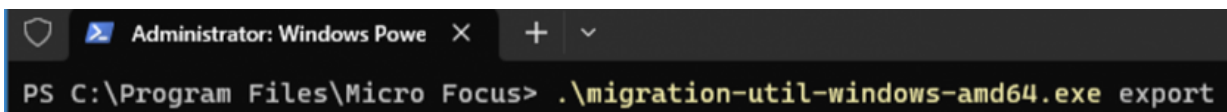A new single-node installation to import the data.

Detailed Migration Steps

To migrate your existing data:

1. In the new installation, open Administrative Console > Configure Settings > Migration.

2. **Download** the appropriate migration utility for your platform (Windows or Linux).

3. Run the utility as Administrator (Windows) or sudo/root (Linux) on the previous installation:

   a. Open a command prompt or terminal.

   b. Navigate to the installation directory of your previous installation. The default paths are:

   - **Windows** `C:\Program Files\Micro Focus\`

   - **Linux** `/usr/local/microfocus/` or `/opt/microfocus/`

   c. Run the utility. For example, on Windows:

   The result is a zip file that contains data from MSS, HACloud, and RWeb, depending on what was installed.

   d. Save the zip file to a location that is navigable from the new installation.

4. Return to Admin Console > Configure Settings > Migration and click **Import**. Navigate to and click your saved zip file.

   When successful, you'll see this message: "Settings Imported. Please redeploy the MSS server now."

5. **After importing the data**, you must redeploy the MSS server.

   a. In the MSS Administrative Console, open **Cluster Management** from the top left drop-down menu.

   b. Open **Services** and locate `mss-mss-server`.

   c. On the far right, click ⋯ **Redeploy All**.

   d. Wait for the service to redeploy. Then refresh your browser. (Or, click Administrative Console in the drop-down menu.)

   You will be prompted to log in again.

When complete, check to be sure the supported data was migrated, and that users can launch their sessions.

Run Reports

Run Reports

Reports provide information about Management and Security Server components and products.

View the activity for the features you are using.

Usage Metering Reports

Security Proxy Server Reports

Assigned Access Reports

Credential Store Reports (Reflection for the Web)

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.

In the Metering Console, click the report of choice. Then on the report page, click Help for more information.

Available reports:

Current activity

Usage by Attribute

Usage by User or Machine

All Usage Activity

Host Connections

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 Product Activation.

After you install the Security Proxy server, configure sessions to use the Security Proxy.

To view a report of the Security Proxy server activity:

1. Select a **Report Type**

2. Select a **Security proxy server**

3. Click **SHOW REPORT**.

Report types:

    Current user activity

    Connections per proxy server

> 💡 **Note**
>
> See the Security Proxy Server technical reference for instructions to set and view Security Proxy logs.

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: When **Resolve client machine DNS name** is `off` (the default), this column shows the client's IP address and port number. When **client name resolution** is `on`, the client's DNS name and port are displayed.

Destination: When **Resolve remote host DNS name** is `on` (the default), this column shows the destination host's DNS name and port number. When **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.

Connections per proxy server

This report shows the total current connections of all security proxy servers.

- **Security proxy address:** The security proxy server and its associated port.

- **Security proxy current connections:** Tthe count of current connections for that server.

> 💡 **Note**
>
> A single FTP session connecting through a security proxy server produces a count of three separate connections.

Assigned Access Reports

Use this report to view your assigned sessions. You can filter by **Users and Groups** or by **Sessions**.

Users and Groups

This report lists all users and groups and the sessions that are assigned to them. The report also indicates whether a user or group has access to the MSS Administrative Console.

Enter a **Search field** string to limit the report to all users and groups that include the search string. The search is not case-sensitive.

Click **SHOW REPORT**.

Sessions

This report lists the sessions and the users and groups that are assigned to that session. Individual members of a group are not listed.

Enter a **Search field** string to limit the report to all sessions that include the search string. The search is not case-sensitive.

Click **SHOW REPORT**.

Credential Store Reports - Reflection for the Web

Credential Store Reports are available *only* for **Reflection for the Web**. You can run reports to see the **Credential Store Users** and to the **Usage History** (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.

The **Users** report displays the count of credential store users. The **Show list of users** report includes 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 are empty when credential store logging is disabled. To enable logging for the Credential store, go to **Configure Settings > Logging**.

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.

Usage History- 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.

Usage History - 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.

Other Applications

Other Applications

Some features no longer require configuration settings in the product UI. They either run automatically or can be set separately.

Metering

Security Proxy Server

Terminal ID Manager

Setting Advanced Properties

Metering

The Metering Server is a component of Host Access Management and Security Server (MSS) that enables you to view the activity of users who open sessions and connect to your hosts. The Metering server and the clients to be metered must be configured.

High Availability

The Metering server is always installed and enabled with your product. Use multiple nodes to provide high availability. A minimum of three nodes is recommended for high availability. To configure a cluster, see the **Clustering** topic in the MSS Deployment Guide.

When multiple nodes are clustered, emulation clients can continue to function even if a node becomes unavailable. Clustering and replication of metering license data is backed by a database.

The Metering Console

The Metering Console is used to configure Metering and to run reports. To open the Metering Console:

1. From the MSS Administrative Console drop-down menu, click Cluster Management.

2. Click Services.

3. Next to the `mss-metering` service, notice the two links:

- **Metering**: `https://hostname/meter.html`

Use this link to View Reports.

- **Metering Administration**: `https://hostname/meter/AdminStart.html`

This link opens the Metering Console to configure license pools, server settings, and run reports. Open Help for assistance.

When prompted for a password, enter the MSS administrative password, which is shared with metering administration. The default password is `admin`. A different password can be set for other users to view Reports. See the Metering Console help.

Use the Metering Console Help for configuration details:

```
 - License Pool settings
 - Server settings
 - Client setup
```

Once configuration is complete and users begin to access metered sessions, you can run reports to view the data.

Security Proxy Server

The Security Proxy Server provides token-based access control and encrypted network traffic to and from user workstations. The Security Proxy can be used by Reflection Desktop and Reflection for the Web.

Enabling the Security Proxy Server

For Reflection Desktop. The Security Proxy is enabled by installing an activation file, which is available for download and is licensed separately. To enable:

1. In the MSS Administrative Console, click Configure Settings - Product Activation.
2. Click ACTIVATE NEW and browse to and click the activation file for the security proxy:

   `activation.security_proxy-<version>.jaw`

   The Security Proxy is added to the Product list.

For Reflection for the Web. The Security Proxy entitlement is included in the Reflection for the Web activation file.

Configuring the Security Proxy

The Cluster Certificate is automatically shared across all nodes in a cluster, and is used as the identity for the Security Proxy. You must define and add the Cluster Certificate, which will be used by the Security Proxy.

> 💡 **Note**
>
> The Security Proxy Wizard, previously used to managed certificates, is no longer used for configuration.

To define and add the Cluster Certificate:

1. Log in to the MSS Administrative Console at `https://hostname/adminconsole` .

2. From the drop-down menu, click **Cluster Management**.

3. Click **Settings**, and expand the Certificate and Private Key panels.

4. Click Import File and navigate to your certificate and key.

5. Select and import the files. Or, you can drag and drop the certificate and key files into the fields.

   To verify: first close and re-open your web browser; then access the session server and note the updated certificate that is reported by the browser's site information.

6. Redeploy the Security Proxy service:

   a. In the **Cluster Management** console, click **Services**.

   b. Next to the `mss-security-proxy` service, click ⋯ Redeploy All.

> 🔥 **Important**
>
> Be aware that end users may be affected when a service is redeployed.

Advanced Configuration

You can customize your Security Proxy installation by editing the Security Proxy service properties. Work with Customer Support to set custom properties, such as specifying non-default values for the TLS version, Crypto Suites, and OCSP.

1. In the **Cluster Management** console, click **Services**.

2. Next to the `mss-security-proxy` service, click ⋯ Scale.

3. You must **explicitly scale** the number of instances needed.

> 💡 **Note**
>
> By default, the Security Proxy is set to zero (0) instances because it is capable of handling a high volume of connections, and requires resource allocation that is commensurate to its performance.

4. Next to the `mss-security-proxy` service, click ⋯ Edit Properties.

5. Enter the Key and Value for each custom property.

6. In some cases, you may be asked to Redeploy a service after editing the properties.

   Next to the `mss-security-proxy` service, click ⋯ Redeploy All.

> 🔥 **Important**
>
> Be aware that end users may be affected when a service is redeployed.

Setting the Logging Level

To set logging properties for the Security Proxy Server:

1. Open the **Cluster Management** console, and click **Services**.

2. Next to the `mss-security-proxy` service, click ⋯ Edit Properties.

3. For detailed logging, add this key/value pair.

Key: `logging.level.root`

Value: `DEBUG`

Other values: `INFO`, `WARN`, `SEVERE`

To view the Security Proxy logs:

1. From the MSS Administrative Console drop-down menu, open the Cluster Management console.

2. On the Services page, click `mss-security-proxy`.

3. Click `•••` and View Recent Logs or Download Logs.

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.

To configure the Security Proxy to run in FIPS-approved mode, edit the `mss-security-proxy` service properties with this key/value pair:

Key: `fipsApprovedMode`

Value: `on`

For detailed steps to set properties for the Security Proxy service, see Advanced Configuration.

Running Reports

After you configure sessions to use the Security Proxy, you can run reports to view the current user activity and the connections per Security Proxy server.

See Run Reports - Security Proxy Server.

Terminal ID Manager

Terminal ID Manager enables you to conserve terminal ID resources by providing IDs to client applications at runtime. Terminal ID Manager is an MSS Add-on product that is installed and enabled by default; however, it does require a separate activation file.

Use the **Terminal ID Manager Console** to set up and manage terminal IDs. To log in, go to `https://hostname/tidm/`. If you are not able to log in to the console, the Terminal ID Manager needs to be activated.

Refer to the Terminal ID Manager Guide for the complete set of configuration steps.

Setting Advanced Properties

You may occasionally need to change or add properties to your product services. Properties are set in the Cluster Management console.

Follow these steps:

1. Log in to the MSS Administrative Console at `https://hostname/adminconsole` .

2. Click Cluster Management from the drop-down menu.
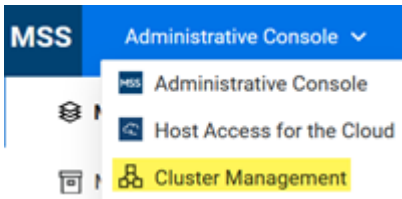
3. Click Services.

4. Next to the service of interest, click ••• Edit Properties.

5. Add or edit the Key/Value pair accordingly.

6. For the same service, click ••• Redeploy All.

> 💡 **Note**
>
> Be aware that end users may be affected when redeploying a service.

Technical References

Technical References

Configuring MSS Automated Sign-On for Host Access

Configuring MSS Automated Sign-On for Host Access

MSS Automated Sign-On for Host Access (ASO) enables an end user to automatically log on to a host application using a terminal emulation client and a one-time password (OTP). Automated Sign-On for Host Access is designed for **non-z/OS** systems.

The one-time password is obtained from the ASO service. It is time-limited and takes the place of the user's usual password. Use of a one-time password helps to increase the security of the host system because OTPs are short-lived, randomly generated, and can be used only once, making it more difficult to compromise a user's identity.

Automated Sign-On (ASO) settings need to be configured in different locations:

> **MSS**: Edit settings on the server and in the Administrative Console.

> **the client:** Create an automated login macro.

> **the host:** Enable the use of one-time passwords.

> 💡 **Note**
>
> If you are using a **z/OS system**, refer to the Automated Sign-On for Mainframe - Administrator Guide to leverage the existing z/OS functionalities of DCAS and RACF.

Prerequisites

a separate license for MSS Automated Sign-On for Host Access Add-On product

an LDAP server for authorization

a Micro Focus terminal emulation client that supports ASO:

Reflection Desktop 18.0 or higher

InfoConnect Desktop 18.0 or higher

Host Access for the Cloud 3.0 or higher

Steps at a glance:

Integrate the ASO protocol into your host system.

Install the activation file.

Enable the ASO service.

Import the Host CA Certificate.

Configure ASO in the MSS Administrative Console.

Configure the client to use Automated Sign-On.

Assign access to the automated sign-on sessions.

1. Integrate the ASO protocol into your host system

Use of MSS Automated Sign-On for Host Access requires **custom programming on the host computer** before you begin configuring.

Work with your Micro Focus sales representative to learn about the MSS Automated Sign-On for Host Access (ASO) protocol that you must implement on your specific host system. The host must be adapted to process one-time passwords issued by users during logon and validate them with the ASO service.

2. Install the activation file

The activation file for Automated Sign-On for Host Access is

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

You can install the activation file while installing MSS or via the MSS Administrative Console.

To install while installing MSS, see the MSS Deployment Guide.

To use the MSS Administrative Console, see Installing an Activation File for an Additional Product.

3. Enable the ASO service on the MSS server

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

2. Check **Enable MSS Automated Sign-On for Host Access**. If the check box is disabled, the activation file needs to be installed (step #2).

   When Automatic Sign-On is enabled:

it will be automatically scaled to one instance in a cluster.

you must select a certificate (see step #4).

other settings become available.

4. Import the Host CA Certificate

To establish trust with the host, click IMPORT CERTIFICATE and choose a CA certificate.

> ♀ **Note**
>
> The certificate must be in PEM format.

5. Configure ASO in the MSS Administrative Console

Configure the LDAP directory settings that are used to retrieve user names for Automated Sign-On to the host.

- Configure a secondary LDAP directory when user names are stored in a directory that is different from the authenticating directory.
  Note: When secondary LDAP directory is enabled, other settings become available.

- Specify a User Principal Name (UPN) when the UPN attribute in the authenticating directory starts with the user name. Example: **username**@domain.com

- *Note:* When assigning ASO capabilities to sessions, you may specify an LDAP attribute from either directory as the source of the user name.

6. Configure the client to use Automated Sign-On

1. Your Desktop emulator session must either be configured for centralized management or be launched from the Assigned Sessions page.

2. In the MSS Administrative Console - Manage Settings, **add a session** that you want to make available for automatic login.

3. In the launched session, **record and edit a login macro**.

   The steps to create a macro vary based on your specific emulator and session type. Refer to your emulator client's product documentation.

4. **Save** the session.

7. Assign Access

After the client session is configured with an automated sign-on macro, you are ready to assign those sessions to users. See Search & Assign.

Be sure to click **EDIT** and set the Source of user name on host computer.

Legal Notice